Contents

Part I: Introduction

1 History of finite fields . . . 2
1.1 Finite fields in the 18-th and 19-th centuries *Roderick Gow* . . . 2
1.1.1 Introduction . . . 2
1.1.2 Early anticipations of finite fields . . . 3
1.1.3 Gauss's Disquisitiones Arithmeticae . . . 3
1.1.4 Gauss's Disquisitiones Generales de Congruentiis . . . 4
1.1.5 Galois's Sur la théorie des nombres . . . 5
1.1.6 Serret's Cours d'algèbre supérieure . . . 7
1.1.7 Contributions of Schönemann and Dedekind . . . 8
1.1.8 Moore's characterization of abstract finite fields . . . 9
1.1.9 Later developments . . . 9
2 Introduction to finite fields . . . 11
2.1 Basic properties of finite fields *Gary L. Mullen and Daniel Panario* . . . 11
2.1.1 Basic definitions . . . 11
2.1.2 Fundamental properties of finite fields . . . 12
2.1.3 Extension fields . . . 16
2.1.4 Trace and norm functions . . . 18
2.1.5 Bases . . . 19
2.1.6 Linearized polynomials . . . 21
2.1.7 Miscellaneous results . . . 22
2.1.7.1 The finite field polynomial Φ function . . . 22
2.1.7.2 Cyclotomic polynomials . . . 22
2.1.7.3 Lagrange interpolation . . . 24
2.1.7.4 Discriminants . . . 24
2.1.7.5 Jacobi logarithms . . . 25
2.1.7.6 Field-like structures . . . 25
2.1.7.7 Galois rings . . . 26
2.1.8 Finite field related books . . . 29
2.1.8.1 Textbooks . . . 29
2.1.8.2 Finite field theory . . . 29
2.1.8.3 Applications . . . 29
2.1.8.4 Algorithms . . . 29
2.1.8.5 Conference proceedings . . . 30
2.2 Tables *David Thomson* . . . 30
2.2.1 Low-weight irreducible and primitive polynomials . . . 30
2.2.2 Low-complexity normal bases . . . 35
2.2.2.1 Exhaustive search for low complexity normal bases . . . 36
2.2.2.2 Minimum type of a Gauss period admitting a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ . . . 38
2.2.2.3 Minimum-known complexity of a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, $n \geq 40$ . . . 39
2.2.3 Resources and Standards . . . 44

Part II: Theoretical Properties

3 Irreducible polynomials . . . 49
3.1 Counting irreducible polynomials *Joseph L.Yucas* . . . 49
3.1.1 Prescribed trace or norm . . . 50
3.1.2 Prescribed coefficients over the binary field . . . 51
3.1.3 Self-reciprocal polynomials . . . 52
3.1.4 Compositions of powers . . . 53
3.1.5 Translation invariant polynomials . . . 54
3.1.6 Normal replicators . . . 54
3.2 Construction of irreducibles *Melsik Kyuregyan* . . . 55
3.2.1 Construction by composition . . . 55
3.2.2 Recursive constructions . . . 59
3.3 Conditions for reducible polynomials *Daniel Panario* . . . 62
3.3.1 Composite polynomials . . . 62
3.3.2 Swan-type theorems . . . 63
3.4 Weights of irreducible polynomials *Omran Ahmadi* . . . 66
3.4.1 Basic definitions . . . 66
3.4.2 Existence results . . . 66
3.4.3 Conjectures . . . 68
3.5 Prescribed coefficients *Stephen D. Cohen* . . . 69
3.5.1 One prescribed coefficient . . . 70
3.5.2 Prescribed trace and norm . . . 71
3.5.3 More prescribed coefficients . . . 72
3.5.4 Further exact expressions . . . 73
3.6 Multivariate polynomials *Xiang-dong Hou* . . . 75
3.6.1 Counting formulas . . . 76
3.6.2 Asymptotic formulas . . . 76
3.6.3 Results for the vector degree . . . 77
3.6.4 Indecomposable polynomials and irreducible polynomials . . . 79
3.6.5 Algorithms for the gcd of multivariate polynomials . . . 80
4 Primitive polynomials . . . 82
4.1 Introduction to primitive polynomials *Gary L. Mullen and Daniel Panario* 82
4.2 Prescribed coefficients *Stephen D. Cohen* . . . 85
4.2.1 Approaches to results on prescribed coefficients . . . 86
4.2.2 Existence theorems for primitive polynomials . . . 87
4.2.3 Existence theorems for primitive normal polynomials . . . 88
4.3 Weights of primitive polynomials *Stephen D. Cohen* . . . 90
4.4 Elements of high order *José Felipe Voloch* . . . 93
4.4.1 Elements of high order from elements of small orders . . . 93
4.4.2 Gao's construction and a generalization . . . 93
4.4.3 Iterative constructions . . . 94
5 Bases . . . 95
5.1 Duality theory of bases *Dieter Jungnickel* . . . 95
5.1.1 Dual bases . . . 95
5.1.2 Self-dual bases . . . 97
5.1.3 Weakly self-dual bases . . . 98
5.1.4 Binary bases with small excess . . . 100
5.1.5 Almost weakly self-dual bases . . . 101
5.1.6 Connections to hardware design . . . 103

5.2 Normal bases *Shuhong Gao and Qunying Liao* . . . 103
5.2.1 Basics on normal bases . . . 104
5.2.2 Self-dual normal bases . . . 108
5.2.3 Primitive normal bases . . . 109
5.3 Complexity of normal bases *Shuhong Gao and David Thomson* . . . 110
5.3.1 Optimal and low complexity normal bases . . . 110
5.3.2 Gauss periods . . . 113
5.3.3 Normal bases from elliptic periods . . . 115
5.3.4 Complexities of dual and self-dual normal bases . . . 117
5.3.4.1 Duals of Gauss periods . . . 118
5.3.5 Fast arithmetic using normal bases . . . 119
5.4 Completely normal bases *Dirk Hachenberger* . . . 122
5.4.1 The complete normal basis theorem . . . 122
5.4.2 The class of completely basic extensions . . . 124
5.4.3 Cyclotomic modules and complete generators . . . 125
5.4.4 A decomposition theory for complete generators . . . 126
5.4.5 The class of regular extensions . . . 128
5.4.6 Complete generators for regular cyclotomic modules . . . 128
5.4.7 Towards a primitive complete normal basis theorem . . . 130
6 Exponential and character sums . . . 133
6.1 Gauss, Jacobi, and Kloosterman sums *Ronald J. Evans* . . . 133
6.1.1 Properties of Gauss and Jacobi sums of general order . . . 133
6.1.2 Evaluations of Jacobi and Gauss sums of small orders . . . 142
6.1.3 Prime ideal divisors of Gauss and Jacobi sums . . . 145
6.1.4 Kloosterman sums . . . 148
6.1.5 Gauss and Kloosterman sums over finite rings . . . 153
6.2 More general exponential and character sums *Antonio Rojas León* . . . 155
6.2.1 One variable character sums . . . 155
6.2.2 Additive character sums . . . 156
6.2.3 Multiplicative character sums . . . 159
6.2.4 Generic estimates . . . 161
6.2.5 More general types of character sums . . . 162
6.3 Some applications of character sums *Alina Ostafe and Arne Winterhof* . . . 164
6.3.1 Applications of a simple character sum identity . . . 164
6.3.1.1 Hadamard matrices . . . 164
6.3.1.2 Cyclotomic complete mappings and check digit systems 164
6.3.1.3 Periodic autocorrelation of cyclotomic generators . . . 166
6.3.2 Applications of Gauss and Jacobi sums . . . 166
6.3.2.1 Reciprocity laws . . . 167
6.3.2.2 Distribution of linear congruential pseudorandom numbers . . . 168
6.3.2.3 Diagonal equations, Waring's problem in finite fields, and covering radius of certain cyclic codes . . . 169
6.3.2.4 Hidden number problem and noisy interpolation . . . 170
6.3.3 Applications of the Weil bound . . . 170
6.3.3.1 Superelliptic and Artin-Schreier equations . . . 171
6.3.3.2 Stable quadratic polynomials . . . 171
6.3.3.3 Hamming distance of dual BCH codes . . . 172
6.3.4 Applications of Kloosterman sums . . . 173
6.3.4.1 Kloosterman equations and Kloosterman codes . . . 173

6.3.4.2 Distribution of inversive congruential pseudorandom numbers . . . 174
6.3.4.3 Nonlinearity of Boolean functions . . . 174
6.3.5 Incomplete character sums . . . 175
6.3.5.1 Finding deterministically linear factors of polynomials . . . 175
6.3.5.2 Measures of pseudorandomness . . . 176
6.3.6 Other character sums . . . 176
6.3.6.1 Distribution of primitive elements and powers . . . 177
6.3.6.2 Distribution of Diffie-Hellman triples . . . 177
6.3.6.3 Thin sets with small discrete Fourier transform . . . 178
6.3.6.4 Character sums over arbitrary sets . . . 178
6.4 Sum-product theorems and applications *Moubariz Z. Garaev* . . . 179
6.4.1 Notation . . . 179
6.4.2 The sum-product estimate and its variants . . . 180
6.4.3 Applications . . . 182
7 Equations over finite fields . . . 187
7.1 General forms *Daqing Wan* . . . 187
7.1.1 Affine hypersurfaces . . . 187
7.1.2 Projective hypersurfaces . . . 189
7.1.3 Toric hypersurfaces . . . 190
7.1.4 Artin-Schreier hypersurfaces . . . 191
7.1.5 Kummer hypersurfaces . . . 192
7.1.6 p-Adic estimates . . . 193
7.2 Quadratic forms *Robert Fitzgerald* . . . 195
7.2.1 Basic definitions . . . 195
7.2.2 Quadratic forms over finite fields . . . 196
7.2.3 Trace forms . . . 198
7.2.4 Applications . . . 199
7.3 Diagonal equations *Francis Castro and Ivelisse Rubio* . . . 200
7.3.1 Preliminaries . . . 200
7.3.2 Solutions of diagonal equations . . . 201
7.3.3 Generalizations of diagonal equations . . . 204
7.3.4 Waring's problem in finite fields . . . 205
8 Permutation polynomials . . . 208
8.1 One variable *Gary L. Mullen and Qiang Wang* . . . 208
8.1.1 Introduction . . . 208
8.1.2 Criteria . . . 209
8.1.3 Enumeration and distribution of PPs . . . 210
8.1.4 Constructions of PPs . . . 213
8.1.5 PPs from permutations of multiplicative groups . . . 214
8.1.6 PPs from permutations of additive groups . . . 217
8.1.7 Other types of PPs from the AGW criterion . . . 217
8.1.8 Dickson and Reversed Dickson PPs . . . 219
8.1.9 Miscellaneous PPs . . . 220
8.2 Several variables *Rudolf Lidl and Gary L. Mullen* . . . 223
8.3 Value sets of polynomials *Gary L. Mullen and Michael E. Zieve* . . . 225
8.3.1 Large value sets . . . 225
8.3.2 Small value sets . . . 226
8.3.3 General polynomials . . . 226
8.3.4 Lower bounds . . . 227
8.3.5 Examples . . . 227

8.3.6 Further value set papers . . . 228
8.4 Exceptional polynomials *Michael E. Zieve* . . . 229
8.4.1 Fundamental properties . . . 229
8.4.2 Indecomposable exceptional polynomials . . . 230
8.4.3 Exceptional polynomials and permutation polynomials . . . 231
8.4.4 Miscellany . . . 231
8.4.5 Applications . . . 232
9 Special functions over finite fields . . . 234
9.1 Boolean functions *Claude Carlet* . . . 234
9.1.1 Representation of Boolean functions . . . 235
9.1.1.1 Algebraic normal form . . . 235
9.1.1.2 Trace representation . . . 236
9.1.2 The Walsh transform . . . 236
9.1.3 Parameters of Boolean functions . . . 237
9.1.4 Equivalence of Boolean functions . . . 239
9.1.5 Boolean functions and cryptography . . . 239
9.1.6 Constructions of cryptographic Boolean functions . . . 242
9.1.6.1 Primary constructions . . . 242
9.1.6.2 Secondary constructions . . . 242
9.1.7 Boolean functions and error correcting codes . . . 243
9.1.7.1 Reed-Muller codes . . . 244
9.1.7.2 Kerdock codes . . . 244
9.1.8 Boolean functions and sequences . . . 244
9.1.8.1 Boolean functions and cross correlation of m-sequences 244
9.2 PN and APN functions *Pascale Charpin* . . . 245
9.2.1 Functions from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^m}$ . . . 246
9.2.2 Perfect Nonlinear (PN) functions . . . 247
9.2.3 Almost Perfect Nonlinear (APN) and Almost Bent (AB) functions 248
9.2.4 APN permutations . . . 249
9.2.5 Properties of stability . . . 250
9.2.6 Coding theory point of view . . . 251
9.2.7 Quadratic APN functions . . . 251
9.2.8 APN monomials . . . 253
9.3 Bent and related functions *Alexander Kholosha and Alexander Pott* . . . 254
9.3.1 Definitions and examples . . . 255
9.3.2 Basic properties of bent functions . . . 257
9.3.3 Bent functions and other combinatorial objects . . . 258
9.3.4 Fundamental classes of bent functions . . . 258
9.3.5 Boolean monomial and Niho bent functions . . . 261
9.3.6 P-ary bent functions in univariate form . . . 262
9.3.7 Constructions using planar and s-plateaued functions . . . 264
9.3.8 Vectorial bent functions and Kerdock codes . . . 265
9.4 κ-polynomials and related algebraic objects *Robert Coulter* . . . 266
9.4.1 Definitions and preliminaries . . . 266
9.4.2 Pre-semifields, semifields and isotopy . . . 267
9.4.3 Semifield constructions . . . 268
9.4.4 Semifields and nuclei . . . 269
9.5 Planar functions and commutative semifields *Robert Coulter* . . . 270
9.5.1 Definitions and preliminaries . . . 271
9.5.2 Constructing affine planes using planar functions . . . 271
9.5.3 Examples, constructions and equivalence . . . 272

9.5.4 Classification results, necessary conditions and the Dembowski-Ostrom Conjecture . . . 272
9.5.5 Planar DO polynomials and commutative semifields of odd order 273
9.6 Dickson polynomials *Qiang Wang and Joseph L. Yucas* . . . 274
9.6.1 Basics . . . 275
9.6.2 Factorization . . . 276
9.6.2.1 a-reciprocals of polynomials . . . 277
9.6.2.2 The maps Φ_a and Ψ_a . . . 278
9.6.2.3 Factors of Dickson polynomials . . . 278
9.6.2.4 a-cyclotomic polynomials . . . 279
9.6.3 Dickson polynomials of the $(k+1)$-st kind . . . 280
9.6.4 Multivariate Dickson polynomials . . . 281
9.7 Schur's conjecture and exceptional covers *Michael D. Fried* . . . 282
9.7.1 Rational function definitions . . . 282
9.7.2 MacCluer's Theorem and Schur's Conjecture . . . 284
9.7.3 Fiber product of covers . . . 287
9.7.4 Combining exceptional covers; the $(\mathbb{F}_q, Z)$ exceptional tower . . . 289
9.7.5 Exceptional rational functions; Serre's Open Image Theorem . . . 290
9.7.6 Davenport pairs and Poincaré series . . . 293
10 Sequences over finite fields . . . 296
10.1 Finite field transforms *Gary McGuire* . . . 296
10.1.1 Basic definitions and important examples . . . 296
10.1.2 Functions between two groups . . . 299
10.1.3 Discrete Fourier Transform . . . 300
10.1.4 Further topics . . . 301
10.1.4.1 Fourier spectrum . . . 302
10.1.4.2 Nonlinearity . . . 302
10.1.4.3 Characteristic functions . . . 302
10.1.4.4 Gauss sums . . . 303
10.1.4.5 Uncertainty principle . . . 303
10.2 LFSR sequences and maximal period sequences *Harald Niederreiter* . . . 304
10.2.1 General properties of LFSR sequences . . . 304
10.2.2 Operations with LFSR sequences and characterizations . . . 306
10.2.3 Maximal period sequences . . . 308
10.2.4 Distribution properties of LFSR sequences . . . 308
10.2.5 Applications of LFSR sequences . . . 309
10.3 Correlation and autocorrelation of sequences *Tor Helleseth* . . . 310
10.3.1 Basic definitions . . . 310
10.3.2 Autocorrelation of sequences . . . 311
10.3.3 Sequence families with low correlation . . . 312
10.3.4 Quaternary sequences . . . 314
10.3.5 Other correlation measures . . . 315
10.4 Linear complexity of sequences and multisequences *Wilfried Meidl and Arne Winterhof* . . . 317
10.4.1 Linear complexity measures . . . 317
10.4.2 Analysis of the linear complexity . . . 320
10.4.3 Average behaviour of the linear complexity . . . 322
10.4.4 Some sequences with large n-th linear complexity . . . 324
10.4.4.1 Explicit sequences . . . 325
10.4.4.2 Recursive nonlinear sequences . . . 325
10.4.4.3 Legendre sequence and related bit sequences . . . 326

10.4.4.4 Elliptic curve sequences . . . 327
10.4.5 Related measures . . . 327
10.4.5.1 Kolmogorov complexity . . . 327
10.4.5.2 Lattice test . . . 328
10.4.5.3 Correlation measure of order k . . . 328
10.4.5.4 FCSR and p-adic span . . . 328
10.4.5.5 Discrepancy . . . 329
10.5 Algebraic dynamical systems over finite fields *Igor Shparlinski* . . . 330
10.5.1 Introduction . . . 330
10.5.2 Background and main definitions . . . 330
10.5.3 Degree growth . . . 331
10.5.4 Linear independence and other algebraic properties of iterates . . . 333
10.5.5 Multiplicative independence of iterates . . . 334
10.5.6 Trajectory length . . . 334
10.5.7 Irreducibility of iterates . . . 335
10.5.8 Diameter of partial trajectories . . . 336
11 Algorithms . . . 338
11.1 Computational techniques *Christophe Doche* . . . 338
11.1.1 Preliminaries . . . 339
11.1.1.1 Prime field generation . . . 339
11.1.1.2 Extension field generation . . . 340
11.1.1.3 Primitive elements . . . 341
11.1.1.4 Order of an irreducible polynomial and primitive polynomials . . . 342
11.1.1.5 Minimal polynomial of an element . . . 343
11.1.2 Representation of finite fields . . . 343
11.1.3 Modular reduction . . . 344
11.1.3.1 Prime fields . . . 344
11.1.3.2 Extension fields . . . 346
11.1.4 Addition . . . 347
11.1.5 Multiplication . . . 347
11.1.5.1 Prime fields . . . 347
11.1.5.2 Extension fields . . . 348
11.1.6 Squaring . . . 349
11.1.6.1 Finite fields of odd characteristic . . . 349
11.1.6.2 Finite fields of characteristic two . . . 349
11.1.7 Exponentiation . . . 349
11.1.7.1 Prime fields . . . 349
11.1.7.2 Extension fields . . . 350
11.1.8 Inversion . . . 351
11.1.8.1 Prime fields . . . 352
11.1.8.2 Extension fields . . . 353
11.1.9 Squares and square roots . . . 353
11.1.9.1 Finite fields of odd characteristic . . . 354
11.1.9.2 Finite fields of even characteristic . . . 356
11.2 Univariate polynomial counting and algorithms *Daniel Panario* . . . 357
11.2.1 Classical counting results . . . 357
11.2.2 Analytic combinatorics approach . . . 358
11.2.3 Some illustrations of polynomial counting . . . 360
11.2.3.1 Number of irreducible factors of a polynomial . . . 360
11.2.3.2 Factorization patterns . . . 361

11.2.3.3 Largest and smallest degree irreducibles 362
11.2.3.4 Greatest common divisor of polynomials 364
11.2.3.5 Relations to permutations and integers 365
11.3 Algorithms for irreducibility testing and for constructing irreducible polynomials *Mark Giesbrecht* 367
11.3.1 Introduction 367
11.3.2 Early irreducibility tests of univariate polynomials 368
11.3.3 Rabin's irreducibility test 368
11.3.4 Constructing irreducible polynomials: randomized algorithms . . 369
11.3.5 Ben-Or's algorithm for construction of irreducible polynomials . 370
11.3.6 Shoup's algorithm for construction of irreducible polynomials . . 371
11.3.7 Constructing irreducible polynomials: deterministic algorithms . 371
11.3.8 Construction of irreducible polynomials of approximate degree . 372
11.4 Factorization of univariate polynomials *Joachim von zur Gathen* 373
11.5 Factorization of multivariate polynomials *Erich Kaltofen and Grégoire Lecerf* 375
11.5.1 Factoring dense multivariate polynomials 375
11.5.1.1 Separable factorization 375
11.5.1.2 Squarefree factorization 377
11.5.1.3 Bivariate irreducible factorization 377
11.5.1.4 Reduction from any number to two variables 379
11.5.2 Factoring sparse multivariate polynomials 380
11.5.2.1 Ostrowski's theorem 381
11.5.2.2 Irreducibility tests based on indecomposability of polytopes 381
11.5.2.3 Sparse bivariate Hensel lifting driven by polytopes . 381
11.5.2.4 Convex-dense bivariate factorization 382
11.5.3 Factoring straight-line programs and black boxes 383
11.6 Discrete logarithms over finite fields *Andrew Odlyzko* 386
11.6.1 Basic definitions 386
11.6.2 Modern computer implementations 387
11.6.3 Historical remarks 387
11.6.4 Basic properties of discrete logarithms 388
11.6.5 Chinese Remainder Theorem reduction: The Silver–Pohlig–Hellman algorithm 388
11.6.6 Baby steps–giant steps algorithm 389
11.6.7 Pollard rho and kangaroo methods for discrete logarithms . . . 390
11.6.8 Index calculus algorithms for discrete logarithms in finite fields . 391
11.6.9 Smooth integers and smooth polynomials 392
11.6.10 Sparse linear systems of equations 392
11.6.11 Current discrete logarithm records 393
11.7 Standard models for finite fields *Bart de Smit and Hendrik Lenstra* . . . 394
12 Curves over finite fields 398
12.1 Introduction to function fields and curves *Arnaldo Garcia and Henning Stichtenoth* 399
12.1.1 Valuations and places 399
12.1.2 Divisors and Riemann–Roch theorem 401
12.1.3 Extensions of function fields 405
12.1.4 Differentials 412
12.1.5 Function fields and curves 414
12.2 Elliptic curves *Joseph Silverman* 415
12.2.1 Weierstrass equations 416

12.2.2 The group law . . . 418
12.2.3 Isogenies and endomorphisms . . . 420
12.2.4 The number of points in $E(\mathbb{F}_q)$ . . . 423
12.2.5 Twists . . . 424
12.2.6 The torsion subgroup and the Tate module . . . 425
12.2.7 The Weil pairing and the Tate pairing . . . 426
12.2.8 The endomorphism ring and automorphism group . . . 428
12.2.9 Ordinary and supersingular elliptic curves . . . 429
12.2.10 The zeta function of an elliptic curve . . . 431
12.2.11 The elliptic curve discrete logarithm problem . . . 432
12.3 Addition formulas for elliptic curves *Daniel J. Bernstein and Tanja Lange* 433
12.3.1 Curve shapes . . . 433
12.3.2 Addition . . . 434
12.3.3 Coordinate systems . . . 435
12.3.4 Explicit formulas . . . 436
12.3.5 Short Weierstrass curves, large characteristic: $y^2 = x^3 - 3x + b$ 437
12.3.6 Short Weierstrass curves, characteristic 2, ordinary case: $y^2 + xy = x^3 + a_2x^2 + a_6$ . . . 437
12.3.7 Montgomery curves: $by^2 = x^3 + ax^2 + x$ . . . 438
12.3.8 Twisted Edwards curves: $ax^2 + y^2 = 1 + dx^2y^2$ . . . 439
12.4 Hyperelliptic curves *Michael John Jacobson, Jr. and Renate Scheidler* . . . 440
12.4.1 Hyperelliptic equations . . . 440
12.4.2 The degree zero divisor class group . . . 442
12.4.3 Divisor class arithmetic over finite fields . . . 444
12.4.4 Endomorphisms and supersingularity . . . 446
12.4.5 Class number computation . . . 447
12.4.6 The Tate-Lichtenbaum pairing . . . 447
12.4.7 The hyperelliptic curve discrete logarithm problem . . . 448
12.5 Rational points on curves *Arnaldo Garcia and Henning Stichtenoth* . . . 450
12.5.1 Rational places . . . 450
12.5.2 The Zeta function of a function field . . . 451
12.5.3 Bounds for the number of rational places . . . 452
12.5.4 Maximal function fields . . . 454
12.5.5 Asymptotic bounds . . . 455
12.6 Towers *Arnaldo Garcia and Henning Stichtenoth* . . . 457
12.6.1 Introduction to towers . . . 457
12.6.2 Examples of towers . . . 459
12.7 Zeta functions and L-functions *Lei Fu* . . . 462
12.7.1 Zeta functions . . . 462
12.7.2 L-functions . . . 467
12.7.3 The case of curves . . . 469
12.8 P-adic estimates of zeta functions and L-functions *Régis Blache* . . . 472
12.8.1 Introduction . . . 472
12.8.2 Lower bounds for the first slope . . . 473
12.8.3 Uniform lower bounds for Newton polygons . . . 474
12.8.4 Variation of Newton polygons in a family . . . 476
12.8.5 The case of curves and abelian varieties . . . 478
12.9 Computing the number of rational points and zeta functions *Daqing Wan* 481
12.9.1 Point counting: sparse input . . . 481
12.9.2 Point counting: dense input . . . 482
12.9.3 Computing zeta functions: general case . . . 483

12.9.4 Computing zeta functions: curve case . . . 484
13 Miscellaneous theoretical topics . . . 485
13.1 Relations between integers and polynomials over finite fields *Gove Effinger* 485
13.1.1 The density of primes and irreducibles . . . 486
13.1.2 Primes and irreducibles in arithmetic progression . . . 487
13.1.3 Twin primes and irreducibles . . . 487
13.1.4 The generalized Riemann hypothesis . . . 488
13.1.5 The Goldbach problem over finite fields . . . 489
13.1.6 The Waring problem over finite fields . . . 490
13.2 Matrices over finite fields *Dieter Jungnickel* . . . 492
13.2.1 Matrices of specified rank . . . 492
13.2.2 Matrices of specified order . . . 493
13.2.3 Matrix representations of finite fields . . . 494
13.2.4 Circulant and orthogonal matrices . . . 496
13.2.5 Symmetric and skew-symmetric matrices . . . 498
13.2.6 Hankel and Toeplitz matrices . . . 499
13.2.7 Determinants . . . 501
13.3 Classical groups over finite fields *Zhe-Xian Wan* . . . 502
13.3.1 Linear groups over finite fields . . . 502
13.3.2 Symplectic groups over finite fields . . . 504
13.3.3 Unitary groups over finite fields . . . 506
13.3.4 Orthogonal groups over finite fields of characteristic not two . . . 508
13.3.5 Orthogonal groups over finite fields of characteristic two . . . 511
13.4 Computational linear algebra over finite fields *Jean-Guillaume Dumas and Clément Pernet* . . . 513
13.4.1 Dense matrix multiplication . . . 513
13.4.1.1 Tiny finite fields . . . 513
13.4.1.2 Word size prime fields . . . 516
13.4.1.3 Large finite fields . . . 516
13.4.1.4 Large matrices: subcubic time complexity . . . 516
13.4.2 Dense Gaussian elimination and echelon forms . . . 517
13.4.2.1 Building blocks . . . 517
13.4.2.2 PLE decomposition . . . 518
13.4.2.3 Echelon forms . . . 519
13.4.3 Minimal and characteristic polynomial of a dense matrix . . . 520
13.4.4 Blackbox iterative methods . . . 522
13.4.4.1 Minimal polynomial and the Wiedemann algorithm . . . 522
13.4.4.2 Rank, Determinant and Characteristic Polynomial . . . 523
13.4.4.3 System solving and the Lanczos algorithm . . . 524
13.4.5 Sparse and structured methods . . . 524
13.4.5.1 Reordering . . . 524
13.4.5.2 Structured matrices and displacement rank . . . 525
13.4.6 Hybrid methods . . . 526
13.4.6.1 Hybrid sparse-dense methods . . . 526
13.4.6.2 Block-iterative methods . . . 527
13.5 Carlitz and Drinfeld modules *David Goss* . . . 528
13.5.1 Quick review . . . 528
13.5.2 Drinfeld modules: definition and analytic theory . . . 529
13.5.3 Drinfeld modules over finite fields . . . 531
13.5.4 The reduction theory of Drinfeld modules . . . 532
13.5.5 The A-module of rational points . . . 532

13.5.6 The invariants of a Drinfeld module . . . 532
13.5.7 The L-series of a Drinfeld module . . . 533
13.5.8 Special values . . . 534
13.5.9 Measures and symmetries . . . 535
13.5.10 Multizeta . . . 536
13.5.11 Modular theory . . . 536
13.5.12 Transcendency results . . . 538

Part III: Applications

14 Combinatorial . . . 540
14.1 Latin squares *Gary L. Mullen* . . . 541
14.1.1 Prime powers . . . 543
14.1.2 Non-prime powers . . . 543
14.1.3 Frequency squares . . . 544
14.1.4 Hypercubes . . . 545
14.1.5 Connections to affine and projective planes . . . 546
14.1.6 Other finite field constructions for MOLS . . . 547
14.2 Lacunary polynomials over finite fields *Simeon Ball and Aart Blokhuis* . . . 547
14.2.1 Introduction . . . 548
14.2.2 Lacunary polynomials . . . 548
14.2.3 Directions and Rédei polynomials . . . 549
14.2.4 Sets of points determining few directions . . . 550
14.2.5 Lacunary polynomials and blocking sets . . . 551
14.2.6 Lacunary polynomials and blocking sets in planes of prime order 552
14.2.7 Lacunary polynomials and multiple blocking sets . . . 553
14.3 Affine and projective planes *Gary Ebert and Leo Storme* . . . 555
14.3.1 Projective planes . . . 555
14.3.2 Affine planes . . . 556
14.3.3 Translation planes and spreads . . . 557
14.3.4 Nest planes . . . 558
14.3.5 Flag-transitive affine planes . . . 559
14.3.6 Subplanes . . . 561
14.3.7 Embedded unitals . . . 562
14.3.8 Maximal arcs . . . 563
14.3.9 Other results . . . 564
14.4 Projective spaces *James W.P. Hirschfeld and Joseph A. Thas* . . . 566
14.4.1 Projective and affine spaces . . . 566
14.4.2 Collineations, correlations and coordinate frames . . . 568
14.4.3 Polarities . . . 570
14.4.4 Partitions and cyclic projectivities . . . 573
14.4.5 k-Arcs . . . 575
14.4.6 k-Arcs and linear MDS codes . . . 577
14.4.7 k-Caps . . . 579
14.5 Block designs *Charles J. Colbourn and Jeffrey H. Dinitz* . . . 581
14.5.1 Basics . . . 581
14.5.2 Triple systems . . . 582
14.5.3 Difference families and balanced incomplete block designs . . . 584
14.5.4 Nested designs . . . 586
14.5.5 Pairwise balanced designs . . . 587

14.5.6 Group divisible designs . . . 588
14.5.7 t-designs . . . 589
14.5.8 Packing and covering . . . 589
14.6 Difference sets *Alexander Pott* . . . 590
14.6.1 Basics . . . 590
14.6.2 Difference sets in cyclic groups . . . 593
14.6.3 Difference sets in the additive groups of finite fields . . . 594
14.6.4 Difference sets and Hadamard matrices . . . 595
14.6.5 Further families of difference sets . . . 596
14.6.6 Difference sets and character sums . . . 597
14.6.7 Multipliers . . . 597
14.7 Other combinatorial structures *Jeffrey H. Dinitz and Charles J. Colbourn* 598
14.7.1 Association schemes . . . 598
14.7.2 Costas arrays . . . 599
14.7.3 Conference matrices . . . 600
14.7.4 Covering arrays . . . 601
14.7.5 Hall triple systems . . . 602
14.7.6 Ordered designs and perpendicular arrays . . . 602
14.7.7 Perfect hash families . . . 603
14.7.8 Room squares and starters . . . 605
14.7.9 Strongly regular graphs . . . 608
14.7.10 Whist tournaments . . . 608
14.8 (t, m, s)-nets and (t, s)-sequences *Harald Niederreiter* . . . 610
14.8.1 (t, m, s)-nets . . . 611
14.8.2 Digital (t, m, s)-nets . . . 612
14.8.3 Constructions of (t, m, s)-nets . . . 614
14.8.4 (t, s)-sequences and $(\mathbf{T}, s)$-sequences . . . 616
14.8.5 Digital (t, s)-sequences and digital $(\mathbf{T}, s)$-sequences . . . 617
14.8.6 Constructions of (t, s)-sequences and $(\mathbf{T}, s)$-sequences . . . 619
14.9 Applications and weights of multiples of primitive and other polynomials *Brett Stevens* . . . 621
14.9.1 Applications where weights of multiples of a base polynomial are relevant . . . 621
14.9.1.1 Applications from other Handbook sections . . . 621
14.9.1.2 Application of polynomials to the construction of orthogonal arrays . . . 622
14.9.1.3 Application of polynomials to a card trick . . . 623
14.9.2 Weights of multiples of polynomials . . . 624
14.9.2.1 General bounds on $d((C_n^f)^\perp)$ . . . 624
14.9.2.2 Bounds on $d((C_n^f)^\perp)$ for polynomials of specific degree 626
14.9.2.3 Bounds on $d((C_n^f)^\perp)$ for polynomials of specific weight 629
14.10 Ramanujan and expander graphs *M. Ram Murty and Sebastian M. Cioabă* 633
14.10.1 Graphs, adjacency matrices and eigenvalues . . . 634
14.10.2 Ramanujan graphs . . . 637
14.10.3 Expander graphs . . . 639
14.10.4 Cayley graphs . . . 640
14.10.5 Explicit constructions of Ramanujan graphs . . . 643
14.10.6 Combinatorial constructions of expanders . . . 646
14.10.7 Zeta functions of graphs . . . 648
15 Algebraic coding theory . . . 650
15.1 Basic coding properties and bounds *Ian Blake and W. Cary Huffman* . . . 650

15.1.1 Channel models and error correction . . . 650
15.1.2 Linear codes . . . 652
15.1.2.1 Standard array decoding of linear codes . . . 656
15.1.2.2 Hamming codes . . . 657
15.1.2.3 Reed-Muller codes . . . 658
15.1.2.4 Subfield and trace codes . . . 659
15.1.2.5 Modifying linear codes . . . 660
15.1.2.6 Bounds on codes . . . 661
15.1.2.7 Asymptotic bounds . . . 664
15.1.3 Cyclic codes . . . 665
15.1.3.1 Algebraic prerequisites . . . 666
15.1.3.2 Properties of cyclic codes . . . 667
15.1.3.3 Classes of cyclic codes . . . 668
15.1.4 A spectral approach to coding . . . 680
15.1.5 Codes and combinatorics . . . 681
15.1.6 Decoding . . . 683
15.1.6.1 Decoding BCH codes . . . 683
15.1.6.2 The Peterson-Gorenstein-Zierler decoder . . . 683
15.1.6.3 Berlekamp-Massey decoding . . . 684
15.1.6.4 Extended Euclidean algorithm decoding . . . 685
15.1.6.5 Welch-Berlekamp decoding of GRS codes . . . 686
15.1.6.6 Majority logic decoding . . . 687
15.1.6.7 Generalized minimum distance decoding . . . 687
15.1.6.8 List decoding - decoding beyond the minimum distance bound . . . 689
15.1.7 Codes over $\mathbb{Z}_4$ . . . 690
15.1.8 Conclusion . . . 693
15.2 Algebraic-geometry codes *Harald Niederreiter* . . . 694
15.2.1 Classical algebraic-geometry codes . . . 694
15.2.2 Generalized algebraic-geometry codes . . . 696
15.2.3 Function-field codes . . . 699
15.2.4 Asymptotic bounds . . . 701
15.3 LDPC and Gallager codes over finite fields *Ian Blake and W. Cary Huffman* 704
15.4 Turbo codes over finite fields *Oscar Takeshita* . . . 710
15.4.1 Introduction . . . 710
15.4.1.1 Historical background . . . 710
15.4.1.2 Terminology . . . 710
15.4.2 Convolutional codes . . . 712
15.4.2.1 Non-recursive convolutional codes . . . 712
15.4.2.2 Distance properties of non-recursive convolutional codes 713
15.4.2.3 Recursive convolutional codes . . . 714
15.4.2.4 Distance properties of recursive convolutional codes 714
15.4.3 Permutations and interleavers . . . 715
15.4.4 Encoding and decoding . . . 716
15.4.5 Design of turbo codes . . . 716
15.4.5.1 Design of the recursive convolutional code . . . 717
15.4.5.2 Design of interleavers . . . 717
15.5 Raptor codes *Ian Blake and W. Cary Huffman* . . . 718
15.5.1 Tornado codes . . . 719
15.5.2 LT and fountain codes . . . 721
15.5.3 Raptor codes . . . 724

15.6 Polar codes *Simon Litsyn* . . . 726
15.6.1 Space decomposition . . . 726
15.6.2 Vector transformation . . . 727
15.6.3 Decoding . . . 728
15.6.4 Historical notes and other results . . . 730
16 Cryptography . . . 731
16.1 Introduction *Alfred Menezes* . . . 731
16.1.1 Goals of cryptography . . . 732
16.1.2 Symmetric-key cryptography . . . 732
16.1.2.1 Stream ciphers . . . 732
16.1.2.2 Block ciphers . . . 733
16.1.3 Public-key cryptography . . . 734
16.1.3.1 RSA . . . 734
16.1.3.2 Discrete logarithm cryptosystems . . . 735
16.1.3.3 DSA . . . 736
16.1.4 Pairing-based cryptography . . . 737
16.1.5 Post-quantum cryptography . . . 739
16.2 Stream and block ciphers *Guang Gong and Kishan Chand Gupta* . . . 740
16.2.1 Basic concepts of stream ciphers . . . 741
16.2.2 (Alleged) RC4 algorithm . . . 743
16.2.3 WG stream cipher . . . 744
16.2.4 Basic structures of block ciphers . . . 748
16.2.5 RC6 . . . 749
16.2.6 Advanced Encryption Standard (AES) RIJNDAEL . . . 750
16.3 Multivariate cryptographic systems *Jintai Ding* . . . 754
16.3.1 The basics of multivariate PKCs . . . 755
16.3.1.1 The standard (bipolar) construction of MPKCs . . . 755
16.3.1.2 Implicit form MPKCs . . . 756
16.3.1.3 Isomorphism of polynomials . . . 757
16.3.2 Main constructions and variations . . . 758
16.3.2.1 Historical constructions . . . 758
16.3.2.2 Triangular constructions . . . 759
16.3.2.3 Big-field families: Matsumoto-Imai (C^*) and HFE . 760
16.3.2.4 Oil and vinegar (unbalanced and balanced) and variations . . . 761
16.3.2.5 UOV as a booster stage . . . 762
16.3.2.6 Plus-Minus variations . . . 763
16.3.2.7 Internal perturbation . . . 764
16.3.2.8 Vinegar as an external perturbation and projection . 764
16.3.2.9 TTM and related schemes: “lock” or repeated triangular 765
16.3.2.10 Intermediate fields: MFE and ℓIC . . . 766
16.3.2.11 Odd Characteristic . . . 766
16.3.2.12 Other constructions . . . 766
16.3.3 Standard attacks . . . 766
16.3.3.1 Linearization equations . . . 767
16.3.3.2 Critical bilinear relations . . . 767
16.3.3.3 HOLEs (higher-order linearization equations) . . . 767
16.3.3.4 Differential attacks . . . 768
16.3.3.5 Attacking internal perturbations . . . 768
16.3.3.6 The skew symmetric transformation . . . 769
16.3.3.7 Multiplicative symmetry . . . 769

16.3.3.8 Rank attacks . . . 770
16.3.3.9 MinRank attacks on big-field schemes . . . 770
16.3.3.10 Distilling oil from vinegar and other attacks on UOV 771
16.3.3.11 Reconciliation . . . 771
16.3.3.12 Direct attacks using polynomial solvers . . . 772
16.3.4 The future . . . 773
16.4 Elliptic curve cryptographic systems *Andreas Enge* . . . 774
16.4.1 Cryptosystems based on elliptic curve discrete logarithms . . . 774
16.4.1.1 Key sizes . . . 775
16.4.1.2 Cryptographic primitives . . . 775
16.4.1.3 Special curves . . . 776
16.4.1.4 Random curves: point counting . . . 778
16.4.2 Pairing based cryptosystems . . . 779
16.4.2.1 Cryptographic pairings . . . 779
16.4.2.2 Pairings and twists . . . 782
16.4.2.3 Explicit isomorphisms . . . 783
16.4.2.4 Curve constructions . . . 783
16.4.2.5 Hashing into elliptic curves . . . 786
16.5 Hyperelliptic curve cryptographic systems *Nicolas Thériault* . . . 787
16.5.1 Cryptosystems based on hyperelliptic curve discrete logarithms . 788
16.5.2 Curves of genus 2 . . . 788
16.5.3 Curves of genus 3 . . . 789
16.5.4 Curves of higher genus . . . 790
16.5.5 Key sizes . . . 790
16.5.6 Special curves . . . 792
16.5.7 Random curves: point counting . . . 793
16.5.8 Pairings in hyperelliptic curves . . . 794
16.6 Cryptosystems arising from Abelian varieties *Kumar Murty* . . . 794
16.6.1 Definitions . . . 795
16.6.2 Examples . . . 795
16.6.3 Jacobians of curves . . . 795
16.6.4 Restriction of scalars . . . 795
16.6.5 Endomorphisms . . . 796
16.6.6 The characteristic polynomial of an endomorphism . . . 796
16.6.7 Zeta functions . . . 796
16.6.8 Arithmetic on an Abelian variety . . . 798
16.6.9 The group order . . . 799
16.6.10 The discrete logarithm problem . . . 799
16.6.11 Weil descent attack . . . 800
16.6.12 Pairings based cryptosystems . . . 801
16.7 Binary extension field arithmetic for hardware implementations *M. Anwarul Hasan and Haining Fan* . . . 802
16.7.1 Preamble and basic terminologies . . . 802
16.7.2 Arithmetic using polynomial operations . . . 803
16.7.3 Arithmetic using matrix operations . . . 807
16.7.4 Arithmetic using normal bases . . . 808
16.7.5 Multiplication using optimal normal bases . . . 810
16.7.6 Additional notes . . . 813
17 Miscellaneous applications . . . 815
17.1 Finite fields in biology *Franziska Hinkelmann and Reinhard Laubenbacher* 815

17.1.1 Polynomial dynamical systems as framework for discrete models in systems biology . . . 815
17.1.2 Polynomial dynamical systems . . . 816
17.1.3 Discrete model types and their translation into PDS . . . 817
17.1.3.1 Boolean network models . . . 819
17.1.3.2 Logical models . . . 819
17.1.3.3 Petri nets and agent-based models . . . 820
17.1.4 Reverse engineering and parameter estimation . . . 821
17.1.4.1 The minimal-sets algorithm . . . 821
17.1.4.2 Parameter estimation using the Gröbner fan of an ideal 821
17.1.5 Software for biologists and computer algebra software . . . 821
17.1.6 Specific polynomial dynamical systems . . . 822
17.1.6.1 Nested canalyzing functions . . . 822
17.1.6.2 Parameter estimation resulting in nested canalyzing functions . . . 824
17.1.6.3 Linear polynomial dynamical systems . . . 824
17.1.6.4 Conjunctive/disjunctive networks . . . 824
17.2 Finite fields in quantum information theory *Martin Roetteler and Arne Winterhof* . . . 824
17.2.1 Mutually unbiased bases . . . 825
17.2.2 Positive operator-valued measures . . . 826
17.2.3 Quantum error-correcting codes . . . 827
17.2.4 Period finding . . . 829
17.2.5 Quantum function reconstruction . . . 829
17.2.6 Further connections . . . 830
17.3 Finite fields in engineering *Jonathan Jedwab and Kai-Uwe Schmidt* . . . 831
17.3.1 Binary sequences with small aperiodic autocorrelation . . . 831
17.3.2 Sequence sets with small aperiodic auto- and crosscorrelation . . . 832
17.3.3 Binary Golay sequence pairs . . . 833
17.3.4 Optical orthogonal codes . . . 834
17.3.5 Sequences with small Hamming correlation . . . 835
17.3.6 Rank distance codes . . . 836
17.3.7 Space-time coding . . . 837
17.3.8 Coding over networks . . . 838
Bibliography . . . 840
Index . . . 1002

14.1 Latin squares 541
Prime powers • Non-prime powers • Frequency squares • Hypercubes • Connections to affine and projective planes • Other finite field constructions for MOLS

14.2 Lacunary polynomials over finite fields..... 547
Introduction • Lacunary polynomials • Directions and Rédei polynomials • Sets of points determining few directions • Lacunary polynomials and blocking sets • Lacunary polynomials and blocking sets in planes of prime order • Lacunary polynomials and multiple blocking sets

14.3 Affine and projective planes 555
Projective planes • Affine planes • Translation planes and spreads • Nest planes • Flag-transitive affine planes • Subplanes • Embedded unitals • Maximal arcs • Other results

14.4 Projective spaces 566
Projective and affine spaces • Collineations, correlations and coordinate frames • Polarities • Partitions and cyclic projectivities • k-Arcs • k-Arcs and linear MDS codes • k-Caps

14.5 Block designs 581
Basics • Triple systems • Difference families and balanced incomplete block designs • Nested designs • Pairwise balanced designs • Group divisible designs • t-designs • Packing and covering

14.6 Difference sets 590
Basics • Difference sets in cyclic groups • Difference sets in the additive groups of finite fields • Difference sets and Hadamard matrices • Further families of difference sets • Difference sets and character sums • Multipliers

14.7 Other combinatorial structures..... 598
Association schemes • Costas arrays • Conference matrices • Covering arrays • Hall triple systems • Ordered designs and perpendicular arrays • Perfect hash families • Room squares and starters • Strongly regular graphs • Whist tournaments

14.8 (t, m, s)-nets and (t, s)-sequences 610
(t, m, s)-nets • Digital (t, m, s)-nets • Constructions of (t, m, s)-nets • (t, s)-sequences and $(\mathbf{T}, s)$-sequences • Digital (t, s)-sequences and digital $(\mathbf{T}, s)$-sequences • Constructions of (t, s)-sequences and $(\mathbf{T}, s)$-sequences

14.9 Applications and weights of multiples of primitive and other polynomials 621
Applications where weights of multiples of a base polynomial are relevant • Weights of multiples of polynomials

14.10 Ramanujan and expander graphs 633
Graphs, adjacency matrices and eigenvalues • Ramanujan graphs • Expander graphs • Cayley graphs • Explicit constructions of Ramanujan graphs • Combinatorial constructions of expanders • Zeta functions of graphs

14.1 Latin squares

Gary L. Mullen, The Pennsylvania State University

14.1.1 Definition A *latin square of order n* is an $n \times n$ array based upon n distinct symbols with the property that each row and each column contains each of the n symbols exactly once.

14.1.2 Example The following are latin squares of orders 3 and 5

$$\begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array}, \qquad \begin{array}{ccccc} 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \\ 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \end{array}.$$

14.1.3 Remark Given any latin square of prime power order q (with symbols from $\mathbb{F}_q$, the finite field of order q), using the Lagrange Interpolation Formula from Theorem 2.1.131, we can construct a polynomial $P(x, y)$ of degree at most $q-1$ in both x and y which represents the given latin square. The field element $P(a, b)$ is placed at the intersection of row a and column b. For example, the two squares given in the previous example can be represented by the polynomials $x + y$ over $\mathbb{F}_3$ and $2x + y + 1$ over $\mathbb{F}_5$.

14.1.4 Definition Assume that a latin square of order n is based upon the n distinct symbols $1, 2, \ldots, n$. Such a latin square of order n is *reduced* if the first row and first column are in the standard order $1, 2, \ldots, n$. Let l_n denote the number of reduced latin squares of order n. Let L_n denote the total number of distinct latin squares of order n.

14.1.5 Theorem [700] For each $n \geq 2$, $L_n = n!(n-1)!l_n$.

14.1.6 Remark Using the addition table of the ring $\mathbb{Z}_n$ of integers modulo n, it is easy to see that $l_n \geq 1$ and hence $L_n \geq n!(n-1)!$ for each $n \geq 2$. The total number L_n of latin squares of order n is unknown if $n > 11$ [2040]. The table from [700, p. 142], gives the values of l_n for $n \leq 11$.

14.1.7 Definition Two latin squares of order n are *orthogonal* if upon placing one of the squares on top of the other, we obtain each of the possible n^2 distinct ordered pairs exactly once. In addition, a set $\{L_1, \ldots, L_t\}$ of latin squares all of the same order is *orthogonal* if each distinct pair of squares is orthogonal, i.e., if L_i is orthogonal to L_j whenever $i \neq j$. Such a set of squares is a set of *mutually orthogonal latin squares (MOLS)*.

14.1.8 Remark There are numerous combinatorial objects which are equivalent to sets of MOLS. These include transversal designs, orthogonal arrays, edge-partitions of a complete bipartite graph, and (k, n)-nets. We refer to Chapter III, Theorem 3.18 of [700] for a more detailed discussion of these topics; see also Sections 14.5 and 14.7.

14.1.9 Definition Let $N(n)$ denote the maximum number of mutually orthogonal latin squares (MOLS) of order n.

14.1.10 Theorem [700] For $n \geq 2$, $N(n) \leq n - 1$.

14.1.11 Definition A set $\{L_1, \ldots, L_t\}$ of MOLS of order n is *complete* if $t = n - 1$.

14.1.1 Prime powers

14.1.12 Theorem [353] For any prime power q, the polynomials $ax + y$ with $a \neq 0 \in \mathbb{F}_q$ represent a complete set of $q-1$ MOLS of order q by placing the field element $ax+y$ at the intersection of row x and column y of the a-th square.

14.1.13 Remark In Subsection 14.1.5 we discuss connections of complete sets of MOLS with other combinatorial objects; in particular with affine and projective planes where it is stated that the existence of a complete set of MOLS of order n is equivalent to the existence of an affine, or projective, plane of order n.

14.1.14 Example The following gives a complete set of 4 MOLS of order 5, arising from the polynomials $x + y, 2x + y, 3x + y, 4x + y$ over the field $\mathbb{F}_5$

$$\begin{array}{ccccc} 0&1&2&3&4\\ 1&2&3&4&0\\ 2&3&4&0&1\\ 3&4&0&1&2\\ 4&0&1&2&3 \end{array}, \quad \begin{array}{ccccc} 0&1&2&3&4\\ 2&3&4&0&1\\ 4&0&1&2&3\\ 1&2&3&4&0\\ 3&4&0&1&2 \end{array}, \quad \begin{array}{ccccc} 0&1&2&3&4\\ 3&4&0&1&2\\ 1&2&3&4&0\\ 4&0&1&2&3\\ 2&3&4&0&1 \end{array}, \quad \begin{array}{ccccc} 0&1&2&3&4\\ 4&0&1&2&3\\ 3&4&0&1&2\\ 2&3&4&0&1\\ 1&2&3&4&0 \end{array}.$$

14.1.15 Theorem For $q \geq 5$ an odd prime power, the polynomials $ax + y, a \neq 0, 1, -1 \in \mathbb{F}_q$ give a (maximal) set of $q - 3$ MOLS of order q, each of which is diagonal, i.e., which has distinct elements on both of the main diagonals. When $q \geq 4$ is even the same construction with $a \neq 0, 1 \in \mathbb{F}_q$ gives a (maximal) set of $q - 2$ diagonal MOLS of order q.

14.1.16 Remark The construction of sets of infinite latin squares containing nested sets of mutually orthogonal finite latin squares is discussed in [394, 395]. The construction involves use of polynomials of the form $ax + y$ over infinite algebraic extensions of finite fields.

14.1.17 Remark If q is odd, a latin square of order $q - 1$ which is the multiplication table of the group $\mathbb{F}_q^*$, is mateless; i.e., there is no latin square which is orthogonal to the given square. In fact, a latin square arising from the multiplication table of a cyclic group of even order is mateless; $\mathbb{F}_q$ with q odd is such an example.

14.1.18 Conjecture [1863] A complete set of $n - 1$ MOLS of order n exists if and only if n is a prime power.

14.1.19 Remark The above conjecture is the *prime power conjecture*, and is discussed in many articles. In [2163] this conjecture is referred to as the *next Fermat problem*.

14.1.2 Non-prime powers

14.1.20 Definition If A is a latin square of order m and B is a latin square of order n, denote the entry at row i and column j of A by a_{ij}. Similarly we denote the (i, j) entry of B by b_{ij}. Then the *Kronecker product* of A and B is the $mn \times mn$ square $A \otimes B$, given by

$$A \otimes B = \begin{array}{cccc} (a_{11}, B) & (a_{12}, B) & \cdots & (a_{1m}, B)\\ (a_{21}, B) & (a_{22}, B) & \cdots & (a_{2m}, B)\\ \vdots & \vdots & & \vdots\\ (a_{m1}, B) & (a_{m2}, B) & \cdots & (a_{mm}, B) \end{array}$$

where for each entry a of A, (a, B) is the $n \times n$ matrix

$$(a,B) = \begin{matrix} (a,b_{11}) & (a,b_{12}) & \cdots & (a,b_{1n}) \\ (a,b_{21}) & (a,b_{22}) & \cdots & (a,b_{2n}) \\ \vdots & \vdots & & \vdots \\ (a,b_{n1}) & (a,b_{n2}) & \cdots & (a,b_{nn}) \end{matrix}.$$

14.1.21 Example As an illustration of this Kronecker product construction, for $m = 2, n = 3$ let

$$A = \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}, \qquad B = \begin{matrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{matrix}.$$

Then the Kronecker product construction using A and B yields the following 6×6 square whose elements are ordered pairs:

$$\begin{matrix} 00 & 01 & 02 & 10 & 11 & 12 \\ 01 & 02 & 00 & 11 & 12 & 10 \\ 02 & 00 & 01 & 12 & 10 & 11 \\ 10 & 11 & 12 & 00 & 01 & 02 \\ 11 & 12 & 10 & 01 & 02 & 00 \\ 12 & 10 & 11 & 02 & 00 & 01 \end{matrix}.$$

14.1.22 Lemma If H and K are latin squares of orders n_1 and n_2, then $H \otimes K$ is a latin square of order $n_1 n_2$.

14.1.23 Lemma If H_1 and H_2 are orthogonal latin squares of order n_1 and K_1 and K_2 are orthogonal latin squares of order n_2, then $H_1 \otimes K_1$ and $H_2 \otimes K_2$ are orthogonal latin squares of order $n_1 n_2$.

14.1.24 Corollary If there is a pair of MOLS of order n and a pair of MOLS of order m, then there is a pair of MOLS of order mn.

14.1.25 Theorem If $n = q_1 \cdots q_r$, where the q_i are distinct prime powers with $q_1 < \cdots < q_r$, then $N(n) \geq q_1 - 1$.

14.1.26 Remark In 1922, MacNeish [1975] conjectured that $N(n) = q_1 - 1$. This has been shown to be false for all non-prime power values of $n \leq 62$; it is in fact conjectured in [1864] that this conjecture is false at all values of n other than 6 and prime powers.

14.1.3 Frequency squares

14.1.27 Definition Let $n = \lambda m$. An $F(n; \lambda)$ *frequency square* is an $n \times n$ square based upon m distinct symbols so that each of the m symbols occurs exactly λ times in each row and column. Thus an $F(n; 1)$ frequency square is a latin square of order n. Two $F(n; \lambda)$ frequency squares are *orthogonal* if when one square is placed on top of the other, each of the m^2 possible distinct ordered pairs occurs exactly λ^2 times [2159]. A set of such squares is *orthogonal* if any two distinct squares are orthogonal. Such a set of mutually orthogonal squares is a set of *MOFS*.

14.1.28 Theorem [1446] The maximum number of MOFS of the form $F(n; \lambda)$ is bounded above by $(n-1)^2/(m-1)$.

14.1.29 Theorem [2159] If q is a prime power and $i \geq 1$ is an integer, a complete set of $(q^i-1)^2/(q-1)$, $F(q^i; q^{i-1})$ MOFS can be constructed using the linear polynomials $a_1x_1 + \cdots + a_{2i}x_{2i}$ over the field $\mathbb{F}_q$ where

1. The vector $(a_1, \ldots, a_i) \neq (0, \ldots, 0)$,
2. The vector $(a_{i+1}, \ldots, a_{2i}) \neq (0, \ldots, 0)$,
3. The vector $(a'_1, \ldots, a'_{2i}) \neq e(a_1, \ldots, a_{2i})$ for any $e \neq 0 \in \mathbb{F}_q$.

14.1.4 Hypercubes

14.1.30 Definition A *d-dimensional hypercube* of order n is an $n \times \cdots \times n$ array with n^d points based on n distinct symbols with the property that if any single coordinate is fixed, each of the n symbols occurs exactly n^{d-2} times in that subarray. Such a hypercube is of *type* j, $0 \leq j \leq d-1$ if whenever any j of the coordinates are fixed, each of the n symbols appears n^{d-j-1} times in that subarray. Note that the definition implies that a hypercube of type j is also of types $0, 1, \ldots, j-1$.

14.1.31 Definition Two hypercubes are *orthogonal* if, when superimposed, each of the n^2 ordered pairs appears n^{d-2} times. Again the $d = 2$ case reduces to that of latin squares. A set of $t \geq 2$ hypercubes is *orthogonal* if every pair of distinct hypercubes is orthogonal.

14.1.32 Theorem [1864] The maximum number of mutually orthogonal hypercubes of order $n \geq 2$, dimension $d \geq 2$, and fixed type j with $0 \leq j \leq d-1$ is bounded above by

$$\frac{1}{n-1}\left(n^d - 1 - \binom{d}{1}(n-1) - \binom{d}{2}(n-1)^2 - \cdots - \binom{d}{j}(n-1)^j\right).$$

14.1.33 Corollary The maximum number of order n, dimension d, and type 1 hypercubes is bounded above by

$$N_d(n) \leq \frac{n^d - 1}{n-1} - d.$$

14.1.34 Remark In the case that $d = 2$, $N_d(n)$ reduces to the familiar bound of $n-1$ for sets of MOLS of order n. As was the case for $d = 2$, the bound for $d > 2$ can always be realized when n is a prime power.

14.1.35 Corollary There are at most

$$(n-1)^{d-1} + \binom{d}{d-1}(n-1)^{d-2} + \cdots + \binom{d}{j+1}(n-1)^j$$

hypercubes of order n, type j, and dimension d.

14.1.36 Theorem The polynomials $a_1x_1 + \cdots + a_dx_d$ with

1. the elements $a_i \in \mathbb{F}_q$ for $i = 1, \ldots, d$ with at least $j+1$ of the $a_i \neq 0$,
2. and $(a'_1, \ldots, a'_d) \neq e(a_1, \ldots, a_d)$ for any $e \neq 0 \in \mathbb{F}_q$, represent a complete set of mutually orthogonal hypercubes of dimension d, order q, and type j.

14.1.37 Remark In [2141] another definition of orthogonality for hypercubes, called *equi-orthogonality* is studied. In [987, 988] sets of hypercubes using various other definitions of orthogonality are considered. Such stronger definitions of orthogonality turn out to be useful in the study of MDS codes (see Section 15.1). In one definition, not only does one keep track of the total number of times that ordered pairs occur, but their locations are

cube 1	cube 2	cube 3	cube 4	cube 5	cube 6	cube 7	cube 8	cube 9	cube 10
012	012	012	012	000	000	012	012	012	012
120	201	012	012	111	111	120	201	201	120
201	120	012	012	222	222	201	120	120	201
012	012	120	201	111	222	120	201	120	201
120	201	120	201	222	000	201	120	012	012
201	120	120	201	000	111	012	012	201	120
012	012	201	120	222	111	201	120	201	120
120	201	201	120	000	222	012	012	120	201
201	120	201	120	111	000	120	201	012	012
$x+y$	$2x+y$	$y+z$	$y+2z$	$x+z$	$x+2z$	$x+y$ $+z$	$2x+y$ $+2z$	$2x+y$ $+z$	$x+y$ $+2z$

Figure 14.1.1 A complete set of mutually orthogonal cubes of order 3.

also taken into account. In other definitions, one studies various notions of orthogonality involving more than the usual two hypercubes at a time. In all of these definitions, polynomials over finite fields are used to construct complete sets of such orthogonal hypercubes of prime power orders.

14.1.38 Remark In [2720] sets of very general mutually orthogonal frequency hyperrectangles of prime power orders are constructed using linear polynomials over finite fields.

14.1.5 Connections to affine and projective planes

14.1.39 Remark Affine and projective planes are discussed in Section 14.3. We first state the following fundamental result; and then discuss a few other related results.

14.1.40 Theorem [353], [700, Theorem III.3.20] There exists a projective plane (or an affine plane) of order n if and only if there exists a complete set of MOLS of order n.

14.1.41 Definition Two complete sets of MOLS of order n are *isomorphic* if after permuting the rows, permuting the columns with a possibly different permutation, and permuting the symbols with a third possibly different permutation of each square of the first set, we obtain the second set of MOLS. See Part III of [700] for further discussion of non-isomorphic sets of MOLS, affine, and projective planes.

14.1.42 Conjecture If p is a prime, any two complete sets of MOLS of order p are isomorphic.

14.1.43 Remark The above conjecture is only known to be true for $p = 3, 5, 7$. Truth of the conjecture would imply that all planes of prime order are Desarguesian.

14.1.44 Theorem [2899, 2900] For $q = p^n$, let $0 \leq k < n$, $N = (q-1)/(q-1, p^k-1)$ and set $e = q - N$. Let u be a primitive N-th root of unity in $\mathbb{F}_q$. Assume that $x^{p^k} + c_i x$ is a permutation polynomial for e elements $c_1, \ldots, c_e \in \mathbb{F}_q$, where one can assume that

$c_1 - 1 = c_2$. Let $a \neq 0$ and c_1 be such that $f(x) = ax^{p^k} + c_1 x$ is an orthomorphism of $\mathbb{F}_q$ (so f is a permutation polynomial with $f(0) = 0$, and $f(x) - x$ is also a permutation). Let $d_i = c_1 - c_i$. Then the polynomials $au^j x^{p^k} + c_1 x + y, j = 1, \ldots, N; d_i x + y, i = 3, \ldots, e; x + y$ represent a complete set of $q - 1$ MOLS of order q.

14.1.45 Corollary For each $n \geq 2$ and any odd prime p, the above construction gives $\tau(n) \geq 2$, non-isomorphic complete sets of MOLS of order p^n, where $\tau(n)$ denotes the number of positive divisors of n.

14.1.46 Example For any odd prime p, this construction gives an example of a non-Desarguesian affine translation plane of order p^2, constructed without the use of a right quasifield as used in [812].

14.1.47 Remark For $q = 9$, let $\mathbb{F}_9$ be generated by the primitive polynomial $f(x) = x^2 + 2x + 2$ over $\mathbb{F}_3$. Let α be a root of $f(x)$. The Desarguesian plane of order 9 may be constructed by using the polynomials $\alpha^i x + y, i = 0, \ldots, 7$. Since $u = \alpha^2$ is a primitive 4-th root of unity, the construction from the above corollary leads to the polynomials $\alpha x^3 + y, \alpha^3 x^3 + y, \alpha^5 x^3 + y, \alpha^7 x^3 + y$ which represent four MOLS of order 9. To extend these four MOLS to a complete set of 8 MOLS of order 9, we consider the polynomials $x + y, \alpha^2 x + y, \alpha^4 x + y, \alpha^6 x + y$. Thus four of the latin squares are the same in both the Desarguesian and non-Desarguesian constructions.

14.1.6 Other finite field constructions for MOLS

14.1.48 Remark There are other finite field constructions for sets of MOLS; here we briefly allude to a few of them which are described in much more detail in [700]. Quasi-difference matrices and $V(m, t)$ vectors are discussed in Section VI.17.4; self-orthogonal latin squares are considered in Section III.5.6; MOLS with holes are considered in Section III.1.7; starters are studied in VI.55.; and atomic latin squares are studied in Section III.1.6.

See Also

§14.3	Discusses affine and projective planes.
§14.5	Discusses block designs.
[700]	Part III discusses latin squares.
[700]	Part III, Section 3 discusses sets of MOLS.
[1863]	Discusses topics in discrete mathematics with topics motivated by latin squares.

References Cited: [353, 394, 395, 700, 812, 987, 988, 1446, 1863, 1864, 1975, 2040, 2141, 2159, 2163, 2720, 2899, 2900]

14.2 Lacunary polynomials over finite fields

Simeon Ball, *Universitat Politècnica de Catalunya*
Aart Blokhuis, *Eindhoven University of Technology*

14.2.1 Introduction

14.2.1 Remark In 1970 Rédei published his treatise *Lückenhafte Polynome über endlichen Körpern* [2428], soon followed by the English translation *Lacunary Polynomials over Finite Fields* [2429], the title of this chapter. One of the important applications of his theory is to give information about the following two sets.

14.2.2 Definition For $f\colon \mathbb{F}_q \to \mathbb{F}_q$, or $f \in \mathbb{F}_q[X]$ define the set of directions (slopes of secants of the graph):

$$D(f) := \left\{ \frac{f(x)-f(y)}{x-y} \,|\, x \neq y \in \mathbb{F}_q \right\}.$$

14.2.3 Definition For $f \in \mathbb{F}_q[X]$ let

$$P(f) := \{m \in \mathbb{F}_q \,|\, f(X) + mX \text{ is a permutation polynomial}\}.$$

14.2.4 Remark The sets $P(f)$ and $D(f)$ partition $\mathbb{F}_q$. If $(f(x)-f(y))/(x-y) = m$ then the polynomial $f(x)+mx = f(y)+my$, so m is a direction determined by f precisely when $f(X)+mX$ is *not* a permutation polynomial (on $\mathbb{F}_q$).

14.2.2 Lacunary polynomials

14.2.5 Definition Let K be a (finite) field. A polynomial $f \in K[x]$ is *fully reducible* if K is a splitting field for f, that is, if f factors completely into linear factors in $K[X]$.

14.2.6 Definition Denote by f° the degree of f, and by $f^{\circ\circ}$ the second degree, the degree of the polynomial we obtain by removing the leading term.

14.2.7 Definition If $f^{\circ\circ} < f^\circ - 1$ then f is *lacunary* and the difference $f^\circ - f^{\circ\circ}$ is the *gap*.

14.2.8 Remark We want to survey what is known about lacunary polynomials (with a large gap) that are fully reducible. In many applications however the gap is not between the degree and the second degree, so instead of being of the form $f(X) = X^n + h(X)$, where $h^\circ \leq n-2$, it is of the more general form $f(X) = g(X)X^n + h(X)$, where $h^\circ \leq n-2$, for some polynomial g.

14.2.9 Example For $d \,|\, (q-1)$ the field $K = \mathbb{F}_q$ contains the d-th roots of unity, so the polynomial $X^d - a^d$ is fully reducible.

14.2.10 Remark In many applications the degree $f^\circ = q$, as is the case in the following examples.

14.2.11 Example The lacunary polynomials $X^q + c$, $X^q - X$, and if q is odd then $X^q \pm X^{(q+1)/2}$ and $X^q \pm 2X^{(q+1)/2} + X$, are fully reducible in $\mathbb{F}_q[X]$.

14.2.12 Theorem [2429] Let $f(X) = X^p + g(X)$, with $g^\circ = f^{\circ\circ} < p$, be fully reducible in $\mathbb{F}_p[X]$, p prime. Then either g is constant, or $g = -X$ or g° is at least $(p+1)/2$.

14.2.13 Remark Let $s(X)$ be the zeros polynomial of f, that is the polynomial with the same set of zeros as f, but each with multiplicity one. So $s = \gcd(f, X^p - X)$. It follows that

$$s \,|\, f - (X^p - X) = X + g.$$

We may write $f = s \cdot r$, where r is the fully reducible polynomial that has the zeroes of f with multiplicity one less. Hence r divides the derivative $f' = g'$. So we conclude that

$$f = s \cdot r \mid (X + g)g'.$$

If the right hand side is zero, then either $g = -X$, corresponding to the fully reducible polynomial $f(X) = X^q - X$, or $g' = 0$ which (since $g^\circ < p$) implies $g(X) = c$ for some $c \in K$ and $f(X) = X^p + c = (X + c)^p$. If the right hand side is nonzero, then, being divisible by f, it has degree at least p, so $g^\circ + g^\circ - 1 \geq p$ which gives $g^\circ \geq (p + 1)/2$.

14.2.14 Remark In the next section we see how this result can be applied to obtain information about the number of directions determined by a function.

14.2.3 Directions and Rédei polynomials

14.2.15 Definition Let $AG(2, q)$ be the Desarguesian affine plane of order q, where points of $AG(2, q)$ are denoted by pairs (a, b), $a, b \in \mathbb{F}_q$.

14.2.16 Definition Let $PG(2, q)$ be the Desarguesian projective plane of order q with homogeneous point coordinates $(a : b : c)$ and line coordinates $[u : v : w]$. The point $(a : b : c)$ is *incident* with the line $[u : v : w]$ precisely when $au + bv + cw = 0$. The equation of the line $[u : v : w]$ is then $uX + vY + wZ = 0$.

14.2.17 Remark We consider $AG(2, q)$ as part of the projective plane $PG(2, q)$ where $[0 : 0 : 1]$ is the line at infinity, the line with equation $Z = 0$. The affine point (a, b) corresponds to the projective point $(a : b : 1)$.

14.2.18 Definition Let $u = (u_1, u_2)$ and $v = (v_1, v_2)$ be two affine points. The pair u, v determines the *direction* m if the line joining them has slope m, or equivalently, if $(u_2 - v_2)/(u_1 - v_1) = m$.

14.2.19 Definition Let R be a set of q points in $AG(2, q)$. We define $D_R \subseteq \mathbb{F}_q \cup \{\infty\}$ to be the set of directions determined by the pairs of points in R.

14.2.20 Remark The reason we take R to have size q is two-fold. Firstly, in Rédei's formulation of the problem R is the graph of a function f and $D_R = D_f$. Secondly, any set with more than q points determines all directions, by the pigeon hole principle: there are exactly q lines in every parallel class, so if $|R| > q$, then there is a line with at least two points of R in each parallel class. For results concerning the case $|R| < q$, see [2739].

14.2.21 Definition With R we associate its *Rédei polynomial*

$$F(U, W) = \prod_{(a,b)\in R} (W + aU + b).$$

14.2.22 Lemma If the direction $m \notin D_R$ then $F(m, W) = W^q - W$.

14.2.23 Lemma If the direction $m \in D_R$, then $F(m, W)$ is a fully reducible lacunary polynomial of degree q, and second degree at most $|D_R| - 1$.

14.2.24 Theorem [320, Theorem 1] Let R be a set of q points in $AG(2,q)$, and let $N = |D_R|$. Then either $N = 1$, or $N \geq (q+3)/2$, or $2 + (q-1)/(p^e+1) \leq N \leq (q-1)/(p^e-1)$ for some e, $1 \leq e \leq \lfloor n/2 \rfloor$.

14.2.4 Sets of points determining few directions

14.2.25 Remark The third case in Theorem 14.2.24, $2 + (q-1)/(p^e+1) \leq N \leq (q-1)/(p^e-1)$ for some e satisfying $1 \leq e \leq \lfloor n/2 \rfloor$, is not sharp. The following are some examples of functions that determine few directions.

14.2.26 Example The function $f(X) = X^{(q+1)/2}$, where q is odd, determines $(q+3)/2$ directions.

14.2.27 Example The function $f(X) = X^s$, where $s = p^e$ is the order of a subfield of $\mathbb{F}_q$, determines $(q-1)/(s-1)$ directions.

14.2.28 Example The function $f(X) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_s}(X)$, the trace from $\mathbb{F}_q$ to the subfield $\mathbb{F}_s$, determines $(q/s)+1$ directions.

14.2.29 Example If $f(X) \in \mathbb{F}_q[X^s]$, where s is the order of a subfield of $\mathbb{F}_q$ and is chosen maximal with this property, in other words, f is $\mathbb{F}_s$-linear (apart from the constant term) but not linear over a larger subfield, then $(q/s)+1 \leq N \leq (q-1)/(s-1)$.

14.2.30 Remark Motivated by the form of the examples the following theorem was obtained (in a number of steps) by Ball, Blokhuis, Brouwer, Storme and Szőnyi. Initial results are in [320], then the classification was all but obtained in [319], and completed in [184].

14.2.31 Theorem [184] If, for $f\colon \mathbb{F}_q \to \mathbb{F}_q$, with $f(0) = 0$, the number $N = |D(f)| > 1$ of directions determined by f is less than $(q+3)/2$, then for a subfield $\mathbb{F}_s$ of $\mathbb{F}_q$

$$\frac{q}{s} + 1 \leq N \leq \frac{q-1}{s-1},$$

and if $s > 2$ then f is $\mathbb{F}_s$-linear.

14.2.32 Remark This result is obtained using several lemmas about fully reducible lacunary polynomials which are of independent interest.

14.2.33 Lemma [2429, Satz 18] Let $s = p^e$ be a power of p with $1 \leq s < q$. If

$$X^{q/s} + g(X) \in \mathbb{F}_q[X] \setminus \mathbb{F}_q[X^p]$$

is fully reducible over $\mathbb{F}_q$ then either $s = 1$ and $g(X) = -X$ or

$$g^\circ \geq ((q/s)+1)/(s+1).$$

14.2.34 Lemma [184] Let s be a power of p with $1 \leq s < q$ and suppose that

$$X^{q/s} + g(X) \in \mathbb{F}_q[X] \setminus \mathbb{F}_q[X^p]$$

is fully reducible over $\mathbb{F}_q$. If $s > 2$, $g^\circ = q/s^2$ and $2(g')^\circ < g^\circ$ then $X^{q/s} + g(X)$ is $\mathbb{F}_s$-linear.

14.2.35 Remark Theorem 14.2.31 completely characterizes the case in which the number of directions is *small*, that is less than $(q+3)/2$. In the case that $q = p$ is prime, $N < (p+3)/2$ implies $N = 1$, and the characterisation of $N = (p+3)/2$ directions was given by Lovász and Schrijver [1948].

14.2.36 Theorem [1948] If $f \in \mathbb{F}_p[X]$, p prime, determines $(p+3)/2$ directions, then $f(X) = X^{(p+1)/2}$ up to affine equivalence.

14.2.37 Remark Much more can be said in this case, the following surprising theorem by Gács [1145] shows that there is a huge gap in the spectrum of possible number of directions.

14.2.38 Theorem [1145] If the number of directions determined by $f \in \mathbb{F}_p[X]$, p prime, is more than $(p+3)/2$, then it is at least $\left\lceil \frac{2}{3}(p-1) \right\rceil + 1$.

14.2.39 Remark This bound is almost tight, there are examples that determine $\frac{2}{3}(p-1)+2$ directions if $p \equiv 1 \pmod 3$. Progress was made using Gács' approach in [189] indicating that a further gap is possible from $2p/3$ to $3p/4$. If there is an example with less than $3p/4$ directions then lines meet the graph of f in at most 3 points or at least $p/4$. Futhermore, if there are 3 lines meeting the graph of f in more than 3 points then the graph of f is contained in these 3 lines. There are examples that determine $\frac{3}{4}(p-1)+2$ directions if $p \equiv 1 \pmod 4$ and some constructions where $|D(f)| \approx 7p/9$ can be found in [1413].

14.2.40 Remark For results concerning the case $q = p^2$, see [1146]. For related results on functions $f\colon \mathbb{F}_q^k \to \mathbb{F}_q$, with $k \geq 2$, that determine few directions, see [185], and for results on functions $f, g\colon \mathbb{F}_q \to \mathbb{F}_q$, where the set

$$P(f,g) = \{(r,s) \in \mathbb{F}_q^2 \mid X + rf(X) + sg(X) \text{ is a permutation polynomial}\}$$

is large [190].

14.2.5 Lacunary polynomials and blocking sets

14.2.41 Remark Let R be a subset of $AG(2,q)$ of size q. The set of points of $PG(2,q)$

$$B = \{(a:b:1) \mid (a,b) \in R\} \cup \{(1:m:0) \mid m \in D_R\}$$

has the property that every line of $PG(2,q)$ intersects B.

14.2.42 Definition A *blocking set* of $PG(2,q)$ is a set of points B of $PG(2,q)$ with the property that every line of is incident with a point of B.

14.2.43 Lemma [356] A blocking set of $PG(2,q)$ has at least $q+1$ points and equality can only be obtained if these points all are on a line.

14.2.44 Definition A blocking set of $PG(2,q)$ that contains a line is *trivial*.

14.2.45 Remark We tacitly assume that all blocking sets under consideration are *minimal*, so they do not contain a proper subset that is also a blocking set. For blocking sets of non-Desarguesian planes and for further reading on blocking sets see [318, 327, 427, 429, 430, 1144, 1147] and for more recent references, see Remark 14.2.54.

14.2.46 Lemma [317] Suppose that B is a blocking set of size $q+k+1$ and that $(1:0:0) \in B$ and assume that the line with equation $Z = 0$, that is $[0:0:1]$ is a tangent to B. Then the non-horizontal lines $[1:u:v]$ are blocked by the affine points of B and the Rédei polynomial of the affine part of B can be written as

$$F(V,W) = (V^q - V)G(V,W) + (W^q - W)H(V,W),$$

where G and H are of total degree k in the variables V and W.

14.2.47 Lemma [317] Let F_0 denote the part of F that is homogeneous of degree $q+k$, and let G_0 and H_0 be the parts of G and H that are homogeneous of total degree k. Restricting to the terms of total degree $q+k$ we obtain the homogeneous equation

$$F_0 = V^q G_0 + W^q H_0,$$

with

$$F_0(V,W) = \prod_{(a:b:1)\in B} (bV + W).$$

Writing $f(W) = F_0(1,W)$ and defining g and h analogously, we obtain a one-variable fully reducible lacunary polynomial in $\mathbb{F}_q[W]$,

$$f(W) = g(W) + W^q h(W).$$

14.2.48 Lemma [318] Let $f \in \mathbb{F}_q[X]$ be fully reducible, and suppose that $f(X) = X^q g(X) + h(X)$, where g and h have no common factor. Let k be the maximum of the degrees of g and h. Then $k = 0$, or $k = 1$ and $f(X) = a(X^q - X)$ for some $a \in \mathbb{F}_q^*$, or q is prime and $k \geq (q+1)/2$, or q is a square and $k \geq \sqrt{q}$, or $q = p^{2e+1}$ for some prime p and $k \geq p^{e+1}$.

14.2.49 Theorem [427] A non-trivial blocking set B in $PG(2,q)$, q square, has at least $q + \sqrt{q} + 1$ points. If equality holds then B consists of the points of a subplane of order $\sqrt{q}$.

14.2.50 Theorem [318] A non-trivial blocking set B in $PG(2,q)$, $q = p^{2e+1}$, p prime, $q \neq p$, has at least $q + p^{e+1} + 1$ points. This bound is sharp only in the case $e = 1$.

14.2.51 Theorem [317] A non-trivial blocking set B in $PG(2,p)$, p prime, has at least $\frac{3}{2}(p+1)$ points. If equality holds then every point of B is on precisely $\frac{1}{2}(p-1)$ tangents.

14.2.52 Remark The bound in Theorem 14.2.51 was conjectured in [825].

14.2.53 Remark The proof of Lemma 14.2.48 leads to the following divisibility condition

$$f | (Xg + h)(h'g - g'h).$$

It would be good (and probably not infeasible) to characterize the case of equality in the case p is prime, that is find all f, g and h with f of degree $q + (q+1)/2$, g and h of degree at most $(q+1)/2$ and $f \hat{=} (Xg+h)(h'g - g'h)$, where $a \hat{=} b$ means there exists a scalar $c \in \mathbb{F}_q$ such that $a = cb$. This is the subject of the next section.

14.2.54 Remark Blocking sets in $PG(2,p^n)$, p prime, of size less than $3(p^n+1)/2$ have been classified for $n = 2$ [2740] and $n = 3$ [2402] and they come from the construction in Remark 14.2.41. However, for $n \geq 4$, there are examples known which are not of this form. These examples, called linear blocking sets, include those obtained by the construction in Remark 14.2.41. It is conjectured that all small blocking sets are linear blocking sets. More precisely, we have the following conjecture which is called the linearity conjecture. For recent articles concerning this conjecture see [1860, 1964, 1965, 2393, 2738, 2740].

14.2.55 Conjecture [2738] If B is a blocking set in $PG(2,p^n)$, p prime, of less than $3(p^n+1)/2$ points then there exists an n-dimensional subspace U of $PG(3n-1,p)$ with the property that every point of B, when viewed as an $(n-1)$-dimensional subspace of $PG(3n-1,p)$, has non-trivial intersection with U.

14.2.6 Lacunary polynomials and blocking sets in planes of prime order

14.2.56 Remark The blocking set problem in $PG(2,p)$, p prime, leads one to search for polynomials $f(X)$, $g(X)$, $h(X)$, where $f = X^p g + h$ factors completely into linear factors and g and h

have degree at most $\frac{1}{2}(p+1)$. More precisely, given a blocking set B of size $\frac{3}{2}(p+1)$, for each point $P \in B$, and each tangent ℓ passing through P, there is a polynomial f with the above property. A factor of f of multiplicity e corresponds to a line incident with P distinct from ℓ meeting B in $e+1$ points.

14.2.57 Remark The equation $f \hat{=} (Xg+h)(h'g-g'h)$ has several infinite families of solutions, and some sporadic ones, not all of them necessarily corresponding to blocking sets.

14.2.58 Theorem [321] The following list contains all non-equivalent solutions for $f = X^p g + h$, where f factors completely into linear factors and g and h have degree at most $\frac{1}{2}(p+1)$, for $p < 41$.

1. (For odd p, say $p = 2r+1$.) Take $f(X) = X\prod(X-a)^3$ where the product is over the nonzero squares a. Then f satisfies $f(X) = X(X^r-1)^3 = X^p g + h$ with $g(X) = X^r - 3$, $h(X) = 3X^{r+1} - X$. This would correspond to line intersections of the lines incident with P (with frequencies written as exponents) 1^r, 2^2, 4^r. For $p = 7$ this is the function for the blocking set $\{(1:0:0),(0:1:0),(0:0:1)\} \cup \{(a:b:1) \mid a,b \in \{1,2,4\}\}$.
2. (For $p = 4t+1$.) Take $f(X) = X\prod(X-a)\prod(X-b)^4$ where the product is over the nonzero squares a and fourth powers b. Here $f(X) = X(X^{2t}-1)(X^t-1)^4 = X^p g + h$ with $g(X) = X^{2t} - 4X^t + 5$ and $h(X) = -5X^{2t+1} + 4X^{t+1} - X$. This would correspond to line intersections 1^{2t}, 2^{t+2}, 6^t.
3. (For $p = 4t+1$.) Take $f(X) = X^{t+1}\prod(X-a)\prod(X-b)^2$ where the product is over the nonzero squares a and fourth powers b. Here $f(X) = X^{t+1}(X^{2t}-1)(X^t-1)^2 = X^p g + h$ with $g(X) = X^t - 2$ and $h(X) = 2X^{2t+1} - X^{t+1}$. This would correspond to line intersections 1^{2t}, 2^t, 4^t $(t+2)^2$. For $p = 13$ this is a function for the blocking set $\{(1:0:0),(0:1:0),(0:0:1)\} \cup \{(1:a:0),(0:1:a),(a:0:1) \mid a^3 = -1\} \cup \{(b:c:1) \mid b^3 = c^3 = 1\}$.
4. (For $p = 13$.) Take $f(X) = X\prod(X-a)^4\prod(X-\frac{1}{2}a)$ where the product is over the values a with $a^3 = 1$. Here $f(X) = X(X^3-1)^4(X^3-\frac{1}{8}) = X^p g + h$ with $g(X) = X^3 + 4$ and $h(X) = 5X^7 - 5X^4 - 5X$. This corresponds to line intersections 1^6, 2^4, 5^4, and indeed occurs.
5. Take $f(X) = X^p - X^{(p+1)/2} = X^{(p+1)/2}\prod(X-a)$ where the product is over the nonzero squares a.
6. Take $f(X) = X^p - 2X^{(p+1)/2} + X = X\prod(X-a)^2$ where the product is over the nonzero squares a.

14.2.59 Remark These lacunary polynomials are just weighted subsets of the projective line, so equivalence means that $f = X^p g + h$ is equivalent to those polynomials obtained under the maps $f(X) \mapsto (cX+d)^{3(p+1)/2} f((aX+b)/(cX+d))$, for some $a,b,c,d \in \mathbb{F}_p$, where $ad \neq bc$.

14.2.60 Theorem [321] Let B be a non-trivial blocking set in $PG(2,p)$ of size $\frac{3}{2}(p+1)$, where p is a prime less than 41. Then either there is a line incident with $(p+3)/2$ points of B (and hence is the example characterized in Theorem 14.2.36) or $p \in \{7,13\}$ and there is a unique other example in both cases.

14.2.61 Conjecture [321] The restriction $p < 41$ is unnecessary in the above theorem.

14.2.7 Lacunary polynomials and multiple blocking sets

14.2.62 Definition A t-fold blocking set B of $PG(2,q)$ is a set of points such that every line is incident with at least t points of B.

14.2.63 Theorem [326] Let B be a t-fold blocking set in $PG(2,q)$, $q=p^h$, p prime, of size $t(q+1)+c$. Let $c_2=c_3=2^{-1/3}$ and $c_p=1$ for $p>3$.

1. If $q=p^{2d+1}$ and $t<q/2-c_p\,q^{2/3}/2$, then $c\geq c_p\,q^{2/3}$, unless $t=1$ in which case B, with $|B|<q+1+c_p\,q^{2/3}$, contains a line.
2. If $4<q$ is a square, $t<q^{1/4}/2$ and $c<c_p\,q^{2/3}$, then $c\geq t\sqrt{q}$ and B contains the union of t disjoint Baer subplanes, except for $t=1$ in which case B contains a line or a Baer subplane.
3. If $q=p^2$, p prime, and $t<q^{1/4}/2$ and $c<p\left\lceil\frac{1}{4}+\sqrt{\frac{p+1}{2}}\right\rceil$, then $c\geq t\sqrt{q}$ and B contains the union of t disjoint Baer subplanes, except for $t=1$ in which case B contains a line or a Baer subplane.

14.2.64 Remark For more precise results in the case $t=2$ see [187]; for $t=3$ see [183]; for $q=p^3$ see [2401, 2402, 2403]; for $q=p^{6n+3}$ see [326]; and for $q=p^{6n}$ see [326, 2403].

14.2.65 Remark The proof of Theorem 14.2.63 starts with the main theorem of [328] on fully reducible lacunary polynomials.

14.2.66 Theorem [328] Let $f\in\mathbb{F}_q[X]$, $q=p^n$, p prime, be fully reducible, $f(X)=X^q g(X)+h(X)$, where $(g,h)=1$. Let $k=\max(g^\circ,h^\circ)<q$. Let e be maximal such that f is a p^e-th power. Then we have one of the following:

1. $e=n$ and $k=0$;
2. $e\geq 2n/3$ and $k\geq p^e$;
3. $2n/3>e>n/2$ and $k\geq p^{n-e/2}-(3/2)p^{n-e}$;
4. $e=n/2$ and $k=p^e$ and $f(X)=a\mathrm{Tr}\,(bX+c)+d$ or $f(X)=a\,\mathrm{Norm}(bX+c)+d$ for suitable constants a,b,c,d. Here Tr and Norm respectively denote the trace and norm function from $\mathbb{F}_q$ to $\mathbb{F}_{\sqrt{q}}$;
5. $e=n/2$ and $k\geq p^e\left\lceil\frac{1}{4}+\sqrt{(p^e+1)/2}\right\rceil$;
6. $n/2>e>n/3$ and $k\geq p^{n/2+e/2}-p^{n-e}-p^e/2$, or if $3e=n+1$ and $p\leq 3$, then $k\geq p^e(p^e+1)/2$;
7. $n/3\geq e>0$ and $k\geq p^e\lceil(p^{n-e}+1)/(p^e+1)\rceil$;
8. $e=0$ and $k\geq(q+1)/2$;
9. $e=0$, $k=1$ and $f(X)=a(X^q-X)$.

14.2.67 Remark Lacunary polynomials over finite fields and in particular Redei's theorem, Theorem 14.2.12, and Blokhuis' theorem, Theorem 14.2.51, have also been used in algebra, algebraic number theory, group theory and group factorization. For a survey of these applications, see [2741].

Polynomials over finite fields have been used to tackle a variety of problems associated with incidence geometries. Various extensions of the ideas first used for lacunary polynomials have been studied. This has led to some interesting techniques involving field extensions, algebraic curves which in turn have led to classification, non-existence and stability results concerning subsets of points of a finite projective spaces with a certain given property. For a recent survey, see [186].

See Also

Chapter 8	For more on permutation polynomials over finite fields.
§14.3	For more on affine and projective planes over finite fields.
§14.4	For more on higher dimensional spaces over finite fields.
§14.9	For more on polynomials over finite fields with restricted weights.

References Cited: [183, 184, 185, 186, 187, 189, 190, 318, 319, 320, 326, 327, 328, 317, 321, 356, 427, 430, 429, 825, 1144, 1145, 1146, 1147, 1413, 1860, 1948, 1965, 1964, 2393, 2403, 2401, 2402, 2429, 2428, 2738, 2739, 2740, 2741]

14.3 Affine and projective planes

Gary Ebert, *University of Delaware*
Leo Storme, *Universiteit Gent*

All structures in this section are finite. Reference [1548] is an excellent introduction to projective and affine planes. See Section VII.2 of [700] for a concise description of the Hall, André, Hughes, and Figueroa planes.

14.3.1 Projective planes

14.3.1 Definition A *finite projective plane* is a finite incidence structure of points and lines such that

1. every two distinct points together lie on a unique line;
2. every two distinct lines meet in a unique point;
3. there exists a quadrangle (four points with no three collinear).

14.3.2 Remark If π is a finite projective plane, then there is a positive integer n such that any line of π has exactly $n+1$ points, every point lies on exactly $n+1$ lines, the total number of points is n^2+n+1, and the total number of lines is n^2+n+1. This number n is called the *order* of π.

14.3.3 Construction [1499] The classical examples of finite projective planes are constructed as follows. Let V be a 3-dimensional vector space over the finite field $\mathbb{F}_q$ of order q. Take as *points* the 1-dimensional subspaces of V and as *lines* the 2-dimensional subspaces of V, and let incidence be given by containment. The resulting incidence structure is a finite projective plane of order q, denoted by $\mathrm{PG}(2,q)$. These projective planes are *Desarguesian* since they satisfy the classical configurational theorem of Desargues (for instance, see [552]). Note that this construction shows that there exists a finite projective plane of order q for any prime power q. Alternatively, one may use *homogeneous coordinates* $(x:y:z) = \{(fx, fy, fz) \colon f \in \mathbb{F}_q \backslash \{0\}\}$ for the points of $\mathrm{PG}(2,q)$, and $[a:b:c] = \{[fa, fb, fc] \colon f \in \mathbb{F}_q \backslash \{0\}\}$ for the lines of $\mathrm{PG}(2,q)$, where the point $(x:y:z)$ is incident with the line $[a:b:c]$ if and only if $ax+by+cz=0$.

14.3.4 Remark Some non-classical finite projective planes are discussed in Subsections 14.3.3 to 14.3.5. Many other constructions can be found in [801]. One of the most difficult problems in finite geometry is determining the spectrum of possible orders for finite projective planes. All known examples have prime power order, but it is unknown if this must be true in general. The Bruck-Ryser-Chowla Theorem (Section 14.5) excludes an infinite number of positive integers as possible orders. In addition, order 10 has been excluded via a computer search [1824]. There are precisely four different (*non-isomorphic*, as defined in Subsection 14.3.3) projective planes of order 9, the smallest order for which non-classical examples exist [1823].

An overview of the state of knowledge concerning small projective planes follows:

order n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
existence	y	y	y	y	n	y	y	y	n	y	?	y	n	?	y
number	1	1	1	1	0	1	1	4	0	≥ 1	?	≥ 1	0	?	≥ 22

14.3.2 Affine planes

14.3.5 Definition A *finite affine plane* is a finite incidence structure of points and lines such that

1. any two distinct points together lie on a unique line;
2. for any point P and any line ℓ not containing P, there exists a unique line m through P that has no point in common with ℓ (the "parallel axiom");
3. there exists a triangle (three points not on a common line).

14.3.6 Remark If one defines a *parallelism* on the lines of an affine plane by saying that two lines are parallel if they are equal or have no point in common, then parallelism is an equivalence relation whose equivalence classes are called *parallel classes*. Each parallel class of lines is a partition of the point set, and every line belongs to exactly one parallel class.

14.3.7 Remark If one removes a line ℓ together with all its points from a projective plane π, then one obtains an affine plane $\pi_0 = \pi^\ell$. Two lines of the affine plane π^ℓ are parallel if and only if the projective lines containing them meet the line ℓ in the same point. We call ℓ the *line at infinity* of π_0, and the points of ℓ are called the *points at infinity*. Conversely, to construct a projective plane from an affine plane π_0, create a new point for each parallel class of π_0 and adjoin this new point to each line in that parallel class. Also adjoin a new line that contains all the new points and no other points. The resulting incidence structure is a projective plane π, called the *projective completion* of π_0. The *order* of π_0 is the order of its projective completion.

14.3.8 Construction The classical way to construct finite affine planes is as follows. Take as points the ordered pairs (a, b), with $a, b \in \mathbb{F}_q$, and as lines the sets of points (x, y) satisfying an equation of the form $Y = mX + b$ for some $m, b \in \mathbb{F}_q$ or an equation of the form $X = c$ for some $c \in \mathbb{F}_q$. The resulting structure is an affine plane of order q, denoted by $\mathrm{AG}(2, q)$. Such an affine plane is also *Desarguesian* since the projective completion of $\mathrm{AG}(2, q)$ is (isomorphic to) $\mathrm{PG}(2, q)$. Alternatively, $\mathrm{AG}(2, q)$ may be constructed from a 2-dimensional vector space V over $\mathbb{F}_q$ by taking as points all vectors in V and as lines all cosets of 1-dimensional subspaces, where incidence is then given by containment.

14.3.3 Translation planes and spreads

14.3.9 Definition Let π be a projective plane. A *collineation* (*automorphism*) of π is a bijective map ϕ on the point set of π that preserves collinearity. All collineations of π form the *automorphism group* $\mathrm{Aut}(\pi)$ of π under composition of maps. A *collineation group* of π is any subgroup of $\mathrm{Aut}(\pi)$. Two projective planes are *isomorphic* if there is a bijective map from the point set of one plane to the point set of the other plane that sends collinear points to collinear points.

14.3.10 Definition If ϕ is a collineation of a projective plane π, and ϕ fixes all lines through a point P and all points on a line ℓ, then ϕ is a (P,ℓ)-*perspectivity*. In particular, it is a (P,ℓ)-*elation* if $P \in \ell$.

14.3.11 Definition A projective plane π is (P,ℓ)-*transitive* if for any distinct points A, B not on ℓ and collinear with P ($A \neq P \neq B$), there is a (P,ℓ)-perspectivity ϕ in $\mathrm{Aut}(\pi)$ such that $A^\phi = B$. Similarly, π is (m,ℓ)-*transitive* if it is (P,ℓ)-transitive for all points P on m. If π is (ℓ,ℓ)-transitive for some line ℓ, then ℓ is a *translation line* of π and π is a *translation plane* with respect to ℓ.

14.3.12 Remark If π is a translation plane with respect to a line ℓ, then the affine plane $\pi^\ell = \pi \setminus \ell$ is also a *translation plane*. Most often a translation plane is considered an affine plane, with its line at infinity the translation line. The *translation group* of such an affine plane is the group of all (ℓ,ℓ)-elations, which acts sharply transitively on the points of the affine plane π^ℓ. References [277, 1601] provide extensive information on translation planes.

14.3.13 Remark Translation planes are coordinatized by algebraic structures called *quasifields* (see Section 2.1). Every quasifield has an algebraic substructure called its *kernel*, which in the finite setting is necessarily a finite field. The quasifield is then a finite dimensional vector space over its kernel, and the *dimension* of the translation plane is the dimension of this vector space.

14.3.14 Definition Let $\Sigma = \mathrm{PG}(2t+1,q)$ be a $(2t+1)$-dimensional projective space for some non-negative integer t (see Section 14.4 for the definition of projective space). A *spread* of Σ is a set S of t-subspaces of Σ such that any point of Σ belongs to exactly one element of S. The set-wise stabilizer of S in $\mathrm{Aut}(\Sigma)$ is the *automorphism group* $\mathrm{Aut}(S)$ of the spread.

14.3.15 Construction View the finite field $F = \mathbb{F}_{q^{2t+2}}$ as a $(2t+2)$-dimensional vector space V over its subfield $\mathbb{F}_q$, and let $\Sigma = \mathrm{PG}(2t+1,q)$ be the associated $(2t+1)$-dimensional projective space. If θ is a primitive element of F and $L = \mathbb{F}_{q^{t+1}}$ is the subfield of order q^{t+1}, then for each positive integer i, $\theta^i L$ is a $(t+1)$-dimensional vector subspace of V that represents a t-subspace of Σ. Moreover, $S = \{L, \theta L, \theta^2 L, \ldots, \theta^{q^{t+1}} L\}$ is a spread of Σ. The spreads obtained in this way are *regular* as defined below.

14.3.16 Definition A t-*regulus* of $\mathrm{PG}(2t+1,q)$ is a set R of $q+1$ mutually disjoint t-subspaces such that any line intersecting three elements of R intersects all elements of R. These lines are the *transversals* of R.

14.3.17 Proposition [1504, p. 200] Any three mutually skew t-subspaces of the projective space $\mathrm{PG}(2t+1,q)$ determine a unique t-regulus containing them.

14.3.18 Remark The points covered by a 1-regulus R in $\mathrm{PG}(3,q)$ are the points of a hyperbolic quadric. The transversals to R form another 1-regulus covering the same hyperbolic quadric. This 1-regulus is the *opposite regulus* R^{opp} to R.

14.3.19 Definition Let $q>2$ be a prime power. A spread S in $\mathrm{PG}(2t+1,q)$ is *regular* if for any three elements of S, the t-regulus determined by them is contained in S. (See [1504] for an alternative definition valid for $q=2$.)

14.3.20 Construction (Bruck-Bose [425]) Let $\Sigma \cong \mathrm{PG}(2t+1,q)$ be a hyperplane of $\overline{\Sigma} = \mathrm{PG}(2t+2,q)$, for some integer $t \geq 0$, and let S be a spread of Σ. Define $A(S)$ to be the geometry whose points are the points of $\overline{\Sigma}\backslash\Sigma$, and whose lines are the $(t+1)$-subspaces of $\overline{\Sigma}$ that intersect Σ precisely in an element of S.

14.3.21 Theorem [425] The structure $A(S)$ is an affine translation plane of order q^{t+1} which is at most $(t+1)$-dimensional over its kernel. Conversely, any finite affine translation plane can be constructed in this way for an appropriate choice of t. In particular, every finite translation plane has prime power order. In addition, $A(S)$ is isomorphic to $\mathrm{AG}(2,q^{t+1})$ if and only if S is regular.

14.3.22 Remark The automorphism group of an affine translation plane $A(S)$ is isomorphic to the semidirect product of the translation group with the group of all nonsingular semilinear mappings of the underlying vector space which fix the spread S [104]. The affine translation plane $A(S)$ is completed to a projective plane $P(S)$ by adding the members of the spread S as the points at infinity. Projective planes $P(S_1)$ and $P(S_2)$ are isomorphic if and only if there is a collineation of Σ mapping S_1 to S_2 [1967].

14.3.23 Remark Let $t=1$ above. Replacing a regulus R by its opposite regulus R^{opp} in a regular spread S_0 produces a new spread S which is not regular, provided $q>2$. The associated planes $A(S)$ are the *Hall planes*. Simultaneously replacing mutually disjoint reguli by their opposite reguli in a regular spread S_0 produces a *subregular spread* S, whose associated translation planes $A(S)$ are also called *subregular*. If the set of mutually disjoint reguli in S_0 is "linear" in a well-defined way [424], then the resulting subregular planes are the *André planes* which are two-dimensional over their kernels. Thus Hall planes are André planes, but not necessarily vice versa.

14.3.24 Remark In [1497], a method is given for obtaining a spread of $\mathrm{PG}(3,q^2)$ from a spread of $\mathrm{PG}(3,q)$ for every odd prime power q.

14.3.4 Nest planes

14.3.25 Definition Let S_0 be a regular spread of $\mathrm{PG}(3,q)$. A *nest* N in S_0 is a set of reguli in S_0 such that every line of S_0 belongs to 0 or 2 reguli of N. Thus a nest is a 2-cover of the lines of S_0 which are contained in the nest.

14.3.26 Remark Counting arguments show that the number t of reguli in a nest must satisfy $(q+3)/2 \leq t \leq 2(q-1)$. In particular, we note that q must be odd for nests to exist. If a nest contains t reguli, it is a *t-nest*. If U denotes the $t(q+1)/2$ lines of S_0 contained in the reguli of a t-nest N, there is a natural potential replacement set for U. Namely, if $(q+1)/2$

lines can be found in the opposite regulus to each regulus of N such that the resulting set W of $t(q+1)/2$ lines are mutually disjoint, then $S = (S_0 \setminus U) \cup W$ is a non-regular spread of $\mathrm{PG}(3,q)$ and hence $A(S)$ is a non-Desarguesian translation plane. In this case, the nest N is *replaceable*, and the resulting plane $A(S)$ is a *nest plane*.

14.3.27 Definition An *inversive plane* is a $3-(n^2+1, n+1, 1)$ design (see Section 14.5), for some integer $n \geq 2$. That is, an inversive plane is an incidence structure of n^2+1 points and $n(n^2+1)$ blocks, each block of size $n+1$, such that every three points lie in a unique block. The blocks are the *circles* of the inversive plane.

14.3.28 Construction Let q be any prime power. Take as points the elements of $\mathbb{F}_{q^2}$ together with the symbol ∞. Take as circles the images of $\mathbb{F}_q \cup \{\infty\}$ under the nonsingular linear fractional mappings on $\mathbb{F}_{q^2}$, with the usual conventions on ∞. If incidence is given by containment, this produces an inversive plane with q^2+1 points whose circles have size $q+1$. This inversive plane is *Miquelian* because it satisfies the classical configurational result of Miquel, and is denoted by $M(q)$ [801].

14.3.29 Theorem [424] There is a one-to-one correspondence between the points and circles of $M(q)$, and the lines and reguli of a regular spread of $\mathrm{PG}(3,q)$. There is an associated homomorphism from the stabilizer of the regular spread to the automorphism group of $M(q)$, whose kernel is a cyclic group of order $q+1$.

14.3.30 Remark Using the above correspondence, it is usually easier to search for nests in $M(q)$ rather than directly in a regular spread S_0 of $\mathrm{PG}(3,q)$. Such nests can often be constructed by taking the orbit of some carefully chosen "base" circle under a natural cyclic or elementary abelian subgroup of $\mathrm{Aut}(M(q))$. However, to check if the resulting nest is replaceable, one must pull back to S_0 and work in $\mathrm{PG}(3,q)$. Some nests are replaceable and some are not. Computations involving finite field arithmetic lead to the following results.

14.3.31 Theorem [171, 172, 944, 945, 2359] For any odd prime power $q \geq 5$, there exist replaceable t-nests for $t = q-1, q, q+1, 2(q-1)$. The resulting spreads determine non-Desarguesian translation planes of order q^2 which are two-dimensional over their kernels.

14.3.32 Remark The nesting technique for constructing two-dimensional translation planes is quite robust. In addition to the above examples, replaceable t-nests have been constructed for many values of t in the range $3(q+1)/4 - \sqrt{q}/2 \leq t \leq 3(q+1)/4 + \sqrt{q}/2$; see [173]. Moreover, the translation planes associated with nests often can be characterized by the action of certain collineation groups [1597, 1600, 1602, 1603].

14.3.33 Remark Circle geometries and the notion of subregularity can be extended to higher dimensions. Using algebraic pencils of Sherk surfaces, in [750] several infinite families of non-André subregular translation planes are constructed which are 3-dimensional over their kernels. Proofs use intricate finite field computations involving the trace, norm, and bitrace.

14.3.5 Flag-transitive affine planes

14.3.34 Definition An affine plane is *flag-transitive* if it admits a collineation group which acts transitively on incident point-line pairs.

14.3.35 Remark A straightforward counting argument shows that transitivity on lines implies transitivity on flags for affine planes.

14.3.36 Remark By a celebrated result of Wagner [2871], every finite flag-transitive affine plane is necessarily a translation plane, and hence arises from a spread S of $\mathrm{PG}(2t+1,q)$, for some positive integer t, according to Theorem 14.3.21. The affine plane $A(S)$ is flag-transitive if and only if the spread S admits a transitive collineation group.

14.3.37 Construction Let $F = \mathbb{F}_{q^{2t+2}}$ be treated as a $(2t+2)$-dimensional vector space over its subfield $\mathbb{F}_q$, thus serving as the underlying vector space for $\Sigma = \mathrm{PG}(2t+1,q)$. If θ is a primitive element of $\mathbb{F}$, the collineation $\overline{\theta}$ induced by multiplication by θ is a Singer cycle of Σ; that is, the cyclic group $\langle\overline{\theta}\rangle$ acts sharply transitively on the points and hyperplanes of Σ. If G denotes the Singer subgroup of order $q^{t+1}+1$, let $\mathcal{O}$ denote the partition of the points of Σ into $(q^{t+1}-1)/(q-1)$ G-orbits of size $q^{t+1}+1$ each. As shown in [943], these point orbits are caps when t is odd (see Section 14.4 for the definition of a cap). For future reference we let H denote the index two subgroup of G.

14.3.38 Example [1662] Let q be an odd prime power, and let t be an odd integer. Using the above model, choose $b \in F$ such that $b^{q^{t+1}-1} = -1$. Let $\sigma : F \to F$ via $\sigma : x \mapsto x^q$, and let E denote the subfield of F whose order is q^{t+1}. Then $A_1 = \{x + bx^\sigma : x \in E\}$ represents a t-space Γ_1 of Σ that meets half the G-orbits of $\mathcal{O}$ in two points each (from different H-orbits) and is disjoint from the rest. Similarly, $A_2 = \{bx + b^{\sigma+1}x^\sigma : x \in E\}$ represents a t-space Γ_2 of Σ that meets the G-orbits of $\mathcal{O}$ which are disjoint from Γ_1 in two points each (from different H-orbits). Moreover, $S = \Gamma_1^H \cup \Gamma_2^H$ is a spread of Σ admitting a transitive collineation group, which yields a non-Desarguesian flag-transitive affine plane $A(S)$ of order q^{t+1} with $\mathbb{F}_q$ in its kernel.

14.3.39 Example [1662, 1669] Let q be an odd prime power, and let t be an even integer. Using the notation of Example 14.3.38, Γ_1 now meets every G-orbit of $\mathcal{O}$ in one point each, and hence $S_1 = \Gamma_1^G$ is a spread of Σ which admits a transitive (cyclic) collineation group. The resulting affine plane $A(S_1)$ is a non-Desarguesian flag-transitive affine plane of order q^{t+1} with $\mathbb{F}_q$ in its kernel. If $q \equiv 1 \pmod 4$, then Γ_2 also meets each G-orbit of $\mathcal{O}$ in one point each, and these points lie in H-orbits that are disjoint from Γ_1. Moreover, $S_2 = \Gamma_1^H \cup \Gamma_2^H$ is a spread of Σ admitting a transitive (non-cyclic) collineation group, thereby yielding another non-Desarguesian flag-transitive affine plane $A(S_2)$ of order q^{t+1} with $\mathbb{F}_q$ in its kernel. This plane does not admit a cyclic collineation group acting transitively on the line at infinity. For $q \equiv 3 \pmod 4$, one may obtain such a spread S_2 by replacing Γ_2 with the t-space of Σ represented by $\{\mu x^{q^{t+1}} + \mu b^{q^{t+1}}(x^\sigma)^{q^{t+1}} : x \in E\}$, where $\mu = \theta^{(q^{t+1}-1)/(q-1)}$.

14.3.40 Remark The field automorphism σ in the above examples may be replaced by any element of $\mathrm{Gal}(\mathbb{F}_{q^{2t+2}}/\mathbb{F}_q)$. The resulting planes are non-Desarguesian provided σ does not induce the identity map on the subfield E. Lower bounds are given in [1662, 1669] for the number of mutually non-isomorphic planes obtained as b and σ vary.

14.3.41 Example [1663] Let q be a power of 2, and let $t \geq 2$ be an even integer. Using the notation of Example 14.3.38, let Tr denote the trace from E to $\mathbb{F}_q$, and choose some element $r \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Let Γ' be the t-space of Σ represented by $\{\mathrm{Tr}\,(x) + rx : x \in E\}$. Then Γ' meets every G-orbit of $\mathcal{O}$ in one point each, and hence $S' = (\Gamma')^G$ is a spread of Σ which admits a transitive (cyclic) collineation group. The resulting flag-transitive affine plane $A(S')$ of order q^{t+1} with $\mathbb{F}_q$ in its kernel is non-Desarguesian provided $q^{t+1} > 8$.

14.3.42 Remark Other than the Hering plane [1478] of order 27 and the Lüneburg planes [1966] of order 2^{2d} for odd $d \geq 3$, all known finite flag-transitive affine planes arise from spreads consisting of a single G-orbit or the union of two H-orbits, where G and H are the Singer subgroups defined in Construction 14.3.37. It is shown in [946] that if $q = p^e$ for some odd prime p and some positive integer e and if $\gcd((q^{t+1}+1)/2, (t+1)e) = 1$, then any

flag-transitive affine plane of order q^{t+1} with $\mathbb{F}_q$ in its kernel (other than the above Hering plane) must arise in this way. More can be said for $t = 1, 2$.

14.3.43 Theorem [174] If $q = p^e$ is an odd prime power such that $\gcd((q^2+1)/2, e) = 1$, then any two-dimensional flag-transitive affine plane of order q^2 is isomorphic to one of the planes constructed in Example 14.3.38 with $t = 1$. The number of such isomorphism classes can be determined by Möbius inversion. For $e = 1$ (hence $q = p$ prime), the above gcd condition is necessarily satisfied and the number of isomorphism classes is precisely $(q-1)/2$.

14.3.44 Theorem [168, 175] If $q = p^e$ is an odd prime power such that $\gcd((q^3+1)/2, 3e) = 1$, then any three-dimensional flag-transitive affine plane of order q^3, other than Hering's plane of order 27, is isomorphic to one of the planes constructed in Example 14.3.39 with $t = 2$. For $e = 1$ (hence $q = p$ prime), the number of isomorphism classes of each type arising from Example 14.3.39 is precisely $(q-1)/2$.

14.3.45 Problem For q even, the classification and complete enumeration of finite flag-transitive affine planes of dimension two or three over their kernel remains an open problem. The only known two-dimensional examples are the Lüneburg planes.

14.3.46 Problem The classification of finite flag-transitive affine planes is one of the few open cases in the program announced in [450] to classify all finite flag-transitive linear spaces. For arbitrary dimension over the kernel, it is not known if there exist examples of finite flag-transitive affine planes other than the ones listed above, and the classification seems to be quite difficult. In the projective setting, it is believed that the only flag-transitive projective plane is the Desarguesian one, although this remains an open problem.

14.3.6 Subplanes

14.3.47 Definition Let π be a projective plane with point set $\mathcal{P}$ and line set $\mathcal{L}$. A projective plane π' with point set $\mathcal{P}'$ and line set $\mathcal{L}'$ is a *subplane* of π if $\mathcal{P}' \subseteq \mathcal{P}$ and $\mathcal{L}' \subseteq \mathcal{L}$, and π' inherits its incidence relation from π.

14.3.48 Theorem [422] Let π be a finite projective plane of order n, and let π' be a subplane of π with order $m < n$. Then $n = m^2$ or $m^2 + m \leq n$.

14.3.49 Remark It is unknown whether equality can hold in the above inequality; if so, this would imply that the order $n = m^2 + m$ of π is not a prime power. The case $n = m^2$ is of particular interest. In this case, every point of $\pi \setminus \pi'$ is incident with a unique line of π', and dually every line of $\pi \setminus \pi'$ is incident with a unique point of π'.

14.3.50 Definition A subplane π' of order m in a projective plane π of order $n = m^2$ is a *Baer subplane* of π.

14.3.51 Remark In the classical setting, the lattice of subplanes follows directly from the lattice of subfields. Namely, if $q = p^e$ for some prime p and some positive integer e, then the subplanes of $\mathrm{PG}(2, q)$, up to isomorphism, are precisely $\mathrm{PG}(2, p^k)$ as k varies over all positive divisors of e. So $\mathrm{PG}(2, q)$ has a Baer subplane if and only if q is a square. Moreover, one can easily count the number of subplanes of a given order in this classical (Desarguesian) setting.

14.3.52 Theorem [1499, Lemma 4.20] If q is any prime power and $n \geq 2$ is any integer, then the number of subplanes of order q in $\mathrm{PG}(2, q^n)$, all of which are isomorphic to $\mathrm{PG}(2, q)$, is

$$\frac{q^{3(n-1)}(q^{3n}-1)(q^{2n}-1)}{(q^3-1)(q^2-1)}.$$

In particular, the number of Baer subplanes in $\mathrm{PG}(2, q^2)$ is $q^3(q^3+1)(q^2+1)$.

14.3.53 Remark It is currently unknown if $\mathrm{PG}(2, q^2)$ has the greatest number of Baer subplanes among all projective planes of order q^2. No counter-examples have been found. Amazingly, there are affine planes of order q^2 which contain more affine subplanes of order q than does $\mathrm{AG}(2, q^2)$ [1093].

14.3.54 Definition A *Baer subplane partition*, or BSP for short, of $\mathrm{PG}(2, q^2)$ is a partition of the points of $\mathrm{PG}(2, q^2)$ into subplanes, each isomorphic to $\mathrm{PG}(2, q)$.

14.3.55 Example [423] Consider the full Singer group of order q^4+q^2+1 acting sharply transitively on the points and lines of $\pi = \mathrm{PG}(2, q^2)$. Then the orbits under the Singer subgroup of order q^2+q+1 are Baer subplanes, and the orbit of any one of these Baer subplanes under the complementary Singer subgroup of order q^2-q+1 forms a BSP of π. Such a BSP is *classical*.

14.3.56 Remark It is shown in [170] that any spread of $\mathrm{PG}(5, q)$ admitting a linear cyclic sharply transitive action corresponds to a "perfect" BSP of $\mathrm{PG}(2, q^2)$, and this spread is regular if and only if the BSP is classical. By definition, a BSP is *perfect* if and only if it is an orbit of some Baer subplane under an appropriate Singer subgroup, although the Baer subplane itself need not be a point orbit under a Singer subgroup. Examples 14.3.39 and 14.3.41 for $t = 2$ yield the following result.

14.3.57 Theorem [170] Let $q \neq 2$ be a prime power. Then there exist non-classical BSP's of $\mathrm{PG}(2, q^2)$.

14.3.58 Remark Relatively little is known about the subplane structure of non-Desarguesian planes. There is no known example of a square order projective plane which has been shown not to contain a Baer subplane. However, it is not known if every square order projective plane must contain a Baer subplane. At the other extreme, the Hall planes, the Hughes planes, the Figueroa planes, and many two-dimensional subregular translation planes have been proven to contain subplanes of order two (that is, Fano subplanes). It has been conjectured that every finite non-Desarguesian plane must contain a subplane of order two. More surprisingly, it is shown in [476] that the Hughes plane of order q^2 (q odd) has a subplane of order 3 when $q \equiv 2 \pmod 3$. Extensive, but not exhaustive, computer searches for small q have found no subplanes of order 3 in this plane when $q \equiv 1 \pmod 3$. Very recently [477], subplanes of order 3 have been proven to exist in all odd order Figueroa planes.

14.3.7 Embedded unitals

14.3.59 Remark Reference [204] provides an excellent introduction to the topic of unitals. Proofs and precise statements of most results in this subsection may be found in the above reference.

14.3.60 Definition A *unital* is a $2\text{-}(n^3+1, n+1, 1)$ design for some integer $n \geq 3$ (that is, a geometry having n^3+1 points, with $n+1$ points on each line such that any two distinct points are on exactly one line.)

14.3.61 Remark Here the interest is not in unitals as designs, but in unitals embedded in a projective plane of order n^2. The lines (blocks) of the unital are then the lines of the ambient projective plane which meet the unital in more than one point (and hence in $n+1$ points).

14.3.62 Example Let $\mathrm{PG}(2, q^2)$ be represented using homogeneous coordinates. Then the points $(x : y : z)$ for which $xx^q + yy^q + zz^q = 0$ form a unital. This unital is a *Hermitian curve*.

14.3.63 Construction (Buekenhout [448]) Using the Bruck-Bose representation of Construction 14.3.20, with $t = 1$ for a 2-dimensional translation plane, let S be any spread of Σ and let $\overline{U}$ be an ovoidal cone of $\overline{\Sigma}$ (that is, the point cone over some 3-dimensional ovoid as defined in Section 14.4) that meets Σ in a line of S. Then $\overline{U}$ corresponds to a unital U in $P(S)$ which is tangent to the line at infinity. Also, if $\overline{U}$ is a nonsingular (parabolic) quadric in $\overline{\Sigma}$ that meets Σ in a regulus of the spread S, then $\overline{U}$ corresponds to a unital U in $P(S)$ which meets the line at infinity in $q + 1$ points. Of course, the second construction is valid only for those 2-dimensional translation planes of order q^2 whose associated spread contains at least one regulus.

14.3.64 Remark If the ovoidal cone above is an orthogonal cone (with an elliptic quadric as base), the resulting unital in $P(S)$ is an *orthogonal Buekenhout unital*. Unitals embedded in $P(S)$ which arise from the nonsingular quadric construction are *nonsingular Buekenhout unitals*.

14.3.65 Remark Orthogonal Buekenhout unitals embedded in $\mathrm{PG}(2, q^2)$ have been completely enumerated. In particular, if q is an odd prime, then the number of mutually inequivalent orthogonal Buekenhout unitals in $\mathrm{PG}(2, q^2)$ is $\frac{1}{2}(q + 1)$, one of which is the Hermitian curve. The only nonsingular Buekenhout unital embedded in $\mathrm{PG}(2, q^2)$ is the Hermitian curve. Exhaustive computer searches in [194, 2367] show that there are precisely two inequivalent unitals embedded in each of $\mathrm{PG}(2, 9)$ and $\mathrm{PG}(2, 16)$, the Hermitian curve and one other orthogonal Buekenhout unital. The enumeration of orthogonal and nonsingular Buekenhout unitals in various non-Desarguesian translation planes may be found in [178, 179]. For instance, if $q \geq 5$ is a prime, then, up to equivalence, the Hall plane of order q^2 has $\frac{1}{2}(q + 1)$ nonsingular Buekenhout unitals and $1 + \lfloor \frac{3q}{4} \rfloor$ orthogonal Buekenhout unitals.

14.3.66 Remark In [909], it is shown that the Hall planes contain unitals which are not obtainable from any Buekenhout construction. This is the only infinite family of unitals embedded in translation planes which has been proven to be non-Buekenhout. There are also square-order non-translation planes which are known to contain unitals, necessarily non-Buekenhout. For instance, the Hughes planes of order q^2 are known to contain unitals for all odd prime powers q [2466, 2928]. In [782], the Figueroa planes of order q^6 are shown to contain unitals for any prime power q. In fact, there is no known example of a square-order projective plane which has been shown not to contain a unital.

14.3.8 Maximal arcs

14.3.67 Remark Proofs of almost all results in this subsection may be found in Chapter 12 of [1499].

14.3.68 Definition A $\{k; r\}$-*arc* in $\mathrm{PG}(2, q)$ is a set K of k points such that r is the maximum number of points in K that are collinear. A $\{k; 2\}$-arc is a k-*arc*.

14.3.69 Theorem Let K be a $\{k; r\}$-arc in $\mathrm{PG}(2, q)$. Then $k \leq (q + 1)(r - 1) + 1$.

14.3.70 Definition The $\{k; r\}$-arcs in $\mathrm{PG}(2, q)$ with $k = (q+1)(r-1)+1$ are *maximal* $\{k; r\}$-*arcs*.

14.3.71 Example Singleton points ($r = 1$), the whole plane ($r = q + 1$), and the complement of a line ($r = q$) are *trivial* maximal $\{k; r\}$-arcs. The $\{q + 2; 2\}$-arcs in $\mathrm{PG}(2, q)$ for q even, also called *hyperovals* (see Section VII.2.9 of [700]), are examples of non-trivial maximal $\{k; r\}$-arcs, and have been objects of intense interest for many years.

14.3.72 Lemma If K is a non-trivial maximal $\{k; r\}$-arc in $\mathrm{PG}(2, q)$, then r must be a (proper) divisor of q.

14.3.73 Theorem [188] If $\mathrm{PG}(2, q)$ contains a non-trivial maximal $\{k; r\}$-arc, then q must be even.

14.3.74 Construction [814] Let $X^2 + \beta X + 1$ be an irreducible quadratic polynomial over $\mathbb{F}_q$, q even. Consider the algebraic pencil in $\mathrm{PG}(2, q)$ consisting of the conics $C_\lambda : X_0^2 + \beta X_0 X_1 + X_1^2 + \lambda X_2^2 = 0$ for $\lambda \in \mathbb{F}_q \cup \{\infty\}$. Let A be an additive subgroup of $(\mathbb{F}_q, +)$ of order r, and let K be the set of points which is the union of the conics C_λ for $\lambda \in A$. Then K is a maximal $\{k; r\}$-arc of $\mathrm{PG}(2, q)$.

14.3.75 Construction [2011] Let q be even, and let Tr denote the absolute trace from $\mathbb{F}_q$ to $\mathbb{F}_2$. In $\mathrm{PG}(2, q)$, consider a set $\mathcal{C}$ consisting of conics $C_{\alpha,\beta,\lambda} : \alpha X_0^2 + X_0 X_1 + \beta X_1^2 + \lambda X_2^2 = 0$, where $\alpha, \beta \in \mathbb{F}_q$ with $\mathrm{Tr}(\alpha\beta) = 1$ and $\lambda \in \mathbb{F}_q \cup \{\infty\}$. Define the "composition" of two distinct conics from $\mathcal{C}$ in the following way:

$$C_{\alpha,\beta,\lambda} \oplus C_{\alpha',\beta',\lambda'} = C_{\alpha\oplus\alpha',\beta\oplus\beta',\lambda\oplus\lambda'},$$

where

$$\alpha \oplus \alpha' = \frac{\alpha\lambda + \alpha'\lambda'}{\lambda + \lambda'}, \quad \beta \oplus \beta' = \frac{\beta\lambda + \beta'\lambda'}{\lambda + \lambda'}, \quad \lambda \oplus \lambda' = \lambda + \lambda'.$$

Let $\mathcal{F} \subset \mathcal{C}$ be a set of $2^d - 1$ non-singular conics with common nucleus $(0, 0, 1)$, which is closed under the composition of distinct conics. Then the points of the conics in $\mathcal{F}$, together with $(0, 0, 1)$, form a maximal $\{k; 2^d\}$-arc in $\mathrm{PG}(2, q)$. To obtain one such set $\mathcal{F}$, assume $q = 2^{4m+2}$ and let $\epsilon \in \mathbb{F}_{2^{4m+2}}$ be such that $\mathrm{Tr}(\epsilon) = 1$. Let $A = \{x \in \mathbb{F}_{2^{4m+2}} : x^2 + x \in \mathbb{F}_{2^{2m+1}}\}$, and let $r(\lambda) = \lambda^3 + \epsilon$ for all $\lambda \in A$. Then $|A| = 2^{2m+2}$ and

$$\mathcal{F} = \{C_{1,r(\lambda),\lambda} : \lambda \in A \setminus \{0\}\}$$

is such a subset of $\mathcal{C}$ which determines, as indicated above, a maximal $\{k; 2^{2m+2}\}$-arc in $\mathrm{PG}(2, 2^{4m+2})$. These arcs do not arise from Construction 14.3.74. Other possibilities for $\mathcal{F}$ may be found in [1056, 1396, 1397].

14.3.9 Other results

14.3.76 Remark Semifields (see Section 2.1) are algebraic structures that may be used to coordinatize certain translation planes, called *semifield planes*. These are the only translation planes which are also dual translation planes. Many new examples have recently been found. Chapter 6 of [779] is an excellent source for many of these new developments.

14.3.77 Problem As previously mentioned, all known finite projective (and affine) planes have prime power order, although it is certainly unclear whether this must be true in general. However, it is now known that if a projective plane of order n admits an abelian collineation group of order n^2 or $n^2 - n$, then n must be a prime power [324, 1622]. An equally important open problem is whether any finite projective (or affine) plane of prime order p must be Desarguesian. This appears to be a very difficult problem; the smallest open case is $p = 11$.

14.3.78 Remark A *hyperbolic fibration* of $\mathrm{PG}(3, q)$ is a collection of $q - 1$ hyperbolic quadrics and two lines that partition the points of $\mathrm{PG}(3, q)$. By selecting one of the two reguli ruling each hyperbolic quadric in the fibration, one obtains 2^{q-1} spreads of $\mathrm{PG}(3, q)$, which in turn give rise to 2^{q-1} translation planes of order q^2 which are at most two-dimensional over their kernels. Although there may be some isomorphisms among these planes, this is a very robust method for constructing two-dimensional translation planes (see [176] for isomorphism

counts). An easy example of a hyperbolic fibration is the *hyperbolic pencil*, which is an algebraic pencil of quadrics of the appropriate types. Other examples of hyperbolic fibrations may be found in [169, 177]. All known hyperbolic fibrations have the property that the two lines in the fibration form a conjugate (skew) pair with respect to each of the polarities associated with the $q-1$ hyperbolic quadrics (such hyperbolic fibrations are called *regular* in the literature), and also have the property that all $q-1$ hyperbolic quadrics intersect one of the two skew lines in the same pair of conjugate points with respect to the quadratic extension $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$ (such hyperbolic fibrations are said to *agree* on one of the two skew lines). In [419], it is shown that all hyperbolic fibrations are necessarily regular if q is even (the problem is still open for q odd), and it is also shown for any q that a hyperbolic fibration which agrees on one of its two skew lines is necessarily regular. In [176], it is shown that there is a bijection between regular hyperbolic fibrations which agree on one of their two lines and flocks of a quadratic cone, once a conic of the flock is specified. This further leads to a correspondence with normalized q-clans and certain types of generalized quadrangles.

14.3.79 Remark There are other survey articles on substructures in projective planes. The section on Finite Geometry in *The Handbook of Combinatorial Designs* [700] and the survey article [1502] state the main results on arcs, $\{k;r\}$-arcs, caps, unitals, and blocking sets in $\mathrm{PG}(2,q)$, where exact definitions, tables and supplementary results are provided. In addition, the collected work [779] contains a great variety of results on substructures in $\mathrm{PG}(2,q)$, techniques for investigating these substructures, and important open problems in this area. The *linearity conjecture* on small minimal blocking sets in $\mathrm{PG}(2,q)$ is one of the most important such open problems (see Chapter 3 of [779] for an explicit statement of this conjecture). Proving this conjecture would imply several new results on various substructures in $\mathrm{PG}(2,q)$ as well as in $\mathrm{PG}(n,q)$, for $n>2$. In particular, this would include new results on maximal partial spreads, minihypers, extendability of linear codes, tight sets, and Cameron-Liebler line classes. The investigation of maximal arcs in $\mathrm{PG}(2,q)$ for q even, inspired by the new construction method of Mathon described in Construction 14.3.75, and the investigation of embedded unitals as discussed in Section 14.3.7 are central problems on substructures in projective planes which also merit further research.

See Also

§2.1	For a discussion of traces, norms, and linearized polynomials.
§9.4	For some semifield constructions.
§9.5	For some examples of semifield planes constructed from planar functions.
§13.3	For a discussion of the classical projective groups over finite fields.
§14.4	For a discussion of projective spaces of higher dimensions.
[801]	Develops the notion of inversive planes.
[1548]	Develops the notion of coordinatizing non-Desarguesian projective planes.

References Cited: [104, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 188, 194, 204, 277, 324, 419, 422, 423, 424, 425, 448, 450, 476, 477, 552, 700, 750, 779, 782, 801, 814, 909, 943, 944, 945, 946, 1056, 1093, 1396, 1397, 1478, 1497, 1499, 1502, 1504, 1548, 1597, 1600, 1601, 1602, 1603, 1622, 1662, 1663, 1669, 1823, 1824, 1966, 1967, 2011, 2359, 2367, 2466, 2871, 2928]

14.4 Projective spaces

James W.P. Hirschfeld, *University of Sussex*
Joseph A. Thas, *Ghent University*

14.4.1 Projective and affine spaces

14.4.1 Definition Let $V = V(n+1, F)$, with $n \geq 1$, be an $(n+1)$-dimensional vector space over the field F with zero element 0. Consider the equivalence relation on the elements of $V\backslash\{0\}$ whose equivalence classes are the one-dimensional subspaces of V with the zero deleted. Thus, if $X, Y \in V\backslash\{0\}$, then X is equivalent to Y if $Y = tX$ for some t in $F_0 = F\backslash\{0\}$.

1. The set of equivalence classes is the *n-dimensional projective space over F* and is denoted by $\mathrm{PG}(n, F)$ or, when $F = \mathbb{F}_q$, by $\mathrm{PG}(n, q)$.
2. The elements of $\mathrm{PG}(n, F)$ are *points*; the equivalence class of the vector X is the point $\mathbf{P}(X)$. The vector X is a *coordinate vector* for $\mathbf{P}(X)$ or X is a vector *representing* $\mathbf{P}(X)$. In this case, tX with t in F_0 also represents $\mathbf{P}(X)$; that is, by definition, $\mathbf{P}(tX) = \mathbf{P}(X)$.
3. If $X = (x_0, \ldots, x_n)$ for some basis, then the x_i are the *coordinates* of the point $\mathbf{P}(X)$.
4. The points $\mathbf{P}(X_1), \ldots, \mathbf{P}(X_r)$ are *linearly independent* if a set of vectors $X_1, \ldots, X_r$ representing them is linearly independent.

14.4.2 Definition

1. For any $m = -1, 0, 1, 2, \ldots, n$, a *subspace of dimension m*, or *m-space*, of $\mathrm{PG}(n, F)$ is a set of points all of whose representing vectors form, together with the zero, a subspace of dimension $m+1$ of $V = V(n+1, F)$; it is denoted by Π_m.
2. A subspace of dimension zero is a point; a subspace of dimension -1 is the empty set. A subspace of dimension one is a *line*, of dimension two is a *plane*, of dimension three is a *solid*. A subspace of dimension $n-1$ is a *hyperplane*. A subspace of dimension $n-r$ is a subspace of *codimension r*.

14.4.3 Definition

1. The set of m-spaces of $\mathrm{PG}(n, F)$ is denoted $\mathrm{PG}^{(m)}(n, F)$ or, when $F = \mathbb{F}_q$, by $\mathrm{PG}^{(m)}(n, q)$.
2. For $r, s, m, n \in \mathbb{N}$, let
   (a) $\theta(n, q) = (q^{n+1} - 1)/(q-1)$, also denoted by $\theta(n)$;

(b) $|\mathrm{PG}^{(m)}(n,q)| = \phi(m;n,q)$;
(c) $[r,s]_- = \prod_{i=r}^{s}(q^i-1)$, for $s \geq r$.

14.4.4 Theorem [1499, Chapter 3]
For $n \geq 1$, $m \geq 0$, and q any prime power,

1. $|\mathrm{PG}(n,q)| = \theta(n,q)$;
2. $\phi(m;n,q) = [n-m+1, n+1]_- / [1, m+1]_-$.

14.4.5 Theorem [1499, Chapter 2]

1. A hyperplane is the set of points $\mathbf{P}(X)$ whose vectors $X = (x_0, \ldots, x_n)$ satisfy a linear equation
$$u_0x_0 + u_1x_1 + \cdots + u_nx_n = 0,$$
with $U = (u_0, \ldots, u_n)$ in $F^{n+1}\backslash\{(0,\ldots,0)\}$; it is denoted $\pi(U) = \Pi_{n-1}$.
2. An m-space Π_m is the set of points whose representing vectors $X = (x_0, \ldots, x_n)$ satisfy the equations $XA = 0$, where A is an $(n+1) \times (n-m)$ matrix of rank $n-m$ with coefficients in F.

14.4.6 Remark [1499, Chapter 2] The vector U in the theorem is a *coordinate vector* of the hyperplane; the u_i are *hyperplane* or *tangential coordinates*.

14.4.7 Definition

1. If a point P lies in a subspace Π_m, then P is *incident* with Π_m or, equally well, Π_m is *incident* with P.
2. If Π_r and Π_s are subspaces of $\mathrm{PG}(n,F)$, then the *meet* or *intersection* of Π_r and Π_s, written $\Pi_r \cap \Pi_s$, is the set of points common to Π_r and Π_s; it is also a subspace.
3. The *join* of Π_r and Π_s, written $\Pi_r\Pi_s$, is the smallest subspace containing Π_r and Π_s.

14.4.8 Theorem [1499, Chapter 2] Subspaces have the following properties.

1. If Π_r and Π'_r are both r-spaces in $\mathrm{PG}(n,F)$ and $\Pi'_r \subset \Pi_r$, then $\Pi'_r = \Pi_r$.
2. (Grassmann Identity) If $\Pi_r \cap \Pi_s = \Pi_t$ and $\Pi_r\Pi_s = \Pi_m$, then $r + s = m + t$.
3. A subspace Π_m is the join of $m+1$ linearly independent points; it is also the intersection of $n-m$ linearly independent hyperplanes.
4. Equivalently, the set of all representing vectors of the points of Π_m, together with the zero vector, is the intersection of $n-m$ hyperplanes of the vector space V, which define $n-m$ linearly independent vectors $U = (u_0, \ldots, u_n)$.

14.4.9 Theorem (The principle of duality) [1499, Chapter 2] For any space $S = \mathrm{PG}(n,F)$, there is a *dual* space S^*, whose *points* and *hyperplanes* are respectively the hyperplanes and points of S. For any theorem true in S, there is an equivalent theorem true in S^*. In particular, if T is a theorem in S stated in terms of points, hyperplanes and incidence, the same theorem is true in S^* and gives a dual theorem T^* in S by substituting "hyperplane" for "point" and "point" for "hyperplane". Thus "join" and "meet" are dual. Hence the dual of an r-space in $\mathrm{PG}(n,F)$ is an $(n-r-1)$-space.

14.4.10 Remark For small dimensions, in $\mathrm{PG}(2,F)$, point and line are dual; in $\mathrm{PG}(3,F)$, point and plane are dual, whereas the dual of a line is a line.

14.4.11 Definition

1. If $\mathcal{H}_\infty$ is any hyperplane in $\mathrm{PG}(n,F)$, then $\mathrm{AG}(n,F) = \mathrm{PG}(n,F)\backslash\mathcal{H}_\infty$ is an *affine space of n dimensions over F*. When $F = \mathbb{F}_q$, write $\mathrm{AG}(n,F) = \mathrm{AG}(n,q)$.
2. The *subspaces* of $\mathrm{AG}(n,F)$ are the subspaces of $\mathrm{PG}(n,F)$, apart from $\mathcal{H}_\infty$, with the points of $\mathcal{H}_\infty$ deleted in each case.
3. This hyperplane $\mathcal{H}_\infty$ is the *hyperplane at infinity* of $\mathrm{AG}(n,F)$.

14.4.2 Collineations, correlations and coordinate frames

14.4.12 Definition

1. If S and S' are two spaces $\mathrm{PG}(n,F)$, $n \geq 2$, then a *collineation* $\alpha : S \longrightarrow S'$ is a bijection which preserves incidence; that is, if $\Pi_r \subset \Pi_s$, then $\Pi_r^\alpha \subset \Pi_s^\alpha$.
2. It is sufficient that α is a bijection such that, if $\Pi_0 \subset \Pi_1$, then $\Pi_0^\alpha \subset \Pi_1^\alpha$.
3. When $n = 1$, consider the lines S and S' embedded in planes over F; then a collineation $\alpha : S \longrightarrow S'$ is a transformation induced by a collineation of the planes; that is, if S_0 and S_0' are planes with $S \subset S_0$ and $S' \subset S_0'$, and $\alpha_0 : S_0 \longrightarrow S_0'$ is a collineation mapping S onto S', then let α be the restriction of α_0 to S.

14.4.13 Definition A *projectivity* $\alpha : S \longrightarrow S'$ is a bijection given by a matrix T, necessarily non-singular, such that $\mathbf{P}(X')^\alpha = \mathbf{P}(X)$ if and only if $tX' = XT$, where $t \in F_0$. Write $\alpha = \mathbf{M}(T)$; then $\alpha = \mathbf{M}(\lambda T)$ for any λ in F_0.

14.4.14 Remark A projectivity is a collineation. Mostly the case to be considered is when $S = S'$.

14.4.15 Definition With respect to a fixed basis of $V(n+1,F)$, an automorphism σ of F defines an *automorphic collineation* σ of $S = \mathrm{PG}(n,F)$; in coordinates, this is given by $\mathbf{P}(X)^\sigma = \mathbf{P}(X^\sigma)$, where $X^\sigma = (x_0^\sigma, x_1^\sigma, \ldots, x_n^\sigma)$.

14.4.16 Theorem (The fundamental theorem of projective geometry) [1499, Chapter 2]

1. If $\alpha' : S \longrightarrow S'$ is a collineation, then $\alpha' = \sigma\alpha$, where σ is an automorphic collineation, given by a field automorphism σ, and α is a projectivity. In particular, if $K = \mathbb{F}_q$ with $q = p^h$, p prime, and $\mathbf{P}(X')^{\alpha'} = \mathbf{P}(X)$, then there exists m in $\{1,2,\ldots,h\}$, $t_{ij} \in F$ for $i,j \in \{0,1,\ldots,n\}$, and $t \in F_0$ such that

$$tX' = X^{p^m}T,$$

where

$$\begin{aligned} X^{p^m} &= (x_0^{p^m}, \ldots, x_n^{p^m}), \\ T &= (t_{ij}); \end{aligned}$$

that is,

$$tx_i' = x_0^{p^m}t_{0i} + \cdots + x_n^{p^m}t_{ni},$$

for $i = 0,1,\ldots,n$.

2. If $\{P_0, \ldots, P_{n+1}\}$ and $\{P'_0, \ldots, P'_{n+1}\}$ are both subsets of $\mathrm{PG}(n, F)$ of cardinality $n+2$ such that no $n+1$ points chosen from the same set lie in a hyperplane, then there exists a unique projectivity α such that $P'_i = P_i^\alpha$, for all $i \in \{0, 1, \ldots, n+1\}$.

14.4.17 Remark There are cases where Theorem 14.4.16 simplifies.

1. For $n = 1$, there is a unique projectivity transforming any three distinct points on a line to any other three.
2. When $F = \mathbb{F}_2$, it suffices to give the images of $P_0, \ldots, P_n$ to determine a projectivity. For $n = 1$, the images of two points determine the projectivity.

14.4.18 Remark Part 2 of Theorem 14.4.16 emphasises a difference between the spaces $V(n+1, F)$ and $\mathrm{PG}(n, F)$. In the former, linear transformations are determined by the images of $n+1$ points; in the latter, projectivities are determined by the images of $n+2$ points.

14.4.19 Definition Let $\{P_0, \ldots, P_{n+1}\}$ be any set of $n+2$ points in $\mathrm{PG}(n, F)$, no $n+1$ in a hyperplane. If P is any other point of the space, then a coordinate vector for P is determined in the following manner. Let P_i be represented by the vector X_i for some vector X_i in $V(n+1, F)$. For any given t in F_0 there exist a_i in F for all $i \in \{0, 1, \ldots, n\}$ such that

$$tX_{n+1} = a_0X_0 + \cdots + a_nX_n.$$

So, for any t, the ratios a_i/a_j remain fixed. Thus, if P is any point with $P = \mathbf{P}(X)$, then

$$X = t_0a_0X_0 + \cdots + t_na_nX_n.$$

Hence, with respect to $\{P_0, \ldots, P_{n+1}\}$, the point P is given by $(t_0, \ldots, t_n)$ where the t_i are determined up to a common factor. Then $\{P_0, \ldots, P_n\}$ is the *simplex of reference* and P_{n+1} the *unit point*. Together the $n+2$ points form a (*coordinate*) *frame*.

14.4.20 Remark In $V(n+1, F)$, a basis is a set of $n+1$ linearly independent points and, in $\mathrm{PG}(n, F)$, a frame is a set of $n+2$ points, no $n+1$ in a hyperplane; that is, every set of $n+1$ points is linearly independent.

14.4.21 Theorem [1499, Chapter 2] Again from Theorem 14.4.16, if two coordinate frames are given by the vectors $X = (x_0, \ldots, x_n)$ and $Y = (y_0, \ldots, y_n)$, then a change from one frame to the other is given by $Y = XA$, where A is an $(n+1) \times (n+1)$ non-singular matrix over F. If a projectivity α in the one frame is given by $X' = XT$, then, since $Y' = X'A$, in the other frame it is given by $Y' = X'A = XTA = YA^{-1}TA$.

14.4.22 Definition Let S be a space $\mathrm{PG}(n, F)$ and S' its dual space superimposed on S; that is, the points of S' are the hyperplanes of S and the hyperplanes of S' are the points of S. Consider a function $\alpha : S \longrightarrow S'$. If α is a collineation, it is a *correlation* of S and induces a collineation, also named α, of S' to S; that is, as the points of S are transformed to hyperplanes, then hyperplanes are transformed to points since α preserves incidence. If α is a projectivity, then it is a *reciprocity* of S. In either case, if α is involutory, that is $\alpha^2 = 1$, where 1 is the identity, then α is a *polarity* of S.

14.4.23 Remark If P and P' are points and π is a hyperplane such that $P^\alpha = \pi$ and $\pi^\alpha = P'$, then, in a polarity, $P = P'$.

14.4.24 Definition Let $\mathrm{AG}(n,F) = \mathrm{PG}(n,F)\backslash\mathcal{H}_\infty$ be an affine space over F. Then, in a given coordinate frame where $\mathcal{H}_\infty$ has equation $x_0 = 0$, a point of $\mathrm{AG}(n,F)$ can be written $\mathbf{P}(1,x_1,\ldots,x_n)$ and hence as $(x_1,\ldots,x_n)$. So the points of $\mathrm{AG}(n,F)$ are the elements of $V(n,F)$. The x_i are the *affine* or *non-homogeneous coordinates* of the given point.

14.4.25 Remark It is assumed that, for any $\mathrm{AG}(n,F)$, the coordinate frame is this one.

14.4.26 Theorem [1499, Chapter 2]

1. The subspaces of $\mathrm{AG}(n,F)$ have the form $X+S$, where X is any vector and S is any subspace of $V(n,F)$.
2. Three points X,Y,Z of $\mathrm{AG}(n,F)$ are collinear if and only if there exists λ in $F\backslash\{0,1\}$ such that $X = \lambda Y + (1-\lambda)Z$.

14.4.27 Theorem [1499, Chapter 2]

1. If $\mathbb{F}_{q^n} = \mathbb{F}_q(\beta)$, then the map
$$X = (x_1,\ldots,x_n) \mapsto x = x_1 + x_2\beta + \cdots + x_n\beta^{n-1}$$
gives a bijection between $\mathrm{AG}(n,q)$ and $\mathbb{F}_{q^n}$.
2. Distinct points X,Y,Z in $\mathrm{AG}(n,F)$ are collinear if and only if, in $\mathbb{F}_{q^n}$,
$$(x-y)^{q-1} = (x-z)^{q-1}.$$

14.4.3 Polarities

14.4.28 Theorem [1499, Chapter 2] Suppose that α is a correlation of $\mathrm{PG}(n,F)$; then it is the product of an automorphic collineation σ and a projectivity of $\mathrm{PG}(n,F)$ to its dual space given by the matrix T. Then α is a polarity if and only if
$$\sigma^2 = 1 \quad \text{and} \quad T^\sigma T^{*^{-1}} = tI,$$
where T^* denotes the transpose of T and $t \in F_0$.

14.4.29 Theorem [1499, Chapter 2] If α is a polarity of $\mathrm{PG}(n,F)$, then, with σ and T as in Theorem 14.4.28, there are the following possibilities.

1. If $\sigma = 1$ and $\mathrm{char}\, F \neq 2$, then $T = T^*$ or $T = -T^*$.
2. If $\sigma = 1$ and $\mathrm{char}\, F = 2$, then $T = T^*$.
3. If $\sigma^2 = 1$, $\sigma \neq 1$, then $T^\sigma = tT^*$ with $t^{\sigma+1} = 1$. For a given frame, T can be chosen so that $t = 1$; that is, $T^\sigma = T^*$.

14.4.30 Remark [1548, Chapter 2] If α is a polarity of $\mathrm{PG}(n,F)$ with n even, then, for a given frame, T can be chosen so that $T^\sigma = T^*$ with $\sigma^2 = 1$.

14.4.31 Definition Let α be a polarity of $\mathrm{PG}(n,F)$.

1. If $\sigma = 1$, $\mathrm{char}\, F \neq 2$, and $T = T^*$, then α is an *orthogonal* or *ordinary polarity* or a *polarity with respect to a quadric*.
2. If $\sigma = 1$, $\mathrm{char}\, F \neq 2$, and $T = -T^*$, then α is a *null polarity* or *symplectic polarity* or a *polarity with respect to a linear complex*. Since T is non-singular and skew-symmetric, n is odd.

3. If $\sigma = 1$, $\operatorname{char} F = 2$, $T = T^*$, and all elements on the main diagonal of T are zero, then α is a *null polarity* or *symplectic polarity* or a *polarity with respect to a linear complex*. This only occurs for n odd.
4. If $\sigma = 1$, $\operatorname{char} F = 2$, $T = T^*$, and some element on the main diagonal of T is not zero, then α is a *pseudo-polarity*.
5. If $\sigma \neq 1$, then α is a *Hermitian* or *unitary polarity*.

14.4.32 Definition

1. In a polarity α, if $P^\alpha = \pi$ and $\pi'^\alpha = P'$, with P, P' points and π, π' hyperplanes, then π is the *polar* (*hyperplane*) of P and P' is the *pole* of π'. Since $\alpha^2 = 1$, the converse is also true.
2. If P' lies in $\pi = P^\alpha$, then P lies in $\pi' = P'^\alpha$. In this case, P and P' are *conjugate* points, and π and π' are *conjugate* hyperplanes. The point P is *self-conjugate* if it lies in its own polar hyperplane; the hyperplane π is *self-conjugate* if it contains its own pole.

14.4.33 Remark [1499, Chapter 2] The self-conjugate points $\mathbf{P}(X)$ of α are given by $X^\sigma T X^* = 0$.

14.4.34 Remark For the definition of a linear complex see [1498, Section 15.2].

14.4.35 Definition

1. A *quadric* $\mathcal{Q}$ (or $\mathcal{Q}_n$) in $\mathrm{PG}(n, F)$, $n \geq 1$, is the set of points $\mathbf{P}(x_0, \ldots, x_n)$ satisfying a quadratic equation
$$\sum_{\substack{i,j=0 \\ i \leq j}}^{n} a_{ij} x_i x_j = 0,$$
with a_{ij} in F and not all zero. For $n = 2$, a quadric is a *conic*; for $n = 3$, a quadric is a *quadric surface*.
2. A *Hermitian variety* $\mathcal{H}$ (or $\mathcal{H}_n$) in $\mathrm{PG}(n, F)$, $n \geq 1$, is the set of points $\mathbf{P}(x_0, \ldots, x_n)$ satisfying an equation
$$\sum_{i,j=0}^{n} a_{ij} x_i x_j^\sigma = 0,$$
with a_{ij} in F and not all zero, with σ an automorphism of F of order 2, and with $a_{ij}^\sigma = a_{ji}$. For $n = 2$, a Hermitian variety is a *Hermitian curve*; for $n = 3$, a Hermitian variety is a *Hermitian surface*.

14.4.36 Definition Let $\mathcal{F}$ be a quadric or Hermitian variety in $\mathrm{PG}(n, F)$.

1. The point P of $\mathrm{PG}(n, F)$ is *singular* for $\mathcal{F}$ if $\ell \cap \mathcal{F} = \{P\}$ or $\ell \cap \mathcal{F} = \ell$ for every line ℓ through P.
2. If $\mathcal{F}$ has a singular point, then $\mathcal{F}$ is *singular*; otherwise, it is *non-singular*.

14.4.37 Theorem [1499, Chapters 2,5]

1. If α is an orthogonal polarity of $\mathrm{PG}(n,F)$, then the set of self-conjugate points of α is a non-singular quadric $\mathcal{Q}$ of $\mathrm{PG}(n,F)$.
2. If α is a symplectic polarity of $\mathrm{PG}(n,F)$, then every point of $\mathrm{PG}(n,F)$ is self-conjugate.
3. If α is a pseudo-polarity of $\mathrm{PG}(n,F)$, then the set of self-conjugate points of α is a subspace of $\mathrm{PG}(n,F)$.
4. If α is a Hermitian polarity of $\mathrm{PG}(n,F)$, then the set of self-conjugate points of α is a non-singular Hermitian variety $\mathcal{H}$ of $\mathrm{PG}(n,F)$.

14.4.38 Theorem [1499, Chapter 5] If α is a symplectic polarity of $\mathrm{PG}(n,F)$, then, in a suitable coordinate frame, the matrix of α is

$$T = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ -1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & -1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & 0 & \cdots & -1 & 0 \end{bmatrix}.$$

14.4.39 Theorem [1499, Chapter 5] If α is a pseudo-polarity of $\mathrm{PG}(n,q)$, q even, then, in a suitable coordinate frame, the matrix of α is as follows:

1. for n even,
$$T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix};$$
2. for n odd,
$$T = \begin{bmatrix} 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}.$$

14.4.40 Remark [1499, Chapter 5] Theorem 14.4.39 holds for every field F of characteristic two with the property that $\{x^2 \mid x \in F\} = F$.

14.4.41 Theorem [1499, Chapter 5] Let $\mathcal{Q}$ be a non-singular quadric of $\mathrm{PG}(n,q)$. The coordinate frame can be chosen so that $\mathcal{Q}$ has the following equation:

1. n even,
$$x_0^2 + x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n = 0;$$
2. n odd,

a.
$$x_0x_1 + x_2x_3 + \cdots + x_{n-1}x_n = 0;$$

b.
$$f(x_0, x_1) + x_2x_3 + \cdots + x_{n-1}x_n = 0,$$
where f is any chosen irreducible quadratic form.

Hence, up to a projectivity, there is a unique non-singular quadric in $\mathrm{PG}(n, q)$ with n even; for n odd, there are two types of non-singular quadric.

14.4.42 Definition

1. In case 1 of Theorem 14.4.41, the quadric is *parabolic*. In case 2.a, it is *hyperbolic*; in case 2.b, it is *elliptic*;
2. The *character* w of a non-singular quadric in $\mathrm{PG}(n, q)$ is 0 if it is elliptic, 1 if it is parabolic, and 2 if it is hyperbolic.

14.4.43 Theorem [1499, Chapter 5] If $\mathcal{Q}_n$ is a non-singular quadric of $\mathrm{PG}(n, q)$ with character w, then
$$|\mathcal{Q}_n| = (q^n - 1)/(q - 1) + (w - 1)q^{(n-1)/2}.$$

14.4.44 Theorem [1499, Chapter 5] Let $\mathcal{H}$ be a non-singular Hermitian variety of $\mathrm{PG}(n, q^2)$. The coordinate frame can be chosen so that $\mathcal{H}$ has the following equation:
$$x_0^{q+1} + x_1^{q+1} + \cdots + x_n^{q+1} = 0.$$

14.4.45 Theorem [1499, Chapter 5] If $\mathcal{H}_n$ is a non-singular Hermitian variety of $\mathrm{PG}(n, q^2)$, then
$$|\mathcal{H}_n| = [q^{n+1} + (-1)^n][q^n - (-1)^n]/(q^2 - 1).$$

14.4.4 Partitions and cyclic projectivities

14.4.46 Definition A *spread* $\mathcal{S}$ of $\mathrm{PG}(n, q)$ by r-spaces is a set of r-spaces which partitions $\mathrm{PG}(n, q)$; that is, every point of $\mathrm{PG}(n, q)$ lies in exactly one r-space of $\mathcal{S}$. Hence any two r-spaces of $\mathcal{S}$ are disjoint.

14.4.47 Theorem [1499, Chapter 4] The following are equivalent:

1. there exists a spread $\mathcal{S}$ of r-spaces of $\mathrm{PG}(n, q)$;
2. $\theta(r, q) \mid \theta(n, q)$;
3. $(r + 1) \mid (n + 1)$.

14.4.48 Remark Spreads of $\mathrm{PG}(2r+1, q)$ by r-spaces have been much studied, particularly for their application to non-Desarguesian planes. The latter are considered in more detail in Section 14.3.

14.4.49 Definition Since $\mathbb{F}_q$ is a subfield of $\mathbb{F}_{q^k}$ for $k \in \mathbb{N}\backslash\{0\}$, so $\mathrm{PG}(n, q)$ is naturally embedded in $\mathrm{PG}(n, q^k)$ once the coordinate frame is fixed. Any $\mathrm{PG}(n, q)$ embedded in $\mathrm{PG}(n, q^k)$ is a *subgeometry* of $\mathrm{PG}(n, q^k)$.

14.4.50 Theorem [1499, Chapter 4] If $s(n,q,q^k)$ is the number of subgeometries $\mathrm{PG}(n,q)$ embedded in $\mathrm{PG}(n,q^k)$, then

$$\begin{aligned} s(n,q,q^k) &= |\mathrm{PGL}(n+1,q^k)|/|\mathrm{PGL}(n+1,q)| \\ &= q^{n(n+1)(k-1)/2}\prod_{i=2}^{n+1}[(q^{ki}-1)/(q^i-1)]. \end{aligned}$$

14.4.51 Corollary [1499, Chapter 4] On the line $\mathrm{PG}(1,q^k)$,

1. $s(1,q,q^k) = q^{k-1}(q^{2k}-1)/(q^2-1)$;
2. $s(1,q,q^2) = q(q^2+1)$.

14.4.52 Corollary [1499, Chapter 4] In the plane $\mathrm{PG}(2,q^2)$,

$$s(2,q,q^2) = q^3(q^2+1)(q^3+1).$$

14.4.53 Theorem [1499, Chapter 4] The following are equivalent:

1. there exists a partition of $\mathrm{PG}(n,q^k)$ into subgeometries $\mathrm{PG}(n,q)$;
2. $\theta(n,q) \mid \theta(n,q^k)$;
3. $(k,n+1) = 1$.

14.4.54 Corollary [1499, Chapter 4] The line $\mathrm{PG}(1,q^k)$ can be partitioned into sublines $\mathrm{PG}(1,q)$ if and only if k is odd.

14.4.55 Corollary [1499, Chapter 4] The plane $\mathrm{PG}(2,q^k)$ can be partitioned into subplanes $\mathrm{PG}(2,q)$ if and only if $(k,3) = 1$.

14.4.56 Corollary [1499, Chapter 4] The plane $\mathrm{PG}(2,q^2)$ can be partitioned into q^2-q+1 subplanes $\mathrm{PG}(2,q)$.

14.4.57 Definition A projectivity α which permutes the $\theta(n)$ points of $\mathrm{PG}(n,q)$ in a single cycle is a *cyclic projectivity*; it is a *Singer cycle* and the group it generates a *Singer group*.

14.4.58 Theorem [1499, Chapter 4] A projectivity α of $\mathrm{PG}(n,q)$ is cyclic if and only if the characteristic polynomial of an associated matrix is *subprimitive*; that is, the smallest power m of a characteristic root that lies in $\mathbb{F}_q$ is $m = \theta(n)$.

14.4.59 Corollary [1499, Chapter 4] A cyclic projectivity permutes the hyperplanes of $\mathrm{PG}(n,q)$ in a single cycle.

14.4.60 Corollary [1499, Chapter 4] The number of cyclic projectivities in $\mathrm{PG}(n,q)$ is given by

$$\sigma(n,q) = q^{n(n+1)/2}\prod_{i=1}^{n}(q^i-1)\varphi(\theta(n))/(n+1),$$

where φ is the Euler function.

14.4.61 Corollary [1499, Chapter 4] The number of conjugacy classes of $\mathrm{PGL}(n+1,q)$ consisting of cyclic projectivities is $\varphi(\theta(n))/(n+1)$.

14.4.62 Corollary [1499, Chapter 4] In $\mathrm{PGL}(n+1,q)$ there is just one conjugacy class of Singer groups.

14.4.63 Theorem [1499, Chapter 4] If $(k, n+1) = 1$ and α is a projectivity of $\mathrm{PG}(n, q^k)$ which acts as a cyclic projectivity on some $\mathrm{PG}(n, q)$ embedded in $\mathrm{PG}(n, q^k)$, then, letting

$$u = (q^{k(n+1)} - 1)(q - 1)/[(q^k - 1)(q^{n+1} - 1)],$$

1. there exists a cyclic projectivity ρ of $\mathrm{PG}(n, q^k)$ such that $\rho^u = \alpha$;
2. every orbit of α is a subgeometry $\mathrm{PG}(n, q)$;
3. if γ is any cyclic projectivity of $\mathrm{PG}(n, q^k)$, then the orbits of γ^u are subgeometries $\mathrm{PG}(n, q)$.

14.4.64 Theorem [1499, Chapter 4] If $(k, n+1) = 1$, then the number of projectivities α of $\mathrm{PG}(n, q^k)$ that act cyclically on at least one $\mathrm{PG}(n, q)$ of $\mathrm{PG}(n, q^k)$ is

$$q^{kn(n+1)/2} \prod_{i=1}^{n} (q^{ki} - 1)\varphi(\theta(n, q))/(n + 1).$$

14.4.5 k-Arcs

14.4.65 Definition

1. A *k-arc* in $\mathrm{PG}(n, q)$, $n \geq 2$, is a set $\mathcal{K}$ of k points, with $k \geq n + 1$, such that no $n + 1$ of its points lie in a hyperplane.
2. An arc $\mathcal{K}$ is *complete* if it is not properly contained in a larger arc.
3. Otherwise, if $\mathcal{K} \cup \{P\}$ is an arc for some point P of $\mathrm{PG}(n, q)$, the point P *extends* $\mathcal{K}$.

14.4.66 Definition A *normal rational curve* in $\mathrm{PG}(n, q)$, $n \geq 2$, is any set of points of $\mathrm{PG}(n, q)$ which is projectively equivalent to

$$\{\mathbf{P}(t^n, t^{n-1}, \ldots, t, 1) \mid t \in \mathbb{F}_q\} \cup \{\mathbf{P}(1, 0, \ldots, 0, 0)\}.$$

14.4.67 Remark [1504, Chapter 27] Any normal rational curve contains $q + 1$ points. For $n = 2$, it is a non-singular conic; for $n = 3$, it is a *twisted cubic*. Any $(n + 3)$-arc in $\mathrm{PG}(n, q)$ is contained in a unique normal rational curve of this space.

14.4.68 Problem (The three problems of Segre)

I. For given n and q, what is the maximum value of k such that a k-arc exists in $\mathrm{PG}(n, q)$?

II. For what values of n and q with $q > n + 1$ is every $(q + 1)$-arc of $\mathrm{PG}(n, q)$ a normal rational curve?

III. For given n and q with $q > n + 1$, what are the values of k such that each k-arc of $\mathrm{PG}(n, q)$ is contained in a normal rational curve of this space?

14.4.69 Remark For a survey of solutions to Problems I, II, III, see [1501, 1502] and [1500, Chapter 13].

14.4.70 Theorem [1499, Chapter 8] Let $\mathcal{K}$ be a k-arc of $\mathrm{PG}(2, q)$. Then

1. $k \leq q+2$;
2. for q odd, $k \leq q+1$;
3. any non-singular conic of $\mathrm{PG}(2,q)$ is a $(q+1)$-arc;
4. each $(q+1)$-arc of $\mathrm{PG}(2,q)$, q even, extends to a $(q+2)$-arc.

14.4.71 Definition

1. The $(q+1)$-arcs of $\mathrm{PG}(2,q)$ are *ovals*.
2. The $(q+2)$-arcs of $\mathrm{PG}(2,q)$, q even, are *complete ovals* or *hyperovals*.

14.4.72 Theorem [1499, Chapter 8] In $\mathrm{PG}(2,q)$, q odd, every oval is a non-singular conic.

14.4.73 Remark Theorem 14.4.72 is a celebrated result due to Segre [2559]. For more details on k-arcs in $\mathrm{PG}(2,q)$, ovals and hyperovals see Section 14.3 and [1499, Chapters 8–10]. The fundamental Theorem 14.4.76, also due to Segre [2561], relates k-arcs of $\mathrm{PG}(2,q)$ to plane algebraic curves.

14.4.74 Definition Let $\mathcal{K}$ be a k-arc of $\mathrm{PG}(2,q)$.

1. A *tangent* of $\mathcal{K}$ is a line of $\mathrm{PG}(2,q)$ meeting $\mathcal{K}$ in a unique point.
2. A *secant* of $\mathcal{K}$ is a line meeting $\mathcal{K}$ in two points.

14.4.75 Remark At each point, $\mathcal{K}$ has $t = q+2-k$ tangents; the total number of tangents is tk.

14.4.76 Theorem [1499, Chapter 10]

1. Let $\mathcal{K}$ be a k-arc in $\mathrm{PG}(2,q)$, with q even. Then the tk tangents of $\mathcal{K}$ belong to an algebraic envelope Γ_t of class t, that is, the dual of a plane algebraic curve of order t, with the following properties:
   a. Γ_t is unique if $k > (q+2)/2$;
   b. Γ_t contains no secant of $\mathcal{K}$ and so no pencil with vertex P in $\mathcal{K}$, where a *pencil* is the set of lines through a point;
   c. if Δ_P is the pencil of lines with vertex P in $\mathcal{K}$ and ℓ is a tangent at P, then the intersection multiplicity of Δ_P and Γ_t at ℓ is one.
2. Let $\mathcal{K}$ be a k-arc in $\mathrm{PG}(2,q)$, with q odd. Then the tk tangents of $\mathcal{K}$ belong to an algebraic envelope Γ_{2t} of class $2t$ with the following properties:
   a. Γ_{2t} is unique if $k > (2q+4)/3$;
   b. Γ_{2t} contains no secant of $\mathcal{K}$ and so no pencil with vertex P in $\mathcal{K}$;
   c. if Δ_P is the pencil with vertex P in $\mathcal{K}$ and ℓ is a tangent at P, then the intersection multiplicity of Δ_P and Γ_{2t} at ℓ is two;
   d. Γ_{2t} may contain components of multiplicity at most two, but does not consist entirely of double components.

14.4.77 Corollary [1499, Chapter 10]

1. If q is even and $k > (q+2)/2$, then $\mathcal{K}$ is contained in a unique complete arc of $\mathrm{PG}(2,q)$.
2. If q is odd and $k > (2q+4)/3$, then $\mathcal{K}$ is contained in a unique complete arc of $\mathrm{PG}(2,q)$.

14.4.78 Remark

1. For a survey on k-arcs in $\mathrm{PG}(n,q)$, $n>2$, see [1501, 1502].
2. For q odd, the main results were obtained by induction and projection of the k-arc $\mathcal{K}$ from one of its points P onto a hyperplane not containing P; see Thas [2776] and [1504, Chapter 27].
3. For any q, a theorem of Bruen, Thas and Blokhuis [431] relates k-arcs in $\mathrm{PG}(3,q)$ to dual algebraic surfaces. For q even, this result enables estimates to be made for the three problems of Segre. A generalisation by Blokhuis, Bruen and Thas [322] now follows.

14.4.79 Theorem [1504, Chapter 27] Let $\mathcal{K}=\{P_1,P_2,\ldots,P_k\}$ be a k-arc of $\mathrm{PG}(n,q)$. For distinct $i_1,i_2,\ldots,i_{n-1}\in\{1,2,\ldots,k\}$, let $Z_{\{i_1,i_2,\ldots,i_{n-1}\}}$ be the set of $t=q+n-k$ hyperplanes through the $(n-2)$-dimensional subspace Π_{n-2}, generated by $P_{i_1},P_{i_2},\ldots,P_{i_{n-1}}$, that contains no other point of $\mathcal{K}$.

1. a. For q even, there exists a dual algebraic hypersurface Φ_t of class t in $\mathrm{PG}(n,q)$ which contains the hyperplanes of each set $Z_{\{i_1,i_2,\ldots,i_{n-1}\}}$.
   b. This dual hypersurface is unique when $k>(q+2n-2)/2$.
2. a. For q odd, there exists a dual algebraic hypersurface Φ_{2t} of class $2t$ in $\mathrm{PG}(n,q)$ which contains the hyperplanes of each set $Z_{\{i_1,i_2,\ldots,i_{n-1}\}}$.
   b. The intersection multiplicity of Φ_{2t} and the pencil of hyperplanes with vertex Π_{n-2} at each hyperplane of $Z_{\{i_1,i_2,\ldots,i_{n-1}\}}$ is two.
   c. This dual hypersurface is unique when $k>(2q+3n-2)/3$.

14.4.80 Corollary [1504, Chapter 27]

1. If q is even and $k>(q+2n-2)/2$, then a k-arc $\mathcal{K}$ of $\mathrm{PG}(n,q)$ is contained in a unique complete arc.
2. If q is odd and $k>(2q+3n-2)/3$, then a k-arc $\mathcal{K}$ of $\mathrm{PG}(n,q)$ is contained in a unique complete arc.

14.4.81 Theorem (The duality principle for k-arcs) [1504, Chapter 27] A k-arc of $\mathrm{PG}(n,q)$, with $n\geq 2$ and $k\geq n+4$, exists if and only if a k-arc of $\mathrm{PG}(k-n-2,q)$ exists.

14.4.82 Corollary [1504, Chapter 27] In $\mathrm{PG}(q-2,q)$, q even and $q\geq 4$, there exist $(q+2)$-arcs.

14.4.83 Conjecture [1500, Chapter 13]

1. If $\mathcal{K}$ is a k-arc in $\mathrm{PG}(n,q)$, with $q-1\geq n\geq 2$, then $k\leq q+1$ for q odd and $k\leq q+2$ for q even.
2. In $\mathrm{PG}(n,q)$, with $q\geq n\geq 2$ and q even, there exist $(q+2)$-arcs if and only if $n\in\{2,q-2\}$.

14.4.6 k-Arcs and linear MDS codes

14.4.84 Definition

1. Let C be a *code* of *length* k over an alphabet A of size q with $q\geq 2$. In other words, C is a set of (*code*)*words*, where each word is an ordered k-tuple over A.
2. For a given m with $2\leq m\leq k$, impose the following condition: no two words in C agree in as many as m positions. Then $|C|\leq q^m$. If $|C|=q^m$, then C is a *maximum distance separable* (*MDS*) code.

14.4.85 Remark MacWilliams and Sloane [1978, Chapter 11] introduce the chapter on MDS codes as "one of the most fascinating in all of coding theory".

14.4.86 Definition

1. The (*Hamming*) *distance* between two codewords
$$X = (x_1, \ldots, x_k) \text{ and } Y = (y_1, \ldots, y_k)$$
is the number of indices i for which $x_i \neq y_i$; it is denoted $d(X, Y)$.
2. The *minimum distance* of a code C, with $|C| > 1$, is
$$d(C) = \min\{d(X, Y) \mid X, Y \in C,\ X \neq Y\}.$$

14.4.87 Theorem [2831, Chapter 5] For an MDS code, $d(C) = k - m + 1$; see Section 15.1.

14.4.88 Remark One of the main problems concerning MDS codes is to maximise $d(C)$, and so k, for given m and q. Another problem is to determine the structure of C in the optimal case.

14.4.89 Theorem [431] For an MDS code, $k \leq q + m - 1$.

14.4.90 Remark For $m = 2$, the MDS code C gives a set of q^2 codewords of length k, no two of which agree in more than one position. This is equivalent to the existence of a net of order q and degree k; see also Section 14.1. It follows that $k \leq q + 1$, the case of equality corresponding to an affine plane of order q; see Section 14.3. Theorem 14.4.89 follows by an inductive argument.

14.4.91 Remark

1. The case $m = 3$ and $k = q + 2$ is equivalent to the existence of an affine plane of order q, with q even, containing an appropriate system of $(q + 2)$-arcs. For all known examples the plane is an affine plane $\mathrm{AG}(2, q)$ with $q = 2^h$; see Willems and Thas [2960].
2. For $m = 4$ and $k = q + 3$, it has been shown that either $q = 2$ or 36 divides q; no example other than for $q = 2$ is known to exist; see Bruen and Silverman [428].

14.4.92 Remark Henceforth, only *linear* MDS codes are considered; that is C is an m-dimensional subspace of the vector space $V(k, q)$, which is $\mathbb{F}_q^k$ with the usual addition and scalar multiplication.

14.4.93 Theorem [1500, Chapter 13] For $m \geq 3$, linear MDS codes and arcs are equivalent objects.

14.4.94 Remark Let C be an m-dimensional subspace of $V(k, q)$ and let G be an $m \times k$ generator matrix for C; that is, the rows of G are a basis for C. Then C is MDS if and only if any m columns of G are linearly independent; this property is preserved under multiplication of the columns by non-zero scalars. So consider the columns of G as points $P_1, \ldots, P_k$ of $\mathrm{PG}(m-1, q)$. It follows that C is MDS if and only if $\{P_1, \ldots, P_k\}$ is a k-arc of $\mathrm{PG}(m-1, q)$. This gives the relation between linear MDS codes and arcs.

14.4.95 Theorem [1500, Chapter 13] For $2 \leq m \leq k - 2$, the dual of a linear MDS code is again a linear MDS code.

14.4.96 Remark For $3 \leq m \leq k - 3$, Theorem 14.4.95 is the translation of Theorem 14.4.81 from geometry to coding theory.

14.4.7 k-Caps

14.4.97 Definition

1. In PG(n, q), $n \geq 3$, a set $\mathcal{K}$ of k points no three of which are collinear is a *k-cap*.
2. A k-cap is *complete* if it is not contained in a $(k+1)$-cap.
3. A line of PG(n, q) is a *secant*, *tangent*, or *external line* as it meets $\mathcal{K}$ in $2, 1$ or 0 points.

14.4.98 Theorem [1498, Chapter 16]

1. For any k-cap $\mathcal{K}$ in PG$(3, q)$ with $q \neq 2$, the cardinality k satisfies $k \leq q^2 + 1$.
2. In PG$(3, 2)$, a k-cap satisfies $k \leq 8$; an 8-cap is the complement of a plane.

14.4.99 Definition A (q^2+1)-cap of PG$(3, q)$, $q \neq 2$ is an *ovoid*; the *ovoids* of PG$(3, 2)$ are its elliptic quadrics.

14.4.100 Theorem [1498, Chapter 16] At each point P of an ovoid $\mathcal{O}$ of PG$(3, q)$, there is a unique *tangent plane* π such that $\pi \cap \mathcal{O} = \{P\}$.

14.4.101 Theorem [1498, Chapter 16]

1. Apart from the tangent planes, every plane meets an ovoid $\mathcal{O}$ in a $(q+1)$-arc.
2. When q is even, the $(q^2+1)(q+1))$ tangents of $\mathcal{O}$ are the totally isotropic lines of a symplectic polarity α of PG$(3, q)$, that is, the lines ℓ for which $\ell^\alpha = \ell$.

14.4.102 Theorem [1498, Chapter 16] In PG$(3, q)$, q odd, every ovoid is an elliptic quadric.

14.4.103 Remark Theorem 14.4.102 is a celebrated result, due independently to Barlotti [201] and Panella [2343]. Both proofs rely on Theorem 14.4.72.

14.4.104 Theorem [418] In PG$(3, q)$, q even, every ovoid containing at least one conic section is an elliptic quadric.

14.4.105 Theorem [1498, Chapter 16] In PG$(3, q)$, let $W(q)$ be the incidence structure formed by all the points and the totally isotropic lines of a symplectic polarity α. Then $W(q)$ admits a polarity α' if and only if $q = 2^{2e+1}$; in that case, the absolute points of α', namely the points lying in their image lines, form an ovoid of PG$(3, q)$. Such an ovoid is an elliptic quadric if and only if $q = 2$.

14.4.106 Definition For $q = 2^{2e+1}$, with $e \geq 1$, the ovoids in Theorem 14.4.105 are *Tits ovoids*.

14.4.107 Theorem [1498, Chapter 16] With $q = 2^{2e+1}$, the canonical form of a Tits ovoid is

$$\mathcal{O} = \{\mathbf{P}(1, z, y, x) \mid z = xy + x^{\sigma+2} + y^\sigma\} \cup \{\mathbf{P}(0, 1, 0, 0)\},$$

where σ is the automorphism $t \mapsto t^{2^{e+1}}$ of $\mathbb{F}_q$.

14.4.108 Theorem [1498, Chapter 16] For $q = 2^{2e+1}$, $e \geq 1$, the group of all projectivities of PG$(3, q)$ fixing the Tits ovoid $\mathcal{O}$ is the Suzuki group Sz(q), which acts doubly transitively on $\mathcal{O}$.

14.4.109 Remark The case $q = 4$ is the same as q odd; that is, an ovoid of PG$(3, 4)$ is an elliptic quadric; see Barlotti [201] or [1498, Chapter 16]. For $q = 8$, Segre [2560] found an ovoid

other than an elliptic quadric; Fellegara [1045] showed that this example is a Tits ovoid. She also showed, using a computer program, that every ovoid in PG$(3, 8)$ is either an elliptic quadric or a Tits ovoid. O'Keefe and Penttila [2298, 2299] showed, also using a computer program, that in PG$(3, 16)$ every ovoid is an elliptic quadric. O'Keefe, Penttila and Royle [2300], also using a computer program, showed that in PG$(3, 32)$ every ovoid is an elliptic quadric or a Tits ovoid.

14.4.110 Definition Let $\mathcal{O}$ be an ovoid of PG$(3, q)$ and let $\mathcal{B}$ be the set of all intersections $\pi \cap \mathcal{O}$, with π a non-tangent plane of $\mathcal{O}$. Then the incidence structure formed by the triple $\mathcal{I}(\mathcal{O}) = (\mathcal{O}, \mathcal{B}, \in)$ is a $3-(q^2+1, q+1, 1)$ design. A $3-(n^2+1, n+1, 1)$ design $\mathcal{I} = (\mathcal{P}, \mathcal{B}, \in)$ is an *inversive plane of order* n and the elements of $\mathcal{B}$ are *circles*; the inversive planes arising from ovoids are *egglike*.

14.4.111 Theorem [801, Chapter 6] Every inversive plane of even order is egglike.

14.4.112 Definition If the ovoid $\mathcal{O}$ is an elliptic quadric, then the inversive plane $\mathcal{I}(\mathcal{O})$, and any inversive plane isomorphic to it, is *classical* or *Miquelian*.

14.4.113 Remark By Theorem 14.4.102, an egglike inversive plane of odd order is Miquelian. For odd order, no other inversive planes are known.

14.4.114 Definition Let $\mathcal{I}$ be an inversive plane of order n. For any point P of $\mathcal{I}$, the points of $\mathcal{I}$ other than P, together with the circles containing P with P removed, form a $2-(n^2, n, 1)$ design, that is, an affine plane of order n. This plane is denoted $\mathcal{I}_P$ and is the *internal plane* or *derived plane* of $\mathcal{I}$ at P.

14.4.115 Remark [801, Chapter 6] For an egglike inversive plane $\mathcal{I}(\mathcal{O})$ of order q, each internal plane is Desarguesian, that is, the affine plane AG$(2, q)$ over $\mathbb{F}_q$.

14.4.116 Theorem [2777] Let $\mathcal{I}$ be an inversive plane of odd order n. If, for at least one point P of $\mathcal{I}$, the internal plane $\mathcal{I}_P$ is Desarguesian, then $\mathcal{I}$ is Miquelian.

14.4.117 Remark Up to isomorphism, there is a unique inversive plane of order n for the values $n = 2, 3, 4, 5, 7$; see Chen [603], Denniston [815, 816], Witt [2978]. As a corollary of Theorem 14.4.116 and the uniqueness of the projective plane of order n for $n = 3, 5, 7$, a computer-free proof of the uniqueness of the inversive plane of order n is obtained for these n.

14.4.118 Remark For more information about designs, see Section 14.5. For more information about projective spaces, see [1498, 1499, 1504] and [1500, Chapter 13].

See Also

§12.5 For results on curves which impinge on k-arcs.
§14.2 For a technique to resolve problems on blocking sets.
§14.3 For other aspects of Desarguesian planes.

References Cited: [201, 322, 418, 428, 431, 603, 801, 815, 816, 1045, 1498, 1499, 1500, 1501, 1502, 1504, 1548, 1978, 2298, 2299, 2300, 2343, 2559, 2560, 2561, 2776, 2777, 2831, 2960, 2978]

14.5 Block designs

Charles J. Colbourn, *Arizona State University*
Jeffrey H. Dinitz, *University of Vermont*

14.5.1 Basics

14.5.1 Definition A *balanced incomplete block design* (BIBD) is a pair $(V, \mathcal{B})$ where V is a v-set and $\mathcal{B}$ is a collection of b k-subsets of V (*blocks*) such that each element of V is contained in exactly r blocks and any 2-subset of V is contained in exactly λ blocks. The numbers v, b, r, k, and λ are *parameters* of the BIBD. Its *order* is v; its *replication number* is r; its *blocksize* is k; and its *index* is λ.

14.5.2 Proposition Trivial necessary conditions for the existence of a BIBD(v, b, r, k, λ) are

1. $vr = bk$, and
2. $r(k-1) = \lambda(v-1)$.

Parameter sets that satisfy conditions 1 and 2 are *admissible*.

14.5.3 Remark The three parameters v, k, and λ determine the remaining two as $r = \frac{\lambda(v-1)}{k-1}$ and $b = \frac{vr}{k}$. Hence one often writes (v, k, λ) *design* to denote a BIBD(v, b, r, k, λ).

14.5.4 Example The unique $(6, 3, 2)$ design and the unique $(7, 3, 1)$ design have blocks shown below as columns:

```
0000011122        0001123
1123423433        1242534
2345554545        3654656
```

14.5.5 Definition A BIBD $(V, \mathcal{B})$ with parameters v, b, r, k, λ is

simple	if it has no repeated blocks;
complete or *full*	if it is simple and contains $\binom{v}{k}$ blocks;
decomposable	if $\mathcal{B}$ can be partitioned into two nonempty collections $\mathcal{B}_1$ and $\mathcal{B}_2$ so that $(V, \mathcal{B}_i)$ is a (v, k, λ_i) design for $i = 1, 2$;
Hadamard	if $v = 4n-1$, $k = 2n-1$, and $\lambda = n-1$ for some integer $n \geq 2$;
m-multiple	if $v, \frac{b}{m}, \frac{r}{m}, k, \frac{\lambda}{m}$ are the parameters of a BIBD;
nontrivial	if $3 \leq k < v$;
quasi-symmetric	if every two distinct blocks intersect in either μ_1 or μ_2 elements;
resolvable (an *RBIBD*)	if there exists a partition R of its set of blocks B into *parallel classes*, each of which in turn partitions the set V (R is a *resolution*);
a *Steiner 2-design* $S(2, k, v)$	if $\lambda = 1$;
a *Steiner triple system* STS(v)	if $k = 3$ and $\lambda = 1$;
symmetric	if $v = b$, or equivalently $k = r$;
a *triple system* TS(v, λ)	if $k = 3$.

14.5.2 Triple systems

14.5.6 Remark A Steiner triple system of order v can exist only when $v-1$ is even because every element occurs with $v-1$ others, and in each block in which it occurs it appears with two other elements. Moreover, every block contains three pairs and hence $\binom{v}{2}$ must be a multiple of 3. Thus, it is necessary that $v \equiv 1, 3 \pmod 6$. This condition was shown to be sufficient in 1847.

14.5.7 Theorem [1729] A Steiner triple system of order v exists if and only if $v \equiv 1, 3 \pmod 6$.

14.5.8 Theorem [702] A TS(v, λ) exists if and only if $v \neq 2$ and $\lambda \equiv 0 \pmod{\gcd(v-2, 6)}$.

14.5.9 Remark Existence theorems such as Theorems 14.5.7 and 14.5.8 are typically established by a combination of *direct* constructions to make designs for specific values of v, and *recursive* constructions to make solutions for large values of v from solutions with smaller values of v. Finite fields are most often used in providing direct constructions, both to provide ingredients for recursive constructions, and to produce solutions with specific properties. Examples for triple systems are developed to demonstrate these; see [702].

14.5.10 Construction [2208] Let p be a prime, $n \geq 1$, and $p^n \equiv 1 \pmod 6$. Then there is an STS(p^n). To construct one, let $\mathbb{F}_{p^n}$ be a finite field on a set X of size $p^n = 6t+1$ with 0 as its zero element, and ω a primitive root of unity. Then

$$\{\{\omega^i + j, \omega^{2t+i} + j, \omega^{4t+i} + j\} : 0 \leq i < t, j \in X\}$$

(with computations in $\mathbb{F}_{p^n}$) is the set of blocks of an STS(p^n) on X.

14.5.11 Remark In order to verify Construction 14.5.10, consider two distinct elements $x, y \in \mathbb{F}_{p^n}$. Let $d = x - y$ (arithmetic in $\mathbb{F}_{p^n}$). Now since $d \neq 0$ and $\omega^{2t} - 1 \neq 0$, d can be uniquely written in the form $(\omega^{2t}-1)\omega^{2jt}\omega^i$ for $j \in \{0, 1, 2\}$ and $0 \leq i < 2t$. Since $\omega^{3t} = -1$, if $i \geq t$, we may write

$$-d = y - x = (\omega^{2t} - 1)\omega^{2(j+1)t}\omega^{i-t}.$$

Thus we suppose without loss of generality that $d = x - y$ and $i < t$. Then $\{x, y\}$ appears in the triple $\{\omega^i, \omega^{2t+i}, \omega^{4t+i}\} + (x - \omega^{2(j+1)t+i})$. Consequently, every pair of distinct elements in $\mathbb{F}_{p^n}$ appears in at least one of the triples defined. Because the total number of pairs in the triples defined is precisely $\binom{p^n}{2}$, every pair occurs in exactly one triple.

14.5.12 Definition Two BIBDs (V_1, B_1), (V_2, B_2) are *isomorphic* if there exists a bijection $\alpha : V_1 \to V_2$ such that $B_1\alpha = B_2$. An *automorphism* is an isomorphism of a design with itself. The set of all automorphisms of a design forms a group, the *(full) automorphism group*. An *automorphism group* is any subgroup of the full automorphism group.

14.5.13 Remark If $(V, \mathcal{B})$ is a BIBD(v, b, r, k, λ) with automorphism group G, the action of G partitions $\mathcal{B}$ into classes (*orbits*). A set of orbit representatives is a set of *starter blocks* or *base blocks*. Applying the action of G to a set of base blocks yields a design, the *development*.

14.5.14 Remark In Construction 14.5.10, we can treat $\mathcal{D} = \{\{\omega^i, \omega^{2t+i}, \omega^{4t+i}\} : 0 \leq i < t\}$ as the *base* or *starter triples* of the design. Their *development* is the result of applying the action of the elementary abelian group of order p^n to the base triples. The verification requires that for every *difference* $d \in \mathbb{F}_{p^n} \setminus \{0\}$, there is exactly one way to choose $x, y \in D \in \mathcal{D}$ so that $d = x - y$, with arithmetic in the elementary abelian group of order p^n.

14.5.15 Construction [801] Let p be a prime, $n \geq 1$, and $p^n \equiv 7 \pmod{12}$. Let $\mathbb{F}_{p^n}$ be a finite field on a set X of size $p^n = 6t + 1 = 12s + 7$ with 0 as its zero element and ω a primitive root

of unity. Then

$$\{\{\omega^{2i}+j, \omega^{2t+2i}+j, \omega^{4t+2i}+j\} : 0 \le i < t, j \in X\}$$

forms the blocks of an STS(p^n) on X. (These are the *Netto triple systems.*)

14.5.16 Remark The Netto triple systems provide examples of STS(v)s that admit 2-homogeneous automorphism groups but (for $v > 7$) do not admit 2-transitive groups. We give another construction of the Netto triple systems. Let

$$\Gamma = \{a^2 x\sigma + b \ : \ a, b \in \mathbb{F}_{p^n},\ \sigma \in \mathrm{Aut}(\mathbb{F}_{p^n})\}.$$

Let ε be a primitive sixth root of unity in $\mathbb{F}_{p^n}$. Then the orbit of $\{0, 1, \varepsilon\}$ under the action of Γ is the Netto triple system of order p^n. This illustrates one of the principal reasons for using large automorphism groups, and in particular for using the additive and multiplicative structure of the finite field – a single triple represents the entire triple system.

14.5.17 Construction [1449] Let $p = 2t + 1$ be an odd prime. Let ω be a primitive root of unity in $\mathbb{Z}_p$ satisfying $\omega \equiv 1 \pmod 3$. Then

$$\{\{\omega^i + j, \omega^{2t+i} + j, \omega^{4t+i} + j\} : 0 \le i < t, j \in \mathbb{Z}_{3p}\} \cup \{\{j, j + p, j + 2p\} : j \in \mathbb{Z}_p\}$$

(with computations modulo $3p$) is the set of blocks of an STS($3p$).

14.5.18 Definition A set of blocks is a *partial parallel class (PPC)* if no two blocks in the set share an element. A PPC is an *almost parallel class* if it contains $\frac{v-1}{3}$ blocks; when it contains $\frac{v}{3}$ blocks, it is a *parallel class* or *resolution class*. A partition of all blocks of a TS(v, λ) into parallel classes is a *resolution* and the STS is *resolvable*. An STS(v) together with a resolution of its blocks is a *Kirkman triple system*, KTS(v).

14.5.19 Remark In Construction 14.5.17, the triples $\{\{j, j+p, j+2p\} : j \in \mathbb{Z}_p\}$ form a parallel class. Indeed we can say much more in certain cases. The method of "pure and mixed differences" [354] is applied, using a set of elements $\mathbb{F}_q \times X$, for X a finite set; a *pure(x) difference* is the difference $d = a - b$ associated with the pair $\{(a, x), (b, x)\}$ and a *mixed(x,y) difference* is the difference $d = a - b$ associated with the pair $\{(a, x), (b, y)\}$.

14.5.20 Construction [2424] If $q = p^\alpha \equiv 1 \pmod 6$ is a prime power, then there exists a KTS($3q$). Let $t = (q - 1)/6$. To construct a KTS($3q$), take as elements $\mathbb{F}_q \times \{1, 2, 3\}$, writing a_i for (a, i). Let ω be a primitive element in $\mathbb{F}_q$, and let $\mathcal{B}$ consist of triples:

1. $C = \{0_1, 0_2, 0_3\}$;
2. $B_{ij} = \{\omega_j^i, \omega_j^{i+2t}, \omega_j^{i+4t}\}$, $0 \le i < t$, $j \in \{1, 2, 3\}$;
3. $A_i = \{\omega_1^i, \omega_2^{i+2t}, \omega_3^{i+4t}\}$, $0 \le i < t$.

Each of the (nonzero) pure and mixed differences occurs exactly once in triples of $\mathcal{B}$, and thus $\mathcal{B}$ is the set of starter triples for an STS($3q$). This STS($3q$) is resolvable. Indeed, $R_0 = C \cup \{B_{ij} : 0 \le i < t,\ j \in \{1, 2, 3\}\} \cup \{A_{jt+i} : j \in \{1, 3, 5\}, 0 \le i < t\}$ forms a parallel class; when developed modulo $6t + 1$, it yields a further $6t$ parallel classes. Each A_i, when developed modulo $6t + 1$, also yields a parallel class; taking those parallel classes only from A_{jt+i} with $j \in \{0, 2, 4\}$ and $0 \le i < t\}$ thus yields a further $3t$ parallel classes, for a total of $9t + 1$ forming the resolution.

14.5.21 Construction [2424] If $q = p^\alpha \equiv 1 \pmod 6$ is a prime power, then there exists a KTS($2q+1$). Let $t = (q - 1)/6$. To construct a KTS($2q + 1$), take as elements $(\mathbb{F}_q \times \{1, 2\}) \cup \{\infty\}$. Let ω be a primitive element of $\mathbb{F}_q$, and let m satisfy $2\omega^m = \omega^t + 1$. Let $\mathcal{B}$ consist of triples

1. $C = \{0_1, 0_2, \infty\}$;
2. $B_i = \{\omega_1^i, \omega_1^{i+t}, \omega_2^{i+m}\}$, $0 \le i < t$, $2t \le i < 3t$, or $4t \le i < 5t$;
3. $A_i = \{\omega_2^{i+m}, \omega_2^{i+m+3t}, \omega_2^{i+m+5t}\}$, $0 \le i < t$.

Every pure and every mixed difference occurs exactly once and hence $\mathcal{B}$ is a set of starter triples for an STS$(2q+1)$. But $\mathcal{B}$ itself forms a parallel class, whose development modulo q yields the required q parallel classes for the KTS$(2q+1)$.

14.5.3 Difference families and balanced incomplete block designs

14.5.22 Definition Let $B = \{b_1, ..., b_k\}$ be a subset of an additive group G. The *G-stabilizer* of B is the subgroup G_B of G consisting of all elements $g \in G$ such that $B + g = B$. B is *full* or *short* according to whether G_B is or is not trivial. The *G-orbit* of B is the set $Orb_G B$ of all distinct right translates of B, namely, $Orb_G B = \{B + s \mid s \in S\}$ where S is a complete system of representatives for the right cosets of G_B in G.

14.5.23 Definition The multiset $\Delta B = \{b_i - b_j \mid i, j = 1, \ldots, k, i \ne j\}$ is the *list of differences from* B. The multiplicity in ΔB of an element $g \in G$ is of the form $\mu_g |G_B|$ for some integer μ_g. The *list of partial differences from* B is the multiset ∂B where each $g \in G$ appears exactly μ_g times. ($\Delta B = \partial B$ if and only if B is a full block.)

14.5.24 Definition Let G be a group of order v. A collection $\{B_1, ..., B_t\}$ of k-subsets of G forms a (v, k, λ) *difference family* (or *difference system*) if every nonidentity element of G occurs λ times in $\partial B_1 \cup \cdots \cup \partial B_t$. The sets B_i are *base blocks*. A difference family having at least one short block is *partial*.

14.5.25 Remark

1. All definitions given can be extended to a multiplicative group by replacing $B+g$ with $B \cdot g$ and $b_i - b_j$ with $b_i b_j^{-1}$.
2. If $t = 1$, then B_1 is a (v, k, λ) difference set; see Section 14.6.
3. If $\{B_1, \ldots, B_t\}$ is a (v, k, λ) difference family over G, $Orb_G(B_1) \cup \cdots \cup Orb_G(B_t)$ is the collection of blocks of a BIBD(v, k, λ) admitting G as a sharply point-transitive automorphism group. This BIBD is *cyclic (abelian, nonabelian, dihedral, and so on)* if the group G has the respective property. In this case the difference family is a *cyclic (abelian, nonabelian, dihedral, respectively) difference family*.
4. A BIBD(v, k, λ) with an automorphism group G acting sharply transitively on the points is (up to isomorphism) generated by a suitable (v, k, λ) difference family.
5. Every short block of a $(v, k, 1)$ difference family over an abelian group G is a coset of a suitable subgroup of G.

14.5.26 Theorem [259] The set of order p subgroups of $\mathbb{F}_{p^n}$ forms a $(p^n, p, 1)$ difference family generating the point-line design associated with the affine geometry $AG(n, p)$.

14.5.27 Definition

1. $C = \{c_1, \ldots, c_k\}$ is a *multiple* of $B = \{b_1, \ldots, b_k\}$ if, for some w, $c_i = w \cdot b_i$ for all i.

2. w is a *multiplier* of order n of $B = \{b_1, \ldots, b_k\}$ if $w^n = 1$ but $w^i \neq 1$ for $0 < i < n$, and for some $g \in G$, $B = w \cdot B + g = \{w \cdot b_1 + g, w \cdot b_2 + g, \ldots, w \cdot b_k + g\}$.
3. w is a *multiplier* of a difference family D if, for each base block $B \in D$, there exists $C \in D$ and $g \in G$ for which $w \cdot B + g = C$.
4. If q is a prime power and D is a (q, k, λ) difference family over $\mathbb{F}_q$ in which one base block, B, has a multiplier of order k or $k-1$ and all other base blocks are multiples of B, then D is *radical*.

14.5.28 Theorem [5] Suppose $q \equiv 7 \pmod{12}$ is a prime power and there exists a cube root of unity ω in $\mathbb{F}_q$ such that $x = \omega - 1$ is a primitive root. Then the following base blocks form a (7q,4,1) difference family over $\mathbb{Z}_7 \times \mathbb{F}_q$:

1. $\{(0,0), (0,(x-1)x^{2t-1}), (0,\omega(x-1)x^{2t-1}), (0,\omega^2(x-1)x^{2t-1})\}$ for $1 \leq t \leq (q-7)/12$,
2. $\{(0,0), (1,x^{2t}), (2,\omega x^{2t}), (4,\omega^2 x^{2t})\}$ for $1 \leq t \leq (q-3)/2$, $x^{2t} \neq \omega$, and
3. $\{(0,0), (2^t,\omega^t), (2^t, x \cdot \omega^t), (2^{t+2},0)\}$ for $0 \leq t \leq 2$.

14.5.29 Remark The (7q,4,1) difference families are obtainable by Theorem 14.5.28 for q = 7, 19, 31, 43, 67, 79, 103, 127, 151, 163, 199, 211, 367, 379, 439, 463, 487, 571, but not for q = 139, 223, 271, 283, 307, 331, 523, 547. A more general construction for (7q,4,1) difference families with q a prime power $\equiv 7 \pmod{12}$ can be found in [5].

14.5.30 Theorem [2967] Suppose q is a prime power, and $\lambda(q-1) \equiv 0 \pmod{k(k-1)}$. Then a (q, k, λ) difference family over $\mathbb{F}_q$ exists if

1. λ is a multiple of $k/2$ or $(k-1)/2$;
2. $\lambda \geq k(k-1)$; or
3. $q > \binom{k}{2}^{k(k-1)}$.

14.5.31 Theorem [455] Suppose q is an odd prime power. Then there exists a (q, k, λ) radical difference family if either:

1. λ is a multiple of $k/2$ and $q \equiv 1 \pmod{k-1}$, or
2. λ is a multiple of $(k-1)/2$ and $q \equiv 1 \pmod{k}$.

14.5.32 Remark For radical difference families with $\lambda = 1$, the multiplier must have odd order (that is, order k if k is odd, or order $k-1$ if k is even).

14.5.33 Theorem [455] Let $q = 12t + 1$ be a prime power and 2^e be the largest power of 2 dividing t. Then a $(q, 4, 1)$ radical difference family in $\mathbb{F}_q$ exists if and only if -3 is not a 2^{e+2}-th power in $\mathbb{F}_q$. (This condition holds for q = 13, 25, 73, 97, 109, 121, 169, 181, 193, 229, 241, 277, 289, 313, 337, 409, 421, 433, 457, 529, 541, 577, 601, 625, 673, 709, 733, 757, 769, 829, 841.)

14.5.34 Theorem [455] Let $q = 20t + 1$ be a prime power, and let 2^e be the largest power of 2 dividing t. Then a $(q, 5, 1)$ radical difference family in $\mathbb{F}_q$ exists if and only if $(11 + 5\sqrt{5})/2$ is not a 2^{e+1}-th power in $\mathbb{F}_q$. (This condition holds for q = 41, 61, 81, 241, 281, 401, 421, 601, 641, 661, 701, 761, 821, 881.)

14.5.35 Remark In [456], necessary and sufficient conditions are given for a $(q, k, 1)$ radical difference family with $k \in \{6, 7\}$ to exist over $\mathbb{F}_q$; a sufficient condition is also given for $k \geq 8$.

14.5.36 Theorem [456, 1346, 2967] Among others, $(q, k, 1)$ radical difference families exist for the following values of q and k:

$k = 6$ $q \in \{181, 211, 241, 631, 691, 1531, 1831, 1861, 2791, 2851, 3061\}$;
$k = 7$ $q \in \{337, 421, 463, 883, 1723, 3067, 3319, 3823, 3907, 4621, 4957, 5167, 5419, 5881, 6133, 8233, 8527, 8821, 9619, 9787, 9829\}$;
$k = 8$ $q \in \{449, 1009, 3137, 3697, 6217, 6329, 8233, 9869\}$;
$k = 9$ $q \in \{73, 1153, 1873, 2017, 6481, 7489, 7561, 8359\}$.

14.5.37 Theorem [1260] If there exists a $(p, k, 1)$ radical difference family with p a prime and k odd, there exists a cyclic RBIBD$(kp, k, 1)$ whose resolution is invariant under the action of $\mathbb{Z}_{kp}$.

14.5.4 Nested designs

14.5.38 Theorem [702] Let p be a prime, $n \geq 1$, $p^n \equiv 1 \pmod 6$, and ω be a primitive root of $\mathbb{F}_{p^n}$, $p^n = 6t + 1$. Let $\mathcal{S} = \{\omega^0, \omega^{2t}, \omega^{4t}\}$, and $\mathcal{S}_i = \omega^i \mathcal{S}$.

1. For $0 \leq c < t$, the development of $\{0\} \cup \mathcal{S}_c$ under the addition and multiplication of $\mathbb{F}_{p^n}$ forms a $(p^n, 4, 2)$ design in which the omission of the first element in each block yields an STS(p^n).
2. For $0 \leq c < d < t$, the development of $\mathcal{S}_c \cup \mathcal{S}_d$ under the addition and multiplication of $\mathbb{F}_{p^n}$ forms a $(p^n, 6, 5)$ design.

14.5.39 Remark The STSs in Theorem 14.5.38 Part 1 have been called *nested Steiner triple systems*, but the standard statistical notion of nested design is different – see Definition 14.5.40 and [2145].

14.5.40 Definition If the blocks of a BIBD $(\mathcal{V}, \mathcal{D}_1)$ with v symbols in b_1 blocks of size k_1 are each partitioned into sub-blocks of size k_2, and the $b_2 = b_1 k_1 / k_2$ sub-blocks themselves constitute a BIBD $(V, \mathcal{D}_2)$, then the system of blocks, sub-blocks, and symbols is a *nested balanced incomplete block design* (nested BIBD or NBIBD) with parameters $(v, b_1, b_2, r, k_1, k_2)$, r denoting the common replication. Also $(V, \mathcal{D}_1)$ and $(V, \mathcal{D}_2)$ are the *component BIBDs* of the NBIBD.

14.5.41 Remark A resolvable BIBD (RBIBD) $(V, \mathcal{D})$ is a nested block design $(V, \mathcal{D}_1, \mathcal{D}_2)$ where the blocks of $\mathcal{D}_1$, of size $k_1 = v$, are the resolution classes of $\mathcal{D}$, and $\mathcal{D}_2 = \mathcal{D}$.

14.5.42 Remark Nested block designs may have more than two blocking systems and consequently more than one level of nesting. A *doubly nested* block design is a system $(\mathcal{V}, \mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3)$ where both $(\mathcal{V}, \mathcal{D}_1, \mathcal{D}_2)$ and $(\mathcal{V}, \mathcal{D}_2, \mathcal{D}_3)$ are nested block designs. A resolvable NBIBD is a doubly nested block design.

14.5.43 Definition A *multiply nested* BIBD (MNBIBD) is a nested block design $(\mathcal{V}, \mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_s)$ with parameters $(v, b_1, \ldots, b_s, r, k_1, \ldots, k_s)$ for which the systems $(\mathcal{V}, \mathcal{D}_j, \mathcal{D}_{j+1})$ are NBIBDs for $j = 1, \ldots, s - 1$.

14.5.44 Theorem [2145] Let v be a prime power of the form $v = a_0 a_1 a_2 \cdots a_n + 1$ ($a_0 \geq 1$, $a_n \geq 1$ and $a_i \geq 2$ for $1 \leq i \leq n - 1$ are integers). Then there is an MNBIBD with n component designs having $k_1 = u a_1 a_2 \cdots a_n$, $k_2 = u a_2 a_3 \cdots a_n, \ldots,$ $k_n = u a_n$, and with $a_0 v$ blocks of size k_1, for any integer u with $1 \leq u \leq a_0$ and $u > 1$ if $a_n = 1$. If integer $t \geq 2$ is chosen so that $2 \leq tu \leq a_0$, then there is an MNBIBD with $n + 1$ component designs, with the same number of big blocks but of size $k_0 = t k_1$, and with its n other block sizes being $k_1, \ldots, k_n$ as given. Moreover, if a_0 is even and a_i is odd for $i \geq 1$, then MNBIBDs can be constructed with the same block sizes but with $a_0 v / 2$ blocks of size k_1.

14.5.45 Definition A *nested row-column design* is a system $(\mathcal{V}, \mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3)$ for which (1) each of $(\mathcal{V}, \mathcal{D}_1, \mathcal{D}_2)$ and $(\mathcal{V}, \mathcal{D}_1, \mathcal{D}_3)$ is a nested block design, (2) each block of $\mathcal{D}_1$ may be displayed as a $k_2 \times k_3$ row-column array, one member of the block at each position in the array, so that the columns are the $\mathcal{D}_2$ sub-blocks in that block, and the rows are the $\mathcal{D}_3$ sub-blocks in that block.

14.5.46 Definition A *(completely balanced) balanced incomplete block design with nested rows and columns*, BIBRC(v, b_1, k_2, k_3), is a nested row-column design $(\mathcal{V}, \mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3)$ for which each of $(\mathcal{V}, \mathcal{D}_1, \mathcal{D}_2)$ and $(\mathcal{V}, \mathcal{D}_1, \mathcal{D}_3)$ is a NBIBD.

14.5.47 Theorem [2145] If $v = mpq + 1$ is a prime power and p and q are relatively prime, then initial nesting blocks for a BIBRC(v, mv, sp, tq) are $A_l = x^{l-1}L \otimes M$ for $l = 1, \ldots, m$, where $L_{s\times t} = (x^{i+j-2})_{i,j}$, $M_{p\times q} = (x^{[(i-1)q+(j-1)p]m})_{i,j}$, s and t are integers with $st \leq m$, and x is a primitive element of $\mathbb{F}_v$. (Here $\otimes$ is the Kronecker product.) If m is even and pq is odd, $A_1, \ldots, A_{m/2}$ are intial nesting blocks for BIBRC$(v, mv/2, sp, tq)$;

14.5.48 Theorem [2145] Write $x^{u_i} = 1 - x^{2mi}$ where x is a primitive element of $\mathbb{F}_v$ and $v = 4tm+1$ is a prime power. Let A be the addition table with row margin $(x^0, x^{2m}, \ldots, x^{(4t-2)m})$ and column margin $(x^m, x^{3m}, \ldots, x^{(4t-1)m})$, and set $A_l = x^{l-1}A$. If $u_i - u_j \not\equiv m \pmod{2m}$ for $i, j = 1, \ldots, t$, then $A_1, \ldots, A_m$ are initial nesting blocks for BIBRC$(v, mv, 2t, 2t)$. Including 0 in each margin for A, if further $u_i \not\equiv m \pmod{2m}$ for $i = 1, \ldots, t$, then $A_1, \ldots, A_m$ are initial nesting blocks for BIBRC$(v, mv, 2t + 1, 2t + 1)$.

14.5.5 Pairwise balanced designs

14.5.49 Definition Let K be a subset of positive integers and let λ be a positive integer. A *pairwise balanced design* (PBD(v, K, λ) or (K, λ)-PBD) of order v with block sizes from K is a pair $(\mathcal{V}, \mathcal{B})$, where $\mathcal{V}$ is a finite set (the *point set*) of cardinality v and $\mathcal{B}$ is a family of subsets (*blocks*) of $\mathcal{V}$ that satisfy (1) if $B \in \mathcal{B}$, then $|B| \in K$ and (2) every pair of distinct elements of $\mathcal{V}$ occurs in exactly λ blocks of $\mathcal{B}$. The integer λ is the *index* of the PBD. The notations PBD(v, K) and K-PBD of order v are often used when $\lambda = 1$.

14.5.50 Example A PBD$(10, \{3, 4\})$ is given below where the blocks are listed columnwise.

1	1	1	2	2	2	3	3	3	4	4	4
2	5	8	5	6	7	5	6	7	5	6	7
3	6	9	8	9	10	10	8	9	9	10	8
4	7	10									

14.5.51 Remark Many constructions of pairwise balanced designs employ sub-structures in balanced incomplete block designs. In a (v, k, λ)-design $(V, \mathcal{B})$, useful sub-structures include those specified by a set $S \subset V$ so that for every $B \in \mathcal{B}$, $|B \cap S| \in L$; then setting $K = \{k - \ell : \ell \in L\}$, a $(|V \setminus S|, K, \lambda)$-PBD arises by removing all points of S. When the BIBD is made by a finite field construction, such sub-structures may arise from algebraic properties of the field. Other useful sub-structures arise from the presence of parallel classes; when a parallel class of blocks is present, a new element can be added and adjoined to each block in the parallel class to increase the size of some blocks by one. Example 14.5.50 is produced in this way from a (9,3,1)-design. This can be applied to more than one parallel class, when present [700, §IV]

14.5.6 Group divisible designs

14.5.52 Definition Let K and G be sets of positive integers and let λ be a positive integer. *A group divisible design of index λ and order v* ((K,λ)-GDD) is a triple $(\mathcal{V},\mathcal{G},\mathcal{B})$, where $\mathcal{V}$ is a finite set of cardinality v, $\mathcal{G}$ is a partition of $\mathcal{V}$ into parts (*groups*) whose sizes lie in G, and $\mathcal{B}$ is a family of subsets (*blocks*) of $\mathcal{V}$ that satisfy (1) if $B \in \mathcal{B}$ then $|B| \in K$, (2) every pair of distinct elements of $\mathcal{V}$ occurs in exactly λ blocks or one group, but not both, and (3) $|\mathcal{G}| > 1$. If $v = a_1g_1 + a_2g_2 + \cdots + a_sg_s$, and if there are a_i groups of size g_i, $i = 1, 2, \ldots, s$, then the (K,λ)-GDD is of type $g_1^{a_1}g_2^{a_2}\ldots g_s^{a_s}$. This is *exponential notation* for the group type. Alternatively, if the GDD has groups $G_1, G_2, \ldots, G_t$, then the list $T = [|G_i| : i = 1, 2, \ldots, t]$ is the *type* of the GDD when more convenient. If $K = \{k\}$, then the (K,λ)-GDD is a (k,λ)-GDD. If $\lambda = 1$, the GDD is a K-GDD. Furthermore, a $(\{k\},1)$-GDD is a k-GDD.

14.5.53 Definition Let H be a subgroup of order h of a group G of order v. A collection $\{B_1, ..., B_t\}$ of k-subsets of G forms a (v,h,k,λ) *difference family over G and relative to H* if $\partial B_1 \cup \cdots \cup \partial B_t$ covers each element of $G - H$ exactly λ times and covers no element in H.

14.5.54 Remark

1. A $(v,1,k,\lambda)$ difference family is a (v,k,λ) difference family.
2. If $\{B_1,\ldots,B_t\}$ is a (v,h,k,λ) difference family over G and relative to H, then $Orb_G(B_1) \cup \cdots \cup Orb_G(B_t)$ is the collection of blocks of a (k,λ) GDD of type $h^{v/h}$ where the groups are the right cosets of H in G. This GDD admits G as a sharply point-transitive automorphism group.
3. A (k,λ) GDD of type $h^{v/h}$ with an automorphism group G acting sharply transitively on the points is, up to isomorphisms, generated by a suitable (v,h,k,λ) difference family.
4. If $\{B_1,\ldots,B_t\}$ is a (v,k,k,λ) difference family over G and relative to H, then $\{B_1,\ldots,B_t\} \cup \{\underbrace{H,\ldots,H}_{\lambda \text{ times}}\}$ is a (v,k,λ) difference family.

14.5.55 Theorem [4, 1347] Suppose $q \equiv 1 \pmod{k-1}$ is a prime power. Then a $(kq,k,k,1)$ relative difference family over $\mathbb{F}_k \times \mathbb{F}_q$ exists if one of the following holds:

1. $k \in \{3,5\}$ (for $k = 5$, the initial block B can be taken as $\{(0,0),(1,1),(1,-1),(4,x),(4,-x)\}$ where x is any nonsquare in $\mathbb{F}_q$ such that exactly one of $x-1, x+1$ is a square);
2. $k = 7$ and $q \neq 19$;
3. $k = 9$ and $q \notin \{17, 25, 41, 97, 113\}$;
4. $k = 11, q < 1202$, q is prime, and $q \notin$ [30,192], [240,312] or [490,492].

14.5.56 Theorem [457]

1. Let $q = 12t + 1$ be a prime power, and let 3^e be the largest power of 3 dividing t. If, in $\mathbb{F}_q$, 3 and $2 + \sqrt{3}$ are both 3^e-th powers but not 3^{e+1}-th powers and 6 is not a 3^{e+1}-th power, then a $(13q, 13, 13, 1)$ relative difference family exists.
2. If p and q are odd prime powers with $q > p$, then a $(pq, p, p, (p-1)/2)$ relative difference family exists. If further $p \equiv 1 \pmod 4$ and $q \equiv 1 \pmod{p-1}$, then a $(pq, p, p, (p-1)/4)$ relative difference family exists.

14.5.7 t-designs

14.5.57 Definition A t-(v,k,λ) *design*, a t-design in short, is a pair $(X,\mathcal{B})$ where X is a v-set of *points* and $\mathcal{B}$ is a collection of k-subsets of X (*blocks*) with the property that every t-subset of X is contained in exactly λ blocks. The parameter λ is the *index* of the design.

14.5.58 Example Let q be a prime power and $n > 0$ be an integer. Then $G = \mathrm{PGL}(2, q^n)$ acts sharply 3-transitively on $X = \mathbb{F}_{q^n} \cup \{\infty\}$. If $S \subseteq X$ is the natural inclusion of $\mathbb{F}_q \cup \{\infty\}$, then the orbit of S under G is a 3-$(q^n+1, q+1, 1)$ design. These designs are *spherical geometries*; when $n = 2$, they are *inversive planes* or *Möbius planes*.

14.5.59 Theorem [1547] Let B be a subgroup of the multiplicative group of nonzero elements of $\mathbb{F}_q$. Then the orbit of $S = B \cup \{0, \infty\}$ under the action of $\mathrm{PGL}(2,q)$ is the block set of one of the designs:

1. 3-$(q^n+1, q+1, 1)$ design where q is a prime power and $n \geq 2$ (a spherical geometry);
2. 3-$(q+1, k+1, k(k+1)/2)$ design if $(k-1)|(q-1)$, $k \not| q$, and $k \notin \{3, 5\}$;
3. 3-$(q+1, 4, 3)$ design for $q \equiv 1, 5 \pmod 6$;
4. 3-$(q+1, 6, 5)$ design for $q \equiv 1, 9, 13, 17 \pmod{20}$.

14.5.8 Packing and covering

14.5.60 Remark Packings and coverings relax the conditions on block designs, and have been extensively studied; see [2092] for a more detailed exposition.

14.5.61 Definition Let $v \geq k \geq t$. A t-(v,k,λ) *covering* is a pair $(X,\mathcal{B})$, where X is a v-set of elements (*points*) and $\mathcal{B}$ is a collection of k-subsets (*blocks*) of X, such that every t-subset of points occurs in at least λ blocks in $\mathcal{B}$. Repeated blocks in $\mathcal{B}$ are permitted.

14.5.62 Theorem (Schönheim bound) [2092] $C_\lambda(v,k,t) \geq \lceil v\, C_\lambda(v-1, k-1, t-1)/k \rceil$. Iterating this bound yields $C_\lambda(v,k,t) \geq L_\lambda(v,k,t)$, where

$$L_\lambda(v,k,t) = \left\lceil \frac{v}{k} \left\lceil \frac{v-1}{k-1} \cdots \left\lceil \frac{\lambda(v-t+1)}{k-t+1} \right\rceil \right\rceil \right\rceil .$$

14.5.63 Definition Let $v \geq k \geq t$. A t-(v,k,λ) *packing* is a pair $(X,\mathcal{B})$, where X is a v-set of elements (*points*) and $\mathcal{B}$ is a collection of k-subsets of X (*blocks*), such that every t-subset of points occurs in at most λ blocks in $\mathcal{B}$. If $\lambda > 1$, then $\mathcal{B}$ is allowed to contain repeated blocks.

14.5.64 Remark A t-$(v,k,1)$ packing with b blocks is equivalent to a binary code of length v, size b, constant weight k, and minimum Hamming distance at least $2(k-t+1)$; see Section 15.1.

14.5.65 Theorem (First Johnson bound) [2092] $D_\lambda(v,k,t) \leq \left\lfloor \frac{v D_\lambda(v-1,k-1,t-1)}{k} \right\rfloor$. Iterating this bound yields $D_\lambda(v,k,t) \leq U_\lambda(v,k,t)$, where

$$U_\lambda(v,k,t) = \left\lfloor \frac{v}{k} \left\lfloor \frac{v-1}{k-1} \cdots \left\lfloor \frac{\lambda(v-t+1)}{k-t+1} \right\rfloor \right\rfloor \right\rfloor .$$

Further, if $\lambda(v-1) \equiv 0 \pmod{k-1}$ and $\frac{\delta(k-1)}{2} > \lambda\frac{\delta(\delta-1)}{2}$, where $\delta = \frac{\lambda v(v-1)}{k-1} - kU_\lambda(v,k,2)$, then $D_\lambda(v,k,2) \le U_\lambda(v,k,2) - 1$.

14.5.66 Theorem (Second Johnson bound) [2092] Suppose $d = D_1(v,k,t) = qv + r$, where $0 \le r \le v-1$. Then $q(q-1)v + 2qr \le (t-1)d(d-1)$, and hence $D_1(v,k,t) \le \left\lfloor \frac{v(k+1-t)}{k^2 - v(t-1)} \right\rfloor$.

See Also

§14.1	For latin squares, MOLS, and transversal designs.
§14.3	For affine and projective planes.
§14.4	For projective spaces.
§14.6	For difference sets.
§14.7	For other combinatorial structures.
[259]	A textbook on combinatorial designs.
[260]	Another textbook on combinatorial designs.
[700]	For triple systems (§II.2); balanced incomplete block designs (§II.1,II.3,II.5); t-designs (§II.4,II.5); symmetric designs (§II.6); Hadamard designs and matrices(§V.1); difference sets (§VI.18); resolvable designs (§II.7); pairwise balanced designs and group divisible designs (§IV); coverings (§VI.11); packings (§VI.40); nested designs (§VI.36); connections with MOLS and transversal designs (§III.1,III.3).
[2145]	For nested designs.
[2702]	For an introductory textbook on combinatorial designs.

References Cited: [4, 5, 259, 260, 354, 455, 456, 457, 700, 702, 801, 1260, 1346, 1347, 1449, 1547, 1729, 2092, 2145, 2208, 2424, 2702, 2967]

14.6 Difference sets

Alexander Pott, *Otto-von-Guericke-Universität Magdeburg*

14.6.1 Basics

14.6.1 Definition Let G be an additively written group of order v. A k-subset D of G is a $(v,k,\lambda;n)$-*difference set* of *order* $n = k - \lambda$ if every nonzero element of G has exactly λ representations as a difference $d - d'$ with elements from D. The difference set is *abelian*, *cyclic*, etc., if the group G has the respective property. The redundant parameter n is sometimes omitted, therefore the notion of (v,k,λ)-difference sets is also used.

14.6.2 Example

1. The group G itself and $G\backslash\{g\}$ for an arbitrary $g \in G$ are $(v,v,v,0)$- and $(v, v-1, v-2; 1)$-difference sets.

2. The set $\{1,3,4,5,9\}$ is a cyclic $(11,5,2;3)$-difference set in the group $(\mathbb{Z}/11\mathbb{Z},+)$. These are the squares modulo 11.
3. The set $\{1,2,4\} \subset \mathbb{Z}/7\mathbb{Z}$ is a cyclic $(7,3,1;2)$-difference set.
4. The set $\{(0,1),(0,2),(0,3),(1,0),(2,0),(3,0)\} \subset \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ is a $(16,6,2;4)$ difference set.
5. There is a non-abelian example with the same parameters: Let $G = Q \times \mathbb{Z}/2\mathbb{Z}$, where $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ is the quaternion group, whose generators satisfy $i^2 = j^2 = k^2 = 1$, $ij = jk = ki = -1$. Then the set $D = \{(1,0),(i,0),(j,0),(k,0),(1,1),(-1,1)\}$ is a non-abelian $(16,6,2;4)$-difference set.

14.6.3 Remark A thorough investigation of difference sets is contained in [259], see also the tables in [260]. A short summary, including a list of small examples, is contained in [700]. Classical textbooks are [209] and [1830]. A recent book including a modern treatment of necessary conditions for the existence of difference sets is [2529].

14.6.4 Remark The complement of a $(v,k,\lambda;n)$-difference set is again a difference set but with parameters $(v, v-k, v-2k+\lambda; n)$. Therefore, we may assume $k \leq v/2$ (the case $k = v/2$ is actually impossible).

14.6.5 Remark Many constructions of difference sets are closely related to the connection between the additive and the multiplicative group of a finite field:

1. The set of nonzero squares in a field $\mathbb{F}_q$, $q \equiv 3 \pmod 4$, which is a multiplicative subgroup, is a difference set in the additive group of the field, see Theorem 14.6.38. Case 2 in Example 14.6.2 is such a difference set in $(\mathbb{F}_{11},+)$.
2. The set of elements of trace 0 in $\mathbb{F}_{2^n}$, which is an additive subgroup, forms a difference set in the multiplicative group of $\mathbb{F}_{2^n}$; see Theorem 14.6.22. Case 3 in Example 14.6.2 is such a difference set in $(\mathbb{F}_8^*,\cdot) \cong \mathbb{Z}/7\mathbb{Z}$.

14.6.6 Lemma The parameters v, k and λ of a difference set satisfy

$$\lambda \cdot (v-1) = k \cdot (k-1).$$

14.6.7 Remark Lemma 14.6.6 can be proved by counting differences. It also follows from Theorem 14.6.9 which shows that difference sets are the same objects as symmetric designs with a sharply transitive (regular) automorphism group. We refer the reader to Section 14.5 for the definition of symmetric designs and to [259] for a proof of the important Theorem 14.6.9.

14.6.8 Definition The *development* of a difference set D is the incidence structure *dev(D)* whose points are the elements of G and whose blocks are the translates $g+D := \{g+d : d \in D\}$.

14.6.9 Theorem [260] The existence of a $(v,k,\lambda;n)$-difference set is equivalent to the existence of a symmetric (v,k,λ)-design $\mathcal{D}$ admitting G as a point regular automorphism group; i.e., for any two points P and Q, there is a unique group element g which maps P to Q. The design $\mathcal{D}$ is isomorphic with $dev(D)$.

14.6.10 Remark Necessary conditions on the parameters v, k and λ of a symmetric design are also necessary conditions for the parameters of a difference set. In particular, the following two theorems hold. We emphasize that these are necessary conditions for symmetric designs, even if the designs are not constructed from difference sets.

14.6.11 Theorem [2549] If D is a $(v,k,\lambda;n)$ difference set with v even, then $n = u^2$ is a square.

14.6.12 Theorem [426, 625] If D is a $(v, k, \lambda; n)$ difference set with v odd, then the equation $nx^2 + (-1)^{(v-1)/2}\lambda y^2 = z^2$ must have an integral solution $(x, y, z) \neq (0, 0, 0)$.

14.6.13 Example Not all symmetric designs can be constructed from difference sets. There are, for instance, no difference sets with parameters $(25, 9, 3; 6)$ or $(31, 10, 3; 7)$, but symmetric designs with these parameters exist, see the tables in [260].

14.6.14 Remark The main problem about difference sets is to give necessary and sufficient conditions for their existence. These conditions sometimes depend only on the parameters $(v, k, \lambda; n)$, sometimes also on the structure of the ambient group G. Another problem is to classify all $(v, k, \lambda; n)$-difference sets up to equivalence or isomorphism. In many nonexistence theorems, the exponent of a group plays an important role.

14.6.15 Definition The *exponent* $\exp(G)$ of a (multiplicatively written) finite group G is the smallest integer v^* such that $g^{v^*} = 1$.

14.6.16 Remark There are many necessary conditions that the parameters of a difference set have to satisfy. An important condition is Theorem 14.6.62. Many more restrictions are in [2529].

14.6.17 Definition Two difference sets D_1 (in G_1) and D_2 (in G_2) are *equivalent* if there is a group isomorphism φ between G_1 and G_2 such that $D_1^\varphi = \{d^\varphi : d \in D_1\} = g + D_2$ for a suitable $g \in G_2$. The difference sets are *isomorphic* if the designs $dev(D_1)$ and $dev(D_2)$ are isomorphic.

14.6.18 Remark Equivalent difference sets yield isomorphic designs, but a design may give rise to several inequivalent difference sets, as the following example shows.

14.6.19 Example The following three difference sets in $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ with parameters $(16, 6, 2; 4)$ are pairwise inequivalent, but the designs are all isomorphic:

$$D_1 = \{(0,0), (1,0), (2,0), (0,1), (1,2), (2,3)\},$$
$$D_2 = \{(0,0), (1,0), (2,0), (0,1), (0,3), (3,2)\},$$
$$D_3 = \{(0,0), (1,0), (0,1), (2,1), (1,2), (2,3)\}.$$

14.6.20 Definition Some types of $(v, k, \lambda; n)$-difference sets have special names. A difference set with $\lambda = 1$ is *planar*. The parameters can be written in terms of the order n as $(n^2 + n + 1, n + 1, 1; n)$. The corresponding design is a projective plane. Difference sets with $v = 4n$ are *Hadamard* difference sets, in which case $n = u^2$ must be a square, and the parameters are $(4u^2, 2u^2 - u, u^2 - u; u^2)$. Difference sets with $v = 4n - 1$, hence with parameters $(4n - 1, 2n - 1, n - 1; n)$, are of *Paley* type. Both Hadamard and Paley type difference sets are closely related to Hadamard matrices; see Constructions 14.6.44 and 14.6.52. The parameters $\left(\frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}, \frac{q^{n-2}-1}{q-1}; q^{n-2}\right)$ are the *Singer* parameters; see Theorem 14.6.22.

14.6.21 Remark The parameters of a symmetric design, hence also the parameters of a $(v, k, \lambda; n)$-difference set satisfy $4n - 1 \leq v \leq n^2 + n + 1$. The extremal cases are Paley type difference sets ($v = 4n - 1$) and planar difference sets.

14.6.2 Difference sets in cyclic groups

14.6.22 Theorem [2657] Let α be a generator of the multiplicative group of $\mathbb{F}_{q^n}$, where q is a prime power. Then the set of integers $\{i : 0 \le i < (q^n-1)/(q-1), \mathrm{Tr}\,(\alpha^i) = 0\}$ modulo $(q^n-1)/(q-1)$ form a (cyclic) difference set with Singer parameters

$$\left(\frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}, \frac{q^{n-2}-1}{q-1}; q^{n-2}\right).$$

These difference sets are *Singer difference sets*.

14.6.23 Remark

1. If $q = 2$, the Singer difference set is simply the set of nonzero elements in an additive subgroup of order 2^{n-1}, interpreted as a subset of the multiplicative group of $\mathbb{F}_{2^n}$. These difference sets are of Paley type.
2. In the general case, a Singer difference set can be viewed as follows. Let $U := \{\beta \in \mathbb{F}_{q^n}^* : \mathrm{Tr}\,(\beta) = 0\}$. This is a subgroup of the additive group of $\mathbb{F}_{q^n}$ fixed by multiplication with elements from $\mathbb{F}_q$, hence it is a hyperplane of the vector space $\mathbb{F}_q^n$. The Singer difference set is the image of this hyperplane under the canonical projection $\mathbb{F}_{q^n}^* \to \mathbb{F}_{q^n}^*/\mathbb{F}_q^*$.
3. The design corresponding to a Singer difference set is the classical point-hyperplane design of the projective geometry $\mathrm{PG}(n-1, q)$.

14.6.24 Conjecture If $n = 3$, the Singer parameters are $(q^2+q+1, q+1, 1; q)$. It is conjectured that the only abelian difference sets (up to equivalence) with these parameters are the Singer difference sets. Moreover, it is conjectured that planar difference sets exist only if the order q is a prime power. This holds for all orders $q \le 2,000,000$; see [1316].

14.6.25 Construction The construction of Singer difference sets is easy if a primitive polynomial (see Section 4.1) $f(x) = x^n + \sum_{i=1}^n a_i x^{n-i}$ of degree n in $\mathbb{F}_{q^n}$ is known. Consider the recurrence relation $\gamma_m = -\sum_{i=1}^n a_i \gamma_{m-i}$. Take arbitrary initial values, for instance $\gamma_0 = 1, \gamma_1 = \gamma_2 = \cdots = \gamma_{n-1} = 0$. Then the set of integers $\{0 \le i < (q^n-1)/(q-1) : \gamma_i = 0\}$ is a Singer difference set. For instance, $x^4 + x^3 + 2$ is a primitive polynomial over $\mathbb{F}_3$. The recurrence relation $\gamma_m = 2\gamma_{m-1} + \gamma_{m-3}$ yields the sequence

$$1000121220111222202021120102100221202200200 0\ldots$$

which gives the cyclic $(40, 13, 4; 9)$-difference set

$$\{1, 2, 3, 9, 17, 19, 24, 26, 29, 30, 35, 38, 39\}.$$

14.6.26 Remark In general, there are many difference sets with Singer parameters inequivalent to Singer difference sets (Theorems 14.6.27 and 14.6.29). There are even non-abelian difference sets with Singer parameters; see Example 14.6.70.

14.6.27 Theorem [1314] Let D be an arbitrary cyclic difference set with parameters $\left(\frac{q^s-1}{q-1}, \frac{q^{s-1}-1}{q-1}, \frac{q^{s-2}-1}{q-1}; q^{s-2}\right)$ in a group G. Let G be embedded into $\mathbb{F}_{q^n}^*/\mathbb{F}_q^*$ which is possible if $s|n$. Let α be a primitive element in $\mathbb{F}_{q^n}$. Then the set of integers $\{0 \le i < (q^n-1)(q-1) : \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^s}}(\alpha^i) \in D\}$ is a difference set with classical Singer parameters. The difference sets are *Gordon-Mills-Welch difference sets* corresponding to D. Note that different embeddings of the same difference set D may result in inequivalent difference sets [209].

14.6.28 Remark If D is a Singer difference set, the above construction may be reformulated as follows: if s divides n and if r is relatively prime to $q^s - 1$, then the set of integers $\{0 \le i < (q^n-1)/(q-1) : \mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}[(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^s}}(\alpha^i))^r] = 0\}$ is a Gordon-Mills-Welch difference set.

14.6.29 Theorem [856, 858] Let α be a generator of the multiplicative group of $\mathbb{F}_{2^n}$, and let $t < n/2$ be an integer relatively prime to n, and $k = 4^t - 2^t + 1$. Then the set $D = \{(x+1)^k + x^k + 1 : x \in \mathbb{F}_{2^n}, x \neq 0, 1\} \subseteq \mathbb{F}_{2^n}^*$ is a *Dillon-Dobbertin difference set* with parameters $(2^n - 1, 2^{n-1} - 1, 2^{n-2} - 1; 2^{n-2})$. If $n = 3t \pm 1$, then the set $D = \mathbb{F}_{2^n}^* \setminus \{(x+1)^k + x^k : x \in \mathbb{F}_{2^n}\} \subseteq \mathbb{F}_{2^n}^*$ is a difference set with parameters $(2^n - 1, 2^{n-1} - 1, 2^{n-2} - 1; 2^{n-2})$.

14.6.30 Remark The series of Gordon-Mills-Welch difference sets [1314] and Dillon-Dobbertin difference sets [856, 858] show that the number of inequivalent difference sets grows rapidly. In these two series, inequivalent difference sets are in general also non-isomorphic; see [1664] for the Gordon-Mills-Welch case and [899] for the Dillon-Dobbertin case.

14.6.31 Construction [1295] Cyclic difference sets can be used to construct binary sequences with 2-level autocorrelation function. Let α be the generator of the cyclic group $\mathbb{Z}/v\mathbb{Z}$, and let D be a $(v, k, \lambda; n)$ difference set in $\mathbb{Z}/v\mathbb{Z}$. Define a sequence (a_i) by $a_i = 1$ if $\alpha^i \in D$, otherwise $a_i = 0$. This sequence has period v, and $C_t(a) := \sum_{i=0}^{n-1} (-1)^{a_i + a_{i+t}} = v - 4(k - \lambda)$ for $t = 1, \ldots, v - 1$, which are the *off-phase autocorrelation coefficients*; see also Section 10.3.

14.6.32 Remark Cyclic Paley type difference sets yield sequences with constant off-phase autocorrelation -1. These sequences (difference sets) have numerous applications since the autocorrelation is small (in absolute value) [1295]. It is conjectured that no sequences with constant off-phase autocorrelation 0 exist if $v > 4$; see Remark 14.6.45.

14.6.33 Conjecture (Ryser's Conjecture) [1830, 1897] If $\gcd(v, n) \neq 1$, then there is no cyclic $(v, k, \lambda; n)$ difference set in a cyclic group. A strengthening of this conjecture is due to Lander: if D is a $(v, k, \lambda; n)$-difference set in an abelian group of order v, and p is a prime dividing v and n, then the Sylow p-subgroup of G is not cyclic.

14.6.34 Theorem [1895] Lander's conjecture is true for all abelian difference sets of order $n = p^k$, where $p > 3$ is prime.

14.6.35 Remark

1. The smallest open case for Lander's conjecture is a cyclic $(465, 145, 45; 100)$ difference set.
2. More restrictions on putative counterexamples to Lander's conjecture are contained in [1897].

14.6.36 Theorem [116] Let $R = \{a \in \mathbb{F}_{3^m}^* : a = x + x^6$ has 4 solutions with $x \in \mathbb{F}_{3^m}\}$ with $m > 1$. Then the set $\rho(R)$ is a difference set with Singer parameters $((3^m - 1)/2, (3^{m-1} - 1)/2, (3^{m-2} - 1)/2; 3^{m-2})$, where ρ is the canonical epimorphism $\mathbb{F}_{3^m}^* \to \mathbb{F}_{3^m}^*/\mathbb{F}_3^*$.

14.6.37 Theorem [1467] Let $q = 3^e$, $e \geq 1$, $m = 3k$, $d = q^{2k} - q^k + 1$. If $R = \{x \in \mathbb{F}_{q^m} : \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x + x^d) = 1\}$, then $\rho(R)$ is a difference set with parameters $((q^m - 1)/(q - 1), q^{m-1}, q^{m-1} - q^{m-2}; q^{m-2})$, where ρ is the canonical epimorphism $\mathbb{F}_{q^m}^* \to \mathbb{F}_q^*$.

14.6.3 Difference sets in the additive groups of finite fields

14.6.38 Theorem [260] The following subsets of $\mathbb{F}_q$ are difference sets in the additive group of $\mathbb{F}_q$. They are *cyclotomic difference sets*. Some of these difference sets may have Singer parameters.

1. $\mathbb{F}_q^{(2)} := \{x^2 : x \in \mathbb{F}_q \backslash \{0\}\}$, $q \equiv 3 \pmod 4$ (quadratic residues, *Paley difference sets*);
2. $\mathbb{F}_q^{(4)} := \{x^4 : x \in \mathbb{F}_q \backslash \{0\}\}$, $q = 4t^2 + 1, t$ odd;

3. $\mathbb{F}_q^{(4)} \cup \{0\},\ q = 4t^2 + 9, t$ odd;
4. $\mathbb{F}_q^{(8)} = \{x^8 : x \in \mathbb{F}_q \backslash \{0\}\},\ q = 8t^2 + 1 = 64u^2 + 9, t, u$ odd;
5. $\mathbb{F}_q^{(8)} \cup \{0\},\ q = 8t^2 + 49 = 64u^2 + 441, t$ odd, u even;
6. $H(q) = \{x^i : x \in \mathbb{F}_q \backslash \{0\}, i \equiv 0, 1 \text{ or } 3 \pmod 6\},\ q = 4t^2 + 27, q \equiv 1 \pmod 6$ (*Hall difference sets*).

14.6.39 Remark The proofs of the statements in Theorem 14.6.38 use *cyclotomic numbers* [2708].

14.6.40 Theorem Let q and $q+2$ be prime powers. Then the set $D = \{(x, y) : x, y$ are both nonzero squares or both non-squares or $y = 0\}$ is a *twin prime power difference set* with parameters

$$\left(q^2 + 2q, \frac{q^2 + 2q - 1}{2}, \frac{q^2 + 2q - 3}{4}; \frac{q^2 + 2q + 1}{4}\right)$$

in the group $(\mathbb{F}_q, +) \times (\mathbb{F}_{q+2}, +)$; see [2708].

14.6.41 Definition A difference set D in the group G is *skew symmetric* if D is of Paley type and $\{0, d, -d : d \in D\} = G$, hence $D \cap -D = \emptyset$.

14.6.42 Theorem The following sets are skew symmetric difference sets in the additive group of $\mathbb{F}_q$, $q \equiv 3 \pmod 4$:

1. $\{x^2 : x \in \mathbb{F}_q, x \neq 0\}$ (Paley difference sets);
2. $\{x^{10} \pm x^6 - x^2 : x \in \mathbb{F}_q, x \neq 0\}$ where $q = 3^h$, h odd [868];
3. $\{x^{4a+6} \pm x^{2a} - x^2 : x \in \mathbb{F}_q, x \neq 0\}$ where $q = 3^h$, h odd, $a = 3^{\frac{h+1}{2}}$ [865].

14.6.43 Remark A large class of skew Hadamard difference sets in elementary abelian groups of order q^3 (q prime power) has been recently constructed [2196].

14.6.4 Difference sets and Hadamard matrices

14.6.44 Construction A Hadamard difference set D in a group G of order $4u^2$ (see Definition 14.6.20) gives rise to a Hadamard matrix (Section 14.5) as follows: Label the rows and columns of a matrix $H = (h_{x,y})$ by the elements of G, and put $h_{x,y} = 1$ if $x - y \in D$, otherwise $h_{x,y} = -1$. This matrix is a Hadamard matrix, see Section 14.5.

14.6.45 Remark A special case of Rysers's Conjecture 14.6.33 is that there are no cyclic Hadamard difference sets with $v > 4$ (if $v = 4$, there is a trivial cyclic $(4, 1, 0; 1)$-difference set). This is also known as the *circulant Hadamard matrix conjecture*. The smallest open case for which one cannot prove the nonexistence of a cyclic Hadamard difference set with $v = 4u^2$ so far is $u = 11715 = 3 \cdot 5 \cdot 11 \cdot 71$; see [1898] and also [2154] for the connection to the Barker sequence conjecture (Section 10.3).

14.6.46 Remark [260] Hadamard difference sets in elementary abelian groups are equivalent to bent functions (Section 9.3). The bent function is the characteristic function of the Hadamard difference set. The following theorem gives an explicit construction.

14.6.47 Theorem The set

$$\{(x_1, \ldots, x_{2m}) \in \mathbb{F}_2^{2m} : x_1x_2 + x_3x_4 + \cdots + x_{2m-1}x_{2m} = 1\} \subset \mathbb{F}_2^{2m}$$

is a Hadamard difference set with parameters $(2^{2m}, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1}; 2^{2m-2})$.

14.6.48 Remark There are several other constructions of difference sets with these parameters, also in other groups. Two major construction methods are the Maiorana-McFarland method (Sections 9.1 and 9.3) and the use of partial spreads (Section 9.3).

14.6.49 Theorem [775, 1790, 2812] An abelian Hadamard difference set in a group G of order 2^{2m+2} exists if and only if $\exp(G) \leq 2^{m+2}$.

14.6.50 Remark In the following theorem, we combine knowledge about the existence of abelian Hadamard difference sets. Many authors contributed to this theorem.

14.6.51 Theorem [259] Let $G \cong H \times EA(w^2)$ be an abelian group of order $4u^2$ with $u = 2^a 3^b w^2$ where w is the product of not necessarily distinct primes $p \equiv 3 \pmod 4$ and $EA(w^2)$ denotes the group of order w^2 which is the direct product of groups of prime order. If H is of type $(2^{a_1})(2^{a_2}) \cdots (2^{a_s})(3^{b_1})^2 \cdots (3^{b_r})^2$ with $\sum a_i = 2a+2$ ($a \geq 0$, $a_i \leq a+2$), $\sum b_i = 2b$ ($b \geq 0$), then G contains a Hadamard difference set of order u^2.

14.6.52 Construction [260] Difference sets with parameters $(4n-1, 2n-1, n-1; n)$ (hence of Paley type) in G can be used to construct Hadamard matrices: Label the rows and columns of a matrix H by the elements of $G \cup \{\infty\}$. The matrix $H = (h_{u,v})$ such that $h_{u,v} = 1$ if $u = \infty$ or $v = \infty$ or $u - v \in D$ is a Hadamard matrix of order $4n$.

14.6.53 Theorem For the following orders n, Paley type difference sets exist in groups of order $v = 4n - 1$:

1. $4n - 1$ is a prime power (Theorem 14.6.38);
2. $4n-1$ is the product $q(q+2)$ of two prime powers q and $q+2$ (Theorem 14.6.40);
3. $4n - 1 = 2^m - 1$ (Theorem 14.6.22).

14.6.54 Problem It is an open question whether Paley type difference sets exist for other values.

14.6.5 Further families of difference sets

14.6.55 Theorem [2038] Let q be a prime power and d a positive integer. Let G be a group of order $v = q^{d+1}(q^d + \cdots + q^2 + q + 2)$ which contains an elementary abelian subgroup E of order q^{d+1} in its center. View E as the additive group of $\mathbb{F}_q^{d+1}$. Put $r = (q^{d+1} - 1)/(q - 1)$ and let $H_1, \ldots, H_r$ be the hyperplanes of order q^d of E. If $g_0, \ldots, g_r$ are distinct coset representatives of E in G, then $D = (g_1 + H_1) \cup (g_2 + H_2) \cup \cdots \cup (g_r + H_r)$ is a *McFarland difference set* with parameters

$$\left(q^{d+1}(1 + \tfrac{q^{d+1}-1}{q-1}), q^d \cdot \tfrac{q^{d+1}-1}{q-1}, q^d \cdot \tfrac{q^d-1}{q-1}; q^{2d}\right).$$

14.6.56 Remark

1. If $q = 2$, the McFarland construction gives Hadamard difference sets.
2. If $q = 2$ and G is elementary abelian, this construction is known as the Maiorana-McFarland construction of bent functions; see Section 9.3.

14.6.57 Theorem [604, 776] Let q be a prime power, and let t be any positive integer. Difference sets with parameters

$$\left(4q^{2t}\frac{q^{2t}-1}{q^2-1}, q^{2t-1}\frac{2q^{2t}+q-1}{q+1}, q^{2t-1}(q-1)\frac{q^{2t-1}+1}{q+1}; q^{4t-2}\right)$$

exist in abelian groups G in the following cases:

1. $q = 3^f$, the Sylow 3-subgroup of G is elementary abelian;

2. $q = p^{2f}$, p odd, the Sylow p-subgroup of G is elementary abelian;
3. $q = 2^f$, the Sylow 2-subgroup of G has rank $\geq 2f + 1$;
4. $q = 2$, $\exp(G) \leq 4$.

If $t = 1$, these difference sets are Hadamard difference sets.

14.6.6 Difference sets and character sums

14.6.58 Remark The existence of difference sets is closely related to character sums. Most necessary conditions on the existence of difference sets are derived from character sums and number theoretic conditions.

14.6.59 Theorem [260, 2812] Let D be a $(v, k, \lambda; n)$ difference set in G, and let χ be a homomorphism from G into the multiplicative group of a field. If $\chi(g) = 1$ for all $g \in G$ (in which case the homomorphism is denoted χ_0), then $\sum_{g \in D} \chi_0(d) = k$. If $\chi \neq \chi_0$, then

$$\left(\sum_{d \in D} \chi(d)\right) \cdot \left(\sum_{d \in D} \chi(d^{-1})\right) = n.$$

14.6.60 Remark Theorem 14.6.59 is very useful if χ is complex-valued. In this case, the sum $\chi(D) := \sum_{d \in D} \chi(d)$ is an element in the ring $\mathbb{Z}[\zeta_{v^*}]$, where $\zeta_{v^*} = e^{2\pi i / v^*}$ is a primitive v^*-th root of unity, and v^* is the exponent of G.

14.6.61 Remark If χ is complex-valued, Theorem 14.6.59 may be also viewed as an equation about the ideal generated by $\chi(D)$: For $\chi \neq \chi_0$, we have $(\chi(D))(\overline{\chi(D)}) = (n)$, where $(\cdot)$ denotes an ideal generated in $\mathbb{Z}[\zeta_{v^*}]$ and $\overline{(\ )}$ is complex conjugation. Using results from algebraic number theory, many necessary conditions can be obtained.

14.6.62 Theorem [2812] Let D be an abelian $(v, k, \lambda; n)$ difference set in G, and let w be a divisor of v. If p is prime, $p|n$ and $p^j \equiv -1 \pmod{w}$, then an integer i exists such that $p^{2i}|n$, but p^{2i+1} is not a divisor of n. If w is the exponent v^* of G, then p does not divide n.

14.6.63 Example [260, 1830] There is no $(40, 13, 4; 9)$-difference set in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ (use $v^* = 10$ and $p = 3$ in Theorem 14.6.62). Using a different (though similar) theorem, one can also rule out the existence of a $(40, 13, 4; 9)$-difference set in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Note that a cyclic difference set with these parameters exists (Construction 14.6.25).

14.6.7 Multipliers

14.6.64 Definition Let D be a difference set in G. Then $\varphi \in \mathrm{Aut}(G)$ is a *multiplier* of D if $D^\varphi := \{\varphi(D) : d \in D\} = g + D$ for some $g \in G$. If G is abelian and φ is the automorphism that maps h to $t \cdot h$, then t is a *numerical* multiplier.

14.6.65 Theorem If φ is a multiplier of the difference set D, then there is at least one translate $g + D$ of D which is fixed by φ. If D is abelian and $\gcd(v, k) = 1$, then there is a translate fixed by all multipliers [259].

14.6.66 Remark

1. Multipliers play an important role, in particular in the theory of abelian difference sets.

2. The content of a multiplier theorem is the assertion that certain automorphisms (integers) have to be (numerical) multipliers of an abelian difference set depending only on the parameters v, k and λ. Theorem 14.6.67 is the *first multiplier theorem* [259].

14.6.67 Theorem Let D be an abelian $(v, k, \lambda; n)$-difference set. If p is a prime which satisfies $\gcd(p, v) = 1$, $p|n$ and $p > \lambda$, then p is a numerical multiplier.

14.6.68 Conjecture Every prime divisor p of n which is relatively prime to v is a multiplier of a $(v, k, \lambda; n)$-difference set, i.e. the condition $p > \lambda$ in Theorem 14.6.67 is not necessary.

14.6.69 Remark

1. Multipliers are quite useful in constructing difference sets and in proofs of nonexistence.
2. Several attempts have been made to weaken the assumption "$p > \lambda$" in Theorem 14.6.67 (second multiplier theorem, McFarland's multiplier theorem) [259].

14.6.70 Example Multipliers may be used to construct non-abelian difference sets: The set $D = \{3, 6, 7, 12, 14\}$ is a $(21, 5, 1; 4)$-difference set in $(\mathbb{Z}/21\mathbb{Z}, +)$ with multiplier 4. Denote the automorphism $x \mapsto x + 3$ by a, and the automorphism $x \mapsto 4x + 1$ by b. Then $G = \langle a, b \colon a^7 = b^3 = 1, b^{-1}ab = a^4 \rangle$ acts regularly on the points of $dev(D)$. A difference set D' in G corresponding to this action is $D' = \{a, a^2, a^4, a^4b, a^5b\}$.

See Also

§9.2	Relative difference sets are a generalization of difference sets. An important class of relative difference sets can be described by planar functions (PN functions).
§9.3	Bent functions are equivalent to elementary abelian Hadamard difference sets.
§10.3	Cyclic difference sets are binary sequences with two-level autocorrelation function.
§14.5	Difference sets are an important tool to construct combinatorial designs.

References Cited: [116, 209, 259, 260, 426, 604, 625, 700, 775, 776, 856, 858, 865, 868, 899, 1295, 1314, 1316, 1467, 1664, 1790, 1830, 1895, 1897, 1898, 2038, 2154, 2196, 2529, 2549, 2657, 2708, 2812]

14.7 Other combinatorial structures

Jeffrey H. Dinitz, *University of Vermont*
Charles J. Colbourn, *Arizona State University*

14.7.1 Association schemes

14.7.1 Definition Let d denote a positive integer, and let X be a nonempty finite set. A *d-class symmetric association scheme* on X is a sequence $R_0, R_1, \ldots, R_d$ of nonempty subsets of the Cartesian product $X \times X$, satisfying

1. $R_0 = \{(x, x) \mid x \in X\}$,
2. $X \times X = R_0 \cup R_1 \cup \cdots \cup R_d$ and $R_i \cap R_j = \emptyset$ for $i \neq j$,
3. for all $i \in \{0, 1, \ldots, d\}$, $R_i^T = R_i$ where $R_i^T := \{(y, x) \mid (x, y) \in R_i\}$,
4. for all integers $h, i, j \in \{0, 1, \ldots, d\}$, and for all $x, y \in X$ such that $(x, y) \in R_h$, the number $p_{ij}^h := |\{z \in X \mid (x, z) \in R_i,\ (z, y) \in R_j\}|$ depends only on h, i, j, and not on x or y.

14.7.2 Example The *Hamming scheme* $H(n, q)$ has the set F^n of all words of length n over an alphabet F of q symbols as its vertex set. Two words are *i-th* associates if and only if the Hamming distance between them is i. Generally the alphabet F is $\mathbb{F}_2$, but other finite fields are also used.

14.7.3 Example The *cyclotomic schemes* are obtained as follows. Let q be a prime power and k a divisor of $q-1$. Let C_1 be the subgroup of the multiplicative subgroup of $\mathbb{F}_q$ of index k, and let $C_i, i = 1, 2, \ldots, k$ be the cosets of C_1 (the *cyclotomic classes*). The points of the scheme are the elements of $\mathbb{F}_q$, and two points x, y are *i-th* associates if $x - y \in C_i$ (zero associates if $x - y = 0$). In order for this to be an association scheme one must have $-1 \in C_1$ or equivalently $2k$ must divide $q - 1$ if q is odd.

14.7.2 Costas arrays

14.7.4 Definition A *Costas array* of *order* n is an $n \times n$ array of dots and blanks that satisfies:

1. There are n dots and $n(n-1)$ blanks, with exactly one dot in each row and column.
2. All the segments between pairs of dots differ in length or in slope.

$C(n)$ denotes the number of distinct $n \times n$ Costas arrays.

14.7.5 Construction (Welch construction) Let p be prime and α be a primitive element in the field $\mathbb{F}_p$. Let $n = p - 1$. A Costas array of order n is obtained by placing a dot at (i, j) if and only if $i = \alpha^j$, for $a \leq j < n + a$, a a nonnegative integer, and $i = 1, \ldots, n$.

14.7.6 Construction [1293] Let α and β be primitive elements in the field $\mathbb{F}_q$ for q a prime power. Let $n = q - 2$. Costas arrays of order n are obtained by

1. *Lempel construction:* Put a dot at (i, j) if and only if $\alpha^i + \alpha^j = 1$, $1 \leq i, j \leq n$.
2. *Golomb construction:* Put a dot at (i, j) if and only if $\alpha^i + \beta^j = 1$, $1 \leq i, j \leq n$.

14.7.7 Remark Using Constructions 14.7.5 and 14.7.6, $C(p-1) > 1$ and $C(q-2) > 1$. Also, if a corner dot is present in a Costas array of order n, it can be removed along with its row and column to obtain a Costas array of order $n - 1$.

14.7.8 Theorem [1296] If $q > 2$ is a prime power, then there exist primitive elements α and β in $\mathbb{F}_q$ such that $\alpha + \beta = 1$.

14.7.9 Corollary Removing the corner dot at $(1, 1)$ in the Costas array of order $q - 2$ from Construction 14.7.6 Part 2 yields $C(q - 3) \geq 1$.

14.7.10 Example If there exist primitive elements α and β satisfying the conditions stated, then a Costas array of order n can be obtained by removing one or more corner dots.

Conditions	n
$\alpha^1 = 2$	$q-3$
$\alpha^1 + \beta^1 = 1$ and $\alpha^2 + \beta^2 = 1$	$q-4$
$\alpha^2 + \alpha^1 = 1$	$q-4$
$\alpha^1 + \beta^1 = 1$ and $\alpha^2 + \beta^{-1} = 1$	$q-4$
and necessarily $\alpha^{-1} + \beta^2 = 1$	$q-5$

14.7.11 Remark All Costas arrays of order 28 are accounted for by the Golomb and Welch construction methods [912], making 28 the first order (larger than 5) for which no sporadic Costas array exists.

14.7.12 Remark For $n \geq 30$, $n \notin \{31, 53\}$, the only orders for which Costas arrays are known are orders $n = p - 1$ or $n = q - 2$ or orders for which some algebraic condition exists that guarantees corner dots whose removal leaves a smaller Costas array.

14.7.13 Remark The properties of a Costas array make it an ideal discrete waveform for Doppler sonar. Having one dot in each row and column minimizes reverberation. Distinct segments between pairs of dots give it a thumbtack ambiguity function because, shifted left-right in time and up-down in frequency, copies of the pattern can only agree with the original in one dot, no dots, or all n dots at once. Thus, the spike of the thumbtack makes a sharp distinction between the actual shift and all the near misses. See [910] for a survey on Costas arrays and `http://www.costasarrays.org/` for up-to-date information on Costas arrays.

14.7.3 Conference matrices

14.7.14 Definition A *conference matrix* of order n is an $n \times n$ $(0, \pm 1)$-matrix C with zero diagonal satisfying $CC^T = (n-1)I$. A conference matrix is *normalized* if all entries in its first row and first column are 1 (except the (1,1) entry which is 0). A square matrix A is *symmetric* if $A = A^T$ and *skew-symmetric* if $A = -A^T$. The *core* of a normalized conference matrix C consists of all the rows and columns of C except the first row and column.

14.7.15 Theorem [2833, page 360] If there exists a conference matrix of order n, then n is even; furthermore, if $n \equiv 2 \pmod 4$, then, for any prime $p \equiv 3 \pmod 4$, the highest power of p dividing $n-1$ is even.

14.7.16 Theorem [2330] Let q be an odd prime power.

1. If $q \equiv 1 \pmod 4$, then there is a symmetric conference matrix of order $q+1$.
2. If $q \equiv 3 \pmod 4$, then there is a skew-symmetric conference matrix of order $q+1$.

14.7.17 Construction In the construction for Theorem 14.7.16, let q be an odd prime power and let χ denote the quadratic character on the finite field $\mathbb{F}_q$ (i.e. $\chi(x) = 0$ if $x = 0$, $\chi(x) = 1$ if x is a square and $\chi(x) = -1$ if x is a nonsquare). Number the elements of $\mathbb{F}_q : 0 = a_0, a_1, \ldots, a_{q-1}$ and define a $q \times q$ matrix Q by $q_{i,j} := \chi(a_i - a_j)$ for $0 \leq i, j < q-1$. It follows that Q is symmetric if $q \equiv 1 \pmod 4$ and skew-symmetric if $q \equiv 3 \pmod 4$. Define the $(q+1) \times (q+1)$ matrix C by

$$\begin{pmatrix} 0 & 1 & 1 & \cdots & 1 \\ \pm 1 & & & & \\ \vdots & & & Q & \\ \pm 1 & & & & \end{pmatrix}$$

where the terms ± 1 are $+1$ when $q \equiv 1 \pmod 4$ and -1 when $q \equiv 3 \pmod 4$. It follows that C is a conference matrix of order $q+1$. In the special case when q is prime, Q is circulant.

14.7.18 Lemma 1. If C is an skew-symmetric conference matrix, then $I + C$ is a Hadamard matrix. 2. If C is a symmetric conference matrix of order n, then

$$\begin{pmatrix} I+C & -I+C \\ -I+C & -I-C \end{pmatrix}$$

is a Hadamard matrix of order $2n$.

14.7.19 Remark Theorem 14.7.20 follows from Theorem 14.7.16 and Lemma 14.7.18.

14.7.20 Theorem If q is a power of an odd prime, then a Hadamard matrix of order $q+1$ exists if $q \equiv 3 \pmod 4$, and a Hadamard matrix of order $2(q+1)$ exists if $q \equiv 1 \pmod 4$.

14.7.21 Construction Let A be a $(0, \pm 1)$-matrix of order n and B a ± 1-matrix of order n such that $AB = BA$ and $AA^T + BB^T = (2n-1)I$. Then the matrix $C = \begin{pmatrix} A & B \\ B^T & -A^T \end{pmatrix}$ is a conference matrix of order $2n$.

14.7.22 Definition When A and B are circulant matrices, the conference matrix C in Construction 14.7.21 is *constructible from two circulant matrices* or for short, *two circulants type.*

14.7.23 Theorem [1281, 2813, 2956] If $q \equiv 1 \pmod 4$ is a prime power, then there is a symmetric conference matrix C of order $q+1$ of two circulants type.

14.7.24 Theorem [2010] There is a symmetric conference matrix of order $q^2(q+2)+1$ whenever q is a prime power, $q \equiv 3 \pmod 4$, and $q+3$ is the order of a conference matrix.

14.7.4 Covering arrays

14.7.25 Definition A *covering array* $\mathrm{CA}_\lambda(N; t, k, v)$ is an $N \times k$ array containing v different symbols. In every $N \times t$ subarray, each t-tuple occurs at least λ times. Then t is the *strength* of the coverage of interactions, k is the number of components (*degree*), λ is the *index*, and v is the number of symbols for each component (*order*). Only the case when $\lambda = 1$ is treated; the subscript is then omitted in the notation.

14.7.26 Definition The size of a covering array is the *covering array number* $\mathrm{CAN}(t, k, v)$. The covering array is *optimal* if it has the minimum possible number of rows.

14.7.27 Construction [1447] Let q be a prime power and $q \geq s \geq 2$. Over the finite field $\mathbb{F}_q$, let $\mathcal{F} = \{f_1, \ldots, f_{q^s}\}$ be the set of all polynomials of degree less than s. Let $\mathcal{A}$ be a subset of $\mathbb{F}_q \cup \{\infty\}$. Define an $q^s \times |\mathcal{A}|$ array in which the entry in cell (j, a) is $f_j(a)$ when $a \in \mathbb{F}_q$, and is the coefficient of the term of degree $s-1$ when $a = \infty$. The result is a $\mathrm{CA}(q^s; s, |\mathcal{A}|, q)$. Because every t-tuple is covered exactly once, it is in fact an *orthogonal array* of index one and strength s.

14.7.28 Remark Covering arrays are typically constructed by a combination of computational, direct, and recursive constructions [699]. Finite fields arise most frequently in the direct construction of covering arrays. One example is the use of *permutation vectors* to construct covering arrays [2594]. A second, outlined next, uses Weil's theorem and character theoretic arguments to establish that certain cyclotomic matrices form covering arrays.

14.7.29 Construction [698] Let ω be a primitive element of $\mathbb{F}_q$, with $q \equiv 1 \pmod{v}$. For each q and ω, form a *cyclotomic vector* $\mathbf{x}_{q,v,\omega} = (x_i : i \in \mathbb{F}_q) \in \mathbb{F}_q^q$ by setting $x_0 = 0$ and $x_i \equiv j \pmod{v}$ when $i = \omega^j$ for $i \in \mathbb{F}_q^\star$. Choosing a different primitive element of $\mathbb{F}_q$ can lead to the same vector $\mathbf{x}_{q,v,\omega}$, or, for some number m that is coprime to v, to a vector in which each element is multiplied by m and reduced modulo v. For our purposes, the vectors produced are equivalent, so henceforth let $\mathbf{x}_{q,v}$ denote any vector so obtained. From $\mathbf{x}_{q,v} = (x_i : i \in \mathbb{F}_q)$, form a $q \times q$ matrix $A_{q,v} = (a_{ij})$ with rows and columns indexed by $\mathbb{F}_q$, by setting $a_{ij} = x_{j-i}$ (computing the subscript in $\mathbb{F}_q$).

14.7.30 Theorem [698] When $q > t^2v^{2t}$, $A_{q,v}$ from Construction 14.7.29 is a covering array of strength t.

14.7.5 Hall triple systems

14.7.31 Definition [1394] A *Hall triple system* (HTS) is a pair $(S, \mathcal{L})$ where S is a set of elements (*points*) and $\mathcal{L}$ a set of *lines* satisfying:

1. every line is a 3-subset of S,
2. any two distinct points lie in exactly one line, and
3. for any two intersecting lines, the smallest subsystem containing them is isomorphic to the affine plane of nine points, AG(2,3).

14.7.32 Example Let S be some $(n+1)$-dimensional vector space over $\mathbb{F}_3$, with $n \geq 3$. Let $\{e_0, e_1, \ldots, e_n\}$ be a basis for S. For any two points $x = \sum \alpha_i e_i$ and $y = \sum \beta_i e_i$ set $z = x \circ y$ when $x + y + z = (\alpha_1 - \beta_1)(\alpha_2\beta_3 - \alpha_3\beta_2)e_0$. This defines a binary operation on S. One either has $x = y = z$, or the three points x, y, z are pairwise distinct. The 3-subsets of the form $\{x, y, z\}$ such that $z = x \circ y$ provide S with a structure of an HTS. This HTS is referred to as $H(n)$.

14.7.33 Example Any affine space $\mathrm{AG}(n, 3)$ over $\mathbb{F}_3$ with the usual lines may be viewed as an HTS. Such an HTS is an *affine* HTS.

14.7.34 Theorem [1393, 3018] The cardinality of any HTS is 3^m for some integer $m \geq 2$. Nonaffine HTS of order 3^m exist for any $m \geq 4$ and do not exist for $m \in \{2, 3\}$.

14.7.35 Remark When $m > 3$, the existence of a nonaffine HTS of order 3^m is provided by $H(m-1)$ in Example 14.7.32. For the orders 3^4 and 3^5, there is a unique nonaffine HTS, namely, $H(3)$ and $H(4)$, respectively.

14.7.6 Ordered designs and perpendicular arrays

14.7.36 Definition An *ordered design* $\mathrm{OD}_\lambda(t, k, v)$ is a $k \times \lambda \cdot \binom{v}{t} \cdot t!$ array with v entries such that

1. each column has k distinct entries, and
2. each tuple of t rows contains each column tuple of t distinct entries precisely λ times.

14.7.37 Definition A *perpendicular array* $\mathrm{PA}_\lambda(t,k,v)$ is a $k \times \lambda \cdot \binom{v}{t}$ array with v entries such that

1. each column has k distinct entries, and
2. each set of t rows contains each set of t distinct entries as a column precisely λ times.

14.7.38 Definition For $0 \le s \le t$, a $\mathrm{PA}_\lambda(t,k,v)$ is an s-$\mathrm{PA}_\lambda(t,k,v)$ if, for each $w \le t$ and $u \le \min(s,w)$, the following holds. Let E_1, E_2 be disjoint sets of entries, $E_1 \cap E_2 = \emptyset$ with $|E_1| = u$ and $|E_2| = w-u$. Then the number of columns containing $E_1 \cup E_2$ and having E_2 in a given set U of $w-u$ rows is a constant, independent of the choice of E_1, E_2, and U. *Authentication perpendicular arrays* (APA) are 1-PA.

14.7.39 Definition A set $S \subseteq S_n$ of permutations is (uniformly) *t-homogeneous* if it is an $\mathrm{APA}_\lambda(t,n,n)$; it is *$t$-transitive* if it is an $\mathrm{OD}_\lambda(t,n,n)$.

14.7.40 Theorem [273] Permutation *groups* yield special cases of t-transitive or t-homogeneous sets.

1. The groups $\mathrm{PGL}_2(q), q$ a prime power, form $\mathrm{OD}_1(3, q+1, q+1)$; the groups $\mathrm{PSL}_2(q), q \equiv 3 \pmod 4$ are $\mathrm{APA}_3(3, q+1, q+1)$. The special cases of this last family when the prime power $q \equiv 3, 11 \pmod{12}$ form the only known infinite family of $\mathrm{APA}_\lambda(t,n,n)$ with $t > 2$ and minimal λ.
2. The groups $\mathrm{AGL}_1(q), (q$ a prime power), of order $q \cdot (q-1)$ form an $\mathrm{OD}_1(2,q,q)$; the groups $\mathrm{ASL}_1(q), (q$ a prime power $\equiv 3 \pmod 4)$ of order $q \cdot (q-1)/2$ form $\mathrm{APA}_1(2,q,q)$.

14.7.41 Definition Let $q \equiv 3 \pmod 4$ be a prime power, k odd. An $\mathrm{APAV}(q,k)$ (V stands for *vector*) is a tuple $(x_1, \ldots, x_k)$ where $x_i \in \mathbb{F}_q$ and such that for each i the $x_i - x_j, j \ne i$ are evenly distributed on squares and nonsquares [1254].

14.7.42 Remark An $\mathrm{APAV}(q,k)$ implies the existence of $\mathrm{APA}_1(2,k,q)$. In [601] a theorem on character sums based on the Hasse–Weil inequality is used to prove existence of an $\mathrm{APAV}(q,k)$ when q is large enough with respect to k.

14.7.43 Theorem [601] The following exist, for a prime power q with $q \equiv 3 \pmod 4$,

1. $\mathrm{APAV}(q,7)$ for $q \ge 7, q \notin \{11, 19\}$,
2. $\mathrm{APAV}(q,9)$ for $q \ge 19$,
3. $\mathrm{APAV}(q,11)$ for $q \ge 11, q \notin \{19, 27\}$,
4. $\mathrm{APAV}(q,13)$ for $q \ge 13, q \notin \{19, 23, 31\}$, and
5. $\mathrm{APAV}(q,15)$ for $q \ge 31$.

14.7.7 Perfect hash families

14.7.44 Definition Let n, q, t, and s be positive integers and suppose (to avoid trivialities) that $n > q \ge t \ge 2$. Let V be a set of cardinality n and let W be a set of cardinality q. A function $f : V \to W$ *separates* a subset X of V if f is an injection when restricted to X. An (n,q,t)-*perfect hash family* of *size* s is a collection $\mathcal{F} = \{f_1, f_2, \ldots, f_s\}$ of functions

from V to W with property that for all sets $X \subseteq V$ such that $|X| = t$, at least one of the functions $f_1, f_2, \ldots, f_s$ separates X. The notation PHF$(s; n, q, t)$ is used for an (n, q, t)-perfect hash family of size s. A perfect hash family is *optimal* if s is as small as possible, given n, q, t.

14.7.45 Theorem A PHF$(s; n, q, t)$ is equivalent to an $s \times n$ array A of elements from a q-set F, such that, for any t columns of A, there exists a row of A, say r, such that the entries in the t given columns of row r of A are distinct.

14.7.46 Theorem [2704] Suppose that there exists a q-ary code $\mathcal{C}$ of length K, with N codewords, having minimum distance D. Then there exists a PHF$(N; K, q, t)$, where $(N - D)\binom{t}{2} < N$.

14.7.47 Corollary [2704] Suppose N and v are given, with v a prime power and $N \leq v + 1$. Then there exists a PHF$(N; v^{\lceil N/\binom{t}{2} \rceil}, v, t)$ based on a Reed–Solomon code.

14.7.48 Theorem [2835] A PHF$((i+1)^2; v^{i+1}, v, 3)$ exists whenever v is a prime power, $v \geq 3$, and $i \geq 1$. A PHF$(\frac{5}{6}(2i^3 + 3i^2 + i) + i + 1; v^{i+1}, v, 4)$ exists whenever v is a prime power, $v \geq 4$, and $i \geq 1$.

14.7.49 Theorem [2704] For any prime power q and for any positive integers n, m, i such that $n \geq m$ and $2 \leq i \leq q^n$, there exists a PHF$(q^n; q^{m+(i-1)n}, q^m, t)$ when $\binom{t}{2} < \frac{q^m}{i-1}$.

14.7.50 Definition A PHF$(N; q^s, q, t)$ is *linear* if it is an $N \times q^s$ array with rows indexed by elements of $\mathbb{F}_q \cup \{\infty\}$ and columns indexed by the polynomials of degree less than s over $\mathbb{F}_q$; each entry of the array is the evaluation of the polynomial corresponding to the column on the row index, when that index is in $\mathbb{F}_q$; otherwise it is the coefficient of the term of degree $s - 1$ in the polynomial.

14.7.51 Remark In a linear PHF, columns correspond to polynomials of degree less than s over $\mathbb{F}_q$. It follows directly that two columns agree in at most $s - 1$ entries, and hence that if the linear PHF has more than $(s-1)\binom{t}{2}$ rows, it has strength at least t. By judicious selection of the particular rows (i.e., a subset $\mathcal{A}$ of $\mathbb{F}_q \cup \{\infty\}$), fewer rows can often be employed. The key observation, developed in [205, 300, 701], is that when $\mathcal{A}$ is chosen properly, a system of equations over $\mathbb{F}_q$ for each set of t chosen columns never admits a solution. This is developed in an algebraic setting in [300], in a geometric setting in [205], and in a graph-theoretic setting in [701]. The results to follow all employ this basic strategy.

14.7.52 Theorem [300] Let $s \geq 2$ and $t \geq 2$. When q is a sufficiently large prime power, there is an optimal linear PHF$(s(t-1); q^s, q, t)$.

14.7.53 Theorem [205, 206, 300]

1. An optimal linear PHF$(6; q^2, q, 4)$ exists if and only if $q \geq 11$ is a prime power and $q \neq 13$.
2. An optimal linear PHF$(6; q^3, q, 3)$ exists if and only if $q \geq 11$ is a prime power.

14.7.54 Theorem [701] Let p be a prime.

1. A PHF$(9; p^4, p, 3)$ exists when $p \geq 17$.
2. A PHF$(8; p^4, p, 3)$ exists when $p \geq 19$.
3. A PHF$(12; p^3, p, 4)$ exists when $p \geq 17$.
4. A PHF$(11; p^3, p, 4)$ exists when $p \geq 29$.
5. A PHF$(10; p^3, p, 4)$ exists when $p \geq 251$ and $p \notin \{257, 263\}$.

6. A PHF$(10; p^2, p, 5)$ exists when $p \geq 19$.
7. A PHF$(9; p^2, p, 5)$ exists when $p \geq 41$.
8. A PHF$(8; p^2, p, 5)$ exists when $p \geq 241$ and $p \notin \{251, 257\}$.
9. A PHF$(15; p^2, p, 6)$ exists when $p \geq 29$.
10. A PHF$(14; p^2, p, 6)$ exists when $p \geq 41$.
11. A PHF$(13; p^2, p, 6)$ exists when $p \geq 73$.

14.7.8 Room squares and starters

14.7.55 Definition A *starter* in the odd order abelian group G (written additively), where $|G| = g$ is a set of unordered pairs $S = \{\{s_i, t_i\} : 1 \leq i \leq (g-1)/2\}$ that satisfies:

1. $\{s_i : 1 \leq i \leq (g-1)/2\} \cup \{t_i : 1 \leq i \leq (g-1)/2\} = G \backslash \{0\}$, and
2. $\{\pm(s_i - t_i) : 1 \leq i \leq (g-1)/2\} = G \backslash \{0\}$.

14.7.56 Definition A *strong starter* is a starter $S = \{\{s_i, t_i\}\}$ in the abelian group G with the additional property that $s_i + t_i = s_j + t_j$ implies $i = j$, and for any i, $s_i + t_i \neq 0$.

14.7.57 Definition A *skew starter* is a starter $S = \{\{s_i, t_i\}\}$ in the abelian group G with the additional property that $s_i + t_i = \pm(s_j + t_j)$ implies $i = j$, and for any i, $s_i + t_i \neq 0$.

14.7.58 Example A strong starter in $\mathbb{Z}_{17}$ is

$$\{9, 10\}, \{3, 5\}, \{13, 16\}, \{11, 15\}, \{1, 6\}, \{2, 8\}, \{7, 14\}, \{4, 12\}$$

14.7.59 Definition Let $S = \{\{s_i, t_i\} : 1 \leq i \leq (g-1)/2\}$ and $T = \{\{u_i, v_i\} : 1 \leq i \leq (g-1)/2\}$ be two starters in G. Without loss of generality, assume that $s_i - t_i = u_i - v_i$, for all i. Then S and T are *orthogonal* starters if $u_i - s_i = u_j - s_j$ implies $i = j$, and if $u_i \neq s_i$ for all i.

14.7.60 Definition Let q be a prime power that can be written in the form $q = 2^k t + 1$, where $t > 1$ is odd and let ω be a primitive element in the field $\mathbb{F}_q$. Then define

1. C_0 to be the multiplicative subgroup of $\mathbb{F}_q \backslash \{0\}$ of order t,
2. $C_i = \omega^i C_0$, $0 \leq i \leq 2^k - 1$ to be the cosets of C_0 (*cyclotomic classes*), and
3. $\Delta = 2^{k-1}$, $H = \cup_{i=0}^{\Delta - 1} C_i$ and $C_i^a = (1/(a-1))C_i$.

14.7.61 Theorem [2184] Let $T = \{\{x, \omega^\Delta x\} : x \in H\}$. Then T is a skew starter (the *Mullin–Nemeth starter*) in the additive subgroup of $\mathbb{F}_q$.

14.7.62 Theorem [891] For each $a \in C_\Delta$, let $S_a = \{\{x, ax\} : x \in \cup_{i=0}^{\Delta-1} C_i^a\}$. Then for any $a \in C_\Delta$, S_a is a strong starter in the additive group of $\mathbb{F}_q$. Further, S_a and S_b are orthogonal if $a, b \in C_\Delta$ with $a \neq b$. Hence, the set $\{S_a | a \in C_\Delta\}$ is a set of t pairwise orthogonal starters of order q.

14.7.63 Theorem [617] Let $p = 2^{2^n}$ be a Fermat prime with $n \geq 2$. There exists a strong starter in the additive group of $\mathbb{F}_p$.

14.7.64 Remark [1526] No strong starter in the additive groups of $\mathbb{F}_3$, $\mathbb{F}_5$, or $\mathbb{F}_9$ exists.

14.7.65 Definition Let G be an additive abelian group of order g, and let H be a subgroup of order h of G, where $g-h$ is even. A *Room frame starter* in $G\backslash H$ is a set of unordered pairs $S = \{\{s_i, t_i\} : 1 \le i \le (g-h)/2\}$ such that

1. $\{s_i : 1 \le i \le (g-h)/2\} \cup \{t_i : 1 \le i \le (g-h)/2\} = G\backslash H$, and
2. $\{\pm(s_i - t_i) : 1 \le i \le (g-h)/2\} = G\backslash H$.

14.7.66 Remark A starter is the special case of a frame starter when $H = \{0\}$. The concepts of strong, skew, and orthogonal for Room frame starters are as for starters replacing $\{0\}$ by H and $(g-1)/2$ by $(g-h)/2$.

14.7.67 Theorem [892] Let $q \equiv 1 \pmod 4$ be a prime power such that $q = 2^k t + 1$, where $t > 1$ is odd. Then there exist t orthogonal Room frame starters in $(\mathbb{F}_q \times (\mathbb{Z}_2)^n)\backslash(\{0\} \times (\mathbb{Z}_2)^n)$ for all $n \ge 1$.

14.7.68 Theorem [93] If $p \equiv 1 \pmod 6$ is a prime and $p \ge 19$, then there exist three orthogonal frame starters in $(\mathbb{F}_p \times (\mathbb{Z}_3))\backslash(\{0\} \times (\mathbb{Z}_3))$

14.7.69 Definition Let S be a set of $n+1$ elements (*symbols*). A *Room square* of side n (on symbol set S), RS(n), is an $n \times n$ array, F, that satisfies the following properties:

1. every cell of F either is empty or contains an unordered pair of symbols from S,
2. each symbol of S occurs once in each row and column of F,
3. every unordered pair of symbols occurs in precisely one cell of F.

14.7.70 Definition A Room square of side n is *standardized* (with respect to the symbol ∞) if the cell (i,i) contains the pair $\{\infty, i\}$.

14.7.71 Definition A standardized Room square of side n is *skew* if for every pair of cells (i,j) and (j,i) (with $i \ne j$) exactly one is filled.

14.7.72 Definition A standardized Room square of side n is *cyclic* if $S = \mathbb{Z}_n \cup \{\infty\}$ and if whenever $\{a,b\}$ occurs in the cell (i,j), then $\{a+1, b+1\}$ occurs in cell $(i+1, j+1)$ where all arithmetic is performed in $\mathbb{Z}_n$ (and $\infty + 1 = \infty$).

14.7.73 Example Below are skew Room squares of sides 7 and 9; the Room square of side 7 is cyclic.

∞0			15		46	23
34	∞1			26		50
61	45	∞2			30	
	02	56	∞3			41
52		13	60	∞4		
	63		24	01	∞5	
		04		35	12	∞6

∞1		49	37	28		56		
89	∞2				57	34		16
	58	∞3		69	24		17	
	36	78	∞4		19		25	
	79		12	∞5	38		46	
45					∞6	18	39	27
		26	59	13		∞7		48
67	14					29	∞8	35
23		15	68	47				∞9

14.7.74 Theorem [893] The existence of d pairwise orthogonal starters in an abelian group of order n implies the existence of a Room d-cube of side n.

14.7.75 Remark Construction 14.7.77 is used to establish Theorem 14.7.74 when $d = 2$. It is easily extended when $d > 2$.

14.7.76 Definition An *adder* for the starter $S = \{\{s_i, t_i\} : 1 \le i \le (g-1)/2\}$ is an ordered set $A_S = \{a_1, a_2, \ldots, a_{(g-1)/2}\}$ of $(g-1)/2$ distinct nonzero elements from G such that the set $T = \{\{s_i + a_i, t_i + a_i\} : 1 \le i \le (g-1)/2\}$ is also a starter in the group G.

14.7.77 Construction Let $S = \{\{s_i, t_i\} : 1 \le i \le (n-1)/2\}$ and $T = \{\{u_i, v_i\} : 1 \le i \le (n-1)/2\}$ be two orthogonal starters in G (usually $\mathbb{Z}_n$), (n odd) with $A_S = \{a_i : 1 \le i \le (n-1)/2\}$ the associated adder. Let R be an $n \times n$ array indexed by the elements of G. Each $\{s_i, t_i\} \in S$ is placed in the first row in cell $R(0, -a_i)$. This is cycled so that the pair $\{s_i + x, t_i + x\}$ is in the cell $R(x, -a_i + x)$, where all arithmetic is performed in G. Finally, for each $x \in G$, place the pair $\{\infty, x\}$ in cell $R(x, x)$. Then R is a Room square of side n.

14.7.78 Remark Construction 14.7.77 in conjunction with Theorem 14.7.61 yields skew Room squares of prime power orders $q \equiv 3 \pmod 4$. This is useful in proving Theorem 14.7.79.

14.7.79 Theorem [893] A (skew) Room square of side n exists if and only if n is odd and $n \notin \{3, 5\}$.

14.7.80 Theorem [1920] A cyclic skew Room square of side n exists if $n = \prod {p_i}^{\alpha_i}$ where each p_i is a non-Fermat prime or if $n = pq$ with p, q distinct Fermat primes.

14.7.81 Definition If $\{S_1, \ldots, S_n\}$ is a partition of a set S, an $\{S_1, \ldots, S_n\}$-*Room frame* is an $|S| \times |S|$ array, F, indexed by S, satisfying:

1. every cell of F either is empty or contains an unordered pair of symbols of S,
2. the subarrays $S_i \times S_i$ are empty, for $1 \le i \le n$ (these subarrays are *holes*),
3. each symbol $x \notin S_i$ occurs once in row (or column) s for any $s \in S_i$, and
4. the pairs occurring in F are those $\{s, t\}$, where $(s, t) \in (S \times S) \backslash \bigcup_{i=1}^{n} (S_i \times S_i)$.

The *type* of a Room frame F is the multiset $\{|S_i| : 1 \le i \le n\}$. An "exponential" notation is used to describe types; a Room frame has type ${t_1}^{u_1} {t_2}^{u_2} \cdots {t_k}^{u_k}$ if there are u_i S_js of cardinality t_i, $1 \le i \le k$.

14.7.82 Remark Theorem 14.7.83 gives the connection between frame starters and Room frames. The construction for a Room frame from a pair of orthogonal frame starters is a generalization of Construction 14.7.77.

14.7.83 Theorem [892] Suppose a pair of orthogonal frame starters in $G \backslash H$ exists, where $|G| = g$ and $|H| = h$. Then there exists a Room frame of type $h^{g/h}$.

14.7.84 Remark Theorems 14.7.67 and 14.7.68 in conjunction with Theorem 14.7.83 yield Corollary 14.7.85. Theorem 14.7.86 details the existence of Room frames of type t^u.

14.7.85 Corollary a) Let $q \equiv 1 \pmod 4$ be a prime power such that $q = 2^k t + 1$, where $t > 1$ is odd. Then there exist a Room frame of type $(2^n)^q$ for all $n \ge 1$. b) If $p \equiv 1 \pmod 6$ is a prime and $p \ge 19$, then there exist a Room frame of type 3^p.

14.7.86 Theorem (Existence theorems for uniform Room frames) [700, §VI.50] and [894]

1. There does not exist a Room frame of type t^u if any of the following conditions hold: (i) $u = 2$ or 3; (ii) $u = 4$ and $t = 2$; (iii) $u = 5$ and $t = 1$; (iv) $t(u-1)$ is odd.

2. Suppose t and u are positive integers, $u \geq 4$ and $(t,u) \neq (1,5),(2,4)$. Then there exists a uniform Room frame of type t^u if and only if $t(u-1)$ is even.

14.7.9 Strongly regular graphs

14.7.87 Definition A *strongly regular graph* with parameters (v,k,λ,μ) is a finite graph on v vertices, without loops or multiple edges, regular of degree k (with $0 < k < v-1$, so that there are both edges and nonedges), and such that any two distinct vertices have λ common neighbors when they are adjacent, and μ common neighbors when they are nonadjacent.

14.7.88 Remark There are many constructions for strongly regular graphs. Example 14.7.89 gives several that use finite fields. For a table of the existence of strongly regular graphs with $v \leq 280$ see [700, pp. 852–866]

14.7.89 Example [416]

1. *Paley(q):* For prime powers $q = 4t+1$, the graph with vertex set $\mathbb{F}_q$ where two vertices are adjacent when they differ by a square. This strongly regular graph has parameters $(q, \frac{1}{2}q-1, \frac{1}{4}(q-5), \frac{1}{4}(q-1))$.
2. *van Lint–Schrijver(u):* a graph constructed by the cyclotomic construction in [2832], by taking the union of u classes.
3. $A_{n-1,2}(q)$ or $\begin{bmatrix} n \\ 2 \end{bmatrix}_q$: the graph on the lines in $\mathrm{PG}(n-1,q)$, adjacent when they have a point in common.
4. $Bilin_{2\times d}(q)$: the graph on the $2 \times d$ matrices over $\mathbb{F}_q$, adjacent when their difference has rank 1.
5. $O^{\varepsilon}_{2d}(q)$: the graph on the isotropic points on a nondegenerate quadric in $\mathrm{PG}(2d-1,q)$, where two points are joined when the connecting line is totally singular.
6. $Sp_{2d}(q)$: the graph on the points of $\mathrm{PG}(2d-1,q)$ provided with a nondegenerate symplectic form, where two points are joined when the connecting line is totally isotropic.
7. $U_d(q)$: the graph on the isotropic points of $\mathrm{PG}(d-1,q^2)$ provided with a nondegenerate Hermitian form, where two points are joined when the connecting line is totally isotropic.
8. *Affine difference sets* [475]: Let V be an n-dimensional vector space over $\mathbb{F}_q$ and let X be a set of directions (a subset of the projective space PV). Two vectors are *adjacent* when the line joining them has a direction in X. Then $v = q^n$ and $k = (q-1)|X|$. This graph is strongly regular if and only if there are two integers w_1, w_2 such that all hyperplanes of PV miss either w_1 or w_2 points of X. If this is the case, then $r = k - qw_1$, $s = k - qw_2$ (assuming $w_1 < w_2$), and hence $\mu = k + (k-qw_1)(k-qw_2)$, $\lambda = k - 1 + (k - qw_1 + 1)(k - qw_2 + 1)$.

14.7.10 Whist tournaments

14.7.90 Definition A *whist tournament* $\mathrm{Wh}(4n)$ for $4n$ players is a schedule of games each involving two players opposing two others, such that

1. the games are arranged into $4n-1$ rounds, each of n games;

2. each player plays in exactly one game in each round;
3. each player partners every other player exactly once;
4. each player opposes every other player exactly twice.

14.7.91 Definition Each game is denoted by an ordered 4-tuple (a, b, c, d) in which the pairs $\{a, c\}$, $\{b, d\}$ are *partner pairs*; $\{a, c\}$ is a *partner pair of the first kind*, and $\{b, d\}$ is a *partner pair of the second kind*. The other pairs are *opponent pairs*; in particular $\{a, b\}$, $\{c, d\}$ are *opponent pairs of the first kind*, and $\{a, d\}$, $\{b, c\}$ are *opponent pairs of the second kind*.

14.7.92 Definition A *whist tournament* $\mathrm{Wh}(4n+1)$ for $4n+1$ players is defined as for $4n$, except that Conditions $1, 2$ are replaced by

$1'$. the games are arranged into $4n+1$ rounds each of n games;
$2'$. each player plays in one game in each of $4n$ rounds, but does not play in the remaining round.

14.7.93 Definition A $\mathrm{Wh}(4n)$ is $\mathbb{Z}$-cyclic if the players are $\infty, 0, 1, \ldots, 4n-2$ and each round is obtained from the previous one by adding 1 modulo $4n-1$ to each non-∞ entry. A $\mathrm{Wh}(4n+1)$ is $\mathbb{Z}$-cyclic if the players are $0, 1, \ldots, 4n$ and the rounds are similarly developed modulo $4n+1$.

14.7.94 Theorem [166] If $p = 4n+1$ is prime and w is a primitive root of p, then the games $(w^i, w^{i+n}, w^{i+2n}, w^{i+3n})$, $0 \le i \le n-1$, form the initial round of $\mathbb{Z}$-cyclic $\mathrm{Wh}(4n+1)$.

14.7.95 Theorem Let P denote any product of primes p with each $p \equiv 1 \pmod 4$, and let q, r denote primes with both $q, r \equiv 3 \pmod 4$.
A $\mathbb{Z}$-cyclic $\mathrm{Wh}(4n)$ is known to exist when:

1. $4n \le 132$ (see [7, 98]);
2. $4n = 2^\alpha (\alpha \ge 2)$ (see [100]);
3. $4n = qP + 1$, $q \in \{3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107, 127\}$ (see [7]);
4. $4n = 3P + 1$ (see [100]);
5. $4n = 3^{2m+1} + 1$, $m \ge 0$ (see [101]);
6. $4n = qr^2P + 1$, q and r distinct, $q < 60$, $r < 100$ (see [7]).

A $\mathbb{Z}$-cyclic $\mathrm{Wh}(4n+1)$ is known to exist when:

1. $4n+1 = P$ or r^2P and $r \le 100$ (see [7, 102]);
2. $4n+1 \le 149$ (see [7]);
3. $4n+1 = 3^{2m}$ or $3^{2m}P$ (see [101]);
4. $4n+1 = 3sP$, $s \in \{7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47\}$ (see [7]).

14.7.96 Definition A *triplewhist tournament* $\mathrm{TWh}(v)$ is a $\mathrm{Wh}(v)$ with Condition 4 replaced by $(4'')$ each player has every other player once as an opponent of the first kind and once as an opponent of the second kind.

14.7.97 Theorem A TWh$(4n+1)$ exists for all $n \geq 5$, and possibly for $n = 4$. A TWh$(4n)$ exists for all $n \geq 1$ except for $n = 3$; see [7, 1952].

14.7.98 Theorem A $\mathbb{Z}$-cyclic TWh$(4n+1)$ exists when:

1. $4n+1$ is a prime $p \equiv 1 \pmod 4$, $p \geq 29$ (see [458]);
2. $4n+1 = q^2$ where q is prime, $q \equiv 3 \pmod 4$, $7 \leq q \leq 83$ (see [6]);
3. $4n+1 = 5^n$ or 13^n $(n \geq 2)$ (see [6]);
4. $4n+1$ is the product of any values in the above three items (see [102]).

14.7.99 Theorem A $\mathbb{Z}$-cyclic TWh$(4n)$ exists when:

1. $4n = qP + 1$, where P denotes any product of primes p with each $p \equiv 1 \pmod 4$ and $q \in \{3, 7, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107, 127, 131\}$ (see [7]);
2. $4n = 2^n$ $(n \geq 2)$ (see [100]);
3. $4n = 3^m + 1$ (m odd) (see [101]).

See Also

§14.1	For Latin squares, MOLS, and transversal designs.
§14.3	For affine and projective planes.
§14.4	For projective spaces.
§14.5	For block designs.
§14.6	For difference sets.
[99]	Textbook on combinatorial designs.
[259]	Advanced textbook on combinatorial designs.
[260]	Another advanced textbook on combinatorial designs.
[700]	For association schemes (§VI.1), Costas arrays (§VI.9), conference matrices (§V.6), covering arrays (§VI.10), Hadamard designs and matrices(§V.1); Hall triple systems (§VI.28), ordered designs and perpendicular arrays (§VI.38), perfect hash families (§VI.43), Room squares (§VI.50), strongly regular graphs (§VII.11), whist tournaments (§VI.64).
[2702]	Another textbook on combinatorial designs.

References Cited: [6, 7, 93, 98, 99, 100, 101, 102, 166, 205, 206, 259, 260, 273, 300, 416, 458, 475, 601, 617, 698, 699, 700, 701, 891, 892, 893, 894, 910, 912, 1254, 1281, 1293, 1296, 1393, 1394, 1447, 1526, 1920, 1952, 2010, 2184, 2330, 2594, 2702, 2704, 2813, 2832, 2833, 2835, 2956, 3018]

14.8 (t, m, s)-nets and (t, s)-sequences

Harald Niederreiter, KFUPM

14.8.1 (t, m, s)-nets

14.8.1 Remark The theory of (t, m, s)-nets and (t, s)-sequences is significant for quasi-Monte Carlo methods in scientific computing (see the books [833] and [2234] and the recent survey article [2245]). For both (t, m, s)-nets and (t, s)-sequences, the idea is to sample the s-dimensional unit cube $[0, 1]^s$ in a uniform and equitable manner. In a nutshell, (t, m, s)-nets are finite samples (or point sets) and (t, s)-sequences are infinite sequences with special uniformity properties. The definition of a (t, m, s)-net (see Definition 14.8.2 below) has *a priori* no connection with finite fields, but it turns out that most of the interesting constructions of (t, m, s)-nets use finite fields as a tool. By a *point set* we mean a multiset in the sense of combinatorics, i.e., a set in which multiplicities of elements are allowed and taken into account.

14.8.2 Definition [2222, 2673] For integers $b \geq 2$ and $0 \leq t \leq m$ and a given dimension $s \geq 1$, a (t, m, s)-*net in base* b is a point set P consisting of b^m points in $[0, 1]^s$ such that every subinterval of $[0, 1]^s$ of volume b^{t-m} which has the form

$$\prod_{i=1}^{s} [a_i b^{-d_i}, (a_i + 1)b^{-d_i})$$

with integers $d_i \geq 0$ and $0 \leq a_i < b^{d_i}$ for $1 \leq i \leq s$ contains exactly b^t points of P.

14.8.3 Remark It is easily seen that a (t, m, s)-net in base b is also a (u, m, s)-net in base b for all integers u with $t \leq u \leq m$. Any point set consisting of b^m points in $[0, 1)^s$ is a (t, m, s)-net in base b with $t = m$. Smaller values of t mean stronger uniformity properties of a (t, m, s)-net in base b. The number t is the *quality parameter* of a (t, m, s)-net in base b.

14.8.4 Definition A (t, m, s)-net P in base b is a *strict* (t, m, s)-*net in base* b if t is the least integer u such that P is a (u, m, s)-net in base b.

14.8.5 Example Let $s = 2$ and let $b \geq 2$ and $m \geq 1$ be given integers. For any integer n with $0 \leq n < b^m$, let $n = \sum_{r=0}^{m-1} a_r(n) b^r$ with $a_r(n) \in \mathbb{Z}_b = \{0, 1, \ldots, b - 1\}$ be the digit expansion of n in base b and put $\phi_b(n) = \sum_{r=0}^{m-1} a_r(n) b^{-r-1}$. Then the point set consisting of the points $(nb^{-m}, \phi_b(n)) \in [0, 1]^2$, $n = 0, 1, \ldots, b^m - 1$, is a $(0, m, 2)$-net in base b. This point set is the *Hammersley net* in base b.

14.8.6 Example Let $b \geq 2$, $s \geq 1$, and $t \geq 0$ be given integers. Then the point set consisting of the points $(nb^{-1}, \ldots, nb^{-1}) \in [0, 1]^s$, $n = 0, 1, \ldots, b - 1$, each taken with multiplicity b^t, is a $(t, t + 1, s)$-net in base b.

14.8.7 Remark According to Remark 14.8.3 and Example 14.8.6, a (t, m, s)-net in base b always exists for $m = t$ and $m = t + 1$. For $m \geq t + 2$ there are combinatorial obstructions to the general existence of (t, m, s)-nets in base b. This was first observed in [2222]. Later, a combinatorial equivalence between (t, m, s)-nets in base b and ordered orthogonal arrays as defined in Definition 14.8.8 below was established.

14.8.8 Definition Let b, s, k, T, λ be positive integers with $b \geq 2$ and $sT \geq k$. An *ordered orthogonal array* $\mathrm{OOA}_b(s, k, T, \lambda)$ is a $(\lambda b^k) \times (sT)$ matrix with entries from $\mathbb{Z}_b$ and column labels (i, j) for $1 \leq i \leq s$ and $1 \leq j \leq T$ such that, for any integers $0 \leq d_1, \ldots, d_s \leq T$ with $\sum_{i=1}^{s} d_i = k$, the $(\lambda b^k) \times k$ submatrix obtained by restricting to the columns (i, j), $1 \leq j \leq d_i$, $1 \leq i \leq s$, contains among its rows every element of $\mathbb{Z}_b^k$ with the same frequency λ.

14.8.9 Theorem [1861, 2169] Let $b \geq 2$, $s \geq 2$, $k \geq 2$, and $t \geq 0$ be integers. Then there exists a $(t, t+k, s)$-net in base b if and only if there exists an ordered orthogonal array $\mathrm{OOA}_b(s, k, k-1, b^t)$.

14.8.10 Corollary [2222] There exists a $(0, 2, s)$-net in base b if and only if there exist $s-2$ mutually orthogonal latin squares of order b.

14.8.11 Corollary [2222] For $m \geq 2$, a $(0, m, s)$-net in base b can exist only if $s \leq M(b) + 2$, where $M(b)$ is the maximum cardinality of a set of mutually orthogonal latin squares of order b. In particular, if $m \geq 2$, then a necessary condition for the existence of a $(0, m, s)$-net in base b is $s \leq b + 1$.

14.8.12 Remark The equivalence between nets and ordered orthogonal arrays enunciated in Theorem 14.8.9, when combined with extensions of standard parameter bounds for orthogonal arrays to the case of ordered orthogonal arrays, leads to lower bounds on the quality parameter for nets. Examples of such bounds are the linear programming bound [1995], the Rao bound [1994], and the dual Plotkin bound [269, 1996]. Extensive numerical data on these bounds are available at `http://mint.sbg.ac.at`.

14.8.2 Digital (t, m, s)-nets

14.8.13 Remark Most of the known constructions of nets are based on the *digital method* which goes back to [2222]. In order to describe the digital method for the construction of (t, m, s)-nets in base b, we need the following ingredients. First of all, let integers $b \geq 2$, $m \geq 1$, and $s \geq 1$ be given. Then we choose:

1. a commutative ring R with identity and of cardinality b;
2. bijections $\eta_j^{(i)} : R \to \mathbb{Z}_b$ for $1 \leq i \leq s$ and $1 \leq j \leq m$;
3. $m \times m$ matrices $C^{(1)}, \ldots, C^{(s)}$ over R.

Now let $\mathbf{r} \in R^m$ be an m-tuple of elements of R and define

$$\pi_j^{(i)}(\mathbf{r}) = \eta_j^{(i)}(\mathbf{c}_j^{(i)} \cdot \mathbf{r}) \in \mathbb{Z}_b \qquad \text{for } 1 \leq i \leq s,\ 1 \leq j \leq m,$$

where $\mathbf{c}_j^{(i)}$ is the j-th row of the matrix $C^{(i)}$ and $\cdot$ denotes the standard inner product. Next we put

$$\pi^{(i)}(\mathbf{r}) = \sum_{j=1}^{m} \pi_j^{(i)}(\mathbf{r}) b^{-j} \in [0, 1] \qquad \text{for } 1 \leq i \leq s$$

and

$$P(\mathbf{r}) = (\pi^{(1)}(\mathbf{r}), \ldots, \pi^{(s)}(\mathbf{r})) \in [0, 1]^s.$$

By letting $\mathbf{r}$ range over all b^m elements of R^m, we arrive at a point set P consisting of b^m points in $[0, 1]^s$.

14.8.14 Definition If the point set P constructed in Remark 14.8.13 forms a (t, m, s)-net in base b, then P is a *digital (t, m, s)-net in base b*. If we want to emphasize that the construction uses the ring R, then we speak also of a *digital (t, m, s)-net over R*. If P is a strict (t, m, s)-net in base b, then P is a *digital strict (t, m, s)-net in base b* (or *over R*).

14.8.15 Remark The matrices $C^{(1)}, \ldots, C^{(s)}$ in Remark 14.8.13 are *generating matrices* of the digital net. The quality parameter t of the digital net depends only on the generating matrices. For a convenient algebraic condition on the generating matrices to guarantee a

certain value of t, we refer to Theorem 4.26 in [2234]. In the important case where the ring R is a finite field, an even simpler condition is given in Theorem 14.8.18 below.

14.8.16 Example Let $s = 2$ and let $b \geq 2$ and $m \geq 1$ be given integers. Choose $R = \mathbb{Z}_b$ and let the bijections $\eta_j^{(i)}$ in Remark 14.8.13 be identity maps. Let $C^{(1)}$ be the $m \times m$ identity matrix over $\mathbb{Z}_b$ and let $C^{(2)} = (c_{i,j})_{1 \leq i,j \leq m}$ be the $m \times m$ antidiagonal matrix over $\mathbb{Z}_b$ with $c_{i,j} = 1$ if $i + j = m + 1$ and $c_{i,j} = 0$ otherwise. Then the Hammersley net in Example 14.8.5 is easily seen to be a digital $(0, m, 2)$-net over $\mathbb{Z}_b$ with generating matrices $C^{(1)}$ and $C^{(2)}$.

14.8.17 Definition Let $C^{(1)}, \ldots, C^{(s)}$ be $m \times m$ matrices over the finite field $\mathbb{F}_q$ and for $1 \leq i \leq s$ and $1 \leq j \leq m$ let $\mathbf{c}_j^{(i)}$ denote the j-th row of the matrix $C^{(i)}$. Then $\varrho(C^{(1)}, \ldots, C^{(s)})$ is defined to be the largest nonnegative integer d such that, for any integers $0 \leq d_1, \ldots, d_s \leq m$ with $\sum_{i=1}^{s} d_i = d$, the vectors $\mathbf{c}_j^{(i)}$, $1 \leq j \leq d_i$, $1 \leq i \leq s$, are linearly independent over $\mathbb{F}_q$ (this property is assumed to be vacuously satisfied for $d = 0$).

14.8.18 Theorem [2222] The point set P constructed in Remark 14.8.13 with $R = \mathbb{F}_q$ and $m \times m$ generating matrices $C^{(1)}, \ldots, C^{(s)}$ over $\mathbb{F}_q$ is a digital strict (t, m, s)-net over $\mathbb{F}_q$ with $t = m - \varrho(C^{(1)}, \ldots, C^{(s)})$.

14.8.19 Example Let $s = 2$, let $b = p$ be a prime, and let the $m \times m$ matrices $C^{(1)}$ and $C^{(2)}$ over $\mathbb{F}_p$ be as in Example 14.8.16. Then it is easily seen that $\varrho(C^{(1)}, C^{(2)}) = m$. Using Theorem 14.8.18, this shows again that the Hammersley net in base $b = p$ is a digital $(0, m, 2)$-net over $\mathbb{F}_p$.

14.8.20 Remark The equivalence between nets and ordered orthogonal arrays stated in Theorem 14.8.9 has an analog for digital nets. The special family of linear ordered orthogonal arrays was introduced in [274] and it was shown that these arrays correspond to digital nets.

14.8.21 Remark There is a very useful duality theory for digital nets which facilitates many constructions of good digital nets. A crucial ingredient is the weight function V_m on $\mathbb{F}_q^{ms}$ introduced in Definition 14.8.22 below. The main result of this duality theory is Theorem 14.8.26 below.

14.8.22 Definition Let $m \geq 1$ and $s \geq 1$ be integers. Put $v_m(\mathbf{a}) = 0$ if $\mathbf{a} = \mathbf{0} \in \mathbb{F}_q^m$, and for $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{F}_q^m$ with $\mathbf{a} \neq \mathbf{0}$ let $v_m(\mathbf{a})$ be the largest value of j such that $a_j \neq 0$. Write a vector $\mathbf{A} \in \mathbb{F}_q^{ms}$ as the concatenation of s vectors of length m, i.e., $\mathbf{A} = (\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(s)}) \in \mathbb{F}_q^{ms}$ with $\mathbf{a}^{(i)} \in \mathbb{F}_q^m$ for $1 \leq i \leq s$. Then the *NRT weight* of $\mathbf{A}$ is defined by

$$V_m(\mathbf{A}) = \sum_{i=1}^{s} v_m(\mathbf{a}^{(i)}).$$

14.8.23 Remark The NRT weight is named after the work of Niederreiter [2220] and Rosenbloom and Tsfasman [2467]. The *NRT space* is $\mathbb{F}_q^{ms}$ with the metric $d_m(\mathbf{A}, \mathbf{B}) = V_m(\mathbf{A} - \mathbf{B})$ for $\mathbf{A}, \mathbf{B} \in \mathbb{F}_q^{ms}$. For $m = 1$ the NRT space reduces to the Hamming space in coding theory.

14.8.24 Definition The *minimum distance* $\delta_m(\mathcal{N})$ of a nonzero $\mathbb{F}_q$-linear subspace $\mathcal{N}$ of $\mathbb{F}_q^{ms}$ is given by

$$\delta_m(\mathcal{N}) = \min_{\mathbf{A} \in \mathcal{N} \setminus \{\mathbf{0}\}} V_m(\mathbf{A}).$$

14.8.25 Remark Let the $m \times m$ matrices $C^{(1)}, \ldots, C^{(s)}$ over $\mathbb{F}_q$ be generating matrices of a digital net P. Set up an $m \times ms$ matrix M over $\mathbb{F}_q$ as follows: for $1 \le j \le m$, the j-th row of M is obtained by concatenating the transposes of the j-th columns of $C^{(1)}, \ldots, C^{(s)}$. Let $\mathcal{M} \subseteq \mathbb{F}_q^{ms}$ be the row space of M and let $\mathcal{M}^\perp$ be its dual space, i.e.,

$$\mathcal{M}^\perp = \{\mathbf{A} \in \mathbb{F}_q^{ms} : \mathbf{A} \cdot \mathbf{M} = 0 \text{ for all } \mathbf{M} \in \mathcal{M}\},$$

where $\cdot$ is the standard inner product in $\mathbb{F}_q^{ms}$.

14.8.26 Theorem [2253] Let $m \ge 1$ and $s \ge 2$ be integers. Then the point set P in Remark 14.8.25 is a digital strict (t, m, s)-net over $\mathbb{F}_q$ with $t = m + 1 - \delta_m(\mathcal{M}^\perp)$.

14.8.27 Corollary [2253] Let $m \ge 1$ and $s \ge 2$ be integers. Then from any $\mathbb{F}_q$-linear subspace $\mathcal{N}$ of $\mathbb{F}_q^{ms}$ with $\dim(\mathcal{N}) \ge ms - m$ we can construct a digital strict (t, m, s)-net over $\mathbb{F}_q$ with $t = m + 1 - \delta_m(\mathcal{N})$.

14.8.28 Remark There are digital nets for which a property analogous to that in Definition 14.8.2 holds for a wider range of subintervals of $[0, 1]^s$. Such generalized digital nets were introduced in [829] and are also studied in detail in Chapter 15 of [833].

14.8.29 Remark There is a generalization of the digital method which can be viewed as a nonlinear analog of the construction in Remark 14.8.13. For simplicity we consider only the case where $R = \mathbb{F}_q$ (see [2244] for a general ring R). Compared to Remark 14.8.13, the only change is that instead of linear forms $\mathbf{c}_j^{(i)} \cdot \mathbf{r}$ we now use polynomial functions, that is, for $1 \le i \le s$ and $1 \le j \le m$ we choose polynomials $f_j^{(i)}$ over $\mathbb{F}_q$ in m variables and then we replace $\mathbf{c}_j^{(i)} \cdot \mathbf{r}$ by $f_j^{(i)}(\mathbf{r})$ for $\mathbf{r} \in \mathbb{F}_q^m$. The following criterion uses the concept of permutation polynomial in several variables (see Section 8.2).

14.8.30 Theorem [2244] The point set constructed in Remark 14.8.29 is a (t, m, s)-net in base q if and only if, for any integers $d_1, \ldots, d_s \ge 0$ with $\sum_{i=1}^s d_i = m - t$, the polynomials $f_j^{(i)}$, $1 \le j \le d_i$, $1 \le i \le s$, have the property that all of their nontrivial linear combinations with coefficients from $\mathbb{F}_q$ are permutation polynomials over $\mathbb{F}_q$ in m variables.

14.8.3 Constructions of (t, m, s)-nets

14.8.31 Remark A general principle for the construction of (t, m, s)-nets with $s \ge 2$ is based on the use of Proposition 14.8.50 below in conjunction with the constructions of $(t, s-1)$-sequences in Subsection 14.8.6. In the present subsection, we describe constructions of (t, m, s)-nets that are not derived from this principle. One of the first constructions of this type was that of *polynomial lattices* in [2233]. Choose $f \in \mathbb{F}_q[x]$ with $\deg(f) = m \ge 1$ and an s-tuple $\mathbf{g} = (g_1, \ldots, g_s) \in \mathbb{F}_q[x]^s$ with $\deg(g_i) < m$ for $1 \le i \le s$. Consider the Laurent series expansions

$$\frac{g_i(x)}{f(x)} = \sum_{k=1}^{\infty} u_k^{(i)} x^{-k} \in \mathbb{F}_q((x^{-1})) \qquad \text{for } 1 \le i \le s.$$

Then for $1 \le i \le s$ the generating matrix $C^{(i)} = (c_{j,r})$ is the Hankel matrix given by $c_{j,r} = u_{j+r}^{(i)} \in \mathbb{F}_q$ for $1 \le j \le m$, $0 \le r \le m - 1$. The bijections $\eta_j^{(i)}$ in Remark 14.8.13 are chosen arbitrarily. The resulting digital net over $\mathbb{F}_q$ is denoted by $P(\mathbf{g}, f)$.

14.8.32 Definition Let $s \ge 2$ and let f and $\mathbf{g}$ be as in Remark 14.8.31. Then the *figure of merit* $\varrho(\mathbf{g}, f)$ is defined by

$$\varrho(\mathbf{g}, f) = s - 1 + \min \sum_{i=1}^{s} \deg(h_i),$$

where the minimum is over all nonzero s-tuples $(h_1, \ldots, h_s) \in \mathbb{F}_q[x]^s$ with $\deg(h_i) < m$ for $1 \le i \le s$ and f dividing $\sum_{i=1}^{s} h_i g_i$. Here we use the convention $\deg(0) = -1$.

14.8.33 Theorem [2233] For $s \ge 2$, the point set $P(\mathbf{g}, f)$ in Remark 14.8.31 is a digital strict (t, m, s)-net over $\mathbb{F}_q$ with $t = m - \varrho(\mathbf{g}, f)$.

14.8.34 Remark It is clear from Theorem 14.8.33 that in order to obtain a good (t, m, s)-net by this construction, i.e., a net with a small value of t, we need to find $\mathbf{g}$ and f with a large figure of merit $\varrho(\mathbf{g}, f)$. A systematic method for the explicit construction of good polynomial lattices is the component-by-component algorithm in [830]; see also Chapter 10 in [833].

14.8.35 Remark Several constructions of digital nets are based on Corollary 14.8.27. A powerful construction of this type uses algebraic function fields (see Section 12.1 for background on algebraic function fields). We present only a simple version of this construction; more refined versions can be found in [2247]. Let F be an algebraic function field (of one variable) with full constant field $\mathbb{F}_q$, that is, $\mathbb{F}_q$ is algebraically closed in F. Let $N(F)$ denote the number of rational places of F. For a given dimension $s \ge 2$, we assume that $N(F) \ge s$ and let $P_1, \ldots, P_s$ be s distinct rational places of F. Let G be a divisor of F. For each $i = 1, \ldots, s$, let $t_i \in F$ be a prime element at P_i and let $n_i \in \mathbb{Z}$ be the coefficient of P_i in G. For f in the Riemann-Roch space $\mathcal{L}(G)$ and a given integer $m \ge 1$, let $\theta^{(i)}(f) \in \mathbb{F}_q^m$ be the vector whose coordinates are, in descending order, the coefficients of t_i^j, $j = -n_i + m - 1, -n_i + m - 2, \ldots, -n_i$, in the local expansion of f at P_i. Now define the $\mathbb{F}_q$-linear map $\theta : \mathcal{L}(G) \to \mathbb{F}_q^{ms}$ by

$$\theta(f) = (\theta^{(1)}(f), \ldots, \theta^{(s)}(f)) \qquad \text{for all } f \in \mathcal{L}(G).$$

A digital net over $\mathbb{F}_q$ is then obtained by applying Corollary 14.8.27 with $\mathcal{N}$ being the image of the map θ. A suitable choice of the divisor G leads to the following result.

14.8.36 Theorem [2247] Let $s \ge 2$ be an integer and let F be an algebraic function field with full constant field $\mathbb{F}_q$, genus $g \ge 1$, and $N(F) \ge s$. If k and m are integers with $0 \le k \le g - 1$ and $m \ge \max(1, g - k - 1)$, then there exists a digital $(g - k - 1, m, s)$-net over $\mathbb{F}_q$ provided that

$$\binom{s + m + k - g}{s - 1} A_k(F) < h(F),$$

where $A_k(F)$ is the number of positive divisors of F of degree k and $h(F)$ is the divisor class number of F.

14.8.37 Example Let $q = 9$ and let F be the Hermitian function field over $\mathbb{F}_9$, that is, $F = \mathbb{F}_9(x, y)$ with $y^3 + y = x^4$. Then $g = 3$, $N(F) = 28$, and $h(F) = 4096$. We apply Theorem 14.8.36 with $s = 28$, $k = 0$, $m = 5$, and we obtain a digital $(2, 5, 28)$-net over $\mathbb{F}_9$. The value $t = 2$ is the currently best value of the quality parameter for a $(t, 5, 28)$-net in base 9, according to the website `http://mint.sbg.ac.at` which contains an extensive database for parameters of (t, m, s)-nets.

14.8.38 Remark Another construction based on Corollary 14.8.27 was introduced in [2241]. For integers $m \ge 1$ and $s \ge 2$, consider the $\mathbb{F}_q$-linear space $\mathcal{P} = \{f \in \mathbb{F}_{q^m}[x] : \deg(f) < s\}$. Fix $\alpha \in \mathbb{F}_{q^m}$ and define the $\mathbb{F}_q$-linear subspace $\mathcal{P}_\alpha = \{f \in \mathcal{P} : f(\alpha) = 0\}$ of $\mathcal{P}$. Set up a map $\tau : \mathcal{P} \to \mathbb{F}_q^{ms}$ as follows. Write $f \in \mathcal{P}$ explicitly as $f(x) = \sum_{i=1}^{s} \gamma_i x^{i-1}$ with $\gamma_i \in \mathbb{F}_{q^m}$ for $1 \le i \le s$. For each $i = 1, \ldots, s$, choose an ordered basis B_i of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and let $\mathbf{c}_i(f) \in \mathbb{F}_q^m$ be the coordinate vector of γ_i with respect to B_i. Then define

$$\tau(f) = (\mathbf{c}_1(f), \ldots, \mathbf{c}_s(f)) \in \mathbb{F}_q^{ms} \qquad \text{for all } f \in \mathcal{P}.$$

A digital net over $\mathbb{F}_q$ is now obtained by applying Corollary 14.8.27 with $\mathcal{N}$ being the image of the subspace $\mathcal{P}_\alpha$ under τ. The resulting digital net is a *cyclic digital net* over $\mathbb{F}_q$ relative to the bases $B_1, \ldots, B_s$.

14.8.39 Remark A generalization of the construction in Remark 14.8.38 was presented in [2383]. For integers $m \geq 1$ and $s \geq 2$, consider $\mathcal{Q} = \mathbb{F}_{q^m}^s$ as a vector space over $\mathbb{F}_q$. Fix $\boldsymbol{\alpha} \in \mathcal{Q}$ with $\boldsymbol{\alpha} \neq \mathbf{0}$ and put $\mathcal{Q}_{\boldsymbol{\alpha}} = \{\boldsymbol{\beta} \in \mathcal{Q} : \boldsymbol{\alpha} \cdot \boldsymbol{\beta} = 0\}$. Then $\mathcal{Q}_{\boldsymbol{\alpha}}$ is an $\mathbb{F}_q$-linear subspace of $\mathcal{Q}$. Let $\sigma : \mathcal{Q} \to \mathbb{F}_q^{ms}$ be an isomorphism between vector spaces over $\mathbb{F}_q$. A digital net over $\mathbb{F}_q$ is now obtained by applying Corollary 14.8.27 with $\mathcal{N}$ being the image of the subspace $\mathcal{Q}_{\boldsymbol{\alpha}}$ under σ. The resulting digital net is a *hyperplane net* over $\mathbb{F}_q$. Detailed information on hyperplane nets and cyclic digital nets can be found in Chapter 11 of [833].

14.8.40 Theorem [1862] Given a linear code over $\mathbb{F}_q$ with length n, dimension k, and minimum distance $d \geq 3$, we can construct a digital $(n-k-d+1, n-k, s)$-net over $\mathbb{F}_q$ with $s = \lfloor (n-1)/h \rfloor$ if $d = 2h+2$ is even and $s = \lfloor n/h \rfloor$ if $d = 2h+1$ is odd.

14.8.41 Remark Further applications of coding theory to the construction of digital nets are discussed in the survey articles [2237] and [2242]. We specifically mention some principles of combining several digital nets to obtain a new digital net that are inspired by coding theory. For instance, the well-known Kronecker-product construction in coding theory has an analog for digital nets [274]. The following result is an analog of the matrix-product construction of linear codes.

14.8.42 Theorem [2249] Let h be an integer with $2 \leq h \leq q$. If for $k = 1, \ldots, h$ a digital (t_k, m_k, s_k)-net over $\mathbb{F}_q$ is given and if $s_1 \leq s_2 \leq \cdots \leq s_h$, then we can construct a digital $(t, \sum_{k=1}^h m_k, \sum_{k=1}^h s_k)$-net over $\mathbb{F}_q$ with

$$t = 1 + \sum_{k=1}^{h} m_k - \min_{1 \leq k \leq h} (h-k+1)(m_k - t_k + 1).$$

14.8.43 Proposition Given a (t, m, s)-net in base b, we can construct:

1. a (t, u, s)-net in base b for $t \leq u \leq m$;
2. a (t, m, r)-net in base b for $1 \leq r \leq s$;
3. a $(t+u, m+u, s)$-net in base b for any integer $u \geq 0$.

14.8.44 Remark A result of the type appearing in Proposition 14.8.43 is called a *propagation rule* for nets. There are also propagation rules for digital nets, in the sense that the input net and the output net are both digital nets. Furthermore, there are propagation rules that involve a base change, typically moving from a base b to a base that is a power b^k with $k \geq 2$ or vice versa. A detailed discussion of propagation rules is presented in Chapter 9 of [833].

14.8.4 (t, s)-sequences and $(\mathbf{T}, s)$-sequences

14.8.45 Remark There is an analog of (t, m, s)-nets for sequences of points in $[0,1]^s$, given in Definition 14.8.46 below. First we need some notation. For an integer $b \geq 2$ and a real number $x \in [0,1]$, let $x = \sum_{j=1}^{\infty} y_j b^{-j}$ with all $y_j \in \mathbb{Z}_b$ be a b-adic expansion of x, where the case $y_j = b-1$ for all sufficiently large j is allowed. For any integer $m \geq 1$, we define the truncation $[x]_{b,m} = \sum_{j=1}^{m} y_j b^{-j}$. Note that this truncation operates on the expansion of x and not on x itself, since it may yield different results depending on which b-adic expansion of x is used. If $\mathbf{x} = (x^{(1)}, \ldots, x^{(s)}) \in [0,1]^s$ and the $x^{(i)}$, $1 \leq i \leq s$, are given by prescribed b-adic expansions, then we define

$$[\mathbf{x}]_{b,m} = ([x^{(1)}]_{b,m}, \ldots, [x^{(s)}]_{b,m}).$$

14.8.46 Definition [2222, 2673] Let $b \geq 2$, $s \geq 1$, and $t \geq 0$ be integers. A sequence $\mathbf{x}_0, \mathbf{x}_1, \ldots$ of points in $[0,1]^s$ is a (t,s)-*sequence in base* b if for all integers $k \geq 0$ and $m > t$ the points $[\mathbf{x}_n]_{b,m}$ with $kb^m \leq n < (k+1)b^m$ form a (t,m,s)-net in base b. Here the coordinates of all points $\mathbf{x}_n$, $n = 0, 1, \ldots$, are given by prescribed b-adic expansions.

14.8.47 Remark It is easily seen that a (t,s)-sequence in base b is also a (u,s)-sequence in base b for all integers $u \geq t$. Smaller values of t mean stronger uniformity properties of a (t,s)-sequence in base b. The number t is the *quality parameter* of a (t,s)-sequence in base b.

14.8.48 Definition A (t,s)-sequence S in base b is a *strict* (t,s)-*sequence in base* b if t is the least integer u such that S is a (u,s)-sequence in base b.

14.8.49 Example Let $s = 1$ and let $b \geq 2$ be an integer. For $n = 0, 1, \ldots$, let $n = \sum_{r=0}^{\infty} a_r(n) b^r$ with all $a_r(n) \in \mathbb{Z}_b$ and $a_r(n) = 0$ for all sufficiently large r be the digit expansion of n in base b. Put $\phi_b(n) = \sum_{r=0}^{\infty} a_r(n) b^{-r-1}$. Then the sequence $\phi_b(0), \phi_b(1), \ldots$ is a $(0,1)$-sequence in base b. This sequence is the *van der Corput sequence* in base b.

14.8.50 Proposition [2222] Given a (t,s)-sequence in base b, we can construct a $(t,m,s+1)$-net in base b for any integer $m \geq t$.

14.8.51 Remark The following result is obtained by combining Corollary 14.8.11 and Proposition 14.8.50.

14.8.52 Corollary [2222] A $(0,s)$-sequence in base b can exist only if $s \leq M(b) + 1$. In particular, a necessary condition for the existence of a $(0,s)$-sequence in base b is $s \leq b$.

14.8.53 Remark It was shown in [2224] that for any integers $b \geq 2$ and $s \geq 1$ there exists a (t,s)-sequence in base b for some value of t. Therefore it is meaningful to define $t_b(s)$ as the least value of t for which there exists a (t,s)-sequence in base b.

14.8.54 Theorem [2269, 2548] For any integers $b \geq 2$ and $s \geq 1$, we have

$$t_b(s) \geq \frac{s}{b-1} - c_b \log(s+1)$$

with a constant $c_b > 0$ depending only on b.

14.8.55 Definition [1846] Let $b \geq 2$ and $s \geq 1$ be integers and let $\mathbb{N}_0$ denote the set of nonnegative integers. Let $\mathbf{T} : \mathbb{N} \to \mathbb{N}_0$ be a function with $\mathbf{T}(m) \leq m$ for all $m \in \mathbb{N}$. Then a sequence $\mathbf{x}_0, \mathbf{x}_1, \ldots$ of points in $[0,1]^s$ is a $(\mathbf{T},s)$-*sequence in base* b if for all $k \in \mathbb{N}_0$ and $m \in \mathbb{N}$, the points $[\mathbf{x}_n]_{b,m}$ with $kb^m \leq n < (k+1)b^m$ form a $(\mathbf{T}(m),m,s)$-net in base b. Here the coordinates of all points $\mathbf{x}_n$, $n = 0, 1, \ldots$, are given by prescribed b-adic expansions. A $(\mathbf{T},s)$-sequence S in base b is a *strict* $(\mathbf{T},s)$-*sequence in base* b if there is no function $\mathbf{U} : \mathbb{N} \to \mathbb{N}_0$ with $\mathbf{U}(m) \leq m$ for all $m \in \mathbb{N}$ and $\mathbf{U}(m) < \mathbf{T}(m)$ for at least one $m \in \mathbb{N}$ such that S is a $(\mathbf{U},s)$-sequence in base b.

14.8.56 Remark If the function $\mathbf{T}$ in Definition 14.8.55 is such that for some integer $t \geq 0$ we have $\mathbf{T}(m) = m$ for $m \leq t$ and $\mathbf{T}(m) = t$ for $m > t$, then the concept of a $(\mathbf{T},s)$-sequence in base b reduces to that of a (t,s)-sequence in base b.

14.8.5 Digital (t,s)-sequences and digital $(\mathbf{T},s)$-sequences

14.8.57 Remark There is an analog of the digital method in Remark 14.8.13 for the construction of sequences. Let integers $b \geq 2$ and $s \geq 1$ be given. Then we choose:

1. a commutative ring R with identity and of cardinality b;
2. bijections $\psi_r : \mathbb{Z}_b \to R$ for $r = 0, 1, \ldots$, with $\psi_r(0) = 0$ for all sufficiently large r;
3. bijections $\eta_j^{(i)} : R \to \mathbb{Z}_b$ for $1 \le i \le s$ and $j \ge 1$;
4. $\infty \times \infty$ matrices $C^{(1)}, \ldots, C^{(s)}$ over R.

For $n = 0, 1, \ldots$, let $n = \sum_{r=0}^{\infty} a_r(n) b^r$ with all $a_r(n) \in \mathbb{Z}_b$ and $a_r(n) = 0$ for all sufficiently large r be the digit expansion of n in base b. We put $\mathbf{n} = (\psi_r(a_r(n)))_{r=0}^{\infty} \in R^{\infty}$. Next we define

$$y_{n,j}^{(i)} = \eta_j^{(i)}(\mathbf{c}_j^{(i)} \cdot \mathbf{n}) \in \mathbb{Z}_b \qquad \text{for } n \ge 0,\ 1 \le i \le s, \text{ and } j \ge 1,$$

where $\mathbf{c}_j^{(i)}$ is the j-th row of the matrix $C^{(i)}$. Note that the inner product $\mathbf{c}_j^{(i)} \cdot \mathbf{n}$ is meaningful since $\mathbf{n}$ has only finitely many nonzero coordinates. Then we put

$$x_n^{(i)} = \sum_{j=1}^{\infty} y_{n,j}^{(i)} b^{-j} \qquad \text{for } n \ge 0 \text{ and } 1 \le i \le s.$$

Finally, we define the sequence S consisting of the points

$$\mathbf{x}_n = (x_n^{(1)}, \ldots, x_n^{(s)}) \in [0,1]^s \qquad \text{for } n = 0, 1, \ldots.$$

14.8.58 Definition If the sequence S constructed in Remark 14.8.57 forms a (t, s)-sequence in base b, then S is a *digital (t, s)-sequence in base b*. If we want to emphasize that the construction uses the ring R, then we speak also of a *digital (t, s)-sequence over R*. If S is a strict (t, s)-sequence in base b, then S is a *digital strict (t, s)-sequence in base b* (or *over R*).

14.8.59 Definition If the sequence S constructed in Remark 14.8.57 forms a (strict) $(\mathbf{T}, s)$-sequence in base b, then S is a *digital (strict) $(\mathbf{T}, s)$-sequence in base b* (or *over R*).

14.8.60 Remark The matrices $C^{(1)}, \ldots, C^{(s)}$ in Remark 14.8.57 are *generating matrices* of the digital sequence. The value of t for a digital (t, s)-sequence and the function $\mathbf{T}$ for a digital $(\mathbf{T}, s)$-sequence depend only on the generating matrices. For the determination of t in the general case, we refer to Theorem 4.35 in [2234]. For the case $R = \mathbb{F}_q$, see Theorem 14.8.62 below.

14.8.61 Example Let $s = 1$ and let $b \ge 2$ be an integer. Choose $R = \mathbb{Z}_b$ and let the bijections ψ_r and $\eta_j^{(i)}$ in Remark 14.8.57 be identity maps. Let $C^{(1)}$ be the $\infty \times \infty$ identity matrix over $\mathbb{Z}_b$. Then the van der Corput sequence in Example 14.8.49 is easily seen to be a digital $(0, 1)$-sequence over $\mathbb{Z}_b$ with generating matrix $C^{(1)}$.

14.8.62 Theorem Let S be the sequence constructed in Remark 14.8.57 with $R = \mathbb{F}_q$ and $\infty \times \infty$ generating matrices $C^{(1)}, \ldots, C^{(s)}$ over $\mathbb{F}_q$. For $1 \le i \le s$ and $m \in \mathbb{N}$, let $C_m^{(i)}$ denote the left upper $m \times m$ submatrix of $C^{(i)}$. Then S is a digital strict $(\mathbf{T}, s)$-sequence over $\mathbb{F}_q$ with $\mathbf{T}(m) = m - \varrho(C_m^{(1)}, \ldots, C_m^{(s)})$ for all $m \in \mathbb{N}$, where $\varrho(C_m^{(1)}, \ldots, C_m^{(s)})$ is given by Definition 14.8.17.

14.8.63 Remark It was shown in [2224] that for any prime power q and any integer $s \ge 1$, there exists a digital (t, s)-sequence over $\mathbb{F}_q$ for some value of t. In analogy with $t_b(s)$ in Remark 14.8.53, we define $d_q(s)$ as the least value of t for which there exists a digital (t, s)-sequence over $\mathbb{F}_q$. It is trivial that $t_q(s) \le d_q(s)$, and so Theorem 14.8.54 provides also a lower bound on $d_q(s)$.

14.8.64 Problem With the previous notation, it is an open problem whether we can ever have $t_q(s) < d_q(s)$.

14.8.65 Remark An analog of the duality theory for digital nets described in Subsection 14.8.2 was developed in [832] for the case of digital $(\mathbf{T}, s)$-sequences. Let the weight function v_m on $\mathbb{F}_q^m$ be as in Definition 14.8.22. For $\mathbf{A} = (\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(s)}) \in \mathbb{F}_q^{ms}$ with $\mathbf{a}^{(i)} \in \mathbb{F}_q^m$ for $1 \le i \le s$, we put

$$U_m(\mathbf{A}) = \max_{1 \le i \le s} v_m(\mathbf{a}^{(i)}).$$

14.8.66 Definition Let $s \ge 2$ be an integer. For each integer $m \ge 1$, let $\mathcal{N}_m$ be an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^{ms}$ with $\dim(\mathcal{N}_m) \ge ms - m$. Let $\mathcal{N}_{m+1,m}$ be the projection of the set $\{\mathbf{A} \in \mathcal{N}_{m+1} : U_{m+1}(\mathbf{A}) \le m\}$, where $\mathbf{A} = (\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(s)})$ with all $\mathbf{a}^{(i)} \in \mathbb{F}_q^{m+1}$, on the first m coordinates of each $\mathbf{a}^{(i)}$ for $1 \le i \le s$. Suppose that $\mathcal{N}_{m+1,m}$ is an $\mathbb{F}_q$-linear subspace of $\mathcal{N}_m$ with $\dim(\mathcal{N}_{m+1,m}) \ge \dim(\mathcal{N}_m) - 1$ for all $m \ge 1$. Then the sequence $(\mathcal{N}_m)_{m \ge 1}$ of spaces is a *dual space chain* over $\mathbb{F}_q$.

14.8.67 Theorem [832] Let $s \ge 2$ be an integer. Then from any dual space chain $(\mathcal{N}_m)_{m \ge 1}$ over $\mathbb{F}_q$ we can construct a digital strict $(\mathbf{T}, s)$-sequence over $\mathbb{F}_q$ with $\mathbf{T}(m) = m + 1 - \delta_m(\mathcal{N}_m)$ for all $m \ge 1$.

14.8.68 Remark In analogy with the generalized digital nets mentioned in Remark 14.8.28, there are generalized digital sequences as introduced in [829] and also studied in Chapter 15 of [833].

14.8.69 Remark The nonlinear digital method described in Remark 14.8.29 can be used also for the construction of (t, s)-sequences [2244].

14.8.6 Constructions of (t, s)-sequences and $(\mathbf{T}, s)$-sequences

14.8.70 Remark A general family of digital (t, s)-sequences is formed by *Niederreiter sequences* [2224]. We describe only the simplest case of this construction. For a given dimension $s \ge 1$, let $p_1, \ldots, p_s \in \mathbb{F}_q[x]$ be pairwise coprime polynomials over $\mathbb{F}_q$. Let $e_i = \deg(p_i) \ge 1$ for $1 \le i \le s$. For $1 \le i \le s$ and integers $u \ge 1$ and $0 \le k < e_i$, consider the Laurent series expansion

$$\frac{x^k}{p_i(x)^u} = \sum_{r=0}^{\infty} a^{(i)}(u, k, r) x^{-r-1} \in \mathbb{F}_q((x^{-1})).$$

Then define $c_{j,r}^{(i)} = a^{(i)}(Q+1, k, r) \in \mathbb{F}_q$ for $1 \le i \le s$, $j \ge 1$, and $r \ge 0$, where $j - 1 = Qe_i + k$ with integers $Q = Q(i, j)$ and $k = k(i, j)$ satisfying $0 \le k < e_i$. The generating matrices of the Niederreiter sequence are now given by $C^{(i)} = (c_{j,r}^{(i)})_{j \ge 1, r \ge 0}$ for $1 \le i \le s$. The bijections ψ_r and $\eta_j^{(i)}$ in Remark 14.8.57 are chosen arbitrarily.

14.8.71 Theorem [831, 2224] The Niederreiter sequence based on the pairwise coprime non-constant polynomials $p_1, \ldots, p_s \in \mathbb{F}_q[x]$ is a digital strict (t, s)-sequence over $\mathbb{F}_q$ with $t = \sum_{i=1}^{s} (\deg(p_i) - 1)$.

14.8.72 Remark If q is a prime, $1 \le s \le q$, and $p_i(x) = x - i + 1 \in \mathbb{F}_q[x]$ for $1 \le i \le s$, then we obtain the digital $(0, s)$-sequences over $\mathbb{F}_q$ called *Faure sequences* [1040]. An analogous construction of digital $(0, s)$-sequences over $\mathbb{F}_q$ for arbitrary prime powers q and dimensions $1 \le s \le q$ was given in [2222]. Note that in view of Corollary 14.8.52, $s \le q$ is also a necessary condition for the existence of a $(0, s)$-sequence in base q. If $q = 2$, $s \ge 1$ is an arbitrary dimension, $p_1(x) = x \in \mathbb{F}_2[x]$, and $p_2, \ldots, p_s$ are distinct primitive polynomials over $\mathbb{F}_2$, then we obtain *Sobol' sequences* [2673].

14.8.73 Remark The construction of Niederreiter sequences in Remark 14.8.70 is optimized by letting $p_1, \ldots, p_s$ be s distinct monic irreducible polynomials over $\mathbb{F}_q$ of least degrees. If with this choice we put $T_q(s) = \sum_{i=1}^{s}(\deg(p_i) - 1)$, then for fixed q the quantity $T_q(s)$ is of the order of magnitude $s \log s$ as $s \to \infty$. Let $U(s)$ denote the least value of t that is known to be achievable by Sobol' sequences for given s. Then $T_2(s) = U(s)$ for $1 \leq s \leq 7$ and $T_2(s) < U(s)$ for all $s \geq 8$.

14.8.74 Remark Substantial improvements on the construction of Niederreiter sequences in Remark 14.8.70 can be obtained by using tools from the theory of algebraic function fields over finite fields (see Section 12.1 for this theory). This leads to the family of *Niederreiter-Xing sequences* [2268, 2999]. Let F be an algebraic function field with full constant field $\mathbb{F}_q$ and genus g. Assume that F contains at least one rational place P_∞ and let D be a divisor of F with $\deg(D) = 2g$ and $P_\infty \notin \mathrm{supp}(D)$. Furthermore, we choose s distinct places $P_1, \ldots, P_s$ of F with $P_i \neq P_\infty$ for $1 \leq i \leq s$. There exist integers $0 = n_0 < n_1 < \cdots < n_g \leq 2g$ such that

$$\ell(D - n_u P_\infty) = \ell(D - (n_u + 1)P_\infty) + 1 \qquad \text{for } 0 \leq u \leq g.$$

We choose

$$w_u \in \mathcal{L}(D - n_u P_\infty) \setminus \mathcal{L}(D - (n_u + 1)P_\infty) \qquad \text{for } 0 \leq u \leq g.$$

For each $i = 1, \ldots, s$, we consider the chain $\mathcal{L}(D) \subset \mathcal{L}(D + P_i) \subset \mathcal{L}(D + 2P_i) \subset \cdots$ of vector spaces over $\mathbb{F}_q$. By starting from the basis $\{w_0, w_1, \ldots, w_g\}$ of $\mathcal{L}(D)$ and successively adding basis vectors at each step of the chain, we obtain for each $n \geq 1$ a basis

$$\{w_0, w_1, \ldots, w_g, f_1^{(i)}, f_2^{(i)}, \ldots, f_{n \deg(P_i)}^{(i)}\}$$

of $\mathcal{L}(D + nP_i)$. For a prime element z at P_∞ and for $r = 0, 1, \ldots$, we put $z_r = z^r$ if $r \notin \{n_0, n_1, \ldots, n_g\}$ and $z_r = w_u$ if $r = n_u$ for some $u \in \{0, 1, \ldots, g\}$. Each $f_j^{(i)}$ with $1 \leq i \leq s$ and $j \geq 1$ has then a local expansion at P_∞ of the form $f_j^{(i)} = \sum_{r=0}^{\infty} a_{j,r}^{(i)} z_r$ with all $a_{j,r}^{(i)} \in \mathbb{F}_q$. Let $\mathbf{c}_j^{(i)}$ be the sequence obtained from the sequence $a_{j,r}^{(i)}$, $r = 0, 1, \ldots$, by deleting the terms with $r = n_u$ for some $u \in \{0, 1, \ldots, g\}$. For $1 \leq i \leq s$, the generating matrix $C^{(i)}$ of the Niederreiter-Xing sequence is now the matrix whose j-th row is $\mathbf{c}_j^{(i)}$ for $j \geq 1$. The bijections ψ_r and $\eta_j^{(i)}$ in Remark 14.8.57 are chosen arbitrarily.

14.8.75 Theorem [2999] Let F be an algebraic function field with full constant field $\mathbb{F}_q$ and genus g which contains at least one rational place P_∞. Let D be a divisor of F with $\deg(D) = 2g$ and $P_\infty \notin \mathrm{supp}(D)$ and let $P_1, \ldots, P_s$ be distinct places of F with $P_i \neq P_\infty$ for $1 \leq i \leq s$. Then the corresponding Niederreiter-Xing sequence is a digital (t, s)-sequence over $\mathbb{F}_q$ with $t = g + \sum_{i=1}^{s}(\deg(P_i) - 1)$.

14.8.76 Corollary [2268] For every prime power q and every dimension $s \geq 1$, there exists a digital $(V_q(s), s)$-sequence over $\mathbb{F}_q$, where $V_q(s) = \min\{g \geq 0 : N_q(g) \geq s + 1\}$ and $N_q(g)$ is the maximum number of rational places that an algebraic function field with full constant field $\mathbb{F}_q$ and genus g can have.

14.8.77 Remark It was shown in [2268] that $V_q(s) = O(s)$ as $s \to \infty$. Since $t_q(s) \leq d_q(s) \leq V_q(s)$ by Remark 14.8.63 and Corollary 14.8.76, we obtain $t_q(s) = O(s)$ and $d_q(s) = O(s)$ as $s \to \infty$. In view of Theorem 14.8.54, these asymptotic bounds are best possible.

14.8.78 Remark The only improvements on Niederreiter-Xing sequences were obtained, in some special cases, in the more recent paper [2252]. For instance, let q be an arbitrary prime power and let $s = q+1$. Then $t_q(q+1) = d_q(q+1) = 1$. On the other hand, the construction in [2252] yields a digital $(\mathbf{T}, q + 1)$-sequence over $\mathbb{F}_q$ with $\mathbf{T}(m) = 0$ for even $m \geq 2$ and $\mathbf{T}(m) = 1$ for odd $m \geq 1$.

See Also

§14.1	For orthogonal arrays and related combinatorial designs.
§15.1	For related constructions of linear codes.

References Cited: [269, 274, 829, 830, 831, 832, 833, 1040, 1846, 1861, 1862, 1994, 1995, 1996, 2169, 2220, 2222, 2224, 2233, 2234, 2237, 2241, 2242, 2244, 2245, 2247, 2249, 2252, 2253, 2268, 2269, 2383, 2467, 2548, 2673, 2999]

14.9 Applications and weights of multiples of primitive and other polynomials

Brett Stevens, Carleton University

14.9.1 Applications where weights of multiples of a base polynomial are relevant

14.9.1 Remark The performance of several applications of polynomials, frequently primitive, depend on the weights of multiples of the base polynomial. Many of these applications are discussed in this Handbook.

14.9.1.1 Applications from other Handbook sections

14.9.2 Remark The multiples of a polynomial f with weight w influence the statistical bias of the linear feedback shift register sequence generated from f. Fewer multiples with a given weight, w reduces the w-th moment of the Hamming weight [1610, 1932]. For more information on bias and randomness of linear feedback shift register sequences see Section 10.2.

14.9.3 Remark In Section 15.1 the use of primitive polynomials f, to generate *cyclic redundancy check codes* is discussed. The undetectable error patterns of these codes are precisely those whose errors correspond to multiples of f. This has the consequences that burst errors of length up to $\deg(f)$ are always detectable and that to understand how many arbitrary errors can be detected requires having knowledge of the weights of multiples of f.

14.9.4 Remark In Section 15.4, turbo codes are discussed. Turbo codes use feedback polynomials that are often primitive. The bit error rate (BER) of the turbo code's interleaver design depends on the weights of polynomials divisible by the feedback polynomial [2497].

14.9.5 Remark Low weight multiples of a public polynomial compromise the private key for the $\mathcal{TCHo}$ cryptosystem and its security therefore rests on the difficulty of finding low weight multiples [146, 1481]. The weight of polynomials and their multiples is important in linear feedback shift register cryptanalysis and certain attacks depend on the sparsity of feedback polynomial or one of its multiples [2060]. Chapter 16 discusses the many connections between finite fields and cryptography.

14.9.1.2 Application of polynomials to the construction of orthogonal arrays

14.9.6 Remark We present a discussion of applications of polynomials and the weights of their multiples to the construction and strength of orthogonal arrays.

14.9.7 Definition An *orthogonal array* of *size* N, with k constraints (or k *factors* or of *degree* k), s *levels* (or of *order* s), and *strength* t, denoted $\mathrm{OA}(N, k, s, t)$, is a $k \times N$ array (sometimes $N \times k$) with entries from a set of $s \geq 2$ symbols, having the property that in every $t \times N$ submatrix, every $t \times 1$ column vector appears the same number $\lambda = \frac{N}{s^t}$ of times. The parameter λ is the *index* of the orthogonal array. An $\mathrm{OA}(N, k, s, t)$ is also denoted by $\mathrm{OA}_\lambda(t, k, s)$.

14.9.8 Remark From the definition, an orthogonal array of strength t is also an orthogonal array of strength t' for all $1 \leq t' \leq t$.

14.9.9 Theorem [355, 1447] Let C be a linear code over $\mathbb{F}_q$ with words of length n. Then the $n \times |C|$ array formed with the words of C as the columns is a (linear) orthogonal array of maximal strength t if and only if $C^\perp$, its dual code, has minimum weight $t + 1$.

14.9.10 Remark The half of Theorem 14.9.9 that gives the strength of the orthogonal array from the minimum weight of the dual code was known as early as 1947 [1447, 1715]. Delsarte was able to generalize Theorem 14.9.9 to the case where the code and the orthogonal array are not required to be linear [795]. We can extend Theorem 14.9.9 and exactly determine the number of times each vector appears in any $(t + 1) \times n$ submatrix of the orthogonal array.

14.9.11 Theorem [2190] Let C be a linear code of length n over $\mathbb{F}_q$ and assume that the words of C form the columns of an orthogonal array of strength t. Then for any $t + 1$-subset $T = \{i_1, \ldots i_t\} \subset \{1, \ldots, n\}$ and for any $t + 1$-tuple $b \in \mathbb{F}_q^{t+1}$, the number of times that b appears as a column of the $(t + 1) \times n$ submatrix determined by T, $\lambda_b^T(C)$, is

$$\lambda_b^T(C) = \begin{cases} |C|/q^t & \text{if there is no } u \in C^\perp \text{ with support } T; \\ |C|/q^{t-1} & \text{if there exists a } u \in C^\perp \text{ with support } T \text{ and } u_{i_j} = b_j \text{ for } i_j \in T; \\ 0 & \text{otherwise.} \end{cases}$$

14.9.12 Theorem [2190] Let f be a primitive polynomial of degree m over $\mathbb{F}_q$ and let C_n^f be the set of all subintervals of the shift-register sequence with length n generated by f, together with the zero vector of length n. The dual code of C_n^f is given by

$$(C_n^f)^\perp = \{(b_1, \ldots, b_n) : \sum_{i=0}^{n-1} b_{i+1} x^i \text{ is divisible by } f\}.$$

14.9.13 Remark [2190] Munemasa only proves Theorem 14.9.12 over $\mathbb{F}_2$ but the proof works more generally for any finite field.

14.9.14 Remark [2339] The primitivity condition in Theorem 14.9.12 can be substantially relaxed to polynomials with distinct roots.

14.9.15 Remark The combined effect of Theorems 14.9.9 and 14.9.12 is that to know the strength of the orthogonal array derived from a polynomial f, and its shift register sequences, it is essential to know about the weights of multiples of f.

14.9.1.3 Application of polynomials to a card trick

14.9.16 Remark Although the weight of multiples of primitive $f = x^5 + x^2 + 1 \in \mathbb{F}_2[x]$ is not relevant to this application to a card trick, the low weight of f itself facilitates the mental arithmetic so we include this application in this subsection.

14.9.17 Remark The polynomial $f(x) = x^5 + x^2 + 1 \in \mathbb{F}_2[x]$ is primitive and generates the binary shift register sequence with the property that $a_{k+5} = a_k + a_{k+2}$

$$0000100101100111110001101110101.$$

14.9.18 Remark The set of cards from a standard deck which contains Ace, 2, 3, 4, 5, 6, and 7 of each suit and the 8 of spades, clubs and hearts can be encoded uniquely with the non-zero binary words of length 5. The first digit encodes the cards color, 0 for red and 1 for black. The second digit encodes whether the suit is major or minor in bridge: 0 for clubs or diamonds; 1 for hearts or spades. The remaining three digits encode the value of the card via the last three digits in the binary representation of the card's value: 000 for 8, 001 for Ace, 010 for 2, 011 for 3, 100 for 4, 101 for 5, 110 for 6, and 111 for 7. This encoding has the property that the first digit in a card's code corresponds to the color of that card. Other encodings have the required properties as well [827].

14.9.19 Remark Using the shift register sequence from Remark 14.9.17 and the card encoding from Remark 14.9.18 we obtain the following sequence of cards:

$$A\diamondsuit, 2\diamondsuit, 4\diamondsuit, A\heartsuit, 2\clubsuit, 5\diamondsuit, 3\heartsuit, 6\clubsuit, 4\heartsuit, A\spadesuit, 3\clubsuit, 7\diamondsuit, 7\heartsuit, 7\spadesuit, 6\spadesuit, 4\spadesuit,$$
$$8\spadesuit, A\clubsuit, 3\diamondsuit, 6\diamondsuit, 5\heartsuit, 3\spadesuit, 7\clubsuit, 6\heartsuit, 5\spadesuit, 2\spadesuit, 5\clubsuit, 2\heartsuit, 4\clubsuit, 8\heartsuit, 8\clubsuit$$

14.9.20 Remark A deck of these 31 cards arranged in this order looks upon casual inspection to be randomly ordered. The deck can be cut arbitrarily many times (since the shift register sequence is cyclic) before removing five cards in sequence from the top of the deck. With the knowledge which cards are black, the identity of all five chosen cards can be determined [826].

14.9.21 Remark Due to the low weight of primitive $f = x^5 + x^2 + 1$, the encoding scheme and the generating polynomial are simple enough to be quickly calculated mentally which is important for the appearance of the trick [826].

14.9.22 Remark Much can be done to augment the impression this trick makes on an audience. For ideas see [826, 827, 2155]. Two sets of these 31 cards with identical backs can be placed in this order repeated to give the impression of a more normal sized deck.

14.9.23 Remark The $8\diamondsuit$, corresponding to the binary string 00000, can be added to the deck between the $8\clubsuit$ and $A\diamondsuit$. This deviation from the linear shift register can simply be memorized ad-hoc or a new, nonlinear shift register sequence memorized:

$$a_{k+5} = (1 + \overline{a_{k+1}} \cdot \overline{a_{k+2}} \cdot \overline{a_{k+3}} \cdot \overline{a_{k+4}})(a_k + a_{k+2}) + (\overline{a_k} \cdot \overline{a_{k+1}} \cdot \overline{a_{k+2}} \cdot \overline{a_{k+3}} \cdot \overline{a_{k+4}}),$$

where $\overline{a_i}$ is the complement of a_i.

14.9.24 Remark For other mathematical card tricks see [216, 826, 827, 2155].

14.9.25 Remark The applications discussed in Remarks 14.9.2 through 14.9.15 strongly motivate researching the distributions and patterns of weights of multiples of polynomials f over finite fields. Subsection 14.9.2 gives a summary of the knowledge in this area to date.

14.9.2 Weights of multiples of polynomials

14.9.26 Remark Polynomials in $\mathbb{F}_2[x]$ which have large weight or large degree will sometimes be given in hexadecimal notation. For example the polynomial

$$f = x^8 + x^7 + x^6 + x^5 + x + 1 = 1x^8 + 1x^7 + 1x^6 + 1x^5 + 0x^4 + 0x^3 + 0x^2 + 1x^1 + 1x^0$$

is 111100011 in binary notation and, grouping these from the right into fours, is 1E3 in hexadecimal notation. The use of the two notations for polynomials will always be clear in the context. Be aware that some authors in the literature denote binary polynomials in hexidecimal *after deleting* the rightmost 1, since most polynomials used in applications have a constant term 1, so it can be assumed present in many contexts.

14.9.27 Definition The set of polynomials of degree d in $\mathbb{F}_q[x]$ is denoted by $\mathbf{P}_{q,d}$. For $f \in \mathbb{F}[x]$, the dual code of length n, $(C_n^f)^\perp$, defined in Theorem 14.9.12 can be identified with all polynomials divisible by f of degree less than n. The minimum weight of a polynomial from this set is denoted by $d((C_n^f)^\perp)$. This is also the minimum weight of the code $(C_n^f)^\perp$.

14.9.28 Remark We begin with some general bounds on $d((C_n^f)^\perp)$, followed by results for polynomials f of specific degree and end with results for polynomials f of specific weights.

14.9.2.1 General bounds on $d((C_n^f)^\perp)$

14.9.29 Proposition An application of Theorem 14.9.12 with bounds on the period of polynomials gives that if $f \in \mathbf{P}_{q,m}$, then $d((C_n^f)^\perp) = 2$ for all $n \geq q^m - 1$.

14.9.30 Theorem [2069] Let $f \in \mathbf{P}_{2,m}$ and $0 \leq t \leq (m-1)/2$. Let $n_1(t)$ be the smallest positive integer such that

$$\sum_{j=0}^{t+1} \binom{n_1(t)}{j} > 2^m.$$

Set $n_2(0) = \infty$ and for $t > 0$, let $n_2(t) = 2^{\lfloor (m-1)/t \rfloor} - 1$. If $n_1(t) < n_2(t)$, then for all $n_1(t) \leq n \leq n_2(t)$, $d((C_n^f)^\perp) \leq 2t + 2$. In other words, for such n, there will always be a multiple of f of weight less than $2t + 3$ and degree less than n.

14.9.31 Theorem [2069] Let $e = \lfloor (m-1)/t \rfloor$ and $n_2(t) = 2^e - 1$. Let α be a primitive element in $\mathbb{F}_{2^e}$ and $M^{(i)}(x)$ be the minimal polynomial of α^i. Let

$$g = \operatorname{lcm}\{M^{(i)}(x) | 0 \leq i \leq 2t\},$$

then $d((C_{2^e-1}^g)^\perp) \geq 2t + 2$ and the BCH code (see Section 15.1) generated by g can be truncated to a code meeting the bound in Theorem 14.9.30 for any admissible $n_1(t) \leq n \leq n_2(t)$.

14.9.32 Proposition [2069] In Theorem 14.9.30, $n_1(t) \leq t + 2^{m/(t+1)}(t+1)!^{1/(t+1)}$, and whenever $m > (t+1)^2 + t(t+1)\log_2(t+1)$, we have $n_1(t) < n_2(t)$.

14.9.33 Theorem [1579] If $f \in \mathbf{P}_{2,m}$ is primitive and if $g = x^n + x^k + 1$ is the trinomial multiple of f with minimum degree then

$$n \leq \frac{2^m + 2}{3}.$$

14.9.34 Proposition If $x + 1$ is a factor of $f \in \mathbb{F}_2[x]$ then f does not divide any polynomials of odd weight.

14.9.35 Lemma [555] Let $f \in \mathbb{F}_2[x]$ have simple roots, period n and suppose $(1+x)$ is a factor of f. If $d((C_n^f)^\perp) = d$ then $d((C_{n+1}^{(x+1)f})^\perp) = d$ and $d((C_j^{(x+1)f})^\perp) = 4$ for $n+2 \le j \le 2n$.

14.9.36 Theorem [1579] Let $f \in \mathbb{F}_2[x]$ be an irreducible polynomial with period ρ. Then f divides a trinomial if and only if $\gcd(x^\rho + 1, (x+1)^\rho + 1) \neq 1$.

14.9.37 Theorem [1579] If $f \in \mathbf{P}_{2,m}$ is primitive and if $g = x^n + x^k + 1$ is a trinomial divisible by f then n and k belong to the same-length cyclotomic coset modulo $2^m - 1$.

14.9.38 Theorem [1579] All primitive $f \in \mathbf{P}_{2,m}$ divide some 4-nomial of degree no bigger than

$$\left\lfloor \frac{1 + \sqrt{1 + 4.2^{m+1}}}{2} \right\rfloor.$$

14.9.39 Theorem [1579] For a given $t \ge 2$ and $s \ge 1$, if m is such that

$$1.548^m - 1 \ge (t-1)\binom{m^s + 1}{t}$$

then there exists at least one primitive polynomial of degree m which does not divide any t-nomial of degree less than or equal to m^s.

14.9.40 Theorem [1981] Let $f \in \mathbf{P}_{2,m}$ be a primitive t-nomial. Then there exists a primitive $g \in \mathbf{P}_{2,m}$ which divides some t-nomial of degree sm (s odd) when $\gcd(s, 2^m - 1) = 1$. Moreover $g = \gcd(f(x^s), x^{2^m - 1} - 1)$ is such a polynomial.

14.9.41 Remark The previous results give information about multiples of f that can have small degree relative to the period of f. The following gives information about multiples of f that have relatively large degree.

14.9.42 Remark Let $f \in \mathbb{F}_q[x]$ be primitive of degree m. Let $n = q^m - 1$ and T_2 be the set of binomials of the form $x^i - x^j$, satisfying $0 \le i < j$ with $i \equiv j \pmod n$. Let T_i be the set of all linear combinations of binomials from T_2 which have weight i. Finally define $\mu : \mathbb{F}_q[x] \to \mathbb{F}_q[x]$ by $\mu(\sum_{i=0}^d a_i x^i) = \sum_{i=0}^d a_i x^{i \,(\mathrm{mod}\ n)}$.

14.9.43 Theorem [2497] Suppose that g is a polynomial of weight w and write

$$g = g_1 + g_2$$

where $g_1 \in T_i$, $g_2 \in \mathbb{F}_q[x]$ has weight j, no two exponents of g_2 are congruent modulo n, and the terms of g_1 and g_2 are disjoint (i.e. $w = i + j$). Then g is divisible by f if and only if $\mu(g_2)$ is divisible by f.

14.9.44 Remark In [2497], Theorem 14.9.43 is only stated and proved over $\mathbb{F}_2$. It is true for all finite fields $\mathbb{F}_q$.

14.9.45 Remark Using the fact that f divides $x^{n'} + a$, with $n' = (q^m - 1)/(q-1)$ for some unique $a \in \mathbb{F}_q$, and letting T being the set of corresponding binomials, Theorem 14.9.43 can be further generalized with an increase in the complexity of the statement.

14.9.46 Remark There have also been some interesting results on enumeration and probability of multiples with given weights. We discuss this next.

14.9.47 Theorem [1579] Given $t \ge 2$ and $s \ge 1$, if m is such that $\phi(2^m - 1) > (t-1)\binom{m^s+1}{t}$, then the probability that a randomly chosen primitive polynomial of degree m does not divide any t-nomial of degree less than or equal to m^s is at least

$$1 - \frac{(t-1)\binom{m^s+1}{t}}{\phi(2^m - 1)},$$

where ϕ denotes Euler's function.

14.9.48 Theorem [1579] There exist primitive polynomials of degree m which divide a trinomial of degree $3m$ and a 4-nomial of degree less than $6m$.

14.9.49 Theorem [1352] Let $N_{m,t}$ denote the number of t-nomial multiples with degree no more than $2^m - 2$ of a primitive polynomial of degree m. Then $N_{m,2} = N_{m,1} = 0$ and

$$N_{m,t} = \frac{\binom{2^m-2}{t-2} - N_{m,t-1} - \frac{t-1}{t-2}(2^m - t + 1)N_{m,t-2}}{t-1}.$$

14.9.50 Remark See [1352] for discussion and results for solving this recurrence, and [1821] for an alternative presentation.

14.9.51 Theorem [1352] Given any primitive polynomial of degree m, the sum of the degrees of all its t-nomial multiples is

$$\frac{t-1}{t}(2^m - 1)N_{m,t}.$$

14.9.52 Theorem [1352] Given any primitive polynomial f of degree m, the average degree of its t-nomial multiples with degree no more than $2^m - 2$ is equal to the average of the maximum of all the distinct $(t-1)$-tuples from 1 to $2^m - 2$.

14.9.53 Theorem [1352] Given a primitive polynomial f of degree m, under the assumption that t-nomial multiples of f are distributed as $(t-1)$-tuples, there exists a t-nomial multiple g of f such that the degree of g is less than or equal to

$$2^{\frac{m}{t-1} + \log_2(t-1) + 1}.$$

14.9.54 Remark The assumption in Theorem 14.9.53 is motivated by Theorem 14.9.52 and empirical evidence. See [1352] for precise definition of the assumption and detailed discussion.

14.9.55 Remark Theorem 14.9.53 implies that it is highly likely to get a trinomial multiple with degree no more than $2^{m/2+2}$. This is in contrast to the bound of $(2^m + 2)/3$ from Theorem 14.9.33. In general Theorem 14.9.53 suggests that to avoid sparse multiples, f must be picked with very large degree.

14.9.56 Remark In [1981], Maitra, Gupta, and Venkateswarlu extend this enumerative and probabilistic analysis to include the product of primitive polynomials.

14.9.2.2 Bounds on $d((C_n^f)^\perp)$ for polynomials of specific degree

14.9.57 Proposition The bounds on weights of multiples of *all* polynomials from degree 4 to degree 16 and degrees 24 and 32 in $\mathbb{F}_2[x]$ are given in Table 14.9.2.2. For degrees $4 \le m \le 16$, Koopman and Chakravarty exhaustively searched all polynomials of degree m and all their multiples of degrees $m + 8 \le n \le m + 2048$ [1780]. The $m = 16$ results are from the theoretical work of Merkey and Posner [2069] and exhaustive searches by Castagnoli, Ganz, and Graber [556]. The bounds on weights of multiples of degree 24 polynomials, which are less complete than those for smaller m, are the work of Merkey and Posner [2069] and searches by Castagnoli, Ganz, and Graber [556] and Ray and Koopman [2423]. In all cases for $m = 24$ polynomials attaining the bounds are reported to be known although the specific polynomials have not been published [556, 2069, 2423]. The even more incomplete results for $m = 32$ are reported in [556, 2069].

14.9.58 Example Table 14.9.2.2 gives bounds that apply to *every* polynomial with the given degree. To aid the reading of Table 14.9.2.2, we give an example from it. The information from the

deg(f)	degree range of multiples of f	upper bound on $d(C_n^f)^\perp$	polynomial (in hexadecimal notation) attaining the bound
4	$12 \le n \le 15$	3	$f = 13$
5	$13 \le n \le 15$	4	$f = 2B$
	$16 \le n \le 31$	3	$f = 25$
6	$14 \le n \le 31$	4	$f = 59$
	$32 \le n \le 63$	3	$f = 43$
7	$15 \le n \le 63$	4	$f = B7$
	$64 \le n \le 127$	3	$f = 91$
8	$16 \le n \le 17$	5	$f = 139$
	$18 \le n \le 127$	4	$f = 12F$
	$128 \le n \le 255$	3	$f = 14D$
9	$n = 17$	6	$f = 13C$
	$18 \le n \le 22$	5	$f = 30B$
	$23 \le n \le 255$	4	$f = 297$
	$256 \le n \le 511$	3	$f = 2CF$
10	$18 \le n \le 22$	6	$f = 51D$
	$23 \le n \le 31$	5	$f = 573$
	$32 \le n \le 511$	4	$f = 633$
	$512 \le n \le 1023$	3	$f = 64F$
11	$19 \le n \le 23$	7	$f = AE1$
	$24 \le n \le 33$	6	$f = A65$
	$34 \le n \le 36$	5	$f = BAF$
	$37 \le n \le 1023$	4	$f = B07$
	$1024 \le n \le 2047$	3	$f = C9B$
12	$20 \le n \le 23$	8	$f = 149F$
	$24 \le n \le 39$	6	$f = 1683$
	$40 \le n \le 65$	5	$f = 11F1$
	$66 \le n \le 2047$	4	$f = 180F$
	$2048 \le n \le 2060$	3	$f = 16EB$
13	$21 \le n \le 24$	8	$f = 216F$
	$n = 25$	7	$f = 254B$
	$26 \le n \le 65$	6	$f = 3213$
	$66 \le n \le 2061$	4	$f = 2055$
14	$22 \le n \le 25$	8	$f = 46E3$
	$26 \le n \le 27$	7	$f = 5153$
	$28 \le n \le 71$	6	$f = 6E57$
	$72 \le n \le 127$	5	$f = 425B$
	$128 \le n \le 2062$	4	$f = 43D1$
15	$23 \le n \le 27$	8	$f = C617$
	$28 \le n \le 31$	7	$f = B7AB$
	$32 \le n \le 129$	6	$f = AE75$
	$128 \le n \le 191$	5	$f = D51B$
	$192 \le n \le 2063$	4	$f = 92ED$
16	$n = 18$	12	$f = 15BED$
	$19 \le n \le 21$	10	$f = 1D22F$
	$n = 22$	9	$f = 18F57$
	$23 \le n \le 31$	8	$f = 11FB7$
	$32 \le n \le 35$	7	$f = 126B5$
	$36 \le n \le 151$	6	$f = 13D65$
	$152 \le n \le 257$	5	$f = 15935$
	$258 \le n \le 32767$	4	$f = 1A2EB$
	$32768 \le n \le 65535$	3	$f = 1002D$
24	$18 \le n \le 47$	12	
	$48 \le n \le 50$	10	
	$51 \le n \le 63$	9	
	$64 \le n \le 129$	8	
	$130 \le n \le 255$	7	
	$466 \le n \le 2^{11} - 1$	6	
	$5793 \le n \le 2^{23} - 1$	4	
32	$n = 18$	12	
	$568 \le n \le 2^{10} - 1$	8	
	$2954 \le n \le 2^{15} - 1$	6	
	$92682 \le n \le 2^{31} - 1$	4	

Table 14.9.1 Bounds on weights of multiples of degree n polynomials for $4 \le n \le 16$.

			minimum distance					
f	standard	$d(C_n^f)^\perp$:	12	11	10	9	8	7
13D65	IEC TC57 after 1990	ranges of n:			[17,20]		[21,22]	
1F29F		ranges of n:	17				[18,22]	
15B93	IEC TC57 before 1990	ranges of n:			[17,19]		[20,25]	
15935		ranges of n:				[17,19]	[20,24]	[25,26]
16F63	IEEE WG77.1	ranges of n:		17	18			[19,29]
1A2EB		ranges of n:			[17,18]		[19,27]	
1011B		ranges of n:						
1A097	IBM SDLC	ranges of n:					[17,24]	
11021	CRC-CCITT	ranges of n:						
18005	CRC-ANSI	ranges of n:						

			minimum distance			
f	standard	$d(C_n^f)^\perp$:	6	5	4	2
13D65	IEC TC57 after 1990	ranges of n:	[23,151]			[151,∞]
1F29F		ranges of n:	[23,130]		[131,258]	[259,∞]
15B93	IEC TC57 before 1990	ranges of n:	[26,128]	[129,254]		[255,∞]
15935		ranges of n:	[27,51]	[52,257]		[258,∞]
16F63	IEEE WG77.1	ranges of n:	30	[31,255]		[256,∞]
1A2EB		ranges of n:	[28,109]		[110,32767]	[32768,∞]
1011B		ranges of n:	[17,115]		[116,28658]	[28659,∞]
1A097	IBM SDLC	ranges of n:	[25,83]		[84,32766]	[32767,∞]
11021	CRC-CCITT	ranges of n:			[17,32767]	[32768,∞]
18005	CRC-ANSI	ranges of n:			[17,32767]	[32768,∞]

Table 14.9.2 Distance profiles of specific degree 16 polynomials.

third line of the section for polynomials of degree 11, indicates that for every binary degree 11 polynomial $f \in \mathbf{P}_{2,11}$, there exists multiples of f which have degrees 34, 35, and 36 and weight less than or equal to 5. The polynomial cited in the last column, $f(x) = BAF = x^{11}+x^9+x^8+x^7+x^5+x^3+x^2+x+1$, meets this bound tightly; that is, all of its multiples of degree 34, 35, or 36 have weight 5 or above.

14.9.59 Remark In Table 14.9.2.2, three of the degree 16 polynomials meeting the bounds are known to be unique. For $d(C_n^f)^\perp = 6$, $f = 13D65$ and for $d(C_n^f)^\perp = 4$, $f = 1A2EB$ are the unique tight polynomials, up to reciprocal. For $d(C_n^f)^\perp = 5$, $f = 15935$ is unique [556].

14.9.60 Remark In contrast to Table 14.9.2.2, Tables 14.9.2 through 14.9.4 give the distance distributions of multiples of a few, specific polynomials for degrees 16, 24, and 32.

14.9.61 Remark [556] Table 14.9.2 gives the distance profiles of ten specific polynomials in $\mathbf{P}_{2,16}$ found by Castagnoli, Ganz and Graber. They exhaustively searched all degree 16 polynomials for those with optimum profiles. The polynomial $f = 1F29F$ is the unique polynomial with $d(C_{130}^f)^\perp = 6$ and $d(C_{258}^f)^\perp = 4$. Up to reciprocal, $f = 1011B$ is the unique polynomial with $d(C_{28658}^f)^\perp = 4$ and $d(C_{115}^f)^\perp = 6$. The authors of [556] suggest that any cyclic redundancy check polynomials of degree 16 should be chosen only from the list $\{13D65, 1F29F, 15935, 1A2EB, 1011B\}$.

14.9.62 Example The third polynomial in Table 14.9.2 gives the distance distribution for the polynomial $f(x) = 15B93 = x^{16}+x^{14}+x^{12}+x^{11}+x^9+x^8+x^7+x^4+x+1$, which was the IEC TC57 standard cyclic redundancy check polynomial until 1990. All its multiples of degrees 17–19 have weight 10 or more. All its multiples of degrees 20–25 have weight 8 or more. All its multiples of degrees 26–128 have weight 6 or more. All its multiples of degree 129–254 have weight 5 or more. All its multiples of degrees 255 and higher have weight at least 2. For each degree there exist specific multiples that attain these lower bounds; for example there is a degree 17 multiple of f with weight 10.

14.9.63 Remark Table 14.9.3 gives the distance distribution for some specific polynomials of degree 24. All were constructed via the generalized BCH code method: multiplying together

		minimum distance							
f	$d(C_n^f)^\perp$:	16	15	14	12	11	10	9	ref.
1323009	ranges of n:								[555, 2069]
1401607	ranges of n:								[555, 2069]
1805101	ranges of n:								[2069]
15D6DCB	ranges of n:			25	26		[27,36]		[555]
17B01BD	ranges of n:	[25,26]					[27,41]		[555]
131FF19	ranges of n:		25				[26,33]		[555]
15BC4F5	ranges of n:		[25,26]		[27,28]	[29,31]	[32,33]	[34,35]	[555]
1328B63	ranges of n:				[25,30]		[31,36]		[555]

		minimum distance						
f	$d(C_n^f)^\perp$:	8	7	6	5	4	2	ref.
1323009	ranges of n:	[25,68]		[69,2048]		[2049,4094]	[4095,∞]	[555, 2069]
1401607	ranges of n:	[25,55]		[56,2048]		[2049,4094]	[4095,∞]	[555, 2069]
1805101	ranges of n:			[25,1023]				[2069]
15D6DCB	ranges of n:	[37,83]		[84,2050]		[2051,4098]	[4099,∞]	[555]
17B01BD	ranges of n:	[42,95]		[96,2048]		[2049,4094]	[4095,∞]	[555]
131FF19	ranges of n:		[34,37]	[38,252]	[253,4097]		[4098,∞]	[555]
15BC4F5	ranges of n:	[36,41]	[42,47]	[78,217]	[218,4095]		[4096,∞]	[555]
1328B63	ranges of n:	[37,61]		[62,846]		[847,$^{23}-1$]	[2^{23},∞]	[555]

Table 14.9.3 Distance profiles of specific degree 24 polynomials.

minimal polynomials of elements from $\mathbb{F}_{2^e}$ and small factors, x and $x+1$ [555, 2069]. For discussion of BCH codes, see Section 15.1.

14.9.64 Remark Table 14.9.4 gives the distance distribution for some specific polynomials of degree 32. All were obtained via the generalized BCH code method: multiplying together minimal polynomials of elements from $\mathbb{F}_{2^e}$ and small factors, x and $x+1$ [555, 2069].

14.9.65 Remark For the third polynomial in Table 14.9.4, used in many standards, Jain [1578] has determined and published many of the minimum degree polynomials that establish the ranges given in Table 14.9.4. The actual polynomials are given in Table 14.9.5. Jain has determined all the polynomials that f divides which have the pattern of at most three burst errors of length 4 each and several other specific patterns of errors.

14.9.66 Remark Koopman has performed an exhaustive search over all $f \in \mathbf{P}_{2,32}$ for $40 \le n \le 131104$. His primary concern was finding cyclic redundancy check polynomials which were simultaneously good at typical Ethernet *maximum transmission unit* (MTU) lengths, $n = 12112$, and much longer lengths $n \ge 64,000$, so although his search has in principle solved the $d(C_n^f)^\perp$ problem for all n in this range he did not specifically publish these, rather he highlights the last three polynomials given in Table 14.9.4 and compares them to the others [1779]. Discussion of the benefits and costs of using these various polynomials in different scenarios appear in [555, 1578, 1779, 2069].

14.9.2.3 Bounds on $d((C_n^f)^\perp)$ for polynomials of specific weight

14.9.67 Remark We now present divisibility results that are organized by the weight of the base polynomial.

14.9.68 Theorem [2190] Let $f(x) = x^m + x^l + 1$ be a trinomial over $\mathbb{F}_2$ such that $\gcd(m, l) = 1$. If g is a trinomial multiple of f of degree at most $2m$, then

1. $g(x) = x^{\deg g - m} f(x)$;
2. $g(x) = f(x)^2$;
3. $g(x) = x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 + x + 1)$ or; its reciprocal,

		minimum distance											
f	$d(C_n^f)^\perp$:	20	18	17	16	15	14	13	12	11	10	9	8	ref.
1404098E2	ranges of n:										[33,78]		[79,1023]	[555, 2069]
10884C912	ranges of n:										[33,79]		[80,1023]	[555, 2069]
104C11DB7*	ranges of n:					[33,42]			[43,44]	[45,53]	[54,66]	[67,89]	[90,123]	[555, 1578]
1F1922815	ranges of n:						[33,44]		[45,48]		[49,98]		[99,1024]	[555]
1F4ACFB13	ranges of n:	33	[34,35]		36		37		[38,43]		[44,56]		[57,306]	[555]
1A833982B	ranges of n:					[33,35]			[36,49]	[50,53]	[54,59]		[60,90]	[555]
1572D7285	ranges of n:			[33,34]			35	[36,38]		[39,52]	[53,68]	[69,80]	[81,110]	[555]
11EDC6F41	ranges of n:		33		[34,38]		[39,40]		[41,52]		[53,79]		[80,209]	[555]
1741B8CD7	ranges of n:								[40,48]		[49,50]		[51,184]	[1779]
132583499	ranges of n:								[40,48]		[49,58]		[59,166]	[1779]
120044009	ranges of n:													[1779]
100210801	ranges of n:													[1779]

		minimum distance					
f	$d(C_n^f)^\perp$:	7	6	5	4	3	2	ref.
1404098E2	ranges of n:						[1024,∞]	[555, 2069]
10884C912	ranges of n:						[1024,∞]	[555, 2069]
104C11DB7*	ranges of n:	[124, 203]	[204,300]	[301,3006]	[3007,91639]	[91640,$2^{32}-1$]	[2^{32},∞]	[555, 1578]
1F1922815	ranges of n:				[1025,2046]		[2047,∞]	[555]
1F4ACFB13	ranges of n:		[307,32768]		[32769,65534]		[65535,∞]	[555]
1A833982B	ranges of n:	[91,113]	[114,1092]	[1093,65537]			[65538,∞]	[555]
1572D7285	ranges of n:	[111,266]	[267,1029]	[1030,65535]			[65536,∞]	[555]
11EDC6F41	ranges of n:		[210,5275]		[5276,$2^{31}-1$]		[2^{31},∞]	[555]
1741B8CD7	ranges of n:		[185,16392]		[16393,114695]		[114696,∞]	[1779]
132583499	ranges of n:		[167,32769]		[32770,65538]		[65539,∞]	[1779]
120044009	ranges of n:		[40,32770]		[32771,65538]		[65539,∞]	[1779]
100210801	ranges of n:			[40,65537]			[65538,∞]	[1779]

Table 14.9.4 Distance profiles of degree 32 polynomials.
*The third polynomial $f = 104C11DB7$ is used in the FDDI, IEEE 802, AUTODIN-II standards.

t	smallest degree t-nomial divisible by f
3	$x^{91639} + x^{41678} + 1$
4	$x^{3006} + x^{2846} + x^{2215} + 1$
5	$x^{300} + x^{155} + x^{117} + x^{89} + 1$
6	$x^{203} + x^{196} + x^{123} + x^{85} + x^{79} + 1$
7	$x^{123} + x^{120} + x^{80} + x^{74} + x^{58} + x^{46} + 1$
8	$x^{89} + x^{88} + x^{41} + x^{36} + x^{16} + x^3 + x^2 + 1$
9	$x^{66} + x^{57} + x^{37} + x^{32} + x^{31} + x^{16} + x^7 + x^5 + 1$
10	$x^{53} + x^{38} + x^{36} + x^{33} + x^{30} + x^{27} + x^{26} + x^7 + x^3 + 1$
11	$x^{44} + x^{43} + x^{41} + x^{37} + x^{35} + x^{32} + x^{31} + x^{16} + x^7 + x^5 + 1$
12	$x^{42} + x^{30} + x^{26} + x^{24} + x^{21} + x^{18} + x^{13} + x^8 + x^7 + x^5 + x^3 + 1$
13	$x^{42} + x^{40} + x^{37} + x^{35} + x^{33} + x^{29} + x^{28} + x^{20} + x^{18} + x^{15} + x^6 + x^1 + 1.$

Table 14.9.5 Smallest t-nomial divisors of $f = 104C11DB7$.

4. $g(x) = x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$.

14.9.69 Theorem [820] Let $f(x) = x^m + x^l + x^k + x^j + 1$ be a pentanomial over $\mathbb{F}_2$ such that $\gcd(m, l, k, j) = 1$. If g is a trinomial of degree at most $2m$ divisible by f, with $g = fh$, then

1. f is one of the twenty-five polynomials given in Table 14.9.6 with the corresponding h;
2. $m \equiv 1 \pmod 3$ and f, g, h are as follows

$$\begin{aligned} f(x) &= 1 + x + x^2 + x^{m-3} + x^m \\ &= (1 + x + x^2)(1 + x^{m-3} + x^{m-2}), \\ h(x) &= (1 + x) + (x^3 + x^4) + \cdots + (x^{m-7} + x^{m-6}) + x^{m-4}, \\ f(x)h(x) = g(x) &= 1 + x^{2m-6} + x^{2m-4}; \quad \text{or} \end{aligned}$$

3. f is the reciprocal of one of the polynomials listed in the previous items.

No.	$f(x)$	$h(x)$	type
1	$x^5 + x^4 + x^3 + x^2 + 1$	$x^3 + x^2 + 1$	p
2	$x^5 + x^3 + x^2 + x + 1$	$x^3 + x + 1$	p
3	$x^5 + x^3 + x^2 + x + 1$	$x^4 + x + 1$	p
4	$x^5 + x^4 + x^3 + x + 1$	$x^2 + x + 1$	p
5	$x^6 + x^5 + x^4 + x^3 + 1$	$x^4 + x^3 + 1$	r
6	$x^6 + x^4 + x^2 + x + 1$	$x^3 + x + 1$	i
7	$x^6 + x^4 + x^3 + x + 1$	$x^2 + x + 1$	p
8	$x^6 + x^5 + x^2 + x + 1$	$x^5 + x^4 + x^3 + x + 1$	p
9	$x^6 + x^5 + x^3 + x + 1$	$x^2 + x + 1$	r
10	$x^7 + x^4 + x^2 + x + 1$	$x^3 + x + 1$	r
11	$x^7 + x^4 + x^3 + x^2 + 1$	$x^3 + x^2 + 1$	p
12	$x^7 + x^5 + x^2 + x + 1$	$x^7 + x^6 + x^5 + x^4 + x^3 + x + 1$	p
13	$x^7 + x^5 + x^3 + x^2 + 1$	$x^5 + x^4 + x^3 + x^2 + 1$	r
14	$x^8 + x^5 + x^3 + x + 1$	$x^5 + x^4 + x^2 + x + 1$	p
15	$x^8 + x^5 + x^3 + x^2 + 1$	$x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1$	p
16	$x^8 + x^6 + x^3 + x + 1$	$x^6 + x^4 + x^2 + x + 1$	r
17	$x^8 + x^7 + x^5 + x^2 + 1$	$x^6 + x^5 + x^4 + x^2 + 1$	r
18	$x^9 + x^6 + x^5 + x^2 + 1$	$x^8 + x^5 + x^4 + x^2 + 1$	i
19	$x^9 + x^7 + x^4 + x^3 + 1$	$x^8 + x^6 + x^4 + x^3 + 1$	i
20	$x^9 + x^8 + x^5 + x^2 + 1$	$x^6 + x^5 + x^4 + x^2 + 1$	r
21	$x^{10} + x^4 + x^3 + x^2 + 1$	$x^8 + x^7 + x^4 + x^2 + 1$	i
22	$x^{10} + x^7 + x^2 + x + 1$	$x^6 + x^4 + x^3 + x + 1$	r
23	$x^{11} + x^7 + x^6 + x^2 + 1$	$x^8 + x^7 + x^4 + x^2 + 1$	r
24	$x^{13} + x^{10} + x^2 + x + 1$	$x^9 + x^7 + x^6 + x^4 + x^3 + x + 1$	r
25	$x^{13} + x^{10} + x^9 + x^2 + 1$	$x^{12} + x^9 + x^8 + x^6 + x^4 + x^2 + 1$	p

Table 14.9.6 Table of pentanomials which divide trinomials: 'p' in *type* indicates that the given polynomial f is primitive, 'i' indicates that f is irreducible and 'r' indicates that f is reducible.

14.9.70 Remark All primitive polynomials satisfy the gcd condition of Theorems 14.9.68 and 14.9.69, and thus, in particular, Theorems 14.9.68 and 14.9.69 hold for all primitive trinomials and pentanomials over $\mathbb{F}_2$.

14.9.71 Corollary If $f(x) = x^m + x^l + x^k + x^j + 1$ is primitive over $\mathbb{F}_2$ and not one of the exceptions given in Table 14.9.6 or their reciprocals, then, for $m < n \leq 2m$,

1. C_n^f is an orthogonal array of strength at least 3; or equivalently,
2. $(C_n^f)^\perp$, the dual code of C_n^f, has minimum weight at least 4;
3. the cyclic redundancy check code derived from f, of length n, can detect all errors in three or fewer positions;
4. the bias from the third moment of the Hamming weight in the linear feedback shift register sequence generated from f is small.

14.9.72 Theorem [820] Let $\mathbb{F}$ be any field and $f, g, h \in \mathbb{F}[x]$, $fh = g$, $w(f) = n > 1$ and $w(g) = m$. If there exists an $f_0 \in \mathbb{F}[x]$ such that $f(x) = f_0(x^k)$ for $k > 1$ then there exist $g_i \in \mathbb{F}[x]$, $w(g_i) = m_i$ for $0 \leq i < k$ such that

$$g(x) = \sum_{i=0}^{k-1} g_i(x^k)x^i \tag{14.9.1}$$

$$m = \sum_{i=0}^{k-1} m_i \text{ and } m_i \neq 1. \tag{14.9.2}$$

14.9.73 Remark Theorem 14.9.72 can be used to simplify the analysis of multiples of f. An example used in [2339] is given in Corollary 14.9.74 and was used in the proofs of Theorems 14.9.75 and 14.9.76.

14.9.74 Corollary [820] Let $\mathbb{F}$ be any field and $f, g, h \in \mathbb{F}[x]$, $fh = g$, $w(f) = n$ and $w(g) \leq 3$. If there exists $f_0 \in \mathbb{F}[x]$ such that $f(x) = f_0(x^k)$ for $k > 1$ then there exists $g_0 \in \mathbb{F}[x]$ such that $g(x) = g_0(x^k)$.

14.9.75 Theorem [820] Let $f(x) = a + bx^k + x^m$ $(a, b \neq 0)$ be a monic trinomial over $\mathbb{F}_3$. If $g(x) = c + x^n$ $(c \neq 0)$ is a monic binomial over $\mathbb{F}_3$ with degree at most $3m$ divisible by f with $g = fh$, then f and g are as given in Table 14.9.7.

Case	$f(x)$	$g(x)$
1.1	$1 + bx^{m/2} + x^m$	$-b + x^{3m/2}$
1.2	$-1 + bx^{m/2} + x^m$	$1 + x^{2m}$
1.3	$1 + bx^{m/2} + x^m$	$-1 + x^{3m}$
1.4	$a + x^{m/3} + x^m$	$-1 + x^{8m/3}$
1.5	$b + bx^{2m/3} + x^m$	$-1 + x^{8m/3}$

Table 14.9.7 Polynomials over $\mathbb{F}_3$ such that $g = fh$ for monic trinomial f and monic binomial g.

14.9.76 Theorem [820] Let $f(x) = a + bx^k + x^m$ $(a, b \neq 0)$ be a monic trinomial over $\mathbb{F}_3$. If $g(x) = c + dx^l + x^n$ $(c, d \neq 0)$ is a monic trinomial over $\mathbb{F}_3$ with degree at most $3m$ divisible by f with $g = fh$, then

1. $g = f^3$;
2. f and g are as in the Table 14.9.8;
3. f and g are reciprocals of polynomials listed in Table 14.9.8.

See Also

Case	$f(x)$	$g(x)$
1.1	$-1+bx^{m/2}+x^m$	$1-bx^{m/2}+x^{3m}$
1.2	$1+bx^{m/2}+x^m$	$b+x^{m/2}+x^{5m/2}$
1.3	$-1+bx^{m/2}+x^m$	$b-bx^m+x^{5m/2}$
1.4	$-1+bx^{m/2}+x^m$	$-b-x^{3m/2}+x^{5m/2}$
1.5	$1+bx^{m/2}+x^m$	$b+bx^{4m/2}+x^{5m/2}$
1.6	$1+bx^{m/2}+x^m$	$1+x^m+x^{2m}$
1.7	$-1+bx^{m/2}+x^m$	$b+x^m+x^{3m/2}$
1.8	$-1+bx^{m/2}+x^m$	$-b-bx^m+x^{3m/2}$
1.9	$a-x^{m/3}+x^m$	$-a-x^{m/3}+x^{3m}$
1.10	$a-x^{m/3}+x^m$	$1+x^{2m/3}+x^{8m/3}$
1.11	$a+x^{m/3}+x^m$	$a+ax^{2m/3}+x^{7m/3}$
1.12	$a-x^{m/3}+x^m$	$a-ax^{4m/3}+x^{7m/3}$
1.13	$a-x^{m/3}+x^m$	$-a+x^{5m/3}+x^{7m/3}$
1.14	$a+x^{m/3}+x^m$	$1+ax^{5m/3}+x^{2m}$
1.15	$a-x^{m/3}+x^m$	$a+ax^{4m/3}+x^{5m/3}$
1.16	$-1+bx^{m/4}+x^m$	$-b+bx^{6m/4}+x^{11m/4}$
1.17	$1+bx^{m/4}+x^m$	$1+bx^{9m/4}+x^{10m/4}$

Table 14.9.8 Table of polynomials such that $g = fh$ with f and g monic trinomials over $\mathbb{F}_3$.

§2.2 For tables of primitives of various kinds and weights.
§3.4 For results on the weights of irreducible polynomials.
§4.3 For results on the weights of primitive polynomials.
§10.2 For discussion on bias and randomness of linear feedback shift register sequences.
§14.1 For results of latin squares which are strongly related to orthogonal arrays.
§14.5 For a discussion of block designs, which include orthogonal arrays.
§15.1 Uses primitive polynomials to generate cyclic redundancy check and BCH codes.
§15.4 For results on turbo codes.
§17.3 For more discussion of applications of finite fields and polynomials.

References Cited: [146, 216, 355, 555, 556, 795, 820, 826, 827, 1352, 1447, 1481, 1578, 1579, 1610, 1715, 1779, 1780, 1821, 1932, 1981, 2060, 2069, 2155, 2190, 2339, 2423, 2497]

14.10 Ramanujan and expander graphs

M. Ram Murty, *Queen's University*
Sebastian M. Cioabă, *University of Delaware*

In the last two decades, the theory of Ramanujan graphs has gained prominence primarily for two reasons. First, from a practical viewpoint, they resolve an extremal problem in communication network theory (see for example [267, 1524]). Second, from a more aesthetic viewpoint, they fuse diverse branches of pure mathematics, namely, number theory, representa-

tion theory and algebraic geometry. The purpose of this survey is to unify some of the recent developments and expose certain open problems in the area. This survey is an expanded version of [2194] and is by no means an exhaustive one and demonstrates a highly number-theoretic bias. For other surveys, we refer the reader to [1524, 1910, 1954, 1955, 2508, 2819]. For a more up-to-date survey highlighting the connection between graph theory and automorphic representations, we refer the reader to Li's recent survey article [1912].

14.10.1 Graphs, adjacency matrices and eigenvalues

14.10.1 Definition A *graph* X is a pair (V, E) consisting of a *vertex set* $V = V(X)$ and an *edge set* $E = E(X)$ which is a multiset of unordered pairs of (not necessarily distinct) vertices. Each edge consists of two vertices that are called its *endpoints*. A *loop* is an edge whose endpoints are equal. Multiple edges are edges having the same pair of endpoints. A *simple graph* is a graph having no loops nor multiple edges. If a graph has loops or multiple edges, we will call it a *multigraph*. When two vertices u and v are endpoints of an edge, they are *adjacent* and write $u \sim v$ to indicate this fact. A *directed graph* Y is a pair (W, F) consisting of a set of vertices W and a multiset F of ordered pairs of vertices which are called *arcs*.

14.10.2 Remark All the graphs in this chapter are undirected unless stated explicitly otherwise.

14.10.3 Definition The *degree* of a vertex v of a graph X, denoted by $\deg(v)$, is the number of edges incident with v, where we count a loop with multiplicity 1. A graph X is k-regular if every vertex has degree k.

14.10.4 Proposition (Handshaking Lemma) For any simple graph X, $\sum_{v \in V(X)} \deg(v) = 2|E(X)|$. If X is a k-regular graph with n vertices, then $|E(X)| = kn/2$.

14.10.5 Definition An *adjacency matrix* $A = A(X)$ of a graph X with n vertices is an $n \times n$ matrix with rows and columns indexed by the vertices of X, where the (x, y)-th entry equals the number of edges between vertex x and vertex y. As X is an undirected graph with n vertices, the matrix $A(X)$ is symmetric and therefore, its eigenvalues $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ are real. The multiset of eigenvalues of X is the *spectrum* of X.

14.10.6 Remark We remark that the adjacency matrix defined above depends on the labeling of the vertices of X. Different labelings of the vertices of a graph X may possibly yield different adjacency matrices. However, all these adjacency matrices are similar to each other (by permutation matrices) and thus, their spectrum is the same.

14.10.7 Remark One can define an adjacency matrix of a directed graph $Y = (W, A)$ similarly. Given a labeling of the vertices W of Y, the (x, y)-th entry of the adjacency matrix corresponding to this labeling equals the number of arcs from x to y. Adjacency matrices of directed graphs may be non-symmetric.

14.10.8 Example The spectrum of the *complete graph* K_n on n vertices is $(n-1)^{(1)}, (-1)^{(n-1)}$, where the exponent signifies the multiplicity of the respective eigenvalue. The Petersen graph has spectrum $3^{(1)}, 1^{(5)}, -2^{(4)}$.

14.10.9 Theorem Let X be a graph on n vertices with maximum degree Δ and average degree $\overline{d}$. Then $\overline{d} \leq \lambda_1 \leq \Delta$ and $|\lambda_i| \leq \Delta$ for every $2 \leq i \leq n$.

14.10.10 **Definition** For a multigraph X, a *walk* of *length* r from x to y is a sequence $x = v_0, v_1, \ldots, v_r = y$ of vertices of X such that $v_i v_{i+1}$ is an edge of X for any $i = 0, 1, \ldots, r-1$. The *length* of this walk is r. A *closed walk* is a walk where the starting vertex x is the same as the last vertex y.

14.10.11 **Definition** A *path* is a walk with no repeated vertices. A *cycle* is a closed walk with no repeated vertices except the starting vertex.

14.10.12 **Remark** A word of caution must be inserted here. In graph theory literature, the distinction between a walk and a path is as we have defined it above. However, in number theory circles, the finer distinction is not made and one uses the word "path" to mean a "walk"; see for example, [2506, 2771].

14.10.13 **Definition** A graph X is *connected* if for every two distinct vertices x and y, there is a path from x to y.

14.10.14 **Proposition** For every graph X with adjacency matrix A and any integer $r \geq 1$, the (x, y)-th entry of A^r equals the number of walks of length r between x and y.

14.10.15 **Proposition** The number of closed walks of length r in a graph X with n vertices equals $\lambda_1^r + \lambda_2^r + \cdots + \lambda_n^r$.

14.10.16 **Definition** An *independent set* in a graph X is a subset of vertices that are pairwise non-adjacent. A graph X is *bipartite* if its vertex set can be partitioned into two independent sets A and B; X is *complete bipartite* and denoted by $K_{|A|,|B|}$ if it contains all the edges between A and B.

14.10.17 **Proposition** A graph is bipartite if and only if it does not contain any cycles of odd length.

14.10.18 **Theorem** If X is a k-regular and connected graph with n vertices, then $\lambda_1 = k$ and the multiplicity of k is 1 with the eigenspace of k spanned by the all 1 vector of dimension n. If X is a k-regular and connected graph, then X is bipartite if and only if $\lambda_n = -k$.

14.10.19 **Definition** If X is a k-regular and connected graph, then the eigenvalue k of X is *trivial*. All other eigenvalues of X are *non-trivial*. Let $\lambda(X) = \max |\lambda_i|$, where the maximum is taken over all non-trivial eigenvalues of X. The parameter $\lambda(X)$ is the *second eigenvalue* of X by some authors. The *second largest eigenvalue* of X is $\lambda_2(X)$ and $\lambda(X) \geq \lambda_2(X)$.

14.10.20 **Definition** The *distance* $d(x, y)$ between two distinct vertices x and y of a connected graph X is the length of a shortest path between x and y. The *diameter* D of a connected graph X is the maximum of $d(x, y)$, where the maximum is taken over all pairs of distinct vertices $x \neq y$ of X.

14.10.21 **Remark** When $k \geq 3$, if X is a k-regular and connected graph with n vertices and diameter D, then $n \leq 1 + k + k(k-1) + \cdots + k(k-1)^{D-1} = 1 + k \cdot \frac{(k-1)^D - 1}{k-2}$ and consequently, $D \geq \log_{k-1}\left(\frac{(n-1)(k-2)}{k} + 1\right) > \frac{\log(n-1)}{\log(k-1)} - \frac{\log(k/(k-2))}{\log(k-1)}$. Thus, the diameter of any connected k-regular graph is at least logarithmic in the order of the graph. The next theorem implies that when the non-trivial eigenvalues of a k-regular connected graph are small, then the above inequality is tight up to a multiplicative constant.

14.10.22 Theorem [631] If X is a connected non-bipartite k-regular graph with n vertices and diameter D, then:

$$D \leq \frac{\log(n-1)}{\log(k/\lambda(X))} + 1.$$

14.10.23 Remark Kahale [1629] obtained an upper bound on the minimum distance between i subsets of the same size of a regular graph in terms of the i-th largest eigenvalue in absolute value. Kahale also constructed examples of k-regular graphs on n vertices having $\lambda(X) = (1+o(1))2\sqrt{k-1}$ and $D = 2(1+o(1))\log_{k-1} n$ showing the previous result is asymptotically best possible. Here the $o(1)$ term tends to 0 as n goes to infinity.

14.10.24 Remark A similar result can be derived for k-regular bipartite graphs; if X is a bipartite k-regular and connected graph of diameter D, we have (see Quenell [2418])

$$D \leq \frac{\log(n-2)/2}{\log(k/\lambda'(X))} + 2,$$

where $\lambda'(X)$ is the maximum absolute value of the eigenvalues of X that are not k nor $-k$.

14.10.25 Remark Chung, Faber and Manteuffel [632] and independently, Van Dam and Haemers [2821] obtained slight improvements of the previous diameter bounds.

14.10.26 Definition The *chromatic number* $\chi(X)$ of a graph X is the minimum number of colors that can be assigned to the vertices of a graph such that any two adjacent vertices have different colors. The largest order of an independent set of vertices of X is the *independence number* of X and is denoted by $\alpha(X)$.

14.10.27 Remark The chromatic number of X is the minimum number of independent sets that partition the vertex set of X and consequently, $\chi(X) \geq \frac{|V(X)|}{\alpha(X)}$.

14.10.28 Theorem [1279] If X is a k-regular non-empty graph, then

$$\alpha(X) \leq \frac{n(-\lambda_n)}{k-\lambda_n}$$

and so

$$\chi(X) \geq 1 + \frac{k}{-\lambda_n}.$$

14.10.29 Remark An immediate consequence of the previous result is that $\alpha(X) \leq \frac{n\lambda(X)}{k+\lambda(X)}$ and $\chi(X) \geq 1 + \frac{k}{\lambda(X)}$ for any non-bipartite connected k-regular graph X. These facts show that a good upper bound for the absolute values of the non-trivial eigenvalues of a regular graph will yield non-trivial bounds for the independence and chromatic number.

14.10.30 Remark The following theorem shows that the eigenvalues of a regular graph are closely related to its edge distribution.

14.10.31 Theorem [81] If X is a k-regular connected graph with eigenvalues $k = \lambda_1 > \lambda_2 \geq \cdots \geq \lambda_n \geq -k$, let $\lambda := \max(|\lambda_2|, |\lambda_n|)$. For $S, T \subset V(X)$, denote by $e(S,T)$ the number of edges with one endpoint in S and another in T. Then for all $S, T \subset V(X)$

$$\left| e(S,T) - \frac{k|S||T|}{n} \right| \leq \lambda \sqrt{|S||T| \left(1 - \frac{|S|}{n}\right)\left(1 - \frac{|T|}{n}\right)} < \lambda\sqrt{|S||T|}.$$

14.10.32 Remark The previous theorem states that k-regular graphs X with small non-trivial eigenvalues (compared to k) have their edges uniformly distributed (similar to random k-regular

graphs). Such graphs are called *pseudorandom graphs* and are important in many situations (see Krivelevich-Sudakov's survey [1794]). Bilu and Linial [280] have obtained a converse of the previous result of Alon and Chung.

14.10.2 Ramanujan graphs

14.10.33 Definition A k-regular connected multigraph X is a *Ramanujan multigraph* if $|\lambda_i| \leq 2\sqrt{k-1}$ for every eigenvalue $\lambda_i \neq k$. A *Ramanujan graph* is a Ramanujan multigraph having no loops nor multiple edges.

14.10.34 Remark We mention that the definition of a Ramanujan graph used by other authors is slightly weaker. For example, Sarnak in [2508] calls a k-regular graph Ramanujan if $\lambda_2(X) \leq 2\sqrt{k-1}$.

14.10.35 Example The complete graph K_n is an $(n-1)$-regular Ramanujan graph as its eigenvalues are $(n-1)^{(1)}, -1^{(n-1)}$, where the exponents denote the multiplicities of the eigenvalues. The complete bipartite graph $K_{n,n}$ has eigenvalues $n^{(1)}, 0^{(2n-2)}, -n^{(1)}$ and is an n-regular Ramanujan graph.

14.10.36 Remark In [80, p.95], Alon announced a proof with Boppana of the fact that for any k-regular graph X of order n, $\lambda_2(X) \geq 2\sqrt{k-1} - O((\log_k n)^{-1})$, where the constant in the O term depends only on k. Many researchers refer to this result as the Alon-Boppana Theorem. Other researchers refer to the following statement proved by Nilli (pseudonym for Alon) in [2275] as the Alon-Boppana Theorem.

14.10.37 Theorem [2275] If X is a k-regular and connected graph with diameter $D \geq 2b+2$, then

$$\lambda_2(X) \geq 2\sqrt{k-1} - \frac{2\sqrt{k-1}-1}{b+1}.$$

14.10.38 Remark The Alon-Boppana Theorem and Remark 14.10.21 imply that if $(X_i)_{i\geq 1}$ is a sequence of k-regular and connected graphs with $\lim_{i\to+\infty} |V(X_i)| = +\infty$, then

$$\liminf_{i\to\infty} \lambda_2(X_i) \geq 2\sqrt{k-1}.$$

14.10.39 Remark The best lower bound for the second largest eigenvalue $\lambda_2(X)$ of a k-regular graph of diameter D is due to Friedman [1120] who showed that

$$\lambda_2(X) \geq 2\sqrt{k-1}\cos\theta_{k,t} \geq 2\sqrt{k-1}\cos\frac{\pi}{t+1} \tag{14.10.1}$$

where t is the largest integer such that $D \geq 2t$ and $\theta_{k,t} \in \left[\frac{\pi}{t+5}, \frac{\pi}{t+1}\right]$ is the smallest positive solution of the equation $\frac{k}{2k-2} = \frac{\sin(t+1)\theta\cos\theta}{\sin t\theta}$. The number $2\sqrt{k-1}\cos\theta_{k,t}$ is the largest eigenvalue of the k-regular tree $T_{k,t}$ of depth t; this tree has a root vertex x and exactly $k(k-1)^{i-1}$ vertices at distance i from x for each $1 \leq i \leq t$. Friedman used analytic tools involving Dirichlet and Neumann eigenvalues for graphs with boundaries to prove (14.10.1). Later, Nilli [2276] gave an elementary proof of a slightly weaker bound.

14.10.40 Remark We outline here an elementary proof of the inequality $\lambda_2(X) \geq 2\sqrt{k-1}\cos\frac{\pi}{t+1}$ for every connected k-regular graph X of diameter $D \geq 2t+2$. The first ingredient of the proof is that the largest eigenvalue of any subgraph induced by a ball of radius t of X is larger than the largest eigenvalue of $T_{k,t}$. The second is that if u and v are vertices at distance at least $2t+2$ in X, then the subgraph induced by the vertices at distance at most t from u or v

has exactly two components $X(u)$ and $X(v)$. By Cauchy eigenvalue interlacing, the second largest eigenvalue of X is greater than the minimum of the largest eigenvalue of $X(u)$ and $X(v)$ which by the previous argument is at least $2\sqrt{k-1}\cos\theta_{k,t} \geq 2\sqrt{k-1}\cos\frac{\pi}{t+1}$.

14.10.41 Remark At this point, it is worth stating that Friedman [1120] (see also Nilli [2276]) proved the stronger statement that if X is a k-regular graphs containing a subset of r points each of distance at least $2t$ from one another, then $\lambda_r(X) \geq 2\sqrt{k-1}\cos\theta_{k,t} \geq 2\sqrt{k-1}\cos\frac{\pi}{t+1}$. This implies that the r-th largest eigenvalue $\lambda_r(X)$ of any connected k-regular graph X is at least $2\sqrt{k-1}\left(1-\frac{\pi^2}{2f^2}+O(f^{-4})\right)$, where $f=\frac{\log_{k-1}(n/r)}{2}$.

14.10.42 Remark One might wonder if the behavior of the negative eigenvalues of a connected k-regular graph X is similar to the behavior of the negatives of the positive eigenvalues of X. If X is bipartite, then the spectrum of X is symmetric with respect to 0 and this settles the previous question. In general, it turns out that additional conditions are needed in order to obtain similar results for the negative eigenvalues. This is because there are regular graphs with increasing order whose eigenvalues are bounded from below by an absolute constant. For example, the eigenvalues of a line graph are at least -2. It turns out that the number of odd cycles plays a role in the behavior of the negative eigenvalues of regular graphs. The *odd girth* of a graph X is the smallest length of a cycle of odd length.

14.10.43 Theorem [1120, 2276] If X is a connected k-regular graph of order n with a subset of r points each of distance at least $2t$ from one another, and odd girth at least $2t$, then

$$\lambda_{n-r}(X) \leq -2\sqrt{k-1}\cos\theta_{k,t} = -2\sqrt{k-1}\cos\frac{\pi}{t+1}. \tag{14.10.2}$$

14.10.44 Corollary [1911] If $(X_i)_{i\geq 0}$ is a sequence of k-regular graphs of increasing orders such that the odd girth of X_i tends to infinity as $i\to\infty$, then $\limsup_{i\to\infty}\mu_l(X_i) \leq -2\sqrt{k-1}$, for each $l\geq 1$, where $\mu_l(X)$ denotes the l-th smallest eigenvalue of X.

14.10.45 Theorem [643, 641] For an integer $r\geq 3$, let $c_r(X)$ denote the number of cycles of length r of a graph X. If $(X_i)_{i\geq 0}$ is a sequence of k-regular graphs of increasing orders such that $\lim_{i\to\infty}\frac{c_{2r+1}(X_i)}{|V(X_i)|}=0$ for each $r\geq 1$, then $\limsup_{i\to\infty}\mu_l(X_i)\leq -2\sqrt{k-1}$, for each $l\geq 1$.

14.10.46 Remark The difficulty of constructing infinite families of Ramanujan graphs is also illustrated by the following result of Serre.

14.10.47 Theorem [2578] For any $\epsilon>0$, there exists a positive constant $c=c(\epsilon,k)$ such that for every k-regular graph X on n vertices, the number of eigenvalues λ_i of X such that $\lambda_i > (2-\epsilon)\sqrt{k-1}$ is at least $c\cdot n$.

14.10.48 Remark Different short and elementary proofs of Serre's theorem were found independently by Nilli [2276] and Cioabă [643, 641]. Nilli's proof is similar to Friedman's argument from [1120] while Cioabă's proof uses the fact that the trace of A^l is the number of closed walks of length l. See also [643, 641] for a similar theorem to Theorem 14.10.47 for the smallest eigenvalues of regular graphs. These proofs, as well as extensions of the Alon-Bopanna theorem (see recent work of Mohar [2104]) rely on the notion of the universal cover of a graph; see Definitions 14.10.108 and 14.10.109, and Theorem 14.10.110 for more details.

14.10.49 Remark The idea behind all the proofs of Serre's theorem indicated above is that the universal cover of a finite k-regular graph is the rooted infinite k-regular tree T_k. This implies that the number of closed walks of even length starting at some vertex of a finite k-regular graph is at least the number of closed walks of the same length starting at the root of the infinite k-regular tree. The number $2\sqrt{k-1}$ is the spectral radius of the adjacency operator of the infinite k-regular tree (for more details see [1120, 1524]). In some circumstances, the

lower bound for the second eigenvalue of a k-regular graph can be improved beyond $2\sqrt{k-1}$ [1915, 2104].

14.10.50 Remark Greenberg and Lubotzky (see Chapter 4 of [1954] or [642, 641] for a short elementary proof) extended the Alon-Bopanna bound to any family of general graphs with isomorphic universal cover. If $(X_i)_{i\geq 1}$ is a family of finite connected graphs with universal cover $\tilde{X}$ and ρ is the spectral radius of the adjacency operator of $\tilde{X}$, then $\liminf \lambda_2(X_i) \geq \rho$ as $i \to +\infty$. For extensions of Alon-Boppana theorem and Serre's theorem for irregular graphs, see [642, 641, 1523, 2104].

14.10.51 Remark The notion of Ramanujan graph has been extended to hypergraphs and studied in this setting. Again, these notions lead to the use of the Ramanujan conjecture formulated for higher GL_n in the Langlands program.

14.10.52 Definition A *hypergraph* $X = (V, E)$ is a pair consisting of a vertex set V and a set of *hyperedges* E consisting of subsets of V. If all the edges are of the same size r, X is an r-uniform hypergraph or r-graph. In the familiar setting of a graph, an edge is viewed as a 2-element subset of V and is thus a 2-uniform hypergraph. One class of hypergraphs that are studied are the (k, r)-regular hypergraphs in which each edge contains r elements and each vertex is contained in k edges. For an ordinary graph, $r = 2$ and this generalizes the notion of a k-regular graph. In this special setting, the adjacency matrix A is a $|V| \times |V|$ matrix with zero diagonal entries and the (i, j)-th entry is the number of hyperedges that contain $\{i, j\}$.

14.10.53 Remark One can show easily that $k(r-1)$ is an eigenvalue of A and this is the trivial eigenvalue. With this definition in place, a *Ramanujan hypergraph* is defined as a finite connected (k, r)-regular hypergraph such that every eigenvalue λ of A with $|\lambda| \neq k(r-1)$ satisfies

$$|\lambda - (r-2)| \leq 2\sqrt{(k-1)(r-1)}.$$

We refer the reader to the important work of Li [1913] for further details.

14.10.3 Expander graphs

14.10.54 Definition For any subset A of vertices of a graph X, the *edge boundary* of A, denoted ∂A, is

$$\partial A = \{xy \in E(X) : x \in A, y \notin A\}.$$

That is, the edge boundary of A consists of edges with one endpoint in A and another outside A.

14.10.55 Definition The *edge-expansion constant* of X, denoted by $h(X)$, is defined as

$$h(X) = \min\left\{\frac{|\partial A|}{|A|} : A \subset X, |A| \leq \frac{|V(X)|}{2}\right\}.$$

14.10.56 Definition A family of k-regular graphs $(X_i)_{i\geq 1}$ with $|V(X_i)|$ increasing with i, is a *family of expanders* if there exists a positive absolute constant c such that $h(X_i) > c$ for every $i \geq 1$.

14.10.57 Remark Informally, a family of k-regular expanders is a family of sparse (k fixed and $|V(X_i)| \to +\infty$ as $i \to +\infty$ imply that the number of edges of X_i is linear in its number of vertices), but highly connected graphs ($h(X_i) > c$ means that in order to disconnect X_i, one must remove many edges).

14.10.58 Example [1992] Let X_m denote the following 8-regular graph on m^2 vertices. The vertex set of X_m is $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. The neighbors of a vertex (x, y) are $(x \pm y, y), (x, y \pm x), (x \pm y + 1, y), (x, y \pm x + 1)$. The family $(X_m)_{m\geq 4}$ is the first explicit family of expanders. Margulis [1992] proved that $(X_m)_{m\geq 4}$ are expanders using representation theory. Margulis [1992] used the fact that the group $SL_3(\mathbb{Z})$ has Kazhdan property T. Groups having this property or the weaker property τ can be used to construct infinite families of constant-degree Cayley graphs expanders. We refer the reader to [1524, 1954, 1955] for nice descriptions and explanations of these properties and their relation to expanders.

14.10.59 Remark Expander graphs play an important role in computer science, mathematics and the theory of communication networks; see [267, 1524]. These graphs arise in questions about designing networks that connect many users while using only a small number of switches.

14.10.60 Theorem [80, 2103] If X is a connected k-regular graph, then

$$\sqrt{k^2 - \lambda_2^2} \geq h(X) \geq \frac{k - \lambda_2}{2}.$$

14.10.61 Remark The previous theorem shows that constructing an infinite family of k-regular expanders $(X_i)_{i\geq 1}$ is equivalent to constructing an infinite family of k-regular graphs $(X_i)_{i\geq 1}$ such that $k - \lambda_2(X_i)$ is bounded away from zero.

14.10.4 Cayley graphs

14.10.62 Definition Let G be a group written in multiplicative notation and let S be a subset of elements of G that is closed under taking inverses and does not contain the identity. The *Cayley graph of G with respect to S* (denoted by $X(G, S)$) is the graph whose vertex set is G where $x \sim y$ if and only if $x^{-1}y \in S$. If G is abelian, then it is common to use the additive notation in the definition of $X(G, S)$: $x \sim y$ if and only if $y - x \in S$.

14.10.63 Remark In general, if S is an arbitrary multiset of G, denote by $X(G, S)$ the directed graph with vertex set G and arc set $\{(x, y) : x^{-1}y \in S\}$. If S is inverse-closed and does not contain the identity, then this graph is undirected and has no loops.

14.10.64 Theorem Let G be a finite abelian group and S a symmetric subset of G of size k. The eigenvalues of the adjacency matrix of $X(G, S)$ are given by

$$\lambda_\chi = \sum_{s\in S} \chi(s)$$

where χ ranges over all irreducible characters of G.

14.10.65 Remark For each irreducible character of G, let v_χ denote the column vector $(\chi(g) : g \in G)$. The proof of Theorem 14.10.64 follows by showing that v_χ is an eigenvector of the adjacency matrix of $X(G, S)$ corresponding to eigenvalue $\lambda_\chi = \sum_{s\in S} \chi(s)$.

14.10.66 Remark Notice that for the trivial character $\chi = 1$, we have $\lambda_1 = k$. If we have for all $\chi \neq 1$

$$\left| \sum_{s\in S} \chi(s) \right| < k$$

then the graph is connected by our earlier remarks. Thus, to construct Ramanujan graphs, we require

$$\left|\sum_{s\in S}\chi(s)\right| \leq 2\sqrt{k-1}$$

for every non-trivial irreducible character χ of G. This is the strategy employed in many of the explicit constructions of Ramanujan graphs.

14.10.67 Example A simple example can be given using Gauss sums. If $p \equiv 1 \pmod 4$ is a prime, let $G = \mathbb{Z}/p\mathbb{Z}$ and $S = \{x^2 : x \in \mathbb{Z}/p\mathbb{Z}\}$ be the multiset of squares. The multigraph $X(G, S)$ is easily seen to be Ramanujan in view of the fact (see for example [2193, p. 81])

$$\left|\sum_{x\in\mathbb{Z}/p\mathbb{Z}} e^{2\pi i a x^2/p}\right| = \sqrt{p}$$

for any $a \neq 0$. By our convention in the computation of degree of a vertex, we see that $X(G, S)$ is a p-regular graph.; see [1794] for other related examples.

14.10.68 Example When $q \equiv 1 \pmod 4$ is a prime power, the *Paley graph of order* q is the Cayley graph $X(G, S)$ of the additive group of a finite field $G = \mathbb{F}_q$ with respect to the set S of non-zero squares. This simple and undirected graph has q vertices, is connected and regular of degree $\frac{q-1}{2}$ and its non-trivial eigenvalues are $\frac{-1-\sqrt{q}}{2}$ and $\frac{-1+\sqrt{q}}{2}$, each of multiplicity $\frac{q-1}{2}$. The Paley graph is Ramanujan when $q \geq 9$.

14.10.69 Remark The proof of Theorem 14.10.64 is reminiscent of the Dedekind determinant formula in number theory. This formula computes $\det A$, where A is the matrix whose (i, j)-th entry is $f(ij^{-1})$ for any function f defined on the finite abelian group G of order n. The determinant is

$$\prod_{\chi}\left(\sum_{g\in G} f(g)\chi(g)\right).$$

14.10.70 Definition Let G be an abelian group written in the additive notation and $S \subset G$. The *sum graph of G with respect to S* (denoted by $Y(G, S)$) has G as vertex set and $x \sim y$ if and only if $x + y \in S$.

14.10.71 Theorem [1910, p. 197] Let G be an abelian group. The eigenvalues of $Y(G, S)$ are given as follows. For each irreducible character χ of G, define

$$e_\chi = \sum_{s\in S}\chi(s).$$

If $e_\chi = 0$, then v_χ and $v_{\chi^{-1}}$ are both eigenvectors with eigenvalues 0. If $e_\chi \neq 0$, then

$$|e_\chi| v_\chi \pm e_\chi v_{\chi^{-1}}$$

are two eigenvectors with eigenvalues $\pm|e_\chi|$.

14.10.72 Example Using Theorem 14.10.71, Li [1909] constructed Ramanujan graphs in the following way. Let $\mathbb{F}_q$ denote the finite field of q elements. Let $G = \mathbb{F}_{q^2}$ and take for S the elements of G of norm 1. This is a symmetric subset of G and the Cayley graph $X(G, S)$ turns out to be Ramanujan. The latter is a consequence of a theorem of Weil estimating Kloosterman sums [2573].

14.10.73 Theorem [2194] Let $G = \mathbb{F}_q$ be a finite field of $q = p^m$ elements and $f(x)$ a polynomial with coefficients in $\mathbb{F}_q$ and of degree 2 or 3. Let S be the multiset

$$\{f(x) : x \in \mathbb{F}_q\}.$$

Suppose S is symmetric. Then $X(G, S)$ is a Ramanujan graph if the degree of f is 2 and is almost Ramanujan if the degree of f is 3.

14.10.74 Remark The required character sum estimates in Theorem 14.10.73 come from Weil's proof of the Riemann hypothesis for the zeta functions of curves over finite fields. In particular, we have for all $a \in \mathbb{F}_q$, $a \neq 0$,

$$\left| \sum_{x \in \mathbb{F}_q} \exp(2\pi i \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(af(x))/p) \right| \leq (\deg f - 1)\sqrt{q}$$

provided f is not identically zero; see [1910, p. 94]. In particular, if f has degree 3, we get the estimate of $2\sqrt{q}$ for the exponential sum. For example, if $u \in \mathbb{Z}/p\mathbb{Z}$ and we take

$$S = \{x^3 + ux : x \in \mathbb{Z}/p\mathbb{Z}\},$$

then S is symmetric and, according to our convention, $X(G, S)$ is a p-regular graph. In addition, it is an almost Ramanujan graph since

$$\left| \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \exp(2\pi i a(x^3 + ux)/p) \right| \leq 2\sqrt{p}$$

by virtue of the Riemann hypothesis for curves (proved by Weil).

14.10.75 Remark We observe that even though there are many constructions of Ramanujan graphs that are abelian Cayley graphs, it is actually impossible to construct an infinite family of constant-degree abelian Cayley graphs that are Ramanujan. There are several proofs of this fact in the literature, see [83, 640, 1122]. Friedman, Murty and Tillich [1122] proved that if X is a k-regular abelian Cayley graph of order n, then $\lambda_2(X) \geq k - cn^{-4/k}$, where c is some absolute positive constant. Cioabă [640] proved that for fixed $k \geq 3$ and $\epsilon > 0$, there is a positive constant $C = C(\epsilon, k)$ such that any k-regular abelian Cayley graph on n vertices has at least Cn eigenvalues that are larger than $k - \epsilon$.

14.10.76 Remark Lubotzky and Weiss [1957] proved the stronger result that it is impossible to construct infinite families of constant-degree expanders that are Cayley graphs of solvable groups of bounded derived length.

14.10.77 Remark The eigenvalues of Cayley graphs can be calculated even in the case of non-abelian groups. This is essentially contained in a paper by Diaconis and Shahshahani [828]. Using their results, one can easily generalize the Dedekind determinant formula as follows (and which does not seem to be widely known). Let G be a finite group and f a class function on G. Then the determinant of the matrix A whose rows (and columns) are indexed by the elements of G and whose (i, j)-th entry $f(i^{-1}j)$ is given by

$$\prod_{\chi} \left(\frac{1}{\chi(1)} \sum_{g \in G} f(g)\chi(g) \right)^{\chi(1)}$$

where the product is taken over the distinct irreducible characters of G.

14.10.78 Theorem [828] Let G be a finite group and S a symmetric subset which is stable under conjugation. The eigenvalues of the Cayley graph $X(G,S)$ are given by

$$\lambda_\chi = \frac{1}{\chi(1)} \sum_{s \in S} \chi(s)$$

as χ ranges over all irreducible characters of G. Moreover, the multiplicity of λ_χ is $\chi(1)^2$.

14.10.79 Remark We remark that the λ_χ in the above theorem need not be all distinct. For example, if there is a non-trivial character χ which is trivial on S, then the multiplicity of the eigenvalue $|S|$ is at least $1 + \chi(1)^2$. We refer the reader to Babai [155] for a more detailed proof of the above result in a slightly more general context.

14.10.80 Remark The intriguing question of what groups can be used to construct infinite families of constant-degree Cayley graphs expanders was formulated as a conjecture by Babai, Kantor and Lubotzky [156] in 1989.

14.10.81 Conjecture [156] Let $(G_i)_{i \geq 0}$ be a family of non-abelian simple groups. There exist generating sets S_i of constant size such that $(X(G_i, S_i))_{i \geq 0}$ form a family of expanders.

14.10.82 Remark As a supporting fact of this conjecture, we mention the result of Babai, Kantor and Lubotzky [156] who proved constructively that any simple non-abelian group G contains a set S of at most 7 generators such that the diameter of the Cayley graph $X(G,S)$ is at most $c \log |G|$, where $c > 0$ is some absolute constant.

14.10.83 Remark The previous conjecture of Babai, Kantor and Lubotzky is true and its recent resolution has been possible due to the effort of several researchers. We refer the reader to the works of Kassabov, Lubotzky and Nikolov [1681], Breuillard, Green and Tao [408], and the recent survey by Lubotzky [1955] for a thorough account of the solution of this conjecture.

14.10.5 Explicit constructions of Ramanujan graphs

14.10.84 Definition Let X be a graph. A *non-backtracking walk* of length r in X is a sequence $x_0, x_1, \ldots, x_r$ of vertices of X such that x_i is adjacent to x_{i+1} for each $0 \leq i \leq r-1$ and $x_{i-1} \neq x_{i+1}$ for each $1 \leq i \leq r-1$. For $r \in \mathbb{N}$, define the matrix A_r as follows: $A_r(x,y)$ equals the number of non-backtracking walks of length r that start at x and end at y.

14.10.85 Proposition If X is a k-regular graph with n vertices and adjacency matrix A, then

1. $A_0 = I_n, A_1 = A$;
2. $A_2 = A_1^2 - kI_n$;
3. $A_{r+1} = A_1 A_r - (k-1)A_{r-1}$ for every $r \geq 2$.

14.10.86 Proposition [774, 1956] Let U_m denote the Chebyshev polynomial of the second kind defined by expressing $\frac{\sin(m+1)\theta}{\sin\theta}$ as a polynomial of degree m in $\cos\theta$:

$$U_m(\cos\theta) = \frac{\sin(m+1)\theta}{\sin\theta}.$$

Then

$$\sum_{r=0}^{\lfloor \frac{m}{2} \rfloor} A_{m-2r} = (k-1)^{\frac{m}{2}} U_m\left(\frac{A}{2\sqrt{k-1}}\right).$$

14.10.87 Definition A graph X is *vertex-transitive* if the automorphism group of X acts transitively on its vertex set which means that for any $x, y \in V(X)$ there exists an automorphism σ of X such that $\sigma(x) = y$.

14.10.88 Proposition [774, 1956] If X is a k-regular graph with n vertices and eigenvalues $k = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$, then

$$\sum_{x \in V} \sum_{r=0}^{\lfloor \frac{l}{2} \rfloor} (A_{l-2r})(x,x) = (k-1)^{\frac{l}{2}} \sum_{j=1}^{n} \frac{\sin(l+1)\theta_j}{\sin \theta_j}.$$

where $\cos \theta_j = \frac{\lambda_j}{2\sqrt{k-1}}$ for each $1 \leq j \leq n$. If X is vertex-transitive of degree k, then $(A_j)(x,x) = (A_j)(y,y)$ for any j and $x, y \in V(X)$ and thus,

$$n \sum_{r=0}^{\lfloor \frac{l}{2} \rfloor} (A_{l-2r})(x,x) = (k-1)^{\frac{l}{2}} \sum_{j=1}^{n} \frac{\sin(l+1)\theta_j}{\sin \theta_j}.$$

for every vertex $x \in V(X)$.

14.10.89 Remark Note that $\theta_1 = i \log \sqrt{k-1}$ as $\lambda_1 = k$ and $\theta_n = \pi + i \log \sqrt{k-1}$ if $\lambda_n = -k$. Also, it is important to observe that θ_j is real if $|\lambda_j| = |2\sqrt{k-1} \cos \theta_j| \leq 2\sqrt{k-1}$; otherwise, $\theta_j = iIm(\theta_j)$ is purely imaginary if $\lambda_j > 2\sqrt{k-1}$ and $\theta_j = \pi + iIm(\theta_j)$ if $\lambda_j < 2\sqrt{k-1}$.

14.10.90 Remark The general idea of using quaternions (see Lubotzky, Phillips and Sarnak [1956] or Margulis [1993]) to construct infinite families of k-regular Ramanujan graphs can be summarized in the following two steps:

1. The first step consists of constructing the infinite k-regular tree T_k as the free group of some group $\mathcal{G}$ of quaternions integers with some suitable set of k generators $\mathcal{S}_k$. Thus, T_k will be identified with the Cayley graph $X(\mathcal{G}, \mathcal{S}_k)$.
2. Finite k-regular graphs are constructed from the infinite k-regular tree T_k by taking suitable finite quotients of it. More precisely, by choosing appropriate normal subgroups $\mathcal{H}$ of $\mathcal{G}$ of finite index, one can construct finite k-regular graphs which are the Cayley graphs of the quotient group $\mathcal{G}/\mathcal{H}$ with the set of generators being formed by the cosets of the form $\alpha\mathcal{H}$ where $\alpha \in \mathcal{S}_k$.

14.10.91 Construction [1956, 1993] Let p and q be unequal primes $p, q \equiv 1 \pmod 4$. Let u be an integer so that $u^2 \equiv -1 \pmod q$. By a classical formula of Jacobi, we know that there are $8(p+1)$ solutions $v = (a,b,c,d)$ such that $a^2 + b^2 + c^2 + d^2 = p$. Among these, there are exactly $p+1$ with $a > 0$ and b, c, d even, as is easily shown. To each such v we associate the matrix

$$\tilde{v} = \begin{pmatrix} a + ub & c + ud \\ -c + ud & a - ub \end{pmatrix}$$

which gives $p+1$ matrices in $PGL_2(\mathbb{Z}/q\mathbb{Z})$. We let S be the set of these matrices $\tilde{v}$ and define

$$X^{p,q} = \begin{cases} X(PGL_2(\mathbb{Z}/q\mathbb{Z}), S), & \text{if } \left(\frac{p}{q}\right) = -1, \\ X(PSL_2(\mathbb{Z}/q\mathbb{Z}), S), & \text{if } \left(\frac{p}{q}\right) = 1, \end{cases} \tag{14.10.3}$$

where $\left(\frac{p}{q}\right)$ is the Legendre symbol that equals 1 if p is a square modulo q and -1 if p is not a square modulo q. In [1956], it is shown that the Cayley graphs $X^{p,q}$ are Ramanujan graphs. As we vary q, we get an infinite family of such graphs, all $(p+1)$-regular.

14.10.92 Remark The integer quaternion algebra is

$$\mathrm{H}(\mathbb{Z}) = \{a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} : a_0, a_1, a_2, a_3 \in \mathbb{Z}\},$$

where $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$ and $\mathbf{ij} = -\mathbf{ji} = k, \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \mathbf{ki} = -\mathbf{ik} = \mathbf{j}$. If $\alpha = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$, then $\overline{\alpha} = a_0 - a_1\mathbf{i} - a_2\mathbf{j} - a_3\mathbf{k}$ and $N(\alpha) = \alpha\overline{\alpha} = a_0^2 + a_1^2 + a_2^2 + a_3^2$. The units of $\mathrm{H}(\mathbb{Z})$ are $\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}$. Let p be a prime with $p \equiv 1 \pmod 4$. By Jacobi's Theorem, there are $8(p+1)$ integer quaternions $\alpha = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$ in $\mathrm{H}(\mathbb{Z})$ such that $N(\alpha) = p$. As $p \equiv 1 \pmod 4$, only one of the integers a_i will be odd. Let S be the set of those $p+1$ elements of $\mathrm{H}(\mathbb{Z})$ such that $N(\alpha) = p$, $a_0 > 0$ is odd and a_1, a_2, a_3 even (this last fact is denoted by $\alpha \equiv 1 \pmod 2$ from now on). As $N(\alpha) = N(\overline{\alpha})$, the set S consists of $s = \frac{p+1}{2}$ conjugate pairs $S = \{\alpha_1, \overline{\alpha_1}, \ldots, \alpha_s, \overline{\alpha_s}\}$. A reduced word of length m with letters in S is defined to be a word of length m in the elements of S which does not contain subwords of the form $\alpha_j\overline{\alpha_j}$ nor $\overline{\alpha_j}\alpha_j$.

14.10.93 Construction (Different construction of the graphs $X^{p,q}$) Define $\Lambda'(2) = \{\alpha : \alpha \in \mathbb{Z}, \alpha \equiv 1 \pmod 2, N(\alpha) = p^l, l \in \mathbb{Z}\}$. As $N(\alpha\beta) = N(\alpha)N(\beta)$ and the properties of quaternion multiplication, it follows that $\Lambda'(2)$ is closed under multiplication. Define $\alpha \sim \beta$ for $\alpha, \beta \in \Lambda'(2)$ whenever $\pm p^{v_1}\alpha = p^{v_2}\beta$ for some $v_1, v_2 \in \mathbb{Z}$. This is an equivalence relation and $[\alpha]$ will denote the equivalence class of $\alpha \in \Lambda'(2)$. The set of equivalence classes $\Lambda(2) = \{[\alpha] : \alpha \in \Lambda'(2)\}$ forms a group with the multiplication $[\alpha][\beta] = [\alpha\beta]$ and $[\alpha][\overline{\alpha}] = [1]$. One of the key observations at this point is that, by previous results, the group $\Lambda(2)$ is free on $[\alpha_1], [\alpha_2], \ldots, [\alpha_s]$. This means that the Cayley graph of $\Lambda(2)$ with respect to the set $[S] = \{[\alpha_1], [\overline{\alpha_1}], \ldots, [\alpha_s], [\overline{\alpha_s}]\}$ will be the infinite $(p+1)$-regular tree.

For m coprime with p, let

$$\Lambda(2m) = \{[\alpha] : \alpha = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} \in \Lambda'(2), 2m | a_j, 1 \le j \le 3\}.$$

It can be shown that $\Lambda(2m)$ is a normal subgroup of $\Lambda(2)$ of finite index. Let q be a prime. The graphs $X^{p,q}$ and the Cayley graph of $\Lambda(2)/\Lambda(2q)$ with respect to the set of generators $\alpha_1\Lambda(2q), \overline{\alpha_1}\Lambda(2q), \ldots, \alpha_s\Lambda(2q), \overline{\alpha_s}\Lambda(2q)$ are isomorphic as shown by the next result.

14.10.94 Proposition Let $\phi : \Lambda(2) \to PGL(2, \mathbb{Z}/q\mathbb{Z})$ defined as follows:

$$\phi([a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}]) = \begin{bmatrix} a_0 + ua_1 & a_2 + ua_3 \\ -a_2 + ua_3 & a_0 - ua_1 \end{bmatrix}$$

where $u^2 \equiv -1 \pmod q$. Then ϕ is a group homomorphism whose kernel is $\Lambda(2q)$ and whose image is $PGL(2, \mathbb{Z}/q\mathbb{Z})$ if $\left(\frac{p}{q}\right) = -1$ and $PSL(2, \mathbb{Z}/q\mathbb{Z})$ if $\left(\frac{p}{q}\right) = 1$.

14.10.95 Definition Let $Q = Q(x_0, x_1, x_2, x_3)$ denote the quadratic form

$$Q(x_0, x_1, x_2, x_3) = x_0^2 + (2q)^2x_1^2 + (2q)^2x_2^2 + (2q)^2x_3^2.$$

Denote by $r_Q(n)$ the number of integer solutions of $Q(x_0, x_1, x_2, x_3) = n$ which is the same as the number of $\alpha = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} \in \mathrm{H}(\mathbb{Z})$ such that $2q | \alpha - a_0$ and $N(\alpha) = n$.

14.10.96 Remark Estimating $r_Q(n)$ is an important and difficult problem in number theory. According to [1956], there is no simple explicit formula for $r_Q(n)$ as Jacobi's formula because of additional cusp forms that appear at the higher level. The Ramanujan conjecture for weight 2 cusp forms and its proof by Eichler and Igusa yields a good approximation for $r_Q(n)$. More precisely, if p is a prime and $l \ge 0$, then

$$r_Q(p^l) = C(p^l) + O_\epsilon(p^{\frac{l}{2}+\epsilon})$$

for any $\epsilon > 0$ as $l \to \infty$. Here

$$C(p^l) = \begin{cases} 2\sum_{d|p^l} d = 2\frac{p^{l+1}-1}{p-1} \text{ if } \left(\frac{p}{q}\right) = 1, \\ 4\sum_{d|p^l} d = 4\frac{p^{l+1}-1}{p-1} \text{ if } \left(\frac{p}{q}\right) = -1 \text{ and } l \text{ even}, \\ 0 \text{ if } \left(\frac{p}{q}\right) = -1 \text{ and } l \text{ odd}. \end{cases}$$

14.10.97 Remark The number theoretic facts above and the connection between the eigenvalues and the number of closed nonbacktracking walks in a regular graph were used by Lubotzky, Phillips and Sarnak to prove the following result.

14.10.98 Theorem [1956, 1993] The graphs $X^{p,q}$ are Ramanujan.

14.10.99 Remark If $\left(\frac{q}{p}\right) = -1$, then $X^{p,q}$ is bipartite of high girth; its girth is at least $4\log_p q - \log_p 4 \approx \frac{4}{3}\log_p |V(X^{p,q})|$. If $\left(\frac{q}{p}\right) = 1$, then $X^{p,q}$ also has high girth; its girth is at least $2\log_p q \approx \frac{2}{3}\log_p |V(X^{p,q})|$. From the results of Hoffman, it also follows that these graphs have large chromatic number (at least $1 + \frac{p+1}{2\sqrt{p}}$).

14.10.100 Remark Morgenstern [2146] generalized Lubotzky, Phillips and Sarnak's construction and constructed infinite families of $(q+1)$-regular Ramanujan graphs for every prime power q.

14.10.6 Combinatorial constructions of expanders

14.10.101 Construction Reingold, Vadhan and Wigderson [2432] introduced a new graph product called the *zig-zag product* which they used to construct infinite families of constant-degree expanders.

14.10.102 Definition Let X be a k-regular graph with vertex set $[n] = \{1, \ldots, n\}$. Suppose the edges incident to each vertex of X are labeled from 1 to k in some arbitrary, but fixed way. The rotation map $Rot_X : [n] \times [k] \to [n] \times [k]$ is defined as follows: $Rot_X(u, i) = (v, j)$ if the i-th edge incident to u is the j-th edge incident to v.

14.10.103 Definition Let G_1 be a D_1-regular graph with vertex set $[N_1]$ with rotation map Rot_{G_1} and G_2 be a D_2-regular graph with vertex set $[D_1]$ with rotation map Rot_{G_2}. The *zig-zag product* $G_1 z G_2$ is the D_2^2-regular graph with vertex set $[N_1] \times [D_1]$ whose rotation map $Rot_{G_1 z G_2}$ is:

1. let $(k', i') = Rot_{G_2}(k, i)$;
2. let $(w, l') = Rot_{G_1}(v, k')$;
3. let $(l, j') = Rot_{G_2}(l', j)$;
4. define $Rot_{G_1 z G_2}((v, k), (i, j)) = ((w, l), (i', j'))$.

14.10.104 Definition A graph G is an (n, d, λ)-graph if G has n vertices, is d-regular and the absolute value of any non-trivial eigenvalue of G is at most λd.

14.10.105 Theorem [2432] If G_1 is an (N_1, D_1, μ_1)-graph and G_2 is an (D_1, D_2, μ_2)-graph, then $G_1 z G_2$ is an $(N_1 D_1, D_2^2, \mu_1 + \mu_2 + \mu_2^2)$-graph.

14.10.106 Construction Using the previous theorem, Reingold, Vadhan and Wigderson [2432] constructed infinite families of constant-degree expanders.

14.10.107 Construction Bilu and Linial [280] have used graph lifts to construct infinite families of d-regular graphs whose non-trivial eigenvalues have absolute value at most $C\sqrt{d\log^3 d}$, where C is some positive absolute constant. We outline their method below.

14.10.108 Definition Given two graphs G_1 and G_2, a *graph homomorphism* from G_1 to G_2 is a function $f : V(G_1) \to V(G_2)$ which preserves adjacency, namely if xy is an edge of G_1, then $f(x)f(y)$ is an edge of G_2; the function f is a *graph isomorphism* if it is bijective and preserves both adjacency and non-adjacency, namely xy is an edge of G_1 if and only if $f(x)f(y)$ is an edge of G_2.

14.10.109 Definition A surjective homomorphism $f : V(G_1) \to V(G_2)$ is a *covering map* (see [280, 1120]) if for each vertex x of G_1, the restriction of f to x and its neighbors is bijective. Given a graph G, a cover of G is a pair (H, f), where $f : V(H) \to V(G)$ is a covering map. If in addition G is connected and finite and H is finite, then for each vertex $y \in V(G)$, the preimage $f^{-1}(y)$ has the same cardinality. If $|f^{-1}(y)| = t$ for each $y \in V(G)$, then (H, f) is a *t-cover* or H is a *t-lift* of G.

14.10.110 Remark For every finite graph G, there is a universal cover or a *largest cover* $\tilde{G}$ which is an infinite tree whose vertices can be identified with the set of nonbacktracking walks from a fixed vertex $x \in V(G)$. For example, the universal cover of any finite k-regular graph is the infinite k-regular tree T_k.

14.10.111 Remark An important property of a t-cover (H, f) of a finite graph G is that the graph H inherits the eigenvalues of G. This is because the vertex set of H can be thought as $V(G) \times \{1, \ldots, t\}$ with the preimage (also called the fiber of y) $f^{-1}(y) = \{x : x \in V(H), f(x) = y\} = \{(y, i) : 1 \le i \le t\}$. The edges of H are related to the edges of G as follows: each fiber $f^{-1}(y)$ induces an independent set in H; if $yz \in E(G)$, then the subgraph of H induced by $f^{-1}(y) \cup f^{-1}(z) = \{(y, i), (z, i) : 1 \le i \le t\}$ is a perfect matching (meaning that there exists a permutation $\sigma \in S_t$ such that (y, i) is adjacent to $(z, \sigma(i))$ for each $1 \le i \le t$); if $yz \notin E(G)$, then there are no edges between $f^{-1}(y)$ and $f^{-1}(z)$. The partition of the vertex set of H as $V(H) = \cup_{y \in V(G)} f^{-1}(y)$ is equitable (see [1279]) and its quotient matrix is the same as the adjacency matrix of G. This implies the eigenvalues of $A(G)$ are the eigenvalues of $A(H)$. These eigenvalues of $A(H)$ are *old* and the remaining eigenvalues of $A(H)$ are *new*.

14.10.112 Remark In the case of a 2-lift, the new eigenvalues can be interpreted as eigenvalues of a *signed* adjacency matrix as follows. If H is a 2-lift of G, then for each edge yz of G, the subgraph induced by $f^{-1}(y) \cup f^{-1}(z) = \{(y, 0), (y, 1), (z, 0), (z, 1)\}$ in H has either $(y, 0)$ adjacent to $(z, 0)$ and $(y, 1)$ adjacent to $(z, 1)$ (in which case set $s(y, z) = s(z, y) = 1$) or $(y, 0)$ adjacent to $(z, 1)$ and $(y, 1)$ adjacent to $(z, 0)$ (in which case set $s(y, z) = s(z, y) - 1$). Let $s(y, z) = 0$ for all other $y, z \in V(G)$. The symmetric $\{0, -1, 1\}$ matrix A_s whose (y, z)-th entry is $s(y, z)$ is the *signed adjacency matrix* of the G with respect to the cover H. It is known that the eigenvalues of H are union of the eigenvalues of the adjacency matrix of G and the eigenvalues of the signed adjacency matrix of G. Bilu and Linial [280] proved that every graph G with maximum degree d has a signed adjacency matrix (which can be found efficiently) whose eigenvalues have absolute value at most $C\sqrt{d\log^3 d}$ where C is some positive absolute constant.

14.10.113 Construction Bilu and Linial's idea to construct almost Ramanujan graphs is the following: start with a k-regular Ramanujan graph G_0 (for example, the complete graph K_{k+1}) and then construct a 2-lift of G_i (denoted by G_{i+1}) such that the new eigenvalues of G_{i+1} are small in absolute value for $i \ge 0$. Bilu and Linial [280] prove that every k-regular graph G

has a 2-lift H such that the new eigenvalues of H have absolute value at most $C\sqrt{k \log^3 k}$ where C is some positive absolute constant. In this way the sequence of k-regular graphs G_i has non-trivial eigenvalues bounded from above by $C\sqrt{k \log^3 k}$.

14.10.114 Remark Bilu and Linial [280] make the following conjecture which if true, would imply the existence of infinite sequences of k-regular Ramanujan graphs for every $k \geq 3$.

14.10.115 Conjecture [280] Every k-regular graph has a signed adjacency matrix whose eigenvalues have absolute value at most $2\sqrt{k-1}$.

14.10.116 Construction A different combinatorial construction of almost Ramanujan graphs was proposed by de la Harpe and Musitelli [780], and independently by Cioabă and Murty [644, 641]). The idea of these constructions is that perturbing Ramanujan graphs by adding or removing perfect matchings will yield graphs with small non-trivial eigenvalues. The linear algebraic reason for this fact follows from a theorem of Weyl which bounds the eigenvalues of a sum of two Hermitian matrices in terms of the eigenvalues of the summands. De la Harpe and Musitelli [780] note that adding a perfect matching to any 6-regular Ramanujan graph will yield a 7-regular graph whose 2nd largest eigenvalue is at most $2\sqrt{5}+1 \cong 5.47$ which is larger than the Ramanujan bound of $2\sqrt{6} \cong 4.89$, but strictly less than 7. Cioabă and Murty [644, 641] use known results regarding gaps between consecutive primes to observe that by adding or removing perfect matching from Ramanujan graphs, one can construct k-regular almost Ramanujan graphs for almost all k. More precisely, their result is that given $\epsilon > 0$, for almost all $k \geq 3$, one can construct infinite families of k-regular graphs whose 2nd largest eigenvalue is at most $(2+\epsilon)\sqrt{k-1}$.

14.10.117 Remark The following conjecture was made in [641]; if true, this conjecture would imply the existence of infinite families of k-regular Ramanujan graphs for any $k \geq 3$.

14.10.118 Conjecture [641] Let X be a k-regular Ramanujan graph with an even number of vertices. Then there exists a perfect matching P with $V(P) = V(X)$ such that the $(k+1)$-regular graph obtained from the union of the edges of X and P is Ramanujan.

14.10.119 Remark In a recent outstanding work, Friedman [1121] solved a long-standing conjecture of Alon from the 1980s and proved that almost all regular graphs are almost Ramanujan.

14.10.120 Theorem [1121] Given $\epsilon > 0$ and $k \geq 3$, the probability that a random k-regular graph on n vertices has all non-trivial eigenvalues at most $(2+\epsilon)\sqrt{k-1}$ goes to 1 as n goes to infinity.

14.10.7 Zeta functions of graphs

14.10.121 **Definition** A walk in a graph X is *non-backtracking* if no edge is traversed and then immediately backtracked upon. A non-backtracking walk whose endpoints are equal is a *closed geodesic*. If γ is a closed geodesic, we denote by γ^r the closed geodesic obtained by repeating the walk γ r times. A walk is *tailless* if it is non-backtracking under any cyclic permutation of vertices. A closed geodesic which is not the power of another one and is tailless is a *prime geodesic*. We define an equivalence relation on the closed geodesics as follows: $(x_0, ..., x_n)$ and $(y_0, ..., y_m)$ are equivalent if and only if $m = n$ and there is a d such that $y_i = x_{i+d}$ for all i (and the subscripts are interpreted modulo n). An equivalence class of a prime geodesic is a *prime geodesic cycle*.

14.10.122 **Definition** Let X be a k-regular graph and denote $q = k - 1$. The *Ihara zeta function* is

$$Z_X(s) = \prod_p \left(1 - q^{-s\ell(p)}\right)^{-1}$$

where the product is over all prime geodesic cycles p and $\ell(p)$ is the length of p.

14.10.123 **Theorem** [1556] For $g = (q-1)|X|/2$, we have

$$Z_X(s) = (1-u^2)^{-g} \det(I - Au + qu^2 I)^{-1}, \quad u = q^{-s}.$$

Moreover, $Z_X(s)$ satisfies the *Riemann hypothesis'* (that is, all the singular points in the region $0 < \Re(s) < 1$ lie on $Re(s) = 1/2$) if and only if X is a Ramanujan graph.

14.10.124 **Remark** Hashimoto [1431], as well as Stark and Terras [2684] have defined a zeta function for an arbitrary graph and established its rationality. The definition of this zeta function is simple enough. Let N_r be the number of closed walks γ of length r so that neither γ nor γ^2 have backtracking. Then, the *zeta function* of the graph X is defined as

$$\mathcal{Z}_X(t) = \exp\left(\sum_{r=1}^{\infty} \frac{N_r t^r}{r}\right).$$

This definition is very similar to the zeta function of an algebraic variety.

14.10.125 **Remark** It would be interesting to interpret the singularities of $\mathcal{Z}_X(t)$ in terms of properties of the graph. For instance, these zeta functions have a pole at $t = 1$ and Hashimoto [1431] has shown that the residue at $t = 1$ is related to the number of spanning trees of the graph X. Thus, this number is the graph-theoretic analogue of the class number of an algebraic number field. These constructions raise the intriguing question of whether there is a generalization of the notion of a graph to that of a 'supergraph' whose zeta function would (in some cases) coincide with those higher dimensional zeta functions of varieties. Work in this direction has started [1914].

See Also

§6.1, §6.2	For details on Gauss sums and other character sums.
§12.7	For discussions on zeta functions and L-functions of curves.
§15.1, §15.3	For details on algebraic, LDPC and expander codes.

References Cited: [80, 81, 83, 155, 156, 267, 280, 408, 631, 632, 640, 642, 643, 644, 641, 774, 780, 828, 1120, 1121, 1122, 1279, 1431, 1523, 1524, 1556, 1629, 1681, 1794, 1909, 1912, 1913, 1915, 1910, 1911, 1914, 1954, 1955, 1956, 1957, 1992, 1993, 2103, 2104, 2146, 2193, 2194, 2275, 2276, 2418, 2432, 2506, 2508, 2573, 2578, 2684, 2771, 2819, 2821]

Bibliography

[1] R. Abarzúa, N. Thériault, R. Avanzi, I. Soto, and M. Alfaro, Optimization of the arithmetic of the ideal class group for genus 4 hyperelliptic curves over projective coordinates, *Advances in Mathematics of Communications* 4 (2010) 115–139. <794>

[2] E. Abbe, Randomness and dependencies extraction via polarization, In *Proc. Information Theory and Applications Workshop (ITA)*, 1–7, 2011. <730>

[3] M. Abdón and F. Torres, On maximal curves in characteristic two, *Manuscripta Math.* 99 (1999) 39–53. <454, 456>

[4] R. J. R. Abel, Some new BIBDs with block size 7, *J. Combin. Des.* 8 (2000) 146–150. <588, 590>

[5] R. J. R. Abel and M. Buratti, Some progress on $(v, 4, 1)$ difference families and optical orthogonal codes, *J. Combin. Theory, Ser. A* 106 (2004) 59–75. <585, 590>

[6] R. J. R. Abel, N. J. Finizio, G. Ge, and M. Greig, New Z-cyclic triplewhist frames and triplewhist tournament designs, *Discrete Appl. Math.* 154 (2006) 1649–1673. <610>

[7] R. J. R. Abel and G. Ge, Some difference matrix constructions and an almost completion for the existence of triplewhist tournaments TWh(v), *European J. Combin.* 26 (2005) 1094–1104. <609, 610>

[8] S. S. Abhyankar, Resolution of singularities and modular Galois theory, *Bull. Amer. Math. Soc. (New Ser.)* 38 (2001) 131–169. <232, 233>

[9] S. S. Abhyankar, Symplectic groups and permutation polynomials. II, *Finite Fields Appl.* 8 (2002) 233–255. <232, 233>

[10] F. Abu Salem, S. Gao, and A. G. B. Lauder, Factoring polynomials via polytopes, In *ISSAC '04: Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation*, 4–11, New York, 2004, ACM. <382, 385>

[11] F. K. Abu Salem, An efficient sparse adaptation of the polytope method over $\mathbb{F}_p$ and a record-high binary bivariate factorisation, *J. Symbolic Comput.* 43 (2008) 311–341. <382, 385>

[12] J.-K. Accetta, Z. Mejías, and A. Santos, Número de waring en cuerpos finitos, Preprint, 2011. <205, 207>

[13] W. W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*, American Mathematical Society, Providence, RI, first edition, 1994. <80, 81, 693, 694>

[14] L. Adleman and H. Lenstra, Finding irreducible polynomials over finite fields, In *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing*, 350–355, ACM, New York, NY, USA, 1986. <114, 122, 371, 372, 373, 397>

[15] L. Adleman, K. Manders, and G. Miller, On taking roots in finite fields, In *Proceedings of the Eighteenth Annual Symposium on Foundations of Computer Science*, 175–178, IEEE Computer Society, Washington, DC, USA, 1977. <374, 375>

[16] L. M. Adleman, The function field sieve, In *Algorithmic Number Theory*, volume 877 of *Lecture Notes in Comput. Sci.*, 108–121, Springer, Berlin, 1994. <392, 394>

[17] L. M. Adleman, J. DeMarrais, and M.-D. Huang, A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields, In *Algorithmic Number Theory*, volume 877 of *Lecture Notes in Comput. Sci.*, 28–40, Springer, Berlin, 1994. <448, 449>

[18] L. M. Adleman and M.-D. Huang, Counting points on curves and Abelian varieties over finite fields, *J. Symbolic Comput.* 32 (2001) 171–189. <483, 484>

[19] L. M. Adleman, C. Pomerance, and R. S. Rumely, On distinguishing prime numbers from composite numbers, *Ann. of Math., 2nd Ser.* 117 (1983) 173–206. <340, 356>

[20] A. Adolphson and S. Sperber, On unit root formulas for toric exponential sums, *Alg. Num. Th.*, to appear. <475, 480>

[21] A. Adolphson and S. Sperber, p-adic estimates for multiplicative character sums, Preprint, http://arxiv.org/abs/1103.5513. <476, 480>

[22] A. Adolphson and S. Sperber, p-adic estimates for exponential sums and the theorem of Chevalley-Warning, *Ann. Sci. École Norm. Sup., IVe Ser.* 20 (1987) 545–556. <193, 195, 204, 207, 473, 480>

[23] A. Adolphson and S. Sperber, On the degree of the L-function associated with an exponential sum, *Compositio Math.* 68 (1988) 125–159. <163, 466, 469, 472>

[24] A. Adolphson and S. Sperber, Exponential sums and Newton polyhedra: cohomology and estimates, *Ann. of Math., 2nd Ser.* 130 (1989) 367–406. <159, 163, 190, 195, 204, 207, 469, 472, 475, 480>

[25] A. Adolphson and S. Sperber, p-adic estimates for exponential sums, In *p-adic Analysis*, volume 1454 of *Lecture Notes in Math.*, 11–22, Springer, Berlin, 1990. <207>

[26] A. Adolphson and S. Sperber, On twisted exponential sums, *Math. Ann.* 290 (1991) 713–726. <475, 480>

[27] A. Adolphson and S. Sperber, Twisted exponential sums and Newton polyhedra, *J. Reine Angew. Math.* 443 (1993) 151–177. <475, 480>

[28] A. Adolphson and S. Sperber, On the zeta function of a complete intersection, *Ann. Sci. École Norm. Sup., IVe Ser.* 29 (1996) 287–328. <190, 195, 474, 480>

[29] A. Adolphson and S. Sperber, Exponential sums on A^n. III, *Manuscripta Math.* 102 (2000) 429–446. <157, 163>

[30] A. Adolphson and S. Sperber, On the zeta function of a projective complete intersection, *Illinois J. Math.* 52 (2008) 389–417. <474, 480>

[31] A. Adolphson and S. Sperber, Exponential sums nondegenerate relative to a lattice, *Alg. Num. Th.* 3 (2009) 881–906. <207>

[32] V. B. Afanasyev, Complexity of VLSI implementation of finite field arithmetic, In *Proc. II. Intern. Workshop on Algebraic and Combinatorial Coding Theory, USSR*, 6–7, 1990. <805, 813>

[33] S. Agou, Sur l'irréducibilité des polynômes à coefficients dans un corps fini, *C. R. Acad. Sci. Paris, Sér. A-B* 272 (1971) A576–A577. <58, 61>

[34] S. Agou, Factorisation sur un corps fini $\mathbb{F}_{p^n}$ des polynômes composés $f(X^s)$ lorsque $f(X)$ est un polynôme irréductibile de $\mathbb{F}_{p^n}[X]$, *L' Enseignement Math., IIe Ser.* 22 (1976) 305–312. <56, 58, 61>

[35] S. Agou, Factorisation sur un corps fini K des polynômes composés $f(X^s)$ lorsque $f(X)$ est polynôme irréductibile de $K[X]$, *C. R. Acad. Sci. Paris, Sér. A-B* 282 (1976) Ai, A1067–A1068. <56, 61>

[36] S. Agou, Critères d'irréductibilité des polynômes composés à coefficients dans un corps fini, *Acta Arith.* 30 (1976/77) 213–223. <56, 58, 59, 61>

[37] S. Agou, Factorisation sur un corps fini $\mathbb{F}_{p^n}$ des polynômes composés $f(X^{p^r} - aX)$ lorsque $f(X)$ est un polynôme irréductible de $\mathbb{F}_{p^n}(X)$, *J. Number Theory* 9 (1977) 229–239. <58, 59, 61, 62, 66>

[38] S. Agou, Irréductibilité des polynômes $f(X^{p^r} - aX)$ sur un corps fini $\mathbb{F}_{p^s}$, *J. Reine Angew. Math.* 292 (1977) 191–195. <56, 59, 61>

[39] S. Agou, Irréductibilité des polynômes $f(X^{p^{2r}} - aX^{p^r} - bX)$ sur un corps fini $\mathbb{F}_{p^s}$, *J. Number Theory* 10 (1978) 64–69. <56, 59, 61, 62, 66>

[40] S. Agou, Irréductibilité des polynômes $f(X^{p^{2r}} - aX^{p^r} - bX)$ sur un corps fini $\mathbb{F}_{p^s}$, *J. Number Theory* 11 (1979) 20. <56, 59, 61, 62, 66>

[41] S. Agou, Irréductibilité des polynômes $f(\sum_{i=0}^{m} a_i X^{p^{ri}})$ sur un corps fini $\mathbb{F}_{p^s}$, *Canad. Math. Bull.* 23 (1980) 207–212. <59, 61, 62, 66>

[42] S. Agou, Sur la factorisation des polynômes $f(X^{p^{2r}} - aX^{p^r} - bX)$ sur un corps fini $\mathbb{F}_{p^s}$, *J. Number Theory* 12 (1980) 447–459. <59, 61>

[43] M. Agrawal, N. Kayal, and N. Saxena, PRIMES is in P, *Ann. of Math., 2nd Ser.* 160 (2004) 781–793. <394, 397>

[44] S. Ahmad, Cycle structure of automorphisms of finite cyclic groups, *J. Combinatorial Theory* 6 (1969) 370–374. <221, 222>

[45] O. Ahmadi, Self-reciprocal irreducible pentanomials over $\mathbb{F}_2$, *Des. Codes Cryptogr.* 38 (2006) 395–397. <64, 66>

[46] O. Ahmadi, On the distribution of irreducible trinomials over $\mathbb{F}_3$, *Finite Fields Appl.* 13 (2007) 659–664. <65, 66>

[47] O. Ahmadi, The trace spectra of polynomial bases for $\mathbb{F}_{2^n}$, *Appl. Algebra Engrg. Comm. Comput.* 18 (2007) 391–396. <101, 103>

[48] O. Ahmadi, Generalization of a theorem of Carlitz, *Finite Fields Appl.* 17 (2011) 473–480. <53, 55>

[49] O. Ahmadi and R. Granger, An efficient deterministic test for Kloosterman sum zeros, 2011, submitted. <148, 155>

[50] O. Ahmadi, F. Luca, A. Ostafe, and I. E. Shparlinski, On stable quadratic polynomials, Preprint, 2010. <336, 337>

[51] O. Ahmadi and A. Menezes, On the number of trace-one elements in polynomial bases for $\mathbb{F}_{2^n}$, *Des. Codes Cryptogr.* 37 (2005) 493–507. <101, 103>

[52] O. Ahmadi and A. Menezes, Irreducible polynomials of maximum weight, *Util. Math.* 72 (2007) 111–123. <65, 66, 69>

[53] O. Ahmadi and I. E. Shparlinski, Bilinear character sums and sum-product problems on elliptic curves, *Proc. Edinb. Math. Soc., 2nd Ser.* 53 (2010) 1–12. <182, 186>

[54] O. Ahmadi, I. E. Shparlinski, and J. F. Voloch, Multiplicative order of Gauss periods, *Int. J. Number Theory* 6 (2010) 877–882. <94>

[55] O. Ahmadi and G. Vega, On the parity of the number of irreducible factors of self-reciprocal polynomials over finite fields, *Finite Fields Appl.* 14 (2008) 124–131. <68, 69>

[56] A. V. Aho, J. E. Hopcroft, and J. D. Ullman, *The Design and Analysis of Computer Algorithms*, Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1975, Second printing, Addison-Wesley Series in Computer Science and Information Processing. <352, 356>

[57] W. Aitken, On value sets of polynomials over a finite field, *Finite Fields Appl.* 4 (1998) 441–449. <228, 229>

[58] W. Aitken, M. D. Fried, and L. M. Holt, Davenport pairs over finite fields, *Pacific J. Math.* 216 (2004) 1–38. <232, 233>

[59] M. Ajtai, H. Iwaniec, J. Komlós, J. Pintz, and E. Szemerédi, Construction of a thin set with small Fourier coefficients, *Bull. London Math. Soc.* 22 (1990) 583–590. <178, 179>

[60] A. Akbary, S. Alaric, and Q. Wang, On some classes of permutation polynomials, *Int. J. Number Theory* 4 (2008) 121–133. <216, 217, 222>

[61] A. Akbary, D. Ghioca, and Q. Wang, On permutation polynomials of prescribed shape, *Finite Fields Appl.* 15 (2009) 195–206. <211, 212, 222>

[62] A. Akbary, D. Ghioca, and Q. Wang, On constructing permutations of finite fields, *Finite Fields Appl.* 17 (2010) 1–17. <213, 214, 217, 218, 222>

[63] A. Akbary and Q. Wang, On some permutation polynomials over finite fields, *Int. J. Math. Math. Sci.* 16 (2005) 2631–2640. <215, 222>

[64] A. Akbary and Q. Wang, A generalized Lucas sequence and permutation binomials, *Proc. Amer. Math. Soc.* 134 (2006) 15–22. <211, 215, 222>

[65] A. Akbary and Q. Wang, On polynomials of the form $x^r f(x^{(q-1)/l})$, *Int. J. Math. Math. Sci.* (2007) Art. ID 23408, 7. <214, 215, 216, 222>

[66] S. Akiyama, On the pure Jacobi sums, *Acta Arith.* 75 (1996) 97–104. <140, 155>

[67] M.-L. Akkar, N. T. Courtois, R. Duteuil, and L. Goubin, A fast and secure implementation of Sflash, In *Public Key Cryptography—PKC 2003*, volume 2567 of *Lecture Notes in Comput. Sci.*, 267–278, Springer, Berlin, 2002. <763, 774>

[68] E. Aksoy, A. Çeşmelioğlu, W. Meidl, and A. Topuzoğlu, On the Carlitz rank of permutation polynomials, *Finite Fields Appl.* 15 (2009) 428–440. <221, 222>

[69] A. A. Albert, Symmetric and alternate matrices in an arbitrary field. I, *Trans. Amer. Math. Soc.* 43 (1938) 386–436. <499, 502>

[70] A. A. Albert, *Fundamental Concepts of Higher Algebra*, University of Chicago Press, Chicago, IL, 1958. <57, 58, 59, 61>

[71] A. A. Albert, Finite division algebras and finite planes, In *Proc. Sympos. Appl. Math., Vol. 10*, 53–70, American Mathematical Society, Providence, RI, 1960. <268, 270>

[72] A. A. Albert, Generalized twisted fields, *Pacific J. Math.* 11 (1961) 1–8. <268>

[73] A. A. Albert, Isotopy for generalized twisted fields, *An. Acad. Brasil. Ci.* 33 (1961) 265–275. <268>

[74] R. Albert and H. G. Othmer, The topology of the regulatory interactions predicts the expression pattern of the segment polarity genes in *drosophila melanogaster*, *J. Theoret. Biol.* 223 (2003) 1–18. <815, 824>

[75] W. R. Alford, A. Granville, and C. Pomerance, There are infinitely many Carmichael numbers, *Ann. of Math., 2nd Ser.* 139 (1994) 703–722. <128, 132>

[76] N. Ali, Stabilité des polynômes, *Acta Arith.* 119 (2005) 53–63. <335, 337>

[77] B. Allombert, Explicit computation of isomorphisms between finite fields, *Finite Fields Appl.* 8 (2002) 332–342. <340, 356>

[78] J.-P. Allouche and J. Shallit, *Automatic Sequences: Theory, Applications, Generalizations*, Cambridge University Press, Cambridge, 2003. <538>

[79] J.-P. Allouche and D. S. Thakur, Automata and transcendence of the Tate period in finite characteristic, *Proc. Amer. Math. Soc.* 127 (1999) 1309–1312. <538>

[80] N. Alon, Eigenvalues and expanders, *Combinatorica* 6 (1986) 83–96. <637, 640, 649>

[81] N. Alon and F. R. K. Chung, Explicit construction of linear sized tolerant networks, *Discrete Math.* 72 (1988) 15–19. <636, 649>

[82] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira, and V. Rödl, Measures of pseudorandomness for finite sequences: typical values, *Proc. Lond. Math. Soc., 3rd Ser.* 95 (2007) 778–812. <176, 179>

[83] N. Alon and Y. Roichman, Random Cayley graphs and expanders, *Random Structures Algorithms* 5 (1994) 271–284. <642, 649>

[84] C. Alonso, J. Gutierrez, and T. Recio, A rational function decomposition algorithm by near-separated polynomials, *J. Symbolic Comput.* 19 (1995) 527–544. <292, 295>

[85] H. Aly, R. Marzouk, and W. Meidl, On the calculation of the linear complexity of periodic sequences, In *Finite Fields: Theory and Applications*, volume 518 of *Contemp. Math.*, 11–22, Amer. Math. Soc., Providence, RI, 2010. <322, 329>

[86] H. Aly and W. Meidl, On the linear complexity and k-error linear complexity over $\mathbb{F}_p$ of the d-ary Sidel′nikov sequence, *IEEE Trans. Inform. Theory* 53 (2007) 4755–4761. <327, 329>

[87] H. Aly and A. Winterhof, On the linear complexity profile of nonlinear congruential pseudorandom number generators with Dickson polynomials, *Des. Codes Cryptogr.* 39 (2006) 155–162. <326, 329>

[88] A. Ambainis and N. Nahimovs, Improved constructions of quantum automata, *Theoret. Comput. Sci.* 410 (2009) 1916–1922. <830, 831>

[89] P. R. Amestoy, T. A. Davis, and I. S. Duff, Algorithm 837: AMD, an approximate minimum degree ordering algorithm, *ACM Trans. Math. Software* 30 (2004) 381–388. <525, 527>

[90] G. An, In silico experiments of existing and hypothetical cytokine-directed clinical trials using agent-based modeling., *Crit Care Med* 32 (2004) 2050–2060. <821, 824>

[91] V. Anashin and A. Khrennikov, *Applied Algebraic Dynamics*, volume 49 of *de Gruyter Expositions in Mathematics*, de Gruyter, Berlin, 2009. <330, 331, 337>

[92] H. E. Andersen and O. Geil, Evaluation codes from order domain theory, *Finite Fields Appl.* 14 (2008) 92–123. <696, 703>

[93] B. A. Anderson and K. B. Gross, A partial starter construction, *Congress. Numer.* 21 (1978) 57–64. <606, 610>

[94] G. W. Anderson, t-motives, *Duke Math. J.* 53 (1986) 457–502. <538>

[95] G. W. Anderson, Log-algebraicity of twisted A-harmonic series and special values of L-series in characteristic p, *J. Number Theory* 60 (1996) 165–209. <533>

[96] G. W. Anderson, W. D. Brownawell, and M. A. Papanikolas, Determination of the algebraic relations among special Γ-values in positive characteristic, *Ann. of Math, 2nd Ser.* 160 (2004) 237–313. <538>

[97] G. W. Anderson and D. S. Thakur, Multizeta values for $\mathbb{F}_q[t]$, their period interpretation, and relations between them, *Int. Math. Res. Not. IMRN* (2009) 2038–2055. <536, 538>

[98] I. Anderson, A hundred years of whist tournaments, *J. Combin. Math. Combin. Comput.* 19 (1995) 129–150. <609, 610>

[99] I. Anderson, *Combinatorial Designs and Tournaments*, volume 6 of *Oxford Lecture*

Series in Mathematics and its Applications, The Clarendon Press, Oxford University Press, New York, 1997. <610>

[100] I. Anderson, Some cyclic and 1-rotational designs, In *Surveys in Combinatorics*, volume 288 of *London Math. Soc. Lecture Note Ser.*, 47–73, Cambridge Univ. Press, Cambridge, 2001. <609, 610>

[101] I. Anderson and N. J. Finizio, Some new z-cyclic whist tournament designs, *Discrete Math.* 293 (2005) 19–28. <609, 610>

[102] I. Anderson, N. J. Finizio, and P. A. Leonard, New product theorems for Z-cyclic whist tournaments, *J. Combin. Theory, Ser. A* 88 (1999) 162–166. <609, 610>

[103] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, Nested polar codes for wiretap and relay channels, *IEEE Comm. Letters* 14 (2010) 752–754. <730>

[104] J. André, Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe, *Math. Z.* 60 (1954) 156–186. <558, 565>

[105] B. Angles and C. Maire, A note on tamely ramified towers of global function fields, *Finite Fields Appl.* 8 (2002) 207–215. <456>

[106] J.-C. Anglès d'Auriac, J.-M. Maillard, and C. M. Viallet, On the complexity of some birational transformations, *J. Phys. A* 39 (2006) 3641–3654. <330, 337>

[107] B. Ansari and M. A. Hasan, High-performance architecture of elliptic curve scalar multiplication, *IEEE Trans. Comput.* 57 (2008) 1443–1453. <806, 813>

[108] ANSI, The elliptic curve digital signature algorithm (ECDSA), Working Draft American National Standard: Public Key Cryptography for the Financial Services Industry X9.62-1998, American National Standards Institute, 1998, Available at `http://grouper.ieee.org/groups/1363/private/x9-62-09-20-98.zip`. <776, 787>

[109] ANSI, Key agreement and key transport using elliptic curve cryptography, Working Draft American National Standard: Public Key Cryptography for the Financial Services Industry X9.63-199x, American National Standards Institute, 1999, Available at `http://grouper.ieee.org/groups/1363/private/x9-63-01-08-99.zip`. <776, 787>

[110] N. Anuradha and S. A. Katre, Number of points on the projective curves $aY^l = bX^l + cZ^l$ and $aY^{2l} = bX^{2l} + cZ^{2l}$ defined over finite fields, l an odd prime, *J. Number Theory* 77 (1999) 288–313. <202, 207>

[111] N. Aoki, Abelian fields generated by a Jacobi sum, *Comment. Math. Univ. St. Paul.* 45 (1996) 1–21. <140, 155>

[112] N. Aoki, On the purity problem of Gauss sums and Jacobi sums over finite fields, *Comment. Math. Univ. St. Paul.* 46 (1997) 223–233. <139, 140, 155>

[113] N. Aoki, A finiteness theorem on pure Gauss sums, *Comment. Math. Univ. St. Pauli* 53 (2004) 145–168. <139, 155>

[114] N. Aoki, On the zeta function of some cyclic quotients of Fermat curves, *Comment. Math. Univ. St. Pauli* 57 (2008) 163–185. <140, 155>

[115] N. Aoki, On multi-quadratic Gauss sums, *Comment. Math. Univ. St. Pauli* 59 (2010) 97–117. <144, 155>

[116] K. T. Arasu and K. J. Player, A new family of cyclic difference sets with Singer parameters in characteristic three, *Des. Codes Cryptogr.* 28 (2003) 75–91. <594, 598>

[117] E. Arikan, Channel combining and splitting for cutoff rate improvement, *IEEE Trans. Inform. Theory* 52 (2006) 628–639. <730>

[118] E. Arikan, A performance comparison of polar codes and Reed-Muller codes, *IEEE Comm. Letters* 12 (2008) 447–449. <730>

[119] E. Arikan, Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels, *IEEE Trans. Inform. Theory* 55 (2009) 3051–3073. <729, 730>

[120] E. Arikan, Polar codes: A pipelined implementation, In Proc. Int. Symp. Broadband Communication (ISBC2010), 2010. <730>

[121] E. Arikan, Source polarization, preprint available, `http://arxiv.org/abs/1001.3087`, 2010. <730>

[122] E. Arikan and E. Telatar, On the rate of channel polarization, preprint available, `http://arxiv.com/abs/0807.3806`, 2008. <729, 730>

[123] S. Arita, S. Miura, and T. Sekiguchi, An addition algorithm on the Jacobian varieties of curves, *J. Ramanujan Math. Soc.* 19 (2004) 235–251. <799, 802>

[124] V. L. Arlazarov, E. A. Dinic, M. A. Kronrod, and I. A. Faradžev, The economical construction of the transitive closure of an oriented graph, *Dokl. Akad. Nauk SSSR* 194 (1970) 487–488. <514, 527>

[125] C. Armana, Torsion des modules de Drinfeld de rang 2 et formes modulaires de Drinfeld, *C. R. Math. Acad. Sci. Paris, Ser. I* 347 (2009) 705–708. <537, 538>

[126] C. Armana, Coefficients of Drinfeld modular forms and Hecke operators, *J. Number Theory* 131 (2011) 1435–1460. <537, 538>

[127] M. A. Armand, Multisequence shift register synthesis over commutative rings with identity with applications to decoding cyclic codes over integer residue rings, *IEEE Trans. Inform. Theory* 50 (2004) 220–229. <322, 329>

[128] F. Armknecht and M. Krause, Algebraic attacks on combiners with memory, In *Advances in Cryptology—CRYPTO 2003*, volume 2729 of *Lecture Notes in Comput. Sci.*, 162–175, Springer, Berlin, 2003. <773, 774>

[129] F. Arnault, T. P. Berger, and M. Minier, Some results on FCSR automata with applications to the security of FCSR-based pseudorandom generators, *IEEE Trans. Inform. Theory* 54 (2008) 836–840. <329>

[130] F. Arnault, E. J. Pickett, and S. Vinatier, Construction of self-dual normal bases and their complexity, *Finite Fields Appl.* 18 (2012) 458–472. <36, 37, 40, 46, 109, 110, 117, 122>

[131] V. I. Arnold, *Dynamics, Statistics and Projective Geometry of Galois Fields*, Cambridge University Press, Cambridge, 2011. <29, 30>

[132] M. Arora, G. Ivanyos, M. Karpinski, and N. Saxena, Deterministic polynomial factoring and association schemes, Technical Report 68, ECCC, Electronic Colloquium on Computational Complexity, 2012. <374, 375>

[133] E. Artin, Quadratische Körper im Gebiete der höheren Kongruenzen. I, *Math. Z.* 19 (1924) 153–206. <444, 449>

[134] E. Artin, Quadratische Körper im Gebiete der höheren Kongruenzen. II., *Math. Z.* 19 (1924) 207–246. <69, 75, 487, 492>

[135] E. Artin, *Geometric Algebra*, Interscience Publishers, Inc., New York-London, 1957. <2, 10, 513>

[136] M. Artin, A. Grothendieck, and J. L. Verdier, *Théorie des Topos et Cohomologie Étale des Schémas. Tome 3*, Lecture Notes in Mathematics, Vol. 305. Springer-Verlag, Berlin, 1973, Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck et J. L. Verdier. Avec la collaboration de P. Deligne et B. Saint-Donat. <30, 463, 465, 470, 472>

[137] A. Arwin, Über Kongruenzen von dem fünften und höheren Graden nach einem Primzahlmodulus, *Ark. Mat. Astr. Fys.* 14 (1918) 1–46. <374, 375>

[138] M. Aschbacher, Isotopy and geotopy for ternary rings of projective planes, *J. Algebra* 319 (2008) 868–892. <270>

[139] D. W. Ash, I. F. Blake, and S. A. Vanstone, Low complexity normal bases, *Discrete Appl. Math.* 25 (1989) 191–210. <111, 113, 114, 122>

[140] A. Ashikhmin and E. Knill, Nonbinary quantum stabilizer codes, *IEEE Transactions on Information Theory* 47 (2001) 3065–3072. <827, 831>

[141] E. F. Assmus, Jr. and J. D. Key, *Designs and Their Codes*, volume 103 of *Cambridge Tracts in Mathematics*, Cambridge University Press, Cambridge, 1992. <29, 30, 301, 303>

[142] E. F. Assmus, Jr. and H. F. Mattson, Jr., New 5-designs, *J. Combinatorial Theory* 6 (1969) 122–151. <681, 694>

[143] A. O. L. Atkin and F. Morain, Elliptic curves and primality proving, *Math. Comp.* 61 (1993) 29–68. <340, 356>

[144] Y. Aubry and P. Langevin, On the weights of binary irreducible cyclic codes, In *Coding and Cryptography*, volume 3969 of *Lecture Notes in Comput. Sci.*, 46–54, Springer, Berlin, 2006. <146, 155>

[145] Y. Aubry and M. Perret, A Weil theorem for singular curves, In *Arithmetic, Geometry and Coding Theory*, 1–7, de Gruyter, Berlin, 1996. <231, 233>

[146] J.-P. Aumasson, M. Finiasz, W. Meier, and S. Vaudenay, A hardware-oriented trapdoor cipher, In J. Pieprzyk, H. Ghodosi, and E. Dawson, editors, *Information Security and Privacy*, volume 4586 of *Lecture Notes in Computer Science*, 184–199, Springer Berlin / Heidelberg, 2007. <621, 633>

[147] R. Avanzi, Aspects of hyperelliptic curves over large prime fields in software implementations, In *Proceedings of the Sixth International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 3156 of *Lecture Notes in Comput. Sci.*, 148–162, Springer, Berlin, 2004. <788, 794>

[148] R. Avanzi, N. Thériault, and Z. Wang, Rethinking low genus hyperelliptic Jacobian arithmetic over binary fields: interplay of field arithmetic and explicit formulae, *Journal Mathematical Cryptology* 2 (2008) 227–255. <790, 794>

[149] J. Ax, Zeroes of polynomials over finite fields, *Amer. J. Math.* 86 (1964) 255–261. <193, 195, 207, 473, 480>

[150] N. Axvig, D. Dreher, K. Morrison, E. Psota, L. C. Pérez, and J. L. Walker, Analysis of connections between pseudocodewords, *IEEE Trans. Inform. Theory* 55 (2009) 4099–4107. <709, 710>

[151] M. Ayad and D. L. McQuillan, Irreducibility of the iterates of a quadratic polynomial over a field, *Acta Arith.* 93 (2000) 87–97. <335, 337>

[152] M. Ayad and D. L. McQuillan, Corrections to: "Irreducibility of the iterates of a quadratic polynomial over a field" [Acta Arith. **93** (2000), 87–97; MR1760091 (2001c:11031)], *Acta Arith.* 99 (2001) 97. <335, 337>

[153] M. Baake, J. A. G. Roberts, and A. Weiss, Periodic orbits of linear endomorphisms on the 2-torus and its lattices, *Nonlinearity* 21 (2008) 2427–2446. <330, 337>

[154] L. Babai, The Fourier transform and equations over finite abelian groups, Private Communication. <303>

[155] L. Babai, Spectra of Cayley graphs, *J. Combin. Theory, Ser. B* 27 (1979) 180–189. <643, 649>

[156] L. Babai, W. M. Kantor, and A. Lubotsky, Small-diameter Cayley graphs for finite

simple groups, *European J. Combin.* 10 (1989) 507–522. <643, 649>

[157] E. Bach, J. von zur Gathen, and H. W. Lenstra, Jr., Factoring polynomials over special finite fields, *Finite Fields and Their Applications* 7 (2001) 5–28. <374, 375>

[158] E. Bach and J. Shallit, Factoring with cyclotomic polynomials, *Math. Comp.* 52 (1989) 201–219. <114, 122>

[159] D. V. Bailey, L. Batina, D. J. Bernstein, P. Birkner, J. W. Bos, H.-C. Chen, C.-M. Cheng, G. van Damme, G. de Meulenaer, L. J. Dominguez Perez, J. Fan, T. Güneysu, F. Gurkaynak, T. Kleinjung, T. Lange, N. Mentens, R. Niederhagen, C. Paar, F. Regazzoni, P. Schwabe, L. Uhsadel, A. Van Herrewege, and B.-Y. Yang, Breaking ECC2K-130, preprint, http://eprint.iacr.org/2009/541, 2009. <393, 394>

[160] D. V. Bailey and C. Paar, Optimal extension fields for fast arithmetic in public key algorithms, In *Advances in Cryptology—CRYPTO 1998*, volume 1462 of *Lecture Notes in Comput. Sci.*, Springer, Berlin, 1998. <346, 356>

[161] C. Bajaj, J. Canny, T. Garrity, and J. Warren, Factoring rational polynomials over the complex numbers, *SIAM J. Comput.* 22 (1993) 318–331. <380, 385>

[162] J.-C. Bajard, L.-S. Didier, and P. Kornerup, An RNS Montgomery modular multiplication algorithm, *IEEE Trans. Comput.* 47 (1998) 766–776. <345, 356>

[163] J.-C. Bajard, L. Imbert, and G. A. Jullien, Parallel Montgomery multiplication in $GF(2^k)$ using trinomial residue arithmetic, In *Proc. Seventeenth IEEE Symposium on Computer Arithmetic (ARITH-17)*, 164–171, 2005. <805, 813>

[164] J.-C. Bajard, L. Imbert, and T. Plantard, Arithmetic operations in the polynomial modular number system, In *IEEE Symposium on Computer Arithmetic*, 206–213, 2005. <345, 356>

[165] J.-C. Bajard, L. Imbert, and T. Plantard, Modular number systems: beyond the Mersenne family, In *Selected Areas in Cryptography*, volume 3357 of *Lecture Notes in Comput. Sci.*, 159–169, Springer, Berlin, 2005. <345, 356>

[166] R. Baker, Whist tournaments, *Congr. Numer.* 14 (1975) 89–100. <609, 610>

[167] R. C. Baker, Small solutions of congruences, *Mathematika* 30 (1983) 164–188. <207>

[168] R. D. Baker, C. Culbert, G. L. Ebert, and K. E. Mellinger, Odd order flag-transitive affine planes of dimension three over their kernel, *Adv. Geom.* (2003) S215–S223. <561, 565>

[169] R. D. Baker, J. M. Dover, G. L. Ebert, and K. L. Wantz, Hyperbolic fibrations of $PG(3, q)$, *European J. Combin.* 20 (1999) 1–16. <565>

[170] R. D. Baker, J. M. Dover, G. L. Ebert, and K. L. Wantz, Baer subgeometry partitions, *J. Geom.* 67 (2000) 23–34, Second Pythagorean Conference (Pythagoreion, 1999). <562, 565>

[171] R. D. Baker and G. L. Ebert, Nests of size $q - 1$ and another family of translation planes, *J. London Math. Soc., 2nd Ser.* 38 (1988) 341–355. <559, 565>

[172] R. D. Baker and G. L. Ebert, A new class of translation planes, In *Combinatorics '86*, volume 37 of *Ann. Discrete Math.*, 7–20, North-Holland, Amsterdam, 1988. <559, 565>

[173] R. D. Baker and G. L. Ebert, Filling the nest gaps, *Finite Fields Appl.* 2 (1996) 42–61. <559, 565>

[174] R. D. Baker and G. L. Ebert, Two-dimensional flag-transitive planes revisited, *Geom. Dedicata* 63 (1996) 1–15. <561, 565>

[175] R. D. Baker, G. L. Ebert, K. H. Leung, and Q. Xiang, A trace conjecture and flag-transitive affine planes, *J. Combin. Theory, Ser. A* 95 (2001) 158–168. <561, 565>

[176] R. D. Baker, G. L. Ebert, and T. Penttila, Hyperbolic fibrations and q-clans, *Des. Codes Cryptogr.* 34 (2005) 295–305. <564, 565>

[177] R. D. Baker, G. L. Ebert, and K. L. Wantz, Regular hyperbolic fibrations, *Adv. Geom.* 1 (2001) 119–144. <565>

[178] R. D. Baker, G. L. Ebert, and K. L. Wantz, Enumeration of nonsingular Buekenhout unitals, *Note Mat.* 29 (2009) 69–90. <563, 565>

[179] R. D. Baker, G. L. Ebert, and K. L. Wantz, Enumeration of orthogonal Buekenhout unitals, *Des. Codes Cryptogr.* 55 (2010) 261–283. <563, 565>

[180] M. Bakshi, S. Jaggi, and M. Effros, Concatenated polar codes, In *2010 IEEE International Symposium on Information Theory Proceedings (ISIT)*, 918–922, 2010. <730>

[181] J. Balakrishnan, J. Belding, S. Chisholm, K. Eisenträger, K. E. Stange, and E. Teske, Pairings on hyperelliptic curves, *Fields Inst. Commun.* 58 (2010) 1–34. <448, 449>

[182] R. Balasubramanian and N. Koblitz, The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm, *J. Cryptology* 11 (1998) 141–145. <779, 787>

[183] S. Ball, On the size of a triple blocking set in $\mathrm{PG}(2, q)$, *European J. Combin.* 17 (1996) 427–435. <554, 555>

[184] S. Ball, The number of directions determined by a function over a finite field, *J. Combin. Theory, Ser. A* 104 (2003) 341–350. <550, 555>

[185] S. Ball, On the graph of a function in many variables over a finite field, *Des. Codes Cryptogr.* 47 (2008) 159–164. <551, 555>

[186] S. Ball, The polynomial method in Galois geometries, In *Current Research Topics in Galois Geometry*, Mathematics Research Developments, Nova, 2011, to appear. <554, 555>

[187] S. Ball and A. Blokhuis, On the size of a double blocking set in $\mathrm{PG}(2, q)$, *Finite Fields Appl.* 2 (1996) 125–137. <554, 555>

[188] S. Ball, A. Blokhuis, and F. Mazzocca, Maximal arcs in Desarguesian planes of odd order do not exist, *Combinatorica* 17 (1997) 31–41. <564, 565>

[189] S. Ball and A. Gács, On the graph of a function over a prime field whose small powers have bounded degree, *European J. Combin.* 30 (2009) 1575–1584. <551, 555>

[190] S. Ball, A. Gács, and P. Sziklai, On the number of directions determined by a pair of functions over a prime field, *J. Combin. Theory, Ser. A* 115 (2008) 505–516. <551, 555>

[191] S. Ball and M. Zieve, Symplectic spreads and permutation polynomials, In *Finite Fields and Applications*, volume 2948 of *Lecture Notes in Comput. Sci.*, 79–88, Springer, Berlin, 2004. <222>

[192] A. Balog, Many additive quadruples, In *Additive Combinatorics*, volume 43 of *CRM Proc. Lecture Notes*, 39–49, Amer. Math. Soc., Providence, RI, 2007. <182, 186>

[193] A. Balog and E. Szemerédi, A statistical theorem of set addition, *Combinatorica* 14 (1994) 263–268. <182, 186>

[194] J. Bamberg, A. Betten, C. Praeger, and A. Wassermann, Unitals in the Desargue-

sian projective plane of order sixteen, International Conference on Design of Experiments (ICODOE, 2011). <563, 565>

[195] W. D. Banks, A. Conflitti, J. B. Friedlander, and I. E. Shparlinski, Exponential sums over Mersenne numbers, *Compos. Math.* 140 (2004) 15–30. <183, 186>

[196] W. D. Banks, J. B. Friedlander, S. V. Konyagin, and I. E. Shparlinski, Incomplete exponential sums and Diffie-Hellman triples, *Math. Proc. Cambridge Philos. Soc.* 140 (2006) 193–206. <177, 179>

[197] H. W. Bao, On two exponential sums and their applications, *Finite Fields Appl.* 3 (1997) 115–130. <88, 90>

[198] I. Baoulina, On the number of solutions to certain diagonal equations over finite fields, *Int. J. Number Theory* 6 (2010) 1–14. <202, 207>

[199] B. Barak, G. Kindler, R. Shaltiel, B. Sudakov, and A. Wigderson, Simulating independence: new constructions of condensers, Ramsey graphs, dispersers, and extractors, *J. ACM* 57 (2010) Art. 20, 52. <185, 186>

[200] M. Bardet, J.-C. Faugère, and B. Salvy, On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations, In *Proceedings of the International Conference on Polynomial System Solving*, 71–74, 2004. <773, 774>

[201] A. Barlotti, Un'estensione del teorema di Segre-Kustaanheimo, *Boll. Un. Mat. Ital.* 10 (1955) 498–506. <579, 580>

[202] P. S. L. M. Barreto, S. D. Galbraith, C. Ó'hÉigeartaigh, and M. Scott, Efficient pairing computation on supersingular abelian varieties, *Designs, Codes and Cryptography* 42 (2007) 239–271. <782, 787>

[203] P. S. L. M. Barreto and J. F. Voloch, Efficient computation of roots in finite fields, *Des. Codes Cryptogr.* 39 (2006) 275–280. <353, 356>

[204] S. Barwick and G. Ebert, *Unitals in Projective Planes*, Springer Monographs in Mathematics. Springer, New York, 2008. <562, 565>

[205] S. G. Barwick and W.-A. Jackson, Geometric constructions of optimal linear perfect hash families, *Finite Fields Appl.* 14 (2008) 1–13. <604, 610>

[206] S. G. Barwick, W.-A. Jackson, and C. T. Quinn, Optimal linear perfect hash families with small parameters, *J. Combin. Des.* 12 (2004) 311–324. <604, 610>

[207] L. Batina, S. B. Örs, B. Preneel, and J. Vandewalle, Hardware architectures for public key cryptography, *Integration, the VLSI Journal* 34 (2003) 1 – 64. <103>

[208] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier, PARI/GP, version 2.5.0, 2011, available at `http://pari.math.u-bordeaux.fr/`. <339, 356>

[209] L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics, Vol. 182. Springer-Verlag, Berlin, 1971. <29, 30, 591, 593, 598>

[210] E. Bayer-Fluckiger and H. W. Lenstra, Jr., Forms in odd degree extensions and self-dual normal bases, *Amer. J. Math.* 112 (1990) 359–373. <108, 110>

[211] J. T. Beard, Jr. and K. I. West, Factorization tables for $x^n - 1$ over GF(q), *Math. Comp.* 28 (1974) 1167–1168. <58, 61>

[212] B. Beckermann and G. Labahn, Fraction-free computation of matrix rational interpolants and matrix GCDs, *SIAM J. Matrix Anal. Appl.* 22 (2000) 114–144. <527>

[213] E. Bedford and K. Kim, Continuous families of rational surface automorphisms with positive entropy, *Math. Ann.* 348 (2010) 667–688. <331, 337>

[214] E. Bedford and T. T. Truong, Degree complexity of birational maps related to matrix inversion, *Comm. Math. Phys.* 298 (2010) 357–368. <330, 331, 337>

[215] P. Beelen and I. I. Bouw, Asymptotically good towers and differential equations, *Compos. Math.* 141 (2005) 1405–1424. <457, 462>

[216] D. Behr, Searchable magic book contents, main site:`http://archive.denisbehr.de`, `http://archive.denisbehr.de/archive/route/entries.php?url=10,50,1036`. <623, 633>

[217] K. Belabas, M. van Hoeij, J. Klüners, and A. Steel, Factoring polynomials over global fields, *J. Théor. Nombres Bordeaux* 21 (2009) 15–39. <378, 385>

[218] J. Belding, R. Brker, A. Enge, and K. Lauter, Computing Hilbert class polynomials, In A. van der Poorten and A. Stein, editors, *Algorithmic Number Theory—ANTS-VIII*, volume 5011 of *Lecture Notes in Computer Science*, 282–295, Berlin, 2008, Springer-Verlag. <777, 787>

[219] M. Bellare and P. Rogaway, Minimizing the use of random oracles in authenticated encryption schemes, In Y. Han, T. Okamoto, and S. Qing, editors, *Information and Communications Security*, volume 1334 of *Lecture Notes in Computer Science*, 1–16, Berlin, 1997, Springer-Verlag. <776, 787>

[220] M. P. Bellon and C.-M. Viallet, Algebraic entropy, *Comm. Math. Phys.* 204 (1999) 425–437. <330, 331, 337>

[221] M. Ben-Or, Probabilistic algorithms in finite fields, In *Proc. Twenty Second IEEE Symp. Foundations Computer Science*, 394–398, 1981. <370, 373>

[222] T. D. Bending and D. Fon-Der-Flaass, Crooked functions, bent functions, and distance regular graphs, *Electron. J. Combin.* 5 (1998) Research Paper 34, 14 pp. <252, 254>

[223] S. Benedetto, D. Divsalar, G. Montorsi, and F. Pollara, Serial concatenation of interleaved codes: performance analysis, design, and iterative decoding, *IEEE Trans. Inform. Theory* 44 (1998) 909–926. <712, 718>

[224] A. T. Benjamin and C. D. Bennett, The probability of relatively prime polynomials, *Math. Mag.* 80 (2007) 196–202. <77, 81, 501, 502>

[225] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, In *International Conference on Computers, Systems & Signal Processing*, 1984. <739, 740>

[226] T. P. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy, On almost perfect nonlinear functions over F_2^n, *IEEE Trans. Inform. Theory* 52 (2006) 4160–4170. <249, 252, 254>

[227] E. R. Berlekamp, Distribution of cyclic matrices in a finite field, *Duke Math. J.* 33 (1966) 45–48. <58, 61>

[228] E. R. Berlekamp, Factoring polynomials over finite fields, *Bell System Tech. J.* 46 (1967) 1853–1859. <368, 373, 374, 375, 761, 774>

[229] E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill Book Co., New York, 1968. <29, 30, 56, 61, 64, 65, 66, 199, 200, 307, 310, 358, 360, 367, 652, 683, 684, 694>

[230] E. R. Berlekamp, Factoring polynomials over large finite fields, *Mathematics of Computation* 24 (1970) 713–735. <373, 374, 375>

[231] E. R. Berlekamp, editor, *Key Papers in the Development of Coding Theory*, IEEE Press Sel. Rep. Ser., New York, 1974. <693, 694>

[232] E. R. Berlekamp, Bit-serial Reed-Solomon encoders., *IEEE Trans. Inf. Theory* 28 (1982) 869–874. <103>

[233] E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg, On the inherent intractability of certain coding problems, *IEEE Trans. Information Theory* IT-24 (1978) 384–386. <739, 740>

[234] E. R. Berlekamp, H. Rumsey, and G. Solomon, On the solution of algebraic equations over finite fields, *Information and Control* 10 (1967) 553–564. <65, 66>

[235] L. Bernardin, On square-free factorization of multivariate polynomials over a finite field, *Theoret. Comput. Sci.* 187 (1997) 105–116. <377, 385>

[236] L. Bernardin, On bivariate Hensel lifting and its parallelization, In *ISSAC '98: Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation*, 96–100, New York, 1998, ACM. <378, 385>

[237] L. Bernardin and M. B. Monagan, Efficient multivariate factorization over finite fields, In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 1255 of *Lecture Notes in Comput. Sci.*, 15–28, Springer-Verlag, 1997. <380, 385>

[238] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons Inc., New York, 1998. <29, 30, 133, 134, 135, 136, 137, 139, 140, 141, 142, 143, 144, 145, 146, 147, 150, 153, 154, 155, 167, 179, 200, 207>

[239] D. J. Bernstein, Multiplication for mathematicians, 2001, preprint available at `http://cr.yp.to/papers.html#m3`. <805, 813>

[240] D. J. Bernstein, Pippenger's exponentiation algorithm, 2002, preprint available at `http://cr.yp.to/papers/pippenger.pdf`. <349, 356>

[241] D. J. Bernstein, Batch binary Edwards, In *Advances in Cryptology—CRYPTO 2009*, volume 5677 of *Lecture Notes in Comput. Sci.*, 317–336, Springer, Berlin, 2009. <804, 805, 813>

[242] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters, Twisted Edwards curves, In *Progress in Cryptology—AFRICACRYPT 2008*, volume 5023 of *Lecture Notes in Comput. Sci.*, 389–405, Springer, Berlin, 2008. <434, 440>

[243] D. J. Bernstein, J. Buchmann, and E. Dahmen, editors, *Post-Quantum Cryptography*, Springer-Verlag, Berlin, 2009. <29, 30, 739, 740>

[244] D. J. Bernstein and T. Lange, Explicit-formulas database, `http://hyperelliptic.org/EFD/`. <437, 440>

[245] D. J. Bernstein and T. Lange, Faster addition and doubling on elliptic curves, In *Advances in Cryptology—ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Comput. Sci.*, 29–50, Springer, Berlin, 2007. <434, 435, 440>

[246] D. J. Bernstein and T. Lange, Type-II optimal polynomial bases, In *Arithmetic of Finite Fields*, volume 6087 of *Lecture Notes in Comput. Sci.*, 41–61, Springer, Berlin, 2010. <121, 122, 813>

[247] D. J. Bernstein and T. Lange, A complete set of addition laws for incomplete Edwards curves, *J. Number Theory* 131 (2011) 858–872. <436, 440>

[248] D. J. Bernstein, T. Lange, and C. Peters, Attacking and defending the McEliece cryptosystem, In *Post-Quantum Cryptography*, volume 5299 of *Lecture Notes in Comput. Sci.*, 31–46, Springer, Berlin, 2008. <740>

[249] C. Berrou, A. Glavieux, and P. Thitimajshima, Near Shannon limit error-correcting coding and decoding: turbo-codes, In *Proc. IEEE Int. Conf. on Commun.*, 1064–1070, Geneva, Switzerland, 1993. <710, 718>

[250] C. Berrou, S. K. Y. Saouter, C. Douillard, and M. Jézéquel, Designing good permutations for turbo codes: towards a single model, In *Proc. International Con-*

ference on Communications, volume 1, 341–345, Paris, France, 2004. <717, 718>

[251] P. Berthelot, Cohomologie rigide et théorie de Dwork: le cas des sommes exponentielles, *Astérisque* (1984) 3, 17–49, p-adic cohomology. <163>

[252] P. Berthelot, S. Bloch, and H. Esnault, On Witt vector cohomology for singular varieties, *Compos. Math.* 143 (2007) 363–392. <194, 195>

[253] P. Berthelot and A. Ogus, *Notes on Crystalline Cohomology*, Princeton University Press, Princeton, NJ, 1978. <474, 480>

[254] J. Berthomieu and G. Lecerf, Convex-dense bivariate polynomial factorization, Manuscript available from `http://hal.archives-ouvertes.fr/hal-00526659`, to appear in Math. Comp., 2010. <382, 385>

[255] T. Beth and Z. D. Dai, On the complexity of pseudo-random sequences—or: If you can describe a sequence it can't be random, In *Advances in Cryptology—EUROCRYPT '89*, volume 434 of *Lecture Notes in Comput. Sci.*, 533–543, Springer, Berlin, 1990. <328, 329>

[256] T. Beth and W. Geiselmann, Selbstduale Normalbasen über GF(q), *Arch. Math. (Basel)* 55 (1990) 44–48. <109, 110, 498, 502>

[257] T. Beth, W. Geiselmann, and F. Meyer, Finding (good) normal bases in finite fields, In *Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation*, ISSAC '91, 173–178, New York, NY, USA, 1991, ACM. <114, 122>

[258] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Cambridge University Press, Cambridge, 1986. <29, 30, 164, 179>

[259] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory. Vol. I*, volume 69 of *Encyclopedia of Mathematics and its Applications*, Cambridge University Press, Cambridge, second edition, 1999. <29, 30, 584, 590, 591, 596, 597, 598, 610>

[260] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory. Vol. II*, volume 78 of *Encyclopedia of Mathematics and its Applications*, Cambridge University Press, Cambridge, second edition, 1999. <29, 30, 590, 591, 592, 594, 595, 596, 597, 598, 610>

[261] D. Betten and D. G. Glynn, Über endliche planare Funktionen, ihre zugehörenden Schiebebenen, und ihre abgeleiteten Translationsebenen, *Results Math.* 42 (2002) 32–36. <272, 274>

[262] C. Bey and G. M. Kyureghyan, On Boolean functions with the sum of every two of them being bent, *Des. Codes Cryptogr.* 49 (2008) 341–346. <247, 254>

[263] J. Bezerra, A. Garcia, and H. Stichtenoth, An explicit tower of function fields over cubic finite fields and Zink's lower bound, *J. Reine Angew. Math.* 589 (2005) 159–199. <456, 461, 462>

[264] M. Bhargava and M. E. Zieve, Factoring Dickson polynomials over finite fields, *Finite Fields Appl.* 5 (1999) 103–111. <276, 277, 282>

[265] A. Bhattacharyya, S. Kopparty, G. Schoenebeck, M. Sudan, and D. Zuckerman, Optimal testing of Reed-Muller codes (report no. 86), In *Proceedings of Electronic Colloquium on Computational Complexity (2009)*, volume 3690 of *Lecture Notes in Comput. Sci.*, 269–275, Springer, 2011. <239, 245>

[266] K. Bibak, Additive combinatorics with a view towards computer science and cryptography: An exposition, *arXiv:1108.3790.* <183, 185, 186>

[267] F. Bien, Constructions of telephone networks by group representations, *Notices Amer. Math. Soc.* 36 (1989) 5–22. <633, 640, 649>

[268] J. Bierbrauer, *Introduction to Coding Theory*, Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton, FL, 2005. <29, 30>

[269] J. Bierbrauer, A direct approach to linear programming bounds for codes and (t, m, s)-nets, *Des. Codes Cryptogr.* 42 (2007) 127–143. <612, 621>

[270] J. Bierbrauer, A family of crooked functions, *Des. Codes Cryptogr.* 50 (2009) 235–241. <252, 254>

[271] J. Bierbrauer, New commutative semifields and their nuclei, In *Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, volume 5527 of *Lecture Notes in Comput. Sci.*, 179–185, Springer, Berlin, 2009. <274>

[272] J. Bierbrauer, New semifields, PN and APN functions, *Des. Codes Cryptogr.* 54 (2010) 189–200. <274>

[273] J. Bierbrauer and Y. Edel, Theory of perpendicular arrays, *J. Combin. Des.* 2 (1994) 375–406. <603, 610>

[274] J. Bierbrauer, Y. Edel, and W. C. Schmid, Coding-theoretic constructions for (t, m, s)-nets and ordered orthogonal arrays, *J. Combin. Des.* 10 (2002) 403–418. <613, 616, 621>

[275] J. Bierbrauer and G. M. Kyureghyan, Crooked binomials, *Des. Codes Cryptogr.* 46 (2008) 269–301. <252, 254>

[276] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, *J. Cryptology* 4 (1991) 3–72. <246, 254>

[277] M. Biliotti, V. Jha, and N. L. Johnson, *Foundations of Translation Planes*, volume 243 of *Monographs and Textbooks in Pure and Applied Mathematics*, Marcel Dekker Inc., New York, 2001. <557, 565>

[278] O. Billet and H. Gilbert, Cryptanalysis of Rainbow, In *Security and Cryptography for Networks*, volume 4116 of *Lecture Notes in Comput. Sci.*, 336–347. Springer, 2006. <763, 764, 774>

[279] O. Billet, M. J. B. Robshaw, and T. Peyrin, On building hash functions from multivariate quadratic equations, In J. Pieprzyk, H. Ghodosi, and E. Dawson, editors, *ACISP*, volume 4586 of *Lecture Notes in Computer Science*, 82–95. Springer, 2007. <774>

[280] Y. Bilu and N. Linial, Lifts, discrepancy and nearly optimal spectral gap, *Combinatorica* 26 (2006) 495–519. <637, 647, 648, 649>

[281] G. Bini and F. Flamini, *Finite Commutative Rings and their Applications*, The Kluwer International Series in Engineering and Computer Science, 680. Kluwer Academic Publishers, Boston, MA, 2002. <27, 29>

[282] B. J. Birch, How the number of points of an elliptic curve over a fixed prime field varies, *J. London Math. Soc., 2nd Ser.* 43 (1968) 57–60. <423, 433>

[283] B. J. Birch and H. P. F. Swinnerton-Dyer, Note on a problem of Chowla, *Acta Arith.* 5 (1959) 417–423 (1959). <226, 229>

[284] P. Birkner, Efficient divisor class halving on genus two curves, In *Thirteenth International Workshop on Selected Areas in Cryptography*, volume 4356 of *Lecture Notes in Comput. Sci.*, 317–326, Springer, Berlin, 2007. <788, 794>

[285] P. Birkner and N. Thériault, Faster halvings in genus 2, In *Fifteenth International Workshop on Selected Areas in Cryptography*, volume 5381 of *Lecture Notes in Comput. Sci.*, 1–17, Springer, Berlin, 2009. <788, 794>

[286] P. Birkner and N. Thériault, Efficient halving for genus 3 curves over binary fields, *Advances in Mathematics of Communications* 4 (2010) 23–47. <790, 794>

[287] A. Biró, On polynomials over prime fields taking only two values on the multiplica-

tive group, *Finite Fields Appl.* 6 (2000) 302–308. <226, 229>

[288] R. R. Bitmead and B. D. O. Anderson, Asymptotically fast solution of Toeplitz and related systems of linear equations, *Linear Algebra Appl.* 34 (1980) 103–116. <526, 527>

[289] R. Blache, p-Density, exponential sums and Artin-Schreier curves, preprint available, `http://arxiv.org/abs/0812.3382`, 2008. <473, 477, 480>

[290] R. Blache, First vertices for generic Newton polygons, and p-cyclic coverings of the projective line, preprint available, `http://arxiv.org/abs/0912.2051`, 2009. <477, 480>

[291] R. Blache, Newton polygons for character sums and Poincaré series, *Int. J. Number Theory* 7 (2011) 1519–1542. <478, 480>

[292] R. Blache, J.-P. Cherdieu, and J. Estrada Sarlabous, Some computational aspects of Jacobians of curves in the family $y^3 = \gamma x^5 + \delta$ over $\mathbb{F}_p$, *Finite Fields Appl.* 13 (2007) 348–365. <798, 802>

[293] R. Blache and É. Férard, Newton stratification for polynomials: the open stratum, *J. Number Theory* 123 (2007) 456–472. <477, 480>

[294] R. Blache, É. Férard, and H. J. Zhu, Hodge-Stickelberger polygons for L-functions of exponential sums of $P(x^s)$, *Math. Res. Lett.* 15 (2008) 1053–1071. <477, 478, 480>

[295] S. R. Blackburn, A generalisation of the discrete Fourier transform: determining the minimal polynomial of a periodic sequence, *IEEE Trans. Inform. Theory* 40 (1994) 1702–1704. <321, 329>

[296] S. R. Blackburn, T. Etzion, and K. G. Paterson, Permutation polynomials, de Bruijn sequences, and linear complexity, *J. Combin. Theory, Ser. A* 76 (1996) 55–82. <322, 329>

[297] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez, and I. E. Shparlinski, Predicting the inversive generator, In *Cryptography and Coding*, volume 2898 of *Lecture Notes in Comput. Sci.*, 264–275, Springer, Berlin, 2003. <331, 337>

[298] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez, and I. E. Shparlinski, Predicting nonlinear pseudorandom number generators, *Math. Comp.* 74 (2005) 1471–1494. <331, 337>

[299] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez, and I. E. Shparlinski, Reconstructing noisy polynomial evaluation in residue rings, *J. Algorithms* 61 (2006) 47–59. <331, 337>

[300] S. R. Blackburn and P. R. Wild, Optimal linear perfect hash families, *J. Combin. Theory, Ser. A* 83 (1998) 233–250. <604, 610>

[301] R. E. Blahut, Transform techniques for error control codes, *IBM J. Res. Develop.* 23 (1979) 299–315. <321, 329>

[302] R. E. Blahut, *Theory and Practice of Error Control Codes*, Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1983. <29, 30, 652, 654, 671, 679, 681, 683, 684, 694>

[303] I. F. Blake, editor, *Algebraic Coding Theory: History and Development*, Dowden Hutchinson & Ross Inc., Stroudsburg, Pa., 1973, Benchmark Papers in Electrical Engineering and Computer Science. <693, 694>

[304] I. F. Blake, R. Fuji-Hara, R. C. Mullin, and S. A. Vanstone, Computing logarithms in finite fields of characteristic two, *SIAM J. Algebraic Discrete Methods* 5 (1984) 276–285. <363, 367>

[305] I. F. Blake, S. Gao, and R. J. Lambert, Construction and distribution problems

for irreducible trinomials over finite fields, In *Applications of Finite Fields*, volume 59 of *Inst. Math. Appl. Conf. Ser. (New Ser.)*, 19–32, Oxford Univ. Press, New York, 1996. <68, 69, 84, 85>

[306] I. F. Blake, S. Gao, and R. C. Mullin, Normal and self-dual normal bases from factorization of $cx^{q+1} + dx^q - ax - b$, *SIAM J. Discrete Math.* 7 (1994) 499–512. <112, 118, 122>

[307] I. F. Blake, S. Gao, and R. C. Mullin, Specific irreducible polynomials with linearly independent roots over finite fields, *Linear Algebra Appl.* 253 (1997) 227–249. <107, 110, 124, 131, 132>

[308] I. F. Blake and T. Garefalakis, A transform property of Kloosterman sums, *Discrete Appl. Math.* 158 (2010) 1064–1072. <70, 75>

[309] I. F. Blake and R. C. Mullin, *The Mathematical Theory of Coding*, Academic Press, New York-London, 1975. <29, 30, 652, 674, 678, 694>

[310] I. F. Blake, G. Seroussi, and N. P. Smart, *Elliptic Curves in Cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*, Cambridge University Press, Cambridge, 2000, Reprint of the 1999 original. <29, 30, 778, 787>

[311] I. F. Blake, G. Seroussi, and N. P. Smart, *Advances in Elliptic Curve Cryptography*, volume 317 of *London Mathematical Society Lecture Note Series*, Cambridge University Press, Cambridge, 2005. <29, 30, 776, 779, 787, 794>

[312] R. Blasco-Serrano, R. Thobaben, V. Rathi, and M. Skoglund, Polar codes for compress-and-forward in binary relay channels, In *Proc. Conf Signals, Systems and Computers (ASILOMAR) Record of the Forty Fourth Asilomar Conf*, 1743–1747. <730>

[313] D. Blessenohl, Abelsche Erweiterungen, in denen jedes reguläre Element vollständig regulär ist, *Arch. Math. (Basel)* 54 (1990) 146–156. <123, 124, 132>

[314] D. Blessenohl, Zu einer Vermutung von Morgan und Mullen, *Berichtsreihe des Mathematischen Seminars der Universität Kiel* 05-21 (2005). <131, 132>

[315] D. Blessenohl and K. Johnsen, Eine Verschärfung des Satzes von der Normalbasis, *J. Algebra* 103 (1986) 141–159. <123, 132>

[316] D. Blessenohl and K. Johnsen, Stabile Teilkörper galoisscher Erweiterungen und ein Problem von C. Faith, *Arch. Math. (Basel)* 56 (1991) 245–253. <124, 132>

[317] A. Blokhuis, On the size of a blocking set in $\mathrm{PG}(2, p)$, *Combinatorica* 14 (1994) 111–114. <551, 552, 555>

[318] A. Blokhuis, Blocking sets in Desarguesian planes, In *Combinatorics, Paul Erdős is Eighty, Vol. 2*, volume 2 of *Bolyai Soc. Math. Stud.*, 133–155, János Bolyai Math. Soc., Budapest, 1996. <551, 552, 555>

[319] A. Blokhuis, S. Ball, A. E. Brouwer, L. Storme, and T. Szőnyi, On the number of slopes of the graph of a function defined on a finite field, *J. Combin. Theory, Ser. A* 86 (1999) 187–196. <550, 555>

[320] A. Blokhuis, A. E. Brouwer, and T. Szőnyi, The number of directions determined by a function f on a finite field, *J. Combin. Theory, Ser. A* 70 (1995) 349–353. <550, 555>

[321] A. Blokhuis, A. E. Brouwer, and H. A. Wilbrink, Blocking sets in $\mathrm{PG}(2, p)$ for small p, and partial spreads in $\mathrm{PG}(3, 7)$, *Adv. Geom.* (2003) S245–S253. <553, 555>

[322] A. Blokhuis, A. A. Bruen, and J. A. Thas, Arcs in $\mathrm{PG}(n, q)$, MDS-codes and three fundamental problems of B. Segre—some extensions, *Geom. Dedicata* 35 (1990) 1–11. <577, 580>

[323] A. Blokhuis, R. S. Coulter, M. Henderson, and C. M. O'Keefe, Permutations

amongst the Dembowski-Ostrom polynomials, In *Finite Fields and Applications*, 37–42, Springer, Berlin, 2001. <217, 218, 222>

[324] A. Blokhuis, D. Jungnickel, and B. Schmidt, Proof of the prime power conjecture for projective planes of order n with abelian collineation groups of order n^2, *Proc. Amer. Math. Soc.* 130 (2002) 1473–1476. <271, 274, 564, 565>

[325] A. Blokhuis, M. Lavrauw, and S. Ball, On the classification of semifield flocks, *Adv. Math.* 180 (2003) 104–111. <270>

[326] A. Blokhuis, L. Lovász, L. Storme, and T. Szőnyi, On multiple blocking sets in Galois planes, *Adv. Geom.* 7 (2007) 39–53. <554, 555>

[327] A. Blokhuis, R. Pellikaan, and T. Szőnyi, Blocking sets of almost Rédei type, *J. Combin. Theory, Ser. A* 78 (1997) 141–150. <551, 555>

[328] A. Blokhuis, L. Storme, and T. Szőnyi, Lacunary polynomials, multiple blocking sets and Baer subplanes, *J. London Math. Soc., 2nd Ser.* 60 (1999) 321–332. <554, 555>

[329] C. Blondeau, A. Canteaut, and P. Charpin, Differential properties of power functions, *Int. J. Inf. Coding Theory* 1 (2010) 149–170. <254>

[330] A. W. Bluher, Explicit formulas for strong Davenport pairs, *Acta Arith.* 112 (2004) 397–403. <293, 295>

[331] A. W. Bluher, A Swan-like theorem, *Finite Fields Appl.* 12 (2006) 128–138. <65, 66>

[332] G. Böckle, An eichler-shimura isomorphism over function fields between Drinfeld modular forms and cohomology classes of crystals, *preprint* (2002). <537, 538>

[333] G. Böckle, Global L-functions over function fields, *Math. Ann.* 323 (2002) 737–795. <534, 538>

[334] A. Bodin, Number of irreducible polynomials in several variables over finite fields, *Amer. Math. Monthly* 115 (2008) 653–660. <76, 81>

[335] A. Bodin, Generating series for irreducible polynomials over finite fields, *Finite Fields Appl.* 16 (2010) 116–125. <76, 77, 81>

[336] A. Bodin, P. Dèbes, and S. Najib, Indecomposable polynomials and their spectrum, *Acta Arith.* 139 (2009) 79–100. <79, 81>

[337] E. Bombieri, On exponential sums in finite fields, *Amer. J. Math.* 88 (1966) 71–105. <157, 163, 466, 469, 472>

[338] E. Bombieri, Counting points on curves over finite fields (d'après S. A. Stepanov), In *Séminaire Bourbaki, 25ème année (1972/1973), Exp. No. 430*, 234–241. Lecture Notes in Math., Vol. 383, Springer, Berlin, 1974. <470, 472>

[339] E. Bombieri, On exponential sums in finite fields. II, *Invent. Math.* 47 (1978) 29–39. <158, 163, 294, 295, 466, 469, 472>

[340] E. Bombieri and S. Sperber, On the estimation of certain exponential sums, *Acta Arith.* 69 (1995) 329–358. <158, 163>

[341] D. Bonchev, S. Thomas, A. Apte, and L. B. Kier, Cellular automata modelling of biomolecular networks dynamics, *SAR and QSAR in Environmental Research* 21 (2010) 77–102. <817, 824>

[342] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, *SIAM J. Comput.* 32 (2003) 586–615. <738, 740>

[343] D. Boneh, E.-J. Goh, and K. Nissim, Evaluating 2-DNF formulas on ciphertexts, In J. Kilian, editor, *Theory of Cryptography—TCC 2005*, volume 3378 of *Lecture*

Notes in Computer Science, 325–341, Berlin, 2005, Springer-Verlag. <783, 787>

[344] D. Boneh, B. Lynn, and H. Shacham, Short signatures from the Weil pairing, *J. Cryptology* 17 (2004) 297–319. <738, 740>

[345] D. Boneh and R. Venkatesan, Rounding in lattices and its cryptographic applications, In *Proceedings of the Eighth Annual ACM-SIAM Symposium on Discrete Algorithms*, 675–681, New York, 1997, ACM. <170, 179>

[346] D. Boneh and R. Venkatesan, Breaking RSA may not be equivalent to factoring (extended abstract), In *Advances in Cryptology—EUROCRYPT '98*, volume 1403 of *Lecture Notes in Comput. Sci.*, 59–71, Springer, Berlin, 1998. <170, 179>

[347] T. J. Boothby and R. W. Bradshaw, Bitslicing and the method of four Russians over larger finite fields, preprint available, `http://arxiv.org/abs/0901.1413`, 2009. <514, 527>

[348] H. Borges, Frobenius non-classical curves of type $g(y) = f(x)$, preprint, 2012. <226, 229>

[349] H. Borges and F. Conceição, On the characterization of minimal value set polynomials, preprint, 2012. <226, 229>

[350] P. Borwein, K.-K. S. Choi, and J. Jedwab, Binary sequences with merit factor greater than 6.34, *IEEE Trans. Inform. Theory* 50 (2004) 3234–3249. <316, 317>

[351] J. Bos and M. E. Kaihara, Playstation 3 computing breaks 2^{60} barrier: 112-bit prime ECDLP solved, online annoucement, http://lacal.epfl.ch/112bit_prime, 2009. <393, 394>

[352] S. Bosch, U. Güntzer, and R. Remmert, *Non-Archimedean Analysis: A Systematic Approach to Rigid Analytic Geometry*, volume 261 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*, Springer-Verlag, Berlin, 1984. <529, 538>

[353] R. C. Bose, On the application of the properties of Galois fields to the construction of hyper-graeco-latin squares, *Sankhyā* 3 (1938) 323–338. <543, 546, 547>

[354] R. C. Bose, On the construction of balanced incomplete block designs, *Ann. Eugenics* 9 (1939) 353–399. <583, 590>

[355] R. C. Bose, On some connections between the design of experiments and information theory, *Bull. Inst. Internat. Statist.* 38 (1961) 257–271. <622, 633>

[356] R. C. Bose and R. C. Burton, A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and the MacDonald codes, *J. Combinatorial Theory* 1 (1966) 96–104. <551, 555>

[357] R. C. Bose and D. K. Ray-Chaudhuri, On a class of error correcting binary group codes, *Information and Control* 3 (1960) 68–79. <669, 693, 694>

[358] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system I: The user language, *J. Symbolic Comput.* 24 (1997) 235–265. <380, 385>

[359] W. Bosma, J. Cannon, and A. Steel, Lattices of compatibly embedded finite fields, *J. Symbolic Comput.* 24 (1997) 351–369. <395, 397>

[360] W. Bosma and H. W. Lenstra, Jr., Complete systems of two addition laws for elliptic curves, *J. Number Theory* 53 (1995) 229–240. <436, 440>

[361] A. Bostan, P. Flajolet, B. Salvy, and E. Schost, Fast computation of special resultants, *Journal of Symbolic Computation* 41 (2006) 1–29. <371, 372, 373>

[362] A. Bostan, C.-P. Jeannerod, and É. Schost, Solving structured linear systems with

large displacement rank, *Theoret. Comput. Sci.* 407 (2008) 155–181. <526, 527>

[363] A. Bostan, G. Lecerf, B. Salvy, É. Schost, and B. Wiebelt, Complexity issues in bivariate polynomial factorization, In *ISSAC '04: Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation*, 42–49, New York, 2004, ACM. <378, 385>

[364] A. Bostan, F. Morain, B. Salvy, and E. Schost, Fast algorithms for computing isogenies between elliptic curves, *Mathematics of Computation* 77 (2008) 1755–1778. <778, 787>

[365] A. Böttcher and B. Silbermann, *Introduction to Large Truncated Toeplitz Matrices*, Universitext. Springer-Verlag, New York, 1999. <499, 502>

[366] J. Bourgain, Estimates on exponential sums related to the Diffie-Hellman distributions, *Geom. Funct. Anal.* 15 (2005) 1–34. <177, 178, 179, 183, 186>

[367] J. Bourgain, Mordell's exponential sum estimate revisited, *J. Amer. Math. Soc.* 18 (2005) 477–499. <184>

[368] J. Bourgain, More on the sum-product phenomenon in prime fields and its applications, *Int. J. Number Theory* 1 (2005) 1–32. <185, 186>

[369] J. Bourgain, Multilinear exponential sums in prime fields under optimal entropy condition on the sources, *Geom. Funct. Anal.* 18 (2009) 1477–1502. <167, 170, 179, 181, 182, 183, 186>

[370] J. Bourgain, Estimates on polynomial exponential sums, *Israel J. Math.* 176 (2010) 221–240. <207>

[371] J. Bourgain, On exponential sums in finite fields, In *An Irregular Mind: Szemerédi is 70*, 219–242, Springer, 2010. <184, 186>

[372] J. Bourgain and M.-C. Chang, A Gauss sum estimate in arbitrary finite fields, *C. R. Math. Acad. Sci. Paris* 342 (2006) 643–646. <135, 155, 206, 207>

[373] J. Bourgain and A. Gamburd, Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$, *Ann. of Math., 2nd Ser.* 167 (2008) 625–642. <185, 186>

[374] J. Bourgain, A. Gamburd, and P. Sarnak, Affine linear sieve, expanders, and sum-product, *Invent. Math.* 179 (2010) 559–644. <185, 186>

[375] J. Bourgain and M. Z. Garaev, On a variant of sum-product estimates and explicit exponential sum bounds in prime fields, *Math. Proc. Cambridge Philos. Soc.* 146 (2009) 1–21. <179, 181, 182, 186>

[376] J. Bourgain and A. Glibichuk, Exponential sum estimates over a subgroup in an arbitrary field, *J. Analyse Math.* 115 (2011) 51–70. <181, 184, 186>

[377] J. Bourgain, A. A. Glibichuk, and S. V. Konyagin, Estimates for the number of sums and products and for exponential sums in fields of prime order, *J. London Math. Soc., 2nd Ser.* 73 (2006) 380–398. <167, 170, 179, 180, 182, 185, 186>

[378] J. Bourgain, N. Katz, and T. Tao, A sum-product estimate in finite fields, and applications, *Geom. Funct. Anal.* 14 (2004) 27–57. <180, 186>

[379] H. Boylan and N.-P. Skoruppa, Explicit formulas for Hecke Gauss sums in quadratic number fields, *Abh. Math. Semin. Univ. Hambg.* 80 (2010) 213–226. <154, 155>

[380] S. Boztas, R. Hammons, and P. Kumar, 4-phase sequences with near-optimum correlation properties, *IEEE Trans. Inform. Theory* IT-38 (1992) 1101–1113. <315, 317>

[381] C. Bracken, E. Byrne, N. Markin, and G. McGuire, Determining the nonlinearity of a new family of APN functions, In *Applied Algebra, Algebraic Algorithms and*

Error-Correcting Codes, volume 4851 of *Lecture Notes in Comput. Sci.*, 72–79, Springer, Berlin, 2007. <252, 254, 302, 303>

[382] C. Bracken, E. Byrne, N. Markin, and G. McGuire, On the Walsh spectrum of a new APN function, In *Cryptography and Coding*, volume 4887 of *Lecture Notes in Comput. Sci.*, 92–98, Springer, Berlin, 2007. <252, 254>

[383] C. Bracken, E. Byrne, N. Markin, and G. McGuire, New families of quadratic almost perfect nonlinear trinomials and multinomials, *Finite Fields Appl.* 14 (2008) 703–714. <250, 252, 254>

[384] C. Bracken, E. Byrne, N. Markin, and G. McGuire, Fourier spectra of binomial APN functions, *SIAM J. Discrete Math.* 23 (2009) 596–608. <252, 254, 302, 303>

[385] C. Bracken, E. Byrne, N. Markin, and G. McGuire, A few more quadratic APN functions, *Cryptogr. Commun.* 3 (2011) 43–53. <249, 252, 254>

[386] C. Bracken, E. Byrne, G. McGuire, and G. Nebe, On the equivalence of quadratic APN functions, *Des. Codes Cryptogr.* 61 (2011) 261–272. <252, 254>

[387] A. Braeken, C. Wolf, and B. Preneel, A study of the security of unbalanced oil and vinegar signature schemes, In *Topics in Cryptology—CT-RSA 2005*, volume 3376 of *Lecture Notes in Comput. Sci.*, 29–43, Springer, Berlin, 2005. <771, 774>

[388] N. Brandstätter, T. Lange, and A. Winterhof, On the non-linearity and sparsity of Boolean functions related to the discrete logarithm in finite fields of characteristic two, In *Coding and Cryptography*, volume 3969 of *Lecture Notes in Comput. Sci.*, 135–143, Springer, Berlin, 2006. <243, 245>

[389] N. Brandstätter and A. Winterhof, Some notes on the two-prime generator of order 2, *IEEE Trans. Inform. Theory* 51 (2005) 3654–3657. <327, 329>

[390] N. Brandstätter and A. Winterhof, Linear complexity profile of binary sequences with small correlation measure, *Period. Math. Hungar.* 52 (2006) 1–8. <176, 179, 328, 329>

[391] J. V. Brawley and L. Carlitz, Irreducibles and the composed product for polynomials over a finite field, *Discrete Math.* 65 (1987) 115–139. <62, 63, 66>

[392] J. V. Brawley and L. Carlitz, A test for additive decomposability of irreducibles over a finite field, *Discrete Math.* 76 (1989) 61–65. <63, 66>

[393] J. V. Brawley, L. Carlitz, and J. Levine, Scalar polynomial functions on the $n \times n$ matrices over a finite field, *Linear Algebra and Appl.* 10 (1975) 199–217. <221, 222>

[394] J. V. Brawley and G. L. Mullen, Infinite Latin squares containing nested sets of mutually orthogonal finite Latin squares, *Publ. Math. Debrecen* 39 (1991) 135–141. <543, 547>

[395] J. V. Brawley and G. E. Schnibben, *Infinite Algebraic Extensions of Finite Fields*, volume 95 of *Contemporary Mathematics*, American Mathematical Society, Providence, RI, 1989. <29, 30, 123, 132, 543, 547>

[396] R. Brent, P. Gaudry, E. Thomé, and P. Zimmerman, The software *gf2x*, `http://gf2x.gforge.inria.fr/`, as viewed in July, 2012. <45, 46>

[397] R. P. Brent, P. Gaudry, E. Thomé, and P. Zimmermann, Faster multiplication in GF(2)[x], In *Algorithmic Number Theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, 153–166, Springer, Berlin, 2008. <348, 356>

[398] R. P. Brent and H. T. Kung, Fast algorithms for manipulating formal power series, *J. Assoc. Comput. Mach.* 25 (1978) 581–595. <343, 351, 356, 373, 375>

[399] R. P. Brent and H. T. Kung, Systolic VLSI arrays for linear-time GCD computation, In *VLSI 1983*, 145–154, Elsevier Science Publishers B. V., 1983. <352, 356>

[400] R. P. Brent, S. Larvala, and P. Zimmermann, A fast algorithm for testing reducibility of trinomials mod 2 and some new primitive trinomials of degree 3021377, *Math. Comp.* 72 (2003) 1443–1452. <341, 343, 356>

[401] R. P. Brent, S. Larvala, and P. Zimmermann, A primitive trinomial of degree 6972593, *Math. Comp.* 74 (2005) 1001–1002. <343, 356>

[402] R. P. Brent and P. Zimmermann, Algorithms for finding almost irreducible and almost primitive trinomials, In *High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams*, volume 41 of *Fields Inst. Commun.*, 91–102, Amer. Math. Soc., Providence, RI, 2004. <344, 346, 356>

[403] R. P. Brent and P. Zimmermann, Ten new primitive binary trinomials, *Math. Comp.* 78 (2009) 1197–1199. <91, 93, 343, 356>

[404] R. P. Brent and P. Zimmermann, An $O(M(n) \log n)$ algorithm for the Jacobi symbol, In *Algorithmic Number Theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, 83–95, Springer, Berlin, 2010. <354, 356>

[405] R. P. Brent and P. Zimmermann, The great trinomial hunt, *Notices Amer. Math. Soc.* 58 (2011) 233–239. <44, 46, 91, 93, 343, 356>

[406] R. P. Brent and P. Zimmermann, *Modern Computer Arithmetic*, volume 18 of *Cambridge Monographs on Applied and Computational Mathematics*, Cambridge University Press, Cambridge, 2011. <348, 356>

[407] E. Bresson, O. Chevassut, and D. Pointcheval, The group Diffie-Hellman problems, In *Selected Areas in Cryptography*, volume 2595 of *Lecture Notes in Comput. Sci.*, 325–338, Springer, Berlin, 2003. <388, 394>

[408] E. Breuillard, B. Green, and T. Tao, Suzuki groups as expanders, *ArXiv e-prints* (2010). <643, 649>

[409] J. Brewster Lewis, R. Ini Liu, A. H. Morales, G. Panova, S. V. Sam, and Y. Zhang, Matrices with restricted entries and q-analogues of permutations, *ArXiv e-prints* (2010). <493, 502>

[410] F. Brezing and A. Weng, Elliptic curves suitable for pairing based cryptography, *Des. Codes Cryptogr.* 37 (2005) 133–141. <785, 787>

[411] E. F. Brickell, D. M. Gordon, K. S. McCurley, and D. B. Wilson, Fast exponentiation with precomputation, In *Advances in Cryptology—EUROCRYPT 1992*, volume 658 of *Lecture Notes in Comput. Sci.*, 200–207, Springer, Berlin, 1993. <349, 350, 356>

[412] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., *Factorizations of* $b^n \pm 1$, volume 22 of *Contemporary Mathematics*, American Mathematical Society, Providence, RI, second edition, 1988, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers. <44, 46>

[413] D. Brink, H. Godinho, and P. H. A. Rodrigues, Simultaneous diagonal equations over p-adic fields, *Acta Arith.* 132 (2008) 393–399. <207>

[414] M. Brinkmann and G. Leander, On the classification of APN functions up to dimension five, *Des. Codes Cryptogr.* 49 (2008) 273–288. <250, 254>

[415] D. J. Britten and F. W. Lemire, A structure theorem for rings supporting a discrete Fourier transform, *SIAM J. Appl. Math.* 41 (1981) 222–226. <301, 303>

[416] A. E. Brouwer and J. H. van Lint, Strongly regular graphs and partial geometries, In *Enumeration and Design*, 85–122, Academic Press, Toronto, ON, 1984. <608,

610>

[417] D. R. L. Brown, Generic groups, collision resistance, and ECDSA, *Designs, Codes and Cryptography* 35 (2005) 119–152. <776, 787>

[418] M. R. Brown, Ovoids of PG(3,q), q even, with a conic section, *J. London Math. Soc.* 62 (2000) 569–582. <579, 580>

[419] M. R. Brown, G. L. Ebert, and D. Luyckx, On the geometry of regular hyperbolic fibrations, *European J. Combin.* 28 (2007) 1626–1636. <565>

[420] K. A. Browning, J. F. Dillon, R. E. Kibler, and M. T. McQuistan, APN polynomials and related codes, *Journal of Combinatorics Information and System Sciences* 34 (2009) 135–159. <250, 254>

[421] K. A. Browning, J. F. Dillon, M. T. McQuistan, and A. J. Wolfe, An APN permutation in dimension six, In *Finite Fields: Theory and Applications*, volume 518 of *Contemp. Math.*, 33–42, Amer. Math. Soc., Providence, RI, 2010. <222, 249, 254>

[422] R. H. Bruck, Difference sets in a finite group, *Trans. Amer. Math. Soc.* 78 (1955) 464–481. <561, 565>

[423] R. H. Bruck, Quadratic extensions of cyclic planes, In *Proc. Sympos. Appl. Math., Vol. 10*, 15–44, American Mathematical Society, Providence, RI, 1960. <562, 565>

[424] R. H. Bruck, Construction problems of finite projective planes, In *Combinatorial Mathematics and its Applications*, 426–514, Univ. North Carolina Press, Chapel Hill, N.C., 1969. <558, 559, 565>

[425] R. H. Bruck and R. C. Bose, The construction of translation planes from projective spaces, *J. Algebra* 1 (1964) 85–102. <558, 565>

[426] R. H. Bruck and H. J. Ryser, The nonexistence of certain finite projective planes, *Canadian J. Math.* 1 (1949) 88–93. <592, 598>

[427] A. Bruen, Blocking sets in finite projective planes, *SIAM J. Appl. Math.* 21 (1971) 380–392. <551, 552, 555>

[428] A. A. Bruen and R. Silverman, On the nonexistence of certain MDS codes and projective planes, *Math. Z.* 183 (1983) 171–175. <578, 580>

[429] A. A. Bruen and R. Silverman, Arcs and blocking sets. II, *European J. Combin.* 8 (1987) 351–356. <551, 555>

[430] A. A. Bruen and J. A. Thas, Blocking sets, *Geometriae Dedicata* 6 (1977) 193–203. <551, 555>

[431] A. A. Bruen, J. A. Thas, and A. Blokhuis, On M.D.S. codes, arcs in PG(n, q) with q even, and a solution of three fundamental problems of B. Segre, *Invent. Math.* 92 (1988) 441–459. <577, 578, 580>

[432] L. Brünjes, *Forms of Fermat Equations and their Zeta Functions*, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2004. <465, 472>

[433] H. Brunner, A. Curiger, and M. Hofstetter, On computing multiplicative inverses in GF(2^m), *IEEE Trans. Comput.* 42 (1993) 1010–1015. <353, 356>

[434] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, PhD thesis, Innsbruck, 1965. <772, 774>

[435] J. Buchmann, D. Cabarcas, J. Ding, and M. S. E. Mohamed, Flexible partial enlargement to accelerate Gröbner basis computation over $\mathbb{F}_2$, In *AFRICACRYPT*, volume 6055 of *Lecture Notes in Comput. Sci.*, 69–81. Springer, 2010. <772, 774>

[436] J. Buchmann and V. Shoup, Constructing nonresidues in finite fields and the extended Riemann hypothesis, *Math. Comp.* 65 (1996) 1311–1326. <341, 356>

[437] J. Buchmann and H. C. Williams, A key-exchange system based on imaginary quadratic fields, *J. Cryptology* 1 (1988) 107–118. <736, 740>

[438] J. A. Buchmann and C. S. Hollinger, On smooth ideals in number fields, *J. Number Theory* 59 (1996) 82–87. <392, 394>

[439] A. A. Buchstab, Asymptotic estimates of a general number theoretic function, *Rec. Math. (Mat. Sbornik), New Ser.* 44 (1937) 1239–1246. <363, 367>

[440] L. Budaghyan and C. Carlet, Classes of quadratic APN trinomials and hexanomials and related structures, *IEEE Trans. Inform. Theory* 54 (2008) 2354–2357. <250, 252, 254>

[441] L. Budaghyan and C. Carlet, CCZ-equivalence of single and multi output Boolean functions, In *Finite Fields: Theory and Applications*, volume 518 of *Contemp. Math.*, 43–54, Amer. Math. Soc., Providence, RI, 2010. <239, 245>

[442] L. Budaghyan, C. Carlet, T. Helleseth, and A. Kholosha, Generalized bent functions and their relation to Maiorana-Mcfarland class, In *Proceedings of the 2012 IEEE International Symposium on Information Theory*. IEEE, 2012. <259, 265>

[443] L. Budaghyan, C. Carlet, and G. Leander, Two classes of quadratic APN binomials inequivalent to power functions, *IEEE Trans. Inform. Theory* 54 (2008) 4218–4229. <250, 252, 254>

[444] L. Budaghyan, C. Carlet, and G. Leander, Constructing new APN functions from known ones, *Finite Fields Appl.* 15 (2009) 150–159. <252, 254>

[445] L. Budaghyan, C. Carlet, and A. Pott, New classes of almost bent and almost perfect nonlinear polynomials, *IEEE Trans. Inform. Theory* 52 (2006) 1141–1152. <250, 252, 254>

[446] L. Budaghyan and T. Helleseth, New perfect nonlinear multinomials over $\mathbf{F}_{p^{2k}}$ for any odd prime p, In *Sequences and Their Applications—SETA 2008*, volume 5203 of *Lecture Notes in Comput. Sci.*, 403–414, Springer, Berlin, 2008. <274>

[447] L. Budaghyan and T. Helleseth, New commutative semifields defined by new PN multinomials, *Cryptogr. Commun.* 3 (2011) 1–16. <257, 264, 265, 274>

[448] F. Buekenhout, Existence of unitals in finite translation planes of order q^2 with a kernel of order q, *Geometriae Dedicata* 5 (1976) 189–194. <563, 565>

[449] F. Buekenhout, An introduction to incidence geometry, In *Handbook of Incidence Geometry*, 1–25, North-Holland, Amsterdam, 1995. <29, 30>

[450] F. Buekenhout, A. Delandtsheer, J. Doyen, P. B. Kleidman, M. W. Liebeck, and J. Saxl, Linear spaces with flag-transitive automorphism groups, *Geom. Dedicata* 36 (1990) 89–94. <561, 565>

[451] J. Buhler and N. Koblitz, Lattice basis reduction, Jacobi sums and hyperelliptic cryptosystems, *Bull. Austral. Math. Soc.* 58 (1998) 147–154. <483, 484>

[452] B. Bukh and J. Tsimerman, Sum-product estimates for rational functions, *Proc. London Math. Soc.* <182, 186>

[453] J. R. Bunch and J. E. Hopcroft, Triangular factorization and inversion by fast matrix multiplication, *Math. Comp.* 28 (1974) 231–236. <518, 527>

[454] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), *Bundesanzeiger* 85, June 7 (2011) 2034. <776, 787>

[455] M. Buratti, Improving two theorems of Bose on difference families, *J. Combin. Des.* 3 (1995) 15–24. <585, 590>

[456] M. Buratti, On simple radical difference families, *J. Combin. Des.* 3 (1995) 161–168. <585, 590>

[457] M. Buratti, Old and new designs via difference multisets and strong difference families, *J. Combin. Des.* 7 (1999) 406–425. <588, 590>

[458] M. Buratti, Existence of Z-cyclic triplewhist tournaments for a prime number of players, *J. Combin. Theory, Ser. A* 90 (2000) 315–325. <610>

[459] K. Burde, Zur Herleitung von Reziprozitätsgesetzen unter Benutzung von endlichen Körpern, *J. Reine Angew. Math.* 293/294 (1977) 418–427. <167, 179>

[460] D. A. Burgess, On character sums and primitive roots, *Proc. London Math. Soc., 3rd Ser.* 12 (1962) 179–192. <177, 179>

[461] J. F. Burkhart, N. J. Calkin, S. Gao, J. C. Hyde-Volpe, K. James, H. Maharaj, S. Manber, J. Ruiz, and E. Smith, Finite field elements of high order arising from modular curves, *Des. Codes Cryptogr.* 51 (2009) 301–314. <94>

[462] M. V. D. Burmester, On the commutative non-associative division algebras of even order of L. E. Dickson, *Rend. Mat. e Appl. Ser. V* 21 (1962) 143–166. <268, 270>

[463] J. F. Buss, G. S. Frandsen, and J. O. Shallit, The computational complexity of some problems of linear algebra, In *STACS 97*, volume 1200 of *Lecture Notes in Comput. Sci.*, 451–462, Springer, Berlin, 1997. <770, 774>

[464] M. Butler, On the reducibility of polynomials over a finite field, *Quart. J. Math. Oxford* 5 (1954) 102–107. <368, 373>

[465] M. C. R. Butler, The irreducible factors of $f(x^m)$ over a finite field, *J. London Math. Soc., 2nd Ser.* 30 (1955) 480–482. <56, 58, 61>

[466] J. W. Byers, M. Luby, M. Mitzenmacher, and A. Rege, A digital fountain approach to reliable distribution of bulk data, In *Proceedings of the ACM SIGCOMM '98*, 56–67, New York, 1998, ACM. <719, 721, 725>

[467] K. A. Byrd and T. P. Vaughan, Counting and constructing orthogonal circulants, *J. Combin. Theory, Ser. A* 24 (1978) 34–49. <498, 502>

[468] D. Cabarcas and J. Ding, Linear algebra to compute syzygies and Gröbner bases, In *ISSAC 2011—Proceedings of the Thirty Sixth International Symposium on Symbolic and Algebraic Computation*, 67–74, ACM, New York, 2011. <773, 774>

[469] A. Cafure and G. Matera, Improved explicit estimates on the number of solutions of equations over a finite field, *Finite Fields Appl.* 12 (2006) 155–185. <188, 195>

[470] E. Çakçak and F. Özbudak, Subfields of the function field of the Deligne-Lusztig curve of Ree type, *Acta Arith.* 115 (2004) 133–180. <454, 455, 456>

[471] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel, Z_4-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets, *Proc. London Math. Soc., 3rd Ser.* 75 (1997) 436–480. <825, 831>

[472] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Quantum error correction and orthogonal geometry, *Phys. Rev. Lett.* 78 (1997) 405–408. <825, 828, 831>

[473] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Quantum error correction via codes over GF(4), *IEEE Trans. Inform. Theory* 44 (1998) 1369–1387. <827, 831>

[474] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, *Phys. Rev. A* 54 (1996) 1098–1105. <828, 831>

[475] R. Calderbank and W. M. Kantor, The geometry of two-weight codes, *Bull. London Math. Soc.* 18 (1986) 97–122. <608, 610>

[476] C. Caliskan and G. E. Moorhouse, Subplanes of order 3 in Hughes planes, *Electron. J. Combin.* 18 (2011) Paper 2, 8. <562, 565>

[477] C. Caliskan and B. Petrak, Subplanes of order 3 in Figueroa planes, preprint. <562, 565>

[478] J. Calmet and R. Loos, An improvement of Rabin's probabilistic algorithm for generating irreducible polynomials over $GF(p)$, *Information Processing Letters* 11 (1980) 94–95. <369, 373>

[479] P. J. Cameron and J. J. Seidel, Quadratic forms over $GF(2)$, *Proc. Kon. Nederl. Akad. Wetensch. Ser. A* 76 (1973) 1–8. <199, 200>

[480] P. J. Cameron and J. H. van Lint, *Designs, Graphs, Codes and Their Links*, volume 22 of *London Mathematical Society Student Texts*, Cambridge University Press, Cambridge, 1991. <29, 30>

[481] P. Camion, C. Carlet, P. Charpin, and N. Sendrier, On correlation-immune functions, In *Advances in Cryptology—CRYPTO '91*, volume 576 of *Lecture Notes in Comput. Sci.*, 86–100, Springer, Berlin, 1992. <242, 245>

[482] P. Candelas, X. de la Ossa, and F. Rodriguez-Villegas, Calabi-Yau manifolds over finite fields. II, In *Calabi-Yau Varieties and Mirror Symmetry*, volume 38 of *Fields Inst. Commun.*, 121–157, Amer. Math. Soc., Providence, RI, 2003. <465, 472>

[483] R. Canetti, J. Friedlander, S. Konyagin, M. Larsen, D. Lieman, and I. E. Shparlinski, On the statistical properties of Diffie-Hellman distributions, *Israel J. Math.* 120 (2000) 23–46. <177, 178, 179>

[484] R. Canetti, J. Friedlander, and I. E. Shparlinski, On certain exponential sums and the distribution of Diffie-Hellman triples, *J. London Math. Soc., 2nd Ser.* 59 (1999) 799–812. <177, 179, 183, 186>

[485] A. Canteaut, *Analyse et Conception de Chiffrements à Clef Secrète*, Mémoire d'habilitation à diriger des recherches, Université Paris 6, 2006. <247, 254>

[486] A. Canteaut, Open problems related to algebraic attacks on stream ciphers, In *Coding and Cryptography*, volume 3969 of *Lecture Notes in Comput. Sci.*, 120–134, Springer, Berlin, 2006. <241, 245>

[487] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine, On cryptographic properties of the cosets of $R(1, m)$, *IEEE Trans. Inform. Theory* 47 (2001) 1494–1513. <237, 245>

[488] A. Canteaut, P. Charpin, and H. Dobbertin, A new characterization of almost bent functions, In *Fast Software Encryption 99*, volume 1636 of *Lecture Notes Comput. Sci.*, 186–200. Springer-Verlag, 1999. <254>

[489] A. Canteaut, P. Charpin, and H. Dobbertin, Binary m-sequences with three-valued crosscorrelation: a proof of Welch's conjecture, *IEEE Trans. Inform. Theory* 46 (2000) 4–8. <248, 254>

[490] A. Canteaut, P. Charpin, and H. Dobbertin, Weight divisibility of cyclic codes, highly nonlinear functions on $\mathbf{F}_{2^m}$, and crosscorrelation of maximum-length sequences, *SIAM J. Discrete Math.* 13 (2000) 105–138. <207, 251, 253, 254>

[491] A. Canteaut, P. Charpin, and G. M. Kyureghyan, A new class of monomial bent functions, *Finite Fields Appl.* 14 (2008) 221–241. <247, 254, 261, 265>

[492] A. Canteaut (ed.), D. Augot, C. Cid, H. Englund, H. Gilbert, M. Hell, T. Johansson, M. Parker, T. Pornin, B. Preneel, C. Rechberger, and M. Robshaw, D.STVL.9 - ongoing research areas in symmetric cryptography, ECRYPT – European NoE in Cryptology, 2008. <247, 254>

[493] D. G. Cantor, Computing in the Jacobian of a hyperelliptic curve, *Math. Comp.* 48 (1987) 95–101. <445, 449, 788, 794>

[494] D. G. Cantor and E. Kaltofen, On fast multiplication of polynomials over arbitrary algebras, *Acta Infor.* 28 (1991) 693–701. <367, 373, 375>

[495] D. G. Cantor and H. Zassenhaus, A new algorithm for factoring polynomials over finite fields, *Math. Comp.* 36 (1981) 587–592. <373, 375, 761, 774>

[496] W. Cao, L. Hu, J. Ding, and Z. Yin, Kipnis-shamir attack on unbalanced oil-vinegar scheme, In F. Bao and J. Weng, editors, *ISPEC*, volume 6672 of *Lecture Notes in Computer Science*, 168–180. Springer, 2011. <771, 774>

[497] W. Cao and Q. Sun, A reduction for counting the number of zeros of general diagonal equations over finite fields, *Finite Fields Appl.* 12 (2006) 681–692. <204, 207>

[498] W. Cao and Q. Sun, Factorization formulae on counting zeros of diagonal equations over finite fields, *Proc. Amer. Math. Soc.* 135 (2007) 1283–1291. <204, 207>

[499] X. Cao, A note on the moments of Kloosterman sums, *Appl. Algebra Engrg. Comm. Comput.* 20 (2009) 447–457. <148, 155>

[500] X. Cao and L. Hu, New methods for generating permutation polynomials over finite fields, *Finite Fields Appl.* (in press). <209, 222>

[501] A. Capelli, Sulla rudittibilità delle equazioni algebriche I, *Rend. Acad. Sci. Fis. Mat. Napoli* 3 (1897) 243–252. <56, 57, 61>

[502] A. Capelli, Sulla rudittibilità delle equazioni algebriche II, *Rend. Acad. Sci. Fis. Mat. Napoli* 4 (1898) 243–252. <57, 61>

[503] A. Capelli, Sulla redutibilita delle funzione $x^n - A$ in un campo qualunque di razionalità, *Math. Ann.* 54 (1901) 602–603. <57, 61>

[504] M. Car, Le probléme de Waring pour l'anneau des polynômes sur un corps fini, *C. R. Acad. Sci. Paris, Sér. A-B* 273 (1971) A141–A144. <491, 492>

[505] M. Car, Factorisation dans $F_q[X]$, *C. R. Acad. Sci. Paris, Sér. I, Math.* 294 (1982) 147–150. <361, 367>

[506] M. Car, Théorèmes de densité dans $\mathbf{F}_q[X]$, *Acta Arith.* 48 (1987) 145–165. <362, 363, 367>

[507] M. Car, Waring's problem in function fields, *Proc. London Math. Soc., 3rd Ser.* 68 (1994) 1–30. <207>

[508] M. Car, Distribution des polynômes irréductibles dans $\mathbf{F}_q[T]$, *Acta Arith.* 88 (1999) 141–153. <70, 71, 72, 75>

[509] M. Car, New bounds on some parameters in the Waring problem for polynomials over a finite field, In *Finite Fields and Applications*, volume 461 of *Contemp. Math.*, 59–77, Amer. Math. Soc., Providence, 2008. <491, 492>

[510] M. Car and L. Gallardo, Sums of cubes of polynomials, *Acta Arith.* 112 (2004) 41–50. <491, 492>

[511] M. Car and L. Gallardo, Waring's problem for polynomial biquadrates over a finite field of odd characteristic, *Funct. Approx. Comment. Math.* 37 (2007) 39–50. <207, 491, 492>

[512] P. Carbonne and T. Henocq, Décomposition de la jacobienne sur les corps finis,

Bull. Polish Acad. Sci. Math. 42 (1994) 207–215. <232, 233>

[513] J.-P. Cardinal, On a property of Cauchy-like matrices, *C. R. Acad. Sci. Paris, Sér. I, Math.* 328 (1999) 1089–1093. <526, 527>

[514] I. Cardinali, O. Polverino, and R. Trombetti, Semifield planes of order q^4 with kernel F_{q^2} and center F_q, *European J. Combin.* 27 (2006) 940–961. <269, 270>

[515] C. Carlet, A larger class of cryptographic Boolean functions via a study of the Maiorana-McFarland construction, In *Advances in Cryptology—CRYPTO 2002*, volume 2442 of *Lecture Notes in Comput. Sci.*, 549–564, Springer, Berlin, 2002. <242, 245>

[516] C. Carlet, On the coset weight divisibility and nonlinearity of resilient and correlation-immune functions, In *Sequences and Their Applications*, Discrete Math. Theor. Comput. Sci. (Lond.), 131–144, Springer, London, 2002. <240, 245>

[517] C. Carlet, On the secondary constructions of resilient and bent functions, In *Coding, Cryptography and Combinatorics*, volume 23 of *Progr. Comput. Sci. Appl. Logic*, 3–28, Birkhäuser, Basel, 2004. <242, 245>

[518] C. Carlet, Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications, *IEEE Trans. Inform. Theory* 54 (2008) 1262–1272. <239, 245>

[519] C. Carlet, Boolean functions for cryptography and error correcting codes, In Y. Crama and P. L. Hammer, editors, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, 257–397, Cambridge University Press, 2010. <174, 179>

[520] C. Carlet, Boolean Functions for Cryptography and Error Correcting Codes (Chapter 8), In Y. Crama and P. L. Hammer, editors, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, 257–397, Cambridge University Press, 2010. <236, 237, 238, 240, 241, 242, 243, 245, 255, 260, 265>

[521] C. Carlet, Vectorial Boolean functions for cryptography, In Y. Crama and P. L. Hammer, editors, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, 398–469, Cambridge University Press, 2010. <246, 247, 254, 265>

[522] C. Carlet, P. Charpin, and V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Des. Codes Cryptogr.* 15 (1998) 125–156. <248, 250, 251, 252, 253, 254>

[523] C. Carlet, L. E. Danielsen, M. G. Parker, and P. Solé, Self-dual bent functions, *Int. J. Inf. Coding Theory* 1 (2010) 384–399. <256, 265>

[524] C. Carlet and S. Dubuc, On generalized bent and q-ary perfect nonlinear functions, In *Finite Fields and Applications*, 81–94, Springer, Berlin, 2001. <264, 265>

[525] C. Carlet and K. Feng, An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity, In *Advances in Cryptology—ASIACRYPT 2008*, volume 5350 of *Lecture Notes in Comput. Sci.*, 425–440, Springer, Berlin, 2008. <243, 245>

[526] C. Carlet and P. Gaborit, Hyper-bent functions and cyclic codes, *J. Combin. Theory, Ser. A* 113 (2006) 466–482. <257, 265>

[527] C. Carlet and P. Guillot, A new representation of Boolean functions, In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 1719 of *Lecture Notes in Comput. Sci.*, 94–103, Springer, Berlin, 1999. <236, 245>

[528] C. Carlet, T. Helleseth, A. Kholosha, and S. Mesnager, On the dual of bent func-

tions with 2^r Niho exponents, In *Proceedings of the 2011 IEEE International Symposium on Information Theory*, 657–661. IEEE, 2011. <261, 262, 265>

[529] C. Carlet and S. Mesnager, On Dillon's class H of bent functions, Niho bent functions and o-polynomials, *J. Combin. Theory, Ser. A* 118 (2011) 2392–2410. <261, 262, 265>

[530] C. Carlet and A. Pott, editors, *Sequences and Their Applications*, volume 6338 of *Lecture Notes in Computer Science*, Berlin, 2010. Springer. <30>

[531] C. Carlet and P. Sarkar, Spectral domain analysis of correlation immune and resilient Boolean functions, *Finite Fields Appl.* 8 (2002) 120–130. <240, 245>

[532] C. Carlet and B. Sunar, editors, *Arithmetic of Finite Fields*, volume 4547 of *Lecture Notes in Computer Science*, Berlin, 2007. Springer. <30>

[533] C. Carlet and J. L. Yucas, Piecewise constructions of bent and almost optimal Boolean functions, *Des. Codes Cryptogr.* 37 (2005) 449–464. <200>

[534] L. Carlitz, The arithmetic of polynomials in a Galois field, *Amer. J. Math.* 54 (1932) 39–50. <76, 81, 357, 359, 367>

[535] L. Carlitz, Some applications of a theorem of Chevalley, *Duke Math. J.* 18 (1951) 811–819. <207>

[536] L. Carlitz, Primitive roots in a finite field, *Trans. Amer. Math. Soc.* 73 (1952) 373–382. <130, 132>

[537] L. Carlitz, Some problems involving primitive roots in a finite field, *Proc. Nat. Acad. Sci. U.S.A.* 38 (1952) 314–318; errata, 618. <109, 110>

[538] L. Carlitz, A theorem of Dickson on irreducible polynomials, *Proc. Amer. Math. Soc.* 3 (1952) 693–700. <50, 51, 55, 69, 75>

[539] L. Carlitz, Invariantive theory of equations in a finite field, *Trans. Amer. Math. Soc.* 75 (1953) 405–427. <223, 225>

[540] L. Carlitz, Permutations in a finite field, *Proc. Amer. Math. Soc.* 4 (1953) 538. <231, 233>

[541] L. Carlitz, Representations by quadratic forms in a finite field, *Duke Math. J.* 21 (1954) 123–137. <499, 502>

[542] L. Carlitz, Representations by skew forms in a finite field, *Arch. Math. (Basel)* 5 (1954) 19–31. <499, 502>

[543] L. Carlitz, Solvability of certain equations in a finite field, *Quart. J. Math. Oxford, 2nd Ser.* 7 (1956) 3–4. <204, 207>

[544] L. Carlitz, Some theorems on irreducible reciprocal polynomials over a finite field, *J. Reine Angew. Math.* 227 (1967) 212–220. <53, 55, 278, 282>

[545] L. Carlitz, Kloosterman sums and finite field extensions, *Acta Arith.* 16 (1969/1970) 179–193. <150, 155>

[546] L. Carlitz, D. J. Lewis, W. H. Mills, and E. G. Straus, Polynomials over finite fields with minimal value sets, *Mathematika* 8 (1961) 121–130. <207, 226, 229>

[547] L. Carlitz and S. Uchiyama, Bounds for exponential sums, *Duke Math. J.* 24 (1957) 37–41. <314, 317>

[548] L. Carlitz and C. Wells, The number of solutions of a special system of equations in a finite field, *Acta Arith* 12 (1966/1967) 77–84. <211, 222>

[549] R. Carls and D. Lubicz, A p-adic quasi-quadratic time point counting algorithm, *Int. Math. Res. Not. IMRN* (2009) 698–735. <484>

[550] P. Cartier, Une nouvelle opération sur les formes différentielles, *C. R. Acad. Sci. Paris* 244 (1957) 426–428. <479, 480>

[551] J. Cassaigne, C. Mauduit, and A. Sárközy, On finite pseudorandom binary sequences VII: The measures of pseudorandomness, *Acta Arith.* 103 (2002) 97–118. <176, 179>

[552] R. Casse, *Projective Geometry: an Introduction*, Oxford University Press, Oxford, 2006. <555, 565>

[553] J. W. S. Cassels, Diophantine equations with special reference to elliptic curves, *J. London Math. Soc., 2nd Ser.* 41 (1966) 193–291. <416, 433>

[554] J. W. S. Cassels, *Lectures on Elliptic Curves*, volume 24 of *London Mathematical Society Student Texts*, Cambridge University Press, Cambridge, 1991. <29, 30, 416, 433>

[555] G. Castagnoli, S. Bräuer, and M. Herrmann, Optimization of cyclic redundancy-check codes with 24 and 32 parity bits, *IEEE Transactions on Communications* 41 (1993) 883–892. <625, 629, 630, 633>

[556] G. Castagnoli, J. Ganz, and P. Graber, Optimum cycle redundancy-check codes with 16-bit redundancy, *IEEE Transactions on Communications* 38 (1990) 111–114. <626, 628, 633>

[557] F. N. Castro and C. J. Moreno, Mixed exponential sums over finite fields, *Proc. Amer. Math. Soc.* 128 (2000) 2529–2537. <162, 163>

[558] F. N. Castro, I. Rubio, P. Guan, and R. Figueroa, On systems of linear and diagonal equation of degree p^i+1 over finite fields of characteristic p, *Finite Fields Appl.* 14 (2008) 648–657. <207>

[559] F. N. Castro, I. Rubio, and J. M. Vega, Divisibility of exponential sums and solvability of certain equations over finite fields, *Q. J. Math.* 60 (2009) 169–181. <205, 207>

[560] F. N. Castro and I. M. Rubio, Solvability of systems of polynomial equations with some prescribed monomials, In *Finite Fields: Theory and Applications*, volume 518 of *Contemp. Math.*, 73–81, Amer. Math. Soc., Providence, RI, 2010. <204, 207>

[561] W. Castryck, J. Denef, and F. Vercauteren, Computing zeta functions of nondegenerate curves, *IMRP Int. Math. Res. Pap.* (2006) Art. ID 72017, 57. <484>

[562] K. Cattell, C. R. Miers, F. Ruskey, J. Sawada, and M. Serra, The number of irreducible polynomials over GF(2) with given trace and subtrace, *J. Combin. Math. Combin. Comput.* 47 (2003) 31–64. <52, 55, 74, 75>

[563] A. Cauchy, Recherches sur les nombres, *Ecole Polytechnique* 9 (1813) 99–116. <205, 207>

[564] C. M. Caves, C. A. Fuchs, and R. Schack, Quantum probabilities as Bayesian probabilities, *Phys. Rev. A., 3rd Ser.* 65 (2002) 6 pages. <826, 831>

[565] C. M. Caves, C. A. Fuchs, and R. Schack, Unknown quantum states: the quantum de Finetti representation, *J. Math. Phys.* 43 (2002) 4537–4559. <826, 831>

[566] S. R. Cavior, A note on octic permutation polynomials, *Math. Comp.* 17 (1963) 450–452. <216, 222>

[567] C. Cazacu and D. Simovici, A new approach of some problems concerning polynomials over finite fields, *Information and Control* 22 (1973) 503–511. <64, 66>

[568] A. Çeşmelioğlu, G. McGuire, and W. Meidl, A construction of weakly and non-weakly regular bent functions, *J. Combin. Theory, Ser. A* 119 (2012) 420–429. <264, 265>

[569] A. Çeşmelioğlu and W. Meidl, Bent functions of maximal degree, *IEEE Trans.*

Inform. Theory 58 (2012) 1186–1190. <264, 265>

[570] CCSDS, Low density parity check codes for use in near-Earth and deep space applications, 2007. <704, 710>

[571] M. Cenk, C. Negre, and M. A. Hasan, Improved three-way split formulas for binary polynomial and Toeplitz matrix vector products, Technical Report cacr2011-30, University of Waterloo, Waterloo, 2011. <805, 813>

[572] A. Çeşmelioğlu, W. Meidl, and A. Topuzoğlu, On the cycle structure of permutation polynomials, *Finite Fields Appl.* 14 (2008) 593–614. <221, 222>

[573] F. Chabaud and R. Lercier, ZEN, version 3.0, 2001, available at `http://zenfact.sourceforge.net/`. <339, 356>

[574] F. Chabaud and S. Vaudenay, Links between differential and linear cryptanalysis, In *Advances in Cryptology—EUROCRYPT '94*, volume 950 of *Lecture Notes in Comput. Sci.*, 356–365, Springer, Berlin, 1995. <246, 248, 254>

[575] W. Chambers, Solution of Welch-Berlekamp key equation by Euclidean algorithm, *Electronics Letters* 29 (1993) 1031. <686, 694>

[576] A. Chambert-Loir, Compter (rapidement) le nombre de solutions d'équations dans les corps finis, *Astérisque* (2008) Exp. No. 968, vii, 39–90, Séminaire Bourbaki. Vol. 2006/2007. <484>

[577] D. B. Chandler and Q. Xiang, The invariant factors of some cyclic difference sets, *J. Combin. Theory, Ser. A* 101 (2003) 131–146. <146, 155>

[578] C.-Y. Chang, M. A. Papanikolas, D. S. Thakur, and J. Yu, Algebraic independence of arithmetic gamma values and Carlitz zeta values, *Adv. Math.* 223 (2010) 1137–1154. <538>

[579] C.-Y. Chang and J. Yu, Determination of algebraic relations among special zeta values in positive characteristic, *Adv. Math.* 216 (2007) 321–345. <534, 538>

[580] M.-C. Chang, On a question of Davenport and Lewis and new character sum bounds in finite fields, *Duke Math. J.* 145 (2008) 409–442. <186>

[581] M.-C. Chang, Expansions of quadratic maps in prime fields, Preprint, 2011. <337>

[582] M.-C. Chang and C. Z. Yao, An explicit bound on double exponential sums related to Diffie-Hellman distributions, *SIAM J. Discrete Math.* 22 (2008) 348–359. <177, 178, 179, 183, 186>

[583] Y. Chang, W.-S. Chou, and P. J.-S. Shiue, On the number of primitive polynomials over finite fields, *Finite Fields Appl.* 11 (2005) 156–163. <85>

[584] R. Chapman, Completely normal elements in iterated quadratic extensions of finite fields, *Finite Fields Appl.* 3 (1997) 1–10. <56, 61, 131, 132, 278, 282>

[585] P. Charpin, Open problems on cyclic codes, In *Handbook of Coding Theory, Vol. I, II*, 963–1063, North-Holland, Amsterdam, 1998. <251, 253, 254>

[586] P. Charpin and G. Gong, Hyperbent functions, Kloosterman sums, and Dickson polynomials, *IEEE Trans. Inform. Theory* 54 (2008) 4230–4238. <257, 263, 265>

[587] P. Charpin, T. Helleseth, and V. Zinoviev, Divisibility properties of classical binary Kloosterman sums, *Discrete Math.* 309 (2009) 3975–3984. <148, 155>

[588] P. Charpin and G. Kyureghyan, When does $G(x)+\gamma\mathrm{Tr}(H(x))$ permute $\mathbb{F}_{p^n}$?, *Finite Fields Appl.* 15 (2009) 615–632. <218, 222>

[589] P. Charpin and G. M. Kyureghyan, Cubic monomial bent functions: a subclass of $\mathcal{M}$, *SIAM J. Discrete Math.* 22 (2008) 650–665. <261, 265>

[590] P. Charpin and G. M. Kyureghyan, On a class of permutation polynomials over

$\mathbb{F}_{2^n}$, In *Sequences and Their Applications—SETA 2008*, volume 5203 of *Lecture Notes in Comput. Sci.*, 368–376, Springer, Berlin, 2008. <218, 222>

[591] P. Charpin, A. Pott, and A. Winterhof, Finite Fields and Applications: Character Sums and Polynomials, Radon Series in Computational and Applied Mathematics, de Gruyter, to appear. <30>

[592] S. Chatterjee and A. Menezes, On cryptographic protocols employing asymmetric pairings—the role of Ψ revisited, *Discrete Appl. Math.* 159 (2011) 1311–1322. <783, 787>

[593] Y. M. Chee, Y. Tan, and X. D. Zhang, Strongly regular graphs constructed from p-ary bent functions, *J. Algebraic Combin.* 34 (2011) 251–266. <258, 265>

[594] H. Chen, Fast algorithms for determining the linear complexity of sequences over GF(p^m) with period $2^t n$, *IEEE Trans. Inform. Theory* 51 (2005) 1854–1856. <322, 329>

[595] H. Chen, Reducing the computation of linear complexities of periodic sequences over GF(p^m), *IEEE Trans. Inform. Theory* 52 (2006) 5537–5539. <322, 329>

[596] H. Chen, S. Ling, and C. Xing, Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound, *IEEE Transactions on Information Theory* 47 (2001) 2055–2058. <828, 831>

[597] J. Chen and T. Wang, On the Goldbach problem, *Acta Math. Sinica* 32 (1989) 702–718. <489, 492>

[598] J.-M. Chen and T.-T. Moh, On the Goubin-Courtois attack on TTM, Cryptology ePrint Archive, 2001, http://eprint.iacr.org/2001/072. <765, 774>

[599] J.-M. Chen and B.-Y. Yang, A more secure and efficacious TTS signature scheme, In *Information Security and Cryptology—ICISC 2003*, volume 2971 of *Lecture Notes in Comput. Sci.*, 320–338, Springer, Berlin, 2004. <763, 765, 774>

[600] J.-M. Chen, B.-Y. Yang, and B.-Y. Peng, Tame transformation signatures with Topsy-Yurvy Hashes, In *IWAP'02*, 1–8, 2002, http://dsns.csie.nctu.edu.tw/iwap/proceedings/proceedings/sessionD/7.pdf. <765, 774>

[601] K. Chen and L. Zhu, Existence of APAV(q, k) with q a prime power $\equiv 3 \pmod 4$ and k odd > 1, *J. Combin. Des.* 7 (1999) 57–68. <603, 610>

[602] L. Chen, W. Eberly, E. Kaltofen, B. D. Saunders, W. J. Turner, and G. Villard, Efficient matrix preconditioners for black box linear algebra, *Linear Algebra Appl.* 343/344 (2002) 119–146. <523, 524, 527>

[603] Y. Chen, The Steiner system $S(3, 6, 26)$, *J Geometry* 2 (1972) 7–28. <580>

[604] Y. Q. Chen, A construction of difference sets, *Des. Codes Cryptogr.* 13 (1998) 247–250. <596, 598>

[605] Q. Cheng, Constructing finite field extensions with large order elements, *SIAM J. Discrete Math.* 21 (2007) 726–730 (electronic). <93, 94>

[606] Q. Cheng, S. Gao, and D. Wan, Constructing high order elements through subspace polynomials, In *Proceedings of the Twenty-Third Annual ACM-SIAM Symposium on Discrete Algorithms*, 1457–1463, 2012. <94>

[607] J. H. Cheon, J. Hong, and M. Kim, Accelerating Pollard's rho algorithm in finite fields, *Journal of Cryptology* 25 (2012) 185–242. <390, 394>

[608] R. C. C. Cheung, S. Duquesne, J. Fan, N. Guillermin, I. Verbauwhede, and G. X. Yao, FPGA implementation of pairings using residue number system and lazy reduction, In *Proceedings of the 2011 Workshop on Cryptographic Hardware and Embedded Systems*, 421–441, 2011. <813>

[609] C. Chevalley, Démonstration d'une hypothèse de m. artin, *Abhand. Math. Sem. Hamburg* 11 (1936) 73–75. <201, 207>

[610] G. Chèze, *Des méthodes symboliques-numériques et exactes pour la factorisation absolue des polynômes en deux variables*, PhD thesis, Université de Nice-Sophia Antipolis (France), 2004. <380, 385>

[611] G. Chèze and G. Lecerf, Lifting and recombination techniques for absolute factorization, *J. Complexity* 23 (2007) 380–420. <377, 385>

[612] A. M. Childs, L. J. Schulman, and U. V. Vazirani, Quantum algorithms for hidden nonlinear structures, In *Forty Eighth Annual IEEE Symposium on Foundations of Computer Science*, 395–404, 2007. <830, 831>

[613] A. M. Childs and W. van Dam, Quantum algorithms for algebraic problems, *Rev. Modern Phys.* 82 (2010) 1–52. <824, 831>

[614] K. Chinen and T. Hiramatsu, Hyper-Kloosterman sums and their applications to the coding theory, *Appl. Algebra Engrg. Comm. Comput.* 12 (2001) 381–390. <148, 155>

[615] A. Chistov, Polynomial time construction of a finite field, In *Abstracts of Lectures at Seventh All-Union Conference in Mathematical Logic*, 196, Novosibirsk, USSR, 1984, In Russian. <371, 373>

[616] H. T. Choi and R. Evans, Congruences for sums of powers of Kloosterman sums, *Int. J. Number Theory* 3 (2007) 105–117. <151, 152, 155>

[617] B. C. Chong and K. M. Chan, On the existence of normalized room squares, *Nanta Math.* 7 (1974) 8–17. <605, 610>

[618] W. S. Chou, *Permutation Polynomials on Finite Fields and their Combinatorial Applications*, PhD thesis, Penn. State Univ., University Park, PA, 1990. <221, 222>

[619] W. S. Chou, The period lengths of inversive pseudorandom vector generations, *Finite Fields Appl.* 1 (1995) 126–132. <221, 222>

[620] W.-S. Chou, The factorization of Dickson polynomials over finite fields, *Finite Fields Appl.* 3 (1997) 84–96. <276, 277, 282>

[621] W.-S. Chou and S. D. Cohen, Primitive elements with zero traces, *Finite Fields Appl.* 7 (2001) 125–141. <87, 90>

[622] W. S. Chou, J. Gomez-Calderon, and G. L. Mullen, Value sets of Dickson polynomials over finite fields, *J. Number Theory* 30 (1988) 334–344. <226, 228, 229>

[623] W.-S. Chou, J. Gomez-Calderon, G. L. Mullen, D. Panario, and D. Thomson, Subfield value sets of polynomials over finite fields, *Funct. Approx. Comment. Math.* (In press, 2012) 21 pages. <229>

[624] W.-S. Chou and G. L. Mullen, A note on value sets of polynomials over finite fields, preprint, 2012. <227, 229>

[625] S. Chowla and H. J. Ryser, Combinatorial problems, *Canadian J. Math.* 2 (1950) 93–99. <592, 598>

[626] S. Chowla and H. Zassenhaus, Some conjectures concerning finite fields, *Norske Vid. Selsk. Forh. (Trondheim)* 41 (1968) 34–35. <221, 222>

[627] M. Christopoulou, T. Garefalakis, D. Panario, and D. Thomson, The trace of an optimal normal element and low complexity normal bases, *Des. Codes Cryptogr.* 49 (2008) 199–215. <113, 119, 122>

[628] M. Christopoulou, T. Garefalakis, D. Panario, and D. Thomson, Gauss periods as constructions of low complexity normal bases, *Designs, Codes and Cryptogra-*

phy (2011) 1–20, 10.1007/s10623-011-9490-4. <113, 114, 122>

[629] W. Chu and C. J. Colbourn, Optimal frequency-hopping sequences via cyclotomy, *IEEE Trans. Inform. Theory* 51 (2005) 1139–1141. <836, 839>

[630] D. V. Chudnovsky and G. V. Chudnovsky, Sequences of numbers generated by addition in formal groups and new primality and factorization tests, *Adv. in Appl. Math.* 7 (1986) 385–434. <434, 440>

[631] F. R. K. Chung, Diameters and eigenvalues, *J. Amer. Math. Soc.* 2 (1989) 187–196. <636, 649>

[632] F. R. K. Chung, V. Faber, and T. A. Manteuffel, An upper bound on the diameter of a graph from eigenvalues associated with its Laplacian, *SIAM J. Discrete Math.* 7 (1994) 443–457. <636, 649>

[633] F. R. K. Chung, J. A. Salehi, and V. K. Wei, Optical orthogonal codes: design, analysis, and applications, *IEEE Trans. Inform. Theory* 35 (1989) 595–604. <834, 835, 839>

[634] J. Chung and A. Hasan, More generalized Mersenne numbers, In *Selected Areas in Cryptography*, volume 3006 of *Lecture Notes in Comput. Sci.*, 335–347, Springer, Berlin, 2004. <345, 356>

[635] J.-H. Chung and K. Yang, Bounds on the linear complexity and the 1-error linear complexity over F_p of M-ary Sidel′nikov sequences, In *Sequences and Their Applications—SETA 2006*, volume 4086 of *Lecture Notes in Comput. Sci.*, 74–87, Springer, Berlin, 2006. <327, 329>

[636] S.-Y. Chung, G. D. Forney, T. J. Richardson, and R. L. Urbanke, On the design of low-density parity-check codes within 0.0045 db of the Shannon limit, *IEEE Commun. Lett.* 5 (2001) 58–60. <704, 710>

[637] J. Cilleruelo, Combinatorial problems in finite fields and Sidon sets, Combinatorica, to appear, 2012. <185, 186>

[638] J. Cilleruelo, M. Z. Garaev, O. A., and I. E. Shparlinski, On the concentration of points of polynomial maps and applications, To appear in *Math. Zeitschrift*. <337>

[639] J. Cilleruelo, M. Z. Garaev, O. A., and I. E. Shparlinski, Concentration of points and isomorphism classes of hyperelliptic curves over a finite field in some thin families, Preprint, 2011. <337>

[640] S. M. Cioabă, Closed walks and eigenvalues of abelian Cayley graphs, *C. R. Math. Acad. Sci. Paris* 342 (2006) 635–638. <642, 649>

[641] S. M. Cioabă, *Eigenvalues, Expanders and Gaps Between Primes*, ProQuest LLC, Ann Arbor, MI, 2006, Thesis (Ph.D.)–Queen's University (Canada). <638, 639, 648, 649>

[642] S. M. Cioabă, Eigenvalues of graphs and a simple proof of a theorem of Greenberg, *Linear Algebra Appl.* 416 (2006) 776–782. <639, 649>

[643] S. M. Cioabă, On the extreme eigenvalues of regular graphs, *J. Combin. Theory, Ser. B* 96 (2006) 367–373. <638, 649>

[644] S. M. Cioabă and M. R. Murty, Expander graphs and gaps between primes, *Forum Math.* 20 (2008) 745–756. <648, 649>

[645] J. A. Cipra, Waring's number in a finite field, *Integers* 9 (2009) A34, 435–440. <169, 179, 206, 207>

[646] J. A. Cipra, T. Cochrane, and C. Pinner, Heilbronn's conjecture on Waring's number (mod p), *J. Number Theory* 125 (2007) 289–297. <206, 207>

[647] M. Cipu, Dickson polynomials that are permutations, *Serdica Math. J.* 30 (2004)

177–194. <219, 222>

[648] M. Cipu and S. D. Cohen, Dickson polynomial permutations, In *Finite Fields and Applications*, volume 461 of *Contemp. Math.*, 79–90, Amer. Math. Soc., Providence, RI, 2008. <219, 222>

[649] T. Cochrane, J. Coffelt, and C. Pinner, A further refinement of Mordell's bound on exponential sums, *Acta Arith.* 116 (2005) 35–41. <184, 186>

[650] T. Cochrane, M.-C. Liu, and Z. Zheng, Upper bounds on n-dimensional Kloosterman sums, *J. Number Theory* 106 (2004) 259–274. <154, 155>

[651] T. Cochrane and C. Pinner, Sum-product estimates applied to Waring's problem mod p, *Integers* 8 (2008) A46, 18. <186, 206, 207>

[652] T. Cochrane and C. Pinner, Explicit bounds on monomial and binomial exponential sums, *Q. J. Math.* 62 (2011) 323–349. <333, 337>

[653] T. Cochrane, C. Pinner, and J. Rosenhouse, Bounds on exponential sums and the polynomial Waring problem mod p, *J. London Math. Soc., 2nd Ser.* 67 (2003) 319–336. <207>

[654] T. Cochrane and Z. Zheng, A survey on pure and mixed exponential sums modulo prime powers, In *Number Theory for the Millennium I*, 273–300, A. K. Peters, Natick, MA, 2002. <154, 155>

[655] H. Cohen, *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate Texts in Mathematics*, Springer-Verlag, Berlin, 1993. <339, 340, 352, 355, 356, 397, 787>

[656] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, editors, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Discrete Mathematics and Its Applications. Chapman & Hall/CRC, Boca Raton, FL, 2006. <29, 30, 339, 347, 349, 351, 352, 353, 356, 386, 394, 443, 445, 446, 447, 448, 449, 778, 779, 787, 788, 789, 794>

[657] H. Cohen and H. W. Lenstra, Jr., Primality testing and Jacobi sums, *Math. Comp.* 42 (1984) 297–330. <340, 356>

[658] S. Cohen and H. Niederreiter, editors, *Finite Fields and Applications*, volume 233 of *London Mathematical Society Lecture Note Series*, Cambridge, 1996. Cambridge University Press. <30>

[659] S. D. Cohen, The distribution of irreducible polynomials in several indeterminates over a finite field, *Proc. Edinburgh Math. Soc., Ser. II* 16 (1968/1969) 1–17. <77, 78, 81>

[660] S. D. Cohen, Further arithmetical functions in finite fields, *Proc. Edinburgh Math. Soc., Ser. II* 16 (1968/1969) 349–363. <361, 367>

[661] S. D. Cohen, On irreducible polynomials of certain types in finite fields, *Proc. Cambridge Philos. Soc.* 66 (1969) 335–344. <53, 54, 55, 56, 61>

[662] S. D. Cohen, The distribution of polynomials over finite fields, *Acta Arith.* 17 (1970) 255–271. <67, 69, 210, 222, 226, 227, 229, 233>

[663] S. D. Cohen, Some arithmetical functions in finite fields, *Glasgow Math. J.* 11 (1970) 21–36. <76, 78, 81>

[664] S. D. Cohen, Uniform distribution of polynomials over finite fields, *J. London Math. Soc., 2nd Ser.* 6 (1972) 93–102. <73, 75>

[665] S. D. Cohen, The values of a polynomial over a finite field, *Glasgow Math. J.* 14 (1973) 205–208. <361, 367>

[666] S. D. Cohen, The irreducibility of compositions of linear polynomials over a finite field, *Compos. Math.* 47 (1982) 149–152. <56, 59, 61, 62, 66>

[667] S. D. Cohen, The reducibility theorem for linearised polynomials over finite fields, *Bull. Austral. Math. Soc.* 40 (1989) 407–412. <62, 66>

[668] S. D. Cohen, Windmill polynomials over fields of characteristic two, *Monatsh. Math.* 107 (1989) 291–301. <65, 66, 84, 85>

[669] S. D. Cohen, Exceptional polynomials and the reducibility of substitution polynomials, *Enseign. Math., IIe Ser.* 36 (1990) 53–65. <230, 233>

[670] S. D. Cohen, Primitive elements and polynomials with arbitrary trace, *Discrete Math.* 83 (1990) 1–7. <87, 90>

[671] S. D. Cohen, Proof of a conjecture of Chowla and Zassenhaus on permutation polynomials, *Canad. Math. Bull.* 33 (1990) 230–234. <221, 222>

[672] S. D. Cohen, Permutation polynomials and primitive permutation groups, *Arch. Math. (Basel)* 57 (1991) 417–423. <210, 211, 222>

[673] S. D. Cohen, The explicit construction of irreducible polynomials over finite fields, *Des. Codes Cryptogr.* 2 (1992) 169–174. <56, 60, 61, 278, 282>

[674] S. D. Cohen, Dickson polynomials of the second kind that are permutations, *Canad. J. Math.* 46 (1994) 225–238. <219, 222>

[675] S. D. Cohen, Dickson permutations, In *Number-Theoretic and Algebraic Methods in Computer Science*, 29–51, World Sci. Publ., River Edge, NJ, 1995. <219, 222>

[676] S. D. Cohen, Permutation group theory and permutation polynomials, In *Algebras and Combinatorics*, 133–146, Springer, Singapore, 1999. <209, 222>

[677] S. D. Cohen, Gauss sums and a sieve for generators of Galois fields, *Publ. Math. Debrecen* 56 (2000) 293–312. <84, 85, 87, 89, 90>

[678] S. D. Cohen, Kloosterman sums and primitive elements in Galois fields, *Acta Arith.* 94 (2000) 173–201. <88, 90>

[679] S. D. Cohen, Primitive polynomials over small fields, In *Finite Fields and Applications*, volume 2948 of *Lecture Notes in Comput. Sci.*, 197–214, Springer, Berlin, 2004. <88, 90>

[680] S. D. Cohen, Explicit theorems on generator polynomials, *Finite Fields Appl.* 11 (2005) 337–357. <56, 60, 61, 72, 75>

[681] S. D. Cohen, Primitive polynomials with a prescribed coefficient, *Finite Fields Appl.* 12 (2006) 425–491. <87, 90>

[682] S. D. Cohen and M. D. Fried, Lenstra's proof of the Carlitz-Wan conjecture on exceptional polynomials: an elementary version, *Finite Fields Appl.* 1 (1995) 372–375. <211, 222, 231, 233>

[683] S. D. Cohen and M. J. Ganley, Commutative semifields, two-dimensional over their middle nuclei, *J. Algebra* 75 (1982) 373–385. <269, 270, 274>

[684] S. D. Cohen and D. Hachenberger, Primitive normal bases with prescribed trace, *Appl. Algebra Engrg. Comm. Comput.* 9 (1999) 383–403. <84, 85, 110>

[685] S. D. Cohen and D. Hachenberger, Primitivity, freeness, norm and trace, *Discrete Math.* 214 (2000) 135–144. <87, 89, 90>

[686] S. D. Cohen and S. Huczynska, Primitive free quartics with specified norm and trace, *Acta Arith.* 109 (2003) 359–385. <84, 85, 87, 89, 90, 110>

[687] S. D. Cohen and S. Huczynska, The primitive normal basis theorem—without a computer, *J. London Math. Soc., 2nd Ser.* 67 (2003) 41–56. <88, 90>

[688] S. D. Cohen and S. Huczynska, The strong primitive normal basis theorem, *Acta Arith.* 143 (2010) 299–332. <90, 110>

[689] S. D. Cohen and C. King, The three fixed coefficient primitive polynomial theorem, *JP J. Algebra Number Theory Appl.* 4 (2004) 79–87. <88, 90>

[690] S. D. Cohen and R. W. Matthews, A class of exceptional polynomials, *Trans. Amer. Math. Soc.* 345 (1994) 897–909. <232, 233, 294, 295>

[691] S. D. Cohen and R. W. Matthews, Exceptional polynomials over finite fields, *Finite Fields Appl.* 1 (1995) 261–277. <232, 233>

[692] S. D. Cohen and D. Mills, Primitive polynomials with first and second coefficients prescribed, *Finite Fields Appl.* 9 (2003) 334–350. <88, 90>

[693] S. D. Cohen, G. L. Mullen, and P. J.-S. Shiue, The difference between permutation polynomials over finite fields, *Proc. Amer. Math. Soc.* 123 (1995) 2011–2015. <221, 222>

[694] S. D. Cohen and M. Prešern, Primitive finite field elements with prescribed trace, *Southeast Asian Bull. Math.* 29 (2005) 283–300. <87, 90>

[695] S. D. Cohen and M. Prešern, Primitive polynomials with prescribed second coefficient, *Glasgow Math. J.* 48 (2006) 281–307. <87, 90>

[696] S. D. Cohen and M. Prešern, The Hansen-Mullen primitive conjecture: completion of proof, In *Number Theory and Polynomials*, volume 352 of *London Math. Soc. Lecture Note Ser.*, 89–120, Cambridge Univ. Press, Cambridge, 2008. <87, 90>

[697] R. M. Cohn, *Difference Algebra*, Interscience Publishers John Wiley & Sons, New York-London-Sydeny, 1965. <231, 233>

[698] C. J. Colbourn, Covering arrays from cyclotomy, *Des. Codes Cryptogr.* 55 (2010) 201–219. <602, 610>

[699] C. J. Colbourn, Covering arrays and hash families, In *Information Security and Related Combinatorics*, NATO Peace and Information Security, 99–136, IOS Press, 2011. <601, 610>

[700] C. J. Colbourn and J. H. Dinitz, editors, *Handbook of Combinatorial Designs*, Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton, FL, second edition, 2007. <29, 30, 310, 317, 542, 546, 547, 555, 563, 565, 587, 590, 591, 598, 607, 608, 610>

[701] C. J. Colbourn and A. C. H. Ling, Linear hash families and forbidden configurations, *Des. Codes Cryptogr.* 52 (2009) 25–55. <604, 610>

[702] C. J. Colbourn and A. Rosa, *Triple Systems*, Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1999. <582, 586, 590>

[703] G. E. Collins, Computing multiplicative inverses in GF(p), *Math. Comp.* 23 (1969) 197–200. <352, 356>

[704] G. E. Collins, Lecture notes on arithmetic algorithms, 1980, University of Wisconsin. <352, 356>

[705] A. Commeine and I. Semaev, An algorithm to solve the discrete logarithm problem with the number field sieve, In *Public Key Cryptography—PKC 2006*, volume 3958 of *Lecture Notes in Comput. Sci.*, 174–190, Springer, Berlin, 2006. <392, 394>

[706] "Computer Algebra Group, University of Sydney", Magma Computational Algebra System, `http://magma.maths.usyd.edu.au/magma`, as viewed in July, 2012. <31, 45, 46>

[707] A. Conflitti, On elements of high order in finite fields, In *Cryptography and Computational Number Theory*, volume 20 of *Progr. Comput. Sci. Appl. Logic*, 11–14,

Birkhäuser, Basel, 2001. <94>

[708] K. Conrad, Jacobi sums and Stickelberger's congruence, *Enseign. Math,. IIe Ser.* 41 (1995) 141–153. <146, 155>

[709] K. Conrad, On Weil's proof of the bound for Kloosterman sums, *J. Number Theory* 97 (2002) 439–446. <148, 149, 155>

[710] S. Contini and I. E. Shparlinski, On Stern's attack against secret truncated linear congruential generators, volume 3574 of *Lecture Notes in Comput. Sci.*, 52–60, Springer, Berlin, 2005. <331, 337>

[711] D. Coppersmith, Fast evaluation of logarithms in fields of characteristic two, *IEEE Trans. Inform. Theory* 30 (1984) 587–594. <341, 356, 363, 367, 391, 394>

[712] D. Coppersmith, Solving linear equations over GF(2): block Lanczos algorithm, *Linear Algebra Appl.* 192 (1993) 33–60. <393, 394, 527>

[713] D. Coppersmith, Solving homogeneous linear equations over GF(2) via block Wiedemann algorithm, *Math. Comp.* 62 (1994) 333–350. <393, 394, 527>

[714] D. Coppersmith, Rectangular matrix multiplication revisited, *J. Complexity* 13 (1997) 42–49. <513, 527>

[715] D. Coppersmith, A. M. Odlyzko, and R. Schroeppel, Discrete logarithms in GF(p), *Algorithmica* 1 (1986) 1–15. <393, 394>

[716] D. Coppersmith, J. Stern, and S. Vaudenay, The security of the birational permutation signature schemes, *J. Cryptology* 10 (1997) 207–221. <759, 765, 770, 774>

[717] D. Coppersmith and S. Winograd, Matrix multiplication via arithmetic progressions, *J. Symbolic Comput.* 9 (1990) 251–280. <373, 375, 513, 527>

[718] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*, MIT Press, Cambridge, MA, second edition, 2001. <44, 46>

[719] C. J. Corrada-Bravo and I. Rubio, Deterministic interleavers for turbo codes with random-like performance and simple implementation, In *Proc. Third International Symposium on Turbo Codes*, Brest, France, 2003. <717, 718>

[720] R. S. Coulter, The classification of planar monomials over fields of prime square order, *Proc. Amer. Math. Soc.* 134 (2006) 3373–3378. <273, 274>

[721] R. S. Coulter and M. Henderson, The compositional inverse of a class of permutation polynomials over a finite field, *Bull. Austral. Math. Soc.* 65 (2002) 521–526. <221, 222>

[722] R. S. Coulter and M. Henderson, Commutative presemifields and semifields, *Adv. Math.* 217 (2008) 282–304. <270, 274>

[723] R. S. Coulter, M. Henderson, and P. Kosick, Planar polynomials for commutative semifields with specified nuclei, *Des. Codes Cryptogr.* 44 (2007) 275–286. <269, 270, 274>

[724] R. S. Coulter, M. Henderson, and R. Matthews, A note on constructing permutation polynomials, *Finite Fields Appl.* 15 (2009) 553–557. <217, 218, 222>

[725] R. S. Coulter and F. Lazebnik, On the classification of planar monomials over fields of square order, *Finite Fields Appl.* 18 (2012) 316–336. <273, 274>

[726] R. S. Coulter and R. W. Matthews, Planar functions and planes of Lenz-Barlotti class II, *Des. Codes Cryptogr.* 10 (1997) 167–184. <264, 265, 272, 273, 274>

[727] R. S. Coulter and R. W. Matthews, On the permutation behaviour of Dickson polynomials of the second kind, *Finite Fields Appl.* 8 (2002) 519–530. <219, 222>

[728] R. S. Coulter and R. W. Matthews, On the number of distinct values of a class of functions over a finite field, *Finite Fields Appl.* 17 (2011) 220–224. <229, 273, 274>

[729] N. T. Courtois, Fast algebraic attacks on stream ciphers with linear feedback, In *Advances in Cryptology—CRYPTO 2003*, volume 2729 of *Lecture Notes in Comput. Sci.*, 176–194, Springer, Berlin, 2003. <241, 245>

[730] N. T. Courtois, Algebraic attacks over GF(2^k), application to HFE Challenge 2 and Sflash-v2, In *Public Key Cryptography—PKC 2004*, volume 2947 of *Lecture Notes in Comput. Sci.*, 201–217, Springer, Berlin, 2004. <772, 774>

[731] N. T. Courtois, M. Daum, and P. Felke, On the security of HFE, HFEv- and Quartz, In *Public Key Cryptography—PKC 2003*, volume 2567 of *Lecture Notes in Comput. Sci.*, 337–350, Springer, Berlin, 2002. <761, 771, 774>

[732] N. T. Courtois, L. Goubin, W. Meier, and J.-D. Tacier, Solving underdefined systems of multivariate quadratic equations, In *PubKeyCrypt 2002*, volume 2274 of *Lecture Notes in Computer Science*, 211–227. David Naccache and Pascal Paillier, editors, 2002. <772, 774>

[733] N. T. Courtois, L. Goubin, and J. Patarin, *SFLASH: Primitive specification (second revised version)*, 2002, `https://www.cosic.esat.kuleuven.be/nessie`, Submissions, Sflash, 11 pages. <763, 774>

[734] N. T. Courtois, A. Klimov, J. Patarin, and A. Shamir, Efficient algorithms for solving overdefined systems of multivariate polynomial equations, In *Advances in Cryptology—EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Comput. Sci.*, 392–407, Springer, Berlin, 2000. <771, 772, 774>

[735] N. T. Courtois and W. Meier, Algebraic attacks on stream ciphers with linear feedback, In *Advances in Cryptology—EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Comput. Sci.*, 345–359, Springer, Berlin, 2003. <240, 241, 245>

[736] N. T. Courtois and J. Patarin, About the XL algorithm over GF(2), In *Topics in Cryptology—CT-RSA 2003*, volume 2612 of *Lecture Notes in Comput. Sci.*, 141–157, Springer, Berlin, 2003. <772, 774>

[737] N. T. Courtois and J. Pieprzyk, Cryptanalysis of block ciphers with overdefined systems of equations, In *Advances in Cryptology—ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Comput. Sci.*, 267–287, Springer, Berlin, 2002. <772, 773, 774>

[738] J.-M. Couveignes and T. Henocq, Action of modular correspondences around CM points, In C. Fieker and D. R. Kohel, editors, *Algorithmic Number Theory—ANTS-V*, volume 2369 of *Lecture Notes in Computer Science*, 234–243, Berlin, 2002, Springer-Verlag. <777, 787>

[739] J.-M. Couveignes and J.-G. Kammerer, The geometry of flex tangents to a cubic curve and its parameterizations, *Journal of Symbolic Computation* 47 (2012) 266–281. <787>

[740] J.-M. Couveignes and R. Lercier, Elliptic periods for finite fields, *Finite Fields Appl.* 15 (2009) 1–22. <115, 116, 122>

[741] J.-M. Couveignes and R. Lercier, Fast construction of irreducible polynomials over finite fields, *Israel Journal of Mathematics* (2011), To appear. ArXiv:0905.1642v2. <371, 373>

[742] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms*, Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. <774, 816,

824>

[743] D. A. Cox, *Galois Theory*, Pure and Applied Mathematics (New York). Wiley-Interscience, John Wiley & Sons, Hoboken, NJ, 2004. <2, 8, 10>

[744] R. Crandall, Method and apparatus for public key exchange in a cryptographic system, United States Patent 5,159,632, Date: Oct. 27th 1992. <345, 356>

[745] R. Crandall and C. Pomerance, *Prime Numbers*, Springer, New York, second edition, 2005, A computational perspective. <339, 347, 348, 355, 356, 488, 492>

[746] R. M. Crew, Etale p-covers in characteristic p, *Compositio Math.* 52 (1984) 31–45. <479, 480>

[747] H. S. Cronie and S. B. Korada, Lossless source coding with polar codes, In *Proc. (ISIT) Symp. IEEE Int Information Theory*, 904–908, 2010. <730>

[748] E. Croot, Sums of the form $1/x_1^k + \cdots + 1/x_n^k$ modulo a prime, *Integers* 4 (2004) A20, 6. <207>

[749] S. Crozier, J. Lodge, P. Guinand, and A. Hunt, Performance of turbo codes with relative prime and golden interleaving strategies, In *Proc. of the Sixth International Mobile Satellite Conference (IMSC '99)*, 268–275, Ottawa, Ontario, Canda, 1999. <717, 718>

[750] C. Culbert and G. L. Ebert, Circle geometry and three-dimensional subregular translation planes, *Innov. Incidence Geom.* 1 (2005) 3–18. <559, 565>

[751] T. W. Cusick, Value sets of some polynomials over finite fields GF(2^{2m}), *SIAM J. Comput.* 27 (1998) 120–131 (electronic). <228, 229>

[752] T. W. Cusick, Polynomials over base 2 finite fields with evenly distributed values, *Finite Fields Appl.* 11 (2005) 278–291. <228, 229>

[753] T. W. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory*, volume 66 of *North-Holland Mathematical Library*, Elsevier Science B.V., Amsterdam, revised edition, 2004. <29, 30, 320, 321, 326, 327, 329>

[754] T. W. Cusick and P. Müller, Wan's bound for value sets of polynomials, In *Finite Fields and Applications*, volume 233 of *London Math. Soc. Lecture Note Ser.*, 69–72, Cambridge Univ. Press, Cambridge, 1996. <226, 228, 229>

[755] S. Czapor, K. Geddes, and G. Labahn, *Algorithms for Computer Algebra*, Kluwer Academic Publishers, 1992. <29, 30, 375, 385>

[756] J. Daemen and V. Rijmen, *The Design of Rijndael: AES – the Advanced Encryption Standard*, Springer-Verlag, 2002. <29, 30, 741, 750, 751, 754>

[757] Z. Dai, Multi-continued fraction algorithms and their applications to sequences, In *Sequences and Their Applications—SETA 2006*, volume 4086 of *Lecture Notes in Comput. Sci.*, 17–33, Springer, Berlin, 2006. <322, 329>

[758] Z. Dai and X. Feng, Classification and counting on multi-continued fractions and its application to multi-sequences, *Sci. China, Ser. F* 50 (2007) 351–358. <322, 329>

[759] Z. Dai, K. Wang, and D. Ye, Multi-continued fraction algorithm on multi-formal Laurent series, *Acta Arith.* 122 (2006) 1–16. <322, 329>

[760] Z. Dai and J. Yang, Multi-continued fraction algorithm and generalized B-M algorithm over $\mathbb{F}_q$, *Finite Fields Appl.* 12 (2006) 379–402. <322, 329>

[761] F. Daneshgaran and M. Mondin, Design of interleavers for turbo codes: iterative interleaver growth algorithms of polynomial complexity, *IEEE Trans. Inform. Theory* 45 (1999) 1845–1859. <717, 718>

[762] A. Danilevsky, The numerical solution of the secular equation, *Matem. Sbornik* 44

(1937) 169–171, In Russian. <368, 373>

[763] G. Darbi, Sulla riducibilità delle equazioni aldebriche, *Ann. Mat. Pura Appl.* 4 (1927) 185–208. <58, 61>

[764] H. Darmon and J.-F. Mestre, Courbes hyperelliptiques à multiplications réelles et une construction de Shih, *Canad. Math. Bull.* 43 (2000) 304–311. <232, 233>

[765] P. Das, The number of permutation polynomials of a given degree over a finite field, *Finite Fields Appl.* 8 (2002) 478–490. <212, 222>

[766] P. Das, The number of polynomials of a given degree over a finite field with value sets of a given cardinality, *Finite Fields Appl.* 9 (2003) 168–174. <228, 229>

[767] P. Das, Value sets of polynomials and the Cauchy Davenport theorem, *Finite Fields Appl.* 10 (2004) 113–122. <228, 229>

[768] P. Das and G. L. Mullen, Value sets of polynomials over finite fields, In *Finite Fields with Applications to Coding Theory, Cryptography and Related Areas*, 80–85, Springer, Berlin, 2002. <227, 229>

[769] H. Davenport, Bases for finite fields, *J. London Math. Soc., 2nd Ser.* 43 (1968) 21–39. <109, 110, 130, 132>

[770] H. Davenport and D. J. Lewis, Character sums and primitive roots in finite fields, *Rend. Circ. Mat. Palermo, 2nd Ser.* 12 (1963) 129–136. <175, 179>

[771] H. Davenport and D. J. Lewis, Notes on congruences. I, *Quart. J. Math. Oxford, 2nd Ser.* 14 (1963) 51–60. <231, 233, 285, 295>

[772] J. H. Davenport, Y. Siret, and É. Tournier, *Calcul Formel : Systèmes et Algorithmes de Manipulations Algébriques.*, Masson, Paris, France, 1987. <375, 385>

[773] J. H. Davenport and B. M. Trager, Factorization over finitely generated fields, In *SYMSAC'81: Proceedings of the Fourth ACM Symposium on Symbolic and Algebraic Computation*, 200–205. ACM, 1981. <380, 385>

[774] G. Davidoff, P. Sarnak, and A. Valette, *Elementary Number Theory, Group Theory, and Ramanujan Graphs*, volume 55 of *London Mathematical Society Student Texts*, Cambridge University Press, Cambridge, 2003. <643, 644, 649>

[775] J. A. Davis, Difference sets in abelian 2-groups, *J. Combin. Theory, Ser. A* 57 (1991) 262–286. <596, 598>

[776] J. A. Davis and J. Jedwab, A unifying construction for difference sets, *J. Combin. Theory, Ser. A* 80 (1997) 13–78. <596, 598>

[777] J. A. Davis and J. Jedwab, Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes, *IEEE Trans. Inform. Theory* 45 (1999) 2397–2417. <833, 834, 839>

[778] E. Dawson and L. Simpson, Analysis and design issues for synchronous stream ciphers, In *Coding Theory and Cryptology*, volume 1 of *Lect. Notes Ser. Inst. Math. Sci. Natl. Univ. Singap.*, 49–90, World Sci. Publ., River Edge, NJ, 2002. <319, 329>

[779] J. De Beule and L. Storme, *Current Research Topics in Galois Geometry*, Nova Academic Publishers, Inc., New York, 2012. <29, 30, 564, 565>

[780] P. de la Harpe and A. Musitelli, Expanding graphs, Ramanujan graphs, and 1-factor perturbations, *Bull. Belg. Math. Soc. Simon Stevin* 13 (2006) 673–680. <648, 649>

[781] M. J. de Resmini, D. Ghinelli, and D. Jungnickel, Arcs and ovals from abelian groups, *Des. Codes Cryptogr.* 26 (2002) 213–228. <270, 272, 274>

[782] M. J. de Resmini and N. Hamilton, Hyperovals and unitals in Figueroa planes,

European J. Combin. 19 (1998) 215–220. <563, 565>

[783] B. de Smit and H. W. Lenstra, Standard models for finite fields, in preparation. <394, 395, 397>

[784] B. de Smit and H. W. Lenstra, Standard models for finite fields: the definition, 2008, `http://www.math.leidenuniv.nl/~desmit/papers/standard_models.pdf`, [Online]. <395, 397>

[785] T. Decker and P. Wocjan, Efficient quantum algorithm for hidden quadratic and cubic polynomial function graphs, preprint available, `http://arxiv.org/abs/quant-ph/0703195`, 2007. <830, 831>

[786] W. Decker, G.-M. Greuel, G. Pfister, and H. Schönemann, SINGULAR 3-1-5 — A computer algebra system for polynomial computations, 2012, http://www.singular.uni-kl.de. <45, 46>

[787] R. Dedekind, Abriss einer theorie der höheren congruenzen in bezug auf einen reellen primzahl-modulus, *J. Reine Angew. Math.* 54 (1857) 1–26. <8, 10>

[788] P. Deligne, Les constantes des équations fonctionnelles des fonctions L, In *Modular Functions of One Variable, II (Proc. Internat. Summer School, Univ. Antwerp*, 501–597. Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973. <471, 472>

[789] P. Deligne, La conjecture de Weil. I, *Inst. Hautes Études Sci. Publ. Math.* (1974) 273–307. <157, 163, 189, 191, 195, 463, 465, 466, 469, 472>

[790] P. Deligne, *Applications de la Formule des Traces aux Sommes Trigonometriques,* in *Cohomologie Étale*, Lecture Notes in Mathematics, Vol. 569. Springer-Verlag, Berlin, 1977, Séminaire de Géométrie Algébrique du Bois-Marie SGA 41$\emptyset er$2, Avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie et J. L. Verdier. <163>

[791] P. Deligne, *Cohomologie Étale*, Lecture Notes in Mathematics, Vol. 569. Springer-Verlag, Berlin, 1977, Séminaire de Géométrie Algébrique du Bois-Marie SGA 41$\emptyset er$2, Avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie et J. L. Verdier. <30, 463, 464, 467, 468, 470, 472>

[792] P. Deligne, La conjecture de Weil. II, *Inst. Hautes Études Sci. Publ. Math.* (1980) 137–252. <465, 468, 469, 472, 480>

[793] P. Deligne and N. Katz, *Groupes de Monodromie en Géométrie Algébrique. II*, Lecture Notes in Mathematics, Vol. 340. Springer-Verlag, Berlin, 1973, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 II), Dirigé par P. Deligne et N. Katz. <159, 161, 163, 479, 480>

[794] P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Res. Rep. Suppl.* (1973) vi+97. <244, 245>

[795] P. Delsarte, Four fundamental parameters of a code and their combinatorial significance, *Information and Control* 23 (1973) 407–438. <622, 633, 654, 655, 656, 664, 682, 694>

[796] P. Delsarte, On subfield subcodes of modified Reed-Solomon codes, *IEEE Trans. Information Theory* IT-21 (1975) 575–576. <659, 660, 675, 694>

[797] P. Delsarte, Bilinear forms over a finite field, with applications to coding theory, *J. Combin. Theory, Ser. A* 25 (1978) 226–241. <836, 839>

[798] P. Delsarte and J.-M. Goethals, Alternating bilinear forms over $GF(q)$, *J. Combin. Theory, Ser. A* 19 (1975) 26–50. <693, 694>

[799] P. Delsarte, J.-M. Goethals, and F. J. MacWilliams, On generalized Reed-Muller codes and their relatives, *Information and Control* 16 (1970) 403–442. <677, 694>

[800] P. Delsarte and V. I. Levenshtein, Association schemes and coding theory, *IEEE Trans. Inform. Theory* 44 (1998) 2477–2504, Information theory: 1948–1998. <682, 694>

[801] P. Dembowski, *Finite Geometries*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44. Springer-Verlag, Berlin, 1968. <26, 29, 30, 266, 270, 556, 559, 565, 580, 582, 590>

[802] P. Dembowski and T. G. Ostrom, Planes of order n with collineation groups of order n^2, *Math. Z.* 103 (1968) 239–258. <247, 254, 271, 273, 274>

[803] U. Dempwolff, Automorphisms and equivalence of bent functions and of difference sets in elementary abelian 2-groups, *Comm. Algebra* 34 (2006) 1077–1131. <265>

[804] U. Dempwolff, Semifield planes of order 81, *J. Geom.* 89 (2008) 1–16. <268, 270>

[805] U. Dempwolff and M. Röder, On finite projective planes defined by planar monomials, *Innov. Incidence Geom.* 4 (2006) 103–108. <272, 274>

[806] J. Denef and F. Loeser, Weights of exponential sums, intersection cohomology, and Newton polyhedra, *Invent. Math.* 106 (1991) 275–294. <159, 163, 190, 195, 469, 472>

[807] J. Denef and F. Loeser, Character sums associated to finite Coxeter groups, *Trans. Amer. Math. Soc.* 350 (1998) 5047–5066. <140, 155>

[808] J. Denef and F. Loeser, Definable sets, motives and p-adic integrals, *J. Amer. Math. Soc.* 14 (2001) 429–469. <294, 295>

[809] J. Denef and F. Vercauteren, An extension of Kedlaya's algorithm to Artin-Schreier curves in characteristic 2, In *Algorithmic Number Theory*, volume 2369 of *Lecture Notes in Comput. Sci.*, 308–323, Springer, Berlin, 2002. <447, 449>

[810] J. Denef and F. Vercauteren, Counting points on C_{ab} curves using Monsky-Washnitzer cohomology, *Finite Fields Appl.* 12 (2006) 78–102. <484>

[811] J. Denef and F. Vercauteren, An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2, *J. Cryptology* 19 (2006) 1–25. <447, 449, 484>

[812] J. Dénes and A. D. Keedwell, *Latin Squares and Their Applications*, Academic Press, New York, 1974. <547>

[813] J. Dénes and A. D. Keedwell, *Latin Squares*, volume 46 of *Annals of Discrete Mathematics*, North-Holland Publishing Co., Amsterdam, 1991. <29, 30>

[814] R. H. F. Denniston, Some maximal arcs in finite projective planes, *J. Combinatorial Theory* 6 (1969) 317–319. <564, 565>

[815] R. H. F. Denniston, Uniqueness of the inverse plane of order 5, *Manuscripta Math.* 8 (1973) 11–19. <580>

[816] R. H. F. Denniston, Uniqueness of the inversive plane of order 7, *Manuscripta Math.* 8 (1973) 21–26. <580>

[817] J.-M. Deshouillers, G. Effinger, H. te Riele, and D. Zinoviev, A complete Vinogradov 3-primes theorem under the Riemann hypothesis, *Electron. Res. Announc. Amer. Math. Soc.* 3 (1997) 99–104. <489, 492>

[818] M. Deuring, Galoissche Theorie und Darstellungstheorie, *Math. Ann.* 107 (1933) 140–144. <104, 110>

[819] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Hansischen Univ.* 14 (1941) 197–272. <424, 433>

[820] M. Dewar, L. Moura, D. Panario, B. Stevens, and Q. Wang, Division of trinomials by pentanomials and orthogonal arrays, *Des. Codes Cryptogr.* 45 (2007) 1–17.

<631, 632, 633>

[821] M. Dewar and D. Panario, Linear transformation shift registers, *IEEE Trans. Inform. Theory* 49 (2003) 2047–2052. <65, 66>

[822] M. Dewar and D. Panario, Mutual irreducibility of certain polynomials, In *Finite Fields and Applications*, volume 2948 of *Lecture Notes in Comput. Sci.*, 59–68, Springer, Berlin, 2004. <65, 66>

[823] J.-F. Dhem, *Design of an Efficient Public Key Cryptographic Library for RISC-Based Smart Cards*, PhD thesis, Faculté des sciences appliquées, Laboratoire de microélectronique, Université catholique de Louvain-la-Neuve, Belgique, 1998, available at `http://users.belgacom.net/dhem/these/index.html`. <347, 356>

[824] A. Díaz and E. Kaltofen, FoxBox a system for manipulating symbolic objects in black box representation, In *ISSAC '98: Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation*, 30–37, 1998. <385>

[825] J. W. Di Paola, On minimum blocking coalitions in small projective plane games, *SIAM J. Appl. Math.* 17 (1969) 378–392. <552, 555>

[826] P. Diaconis and R. Graham, Products of universal cycles, In E. D. Demaine, M. L. Demaine, and T. Rodgers, editors, *A Lifetime of Puzzles*, 35–55, A. K. Peters Ltd., Wellesley, MA, 2008. <623, 633>

[827] P. Diaconis and R. Graham, *Magical Mathematics: The Mathematical Ideas that Animate Great Magic Tricks*, Princeton University Press, 2011. <623, 633>

[828] P. Diaconis and M. Shahshahani, Generating a random permutation with random transpositions, *Z. Wahrsch. Verw. Gebiete* 57 (1981) 159–179. <642, 643, 649>

[829] J. Dick, Walsh spaces containing smooth functions and quasi-Monte Carlo rules of arbitrary high order, *SIAM J. Numer. Anal.* 46 (2008) 1519–1553. <614, 619, 621>

[830] J. Dick, P. Kritzer, G. Leobacher, and F. Pillichshammer, Constructions of general polynomial lattice rules based on the weighted star discrepancy, *Finite Fields Appl.* 13 (2007) 1045–1070. <615, 621>

[831] J. Dick and H. Niederreiter, On the exact t-value of Niederreiter and Sobol' sequences, *J. Complexity* 24 (2008) 572–581. <619, 621>

[832] J. Dick and H. Niederreiter, Duality for digital sequences, *J. Complexity* 25 (2009) 406–414. <619, 621>

[833] J. Dick and F. Pillichshammer, *Digital Nets and Sequences: Discrepancy Theory and Quasi-Monte Carlo Integration*, Cambridge University Press, Cambridge, 2010. <611, 614, 615, 616, 619, 621>

[834] L. E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, *Ann. of Math.* 11 (1896/97) 65–120. <209, 222, 230, 232, 233>

[835] L. E. Dickson, Higher irreducible congruences, *Bull. Amer. Math. Soc.* 3 (1897) 381–389. <58, 61>

[836] L. E. Dickson, A class of groups in an arbitrary realm connected with the configuration of the 27 lines on a cubic surface, *Quart. J. Pure Appl. Math.* 33 (1901) 145–173. <10>

[837] L. E. Dickson, Theory of linear groups in an arbitrary field, *Trans. Amer. Math. Soc.* 2 (1901) 363–394. <10>

[838] L. E. Dickson, A new system of simple groups, *Math. Ann.* 60 (1905) 137–150.

<10>

[839] L. E. Dickson, On finite algebras, In *Gesellschaften der Wissenschaften zu Göttingen*, 358–393, 1905. <268, 270>

[840] L. E. Dickson, Criteria for the irreducibility of functions in a finite field, *Bull. Amer. Math. Soc.* 13 (1906) 1–8. <63, 66>

[841] L. E. Dickson, On commutative linear algebras in which division is always uniquely possible, *Trans. Amer. Math. Soc.* 7 (1906) 514–522. <268, 270, 274>

[842] L. E. Dickson, A class of groups in an arbitrary realm connected with the configuration of the 27 lines on a cubic surface (second paper), *Quart. J. Pure Appl. Math.* 39 (1908) 205–209. <10>

[843] L. E. Dickson, A fundamental system of invariants of the general modular linear group with a solution of the form problem, *Trans. Amer. Math. Soc.* 12 (1911) 75–98. <58, 59, 61>

[844] L. E. Dickson, *Linear Groups: With an Exposition of the Galois Field Theory*, with an introduction by W. Magnus. Dover Publications Inc., New York, 1958. <2, 10, 29, 30, 57, 58, 59, 61, 66, 68, 69>

[845] L. E. Dickson, *History of the Theory of Numbers. Vol. I: Divisibility and Primality*, Chelsea Publishing Co., New York, 1966. <2, 10>

[846] C. Diem, The GHS attack in odd characteristic, *Journal of the Ramanujan Mathematical Society* 18 (2003) 1–32. <777, 787, 801, 802>

[847] C. Diem, The XL-algorithm and a conjecture from commutative algebra, In *Advances in Cryptology—ASIACRYPT 2004*, volume 3329 of *Lecture Notes in Comput. Sci.*, 323–337, Springer, Berlin, 2004. <773, 774>

[848] C. Diem, An index calculus algorithm for plane curves of small degree, In *Algorithmic Number Theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, 543–557, Springer, Berlin, 2006. <789, 794, 799, 802>

[849] C. Diem and J. Scholten, Cover Attacks – A report for the AREHCC project, 2003. <793, 794>

[850] C. Diem and E. Thomé, Index calculus in class groups of non-hyperelliptic curves of genus three, *J. Cryptology* 21 (2008) 593–611. <789, 794, 800, 802>

[851] J. Dieudonné, *Sur les Groupes Classiques*, Actualités Sci. Ind., 1040 (Publ. Inst. Math. Univ. Strasbourg Nou. Sér. 1 (1945)). Hermann et Cie., Paris, 1948. <505, 507, 508, 510, 511, 512, 513>

[852] J. A. Dieudonné, *La Géométrie des Groupes Classiques*, Springer-Verlag, Berlin, 1971, IIe ed. <504, 508, 512, 513>

[853] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Trans. Information Theory* IT-22 (1976) 644–654. <177, 179, 736>

[854] W. Diffie and M. E. Hellman, New directions in cryptography, In *Secure Communications and Asymmetric Cryptosystems*, volume 69 of *AAAS Sel. Sympos. Ser.*, 143–180, Westview, Boulder, CO, 1982. <755, 774>

[855] J. F. Dillon, *Elementary Hadamard Difference-Sets*, ProQuest LLC, Ann Arbor, MI, 1974, Thesis (Ph.D.)–University of Maryland, College Park. <258, 259, 260, 262, 263, 265>

[856] J. F. Dillon, Multiplicative difference sets via additive characters, *Des. Codes Cryptogr.* 17 (1999) 225–235. <232, 233, 253, 254, 594, 598>

[857] J. F. Dillon, Geometry, codes and difference sets: exceptional connections, In *Codes and Designs*, volume 10 of *Ohio State Univ. Math. Res. Inst. Publ.*, 73–85, de Gruyter, Berlin, 2002. <232, 233, 253, 254>

[858] J. F. Dillon and H. Dobbertin, New cyclic difference sets with Singer parameters, *Finite Fields Appl.* 10 (2004) 342–389. <232, 233, 253, 254, 261, 265, 312, 317, 594, 598, 745, 746, 754>

[859] J. F. Dillon and G. McGuire, Near bent functions on a hyperplane, *Finite Fields Appl.* 14 (2008) 715–720. <303>

[860] E. Dimitrova, L. D. García-Puente, F. Hinkelmann, A. S. Jarrah, R. Laubenbacher, B. Stigler, M. Stillman, and P. Vera-Licona, Polynome, preprint available, `http://polymath.vbi.vt.edu/polynome/`, 2010. <822, 824>

[861] E. Dimitrova, L. D. García-Puente, F. Hinkelmann, A. S. Jarrah, R. Laubenbacher, B. Stigler, M. Stillman, and P. Vera-Licona, Parameter estimation for Boolean models of biological networks, *Theoret. Comput. Sci.* 412 (2011) 2816–2826. <821, 824>

[862] E. S. Dimitrova, A. S. Jarrah, R. Laubenbacher, and B. Stigler, A Gröbner fan method for biochemical network modeling, In *ISSAC 2007*, 122–126, ACM, New York, 2007. <821, 824>

[863] C. Ding, T. Helleseth, and H. Niederreiter, editors, *Sequences and Their Applications*, Springer Series in Discrete Mathematics and Theoretical Computer Science, London, 1999. Springer-Verlag London Ltd. <30>

[864] C. Ding, D. Pei, and A. Salomaa, *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*, World Scientific Publishing Co. Inc., River Edge, NJ, 1996. <222>

[865] C. Ding, Z. Wang, and Q. Xiang, Skew Hadamard difference sets from the Ree-Tits slice symplectic spreads in $\mathrm{PG}(3, 3^{2h+1})$, *J. Combin. Theory, Ser. A* 114 (2007) 867–887. <222, 273, 274, 595, 598>

[866] C. Ding, Q. Xiang, J. Yuan, and P. Yuan, Explicit classes of permutation polynomials of $\mathbb{F}_{3^{3m}}$, *Sci. China, Ser. A* 52 (2009) 639–647. <219, 222>

[867] C. Ding, G. Xiao, and W. Shan, *The Stability Theory of Stream Ciphers*, volume 561 of *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, 1991. <319, 322, 329>

[868] C. Ding and J. Yuan, A family of skew Hadamard difference sets, *J. Combin. Theory, Ser. A* 113 (2006) 1526–1535. <222, 272, 274, 595, 598>

[869] C. Ding and P. Yuan, Permutation polynomials over finite fields from a powerful lemma, *Finite Fields Appl.* 17 (2011) 560–574. <214, 217, 218, 219, 222>

[870] C. S. Ding, H. Niederreiter, and C. P. Xing, Some new codes from algebraic curves, *IEEE Trans. Inform. Theory* 46 (2000) 2638–2642. <698, 703>

[871] J. Ding, A new variant of the Matsumoto-Imai cryptosystem through perturbation, In *Public Key Cryptography—PKC 2004*, volume 2947 of *Lecture Notes in Comput. Sci.*, 305–318, Springer, Berlin, 2004. <764, 774>

[872] J. Ding, Mutants and its impact on polynomial solving strategies and algorithms, Privately distributed research note, University of Cincinnati and Technical University of Darmstadt, 2006. <772, 773, 774>

[873] J. Ding, Inverting square systems algebraically is exponential, Cryptology ePrint Archive, Report 2011/275, 2011, `http://eprint.iacr.org/`. <761, 766, 773, 774>

[874] J. Ding, J. Buchmann, M. S. E. Mohamed, W. S. A. M. Mohamed, and R.-P. Weinmann, Mutant XL, First International Conference on Symbolic Computation and Cryptography, preprint available `http://www.cdc.informatik.tu-darmstadt.de/reports/reports/MutantXL_Algorithm.pdf`, 2008. <772,

774>

[875] J. Ding, V. Dubois, B.-Y. Yang, O. C.-H. Chen, and C.-M. Cheng, Could SFLASH be repaired?, In *Automata, Languages and Programming. Part II*, volume 5126 of *Lecture Notes in Comput. Sci.*, 691–701, Springer, Berlin, 2008. <763, 764, 770, 774>

[876] J. Ding and J. E. Gower, Inoculating multivariate schemes against differential attacks, In *Public Key Cryptography—PKC 2006*, volume 3958 of *Lecture Notes in Comput. Sci.*, 290–301, Springer, Berlin, 2006. <766, 768, 774>

[877] J. Ding, J. E. Gower, and D. S. Schmidt, *Multivariate Public Key Cryptosystems*, volume 25 of *Advances in Information Security*, Springer, New York, 2006. <754, 774>

[878] J. Ding and T. Hodges, Cryptanalysis of an implementation scheme of the tamed transformation method cryptosystem, *J. Algebra Appl.* 3 (2004) 273–282. <765, 767, 774>

[879] J. Ding and T. Hodges, Inverting the HFE systems is quasi-polynomial for all fields, In *Advances in Cryptology—CRYPTO 2011*, volume 6841 of *Lecture Notes in Comput. Sci*, 724–742, Springer, Berlin, 2011. <761, 766, 773, 774>

[880] J. Ding and D. Schmidt, A common defect of the TTM cryptosystem, In *Proceedings of the Technical Track of the ACNS'03*, 68–78. ICISA Press, 2003, http://eprint.iacr.org/2003/085. <765, 767, 774>

[881] J. Ding and D. Schmidt, The new implementation schemes of the TTM cryptosystem are not secure, In *Coding, Cryptography and Combinatorics*, volume 23 of *Progr. Comput. Sci. Appl. Logic*, 113–127, Birkhäuser, Basel, 2004. <765, 767, 774>

[882] J. Ding and D. Schmidt, Cryptanalysis of HFEv and internal perturbation of HFE, In *Public Key Cryptography—PKC 2005*, volume 3386 of *Lecture Notes in Comput. Sci.*, 288–301, Springer, Berlin, 2005. <764, 774>

[883] J. Ding and D. Schmidt, Rainbow, a new multivariable polynomial signature scheme, In *Conference on Applied Cryptography and Network Security—ACNS 2005*, volume 3531 of *Lecture Notes Comput. Sci.*, 164–175, Springer, 2005. <762, 774>

[884] J. Ding, D. Schmidt, and F. Werner, Algebraic attack on HFE revisited, In *Information Security and Cryptology—ISC 2008*, volume 5352 of *Lecture Notes in Comput. Sci.*, Springer, 2007. <761, 766, 774>

[885] J. Ding, D. Schmidt, and Z. Yin, Cryptanalysis of the new TTS scheme in ches 2004, *Int. J. Inf. Sec.* 5 (2006) 231–240. <763, 774>

[886] J. Ding, C. Wolf, and B.-Y. Yang, l-invertible cycles for Multivariate Quadratic (MQ) public key cryptography, In *Public Key Cryptography—PKC 2007*, volume 4450 of *Lecture Notes in Comput. Sci.*, 266–281, Springer, Berlin, 2007. <765, 766, 774>

[887] J. Ding and B. Yang, Multivariate public key cryptography, In *Post-Quantum Cryptography*, Springer, Berlin, 2009. <754, 774>

[888] J. Ding and B.-Y. Yang, Multivariate polynomials for hashing, In *Inscrypt*, LNCS. Springer, 2007, to appear, cf. `http://eprint.iacr.org/2007/137`. <774>

[889] J. Ding, B.-Y. Yang, C.-H. O. Chen, M.-S. Chen, and C.-M. Cheng, New differential-algebraic attacks and reparametrization of rainbow, In *Applied Cryptography and Network Security*, volume 5037 of *LNCS*, 242–257. Springer, 2008, cf. `http://eprint.iacr.org/2008/108`. <763, 764, 770, 771, 772, 774>

[890] J. Ding and Z. Yin, Cryptanalysis of TTS and Tame–like signature schemes, In *Third International Workshop on Applied Public Key Infrastructures*, 2004. <765, 774>

[891] J. H. Dinitz, New lower bounds for the number of pairwise orthogonal symmetric Latin squares, In *Proceedings of the Tenth Southeastern Conference on Combinatorics, Graph Theory and Computing*, Congress. Numer., XXIII–XXIV, 393–398, Winnipeg, Man., 1979. <605, 610>

[892] J. H. Dinitz and D. R. Stinson, The construction and uses of frames, *Ars Combin.* 10 (1980) 31–53. <606, 607, 610>

[893] J. H. Dinitz and D. R. Stinson, Room squares and related designs, In *Contemporary Design Theory*, Wiley-Intersci. Ser. Discrete Math. Optim., 137–204, Wiley, New York, 1992. <607, 610>

[894] J. H. Dinitz and G. S. Warrington, The spectra of certain classes of Room frames: the last cases, *Electron. J. Combin.* 17 (2010) Research Paper 74, 13 pages. <607, 610>

[895] J. D. Dixon and D. Panario, The degree of the splitting field of a random polynomial over a finite field, *Electron. J. Combin.* 11 (2004) Research Paper 70, 10 pp. <366, 367>

[896] V. Dmytrenko, F. Lazebnik, and J. Williford, On monomial graphs of girth eight, *Finite Fields Appl.* 13 (2007) 828–842. <222>

[897] H. Dobbertin, Almost perfect nonlinear power functions on GF(2^n): the Niho case, *Inform. and Comput.* 151 (1999) 57–72. <222, 254>

[898] H. Dobbertin, Almost perfect nonlinear power functions on GF(2^n): the Welch case, *IEEE Trans. Inform. Theory* 45 (1999) 1271–1275. <222, 254>

[899] H. Dobbertin, Kasami power functions, permutation polynomials and cyclic difference sets, In *Difference Sets, Sequences and Their Correlation Properties*, volume 542 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, 133–158, Kluwer Acad. Publ., Dordrecht, 1999. <232, 233, 594, 598>

[900] H. Dobbertin, Almost perfect nonlinear power functions on GF(2^n): a new case for n divisible by 5, In *Finite Fields and Applications*, 113–121, Springer, Berlin, 2001. <220, 222, 254>

[901] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, and P. Gaborit, Construction of bent functions via Niho power functions, *J. Combin. Theory, Ser. A* 113 (2006) 779–798. <261, 265>

[902] H. Dobbertin, D. Mills, E. N. Müller, A. Pott, and W. Willems, APN functions in odd characteristic, *Discrete Math.* 267 (2003) 95–112. <249, 254>

[903] C. Doche, Redundant trinomials for finite fields of characteristic 2, In *Australasian Conference on Information Security and Privacy – ACISP 2005*, volume 3574 of *Lecture Notes in Comput. Sci.*, 122–133, Springer, Berlin, 2005. <344, 346, 356>

[904] G. Dolinar, A. E. Guterman, B. Kuzma, and M. Orel, On the Polya permanent problem over finite fields, *European J. Combin.* 32 (2011) 116–132. <501, 502>

[905] S. Dolinar and D. Divsalar, Weight distribution of turbo codes using random and nonrandom permutations, TDA Progress Report 42-122, JPL, 1995. <717, 718>

[906] G. Dorfer and H. Maharaj, Generalized AG codes and generalized duality, *Finite Fields Appl.* 9 (2003) 194–210. <699, 703>

[907] G. Dorfer, W. Meidl, and A. Winterhof, Counting functions and expected values

for the lattice profile at n, *Finite Fields Appl.* 10 (2004) 636–652. <328, 329>

[908] G. Dorfer and A. Winterhof, Lattice structure and linear complexity profile of nonlinear pseudorandom number generators, *Appl. Algebra Engrg. Comm. Comput.* 13 (2003) 499–508. <328, 329>

[909] J. M. Dover, A family of non-Buekenhout unitals in the Hall planes, In *Mostly Finite Geometries*, volume 190 of *Lecture Notes in Pure and Appl. Math.*, 197–205, Dekker, New York, 1997. <563, 565>

[910] K. Drakakis, A review of Costas arrays, *J. Appl. Math.* (2006) Art. ID 26385, 32. <600, 610>

[911] K. Drakakis, R. Gow, and G. McGuire, APN permutations on $\mathbb{Z}_n$ and Costas arrays, *Discrete Appl. Math.* 157 (2009) 3320–3326. <222>

[912] K. Drakakis, F. Iorio, and S. Rickard, The enumeration of Costas arrays of order 28 and its consequences, *Adv. Math. Commun.* 5 (2011) 69–86. <600, 610>

[913] V. G. Drinfeld, Elliptic modules, *Mat. Sb. (New Ser.)* 94(136) (1974) 594–627, 656. <528, 530, 532, 537, 538>

[914] V. G. Drinfeld, Elliptic modules. II, *Mat. Sb. (New Ser.)* 102(144) (1977) 182–194, 325. <528, 530, 531, 538>

[915] M. Drmota and D. Panario, A rigorous proof of the Waterloo algorithm for the discrete logarithm problem, *Des. Codes Cryptogr.* 26 (2002) 229–241. <363, 367>

[916] M. Drmota and R. F. Tichy, *Sequences, Discrepancies and Applications*, volume 1651 of *Lecture Notes in Mathematics*, Springer-Verlag, Berlin, 1997. <29, 30, 168, 179>

[917] G. Drolet, A new representation of elements of finite fields $GF(2^m)$ yielding small complexity arithmetic circuits, *IEEE Trans. Comput.* 47 (1998) 938–946. <813>

[918] V. Dubois, P.-A. Fouque, A. Shamir, and J. Stern, Practical cryptanalysis of SFLASH, In *Advances in Cryptology—CRYPTO 2007*, volume 4622 of *Lecture Notes in Comput. Sci.*, 1–12, Springer, Berlin, 2007. <763, 764, 769, 770, 774>

[919] V. Dubois, P.-A. Fouque, and J. Stern, Cryptanalysis of SFLASH with slightly modified parameters, In *Advances in Cryptology—EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Comput. Sci.*, 264–275, Springer, Berlin, 2007. <763, 764, 769, 774>

[920] V. Dubois and N. Gama, The degree of regularity of HFE systems, In *Advances in Cryptology—ASIACRYPT 2010*, volume 6477 of *Lecture Notes in Comput. Sci.*, 557–576, Springer, Berlin, 2010. <773, 774>

[921] J. Dubrois and J.-G. Dumas, Efficient polynomial time algorithms computing industrial-strength primitive roots, *Inform. Process. Lett.* 97 (2006) 41–45. <341, 356>

[922] W. Duke, On multiple Salié sums, *Proc. Amer. Math. Soc.* 114 (1992) 623–625. <149, 155>

[923] J.-G. Dumas, Q-adic transform revisited, In *Proceedings of the 2008 International Symposium on Symbolic and Algebraic Computation*, 63–69, ACM, New York, 2008. <514, 515, 527>

[924] J.-G. Dumas, L. Fousse, and B. Salvy, Simultaneous modular reduction and Kronecker substitution for small finite fields, *J. Symbolic Comput.* 46 (2011) 823–840. <344, 356, 515, 527>

[925] J.-G. Dumas, T. Gautier, M. Giesbrecht, P. Giorgi, B. Hovinen, E. Kaltofen, B. D.

Saunders, W. J. Turner, and G. Villard, LinBox: A generic library for exact linear algebra, In A. M. Cohen, X.-S. Gao, and N. Takayama, editors, *ICMS'2002, Proceedings of the 2002 International Congress of Mathematical Software*, 40–50. World Scientific Pub., 2002. <513, 527>

[926] J.-G. Dumas, T. Gautier, and C. Pernet, Finite field linear algebra subroutines, In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, 63–74, ACM, New York, 2002. <515, 527>

[927] J.-G. Dumas, P. Giorgi, and C. Pernet, Dense linear algebra over word-size prime fields: the FFLAS and FFPACK packages, *ACM Trans. Math. Software* 35 (2008) Art. 19, 35. <343, 356, 516, 517, 527>

[928] J.-G. Dumas, C. Pernet, and Z. Wan, Efficient computation of the characteristic polynomial, In *ISSAC'05*, 140–147, ACM, New York, 2005. <522, 527>

[929] J.-G. Dumas and G. Villard, Computing the rank of sparse matrices over finite fields, In V. G. Ganzha, E. W. Mayr, and E. V. Vorozhtsov, editors, *CASC 2002, Proceedings of the Fifth International Workshop on Computer Algebra in Scientific Computing*, 47–62. Technische Universität München, Germany, 2002. <522, 523, 524, 525, 526, 527>

[930] I. I. Dumer, Concatenated codes and their multilevel generalizations, In *Handbook of Coding Theory, Vol. I, II*, 1911–1988, North-Holland, Amsterdam, 1998. <693, 694>

[931] A. Duran, B. Saunders, and Z. Wan, Hybrid algorithms for rank of sparse matrices, In R. Mathias and H. Woerdeman, editors, *SIAM Conference on Applied Linear Algebra*, 2003. <526, 527>

[932] I. Duursma and H.-S. Lee, Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$, In *Advances in Cryptology—ASIACRYPT 2003*, volume 2894 of *Lecture Notes in Comput. Sci.*, 111–123, Springer, Berlin, 2003. <46>

[933] I. Duursma and K.-H. Mak, On lower bounds for the Ihara constants A(2) and A(3), *arXiv:1102.4127v2[math.NT]* (2011). <456, 457, 462>

[934] P. F. Duvall and J. C. Mortick, Decimation of periodic sequences, *SIAM J. Appl. Math.* 21 (1971) 367–372. <306, 310>

[935] B. Dwork, On the rationality of the zeta function of an algebraic variety, *Amer. J. Math.* 82 (1960) 631–648. <157, 163, 472, 480>

[936] B. Dwork, p-adic cycles, *Inst. Hautes Études Sci. Publ. Math.* 37 (1969) 27–115. <472, 480>

[937] B. Dwork, Bessel functions as p-adic functions of the argument, *Duke Math. J.* 41 (1974) 711–738. <472, 480>

[938] B. M. Dwork, On the zeta function of a hypersurface III, *Ann. of Math., 2nd Ser.* 83 (1966) 457–519. <294, 295>

[939] W. Eberly, Black box Frobenius decompositions over small fields, In *Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation*, 106–113, ACM, New York, 2000. <522, 527>

[940] W. Eberly, Early termination over small fields, In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, ISSAC '03, 80–87, ACM, New York, NY, USA, 2003. <522, 527>

[941] W. Eberly, M. Giesbrecht, P. Giorgi, A. Storjohann, and G. Villard, Faster inversion and other black box matrix computations using efficient block projections, In *ISSAC 2007*, 143–150, ACM, New York, 2007. <527>

[942] W. Eberly and E. Kaltofen, On randomized Lanczos algorithms, In *Proceedings*

of the 1997 International Symposium on Symbolic and Algebraic Computation, 176–183, ACM, New York, 1997. <523, 524, 527>

[943] G. L. Ebert, Partitioning projective geometries into caps, *Canad. J. Math.* 37 (1985) 1163–1175. <560, 565>

[944] G. L. Ebert, Nests, covers, and translation planes, *Ars Combin.* 25 (1988) 213–233. <559, 565>

[945] G. L. Ebert, Spreads admitting regular elliptic covers, *European J. Combin.* 10 (1989) 319–330. <559, 565>

[946] G. L. Ebert, Partitioning problems and flag-transitive planes, *Rend. Circ. Mat. Palermo Ser. II Suppl.* (1998) 27–44, Combinatorics '98 (Mondello). <560, 565>

[947] G. L. Ebert, G. Marino, O. Polverino, and R. Trombetti, Infinite families of new semifields, *Combinatorica* 29 (2009) 637–663. <269, 270>

[948] Y. Edel, G. Kyureghyan, and A. Pott, A new APN function which is not equivalent to a power mapping, *IEEE Trans. Inform. Theory* 52 (2006) 744–747. <250, 254>

[949] Y. Edel and A. Pott, A new almost perfect nonlinear function which is not quadratic, *Adv. Math. Commun.* 3 (2009) 59–81. <249, 254>

[950] G. A. Edgar and C. Miller, Borel subrings of the reals, *Proc. Amer. Math. Soc.* 131 (2003) 1121–1129. <180, 186>

[951] H. M. Edwards, A normal form for elliptic curves, *Bull. Amer. Math. Soc. (New Ser.)* 44 (2007) 393–422 (electronic). <434, 440>

[952] G. Effinger, A Goldbach theorem for polynomials of low degree over odd finite fields, *Acta Arith.* 42 (1983) 329–365. <490, 492>

[953] G. Effinger, A Goldbach 3-primes theorem for polynomials of low degree over finite fields of characteristic 2, *J. Number Theory* 29 (1988) 345–363. <490, 492>

[954] G. Effinger, Toward a complete twin primes theorem for polynomials over finite fields, In *Finite Fields and Applications*, volume 461 of *Contemp. Math.*, 103–110, Amer. Math. Soc., Providence, 2008. <488, 492>

[955] G. Effinger and D. Hayes, A complete solution to the polynomial 3-primes problem, *Bull. Amer. Math. Soc.* 24 (1991) 363–369. <490, 492>

[956] G. Effinger and D. R. Hayes, *Additive Number Theory of Polynomials over a Finite Field*, Oxford Mathematical Monographs. Oxford University Press, New York, 1991. <29, 30, 489, 490, 491, 492>

[957] G. Effinger, K. Hicks, and G. L. Mullen, Twin irreducible polynomials over finite fields, In *Finite Fields with Applications to Coding Theory, Cryptography and Related Areas*, 94–111, Springer, Berlin, 2002. <488, 492>

[958] G. Effinger, K. Hicks, and G. L. Mullen, Integers and polynomials: comparing the close cousins $\mathbb{Z}$ and $\mathbb{F}_q[x]$, *Math. Intelligencer* 27 (2005) 26–34. <486, 492>

[959] M. Einsiedler and T. Ward, *Ergodic Theory with a View Towards Number Theory*, volume 259 of *Graduate Texts in Mathematics*, Springer-Verlag London Ltd., London, 2011. <330, 331, 337>

[960] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans. Inform. Theory* 31 (1985) 469–472. <736, 740>

[961] M. Elia and M. Leone, On the inherent space complexity of fast parallel multipliers for $GF(2^m)$, *IEEE Trans. Comput.* 51 (2002) 346–351. <811, 812, 813>

[962] S. Eliahou, M. Kervaire, and B. Saffari, On Golay polynomial pairs, *Adv. in Appl.*

Math. 12 (1991) 235–292. <833, 839>

[963] N. D. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$, *Invent. Math.* 89 (1987) 561–567. <431, 433>

[964] N. D. Elkies, Distribution of supersingular primes, *Astérisque* 198-200 (1991) 127–132. <431, 433>

[965] N. D. Elkies, Elliptic and modular curves over finite fields and related computational issues, In *Computational Perspectives on Number Theory*, volume 7 of *AMS/IP Stud. Adv. Math.*, 21–76, Amer. Math. Soc., Providence, RI, 1998. <778, 787>

[966] N. D. Elkies, Explicit modular towers, *Proceedings of the Thirty Fifth Allerton Conference on Communication, Control and Computing* (1998) 23–32. <457, 462>

[967] N. D. Elkies, Explicit towers of Drinfeld modular curves, In *European Congress of Mathematics, Vol. II*, volume 202 of *Progr. Math.*, 189–198, Birkhäuser, Basel, 2001. <457, 462>

[968] N. D. Elkies, E. W. Howe, A. Kresch, B. Poonen, J. L. Wetherell, and M. E. Zieve, Curves of every genus with many points. II. Asymptotically good families, *Duke Math. J.* 122 (2004) 399–422. <456>

[969] W. Ellison, Waring's problem, *Amer. Math. Monthly* 78 (1971) 10–36. <491, 492>

[970] B. Elspas, The theory of autonomous linear sequential networks, In *Linear Sequential Switching Circuits*, 21–61, Holden-Day, San Francisco, Calif., 1965. <824>

[971] H. Enderling, M. Chaplain, and P. Hahnfeldt, Quantitative modeling of tumor dynamics and radiotherapy, *Acta Biotheoretica* 58 (2010) 341–353, 10.1007/s10441-010-9111-z. <821, 824>

[972] A. Enge, Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time, *Math. Comp.* 71 (2002) 729–742. <448, 449>

[973] A. Enge, The complexity of class polynomial computation via floating point approximations, *Mathematics of Computation* 78 (2009) 1089–1107. <777, 787>

[974] A. Enge, Computing modular polynomials in quasi-linear time, *Mathematics of Computation* 78 (2009) 1809–1824. <778, 787>

[975] A. Enge and P. Gaudry, A general framework for subexponential discrete logarithm algorithms, *Acta Arith.* 102 (2002) 83–103. <448, 449, 799, 802>

[976] B.-G. Englert and Y. Aharonov, The mean king's problem: prime degrees of freedom, *Phys. Lett. A* 284 (2001) 1–5. <825, 831>

[977] S. S. Erdem, T. Yanık, and Ç. K. Koç, Polynomial basis multiplication over GF(2^m), *Acta Appl. Math.* 93 (2006) 33–55. <103>

[978] P. Erdős and P. Turán, On some problems of a statistical group-theory I, *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete* 4 (1965) 175–186 (1965). <366, 367>

[979] P. Erdős and P. Turán, On some problems of a statistical group-theory II, *Acta math. Acad. Sci. Hungar.* 18 (1967) 151–163. <366, 367>

[980] P. Erdős and P. Turán, On some problems of a statistical group-theory III, *Acta Math. Acad. Sci. Hungar.* 18 (1967) 309–320. <366, 367>

[981] P. Erdős and P. Turán, On some problems of a statistical group-theory IV, *Acta Math. Acad. Sci. Hungar* 19 (1968) 413–435. <366, 367>

[982] S. Erickson, M. J. Jacobson, Jr., N. Shang, S. Shen, and A. Stein, Explicit formulas for real hyperelliptic curves of genus 2 in affine representation, In *Arithmetic of*

Finite Fields, volume 4547 of *Lecture Notes in Comput. Sci.*, 202–218, Springer, Berlin, 2007. <445, 446, 449>

[983] S. Erickson, M. J. Jacobson, Jr., and A. Stein, Explicit formulas for real hyperelliptic curves of genus 2 in affine representation, *Adv. Math. Commun.* 5 (2011) 623–666. <445, 446, 449>

[984] eSTREAM Project, `http://www.ecrypt.eu.org/stream/`. <742, 744, 745, 754>

[985] eSTREAM Project, The eStream report: end of phase II, `http://www.ecrypt.eu.org/stream/PhaseIIreport.pdf`. <748, 754>

[986] O. Etesami and A. Shokrollahi, Raptor codes on binary memoryless symmetric channels, *IEEE Trans. Inform. Theory* 52 (2006) 2033–2051. <725>

[987] J. Ethier and G. L. Mullen, Strong forms of orthogonality for sets of frequency hypercubes, Preprint, 2011. <545, 547>

[988] J. Ethier and G. L. Mullen, Strong forms of orthogonality for sets of hypercubes, Discrete Math., to appear, 2012. <545, 547>

[989] ETSI, Digital video broadcasting (dvb); second generation framing structure, channel coding and modulation systems for broadcasting, interactive services, news gathering and other broadband satellite applications (dvb-s2): Etsi en 302 307, 2009. <704, 710>

[990] ETSI, Digital video broadcasting (dvb); implementation guidelines for a second generation digital terrestrial television broadcasting system (dvb-t2): Etsi ts 102 831, 2010. <704, 710>

[991] T. Etzion, A. Trachtenberg, and A. Vardy, Which codes have cycle-free Tanner graphs?, *IEEE Trans. Inform. Theory* 45 (1999) 2173–2181. <709, 710>

[992] A. B. Evans, Maximal sets of mutually orthogonal Latin squares. II, *European J. Combin.* 13 (1992) 345–350. <221, 222>

[993] A. B. Evans, *Orthomorphism Graphs of Groups*, volume 1535 of *Lecture Notes in Mathematics*, Springer-Verlag, Berlin, 1992. <165, 179, 221, 222>

[994] R. Evans, Residuacity of primes, *Rocky Mountain J. Math.* 19 (1989) 1069–1081. <135, 155>

[995] R. Evans, Character sums as orthogonal eigenfunctions of adjacency operators for Cayley graphs, In *Finite Fields: Theory, Applications, and Algorithms*, volume 168 of *Contemp. Math.*, 33–50, Amer. Math. Soc., Providence, RI, 1994. <149, 155>

[996] R. Evans, Congruences for Jacobi sums, *J. Number Theory* 71 (1998) 109–120. <141, 155>

[997] R. Evans, Gauss sums and Kloosterman sums over residue rings of algebraic integers, *Trans. Amer. Math. Soc.* 353 (2001) 4429–4445. <154, 155>

[998] R. Evans, Gauss sums of orders six and twelve, *Canad. Math. Bull.* 44 (2001) 22–26. <144, 145, 155>

[999] R. Evans, Twisted hyper-Kloosterman sums over finite rings of integers, In *Number Theory for the Millennium I*, 429–448, A. K. Peters, Natick, MA, 2002. <150, 154, 155>

[1000] R. Evans, Hypergeometric ${}_3F_2(1/4)$ evaluations over finite fields and Hecke eigenforms, *Proc. Amer. Math. Soc.* 138 (2010) 517–531. <152, 153, 155>

[1001] R. Evans, Seventh power moments of Kloosterman sums, *Israel J. Math.* 175 (2010) 349–362. <152, 155>

[1002] R. Evans and J. Greene, Clausen's theorem and hypergeometric functions over finite

fields, *Finite Fields Appl.* 15 (2009) 97–109. <140, 155>

[1003] R. Evans and J. Greene, Evaluations of hypergeometric functions over finite fields, *Hiroshima Math. J.* 39 (2009) 217–235. <140, 155>

[1004] R. Evans, H. D. L. Hollmann, C. Krattenthaler, and Q. Xiang, Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets, *J. Combin. Theory, Ser. A* 87 (1999) 74–119. <146, 155>

[1005] R. J. Evans, Identities for products of Gauss sums over finite fields, *Enseign. Math., IIe Ser.* 27 (1981) 197–209 (1982). <140, 155>

[1006] R. J. Evans, Pure Gauss sums over finite fields, *Mathematika* 28 (1981) 239–248 (1982). <139, 155>

[1007] R. J. Evans, Period polynomials for generalized cyclotomic periods, *Manuscripta Math.* 40 (1982) 217–243. <154, 155>

[1008] R. J. Evans, Character sum analogues of constant term identities for root systems, *Israel J. Math.* 46 (1983) 189–196. <140, 155>

[1009] R. J. Evans, The evaluation of Selberg character sums, *Enseign. Math., IIe Ser.* 37 (1991) 235–248. <140, 155>

[1010] R. J. Evans, Selberg-Jack character sums of dimension 2, *J. Number Theory* 54 (1995) 1–11. <140, 155>

[1011] R. J. Evans, J. Greene, and H. Niederreiter, Linearized polynomials and permutation polynomials of finite fields, *Michigan Math. J.* 39 (1992) 405–413. <221, 222>

[1012] S. Evdokimov, Factorization of polynomials over finite fields in subexponential time under GRH, In *Algorithmic Number Theory, First International Symposium, ANTS-I*, number 877 in Lecture Notes in Computer Science, 209–219, 1994. <374, 375>

[1013] S. A. Evdokimov, Efficient factorization of polynomials over finite fields and the generalized Riemann hypothesis, Translation of Zapiski Nauchnyck Seminarov Leningradskgo Otdeleniya Mat. Inst. V.A. Steklova Akad. Nauk SSSR (LOMI), volume 176, 1989, 104–117. <372, 373>

[1014] S. A. Evdokimov, Faktorizatsiya razreshimogo mnogochlena nad konechnym polem i Obobshchennaya Gipoteza Rimana, *Zapiski Nauchnyck Seminarov Leningradskgo Otdeleniya Mat. Inst. V.A. Steklova Akad. Nauk SSSR (LOMI)* 176 (1989) 104–117, With English abstract, S. A. Evdokimov, Factoring a solvable polynomial over a finite field and the Generalized Riemann Hypothesis. <374, 375>

[1015] G. Everest and T. Ward, *Heights of Polynomials and Entropy in Algebraic Dynamics*, Universitext. Springer-Verlag London Ltd., London, 1999. <330, 331, 337>

[1016] J.-H. Evertse, Linear equations with unknowns from a multiplicative group whose solutions lie in a small number of subspaces, *Indag. Math. (New Ser.)* 15 (2004) 347–355. <295>

[1017] C. Faber and G. van der Geer, Complete subvarieties of moduli spaces and the Prym map, *J. Reine Angew. Math.* 573 (2004) 117–137. <479, 480>

[1018] C. C. Faith, Extensions of normal bases and completely basic fields, *Trans. Amer. Math. Soc.* 85 (1957) 406–427. <123, 124, 132>

[1019] G. Faltings, Finiteness theorems for abelian varieties over number fields, In *Arithmetic Geometry*, 9–27, Springer, New York, 1986. <426, 433>

[1020] H. Fan and Y. Dai, Fast bit-parallel $GF(2^n)$ multiplier for all trinomials, *IEEE Trans. Comput.* 54 (2005) 485–490. <813>

[1021] H. Fan and M. A. Hasan, A new approach to subquadratic space complexity parallel multipliers for extended binary fields, *IEEE Trans. Comput.* 56 (2007) 224–233. <804, 807, 808, 813>

[1022] H. Fan and M. A. Hasan, Subquadratic computational complexity schemes for extended binary field multiplication using optimal normal bases, *IEEE Trans. Comput.* 56 (2007) 1435–1437. <810, 812, 813>

[1023] H. Fan, J. Sun, M. Gu, and K. Lam, Overlap-free Karatsuba-Ofman polynomial multiplication algorithms, *IET Information Security* 4 (2010) 8–14. <804, 805, 813>

[1024] S. Fan, Primitive normal polynomials with the last half coefficients prescribed, *Finite Fields Appl.* 15 (2009) 604–614. <89, 90, 110>

[1025] S. Fan and W. Han, Character sums over Galois rings and primitive polynomials over finite fields, *Finite Fields Appl.* 10 (2004) 36–52. <87, 88, 90>

[1026] S. Fan and W. Han, p-adic formal series and Cohen's problem, *Glasgow Math. J.* 46 (2004) 47–61. <86, 87, 90>

[1027] S. Fan and W. Han, p-adic formal series and primitive polynomials over finite fields, *Proc. Amer. Math. Soc.* 132 (2004) 15–31. <87, 88, 90>

[1028] S. Fan and W. Han, Primitive polynomial with three coefficients prescribed, *Finite Fields Appl.* 10 (2004) 506–521. <88, 90>

[1029] S. Fan, W. Han, and K. Feng, Primitive normal polynomials with multiple coefficients prescribed: an asymptotic result, *Finite Fields Appl.* 13 (2007) 1029–1044. <86, 89, 90, 110>

[1030] S. Fan, W. Han, K. Feng, and X. Zhang, Primitive normal polynomials with the first two coefficients prescribed: a revised p-adic method, *Finite Fields Appl.* 13 (2007) 577–604. <89, 90, 110>

[1031] S. Fan and X. Wang, Primitive normal polynomials with a prescribed coefficient, *Finite Fields Appl.* 15 (2009) 682–730. <89, 90, 110>

[1032] S. Fan and X. Wang, Primitive normal polynomials with the specified last two coefficients, *Discrete Math.* 309 (2009) 4502–4513. <87, 89, 90>

[1033] X. Fan, T. Wollinger, and Y. Wang, Effcient doubling on genus 3 curves over binary fields, In *Topics in Cryptology CT-RSA 2006*, volume 3860 of *Lecture Notes in Comput. Sci.*, 64–81, Springer, Berlin, 2006. <788, 794>

[1034] R. R. Farashahi, Hashing into Hessian curves, In *Progress in Cryptology—AFRICACRYPT 2011*, volume 6737 of *Lecture Notes in Comput. Sci.*, 278–289, Springer, Berlin, 2011. <787>

[1035] J.-C. Faugére, A new efficient algorithm for computing Gröbner bases (F_4), *J. Pure Appl. Algebra* 139 (1999) 61–88. <772, 774>

[1036] J.-C. Faugère, A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5), In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, 75–83, ACM, New York, 2002. <772, 774>

[1037] J.-C. Faugère and A. Joux, Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases, In *Advances in Cryptology—CRYPTO 2003*, volume 2729 of *Lecture Notes in Comput. Sci.*, 44–60, Springer, Berlin, 2003. <761, 770, 772, 774>

[1038] J.-C. Faugère and S. Lachartre, Parallel Gaussian elimination for Gröbner bases computations in finite fields, In M. M. Maza and J.-L. Roch, editors, *PASCO 2010, Proceedings of the Fourth International Workshop on Parallel Symbolic*

Computation, 89–97, ACM, New York, 2010. <526, 527>

[1039] J.-C. Faugère and L. Perret, Polynomial equivalence problems: algorithmic and theoretical aspects, In *Advances in Cryptology—EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Comput. Sci.*, 30–47, Springer, Berlin, 2006. <758, 774>

[1040] H. Faure, Discrépance de suites associées à un système de numération (en dimension s), *Acta Arith.* 41 (1982) 337–351. <619, 621>

[1041] K. Fazel and S. Kaiser, *Multi-Carrier and Spread Spectrum Systems from OFDM and MC-CDMA to LTE and WiMAX*, John Wiley & Sons, Ltd, West Sussex, second edition, 2008. <704, 710>

[1042] S. Feisel, J. von zur Gathen, and M. A. Shokrollahi, Normal bases via general Gauss periods, *Math. Comp.* 68 (1999) 271–290. <120, 122>

[1043] H. Feistel, W. Notz, and J. Smith, Some cryptographic techniques for machine-to-machine data communications, *Proceedings of the IEEE* 63 (1975) 1545–1554. <733, 740>

[1044] H. Fell and W. Diffie, Analysis of a public key approach based on polynomial substitution, In *Advances in Cryptology—CRYPTO '85*, volume 218 of *Lecture Notes in Comput. Sci.*, 340–349, Springer, Berlin, 1986. <755, 758, 759, 774>

[1045] G. Fellegara, Gli ovaloidi in uno spazio tridimensionale di Galois di ordine 8, *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat.* 32 (1962) 170–176. <580>

[1046] B. Felszeghy, On the solvability of some special equations over finite fields, *Publ. Math. Debrecen* 68 (2006) 15–23. <204, 207>

[1047] G. Feng, A VLSI architecture for fast inversion in $GF(2^m)$, *IEEE Trans. Comput.* 38 (1989) 1383–1386. <809, 813>

[1048] G. L. Feng and K. K. Tzeng, A generalization of the Berlekamp-Massey algorithm for multisequence shift-register synthesis with applications to decoding cyclic codes, *IEEE Trans. Inform. Theory* 37 (1991) 1274–1287. <322, 329>

[1049] K. Feng, Quantum error-correcting codes, In *Coding Theory and Cryptology*, volume 1 of *Lect. Notes Ser. Inst. Math. Sci. Natl. Univ. Singap.*, 91–142, World Sci. Publ., River Edge, NJ, 2002. <829, 831>

[1050] K. Feng and J. Luo, Value distributions of exponential sums from perfect nonlinear functions and their applications, *IEEE Trans. Inform. Theory* 53 (2007) 3035–3041. <264, 265>

[1051] K. Feng and J. Luo, Weight distribution of some reducible cyclic codes, *Finite Fields Appl.* 14 (2008) 390–409. <199, 200>

[1052] K. Feng, H. Niederreiter, and C. Xing, editors, *Coding, Cryptography and Combinatorics*, volume 23 of *Progress in Computer Science and Applied Logic*, Birkhäuser Verlag, Basel, 2004. <30>

[1053] T. Feng, B. Wen, Q. Xiang, and J. Yin, Partial difference sets from quadratic forms and p-ary weakly regular bent functions, arXiv:1002.2797v2, 2011. <258, 265>

[1054] X. Feng and Z. Dai, Expected value of the linear complexity of two-dimensional binary sequences, In *Sequences and Their Applications—SETA 2004*, volume 3486 of *Lecture Notes in Comput. Sci.*, 113–128, Springer, Berlin, 2005. <323, 329>

[1055] S. T. J. Fenn, M. Benaissa, and D. Taylor, $GF(2^m)$ multiplication and division over the dual basis, *IEEE Trans. Comput.* 45 (1996) 319–327. <813>

[1056] F. Fiedler, K. H. Leung, and Q. Xiang, On Mathon's construction of maximal arcs in Desarguesian planes, *Adv. Geom.* (2003) S119–S139. <564, 565>

[1057] J. P. Fillmore and M. L. Marx, Linear recursive sequences, *SIAM Rev.* 10 (1968) 342–353. <305, 310>

[1058] N. J. Fine and I. N. Herstein, The probability that a matrix be nilpotent, *Illinois J. Math.* 2 (1958) 499–504. <494, 502>

[1059] FIPS 180-3, Secure hash standard (SHS), Federal Information Processing Standards Publication 180-3, National Institute of Standards and Technology, 2008. <735, 740>

[1060] FIPS 186-2, Digital signature standard, Federal Information Processing Standards Publication 186-2, 2000, available at `http://csrc.nist.gov`. <345, 356>

[1061] FIPS 186-3, Digital signature standard (DSS), Federal Information Processing Standards Publication 186-3, National Institute of Standards and Technology, 2009. <736, 740>

[1062] FIPS 46-3, Data encryption standard (DES), Federal Information Processing Standards Publication 46-3, National Institute of Standards and Technology, 1999. <734, 740>

[1063] S. Fischer and W. Meier, Algebraic immunity of s-boxes and augmented functions, In *Proceedings of Fast Software Encryption 2007*, volume 4593 of *Lecture Notes in Comput. Sci.*, 366–381, 2007. <241, 245>

[1064] S. D. Fisher, Classroom notes: matrices over a finite field, *Amer. Math. Monthly* 73 (1966) 639–641. <493, 502>

[1065] R. W. Fitzgerald, A characterization of primitive polynomials over finite fields, *Finite Fields Appl.* 9 (2003) 117–121. <83, 85>

[1066] R. W. Fitzgerald, Highly degenerate quadratic forms over finite fields of characteristic 2, *Finite Fields Appl.* 11 (2005) 165–181. <199, 200>

[1067] R. W. Fitzgerald, Highly degenerate quadratic forms over $\mathbb{F}_2$, *Finite Fields Appl.* 13 (2007) 778–792. <198, 200>

[1068] R. W. Fitzgerald, Invariants of trace forms over finite fields of characteristic 2, *Finite Fields Appl.* 15 (2009) 261–275. <199, 200>

[1069] R. W. Fitzgerald, Trace forms over finite fields of characteristic 2 with prescribed invariants, *Finite Fields Appl.* 15 (2009) 69–81. <198, 199, 200>

[1070] R. W. Fitzgerald and J. L. Yucas, Irreducible polynomials over GF(2) with three prescribed coefficients, *Finite Fields Appl.* 9 (2003) 286–299. <52, 55, 75>

[1071] R. W. Fitzgerald and J. L. Yucas, Pencils of quadratic forms over finite fields, *Discrete Math.* 283 (2004) 71–79. <200>

[1072] R. W. Fitzgerald and J. L. Yucas, Sums of Gauss sums and weights of irreducible codes, *Finite Fields Appl.* 11 (2005) 89–110. <135, 155>

[1073] R. W. Fitzgerald and J. L. Yucas, Generalized reciprocals, factors of Dickson polynomials and generalized cyclotomic polynomials over finite fields, *Finite Fields Appl.* 13 (2007) 492–515. <277, 278, 279, 282>

[1074] P. Flajolet, X. Gourdon, and D. Panario, The complete analysis of a polynomial factorization algorithm over finite fields, *J. Algorithms* 40 (2001) 37–81. <358, 361, 362, 366, 367, 374, 375>

[1075] P. Flajolet and A. Odlyzko, Singularity analysis of generating functions, *SIAM J. Discrete Math.* 3 (1990) 216–240. <359, 367>

[1076] P. Flajolet and A. M. Odlyzko, Random mapping statistics, In *EUROCRYPT*, 329–354, 1989. <744, 754>

[1077] P. Flajolet and R. Sedgewick, *Analytic Combinatorics*, Cambridge University Press,

Cambridge, 2009. <358, 360, 367>

[1078] P. Flajolet and M. Soria, Gaussian limiting distributions for the number of components in combinatorial structures, *J. Combin. Theory, Ser. A* 53 (1990) 165–182. <360, 366, 367>

[1079] P. Flajolet and M. Soria, General combinatorial schemas: Gaussian limit distributions and exponential tails, *Discrete Math.* 114 (1993) 159–180. <360, 366, 367>

[1080] J. J. Flynn, *Near-Exceptionality over Finite Fields*, PhD dissertation, University of California, Berkeley, Department of Mathematics, 2001. <226, 229>

[1081] S. Fomin and A. Zelevinsky, The Laurent phenomenon, *Adv. in Appl. Math.* 28 (2002) 119–144. <330, 337>

[1082] K. Fong, D. Hankerson, J. López, and A. Menezes, Field inversion and point halving revisited, *IEEE Trans. Comput.* 53 (2003) 1047–1059. <356>

[1083] F. Fontein, Groups from cyclic infrastructures and Pohlig-Hellman in certain infrastructures, *Adv. Math. Commun.* 2 (2008) 293–307. <449>

[1084] G. D. Forney, Jr., On decoding BCH codes, *IEEE Trans. Information Theory* IT-11 (1965) 549–557. <685, 693, 694>

[1085] G. D. Forney, Jr., *Concatenated Codes*, M.I.T. Press, Cambridge, MA, 1966. <711, 718>

[1086] G. D. Forney, Jr., Generalized minimum distance decoding, *IEEE Trans. Information Theory* IT-12 (1966) 125–131. <688, 693, 694>

[1087] G. D. Forney, Jr., N. J. A. Sloane, and M. D. Trott, The Nordstrom-Robinson code is the binary image of the octacode, In *Coding and Quantization*, volume 14 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, 19–26, Amer. Math. Soc., Providence, RI, 1993. <692, 694>

[1088] P.-A. Fouque, L. Granboulan, and J. Stern, Differential cryptanalysis for multivariate schemes, In *Advances in Cryptology—EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Comput. Sci.*, 341–353, Springer, Berlin, 2005. <764, 768, 769, 774>

[1089] P.-A. Fouque, G. Macario-Rat, L. Perret, and J. Stern, Total break of the l-IC signature scheme, In *Public Key Cryptography—PKC 2008*, volume 4939 of *Lecture Notes in Comput. Sci.*, 1–17, Springer, Berlin, 2008. <764, 774>

[1090] H. M. Fredricksen, A. W. Hales, and M. M. Sweet, A generalization of Swan's theorem, *Math. Comp.* 46 (1986) 321–331. <64, 66>

[1091] D. Freeman, P. Stevenhagen, and M. Streng, Abelian varieties with prescribed embedding degree, In *Algorithmic Number Theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, 60–73, Springer, Berlin, 2008. <802>

[1092] D. M. Freeman, Converting pairing-based cryptosystems from composite-order groups to prime-order groups, In *Advances in Cryptology—EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, 44–61, Springer-Verlag, Berlin, 2010. <779, 783, 787>

[1093] J. W. Freeman, Reguli and pseudoreguli in PG(3, s^2), *Geom. Dedicata* 9 (1980) 267–280. <562, 565>

[1094] T. S. Freeman, G. Imirzian, E. Kaltofen, and Lakshman Yagati, DAGWOOD: A system for manipulating polynomials given by straight-line programs, *ACM Trans. Math. Software* 14 (1988) 218–240. <384, 385>

[1095] D. Freemann, M. Scott, and E. Teske, A taxonomy of pairing-friendly elliptic curves, *Journal of Cryptology* 23 (2010) 224–280. <784, 785, 787>

[1096] Free Software Foundation, GNU Multiple Precision library, version 5.0.4, 2012, available at `http://gmplib.org/`. <339, 348, 356>

[1097] G. Frei, The unpublished section eight: on the way to function fields over a finite field, In *The Shaping of Arithmetic After C. F. Gauss's Disquisitiones Arithmeticae*, 159–198, Berlin: Springer, 2007. <5>

[1098] G. Frey, Applications of arithmetical geometry to cryptographic constructions, In D. Jungnickel and H. Niederreiter, editors, *Finite Fields and Applications*, 128–161, Springer-Verlag, Berlin, 2001. <777, 787, 800, 802>

[1099] G. Frey and T. Lange, Varieties over special fields, In *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Discrete Math. Appl., 87–113, Chapman & Hall/CRC, Boca Raton, FL, 2006. <29, 30, 449>

[1100] G. Frey, M. Müller, and H.-G. Rück, The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems, *IEEE Trans. Inform. Theory* 45 (1999) 1717–1719. <449>

[1101] G. Frey, M. Perret, and H. Stichtenoth, On the different of abelian extensions of global fields, In *Coding Theory and Algebraic Geometry*, volume 1518 of *Lecture Notes in Math.*, 26–32, Springer, Berlin, 1992. <461, 462>

[1102] G. Frey and H.-G. Rück, A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves, *Math. Comp.* 62 (1994) 865–874. <784, 787, 801, 802>

[1103] M. Fried, On a conjecture of Schur, *Michigan Math. J.* 17 (1970) 41–55. <220, 222, 231, 232, 233, 276, 282, 286, 287, 295>

[1104] M. Fried, The field of definition of function fields and a problem in the reducibility of polynomials in two variables, *Illinois J. Math.* 17 (1973) 128–146. <293, 295>

[1105] M. Fried, On a theorem of Ritt and related Diophantine problems, *J. Reine Angew. Math.* 264 (1973) 40–55. <288, 295>

[1106] M. Fried, On a theorem of MacCluer, *Acta Arith.* 25 (1973/74) 121–126. <285, 295>

[1107] M. Fried, On Hilbert's irreducibility theorem, *J. Number Theory* 6 (1974) 211–231. <287, 289, 292, 295>

[1108] M. Fried, Fields of definition of function fields and Hurwitz families—groups as Galois groups, *Comm. Algebra* 5 (1977) 17–82. <284, 295>

[1109] M. Fried, Galois groups and complex multiplication, *Trans. Amer. Math. Soc.* 235 (1978) 141–163. <232, 233, 291, 292, 295>

[1110] M. Fried and R. Lidl, On Dickson polynomials and Rédei functions, In *Contributions to General Algebra, 5*, 139–149, Hölder-Pichler-Tempsky, Vienna, 1987. <276, 282>

[1111] M. Fried and G. Sacerdote, Solving Diophantine problems over all residue class fields of a number field and all finite fields, *Ann. of Math., 2nd Ser.* 104 (1976) 203–233. <294, 295>

[1112] M. D. Fried, The place of exceptional covers among all Diophantine relations, *Finite Fields Appl.* 11 (2005) 367–433. <284, 285, 286, 287, 288, 289, 290, 292, 293, 294, 295>

[1113] M. D. Fried, Variables separated equations: Strikingly different roles for the branch cycle lemma and the finite simple group classification, *Science China Mathematics* 55 (2012) 1–69. <285, 290, 293, 294, 295>

[1114] M. D. Fried, R. Guralnick, and J. Saxl, Schur covers and Carlitz's conjecture, *Israel*

J. Math. 82 (1993) 157–225. <211, 222, 230, 233, 287, 294, 295>

[1115] M. D. Fried and M. Jarden, *Field Arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*, Springer-Verlag, Berlin, 1986. <29, 30, 287, 292, 294, 295>

[1116] M. D. Fried and M. Jarden, *Field Arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas, 3rd Series. A Series of Modern Surveys in Mathematics]*, Springer-Verlag, Berlin, third edition, 2008, Revised by Jarden. <29, 30, 231, 233>

[1117] M. D. Fried and R. E. MacRae, On curves with separated variables, *Math. Ann.* 180 (1969) 220–226. <292, 295>

[1118] M. D. Fried and R. E. MacRae, On the invariance of chains of fields, *Illinois J. Math.* 13 (1969) 165–171. <286, 295>

[1119] E. Friedman and L. C. Washington, On the distribution of divisor class groups of curves over a finite field, In *Théorie des Nombres*, 227–239, de Gruyter, Berlin, 1989. <443, 449>

[1120] J. Friedman, Some geometric aspects of graphs and their eigenfunctions, *Duke Math. J.* 69 (1993) 487–525. <637, 638, 647, 649>

[1121] J. Friedman, A Proof of Alon's Second Eigenvalue Conjecture and Related Problems, *Mem. Amer. Math. Soc.* 195 (2008). <648, 649>

[1122] J. Friedman, R. Murty, and J.-P. Tillich, Spectral estimates for abelian Cayley graphs, *J. Combin. Theory, Ser. B* 96 (2006) 111–121. <642, 649>

[1123] C. Friesen, A special case of Cohen-Lenstra heuristics in function fields, In *Number Theory*, volume 19 of *CRM Proc. Lecture Notes*, 99–105, Amer. Math. Soc., Providence, RI, 1999. <443, 449>

[1124] C. Friesen, Class group frequencies of real quadratic function fields: the degree 4 case, *Math. Comp.* 69 (2000) 1213–1228. <443, 449>

[1125] C. Friesen, Bounds for frequencies of class groups of real quadratic genus 1 function fields, *Acta Arith.* 96 (2001) 313–331. <443, 449>

[1126] S. Frisch, When are weak permutation polynomials strong?, *Finite Fields Appl.* 1 (1995) 437–439. <225>

[1127] D. Fu and J. Solinas, IKE and IKEv2 authentication using the elliptic curve digital signature algorithm (ECDSA), RFC 4754, Internet Engineering Task Force, 2007, `http://www.ietf.org/rfc/rfc4754.txt`. <776, 787>

[1128] F.-W. Fu, H. Niederreiter, and F. Özbudak, On the joint linear complexity of linear recurring multisequences, In *Coding and Cryptology*, volume 4 of *Ser. Coding Theory Cryptol.*, 125–142, World Sci. Publ., Hackensack, NJ, 2008. <318, 324, 329>

[1129] F.-W. Fu, H. Niederreiter, and F. Özbudak, Joint linear complexity of arbitrary multisequences consisting of linear recurring sequences, *Finite Fields Appl.* 15 (2009) 475–496. <321, 324, 329>

[1130] F.-W. Fu, H. Niederreiter, and F. Özbudak, Joint linear complexity of multisequences consisting of linear recurring sequences, *Cryptogr. Commun.* 1 (2009) 3–29. <324, 329>

[1131] F.-W. Fu, H. Niederreiter, and M. Su, The expectation and variance of the joint linear complexity of random periodic multisequences, *J. Complexity* 21 (2005) 804–822. <324, 329>

[1132] L. Fu, Weights of twisted exponential sums, *Math. Z.* 262 (2009) 449–472. <162,

163>

[1133] L. Fu and C. Liu, Equidistribution of Gauss sums and Kloosterman sums, *Math. Z.* 249 (2005) 269–281. <134, 155>

[1134] L. Fu and D. Wan, Moment L-functions, partial L-functions and partial exponential sums, *Math. Ann.* 328 (2004) 193–228. <163, 192, 195>

[1135] L. Fu and D. Wan, Mirror congruence for rational points on Calabi-Yau varieties, *Asian J. Math.* 10 (2006) 1–10. <194, 195>

[1136] C. A. Fuchs, On the quantumness of a Hilbert space, *Quantum Inf. Comput.* 4 (2004) 467–478. <826, 831>

[1137] C. A. Fuchs and M. Sasaki, Squeezing quantum information through a classical channel: measuring the "quantumness" of a set of quantum states, *Quantum Inf. Comput.* 3 (2003) 377–404. <826, 831>

[1138] R. Fuhrmann, A. Garcia, and F. Torres, On maximal curves, *J. Number Theory* 67 (1997) 29–51. <454, 456>

[1139] R. Fuhrmann and F. Torres, The genus of curves over finite fields with many rational points, *Manuscripta Math.* 89 (1996) 103–106. <454, 456>

[1140] R. Fuji-Hara, K. Momihara, and M. Yamada, Perfect difference systems of sets and Jacobi sums, *Discrete Math.* 309 (2009) 3954–3961. <137, 155>

[1141] W. Fulton, *Algebraic Curves*, Advanced Book Classics. Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989. <399, 414, 415>

[1142] M. Fürer, Fast integer multiplication, In *Proceedings of the Thirty-ninth Annual ACM Symposium on Theory of Computing,* San Diego, California, USA, 57–66. ACM, 2007, Preprint available at `http://www.cse.psu.edu/~furer/Papers/mult.pdf`. <373, 375>

[1143] È. M. Gabidulin, Theory of codes with maximum rank distance, *Problemy Peredachi Informatsii* 21 (1985) 3–16. <836, 839>

[1144] A. Gács, A remark on blocking sets of almost Rédei type, *J. Geom.* 60 (1997) 65–73. <551, 555>

[1145] A. Gács, On a generalization of Rédei's theorem, *Combinatorica* 23 (2003) 585–598. <551, 555>

[1146] A. Gács, L. Lovász, and T. Szőnyi, Directions in $\mathrm{AG}(2, p^2)$, *Innov. Incidence Geom.* 6/7 (2007/08) 189–201. <551, 555>

[1147] A. Gács, P. Sziklai, and T. Szőnyi, Two remarks on blocking sets and nuclei in planes of prime order, *Des. Codes Cryptogr.* 10 (1997) 29–39. <551, 555>

[1148] S. D. Galbraith, Supersingular curves in cryptography, In *Advances in Cryptology—ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Comput. Sci.*, 495–513, Springer, Berlin, 2001. <448, 449>

[1149] S. D. Galbraith, M. Harrison, and D. J. Mireles Morales, Efficient hyperelliptic arithmetic using balanced representation for divisors, In *Algorithmic Number Theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, 342–356, Springer, Berlin, 2008. <444, 445, 449>

[1150] S. D. Galbraith, F. Hess, and N. P. Smart, Extending the GHS Weil descent attack, In L. Knudsen, editor, *Advances in Cryptology—EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, 29–44, Springer-Verlag, Berlin, 2002. <777, 787>

[1151] S. D. Galbraith, F. Hess, and F. Vercauteren, Hyperelliptic pairings, In *Pairing-Based Cryptography—Pairing 2007*, volume 4575 of *Lecture Notes in Comput. Sci.*, 108–131, Springer, Berlin, 2007. <794>

[1152] S. D. Galbraith, J. F. McKee, and P. C. Valença, Ordinary abelian varieties having small embedding degree, *Finite Fields Appl.* 13 (2007) 800–814. <802>

[1153] S. D. Galbraith and K. G. Paterson, editors, *Pairing-Based Cryptography — Pairing 2008*, volume 5209 of *Lecture Notes in Compu. Sci.*, Springer-Verlag, Berlin, 2008. <779, 787>

[1154] S. D. Galbraith and N. P. Smart, A cryptographic application of Weil descent, In M. Walker, editor, *Cryptography and Coding*, volume 1746 of *Lecture Notes in Comput. Sci.*, 191–200, Springer-Verlag, Berlin, 1999. <777, 787>

[1155] Z. Galil, R. Kannan, and E. Szemerédi, On nontrivial separators for k-page graphs and simulations by nondeterministic one-tape Turing machines, *J. Comput. System Sci.* 38 (1989) 134–149. <178, 179>

[1156] R. G. Gallager, Low-density parity-check codes, *IRE Trans.* IT-8 (1962) 21–28. <704, 710>

[1157] R. G. Gallager, *Low-Density Parity-Check Codes*, MIT Press, Cambridge, MA, 1963. <704, 705, 710>

[1158] R. G. Gallager, A simple derivation of the coding theorem and some applications, *IEEE Trans. Information Theory* IT-11 (1965) 3–18. <651, 652, 694>

[1159] R. Gallant, R. Lambert, and S. Vanstone, Improving the parallelized Pollard lambda search on binary anomalous curves, *Mathematics of Computation* 69 (2000) 1699–1705. <776, 787>

[1160] L. H. Gallardo and O. Rahavandrainy, Unitary perfect polynomials over $\mathbb{F}_4$ with less than five prime factors, *Funct. Approx. Comment. Math.* 45 (2011) 67–78. <492>

[1161] L. H. Gallardo and L. N. Vaserstein, The strict Waring problem for polynomial rings, *J. Number Theory* 128 (2008) 2963–2972. <491, 492>

[1162] É. Galois, Sur la théorie des nombres, *Bulletin des Sciences Mathématiques XIII* (1830) 428–435, Reprinted in Écrits et Mémoires Matheématiques d'Évariste Galois, 112-128. <3, 5, 10, 369, 373>

[1163] R. A. Games and A. H. Chan, A fast algorithm for determining the complexity of a binary sequence with period 2^n, *IEEE Trans. Inform. Theory* 29 (1983) 144–146. <322, 329>

[1164] M. J. Ganley, Central weak nucleus semifields, *European J. Combin.* 2 (1981) 339–347. <269, 270, 274>

[1165] F. R. Gantmacher, *The Theory of Matrices. Vol. 1*, AMS Chelsea Publishing, Providence, RI, 1998. <521, 527>

[1166] S. Gao, *Normal Bases over Finite Fields*, PhD thesis, University of Waterloo, Canada, 1993. <56, 59, 60, 61, 96, 103, 106, 110, 113, 122>

[1167] S. Gao, Elements of provable high orders in finite fields, *Proc. Amer. Math. Soc.* 127 (1999) 1615–1623. <93, 94, 334>

[1168] S. Gao, Abelian groups, Gauss periods, and normal bases, *Finite Fields Appl.* 7 (2001) 149–164. <119, 120, 121, 122>

[1169] S. Gao, Absolute irreducibility of polynomials via Newton polytopes, *J. Algebra* 237 (2001) 501–520. <381, 385>

[1170] S. Gao, On the deterministic complexity of factoring polynomials, *Journal of Symbolic Computation* 31 (2001) 19–36. <374, 375>

[1171] S. Gao, Factoring multivariate polynomials via partial differential equations, *Math. Comp.* 72 (2003) 801–822. <379, 380, 385>

[1172] S. Gao and J. von zur Gathen, Berlekamp's and Niederreiter's polynomial factorization algorithms, In *Finite fields: theory, applications, and algorithms*, volume 168 of *Contemp. Math.*, 101–116, Amer. Math. Soc., Providence, RI, 1994. <374, 375>

[1173] S. Gao, J. von zur Gathen, and D. Panario, Gauss periods: orders and cryptographical applications, *Math. Comp.* 67 (1998) 343–352, With microfiche supplement. <119, 122>

[1174] S. Gao, J. von zur Gathen, D. Panario, and V. Shoup, Algorithms for exponentiation in finite fields, *J. Symbolic Comput.* 29 (2000) 879–889. <114, 118, 119, 122, 350, 356, 812, 813>

[1175] S. Gao, J. Howell, and D. Panario, Irreducible polynomials of given forms, In *Finite Fields: Theory, Applications, and Algorithms*, volume 225 of *Contemp. Math.*, 43–54, Amer. Math. Soc., Providence, RI, 1999. <84, 85, 341, 356>

[1176] S. Gao, E. Kaltofen, and A. Lauder, Deterministic distinct degree factorization for polynomials over finite fields, *J. Symbolic Comput.* 38 (2004) 1461–1470. <380, 385>

[1177] S. Gao and A. G. B. Lauder, Hensel lifting and bivariate polynomial factorisation over finite fields, *Math. Comp.* 71 (2002) 1663–1676. <378, 385>

[1178] S. Gao and H. W. Lenstra, Jr., Optimal normal bases, *Des. Codes Cryptogr.* 2 (1992) 315–323. <111, 112, 122>

[1179] S. Gao and T. Mateer, Additive fast Fourier transforms over finite fields, *IEEE Trans. Inform. Theory* 56 (2010) 6265–6272. <107, 110>

[1180] S. Gao and D. Panario, Density of normal elements, *Finite Fields Appl.* 3 (1997) 141–150. <107, 110>

[1181] S. Gao and D. Panario, Tests and constructions of irreducible polynomials over finite fields, In *Foundations of Computational Mathematics*, 346–361, Springer, Berlin, 1997. <340, 341, 356, 363, 367, 369, 370, 373>

[1182] S. Gao and S. A. Vanstone, On orders of optimal normal basis generators, *Math. Comp.* 64 (1995) 1227–1233. <119, 122, 811, 813>

[1183] Z. Gao and D. Panario, Degree distribution of the greatest common divisor of polynomials over $\mathbb{F}_q$, *Random Structures Algorithms* 29 (2006) 26–37. <364, 365, 367>

[1184] Z. Gao and L. B. Richmond, Central and local limit theorems applied to asymptotic enumeration. IV. Multivariate generating functions, *J. Comput. Appl. Math.* 41 (1992) 177–186. <360, 367>

[1185] M. Z. Garaev, Double exponential sums related to Diffie-Hellman distributions, *Int. Math. Res. Not.* (2005) 1005–1014. <177, 178, 179>

[1186] M. Z. Garaev, An explicit sum-product estimate in $\mathbb{F}_p$, *Int. Math. Res. Not. IMRN* (2007) Art. ID rnm035, 11. <181, 186>

[1187] M. Z. Garaev, A quantified version of Bourgain's sum-product estimate in $\mathbb{F}_p$ for subsets of incomparable sizes, *Electron. J. Combin.* 15 (2008) Research paper 58, 8. <181, 186>

[1188] M. Z. Garaev, The sum-product estimate for large subsets of prime fields, *Proc. Amer. Math. Soc.* 136 (2008) 2735–2739. <180, 186>

[1189] M. Z. Garaev, Sums and products of sets and estimates for rational trigonometric sums in fields of prime order, *Uspekhi Mat. Nauk* 65 (2010) 5–66. <181, 183, 186>

[1190] M. Z. Garaev and V. C. Garcia, Waring type congruences involving factorials

modulo a prime, *Arch. Math. (Basel)* 88 (2007) 35–41. <207>

[1191] M. Z. Garaev, F. Luca, and I. E. Shparlinski, Waring problem with factorials, *Bull. Austral. Math. Soc.* 71 (2005) 259–264. <207>

[1192] M. Z. Garaev, F. Luca, I. E. Shparlinski, and A. Winterhof, On the lower bound of the linear complexity over $\mathbb{F}_p$ of Sidelnikov sequences, *IEEE Trans. Inform. Theory* 52 (2006) 3299–3304. <327, 329>

[1193] A. Garcia, M. Q. Kawakita, and S. Miura, On certain subcovers of the Hermitian curve, *Comm. Algebra* 34 (2006) 973–982. <202, 207>

[1194] A. Garcia and H. Stichtenoth, A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound, *Invent. Math.* 121 (1995) 211–222. <458, 460, 462>

[1195] A. Garcia and H. Stichtenoth, On the asymptotic behaviour of some towers of function fields over finite fields, *J. Number Theory* 61 (1996) 248–273. <460, 462>

[1196] A. Garcia and H. Stichtenoth, On the Galois closure of towers, In *Recent Trends in Coding Theory and its Applications*, volume 41 of *AMS/IP Stud. Adv. Math.*, 83–92, Amer. Math. Soc., Providence, RI, 2007. <461, 462>

[1197] A. Garcia, H. Stichtenoth, A. Bassa, and P. Beelen, Towers of function fields over non-prime finite fields, 2012, arXiv:1202.5922v1. <456, 461, 462>

[1198] A. Garcia, H. Stichtenoth, and H.-G. Rück, On tame towers over finite fields, *J. Reine Angew. Math.* 557 (2003) 53–80. <460, 462>

[1199] A. Garcia, H. Stichtenoth, and C.-P. Xing, On subfields of the Hermitian function field, *Compositio Math.* 120 (2000) 137–170. <455, 456>

[1200] A. Garcia and J. F. Voloch, Fermat curves over finite fields, *J. Number Theory* 30 (1988) 345–356. <206, 207>

[1201] M. García-Armas, S. R. Ghorpade, and S. Ram, Relatively prime polynomials and nonsingular Hankel matrices over finite fields, *J. Combin. Theory, Ser. A* 118 (2011) 819–828. <500, 501, 502>

[1202] F. Gardeyn, A Galois criterion for good reduction of τ-sheaves, *J. Number Theory* 97 (2002) 447–471. <534, 538>

[1203] T. Garefalakis, Irreducible polynomials with consecutive zero coefficients, *Finite Fields Appl.* 14 (2008) 201–208. <72, 73, 75>

[1204] T. Garefalakis, Self-irreducible polynomials with prescribed coefficients, *Finite Fields Appl.* 17 (2011). <73, 75>

[1205] T. Garefalakis and D. Panario, The index calculus method using non-smooth polynomials, *Math. Comp.* 70 (2001) 1253–1264. <363, 367>

[1206] T. Garefalakis and D. Panario, Polynomials over finite fields free from large and small degree irreducible factors, *J. Algorithms* 44 (2002) 98–120. <363, 367>

[1207] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-completeness*, W. H. Freeman and Co., San Francisco, Calif., 1979. <772, 774>

[1208] G. Garg, T. Helleseth, and P. V. Kumar, Recent advances in low-correlation sequences, In V. Tarokh, editor, *New Directions in Wireless Communications Research*, chapter 3, 63–92, Springer-Verlag, Berlin, 2009. <310, 316, 317>

[1209] J. von zur Gathen, Factoring sparse multivariate polynomials, In *Twenty Fourth Annual IEEE Symposium on Foundations of Computer Science*, 172–179, Los Alamitos, CA, USA, 1983. <384, 385>

[1210] J. von zur Gathen, Hensel and Newton methods in valuation rings, *Math. Comp.* 42 (1984) 637–661. <378, 385>

[1211] J. von zur Gathen, Irreducibility of multivariate polynomials, *J. Comput. System Sci.* 31 (1985) 225–264. <380, 383, 385>

[1212] J. von zur Gathen, Irreducible polynomials over finite fields, In *Proc. Sixth Conf. Foundations of Software Technology and Theoretical Computer Science*, volume 241 of *Springer Lecture Notes in Computer Science*, 252–262, Delhi, India, 1986. <372, 373>

[1213] J. von zur Gathen, Factoring polynomials and primitive elements for special primes, *Theoretical Computer Science* 52 (1987) 77–89. <374, 375>

[1214] J. von zur Gathen, Tests for permutation polynomials, *SIAM J. Comput.* 20 (1991) 591–602. <210, 222>

[1215] J. von zur Gathen, Values of polynomials over finite fields, *Bull. Austral. Math. Soc.* 43 (1991) 141–146. <228, 229, 231, 233>

[1216] J. von zur Gathen, Irreducible trinomials over finite fields, *Math. Comp.* 72 (2003) 1987–2000. <65, 66, 341, 356>

[1217] J. von zur Gathen, Counting decomposable multivariate polynomials, *Appl. Algebra Engrg. Comm. Comput.* 22 (2011) 165–185. <79, 80, 81>

[1218] J. von zur Gathen and J. Gerhard, Arithmetic and factorization of polynomials over $\mathbb{F}_2$, Technical Report tr-rsfb-96-018, University of Paderborn, Germany, 1996, 43 pages. <373, 375>

[1219] J. von zur Gathen and J. Gerhard, Polynomial factorization over $\mathbb{F}_2$, *Math. Comp.* 71 (2002) 1677–1698. <361, 367, 374, 375>

[1220] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, Cambridge University Press, Cambridge, New York, Melbourne, second edition, 2003. <29, 30, 80, 81, 119, 120, 122, 339, 356, 369, 370, 373, 374, 375, 378, 380, 385>

[1221] J. von zur Gathen, J. L. Imaña, and Ç. K. Koç, editors, *Arithmetic of Finite Fields*, volume 5130 of *Lecture Notes in Computer Science*, Berlin, 2008. Springer, Available electronically at `http://www.springerlink.com/content/978-3-540-69498-4`. <30>

[1222] J. von zur Gathen and E. Kaltofen, Factoring multivariate polynomials over finite fields, *Math. Comp.* 45 (1985) 251–261. <380, 385>

[1223] J. von zur Gathen and E. Kaltofen, Factoring sparse multivariate polynomials, *J. Comput. System Sci.* 31 (1985) 265–287. <383, 384, 385>

[1224] J. von zur Gathen, M. Karpinski, and I. E. Shparlinski, Counting curves and their projections, *Comput. Complexity* 6 (1996/97) 64–99. <481, 484>

[1225] J. von zur Gathen and M. Nöcker, Exponentiation in finite fields: Theory and practice, In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Twelfth International Symposium AAECC-12*, volume 1255 of *Lecture Notes in Comput. Sci.*, 88–113, Springer, 1997. <349, 356>

[1226] J. von zur Gathen and M. Nöcker, Polynomial and normal bases for finite fields, *J. Cryptology* 18 (2005) 337–355. <68, 69, 341, 346, 356>

[1227] J. von zur Gathen and D. Panario, Factoring polynomials over finite fields: a survey, *J. Symbolic Comput.* 31 (2001) 3–17. <374, 375>

[1228] J. von zur Gathen, D. Panario, and B. Richmond, Interval partitions and polynomial factorization, *Algorithmica* 63 (2012) 363–397. <362, 367, 374, 375>

[1229] J. von zur Gathen and F. Pappalardi, Density estimates related to Gauss periods, In *Cryptography and Computational Number Theory*, volume 20 of *Progr.*

Comput. Sci. Appl. Logic, 33–41, Birkhäuser, Basel, 2001. <114, 122>

[1230] J. von zur Gathen and G. Seroussi, Boolean circuits versus arithmetic circuits, *Information and Computation* 91 (1991) 142–154. <374, 375>

[1231] J. von zur Gathen, A. Shokrollahi, and J. Shokrollahi, Efficient multiplication using type 2 optimal normal bases, In *Arithmetic of Finite Fields*, volume 4547 of *Lecture Notes in Comput. Sci.*, 55–68, Springer, Berlin, 2007. <121, 122, 812, 813>

[1232] J. von zur Gathen and V. Shoup, Computing Frobenius maps and factoring polynomials, *Computational Complexity* 2 (1992) 187–224. <361, 367, 369, 373, 374, 375>

[1233] J. von zur Gathen and I. E. Shparlinski, Orders of Gauss periods in finite fields, In *Algorithms and Computations*, volume 1004 of *Lecture Notes in Comput. Sci.*, 208–215, Springer, Berlin, 1995. <119, 122>

[1234] J. von zur Gathen and I. E. Shparlinski, Orders of Gauss periods in finite fields, *Appl. Algebra Engrg. Comm. Comput.* 9 (1998) 15–24. <93, 94>

[1235] J. von zur Gathen and I. E. Shparlinski, Constructing elements of large order in finite fields, In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 1719 of *Lecture Notes in Comput. Sci.*, 404–409, Springer, Berlin, 1999. <94>

[1236] J. von zur Gathen and I. E. Shparlinski, Gauss periods in finite fields, In *Finite Fields and Applications*, 162–177, Springer, Berlin, 2001. <93, 94>

[1237] P. Gaudry, An algorithm for solving the discrete log problem on hyperelliptic curves, In *Advances in Cryptology—EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Comput. Sci.*, 19–34, Springer, Berlin, 2000. <449, 789, 793, 794>

[1238] P. Gaudry, Fast genus 2 arithmetic based on theta functions, *Journal of Mathematical Cryptology* 1 (2007) 243–265. <788, 794>

[1239] P. Gaudry, Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem, *Journal of Symbolic Computation* 44 (2009) 1690–1702. <777, 787, 793, 794>

[1240] P. Gaudry and N. Gürel, Counting points in medium characteristic using Kedlaya's algorithm, *Experiment. Math.* 12 (2003) 395–402. <484>

[1241] P. Gaudry and R. Harley, Counting points on hyperelliptic curves over finite fields, In *Algorithmic Number Theory*, volume 1838 of *Lecture Notes in Comput. Sci.*, 313–332, Springer, Berlin, 2000. <447, 449>

[1242] P. Gaudry, F. Hess, and N. P. Smart, Constructive and destructive facets of Weil descent on elliptic curves, *Journal of Cryptology* 15 (2002) 19–46. <777, 787, 800, 801, 802>

[1243] P. Gaudry and F. Morain, Fast algorithms for computing the eigenvalue in the Schoof–Elkies–Atkin algorithm, In J.-G. Dumas, editor, *Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computations—ISSAC MMVI*, 109–115, ACM, New York, 2006. <778, 787>

[1244] P. Gaudry and É. Schost, Construction of secure random curves of genus 2 over prime fields, In *Advances in Cryptology—EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Comput. Sci.*, 239–256, Springer, Berlin, 2004. <794>

[1245] P. Gaudry and É. Schost, Genus 2 point counting over prime fields, *J. Symb. Comput.* 47 (2012) 368–400. <794>

[1246] P. Gaudry, B. A. Smith, and D. R. Kohel, Counting points on genus 2 curves with real multiplication, In *Advances in Cryptology—ASIACRYPT 2011*, volume

7073 of *Lecture Notes in Comput. Sci.*, 504–519, Springer, Berlin, 2011. <794>

[1247] P. Gaudry and E. Thomé, MPFQ – A finite field library Release 1.0-rc3, 2010, available at `http://mpfq.gforge.inria.fr`. <339, 356>

[1248] P. Gaudry, E. Thomé, N. Thériault, and C. Diem, A double large prime variation for small genus hyperelliptic index calculus, *Math. Comp.* 76 (2007) 475–492. <449, 789, 790, 794>

[1249] C. F. Gauss, *Mathematical Diary.* Original manuscript in Latin: Handschriftenabteilung Niedersächsische Staats- und Universitätsbibliothek Göttingen, Cod. Ms. Gauss Math. 48 Cim., English commented transl. by J. Gray, A commentary on Gauss's Mathematical Diary, 1796–1814, with an English translation. *Exposition. Math.*, 2:97–130, 1984. <5, 10>

[1250] C. F. Gauss, *Disquisitiones Arithmeticae*, Lipsiae: G. Fleischer, 1801, English transl. A. A. Clarke. New Haven: Yale University Press, 1966. <3, 10>

[1251] C. F. Gauss, *Werke,* ed. Königliche Gesellschaft der Wissenschaften zu Göttingen, vol. II*, Höhere Arithmetik.*, Göttingen: Universitäts-Druckerei, 1863. <3, 4, 10>

[1252] D. Gavinsky, M. Rötteler, and J. Roland, Quantum algorithm for the Boolean hidden shift problem, In *Proceedings of the Seventeenth Annual International Computing and Combinatorics Conference (COCCON'11)*, volume 6842 of *Lecture Notes in Computer Science*, 158–167. Springer, 2011. <830, 831>

[1253] D. Gay and W. Vélez, On the degree of the splitting field of an irreducible binomial, *Pacific J. Math.* 78 (1978) 117–120. <58, 61>

[1254] G. Ge and L. Zhu, Authentication perpendicular arrays $\mathrm{APA}_1(2, 5, v)$, *J. Combin. Des.* 4 (1996) 365–375. <603, 610>

[1255] W. Geiselmann, *Algebraische Algorithmenentwicklung am Beispiel der Arithmetik in endlichen Körpern*, PhD thesis, Universit at Karlsruhe, 1992. <37, 39, 46, 117, 122>

[1256] W. Geiselmann and D. Gollmann, Duality and normal basis multiplication, In *Cryptography and Coding, III*, volume 45 of *Inst. Math. Appl. Conf. Ser. (New Ser.)*, 187–195, Oxford Univ. Press, New York, 1993. <37, 46>

[1257] W. Geiselmann and D. Gollmann, Self-dual bases in $\mathbf{F}_{q^n}$, *Des. Codes Cryptogr.* 3 (1993) 333–345. <97, 103>

[1258] W. Geiselmann, W. Meier, and R. Steinwandt, An attack on the isomorphisms of polynomials problem with one secret, *Int. Journal of Information Security* 2 (2003) 59–64. <758, 774>

[1259] E.-U. Gekeler, On the coefficients of Drinfeld modular forms, *Invent. Math.* 93 (1988) 667–700. <537, 538>

[1260] M. Genma, M. Mishima, and M. Jimbo, Cyclic resolvability of cyclic Steiner 2-designs, *J. Combin. Des.* 5 (1997) 177–187. <586, 590>

[1261] S. R. Ghorpade, S. U. Hasan, and M. Kumari, Primitive polynomials, Singer cycles and word-oriented linear feedback shift registers, *Des. Codes Cryptogr.* 58 (2011) 123–134. <494, 502>

[1262] S. R. Ghorpade and G. Lachaud, Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields, *Mosc. Math. J.* 2 (2002) 589–631. <189, 195>

[1263] P. Gianni and B. Trager, Square-free algorithms in positive characteristic, *Appl. Alg. Eng. Comm. Comp.* 7 (1996) 1–14. <377, 385>

[1264] K. S. Gibbins, M. J. Hoffman, and W. K. Wootters, Discrete phase space based on

finite fields, *Phys. Rev. A* 70 (2004) 062101. <826, 831>

[1265] M. Giesbrecht, A. Lobo, and B. D. Saunders, Certifying inconsistency of sparse linear systems, In *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation*, 113–119, New York, 1998, ACM. <524, 527>

[1266] V. Gillot, Bounds for exponential sums over finite fields, *Finite Fields Appl.* 1 (1995) 421–436. <201, 207>

[1267] P. Giorgi, C.-P. Jeannerod, and G. Villard, On the complexity of polynomial matrix computations, In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, 135–142, ACM, New York, 2003. <527>

[1268] D. Giry and J.-J. Quisquater, Bluekrypt cryptographic key length recommendation, 2011, v26.0, April 18, `http://www.keylength.com/`. <775, 787>

[1269] A. Giulietti, L. van der Perre, and M. Strum, Parallel turbo coding interleavers: avoiding collisions in access to storage elements, *IEE Electronics Letters* 38 (2002) 232–234. <717, 718>

[1270] M. Giulietti, J. W. P. Hirschfeld, G. Korchmáros, and F. Torres, Curves covered by the Hermitian curve, *Finite Fields Appl.* 12 (2006) 539–564. <202, 207>

[1271] M. Giulietti and G. Korchmáros, A new family of maximal curves over a finite field, *Math. Ann.* 343 (2009) 229–245. <455, 456>

[1272] M. Giulietti, G. Korchmáros, and F. Torres, Quotient curves of the Suzuki curve, *Acta Arith.* 122 (2006) 245–274. <455, 456>

[1273] D. Glass and R. Pries, Hyperelliptic curves with prescribed p-torsion, *Manuscripta Math.* 117 (2005) 299–317. <479, 480>

[1274] A. Glibichuk and M. Rudnev, On additive properties of product sets in an arbitrary finite field, *J. Anal. Math.* 108 (2009) 159–170. <186, 206, 207>

[1275] A. A. Glibichuk, Sums of powers of subsets of an arbitrary finite field, *Izv. RAN. Ser. Mat.* 75 (2011) 35–68. <169, 179>

[1276] A. A. Glibichuk and S. V. Konyagin, Additive properties of product sets in fields of prime order, In *Additive Combinatorics*, volume 43 of *CRM Proc. Lecture Notes*, 279–286, Amer. Math. Soc., Providence, RI, 2007. <181, 186>

[1277] D. Gligoroski, S. Markovski, and S. J. Knapskog, Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroup, In *Proceedings of The American Conference on Applied Mathematics—MATH08*, Cambridge, Massachusetts, USA, 2008. <766, 774>

[1278] D. Gluck, A note on permutation polynomials and finite geometries, *Discrete Math.* 80 (1990) 97–100. <273, 274>

[1279] C. Godsil and G. Royle, *Algebraic Graph Theory*, volume 207 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 2001. <636, 647, 649>

[1280] J.-M. Goethals, Nonlinear codes defined by quadratic forms over GF(2), *Information and Control* 31 (1976) 43–74. <693, 694>

[1281] J.-M. Goethals and J. J. Seidel, Orthogonal matrices with zero diagonal, *Canad. J. Math.* 19 (1967) 1001–1010. <601, 610>

[1282] W. M. Y. Goh and E. Schmutz, The expected order of a random permutation, *Bull. London Math. Soc.* 23 (1991) 34–42. <366, 367>

[1283] J. S. Golan, *Semirings and their Applications*, Kluwer Academic Publishers, Dordrecht, 1999. <26, 30>

[1284] M. Golay, Notes on digital coding, *Proc. IRE* 37 (1949) 657. <674, 693, 694>

[1285] M. Golay, Static multislit spectrometry and its application to the panoramic display

of infrared spectra, *J. Opt. Soc. Amer.* 41 (1951) 468–472. <833, 839>

[1286] R. Gold, Characteristic linear sequences and their coset functions, *SIAM J. Appl. Math.* 14 (1966) 980–985. <306, 310>

[1287] R. Gold, Maximal recursive sequences with 3-valued recursive crosscorrelation functions, *IEEE Trans. Inform. Theory* 14 (1968) 154–156. <220, 222, 313, 317>

[1288] D. M. Goldschmidt, *Algebraic Functions and Projective Curves*, volume 215 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 2003. <399, 415>

[1289] C. Goldstein, N. Schappacher, and J. Schwermer, editors, *The Shaping of Arithmetic After C. F. Gauss's Disquisitiones Arithmeticae*, Springer, Berlin, 2007. <4, 10>

[1290] D. Gollmann, *Design of Algorithms in Cryptography. (Algorithmenentwurf in der Kryptographie.)*, Aspekte Komplexer Systeme. 1. Mannheim: B.I. Wissenschaftsverlag. viii, 158 p. 68.00; öS 531.00; sFr 68.00 /hc , 1994. <97, 99, 103>

[1291] F. Göloğlu, G. McGuire, and R. Moloney, Binary Kloosterman sums using Stickelberger's theorem and the Gross-Koblitz formula, *Acta Arith.* 148 (2011) 269–279. <148, 155>

[1292] S. W. Golomb, *Shift Register Sequences*, With portions co-authored by Lloyd R. Welch, Richard M. Goldstein, and Alfred W. Hales. Holden-Day Inc., San Francisco, Calif., 1967. <65, 66, 305, 310>

[1293] S. W. Golomb, Algebraic constructions for Costas arrays, *J. Combin. Theory, Ser. A* 37 (1984) 13–21. <599, 610>

[1294] S. W. Golomb, Periodic binary sequences: solved and unsolved problems, In *Sequences, Subsequences, and Consequences*, volume 4893 of *Lecture Notes in Comput. Sci.*, 1–8, Springer, Berlin, 2007. <91, 93>

[1295] S. W. Golomb and G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*, Cambridge University Press, Cambridge, 2005. <29, 30, 166, 179, 236, 244, 245, 310, 317, 594, 598, 746, 754>

[1296] S. W. Golomb and G. Gong, The status of Costas arrays, *IEEE Trans. Inform. Theory* 53 (2007) 4260–4265. <599, 610>

[1297] S. W. Golomb and O. Moreno, On periodicity properties of Costas arrays and a conjecture on permutation polynomials, *IEEE Trans. Inform. Theory* 42 (1996) 2252–2253. <222>

[1298] S. W. Golomb, M. G. Parker, A. Pott, and A. Winterhof, editors, *Sequences and Their Applications*, volume 5203 of *Lecture Notes in Comput. Sci.*, Springer, Berlin, 2008. <30>

[1299] D. Gómez, J. Gutierrez, and Á. Ibeas, Attacking the Pollard generator, *IEEE Trans. Inform. Theory* 52 (2006) 5518–5523. <331, 337>

[1300] D. Gomez and A. P. Nicolás, An estimate on the number of stable quadratic polynomials, *Finite Fields Appl.* 16 (2010) 401–405. <172, 179, 335, 336, 337>

[1301] D. Gomez, A. P. Nicolás, A. Ostafe, and D. Sadornil, Stable polynomials over finite fields, preprint available, `http://arxiv.org/abs/1206.4979`, 2011. <336, 337>

[1302] D. Gomez and A. Winterhof, Waring's problem in finite fields with Dickson polynomials, In *Finite Fields: Theory and Applications*, volume 518 of *Contemp. Math.*, 185–192, Amer. Math. Soc., Providence, RI, 2010. <207>

[1303] J. Gomez-Calderon, On the cardinality of value set of polynomials with coefficients

in a finite field, *Proc. Japan Acad., Ser. A Math. Sci.* 68 (1992) 338–340. <228, 229>

[1304] J. Gomez-Calderon and D. J. Madden, Polynomials with small value set over finite fields, *J. Number Theory* 28 (1988) 167–188. <226, 229>

[1305] G. Gong, T. Helleseth, H. Hu, and A. Kholosha, On the dual of certain ternary weakly regular bent functions, *IEEE Trans. Inform. Theory* 58 (2012) 2237–2243. <263, 265>

[1306] G. Gong, T. Helleseth, H.-Y. Song, and K. Yang, editors, *Sequences and Their Applications*, volume 4086 of *Lecture Notes in Comput. Sci.*, Springer, Berlin, 2006. <30>

[1307] G. Gong and A. M. Youssef, Cryptographic properties of the Welch-Gong transformation sequence generators, *IEEE Transactions on Information Theory* 48 (2002) 2837–2846. <746, 754>

[1308] P. Gopalan, V. Guruswami, and R. J. Lipton, Algorithms for modular counting of roots of multivariate polynomials, In *LATIN 2006: Theoretical Informatics*, volume 3887 of *Lecture Notes in Comput. Sci.*, 544–555, Springer, Berlin, 2006. <482, 484>

[1309] V. D. Goppa, A new class of linear correcting codes, *Problemy Peredači Informacii* 6 (1970) 24–30. <675, 693, 694>

[1310] V. D. Goppa, Rational representation of codes and (L, g)-codes, *Problemy Peredači Informacii* 7 (1971) 41–49. <675, 693, 694>

[1311] V. D. Goppa, Codes that are associated with divisors (Russian), *Problemy Peredači Informacii* 13 (1977) 33–39. <694, 703>

[1312] V. D. Goppa, Codes on algebraic curves (Russian), *Dokl. Akad. Nauk SSSR* 259 (1981) 1289–1290. <694, 703>

[1313] V. D. Goppa, Algebraic-geometric codes (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* 46 (1982) 762–781. <694, 703>

[1314] B. Gordon, W. H. Mills, and L. R. Welch, Some new difference sets, *Canad. J. Math.* 14 (1962) 614–625. <311, 317, 593, 594, 598>

[1315] D. M. Gordon, Discrete logarithms in GF(p) using the number field sieve, *SIAM J. Discrete Math.* 6 (1993) 124–138. <392, 394>

[1316] D. M. Gordon, The prime power conjecture is true for $n < 2,000,000$, *Electron. J. Combin.* 1 (1994) Research Paper 6, approx. 7 pp. <593, 598>

[1317] D. M. Gordon and K. S. McCurley, Massively parallel computation of discrete logarithms, In *Proceedings of the Twelfth Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '92, 312–323, Springer-Verlag, London, UK, 1993. <341, 356>

[1318] J. A. Gordon, Very simple method to find the minimum polynomial of an arbitrary nonzero element of a finite field, *Electron. Lett.* 12 (1976) 663–664. <343, 356>

[1319] D. Gorenstein and N. Zierler, A class of error-correcting codes in p^m symbols, *J. Soc. Indust. Appl. Math.* 9 (1961) 207–214. <669, 683, 693, 694>

[1320] M. Goresky and A. Klapper, Arithmetic crosscorrelations of feedback with carry shift register sequences, *IEEE Trans. Inform. Theory* 43 (1997) 1342–1345. <329>

[1321] M. Goresky and A. M. Klapper, Fibonacci and Galois representations of feedback-with-carry shift registers, *IEEE Trans. Inform. Theory* 48 (2002) 2826–2836. <329>

[1322] D. Goss, π-adic Eisenstein series for function fields, *Compositio Math.* 41 (1980)

3–38. <537, 538>

[1323] D. Goss, *Basic Structures of Function Field Arithmetic*, volume 35 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*, Springer-Verlag, Berlin, 1996. <29, 30, 528, 529, 531, 533, 534, 535, 538>

[1324] D. Goss, Applications of non-Archimedean integration to the L-series of τ-sheaves, *J. Number Theory* 110 (2005) 83–113. <534, 538>

[1325] D. Goss, ζ-phenomenology, In *Noncommutative Geometry, Arithmetic, and Related Topics: Proceedings of the Twenty-First Meeting of the Japan-U.S. Mathematics Institute*, The Johns Hopkins University Press, Baltimore, MD, 2011. <535, 536, 538>

[1326] K. Goto and R. van de Geijn, High-performance implementation of the level-3 BLAS, *ACM Trans. Math. Software* 35 (2009) Art. 4, 14. <515, 527>

[1327] D. Gottesman, Class of quantum error-correcting codes saturating the quantum Hamming bound, *Phys. Rev. A, 3rd Ser.* 54 (1996) 1862–1868. <825, 827, 831>

[1328] D. Gottesman, Fault-tolerant quantum computation with higher-dimensional systems, In *Quantum Computing & Quantum Communications; First NASA International Conference (QCQC'98)*, volume 1509 of *Lecture Notes in Computer Science*, 302–313. Springer, 1998. <828, 831>

[1329] L. Goubin and N. T. Courtois, Cryptanalysis of the TTM cryptosystem, In *Advances in Cryptology—ASIACRYPT 2000*, volume 1976 of *Lecture Notes in Comput. Sci.*, 44–57, Springer, Berlin, 2000. <759, 764, 765, 770, 774>

[1330] A. Gouget and J. Patarin, Probabilistic multivariate cryptography, In P. Q. Nguyen, editor, *VIETCRYPT*, volume 4341 of *Lecture Notes in Computer Science*, 1–18. Springer, 2006. <761, 774>

[1331] X. Gourdon, *Combinatoire, Algorithmique et Géométrie des Polynômes*, PhD dissertation, École Polytechnique, 1996. <362, 366, 367>

[1332] X. Gourdon, Largest component in random combinatorial structures, *Discrete Math.* 180 (1998) 185–209. <366, 367>

[1333] P. Goutet, An explicit factorisation of the zeta functions of Dwork hypersurfaces, *Acta Arith.* 144 (2010) 241–261. <135, 155>

[1334] P. Goutet, On the zeta function of a family of quintics, *J. Number Theory* 130 (2010) 478–492. <135, 155>

[1335] P. Goutet, Isotypic decomposition of the cohomology and factorization of the zeta functions of dwork hypersurfaces, *Finite Fields Appl.* 17 (2011) 113–137. <465, 472>

[1336] R. Gow and J. Sheekey, On primitive elements in finite semifields, *Finite Fields Appl.* 17 (2011) 194–204. <270>

[1337] W. T. Gowers, A new proof of Szemerédi's theorem, *Geom. Funct. Anal.* 11 (2001) 465–588. <182, 186>

[1338] B. Grammaticos, R. G. Halburd, A. Ramani, and C.-M. Viallet, How to detect the integrability of discrete systems, *J. Phys. A* 42 (2009) 454002, 30. <330, 337>

[1339] L. Granboulan, A. Joux, and J. Stern, Inverting HFE is quasipolynomial, In *Advances in Cryptology—CRYPTO 2006*, volume 4117 of *Lecture Notes in Comput. Sci.*, 345–356, Springer, Berlin, 2006. <773, 774>

[1340] A. Granville, S. Li, and S. Qi, On the number of solution of the equation $\sum_{i=1}^{n} x_i/d_i \equiv 0 \pmod 1$, and of diagonal equations in finite fields, *Sichuan Daxue Xuebao* 32 (1995) 243–248. <203, 207>

[1341] M. Grassl, T. Beth, and M. Rötteler, On optimal quantum codes, *International Journal of Quantum Information* 2 (2004) 55–64, See also arXiv preprint quant-ph/0312164. <828, 831>

[1342] M. Grassl, W. Geiselmann, and T. Beth, Quantum Reed-Solomon codes, In *Proceedings of the Thirteenth conference on Applied Algebra, Algebraic Algorithms and Error- Correcting Codes (AAECC'13)*, volume 1719 of *Lecture Notes in Computer Science*, 231–244. Springer, 1999. <828, 831>

[1343] M. Grassl, M. Rötteler, and T. Beth, Efficient quantum circuits for non-qubit quantum error-correcting codes, *International Journal of Foundations of Computer Science* 14 (2003) 757–775. <828, 831>

[1344] R. M. Gray, Toeplitz and circulant matrices: a review, Technical report, Stanford University, 2001. <499, 502>

[1345] D. R. Grayson and M. E. Stillman, Macaulay2, a software system for research in algebraic geometry, Available at http://www.math.uiuc.edu/Macaulay2/, 1992. <45, 46, 822, 824>

[1346] M. Greig, Some balanced incomplete block design constructions, In *Proceedings of the Twenty-first Southeastern Conference on Combinatorics, Graph Theory, and Computing*, volume 77, 121–134, 1990. <585, 590>

[1347] M. Greig, Some group divisible design constructions, *J. Combin. Math. Combin. Comput.* 27 (1998) 33–52. <588, 590>

[1348] F. Griffin, H. Niederreiter, and I. E. Shparlinski, On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders, In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 1719 of *Lecture Notes in Comput. Sci.*, 87–93, Springer, Berlin, 1999. <331, 333, 337>

[1349] F. Griffin and I. E. Shparlinski, On the linear complexity profile of the power generator, *IEEE Trans. Inform. Theory* 46 (2000) 2159–2162. <326, 329>

[1350] D. Gross, Hudson's theorem for finite-dimensional quantum systems, *J. Math. Phys* 47 (2006) 122107. <826, 831>

[1351] J. Guajardo and C. Paar, Itoh-Tsujii inversion in standard basis and its application in cryptography and codes, *Des. Codes Cryptogr.* 25 (2002) 207–216. <809, 813>

[1352] K. C. Gupta and S. Maitra, Multiples of primitive polynomials over GF(2), In *Progress in Cryptology—INDOCRYPT 2001*, volume 2247 of *Lecture Notes in Comput. Sci.*, 62–72, Springer, Berlin, 2001. <626, 633>

[1353] S. Gurak, Gauss and Eisenstein sums of order twelve, *Canad. Math. Bull.* 46 (2003) 344–355. <145, 155>

[1354] S. Gurak, Gauss sums for prime powers in p-adic fields, *Acta Arith.* 142 (2010) 11–39. <154, 155>

[1355] S. Gurak, Jacobi sums and irreducible polynomials with prescribed trace and restricted norm, In *Finite Fields: Theory and Applications*, volume 518 of *Contemp. Math.*, 193–208, Amer. Math. Soc., Providence, RI, 2010. <137, 155>

[1356] S. J. Gurak, Kloosterman sums for prime powers in p-adic fields, *J. Théor. Nombres Bordeaux* 21 (2009) 175–201. <154, 155>

[1357] R. Guralnick and D. Wan, Bounds for fixed point free elements in a transitive group and applications to curves over finite fields, *Israel J. Math.* 101 (1997) 255–287. <226, 229>

[1358] R. M. Guralnick, Rational maps and images of rational points of curves over finite fields, *Irish Math. Soc. Bull.* (2003) 71–95. <226, 229, 232, 233>

[1359] R. M. Guralnick and P. Müller, Exceptional polynomials of affine type, *J. Algebra* 194 (1997) 429–454. <230, 231, 233>

[1360] R. M. Guralnick, P. Müller, and J. Saxl, The rational function analogue of a question of Schur and exceptionality of permutation representations, *Mem. Amer. Math. Soc.* 162 (2003) viii+79. <232, 233, 291, 293, 295>

[1361] R. M. Guralnick, P. Müller, and M. E. Zieve, Exceptional polynomials of affine type, revisited, Preprint, 1999. <230, 231, 233>

[1362] R. M. Guralnick, J. Rosenberg, and M. E. Zieve, A new family of exceptional polynomials in characteristic two, *Ann. of Math., 2nd Ser.* 172 (2010) 1361–1390. <230, 233>

[1363] R. M. Guralnick, T. J. Tucker, and M. E. Zieve, Exceptional covers and bijections on rational points, *Int. Math. Res. Not. IMRN* (2007) Art. ID rnm004, 20. <232, 233>

[1364] R. M. Guralnick and M. E. Zieve, Polynomials with PSL(2) monodromy, *Ann. of Math., 2nd Ser.* 172 (2010) 1315–1359. <230, 233>

[1365] V. Guruswami and A. C. Patthak, Correlated algebraic-geometric codes: improved list decoding over bounded alphabets, *Math. Comp.* 77 (2008) 447–473. <696, 703>

[1366] V. Guruswami and A. Rudra, Limits to list decoding Reed-Solomon codes, *IEEE Trans. Inform. Theory* 52 (2006) 3642–3649. <690, 694>

[1367] V. Guruswami and M. Sudan, Improved decoding of Reed-Solomon and algebraic-geometry codes, *IEEE Trans. Inform. Theory* 45 (1999) 1757–1767. <690, 694>

[1368] F. G. Gustavson, Analysis of the Berlekamp-Massey linear feedback shift-register synthesis algorithm, *IBM J. Res. Develop.* 20 (1976) 204–212. <323, 329>

[1369] J. Gutierrez and D. Gomez-Perez, Iterations of multivariate polynomials and discrepancy of pseudorandom numbers, In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 2227 of *Lecture Notes in Comput. Sci.*, 192–199, Springer, Berlin, 2001. <331, 333, 337>

[1370] J. Gutierrez and Á. Ibeas, Inferring sequences produced by a linear congruential generator on elliptic curves missing high-order bits, *Des. Codes Cryptogr.* 45 (2007) 199–212. <331, 337>

[1371] J. Gutierrez and I. E. Shparlinski, Expansion of orbits of some dynamical systems over finite fields, *Bull. Aust. Math. Soc.* 82 (2010) 232–239. <337>

[1372] J. Gutierrez, I. E. Shparlinski, and A. Winterhof, On the linear and nonlinear complexity profile of nonlinear pseudorandom number-generators, *IEEE Trans. Inform. Theory* 49 (2003) 60–64. <325, 326, 329>

[1373] C. Guyot, K. Kaveh, and V. M. Patankar, Explicit algorithm for the arithmetic on the hyperelliptic Jacobians of genus 3, *Journal of the Ramanujan Mathematical Society* 19 (2004) 75–115. <790, 794>

[1374] K. Gyarmati and A. Sárközy, Equations in finite fields with restricted solution sets I: Character sums, *Acta Math. Hungar.* 118 (2008) 129–148. <178, 179>

[1375] K. Gyarmati and A. Sárközy, Equations in finite fields with restricted solution sets II: Algebraic equations, *Acta Math. Hungar.* 119 (2008) 259–280. <178, 179>

[1376] D. Hachenberger, On completely free elements in finite fields, *Des. Codes Cryptogr.* 4 (1994) 129–143. <123, 132>

[1377] D. Hachenberger, Explicit iterative constructions of normal bases and completely free elements in finite fields, *Finite Fields Appl.* 2 (1996) 1–20. <123, 132>

[1378] D. Hachenberger, Normal bases and completely free elements in prime power extensions over finite fields, *Finite Fields Appl.* 2 (1996) 21–34. <123, 132>

[1379] D. Hachenberger, *Finite Fields: Normal Bases and Completely Free Elements*, The Kluwer International Series in Engineering and Computer Science, 390. Kluwer Academic Publishers, Boston, MA, 1997. <29, 30, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132>

[1380] D. Hachenberger, A decomposition theory for cyclotomic modules under the complete point of view, *J. Algebra* 237 (2001) 470–486. <125, 126, 127, 132>

[1381] D. Hachenberger, Primitive complete normal bases for regular extensions, *Glasgow Math. J.* 43 (2001) 383–398. <90, 128, 131, 132>

[1382] D. Hachenberger, Universal generators for primary closures of Galois fields, In *Finite Fields and Applications*, 208–223, Springer, Berlin, 2001. <131, 132>

[1383] D. Hachenberger, Generators for primary closures of Galois fields, *Finite Fields Appl.* 9 (2003) 122–128. <131, 132>

[1384] D. Hachenberger, Primitive complete normal bases: existence in certain 2-power extensions and lower bounds, *Discrete Math.* 310 (2010) 3246–3250. <90, 131, 132>

[1385] D. Hachenberger, Primitive complete normal bases for regular extensions II: the exceptional case, *unpublished* (2012). <131, 132>

[1386] D. Hachenberger, H. Niederreiter, and C. P. Xing, Function-field codes, *Appl. Algebra Engrg. Comm. Comput.* 19 (2008) 201–211. <699, 703>

[1387] C. D. Haessig, L-functions of symmetric powers of cubic exponential sums, *J. Reine Angew. Math.* 631 (2009) 1–57. <472, 480>

[1388] J. Hagenauer, E. Offer, and L. Papke, Iterative decoding of binary block and convolutional codes, *IEEE Trans. Inform. Theory* 42 (1996) 429–445. <716, 718>

[1389] A. W. Hales and D. W. Newhart, Swan's theorem for binary tetranomials, *Finite Fields Appl.* 12 (2006) 301–311. <64, 66>

[1390] L. Hales and S. Hallgren, An improved quantum Fourier transform algorithm and applications, In *Forty First Annual Symposium on Foundations of Computer Science*, 515–525, IEEE Comput. Soc. Press, Los Alamitos, CA, 2000. <829, 831>

[1391] T. R. Halford, A. J. Grant, and K. M. Chugg, Which codes have 4-cycle-free Tanner graphs?, *IEEE Trans. Inform. Theory* 52 (2006) 4219–4223. <709, 710>

[1392] C. Hall, L-functions of twisted Legendre curves, *J. Number Theory* 119 (2006) 128–147. <488, 492>

[1393] J. I. Hall, On the order of Hall triple systems, *J. Combin. Theory, Ser. A* 29 (1980) 261–262. <602, 610>

[1394] M. Hall, Jr., Automorphisms of Steiner triple systems, *IBM J. Res. Develop* 4 (1960) 460–472. <602, 610>

[1395] K. H. Ham and G. L. Mullen, Distribution of irreducible polynomials of small degrees over finite fields, *Math. Comp.* 67 (1998) 337–341. <70, 75>

[1396] N. Hamilton and R. Mathon, More maximal arcs in Desarguesian projective planes and their geometric structure, *Adv. Geom.* 3 (2003) 251–261. <564, 565>

[1397] N. Hamilton and R. Mathon, On the spectrum of non-Denniston maximal arcs in $\mathrm{PG}(2, 2^h)$, *European J. Combin.* 25 (2004) 415–421. <564, 565>

[1398] R. W. Hamming, Error detecting and error correcting codes, *Bell System Tech. J.* 29 (1950) 147–160. <675, 693, 694>

[1399] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, The $\mathbf{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory* 40 (1994) 301–319. <27, 29, 244, 245, 265, 690, 692, 693, 694>

[1400] D.-G. Han, D. Choi, and H. Kim, Improved computation of square roots in specific finite fields, *IEEE Trans. Comput.* 58 (2009) 188–196. <353, 356>

[1401] W. Han, The distribution of the coefficients of primitive polynomials over finite fields, In *Cryptography and Computational Number Theory*, volume 20 of *Progr. Comput. Sci. Appl. Logic*, 43–57, Birkhäuser, Basel, 2001. <88, 90>

[1402] W. B. Han, The coefficients of primitive polynomials over finite fields, *Math. Comp.* 65 (1996) 331–340. <88, 90>

[1403] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer Professional Computing. Springer-Verlag, New York, 2004. <29, 30, 31, 46, 339, 346, 347, 348, 356, 449>

[1404] J. P. Hansen and J. P. Pedersen, Automorphism groups of Ree type, Deligne-Lusztig curves and function fields, *J. Reine Angew. Math.* 440 (1993) 99–109. <454, 456>

[1405] S. H. Hansen, Error-correcting codes from higher-dimensional varieties, *Finite Fields Appl.* 7 (2001) 530–552. <696, 703>

[1406] T. Hansen and G. L. Mullen, Primitive polynomials over finite fields, *Math. Comp.* 59 (1992) 639–643, S47–S50. <70, 75, 83, 85, 87, 90, 91, 93, 342, 356>

[1407] B. Hanson, D. Panario, and D. Thomson, Swan-like results for binomials and trinomials over finite fields of odd characteristic, *Des. Codes Cryptogr.* 61 (2011) 273–283. <65, 66>

[1408] G. Hardy and E. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford, 2008. <487, 492>

[1409] G. H. Hardy and J. E. Littlewood, Some problems of 'Partitio Numerorum'; IV: The singular series in Waring's problem and the value of the number G(k), *Math. Z.* 12 (1922) 161–188. <490, 492>

[1410] G. H. Hardy and J. E. Littlewood, Some problems of 'Partitio Numerorum'; III: On the expression of a number as a sum of primes, *Acta Math.* 44 (1923) 1–70. <489, 492>

[1411] R. Harley, Fast arithmetic on genus two curves, Preprint, 2000. <788, 794>

[1412] R. Harley, Asymptotically optimal p-adic point-counting, 2002, Posting to the Number Theory List, available at `http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0212&L=NMBRTHRY&P=R1277`. <779, 787>

[1413] N. V. Harrach and C. Mengyán, Minimal blocking sets in PG$(2, q)$ arising from a generalized construction of Megyesi, *Innov. Incidence Geom.* 6/7 (2007/08) 211–226. <551, 555>

[1414] D. Hart, A. Iosevich, and J. Solymosi, Sum-product estimates in finite fields via Kloosterman sums, *Int. Math. Res. Not. IMRN* (2007) Art. ID rnm007, 14. <180, 186>

[1415] D. Hart, L. Li, and C. Yen Shen, Fourier analysis and expanding phenomena in finite fields, preprint available, `http://arxiv.org/abs/0909.5471`, 2009. <182, 186>

[1416] W. B. Hart et al., Fast Library for Number Theory (Version 2.2.0), available at `http://www.flintlib.org`. <45, 46, 339, 344, 356>

[1417] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977, Graduate

Texts in Mathematics, No. 52. <283, 284, 287, 295, 414, 415, 462, 472>

[1418] D. Harvey, Faster arithmetic for number-theoretic transforms, Slides presented at FLINT/Sage Days 35, Warwick, 2011. <347, 356>

[1419] D. Harvey, Kedlaya's algorithm in larger characteristic, *Int. Math. Res. Not. IMRN* (2007) Art. ID rnm095, 29. <482, 484, 779, 787>

[1420] D. Harvey, Faster polynomial multiplication via multipoint Kronecker substitution, *J. Symbolic Comput.* 44 (2009) 1502–1510. <344, 356>

[1421] M. A. Hasan, Shift-register synthesis for multiplicative inversion over $GF(2^m)$, In *Proc. IEEE International Symposium on Information Theory*, 49, 1995. <807, 813>

[1422] M. A. Hasan, On matrix-vector product based sub-quadratic arithmetic complexity schemes for field multiplication, In *Proc. SPIE 6697, 669702*, 2007. <808, 813>

[1423] M. A. Hasan and V. K. Bhargava, Bit-serial systolic divider and multiplier for finite fields $GF(2^m)$, *IEEE Trans. Comput.* 41 (1992) 972–980. <808, 813>

[1424] M. A. Hasan and V. K. Bhargava, Division and bit-serial multiplication over $GF(q^m)$, *IEE Proceedings-E, Computers and Digital Techniques* 139 (1992) 230–236. <807, 808, 813>

[1425] M. A. Hasan and V. K. Bhargava, Architecture for low complexity rate-adaptive Reed-Solomon encoder, *IEEE Trans. Comput.* 44 (1995) 938–942. <813>

[1426] M. A. Hasan and T. Helleseth, editors, *Arithmetic of Finite Fields*, volume 6087 of *Lecture Notes in Computer Science*, Berlin, 2010. Springer. <30>

[1427] M. A. Hasan, A. H. Namin, and C. Negre, New complexity results for field multiplication using optimal normal bases and block recombination, Technical Report cacr2010-19, University of Waterloo, Waterloo, 2010. <812, 813>

[1428] M. A. Hasan and C. Negre, Low space complexity multiplication over binary fields with Dickson polynomial representation, *IEEE Trans. Comput.* 60 (2011) 602–607. <813>

[1429] M. A. Hasan, M. Z. Wang, and V. K. Bhargava, A modified Massey-Omura parallel multiplier for a class of finite fields, *IEEE Trans. Comput.* 42 (1993) 1278–1280. <811, 813>

[1430] S. Hasegawa and T. Kaneko, An attacking method for a public key cryptosystem based on the difficulty of solving a system of non-linear equations, In *Proc. Tenth Symposium on Information Theory and Its Applications*, JA5–3, 1987. <759, 774>

[1431] K. Hashimoto, Zeta functions of finite graphs and representations of p-adic groups, In *Automorphic Forms and Geometry of Arithmetic Varieties*, volume 15 of *Adv. Stud. Pure Math.*, 211–280, Academic Press, Boston, MA, 1989. <649>

[1432] S. H. Hassani, S. B. Korada, and R. Urbanke, The compound capacity of polar codes, In *The Forty Seventh Annual Allerton Conference on Communication, Control, and Computing*, 16–21, 2009. <730>

[1433] H. Hasse, Theorie der relativ-zyklischen algebraischen funktionenkrper, insbesondere bei endlichen konstantkrper, *J. Reine Angew. Math.* 172 (1934) 37–54. <156>

[1434] J. Hastad and M. Näslund, The security of all RSA and discrete log bits, *J. ACM* 51 (2004) 187–230. <388, 394>

[1435] P. Hawkes and G. G. Rose, Exploiting multiples of the connection polynomial in word-oriented stream ciphers, In *Advances in Cryptology—ASIACRYPT 2000*,

volume 1976 of *Lecture Notes in Comput. Sci.*, 303–316, Springer, Berlin, 2000. <319, 329>

[1436] P. Hawkes and G. G. Rose, Rewriting variables: the complexity of fast algebraic attacks on stream ciphers, In *Advances in Cryptology—CRYPTO 2004*, volume 3152 of *Lecture Notes in Comput. Sci.*, 390–406, Springer, Berlin, 2004. <241, 245>

[1437] D. R. Hayes, The distribution of irreducibles in GF[q, x], *Trans. Amer. Math. Soc.* 117 (1965) 101–127. <69, 75, 487, 492>

[1438] D. R. Hayes, The expression of a polynomial as a sum of three irreducibles, *Acta Arith.* 11 (1966) 461–488. <489, 492>

[1439] D. R. Hayes, Explicit class field theory for rational function fields, *Trans. Amer. Math. Soc.* 189 (1974) 77–91. <530, 538>

[1440] D. R. Hayes, Explicit class field theory in global function fields, In *Studies in Algebra and Number Theory*, volume 6 of *Adv. in Math. Suppl. Stud.*, 173–217, Academic Press, New York, 1979. <530, 538>

[1441] D. R. Hayes, A brief introduction to Drinfeld modules, In *The Arithmetic of Function Fields*, volume 2 of *Ohio State Univ. Math. Res. Inst. Publ.*, 1–32, de Gruyter, Berlin, 1992. <528, 538>

[1442] L. S. Heath and N. A. Loehr, New algorithms for generating Conway polynomials over finite fields, *J. Symbolic Comput.* 38 (2004) 1003–1024. <395, 397>

[1443] D. R. Heath-Brown, Arithmetic applications of Kloosterman sums, *Nieuw Arch. Wiskd. (5)* 1 (2000) 380–384. <148, 155>

[1444] D. R. Heath-Brown and S. Konyagin, New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum, *Q. J. Math.* 51 (2000) 221–235. <135, 155, 167, 170, 179>

[1445] D. R. Heath-Brown and S. J. Patterson, The distribution of Kummer sums at prime arguments, *J. Reine Angew. Math.* 310 (1979) 111–130. <144, 155>

[1446] A. Hedayat, D. Raghavarao, and E. Seiden, Further contributions to the theory of F-squares design, *Ann. Statist.* 3 (1975) 712–716. <544, 547>

[1447] A. S. Hedayat, N. J. A. Sloane, and J. Stufken, *Orthogonal Arrays, Theory and Applications*, Springer Series in Statistics. Springer-Verlag, New York, 1999. <601, 610, 622, 633>

[1448] A. Hefez, On the value sets of special polynomials over finite fields, *Finite Fields Appl.* 2 (1996) 337–347. <228, 229>

[1449] L. Heffter, Ueber Tripelsysteme, *Math. Ann.* 49 (1897) 101–112. <583, 590>

[1450] H. Heilbronn, Lecture Notes on Additive Number Theory mod p, *California Institute of Technology* (1964). <206, 207>

[1451] R. Heindl, *New Directions in Multivariate Public Key Cryptography*, PhD dissertation, Clemson University, 2009, `http://etd.lib.clemson.edu/documents/1247508584/`. <766, 774>

[1452] J. Heintz and M. Sieveking, Absolute primality of polynomials is decidable in random polynomial time in the number of variables, In *Automata, Languages and Programming*, volume 115 of *Lecture Notes in Comput. Sci.*, 16–28, Springer-Verlag, 1981. <380, 385>

[1453] H. A. Helfgott, Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, *Ann. of Math., 2nd Ser.* 167 (2008) 601–623. <185, 186>

[1454] H. A. Helfgott, Growth in $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$, *J. Eur. Math. Soc. (JEMS)* 13 (2011) 761–851. <185, 186>

[1455] H. A. Helfgott and M. Rudnev, An explicit incidence theorem in $\mathbb{F}_p$, *Mathematika* 57 (2011) 135–145. <185, 186>

[1456] H. A. Helfgott and A. Seress, On the diameter of permutation groups, *arXiv:1109.3550*. <185, 186>

[1457] T. Helleseth, Some results about the cross-correlation function between two maximal linear sequences, *Discrete Math.* 16 (1976) 209–232. <253, 254, 313, 317>

[1458] T. Helleseth, On the covering radius of cyclic linear codes and arithmetic codes, *Discrete Appl. Math.* 11 (1985) 157–173. <170, 179>

[1459] T. Helleseth, H. D. L. Hollmann, A. Kholosha, Z. Wang, and Q. Xiang, Proofs of two conjectures on ternary weakly regular bent functions, *IEEE Trans. Inform. Theory* 55 (2009) 5272–5283. <263, 265>

[1460] T. Helleseth and A. Kholosha, Monomial and quadratic bent functions over the finite fields of odd characteristic, *IEEE Trans. Inform. Theory* 52 (2006) 2018–2032. <259, 262, 263, 265>

[1461] T. Helleseth and A. Kholosha, On the dual of monomial quadratic p-ary bent functions, In *Sequences, Subsequences, and Consequences*, volume 4893 of *Lecture Notes in Comput. Sci.*, 50–61, Springer, Berlin, 2007. <263, 265>

[1462] T. Helleseth and A. Kholosha, New binomial bent functions over the finite fields of odd characteristic, *IEEE Trans. Inform. Theory* 56 (2010) 4646–4652. <263, 265>

[1463] T. Helleseth and A. Kholosha, Crosscorrelation of m-sequences, exponential sums, bent functions and Jacobsthal sums, *Cryptogr. Commun.* 3 (2011) 281–291. <264, 265>

[1464] T. Helleseth, A. Kholosha, and S. Mesnager, Niho bent functions and Subiaco hyperovals, In *Finite Fields and Applications*, volume 579 of *Contemporary Mathematics*, American Mathematical Society, Providence, RI, 2012. <261, 262, 265>

[1465] T. Helleseth and P. V. Kumar, Sequences with low correlation, In *Handbook of Coding Theory, Vol. I, II*, 1765–1853, North-Holland, Amsterdam, 1998. <200, 258, 265, 310, 312, 313, 314, 315, 317>

[1466] T. Helleseth and P. V. Kumar, Pseudonoise sequences, In J. D. Gibson, editor, *The Mobile Communications Handbook*, The electrical engineering handbook series, chapter 8, CRC Press, London, second edition, 1999. <310, 317>

[1467] T. Helleseth, P. V. Kumar, and H. Martinsen, A new family of ternary sequences with ideal two-level autocorrelation function, *Des. Codes Cryptogr.* 23 (2001) 157–166. <594, 598>

[1468] T. Helleseth, P. V. Kumar, and K. Yang, editors, *Sequences and Their Applications*, Discrete Mathematics and Theoretical Computer Science, Springer-Verlag, London, 2002. <30>

[1469] T. Helleseth, C. Rong, and D. Sandberg, New families of almost perfect nonlinear power mappings, *IEEE Trans. Inform. Theory* 45 (1999) 474–485. <220, 222, 249, 254>

[1470] T. Helleseth, D. Sarwate, H.-Y. Song, and K. Yang, editors, *Sequences and Their Applications*, volume 3486 of *Lecture Notes in Comput. Sci.*, Springer, Berlin, 2005. <30>

[1471] T. Helleseth and V. Zinoviev, New Kloosterman sums identities over $\mathbb{F}_{2^m}$ for all m, *Finite Fields Appl.* 9 (2003) 187–193. <219, 222>

[1472] M. Henderson, A note on the permutation behaviour of the Dickson polynomials of

the second kind, *Bull. Austral. Math. Soc.* 56 (1997) 499–505. <219, 222>

[1473] M. Henderson and R. Matthews, Permutation properties of Chebyshev polynomials of the second kind over a finite field, *Finite Fields Appl.* 1 (1995) 115–125. <219, 222>

[1474] M. Henderson and R. Matthews, Dickson polynomials of the second kind which are permutation polynomials over a finite field, *New Zealand J. Math.* 27 (1998) 227–244. <219, 222>

[1475] B. Hendrickson and E. Rothberg, Improving the run time and quality of nested dissection ordering, *SIAM J. Sci. Comput.* 20 (1998) 468–489. <525, 527>

[1476] K. Hensel, Über die Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor, *J. Reine Angew. Math.* 103 (1888) 230–237. <104, 106, 110>

[1477] I. R. Hentzel and I. F. Rúa, Primitivity of finite semifields with 64 and 81 elements, *Internat. J. Algebra Comput.* 17 (2007) 1411–1429. <270>

[1478] C. Hering, Eine nicht-desarguessche zweifach transitive affine Ebene der Ordnung 27, *Abh. Math. Sem. Univ. Hamburg* 34 (1969/1970) 203–208. <560, 565>

[1479] J. R. Heringa, H. W. J. Blöte, and A. Compagner, New primitive trinomials of Mersenne-exponent degrees for random-number generation, *Internat. J. Modern Phys. C* 3 (1992) 561–564. <91, 93>

[1480] F. Hernando and G. McGuire, Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions, *Journal of Algebra* 343 (2011) 78–92. <253, 254>

[1481] M. Herrmann and G. Leander, A practical key recovery attack on Basic $\mathcal{TCH}o$, In *Public Key Cryptography—PKC 2009*, volume 5443 of *Lecture Notes in Comput. Sci.*, 411–424, Springer, Berlin, 2009. <621, 633>

[1482] F. Hess, Pairing lattices, In S. D. Galbraith and K. Paterson, editors, *Pairing-Based Cryptography—Pairing 2008*, volume 5209 of *Lecture Notes in Comput. Sci.*, 18–38, Springer-Verlag, Berlin, 2008. <782, 787>

[1483] F. Hess and I. E. Shparlinski, On the linear complexity and multidimensional distribution of congruential generators over elliptic curves, *Des. Codes Cryptogr.* 35 (2005) 111–117. <327, 329>

[1484] F. Hess, N. P. Smart, and F. Vercauteren, The eta pairing revisited, *IEEE Transactions on Information Theory* 52 (2006) 4595–4602. <782, 787>

[1485] A. E. Heydtmann, Sudan-decoding generalized geometric Goppa codes, *Finite Fields Appl.* 9 (2003) 267–285. <699, 703>

[1486] K. Hicks, G. Mullen, J. Yucas, and R. Zavislak, A polynomial analogue of the $3n+1$ problem, *Amer. Math. Monthly* 115 (2008) 615–622. <492>

[1487] J. Hietarinta and C. Viallet, Searching for integrable lattice maps using factorization, *J. Phys. A* 40 (2007) 12629–12643. <330, 331, 337>

[1488] D. Hilbert, Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten, *JFRAM* 110 (1892) 104–129. <379, 385>

[1489] D. Hilbert, Beweis fur die darstellbarkeit der ganzen kahlen durch eine feste anzahl nter potenzen (waringsches problem), *Math. Ann.* 67 (1909) 281–300. <490, 492>

[1490] A. Hildebrand and G. Tenenbaum, Integers without large prime factors, *J. Théor. Nombres Bordeaux* 5 (1993) 411–484. <392, 394>

[1491] F. Hinkelmann, M. Brandon, B. Guang, R. McNeill, A. Veliz-Cuba, G. Blekherman, and R. Laubenbacher, Adam: Analysis of analysis of dynamic algebraic models,

Available at http:/adam.vbi.vt.edu/, 2010. <817, 820, 822, 824>

[1492] F. Hinkelmann and A. S. Jarrah, Inferring biologically relevant models: Nested canalyzing functions, *ISRN Biomathematics, to appear* (2012). <824>

[1493] F. Hinkelmann and R. Laubenbacher, Boolean models of bistable biological systems, *Discrete Contin. Dyn. Syst. Ser. S* 4 (2011) 1443–1456. <817, 824>

[1494] F. Hinkelmann, D. Murrugarra, A. Jarrah, and R. Laubenbacher, A mathematical framework for agent based models of complex biological networks, *Bulletin of Mathematical Biology* (2010) 1–20, 10.1007/s11538-010-9582-8. <817, 821, 824>

[1495] Y. Hiramine, A conjecture on affine planes of prime order, *J. Combin. Theory, Ser. A* 52 (1989) 44–50. <273, 274>

[1496] Y. Hiramine, On planar functions, *J. Algebra* 133 (1990) 103–110. <274>

[1497] Y. Hiramine, M. Matsumoto, and T. Oyama, On some extension of 1-spread sets, *Osaka J. Math.* 24 (1987) 123–137. <269, 270, 558, 565>

[1498] J. W. P. Hirschfeld, *Finite Projective Spaces of Three Dimensions*, Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1985. <29, 30, 571, 579, 580>

[1499] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, second edition, 1998. <29, 30, 555, 561, 563, 565, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 580>

[1500] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic Curves over a Finite Field*, Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ, 2008. <29, 30, 399, 415, 455, 456, 575, 577, 578, 580>

[1501] J. W. P. Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces, *J. Statist. Plann. Inference* 72 (1998) 355–380. <575, 577, 580>

[1502] J. W. P. Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces: update 2001, In *Finite Geometries*, volume 3 of *Dev. Math.*, 201–246, Kluwer Acad. Publ., Dordrecht, 2001. <565, 575, 577, 580>

[1503] J. W. P. Hirschfeld, L. Storme, J. A. Thas, and J. F. Voloch, A characterization of Hermitian curves, *J. Geom.* 41 (1991) 72–78. <202, 207>

[1504] J. W. P. Hirschfeld and J. A. Thas, *General Galois Geometries*, Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1991. <29, 30, 558, 565, 575, 577, 580>

[1505] A. Hocquenghem, Codes correcteurs d'erreurs, *Chiffres* 2 (1959) 147–156. <669, 693, 694>

[1506] J. H. Hodges, The matrix equation $X^2 - I = 0$ over a finite field, *Amer. Math. Monthly* 65 (1958) 518–520. <494, 502>

[1507] M. van Hoeij, Factoring polynomials and the knapsack problem, *J. Number Theory* 95 (2002) 167–189. <378, 385>

[1508] J. van der Hoeven and G. Lecerf, On the bit-complexity of sparse polynomial and series multiplication, Manuscript available from `http://hal.archives-ouvertes.fr/hal-00476223/fr`, 2010. <375, 380, 385>

[1509] E. Hof and S. Shamai, Secrecy-achieving polar-coding for binary-input memoryless symmetric wire-tap channels, preprint, 2010. <730>

[1510] J. Hoffstein, J. Pipher, and J. H. Silverman, *An Introduction to Mathematical Cryp-*

tography, Undergraduate Texts in Mathematics. Springer, New York, 2008. <29, 30, 740>

[1511] T. Høholdt, Personal communication, 2011. <674, 694>

[1512] T. Høholdt and H. E. Jensen, Determination of the merit factor of Legendre sequences, *IEEE Trans. Inform. Theory* 34 (1988) 161–164. <316, 317, 832, 839>

[1513] T. Høholdt and R. Pellikaan, On the decoding of algebraic-geometric codes, *IEEE Trans. Inform. Theory* 41 (1995) 1589–1614. <696, 703>

[1514] T. Høholdt, J. H. van Lint, and R. Pellikaan, Algebraic geometry codes, In *Handbook of Coding Theory, Vol. I, II*, 871–961, North-Holland, Amsterdam, 1998. <693, 694>

[1515] H. D. L. Hollmann and Q. Xiang, A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences, *Finite Fields Appl.* 7 (2001) 253–286. <254>

[1516] H. D. L. Hollmann and Q. Xiang, A class of permutation polynomials of $\mathbf{F}_{2^m}$ related to Dickson polynomials, *Finite Fields Appl.* 11 (2005) 111–122. <220, 222>

[1517] S. Hong, Newton polygons of L functions associated with exponential sums of polynomials of degree four over finite fields, *Finite Fields Appl.* 7 (2001) 205–237. <477, 480>

[1518] S. Hong, Newton polygons for L-functions of exponential sums of polynomials of degree six over finite fields, *J. Number Theory* 97 (2002) 368–396. <477, 480>

[1519] I. Honkala and A. Tietäväinen, Codes and number theory, In *Handbook of Coding Theory, Vol. II*, 1141–1194, North-Holland, Amsterdam, 1998. <693, 694>

[1520] C. Hooley, On Artin's conjecture, *J. Reine Angew. Math.* 225 (1967) 209–220. <68, 69>

[1521] C. Hooley, On exponential sums and certain of their applications, In *Number Theory Days*, volume 56 of *London Math. Soc. Lecture Note Ser.*, 92–122, Cambridge Univ. Press, Cambridge, 1982. <158, 163>

[1522] C. Hooley, On the number of points on a complete intersection over a finite field, *J. Number Theory* 38 (1991) 338–358. <189, 195>

[1523] S. Hoory, A lower bound on the spectral radius of the universal cover of a graph, *J. Combin. Theory, Ser. B* 93 (2005) 33–43. <639, 649>

[1524] S. Hoory, N. Linial, and A. Wigderson, Expander graphs and their applications, *Bull. Amer. Math. Soc. (New Ser.)* 43 (2006) 439–561. <633, 634, 638, 640, 649>

[1525] K. J. Horadam, *Hadamard Matrices and Their Applications*, Princeton University Press, Princeton, NJ, 2007. <164, 179>

[1526] J. D. Horton, Orthogonal starters in finite abelian groups, *Discrete Math.* 79 (1990) 265–278. <605, 610>

[1527] A. Hoshi, Explicit lifts of quintic Jacobi sums and period polynomials for $\mathbb{F}_q$, *Proc. Japan Acad., Ser. A, Math. Sci.* 82 (2006) 87–92. <135, 143, 155>

[1528] X.-D. Hou, p-ary and q-ary versions of certain results about bent functions and resilient functions, *Finite Fields Appl.* 10 (2004) 566–582. <257, 265>

[1529] X.-D. Hou, A note on the proof of a theorem of Katz, *Finite Fields Appl.* 11 (2005) 316–319. <193, 195, 207>

[1530] X.-D. Hou, Affinity of permutations of $\mathbb{F}_2^n$, *Discrete Appl. Math.* 154 (2006) 313–325. <222, 249, 254>

[1531] X.-D. Hou, Two classes of permutation polynomials over finite fields, *J. Combin. Theory, Ser. A* 118 (2011) 448–454. <220, 222>

[1532] X.-D. Hou, Classification of self dual quadratic bent functions, *Des. Codes Cryptogr.* 63 (2012) 183–198. <256, 265>

[1533] X.-D. Hou and T. Ly, Necessary conditions for reversed Dickson polynomials to be permutational, *Finite Fields Appl.* 16 (2010) 436–448. <220, 222>

[1534] X.-D. Hou and G. L. Mullen, Number of irreducible polynomials and pairs of relatively prime polynomials in several variables over finite fields, *Finite Fields Appl.* 15 (2009) 304–331. <76, 77, 78, 81>

[1535] X.-D. Hou, G. L. Mullen, J. A. Sellers, and J. L. Yucas, Reversed Dickson polynomials over finite fields, *Finite Fields Appl.* 15 (2009) 748–773. <219, 220, 222>

[1536] X.-D. Hou and C. Sze, On certain diagonal equations over finite fields, *Finite Fields Appl.* 15 (2009) 633–643. <202, 207>

[1537] E. Howe and K. Lauter, Improved upper bounds for the number of points on curves over finite fields, *Ann. Inst. Fourier (Grenoble)* 53 (2003) 1677–1737. <453, 456>

[1538] E. Howe, K. Lauter, C. Ritzenthaler, and G. van der Geer, manYPoints - table of curves with many points, *http://www.manypoints.org/.* <453, 456>

[1539] C.-N. Hsu, The distribution of irreducible polynomials in $\mathbf{F}_q[t]$, *J. Number Theory* 61 (1996) 85–96. <72, 75>

[1540] M.-D. A. Huang, Factorization of polynomials over finite fields and factorization of primes in algebraic number fields, In *Proceedings of the Sixteenth Annual ACM Symposium on Theory of Computing,* Washington DC, 175–182. ACM Press, 1984. <374, 375>

[1541] M.-D. A. Huang, Riemann hypothesis and finding roots over finite fields, In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing,* Providence RI, 121–130. ACM Press, 1985. <374, 375>

[1542] X. Huang and V. Y. Pan, Fast rectangular matrix multiplication and applications, *Journal of Complexity* 14 (1998) 257–299. <373, 375>

[1543] H. Hubrechts, Point counting in families of hyperelliptic curves in characteristic 2, *LMS J. Comput. Math.* 10 (2007) 207–234. <447, 449>

[1544] H. Hubrechts, Point counting in families of hyperelliptic curves, *Found. Comput. Math.* 8 (2008) 137–169. <447, 449, 484>

[1545] S. Huczynska and S. D. Cohen, Primitive free cubics with specified norm and trace, *Trans. Amer. Math. Soc.* 355 (2003) 3099–3116 (electronic). <84, 85, 87, 89, 90>

[1546] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003. <29, 30, 652, 654, 663, 665, 668, 669, 672, 673, 694>

[1547] D. R. Hughes, On t-designs and groups, *Amer. J. Math.* 87 (1965) 761–778. <589, 590>

[1548] D. R. Hughes and F. C. Piper, *Projective Planes*, Springer-Verlag, New York, 1973, Graduate Texts in Mathematics, Vol. 6. <26, 29, 30, 266, 270, 555, 565, 570, 580>

[1549] T. W. Hungerford, *Algebra*, volume 73 of *Graduate Texts in Mathematics*, Springer-Verlag, New York-Berlin, 1980, Reprint of the 1974 original. <75, 81>

[1550] N. E. Hurt, Exponential sums and coding theory: a review, *Acta Appl. Math.* 46

(1997) 49–91. <148, 155>

[1551] D. Husemöller, *Elliptic Curves*, volume 111 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, second edition, 2004. <29, 30, 416, 433>

[1552] H.-K. Hwang, A Poisson $*$ negative binomial convolution law for random polynomials over finite fields, *Random Structures Algorithms* 13 (1998) 17–47. <361, 367>

[1553] J. Y. Hyun, H. Lee, and Y. Lee, MacWilliams duality and a Gleason-type theorem on self-dual bent functions, *Des. Codes Cryptogr.* 63 (2012) 295–304. <256, 265>

[1554] T. Icart, How to hash into elliptic curves, In S. Halevi, editor, *Advances in Cryptology—CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, 303–316, Springer-Verlag, Berlin, 2009. <787>

[1555] IEEE, Standard specifications for public key cryptography, Standard P1363-2000, Institute of Electrical and Electronics Engineering, 2000, Draft D13 available at `http://grouper.ieee.org/groups/1363/P1363/draft.html`. <63, 64, 66, 776, 787>

[1556] Y. Ihara, On discrete subgroups of the two by two projective linear group over p-adic fields, *J. Math. Soc. Japan* 18 (1966) 219–235. <649>

[1557] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 28 (1981) 721–724. <454, 456, 457, 462>

[1558] L. Illusie, *Cohomologie l-adique et Fonctions L*, Lecture Notes in Mathematics, Vol. 589. Springer-Verlag, Berlin, 1977, Séminaire de Géometrie Algébrique du Bois-Marie 1965–1966 (SGA 5), Edité par Luc Illusie. <30, 463, 464, 467, 471, 472>

[1559] L. Illusie, Ordinarité des intersections complètes générales, In *The Grothendieck Festschrift, Vol. II*, volume 87 of *Progr. Math.*, 376–405, Birkhäuser Boston, Boston, MA, 1990. <476, 480>

[1560] L. Illusie, Crystalline cohomology, In *Motives*, volume 55 of *Proc. Sympos. Pure Math.*, 43–70, Amer. Math. Soc., Providence, RI, 1994. <472>

[1561] K. Imamura, On self-complementary bases of $GF(q^n)$ over GF(q)., *Trans. IECE Japan, E* 66 (1983) 717–721. <97, 98, 103>

[1562] K. Imamura and M. Morii, Two classes of finite fields which have no self-complementary normal bases, In *1985 IEEE International Symposium on Information Theory Proceedings (ISIT)*, Brighton, England, 1985. <108, 110>

[1563] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, volume 84 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, second edition, 1990. <200, 207>

[1564] T. Itoh and S. Tsujii, A fast algorithm for computing multiplicative inverses in GF(2^m) using normal bases, *Inform. and Comput.* 78 (1988) 171–177. <353, 356, 809, 813>

[1565] I. D. Ivanović, Geometrical description of quantal state determination, *J. Phys. A* 14 (1981) 3241–3245. <825, 831>

[1566] G. Ivanyos, M. Karpinski, L. Rónyai, and N. Saxena, Trading GRH for algebra: Algorithms for factoring polynomials and related structures, *Mathematics of Computation* 81 (2012) 493–531. <374, 375>

[1567] G. Ivanyos, M. Karpinski, and N. Saxena, Schemes for deterministic polynomial factoring, In *Proceedings of the 2009 International Symposium on Symbolic*

and Algebraic Computation, ISSAC '09, 191–198, ACM, New York, NY, USA, 2009. <374, 375>

[1568] H. Iwaniec, *Topics in Classical Automorphic Forms*, volume 17 of *Graduate Studies in Mathematics*, American Mathematical Society, Providence, RI, 1997. <151, 155>

[1569] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, volume 53 of *American Mathematical Society Colloquium Publications*, American Mathematical Society, Providence, RI, 2004. <134, 148, 150, 151, 154, 155, 175, 179>

[1570] F. Izadi, C_{ab} curves and arithmetic on their Jacobians, In *Algebraic Curves and Cryptography*, volume 58 of *Fields Inst. Commun.*, 99–118, Amer. Math. Soc., Providence, RI, 2010. <798, 802>

[1571] F. Jacob and J. Monod, Genetic regulatory mechanisms in the synthesis of proteins, *Journal of Molecular Biology* 3 (1961) 318–356. <817, 824>

[1572] C. G. J. Jacobi, Uber die kreistheilung und ihre anwendung auf die zahlentheorie, *Gesammelte Werke* 6 (1846) 254–274. <25, 30>

[1573] M. Jacobson, A. Menezes, and A. Stein, Solving elliptic curve discrete logarithm problems using Weil descent, *J. Ramanujan Math. Soc.* 16 (2001) 231–260. <801, 802>

[1574] M. Jacobson, Jr., A. Menezes, and A. Stein, Hyperelliptic curves and cryptography, In *High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams*, volume 41 of *Fields Inst. Commun.*, 255–282, Amer. Math. Soc., Providence, RI, 2004. <445, 448, 449>

[1575] M. Jacobson, Jr., R. Scheidler, and A. Stein, Cryptographic aspects of real hyperelliptic curves, *Tatra Mt. Math. Publ.* 47 (2010) 31–65. <441, 446, 449>

[1576] M. J. Jacobson, Jr., R. Scheidler, and A. Stein, Fast arithmetic on hyperelliptic curves via continued fraction expansions, In *Advances in Coding Theory and Cryptography*, volume 3 of *Ser. Coding Theory Cryptol.*, 200–243, World Sci. Publ., Hackensack, NJ, 2007. <444, 445, 446, 449>

[1577] N. Jacobson, *Basic Algebra. I*, W. H. Freeman and Company, New York, 2nd edition, 1985. <502, 503, 505, 506, 509, 510, 513>

[1578] R. Jain, Error characteristics of fiber distributed data interface (FDDI), *IEEE Transactions on Communications* 38 (1990) 1244–1252. <629, 630, 633>

[1579] K. Jambunathan, On choice of connection-polynomials for LFSR-based stream ciphers, In *Progress in Cryptology—INDOCRYPT 2000*, volume 1977 of *Lecture Notes in Comput. Sci.*, 9–18, Springer, Berlin, 2000. <624, 625, 626, 633>

[1580] N. S. James and R. Lidl, Permutation polynomials on matrices, *Linear Algebra Appl.* 96 (1987) 181–190. <219, 222>

[1581] G. J. Janusz, Separable algebras over commutative rings, *Trans. Amer. Math. Soc.* 122 (1966) 461–479. <27>

[1582] H. Janwa, G. M. McGuire, and R. M. Wilson, Double-error-correcting cyclic codes and absolutely irreducible polynomials over GF(2), *J. Algebra* 178 (1995) 665–676. <253, 254>

[1583] H. Janwa and R. M. Wilson, Hyperplane sections of Fermat varieties in $\mathbf{P}^3$ in char. 2 and some applications to cyclic codes, In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 673 of *Lecture Notes in Comput. Sci.*, 180–194, Springer, Berlin, 1993. <251, 253, 254>

[1584] A. S. Jarrah and R. Laubenbacher, On the algebraic geometry of polynomial dynamical systems, In *Emerging Applications of Algebraic Geometry*, volume 149

of *IMA Vol. Math. Appl.*, 109–123, Springer, New York, 2009. <330, 337>

[1585] A. S. Jarrah, R. Laubenbacher, B. Stigler, and M. Stillman, Reverse-engineering of polynomial dynamical systems, *Advances in Applied Mathematics* 39 (2007) 477–489. <821, 824>

[1586] A. S. Jarrah, R. Laubenbacher, and A. Veliz-Cuba, The dynamics of conjunctive and disjunctive Boolean network models, *Bull. Math. Biol.* 72 (2010) 1425–1447. <824>

[1587] A. S. Jarrah, B. Raposa, and R. Laubenbacher, Nested canalyzing, unate cascade, and polynomial functions, *Phys. D* 233 (2007) 167–174. <823, 824>

[1588] C.-P. Jeannerod and C. Mouilleron, Computing specified generators of structured matrix inverses, In W. Koepf, editor, *Proceedings of the International Symposium of Symbolic and Algebraic Computation—ISSAC 2010*, 281–288. ACM, 2010. <526, 527>

[1589] T. Jebelean, An algorithm for exact division, *J. Symbolic Comput.* 15 (1993) 169–180. <352, 356>

[1590] T. Jebelean, Improving the multiprecision Euclidean algorithm, In *Design and Implementation of Symbolic Computation Systems – DISCO 1993*, volume 722 of *Lecture Notes in Comput. Sci.*, 45–58, Springer, Berlin, 1993. <352, 356>

[1591] J. Jedwab, What can be used instead of a Barker sequence?, In *Finite Fields and Applications*, volume 461 of *Contemp. Math.*, 153–178, Amer. Math. Soc., Providence, RI, 2008. <831, 839>

[1592] J. Jedwab, D. J. Katz, and K.-U. Schmidt, Advances in the merit factor problem for binary sequences, *arXiv:1205.0626v1* (2012). <832, 839>

[1593] J. Jedwab, D. J. Katz, and K.-U. Schmidt, Littlewood polynomials with small L^4 norm, arXiv:1205.0260v1, 2012. <316, 317, 832, 839>

[1594] E. Jensen and M. R. Murty, Artin's conjecture for polynomials over finite fields, In *Number Theory*, Trends in Mathematics, 167–181, Birkhauser, Basel, 2000. <489, 492>

[1595] J. M. Jensen, H. E. Jensen, and T. Høholdt, The merit factor of binary sequences related to difference sets, *IEEE Trans. Inform. Theory* 37 (1991) 617–626. <832, 839>

[1596] V. Jha and N. L. Johnson, An analog of the Albert-Knuth theorem on the orders of finite semifields, and a complete solution to Cofman's subplane problem, *Algebras Groups Geom.* 6 (1989) 1–35. <269, 270>

[1597] V. Jha and N. L. Johnson, Nests of reguli and flocks of quadratic cones, *Simon Stevin* 63 (1989) 311–338. <559, 565>

[1598] X. Jiang, J. Ding, and L. Hu, Kipnis-Shamir attack on HFE revisited, In *Information Security and Cryptology*, volume 4990 of *Lecture Notes in Comput. Sci.*, 399–411, Springer, Berlin, 2008. <771, 774>

[1599] N. L. Johnson, Projective planes of prime order p that admit collineation groups of order p^2, *J. Geom.* 30 (1987) 49–68. <273, 274>

[1600] N. L. Johnson, Nest replaceable translation planes, *J. Geom.* 36 (1989) 49–62. <559, 565>

[1601] N. L. Johnson, V. Jha, and M. Biliotti, *Handbook of Finite Translation Planes*, volume 289 of *Pure and Applied Mathematics*, Chapman & Hall/CRC, Boca Raton, FL, 2007. <557, 565>

[1602] N. L. Johnson and R. Pomareda, André planes and nests of reguli, *Geom. Dedicata* 31 (1989) 245–260. <559, 565>

[1603] N. L. Johnson and R. Pomareda, Mixed nests, *J. Geom.* 56 (1996) 59–86. <559, 565>

[1604] S. C. Johnson, Sparse polynomial arithmetic, *ACM SIGSAM Bull.* 8 (1974) 63–71. <375, 385>

[1605] J.-R. Joly, Équations et variétés algébriques sur un corps fini, *Enseignement Math., IIe Ser.* 19 (1973) 1–117. <200, 207>

[1606] R. Jones, Iterated Galois towers, their associated martingales, and the p-adic Mandelbrot set, *Compos. Math.* 143 (2007) 1108–1126. <330, 335, 337>

[1607] R. Jones, The density of prime divisors in the arithmetic dynamics of quadratic polynomials, *J. Lond. Math. Soc., 2nd Ser.* 78 (2008) 523–544. <330, 335, 337>

[1608] R. Jones and N. Boston, Settled polynomials over finite fields, *Proc. Amer. Math. Soc.* 140 (2012) 1849–1863. <172, 179, 335, 337>

[1609] C. Jordan, *Traité des Substitutions et des Équations Algébriques*, Paris: Gauthier-Villars, 1870. <9, 10>

[1610] H. F. Jordan and D. C. M. Wood, On the distribution of sums of successive bits of shift-register sequences, *IEEE Trans. Computers* C-22 (1973) 400–408. <621, 633>

[1611] J.-P. Jouanolou, *Théorèmes de Bertini et Applications*, volume 42 of *Progress in Mathematics*, Birkhäuser Boston, 1983. <380, 385>

[1612] A. Joux, A one round protocol for tripartite Diffie-Hellman, *J. Cryptology* 17 (2004) 263–276. <737, 740>

[1613] A. Joux, Discrete logarithms in GF(2^{607}) and GF(2^{613}), mailing list announcement, `https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0509\&L=NMBRTHRY\&P=R1490\&D=0\&I=-3\&T=0`, 2005. <393, 394>

[1614] A. Joux and R. Lercier, The function field sieve is quite special, In *Algorithmic Number Theory*, volume 2369 of *Lecture Notes in Comput. Sci.*, 431–445, Springer, Berlin, 2002. <392, 394>

[1615] A. Joux and R. Lercier, Improvements to the general number field sieve for discrete logarithms in prime fields: A comparison with the Gaussian integer method, *Math. Comp.* 72 (2003) 953–967. <392, 394>

[1616] A. Joux and R. Lercier, The function field sieve in the medium prime case, In *Advances in Cryptology—EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Comput. Sci.*, 254–270, Springer, Berlin, 2006. <392, 394>

[1617] A. Joux and V. Vitse, Cover and decomposition index calculus on elliptic curves made practical—Application to a seemingly secure curve over $\mathbb{F}_{p^6}$, In *Advances in Cryptology—EUROCRYPT 2012*, volume 7237 of *Lecture Notes Comput. Sci.*, 9–26, 2011. <777, 787>

[1618] M. Joye, A. Miyaji, and A. Otsuka, editors, *Pairing-Based Cryptography — Pairing 2010*, volume 6487 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, Berlin, 2010. <779, 787>

[1619] D. Jungnickel, *Finite Fields: Structure and Arithmetics*, Bibliographisches Institut, Mannheim, 1993. <11, 29, 30, 37, 39, 46, 95, 97, 99, 100, 103, 107, 110, 111, 117, 122, 164, 177, 179, 318, 320, 321, 322, 329, 495, 496, 497, 498, 502>

[1620] D. Jungnickel, Trace-orthogonal normal bases, *Discrete Appl. Math.* 47 (1993) 233–249. <117, 122>

[1621] D. Jungnickel, T. Beth, and W. Geiselmann, A note on orthogonal circulant matrices over finite fields, *Arch. Math. (Basel)* 62 (1994) 126–133. <498, 502>

[1622] D. Jungnickel and M. J. de Resmini, Another case of the prime power conjecture for finite projective planes, *Adv. Geom.* 2 (2002) 215–218. <564, 565>

[1623] D. Jungnickel, A. J. Menezes, and S. A. Vanstone, On the number of self-dual bases of GF(q^m) over GF(q), *Proc. Amer. Math. Soc.* 109 (1990) 23–29. <98, 103, 109, 110>

[1624] D. Jungnickel and H. Niederreiter, editors, *Finite Fields and Applications*, Springer-Verlag, Berlin, 2001. <30>

[1625] D. Jungnickel and S. A. Vanstone, On primitive polynomials over finite fields, *J. Algebra* 124 (1989) 337–353. <87, 90>

[1626] J. Justesen, A class of constructive asymptotically good algebraic codes, *IEEE Trans. Information Theory* IT-18 (1972) 652–656. <680, 693, 694>

[1627] J. Justesen and T. Høholdt, *A Course in Error-Correcting Codes*, EMS Textbooks in Mathematics. European Mathematical Society (EMS), Zürich, 2004. <652, 694>

[1628] V. Kabanets and R. Impagliazzo, Derandomizing polynomial identity tests means proving circuit lower bounds, *Comput. Complexity* 13 (2004) 1–46. <384, 385>

[1629] N. Kahale, Isoperimetric inequalities and eigenvalues, *SIAM J. Discrete Math.* 10 (1997) 30–40. <636, 649>

[1630] T. Kaida, S. Uehara, and K. Imamura, An algorithm for the k-error linear complexity of sequences over GF(p^m) with period p^n, p a prime, *Inform. and Comput.* 151 (1999) 134–147. <322, 329>

[1631] T. Kailath, S. Y. Kung, and M. Morf, Displacement ranks of a matrix, *Bull. Amer. Math. Soc. (New Ser.)* 1 (1979) 769–773. <525, 527>

[1632] B. S. Kaliski, Jr., The Montgomery inverse and its applications, *IEEE Trans. on Computers* 44 (1995) 1064–1065. <353, 356>

[1633] E. Kaltofen, A polynomial reduction from multivariate to bivariate integral polynomial factorization, In *Proceedings of the Fourteenth Symposium on Theory of Computing*, 261–266. ACM, 1982. <380, 385>

[1634] E. Kaltofen, A polynomial-time reduction from bivariate to univariate integral polynomial factorization, In *Proc. Twenty Third TwentAnnual Symp. Foundations of Comp. Sci.*, 57–64. IEEE, 1982. <374, 375, 380, 385>

[1635] E. Kaltofen, Effective Hilbert irreducibility, *Information and Control* 66 (1985) 123–137. <380, 385>

[1636] E. Kaltofen, Fast parallel absolute irreducibility testing, *J. Symbolic Comput.* 1 (1985) 57–67. <380, 385>

[1637] E. Kaltofen, Sparse Hensel lifting, In *Proceedings of EUROCAL '85, Vol. 2*, volume 204 of *Lecture Notes in Comput. Sci.*, 4–17, Springer-Verlag, 1985. <380, 384, 385>

[1638] E. Kaltofen, Uniform closure properties of p-computable functions, In *Proc. Eighteenth Annual ACM Symp. Theory Comput.*, 330–337, 1986, also published as part of [1640] and [1641]. <383, 384, 385>

[1639] E. Kaltofen, Deterministic irreducibility testing of polynomials over large finite fields, *J. Symbolic Comput.* 4 (1987) 77–82. <380, 385>

[1640] E. Kaltofen, Greatest common divisors of polynomials given by straight-line programs, *J. ACM* 35 (1988) 231–264. <926>

[1641] E. Kaltofen, Factorization of polynomials given by straight-line programs, In S. Micali, editor, *Randomness and Computation*, volume 5 of *Advances in Computing Research*, 375–412, JAI Press Inc., Greenwhich, Connecticut, 1989. <383, 384,

385, 926>

[1642] E. Kaltofen, Polynomial factorization 1982-1986, In D. V. Chudnovsky and R. D. Jenks, editors, *Computers in Mathematics*, volume 125 of *Lecture Notes in Pure and Applied Mathematics*, 285–309, Marcel Dekker, New York, NY, 1990. <380, 385>

[1643] E. Kaltofen, Polynomial factorization 1987-1991, In I. Simon, editor, *Proc. LATIN '92*, volume 583 of *Lect. Notes Comput. Sci.*, 294–313. Springer-Verlag, 1992. <374, 375, 380, 385>

[1644] E. Kaltofen, Asymptotically fast solution of Toeplitz-like singular linear systems, In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, ISSAC '94, 297–304, ACM, New York, NY, USA, 1994. <526, 527>

[1645] E. Kaltofen, Analysis of Coppersmith's block Wiedemann algorithm for the parallel solution of sparse linear systems, *Math. Comp.* 64 (1995) 777–806. <527>

[1646] E. Kaltofen, Effective Noether irreducibility forms and applications, *J. Comput. System Sci.* 50 (1995) 274–295. <379, 386>

[1647] E. Kaltofen, Polynomial factorization: a success story, In *ISSAC '03: Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, 3–4. ACM, 2003. <380, 386>

[1648] E. Kaltofen and P. Koiran, On the complexity of factoring bivariate supersparse (lacunary) polynomials, In *ISSAC '05: Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation*, 208–215. ACM, 2005. <383, 386>

[1649] E. Kaltofen and P. Koiran, Finding small degree factors of multivariate supersparse (lacunary) polynomials over algebraic number fields, In *ISSAC '06: Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation*, 162–168. ACM, 2006. <383, 386>

[1650] E. Kaltofen and W. Lee, Early termination in sparse interpolation algorithms, *J. Symbolic Comput.* 36 (2003) 365–400. <385, 386>

[1651] E. Kaltofen and A. Lobo, Factoring high-degree polynomials by the black box Berlekamp algorithm, Technical report, Department of Computer Science, Rensselaer Polytechnic Institute, 1994. <374, 375>

[1652] E. Kaltofen and A. Lobo, Distributed matrix-free solution of large sparse linear systems over finite fields, *Algorithmica* 24 (1999) 331–348. <522, 527>

[1653] E. Kaltofen and V. Pan, Parallel solution of Toeplitz and Toeplitz-like linear systems over fields of small positive characteristic, In *First International Symposium on Parallel Symbolic Computation—PASCO '94*, volume 5 of *Lecture Notes Ser. Comput.*, 225–233, World Sci. Publ., River Edge, NJ, 1994. <501, 502>

[1654] E. Kaltofen and B. D. Saunders, On Wiedemann's method of solving sparse linear systems, In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 539 of *Lecture Notes in Comput. Sci.*, 29–38, Springer, Berlin, 1991. <523, 526, 527>

[1655] E. Kaltofen and V. Shoup, Subquadratic-time factoring of polynomials over finite fields, *Math. Comp.* 67 (1998) 1179–1197. <361, 367, 369, 373, 374, 375>

[1656] E. Kaltofen and B. Trager, Computing with polynomials given by black boxes for their evaluations: Greatest common divisors, factorization, separation of numerators and denominators, In *Proc. Twenty Ninth Annual Symp. Foundations of Comp. Sci.*, 296–305. IEEE, 1988. <384, 386>

[1657] E. Kaltofen and B. Trager, Computing with polynomials given by black boxes

for their evaluations: Greatest common divisors, factorization, separation of numerators and denominators, *J. Symbolic Comput.* 9 (1990) 301–320. <384, 385, 386, 522, 527>

[1658] E. Kaltofen and G. Villard, On the complexity of computing determinants, *Comput. Complexity* 13 (2004) 91–130. <384, 386, 527>

[1659] N. Kamiya, On multisequence shift register synthesis and generalized-minimum-distance decoding of Reed-Solomon codes, *Finite Fields Appl.* 1 (1995) 440–457. <322, 329>

[1660] J.-G. Kammerer, R. Lercier, and G. Renault, Encoding points on hyperelliptic curves over finite fields in deterministic polynomial time, In M. Joye, A. Miyaji, and A. Otsuka, editors, *Pairing-Based Cryptography—Pairing 2010*, volume 6487 of *Lecture Notes in Computer Science*, 278–297, Springer-Verlag, Berlin, 2010. <787>

[1661] W. M. Kantor, An exponential number of generalized Kerdock codes, *Inform. and Control* 53 (1982) 74–80. <244, 245>

[1662] W. M. Kantor, Two families of flag-transitive affine planes, *Geom. Dedicata* 41 (1992) 191–200. <560, 565>

[1663] W. M. Kantor, 2-transitive and flag-transitive designs, In *Coding Theory, Design Theory, Group Theory*, Wiley-Intersci. Publ., 13–30, Wiley, New York, 1993. <560, 565>

[1664] W. M. Kantor, Note on GMW designs, *European J. Combin.* 22 (2001) 63–69. <594, 598>

[1665] W. M. Kantor, Commutative semifields and symplectic spreads, *J. Algebra* 270 (2003) 96–114. <270>

[1666] W. M. Kantor, Finite semifields, In *Finite Geometries, Groups, and Computation*, 103–114, de Gruyter, Berlin, 2006. <270>

[1667] W. M. Kantor, HMO-planes, *Adv. Geom.* 9 (2009) 31–43. <269, 270>

[1668] W. M. Kantor and R. A. Liebler, Semifields arising from irreducible semilinear transformations, *J. Aust. Math. Soc.* 85 (2008) 333–339. <269, 270>

[1669] W. M. Kantor and C. Suetake, A note on some flag-transitive affine planes, *J. Combin. Theory, Ser. A* 65 (1994) 307–310. <560, 565>

[1670] W. M. Kantor and M. E. Williams, Symplectic semifield planes and $\mathbb{Z}_4$-linear codes, *Trans. Amer. Math. Soc.* 356 (2004) 895–938. <269, 270>

[1671] A. A. Karatsuba, The complexity of computations, *Trudy Mat. Inst. Steklov.* 211 (1995) 186–202. <348, 356>

[1672] A. A. Karatsuba and Y. Ofman, Multiplication of multiplace numbers on automata, *Dokl. Acad. Nauk SSSR* 145 (1962) 293–294, English translation in Soviet Physics-Doklady 7, 595–596,1963. <347, 348, 356, 373, 375, 804, 813>

[1673] M. Karzand and E. Telatar, Polar codes for q-ary source coding, In *Proc. IEEE International Symposium on Information Theory*, 909–912, 2010. <730>

[1674] M. Kasahara and R. Sakai, A construction of public key cryptosystem for realizing ciphtertext of size 100 bit and digital signature scheme, *IEICE Trans. Fundamentals* E87-A (2004) 102–109. <762, 774>

[1675] M. Kasahara and R. Sakai, A construction of public-key cryptosystem based on singular simultaneous equations, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* E88-A (2005) 74–80. <762, 774>

[1676] T. Kasami, Weight distributions of Bose-Chaudhuri-Hocquenghem codes, In *Com-*

binatorial Mathematics and its Applications, 335–357, Univ. North Carolina Press, Chapel Hill, N.C., 1969. <251, 254, 314, 317>

[1677] T. Kasami, The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes, *Information and Control* 18 (1971) 369–394. <251, 252, 254>

[1678] T. Kasami, S. Lin, and W. W. Peterson, Generalized Reed-Muller codes, *Electron. Commun. Japan* 51 (1968) 96–104. <677, 679, 680, 694>

[1679] T. Kasami, S. Lin, and W. W. Peterson, Polynomial codes, *IEEE Trans. Information Theory* IT-14 (1968) 807–814. <679, 680, 694>

[1680] T. Kasimi, The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes, *Inform. and Control* 18 (1971) 369–394. <220, 222>

[1681] M. Kassabov, A. Lubotzky, and N. Nikolov, Finite simple groups as expanders, *Proc. Natl. Acad. Sci. USA* 103 (2006) 6116–6119. <643, 649>

[1682] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, Chapman & Hall/CRC Cryptography and Network Security. Chapman & Hall/CRC, Boca Raton, FL, 2008. <29, 30, 740>

[1683] N. Katz and R. Livné, Sommes de Kloosterman et courbes elliptiques universelles en caractéristiques 2 et 3, *C. R. Acad. Sci. Paris, Sér. I, Math.* 309 (1989) 723–726. <263, 265>

[1684] N. H. Katz and C.-Y. Shen, Garaev's inequality in finite fields not of prime order, *Online J. Anal. Comb.* (2008) Art. 3, 6. <181, 186>

[1685] N. H. Katz and C.-Y. Shen, A slight improvement to Garaev's sum product estimate, *Proc. Amer. Math. Soc.* 136 (2008) 2499–2504. <186>

[1686] N. M. Katz, On a theorem of Ax, *Amer. J. Math.* 93 (1971) 485–499. <193, 195, 204, 207>

[1687] N. M. Katz, Slope filtration of F-crystals, In *Journées de Géométrie Algébrique de Rennes, Vol. I*, volume 63 of *Astérisque*, 113–163, Soc. Math. France, Paris, 1979. <476, 480>

[1688] N. M. Katz, *Sommes Exponentielles*, volume 79 of *Astérisque*, Société Mathématique de France, Paris, 1980, Course taught at the University of Paris, Orsay, Fall 1979, With a preface by Luc Illusie, Notes written by Gérard Laumon, With an English summary. <151, 155, 158, 163>

[1689] N. M. Katz, *Gauss Sums, Kloosterman Sums, and Monodromy Groups*, volume 116 of *Annals of Mathematics Studies*, Princeton University Press, Princeton, NJ, 1988. <29, 30, 134, 149, 151, 153, 155>

[1690] N. M. Katz, An estimate for character sums, *J. Amer. Math. Soc.* 2 (1989) 197–200. <162, 163, 177, 178, 179>

[1691] N. M. Katz, Affine cohomological transforms, perversity, and monodromy, *J. Amer. Math. Soc.* 6 (1993) 149–222. <161, 163>

[1692] N. M. Katz, Estimates for "singular" exponential sums, *Internat. Math. Res. Notices* (1999) 875–899. <159, 163, 191, 195, 333, 337>

[1693] N. M. Katz, Frobenius-Schur indicator and the ubiquity of Brock-Granville quadratic excess, *Finite Fields Appl.* 7 (2001) 45–69. <192, 195>

[1694] N. M. Katz, Sums of Betti numbers in arbitrary characteristic, *Finite Fields Appl.* 7 (2001) 29–44. <466, 467, 469, 472>

[1695] N. M. Katz, Estimates for nonsingular multiplicative character sums, *Int. Math. Res. Not.* 7 (2002) 333–349. <160, 163, 193, 195>

[1696] N. M. Katz, *Moments, Monodromy, and Perversity: a Diophantine Perspective*, volume 159 of *Annals of Mathematics Studies*, Princeton University Press, Princeton, NJ, 2005. <187, 195>

[1697] N. M. Katz, Estimates for nonsingular mixed character sums, *Int. Math. Res. Not. IMRN* (2007) Art. ID rnm069, 19. <162, 163>

[1698] N. M. Katz, Another look at the Dwork family, In *Algebra, Arithmetic, and Geometry: in Honor of Yu. I. Manin. Vol. II*, volume 270 of *Progr. Math.*, 89–126, Birkhäuser Boston Inc., Boston, MA, 2009. <465, 472>

[1699] N. M. Katz, *Convolution and Equidistribution: Sato-Tate Theorems for Finite-Field Mellin Transforms*, Annals of Mathematics Studies. Princeton University Press, Princeton, NJ, 2012. <138, 151, 155>

[1700] N. M. Katz and G. Laumon, Transformation de Fourier et majoration de sommes exponentielles, *Inst. Hautes Études Sci. Publ. Math.* (1985) 361–418. <161, 163>

[1701] N. M. Katz and Z. Zheng, On the uniform distribution of Gauss sums and Jacobi sums, In *Analytic Number Theory, Vol. 2*, volume 139 of *Progr. Math.*, 537–558, Birkhäuser Boston, Boston, MA, 1996. <134, 138, 155>

[1702] S. Kauffman, C. Peterson, B. Samuelsson, and C. Troein, Genetic networks with canalyzing Boolean rules are always stable, *Proceedings of the National Academy of Sciences of the United States of America* 101 (2004) 17102–17107. <822, 824>

[1703] S. A. Kauffman, Metabolic stability and epigenesis in randomly constructed genetic nets, *Journal of Theoretical Biology* 22 (1969) 437–467. <819, 824>

[1704] N. Kayal, Recognizing permutation functions in polynomial time, *ECCC* TR05-008 (2005). <210, 222, 385, 386>

[1705] W. F. Ke and H. Kiechle, On the solutions of the equation $x^m + y^m - z^m = 1$ in a finite field, *Proc. Amer. Math. Soc.* 123 (1995) 1331–1339. <202, 207>

[1706] K. S. Kedlaya, Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology, *J. Ramanujan Math. Soc.* 16 (2001) 323–338. <447, 449, 484>

[1707] K. S. Kedlaya, Errata for: "Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology" [J. Ramanujan Math. Soc. **16** (2001), no. 4, 323–338; MR1877805], *J. Ramanujan Math. Soc.* 18 (2003) 417–418. <447, 449>

[1708] K. S. Kedlaya, Computing zeta functions via p-adic cohomology, In *Algorithmic Number Theory*, volume 3076 of *Lecture Notes in Comput. Sci.*, 1–17, Springer, Berlin, 2004. <484>

[1709] K. S. Kedlaya and C. Umans, Fast modular composition in any characteristic, In *Forty ninth Annual IEEE Symposium on Foundations of Computer Science*, 146–155. IEEE Computer Society, 2008. <343, 351, 356, 369, 371, 373>

[1710] K. S. Kedlaya and C. Umans, Fast polynomial factorization and modular composition, *SIAM J. Comput.* 40 (2011) 1767–1802. <351, 356, 373, 374, 375>

[1711] W. Keller-Gehrig, Fast algorithms for the characteristic polynomial, *Theoret. Comput. Sci.* 36 (1985) 309–317. <522, 527>

[1712] C. A. Kelley and D. Sridhara, Pseudocodewords of Tanner graphs, *IEEE Trans. Inform. Theory* 53 (2007) 4013–4038. <709, 710>

[1713] D. Kelmer, Distribution of twisted Kloosterman sums modulo prime powers, *Int. J. Number Theory* 6 (2010) 271–280. <151, 155>

[1714] H. Kempfert, On the factorization of polynomials, *Journal of Number Theory* 1 (1969) 116–120. <374, 375>

[1715] O. Kempthorne, A simple approach to confounding and fractional replication in factorial experiments, *Biometrika* 34 (1947) 255–272. <622, 633>

[1716] A. M. Kerdock, A class of low-rate nonlinear binary codes, *Information and Control* 20 (1972) 182–187; ibid. 21 (1972), 395. <244, 245, 692, 694>

[1717] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, Nonbinary stabilizer codes over finite fields, *IEEE Trans. Inform. Theory* 52 (2006) 4892–4914. <828, 831>

[1718] H. Kharaghani and B. Tayfeh-Rezaie, A Hadamard matrix of order 428, *J. Combin. Des.* 13 (2005) 435–440. <164, 179>

[1719] K. Khoo, G. Gong, and D. R. Stinson, New family of Gold-like sequences, *IEEE Intern. Symp. Inform. Theory* 2 (2002) 181. <200>

[1720] D. S. Kim, Codes associated with special linear groups and power moments of multidimensional Kloosterman sums, *Ann. Mat. Pura Appl. Ser. IV* 190 (2011) 61–76. <148, 155>

[1721] J. H. Kim, Codes associated with $\mathrm{Sp}(4, q)$ and even-power moments of Kloosterman sums, *Bull. Aust. Math. Soc.* 79 (2009) 427–435. <151, 155>

[1722] J. H. Kim, R. Montenegro, Y. Peres, and P. Tetali, A birthday paradox for Markov chains with an optimal bound for collision in the Pollard rho algorithm for discrete logarithm, *Ann. Appl. Probab.* 20 (2010) 495–521. <390, 394>

[1723] R. Kim and W. Koepf, Parity of the number of irreducible factors for composite polynomials, *Finite Fields Appl.* 16 (2010) 137–143. <65, 66>

[1724] S.-H. Kim and J.-S. No, New families of binary sequences with low correlation, *IEEE Trans. Inform. Theory* 49 (2003) 3059–3065. <200>

[1725] A. Kipnis, J. Patarin, and L. Goubin, Unbalanced oil and vinegar signature schemes, In *Advances in Cryptology—EUROCRYPT '99*, volume 1592 of *Lecture Notes in Comput. Sci.*, 206–222, Springer, Berlin, 1999. <761, 771, 774>

[1726] A. Kipnis and A. Shamir, Cryptanalysis of the oil and vinegar signature scheme, In *Advances in Cryptology—CRYPTO '98*, volume 1462 of *Lecture Notes in Comput. Sci.*, 257–266, Springer, Berlin, 1998. <771, 774>

[1727] A. Kipnis and A. Shamir, Cryptanalysis of the HFE public key cryptosystem by relinearization, In *Advances in Cryptology—CRYPTO '99*, volume 1666 of *Lecture Notes in Comput. Sci.*, 19–30, Springer, Berlin, 1999. <383, 386, 770, 771, 774>

[1728] T. Kiran and B. S. Rajan, Optimal rate-diversity tradeoff STBCs from codes over arbitrary finite fields, In *IEEE Int. Conf. Commun.*, 453–457, 2005. <837, 839>

[1729] T. P. Kirkman, On a problem in combinations, *Cambridge and Dublin Math. J.* 2 (1847) 191–204. <582, 590>

[1730] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi, *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*, American Mathematical Society, Providence, RI, 2002. <824, 831>

[1731] A. Klappenecker and M. Rötteler, Constructions of mutually unbiased bases, In *Finite Fields and Applications*, volume 2948 of *Lecture Notes in Comput. Sci.*, 137–144, Springer, Berlin, 2004. <825, 831>

[1732] A. Klappenecker, M. Rötteler, I. E. Shparlinski, and A. Winterhof, On approximately symmetric informationally complete positive operator-valued measures and related systems of quantum states, *J. Math. Phys.* 46 (2005) 082104, 17. <826, 831>

[1733] A. Klapper, Cross-correlations of geometric sequences in characteristic two, *Des. Codes Cryptogr.* 3 (1993) 347–377. <197, 198, 200>

[1734] A. Klapper, Cross-correlations of quadratic form sequences in odd characteristic, *Des. Codes Cryptogr.* 11 (1997) 289–305. <197, 198, 200>

[1735] A. Klapper, A. H. Chan, and M. Goresky, Cross-correlations of linearly and quadratically related geometric sequences and GMW sequences, *Discrete Appl. Math.* 46 (1993) 1–20. <198, 200>

[1736] A. Klapper and M. Goresky, Feedback shift registers, 2-adic span, and combiners with memory, *J. Cryptology* 10 (1997) 111–147. <328, 329>

[1737] A. M. Klapper, Expected π-adic security measures of sequences, *IEEE Trans. Inform. Theory* 56 (2010) 2486–2501. <329>

[1738] S. L. Kleiman, Bertini and his two fundamental theorems, *Rend. Circ. Mat. Palermo Ser. II Suppl.* 55 (1998) 9–37. <380, 386>

[1739] E. Kleinfeld, Techniques for enumerating Veblen-Wedderburn systems, *J. Assoc. Comput. Mach.* 7 (1960) 330–337. <268, 270>

[1740] T. Kleinjung, Discrete logarithms in GF(p) – 160 digits, mailing list announcement, `https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0702\&L=NMBRTHRY\&P=R45\&D=0\&I=-3\&T=0`, 2007. <393, 394>

[1741] T. Kleinjung, K. Aoki, J. Franke, A. K. Lenstra, E. Thomé, J. W. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, H. te Riele, A. Timofeev, and P. Zimmermann, Factorization of a 768-bit RSA modulus, In *Advances in Cryptology—CRYPTO 2010*, volume 6223 of *Lecture Notes in Comput. Sci.*, 333–350, Springer, Berlin, 2010. <393, 394>

[1742] R. Kloosterman, The zeta function of monomial deformations of Fermat hypersurfaces, *Algebra Number Theory* 1 (2007) 421–450. <472, 480>

[1743] A. A. Klyachko, Monodromy groups of polynomial mappings, In *Studies in Number Theory*, volume 6, 82–91, Izdat. Saratov. Univ., Saratov, 1975. <230, 233>

[1744] A. W. Knapp, *Elliptic Curves*, volume 40 of *Mathematical Notes*, Princeton University Press, Princeton, NJ, 1992. <29, 30, 416, 433>

[1745] M. P. Knapp, Diagonal equations of different degrees over p-adic fields, *Acta Arith.* 126 (2007) 139–154. <207>

[1746] N. Knarr and M. Stroppel, Polarities and unitals in the Coulter-Matthews planes, *Des. Codes Cryptogr.* 55 (2010) 9–18. <272, 274>

[1747] E. Knill and R. Laflamme, Theory of quantum error-correcting codes, *Phys. Rev. A* 55 (1997) 900–911. <827, 831>

[1748] A. Knopfmacher and J. Knopfmacher, Counting polynomials with a given number of zeros in a finite field, *Linear and Multilinear Algebra* 26 (1990) 287–292. <361, 367>

[1749] A. Knopfmacher and J. Knopfmacher, Counting irreducible factors of polynomials over a finite field, *Discrete Math.* 112 (1993) 103–118. <361, 367>

[1750] A. Knopfmacher, J. Knopfmacher, and R. Warlimont, Lengths of factorizations for polynomials over a finite field, In *Finite Fields: Theory, Applications, and Algorithms*, volume 168 of *Contemp. Math.*, 185–206, Amer. Math. Soc., Providence, RI, 1994. <361, 367>

[1751] A. Knopfmacher and R. Warlimont, Distinct degree factorizations for polynomials over a finite field, *Trans. Amer. Math. Soc.* 347 (1995) 2235–2243. <361, 367>

[1752] D. E. Knuth, Finite semifields and projective planes, *J. Algebra* 2 (1965) 182–217. <267, 269, 270>

[1753] D. E. Knuth, *The Art of Computer Programming. Vol. 2: Seminumerical Algorithms*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont, 1969. <358, 360, 367, 390, 394>

[1754] D. E. Knuth, The analysis of algorithms, In *Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 3*, 269–274, Gauthier-Villars, Paris, 1971. <352, 356>

[1755] D. E. Knuth, *The Art of Computer Programming. Vol. 2, Seminumerical Algorithms*, Addison-Wesley Publishing Company, Reading, MA, second edition, 1981, Addison-Wesley Series in Computer Science and Information Processing. <349, 356>

[1756] D. E. Knuth, *The Art of Computer Programming. Vol. 2, Seminumerical algorithms*, Addison-Wesley Publishing Company, Reading, MA, third edition, 1997, Addison-Wesley Series in Computer Science and Information Processing. <339, 347, 348, 356>

[1757] N. Koblitz, p-adic variation of the zeta-function over families of varieties defined over finite fields, *Compositio Math.* 31 (1975) 119–218. <479, 480>

[1758] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Graduate Texts in Mathematics, Vol. 58, Springer-Verlag, New York, 1977. <473, 480>

[1759] N. Koblitz, Elliptic curve cryptosystems, *Math. Comp.* 48 (1987) 203–209. <736, 740, 774, 787>

[1760] N. Koblitz, Hyperelliptic cryptosystems, *J. Cryptology* 1 (1989) 139–150. <736, 740, 788, 794>

[1761] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, volume 97 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, second edition, 1993. <29, 30, 416, 433>

[1762] N. Koblitz, *Algebraic Aspects of Cryptography*, volume 3 of *Algorithms and Computation in Mathematics*, Springer-Verlag, Berlin, 1998. <29, 30, 444, 445, 449>

[1763] Ç. K. Koç and T. Acar, Montgomery multiplication in GF(2^k), *Des. Codes Cryptogr.* 14 (1998) 57–69. <346, 356, 813>

[1764] Ç. K. Koç and B. Sunar, Low-complexity bit-parallel canonical and normal basis multipliers for a class of finite fields, *IEEE Trans. Comput.* 47 (1998) 353–356. <811, 813>

[1765] W. Koepf and R. Kim, The parity of the number of irreducible factors for some pentanomials, *Finite Fields Appl.* 15 (2009) 585–603. <33, 46, 64, 66>

[1766] R. Koetter, W.-C. W. Li, P. O. Vontobel, and J. L. Walker, Characterizations of pseudo-codewords of (low-density) parity-check codes, *Adv. Math.* 213 (2007) 205–229. <709, 710>

[1767] D. R. Kohel, *Endomorphism Rings of Elliptic Curves over Finite Fields*, ProQuest LLC, Ann Arbor, MI, 1996, Thesis (Ph.D.)–University of California, Berkeley. <116, 122>

[1768] J. F. Koksma, *Some Theorems on Diophantine Inequalities*, Scriptum no. 5. Math. Centrum Amsterdam, 1950. <333, 337>

[1769] F. Kong, Z. Cai, J. Yu, and D. Li, Improved generalized Atkin algorithm for computing square roots in finite fields, *Inform. Process. Lett.* 98 (2006) 1–5. <353, 356>

[1770] K. Kononen, More exact solutions to Waring's problem for finite fields, *Acta Arith.* 145 (2010) 209–212. <206, 207>

[1771] K. Kononen, M. Moisio, M. Rinta-Aho, and K. Väänänen, Irreducible polynomials with prescribed trace and restricted norm, *JP J. Algebra Number Theory Appl.* 11 (2008) 223–248. <51, 75, 137, 155>

[1772] K. Kononen, M. Rinta-Aho, and K. Väänänen, On the degree of a Kloosterman sum as an algebraic integer, preprint available, `http://arxiv.org/abs/1107.0188v1`, 2011. <149, 155>

[1773] K. P. Kononen, M. J. Rinta-aho, and K. O. Väänänen, On integer values of Kloosterman sums, *IEEE Trans. Inform. Theory* 56 (2010) 4011–4013. <148, 150, 155, 263, 265>

[1774] S. Konyagin, T. Lange, and I. E. Shparlinski, Linear complexity of the discrete logarithm, *Des. Codes Cryptogr.* 28 (2003) 135–146. <327, 329>

[1775] S. Konyagin and F. Pappalardi, Enumerating permutation polynomials over finite fields by degree, *Finite Fields Appl.* 8 (2002) 548–553. <212, 222>

[1776] S. Konyagin and F. Pappalardi, Enumerating permutation polynomials over finite fields by degree. II, *Finite Fields Appl.* 12 (2006) 26–37. <212, 222>

[1777] S. V. Konyagin, Estimates for Gaussian sums and Waring's problem modulo a prime, *Trudy Mat. Inst. Steklov.* 198 (1992) 111–124. <169, 170, 179, 206, 207>

[1778] S. V. Konyagin, Estimates for trigonometric sums over subgroups and for Gauss sums, In *IV International Conference "Modern Problems of Number Theory and its Applications": Current Problems, Part III (Russian)*, 86–114, Mosk. Gos. Univ. im. Lomonosova, Mekh.-Mat. Fak., Moscow, 2002. <135, 155>

[1779] P. Koopman, 32-bit cyclic redundancy codes for internet applications, In *Proc. of Int'l Conf. Dependable Systems and Networks*, 459–468, 2002. <629, 630, 633>

[1780] P. Koopman and T. Chakravarty, Cyclic redundancy code (CRC) polynomial selection for embedded networks, In *Proc. Dependable Systems and Networks*, 145–154, 2004. <626, 633>

[1781] S. B. Korada, *Polar Codes for Channel and Source Coding*, PhD thesis, EPFL, 2009. <730>

[1782] S. B. Korada, A. Montanari, E. Telatar, and R. Urbanke, An empirical scaling law for polar codes, In *2010 IEEE International Symposium on Information Theory*, 884–888. IEEE, 2010. <730>

[1783] S. B. Korada, E. Sasoglu, and R. Urbanke, Polar codes: Characterization of exponent, bounds, and constructions, preprint available, `http://arxiv.com/abs/0901.0536`, 2009. <730>

[1784] S. B. Korada and R. Urbanke, Polar codes are optimal for lossy source coding, *IEEE Trans. Inform. Theory* 56 (2010) 1751–1768. <730>

[1785] G. Korchmáros and T. Szőnyi, Fermat curves over finite fields and cyclic subsets in high-dimensional projective spaces, *Finite Fields Appl.* 5 (1999) 206–217. <203, 207>

[1786] P. Kosick, *Commutative Semifields of Odd Order and Planar Dembowski-Ostrom Polynomials*, PhD thesis, Department of Mathematical Sciences, University of Delaware, USA, 2010. <274>

[1787] R. Kötter and F. R. Kschischang, Coding for errors and erasures in random network coding, *IEEE Trans. Inform. Theory* 54 (2008) 3579–3591. <838, 839>

[1788] Y. Kou, S. Lin, and M. P. C. Fossorier, Low-density parity-check codes based on finite geometries: a rediscovery and new results, *IEEE Trans. Inform. Theory* 47 (2001) 2711–2736. <709, 710>

[1789] A. G. Kouchnirenko, Polyèdres de Newton et nombres de Milnor, *Invent. Math.* 32 (1976) 1–31. <475, 480>

[1790] R. G. Kraemer, Proof of a conjecture on Hadamard 2-groups, *J. Combin. Theory, Ser. A* 63 (1993) 1–10. <596, 598>

[1791] C. Kramp, *Éléments d'arithmétique universelle*, Cologne: Th. F. Thiriart, 1808. <4, 10>

[1792] W. Krandick and T. Jebelean, Bidirectional exact integer division, *J. Symbolic Comput.* 21 (1996) 441–455. <352, 356>

[1793] R. A. Kristiansen and M. G. Parker, Binary sequences with merit factor > 6.3, *IEEE Trans. Inform. Theory* 50 (2004) 3385–3389. <316, 317>

[1794] M. Krivelevich and B. Sudakov, Pseudo-random graphs, In *More Sets, Graphs and Numbers*, volume 15 of *Bolyai Soc. Math. Stud.*, 199–262, Springer, Berlin, 2006. <637, 641, 649>

[1795] W. Krull, Algebraische Theorie der Ringe. II, *Math. Ann.* 91 (1924) 1–46. <27>

[1796] D. S. Kubert and S. Lichtenbaum, Jacobi-sum Hecke characters and Gauss-sum identities, *Compositio Math.* 48 (1983) 55–87. <140, 155>

[1797] R. Kubota, Waring's problem for $\mathbb{F}_q[x]$, *Dissertationes Math. (Rozprawy Mat.)* 117 (1974) 60pp. <491, 492>

[1798] T. Kumada, H. Leeb, Y. Kurita, and M. Matsumoto, New primitive t-nomials $(t = 3, 5)$ over GF(2) whose degree is a Mersenne exponent, *Math. Comp.* 69 (2000) 811–814. <91, 93>

[1799] P. V. Kumar, R. A. Scholtz, and L. R. Welch, Generalized bent functions and their properties, *J. Combin. Theory, Ser. A* 40 (1985) 90–107. <256, 257, 258, 259, 265>

[1800] V. A. Kurbatov and N. G. Starkov, The analytic representation of permutations, *Sverdlovsk. Gos. Ped. Inst. Učen. Zap.* 31 (1965) 151–158. <210, 222>

[1801] H. Kurzweil, M. Seidl, and J. B. Huber, Reduced-complexity collaborative decoding of interleaved Reed-Solomon and Gabidulin codes, preprint available, `http://arxiv.com/abs/1102.3126`, 2011. <730>

[1802] E. N. Kuz′min, Irreducible polynomials over a finite field and an analogue of Gauss sums over a field of characteristic 2, *Sibirsk. Mat. Zh.* 32 (1991) 100–108, 205. <52, 73, 74, 75>

[1803] G. M. Kyureghyan, Crooked maps in $\mathbb{F}_{2^n}$, *Finite Fields Appl.* 13 (2007) 713–726. <252, 254>

[1804] G. M. Kyureghyan, Constructing permutations of finite fields via linear translators, *J. Combin. Theory, Ser. A* 118 (2011) 1052–1061. <218, 221, 222>

[1805] G. M. Kyureghyan and A. Pott, Some theorems on planar mappings, In *Arithmetic of Finite Fields*, volume 5130 of *Lecture Notes in Comput. Sci.*, 117–122, Springer, Berlin, 2008. <273, 274>

[1806] M. K. Kyuregyan, On the theory of the reducibility of polynomials over finite fields, *Akad. Nauk Armyan. SSR Dokl.* 86 (1988) 17–22. <56, 60, 61>

[1807] M. K. Kyuregyan, Recurrent methods of constructing irreducible polynomials over GF(2^s) (Russian), *J. Inform. Process. Cybernet EIK* 27 (1991) 357–372. <56, 59, 60, 61>

[1808] M. K. Kyuregyan, Recurrent methods for constructing irreducible polynomials over GF(2^s), *Finite Fields Appl.* 8 (2002) 52–68. <56, 59, 60, 61, 278, 282>

[1809] M. K. Kyuregyan, Recurrent methods for constructing irreducible polynomials over

$\mathbb{F}_q$ of odd characteristics, *Finite Fields Appl.* 9 (2003) 39–58. <56, 57, 60, 61>

[1810] M. K. Kyuregyan, Iterated constructions of irreducible polynomials over finite fields with linearly independent roots, *Finite Fields Appl.* 10 (2004) 323–341. <56, 59, 61>

[1811] M. K. Kyuregyan, Recurrent methods for constructing irreducible polynomials over $\mathbb{F}_q$ of odd characteristics. II, *Finite Fields Appl.* 12 (2006) 357–378. <56, 60, 61>

[1812] M. K. Kyuregyan and G. M. Kyureghyan, Irreducible compositions of polynomials over finite fields, *Des. Codes Cryptogr.* 61 (2011) 301–314. <56, 61>

[1813] G. Lachaud, Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis, *C. R. Acad. Sci. Paris, Sér. I, Math.* 305 (1987) 729–732. <454, 456>

[1814] G. Lachaud, The parameters of projective Reed-Muller codes, *Discrete Math.* 81 (1990) 217–221. <678, 694>

[1815] G. Lachaud and J. Wolfmann, The weights of the orthogonals of the extended quadratic binary Goppa codes, *IEEE Trans. Inform. Theory* 36 (1990) 686–692. <253, 254, 263, 265>

[1816] L. Lafforgue, Chtoucas de Drinfeld et correspondance de Langlands, *Invent. Math.* 147 (2002) 1–241. <538>

[1817] L. Lafforgue, Chtoucas de Drinfeld, formule des traces d'Arthur-Selberg et correspondance de Langlands, In *Proceedings of the International Congress of Mathematicians, Vol. I*, 383–400, Higher Ed. Press, Beijing, 2002. <538>

[1818] J. C. Lagarias, Pseudorandom number generators in cryptography and number theory, In *Cryptology and Computational Number Theory*, volume 42 of *Proc. Sympos. Appl. Math.*, 115–143, Amer. Math. Soc., Providence, RI, 1990. <331, 337>

[1819] Y. Laigle-Chapuy, A note on a class of quadratic permutations over $\mathbb{F}_{2^n}$, In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 4851 of *Lecture Notes in Comput. Sci.*, 130–137, Springer, Berlin, 2007. <217, 222>

[1820] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, *Finite Fields Appl.* 13 (2007) 58–70. <211, 216, 222>

[1821] D. Laksov, Linear recurring sequences over finite fields, *Math. Scand.* 16 (1965) 181–196. <626, 633>

[1822] C. Lam, M. Aagaard, and G. Gong, Hardware implementations of multi-output Welch-Gong ciphers, 2011, Technical Report, University of Waterloo, CACR 2011-01. <744, 748, 754>

[1823] C. W. H. Lam, G. Kolesova, and L. Thiel, A computer search for finite projective planes of order 9, *Discrete Math.* 92 (1991) 187–195. <556, 565>

[1824] C. W. H. Lam, L. Thiel, and S. Swiercz, The nonexistence of finite projective planes of order 10, *Canad. J. Math.* 41 (1989) 1117–1123. <556, 565>

[1825] T. Y. Lam and K. H. Leung, Vanishing sums of mth roots of unity in finite fields, *Finite Fields Appl.* 2 (1996) 422–438. <205, 207>

[1826] B. LaMacchia and A. Odlyzko, Solving large sparse linear systems over finite fields, In *Advances in Cryptology—CRYPT0 '90*, volume 537 of *Lecture Notes in Computer Science*, 109–133. Springer, 1991. <393, 394>

[1827] B. A. LaMacchia and A. M. Odlyzko, Solving large sparse linear systems over finite fields, *Lecture Notes in Computer Science* 537 (1991) 109–133. <526, 527>

[1828] R. Lambert, *Computational Aspects of Discrete Logarithms*, PhD thesis, University

of Waterloo, Ontario, Canada, 1996. <522, 527>

[1829] L. Lan, L. Zeng, Y. Y. Tai, L. Chen, S. Lin, and K. Abdel-Ghaffar, Construction of quasi-cyclic LDPC codes for AWGN and binary erasure channels: a finite field approach, *IEEE Trans. Inform. Theory* 53 (2007) 2429–2458. <709, 710>

[1830] E. S. Lander, *Symmetric Designs: an Algebraic Approach*, volume 74 of *London Mathematical Society Lecture Note Series*, Cambridge University Press, Cambridge, 1983. <265, 591, 594, 597, 598>

[1831] S. Lang, *Elliptic Curves: Diophantine Analysis*, volume 231 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*, Springer-Verlag, Berlin, 1978. <29, 30, 416, 433>

[1832] S. Lang, *Abelian Varieties*, Springer-Verlag, New York, 1983. <158, 163>

[1833] S. Lang, *Elliptic Functions*, volume 112 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, second edition, 1987. <29, 30, 416, 433>

[1834] S. Lang, *Algebra*, volume 211 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, third edition, 2002. <408, 415, 529, 538>

[1835] S. Lang and J. Tate (eds.), *The Collected Papers of Emil Artin*, Addison–Wesley Publishing Co., Inc., Reading, Mass.-London, 1965. <68>

[1836] S. Lang and H. Trotter, *Frobenius Distributions in* GL_2*-Extensions*, Springer-Verlag, Berlin, 1976, Lecture Notes in Mathematics, Vol. 504. <30, 431, 433>

[1837] S. Lang and A. Weil, Number of points of varieties in finite fields, *Amer. J. Math.* 76 (1954) 819–827. <188, 195>

[1838] T. Lange, *Efficient Arithmetic on Hyperelliptic Curves*, PhD thesis, Universität Gesamthochschule Essen, 2001. <792, 793, 794>

[1839] T. Lange, Trace zero subvariety for cryptosystems, *Journal of the Ramanujan Mathematical Society* 19 (2004) 15–33. <793, 794>

[1840] T. Lange, Arithmetic on binary genus 2 curves suitable for small devices, In *Proceedings ECRYPT Workshop on RFID and Lightweight Crypto*, 2005. <789, 794>

[1841] T. Lange, Formulae for arithmetic on genus 2 hyperelliptic curves, *Appl. Algebra Eng. Commun. Comput.* 15 (2005) 295–328. <789, 794>

[1842] T. Lange and M. Stevens, Efficient doubling on genus two curves over binary fields, In *Eleventh International Workshop on Selected Areas in Cryptography*, volume 3357 of *Lecture Notes in Comput. Sci.*, 170–181, Springer, Berlin, 2004. <788, 794>

[1843] P. Langevin, Covering radius of $\mathrm{RM}(1,9)$ in $\mathrm{RM}(3,9)$, In *Eurocode '90*, volume 514 of *Lecture Notes in Comput. Sci.*, 51–59, Springer, Berlin, 1991. <238, 245>

[1844] P. Langevin and G. Leander, Monomial bent functions and Stickelberger's theorem, *Finite Fields Appl.* 14 (2008) 727–742. <261, 265>

[1845] V. Laohakosol and U. Pintoptang, A modification of Fitzgerald's characterization of primitive polynomials over a finite field, *Finite Fields Appl.* 14 (2008) 85–91. <83, 85>

[1846] G. Larcher and H. Niederreiter, Generalized (t, s)-sequences, Kronecker-type sequences, and diophantine approximations of formal Laurent series, *Trans. Amer. Math. Soc.* 347 (1995) 2051–2073. <617, 621>

[1847] R. Laubenbacher, A. Jarrah, H. Mortveit, and S. S. Ravi, *Encyclopedia of Complexity and System Science*, chapter A Mathematical Foundation for Agent-Based Computer Simulation, Springer Verlag, New York, 2009. <817, 824>

[1848] R. Laubenbacher and B. Stigler, A computational algebra approach to the reverse engineering of gene regulatory networks, *Journal of Theoretical Biology* 229 (2004) 523–537. <330, 337, 821, 824>

[1849] A. G. B. Lauder, Computing zeta functions of Kummer curves via multiplicative characters, *Found. Comput. Math.* 3 (2003) 273–295. <484>

[1850] A. G. B. Lauder, Counting solutions to equations in many variables over finite fields, *Found. Comput. Math.* 4 (2004) 221–267. <482, 483, 484>

[1851] A. G. B. Lauder, Deformation theory and the computation of zeta functions, *Proc. London Math. Soc., 3rd Ser.* 88 (2004) 565–602. <483, 484>

[1852] A. G. B. Lauder and K. G. Paterson, Computing the error linear complexity spectrum of a binary sequence of period 2^n, *IEEE Trans. Inform. Theory* 49 (2003) 273–280. <322, 329>

[1853] A. G. B. Lauder and D. Wan, Computing zeta functions of Artin-Schreier curves over finite fields. II, *J. Complexity* 20 (2004) 331–349. <447, 449, 484>

[1854] A. G. B. Lauder and D. Wan, Counting points on varieties over finite fields of small characteristic, In *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, 579–612, Cambridge Univ. Press, Cambridge, 2008. <447, 449, 482, 483, 484>

[1855] G. Laumon, Majorations de sommes trigonométriques (d'après P. Deligne et N. Katz), In *The Euler-Poincaré characteristic*, volume 83 of *Astérisque*, 221–258, Soc. Math. France, Paris, 1981. <163>

[1856] G. Laumon, Transformation de Fourier, constantes d'équations fonctionnelles et conjecture de Weil, *Inst. Hautes Études Sci. Publ. Math.* 65 (1987) 131–210. <471, 472>

[1857] G. Laumon, Exponential sums and l-adic cohomology: a survey, *Israel J. Math.* 120 (2000) 225–257. <163>

[1858] M. Lavrauw, G. L. Mullen, S. Nikova, D. Panario, and L. Storme, editors, *Proc. Tenth International Conference on Finite Fields and Applications*, volume 579, Amer. Math. Soc., Providence, RI, 2012. <30>

[1859] M. Lavrauw and O. Polverino, Finite semifields, In L. Storme and J. D. Buele, editors, *Current Research Topics in Galois Geometry*, chapter 6, Nova Publishers, 2011. <267, 270>

[1860] M. Lavrauw, L. Storme, and G. Van de Voorde, A proof of the linearity conjecture for k-blocking sets in $\mathrm{PG}(n, p^3)$, p prime, *J. Combin. Theory, Ser. A* 118 (2011) 808–818. <552, 555>

[1861] K. M. Lawrence, A combinatorial characterization of (t, m, s)-nets in base b, *J. Combin. Des.* 4 (1996) 275–293. <612, 621>

[1862] K. M. Lawrence, A. Mahalanabis, G. L. Mullen, and W. C. Schmid, Construction of digital (t, m, s)-nets from linear codes, In *Finite Fields and Applications*, volume 233 of *London Math. Soc. Lecture Note Ser.*, 189–208, Cambridge University Press, Cambridge, 1996. <616, 621>

[1863] C. F. Laywine and G. L. Mullen, *Discrete Mathematics using Latin Squares*, Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons Inc., New York, 1998. <29, 30, 543, 547>

[1864] C. F. Laywine, G. L. Mullen, and G. Whittle, d-dimensional hypercubes and the Euler and MacNeish conjectures, *Monatsh. Math.* 119 (1995) 223–238. <544, 545, 547>

[1865] D. Lazard, Gröbner bases, Gaussian elimination and resolution of systems of alge-

braic equations, In *Computer Algebra*, volume 162 of *Lecture Notes in Comput. Sci.*, 146–156, Springer, Berlin, 1983. <772, 774>

[1866] G. Leander and A. Kholosha, Bent functions with 2^r Niho exponents, *IEEE Trans. Inform. Theory* 52 (2006) 5529–5532. <261, 265>

[1867] N. G. Leander, Monomial bent functions, *IEEE Trans. Inform. Theory* 52 (2006) 738–743. <261, 263, 265>

[1868] G. Lecerf, Sharp precision in Hensel lifting for bivariate polynomial factorization, *Math. Comp.* 75 (2006) 921–933. <378, 386>

[1869] G. Lecerf, Improved dense multivariate polynomial factorization algorithms, *J. Symbolic Comput.* 42 (2007) 477–494. <379, 386>

[1870] G. Lecerf, Fast separable factorization and applications, *Appl. Alg. Eng. Comm. Comp.* 19 (2008) 135–160. <376, 377, 386>

[1871] G. Lecerf, New recombination algorithms for bivariate polynomial factorization based on Hensel lifting, *Appl. Alg. Eng. Comm. Comp.* 21 (2010) 151–176. <378, 386>

[1872] C. Lee and C. Chang, Low-complexity linear array multiplier for normal basis of type-II, In *Proc. IEEE International Conf. Multimedia and Expo*, 1515–1518, 2004. <812, 814>

[1873] C. Lee and C. W. Chiou, Scalable Gaussian normal basis multipliers over $GF(2^m)$ using Hankel matrix-vector representation, *Journal of Signal Processing Systems* 69 (2012) 197–211. <813, 814>

[1874] D. B. Leep and C. C. Yeomans, The number of points on a singular curve over a finite field, *Arch. Math. (Basel)* 63 (1994) 420–426. <231, 233>

[1875] A. M. Legendre, Recherches d'analyse indeterminee, *Memoires Acad. Sci. Paris* (1785) 465–559. <175, 179>

[1876] D. H. Lehmer, Euclid's Algorithm for Large Numbers, *Amer. Math. Monthly* 45 (1938) 227–233. <352, 356>

[1877] A. Lempel and H. Greenberger, Families of sequences with optimal Hamming correlation properties, *IEEE Trans. Information Theory* IT-20 (1974) 90–94. <835, 836, 839>

[1878] A. Lempel and M. J. Weinberger, Self-complementary normal bases in finite fields, *SIAM J. Discrete Math.* 1 (1988) 193–198. <108, 110>

[1879] D. Lenskoi, On the arithmetic of polynomials over a finite field (Russian), *Volz. Mat. Sb.* 4 (1966) 155–159. <486, 492>

[1880] A. K. Lenstra, Factorization of polynomials, In *Computational Methods in Number Theory, Part I*, volume 154 of *Math. Centre Tracts*, 169–198, Math. Centrum, Amsterdam, 1982. <397>

[1881] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.* 261 (1982) 515–534. <380, 386>

[1882] A. K. Lenstra and E. R. Verheul, Selecting cryptographic key sizes, In H. Imai and Y. Zheng, editors, *Public Key Cryptography—Third International Workshop on Practice and Theory in Public Key Cryptosystems PKC 2000*, volume 1751 of *Lecture Notes in Comput. Sci.*, 446–465, Springer-Verlag, Berlin, 2000. <775, 787>

[1883] H. W. Lenstra, Finding isomorphisms between finite fields, *Math. Comp.* 56 (1991) 329–347. <340, 356, 394, 395, 397>

[1884] H. W. Lenstra, Jr., A normal basis theorem for infinite Galois extensions, *Nederl. Akad. Wetensch. Indag. Math.* 47 (1985) 221–228. <124, 132>

[1885] H. W. Lenstra, Jr., Finding small degree factors of lacunary polynomials, In K. Győry, H. Iwaniec, and J. Urbanowicz, editors, *Number Theory in Progress: Proc. Internat. Conf. Number Theory*, 267–276, Berlin, 1999, de Gruyter. <383, 386>

[1886] H. W. Lenstra, Jr., Exceptional covers, October 1999, MSRI lecture, available at `http://www.msri.org/realvideo/ln/msri/1999/cgt/lenstra/1/index.html`. Accessed April 12, 2012. <231, 233>

[1887] H. W. Lenstra, Jr. and R. J. Schoof, Primitive normal bases for finite fields, *Math. Comp.* 48 (1987) 217–231. <88, 90, 109, 110, 130, 132>

[1888] H. W. Lenstra, Jr. and M. Zieve, A family of exceptional polynomials in characteristic three, In *Finite Fields and Applications*, volume 233 of *London Math. Soc. Lecture Note Ser.*, 209–218, Cambridge Univ. Press, Cambridge, 1996. <232, 233>

[1889] J. S. Leon, J. M. Masley, and V. Pless, Duadic codes, *IEEE Trans. Inform. Theory* 30 (1984) 709–714. <673, 694>

[1890] M. Leone, A new low complexity parallel multiplier for a class of finite fields, In *Proc. Cryptographic Hardware and Embedded Systems (CHES)*, volume 2162 of *Lecture Notes Comput. Sci.*, 160–170. Springer, 2001. <812, 814>

[1891] R. Lercier, *Algorithmique des Courbes Elliptiques dans les Corps Finis*, PhD thesis, École Polytechnique, 1997, In French, available at `http://perso.univ-rennes1.fr/reynald.lercier/file/Ler97a.pdf`. <352, 356>

[1892] R. Lercier and D. Lubicz, Counting points on elliptic curves over finite fields of small characteristic in quasi quadratic time, In E. Biham, editor, *Advances in Cryptology—EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Comput. Sci.*, 360–373, Springer-Verlag, Berlin, 2003. <779, 787>

[1893] R. Lercier and D. Lubicz, A quasi quadratic time algorithm for hyperelliptic curve point counting, *Ramanujan J.* 12 (2006) 399–423. <447, 449, 484>

[1894] C. Leroux, I. Tal, A. Vardy, and W. J. Gross, Hardware architectures for successive cancellation decoding of polar codes, In *2011 IEEE International Conference on Acoustics, Speech and Signal Processing—ICASSP*, 1665–1668, 2011. <730>

[1895] K. H. Leung, S. L. Ma, and B. Schmidt, Nonexistence of abelian difference sets: Lander's conjecture for prime power orders, *Trans. Amer. Math. Soc.* 356 (2004) 4343–4358. <594, 598>

[1896] K. H. Leung, S. L. Ma, and B. Schmidt, New Hadamard matrices of order $4p^2$ obtained from Jacobi sums of order 16, *J. Combin. Theory, Ser. A* 113 (2006) 822–838. <143, 155>

[1897] K. H. Leung, S. L. Ma, and B. Schmidt, On Lander's conjecture for difference sets whose order is a power of 2 or 3, *Des. Codes Cryptogr.* 56 (2010) 79–84. <594, 598>

[1898] K. H. Leung and B. Schmidt, The field descent method, *Des. Codes Cryptogr.* 36 (2005) 171–188. <595, 598>

[1899] V. Levenshtein, Application of Hadamard matrices to a problem of coding theorey, *Problemy Kibernetiki* 5 (1961) 123–136. <164, 179>

[1900] A. Levin, *Difference Algebra*, volume 8 of *Algebra and Applications*, Springer, New York, 2008. <231, 233>

[1901] A. B. Levin, Difference algebra, In *Handbook of Algebra*, volume 4, 241–334, Elsevier/North-Holland, Amsterdam, 2006. <231, 233>

[1902] F. Levy-dit Vehel and L. Perret, Polynomial equivalence problems and applications to multivariate cryptosystems, In *Progress in Cryptology—INDOCRYPT 2003*, volume 2904 of *Lecture Notes in Comput. Sci.*, 235–251, Springer, Berlin, 2003. <758, 774>

[1903] H. Li and H. J. Zhu, Zeta functions of totally ramified p-covers of the projective line, *Rend. Sem. Mat. Univ. Padova* 113 (2005) 203–225. <478, 480>

[1904] J. Li, D. B. Chandler, and Q. Xiang, Permutation polynomials of degree 6 or 7 over finite fields of characteristic 2, *Finite Fields Appl.* 16 (2010) 406–419. <209, 222>

[1905] J. Li and D. Wan, On the subset sum problem over finite fields, *Finite Fields Appl.* 14 (2008) 911–929. <207>

[1906] J. Li and D. Wan, Counting subset sums of finite abelian groups, *J. Combin. Theory, Ser. A* 119 (2012) 170–182. <207>

[1907] K.-Z. Li and F. Oort, *Moduli of Supersingular Abelian Varieties*, volume 1680 of *Lecture Notes in Mathematics*, Springer-Verlag, Berlin, 1998. <479, 480>

[1908] L. Li and O. Roche-Newton, An improved sum-product estimate for general finite fields, *SIAM J. Discrete Math.* 25 (2011) 1285–1296. <182>

[1909] W.-C. Li, Character sums and abelian Ramanujan graphs, *J. Number Theory* 41 (1992) 199–217. <641, 649>

[1910] W.-C. Li, *Number Theory with Applications*, volume 7 of *Series on University Mathematics*, World Scientific Publishing Co. Inc., River Edge, NJ, 1996. <29, 30, 634, 641, 642, 649>

[1911] W.-C. Li, On negative eigenvalues of regular graphs, *C. R. Acad. Sci. Paris, Sér. I, Math.* 333 (2001) 907–912. <638, 649>

[1912] W.-C. Li, Recent developments in automorphic forms and applications, In *Number Theory for the Millennium II*, 331–354, A. K. Peters, Natick, MA, 2002. <634, 649>

[1913] W.-C. Li, Ramanujan hypergraphs, *Geom. Funct. Anal.* 14 (2004) 380–399. <639, 649>

[1914] W.-C. Li, Zeta functions in combinatorics and number theory, In *Fourth International Congress of Chinese Mathematicians*, volume 48 of *AMS/IP Stud. Adv. Math.*, 351–366, Amer. Math. Soc., Providence, RI, 2010. <649>

[1915] W.-C. Li and P. Solé, Spectra of regular graphs and hypergraphs and orthogonal polynomials, *European J. Combin.* 17 (1996) 461–477. <639, 649>

[1916] Y. Li, S. Ling, H. Niederreiter, H. Wang, C. Xing, and S. Zhang, editors, *Coding and Cryptology*, volume 4 of *Series on Coding Theory and Cryptology*. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2008. <30>

[1917] Y. Li and M. Wang, On EA-equivalence of certain permutations to power mappings, *Des. Codes Cryptogr.* 58 (2011) 259–269. <219, 222>

[1918] Q. Liao and K. Feng, On the complexity of the normal bases via prime Gauss period over finite fields, *J. Syst. Sci. Complex.* 22 (2009) 395–406. <118, 122>

[1919] Q. Liao and L. You, Low complexity of a class of normal bases over finite fields, *Finite Fields Appl.* 17 (2011) 1–14. <113, 122>

[1920] Y. S. Liaw, More Z-cyclic Room squares, *Ars Combin.* 52 (1999) 228–238. <607, 610>

[1921] R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field?, *Amer. Math. Monthly* 95 (1988) 243–246. <209, 222>

[1922] R. Lidl and G. L. Mullen, Cycle structure of Dickson permutation polynomials, *Math. J. Okayama Univ.* 33 (1991) 1–11. <221, 222>

[1923] R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field?, II, *Amer. Math. Monthly* 100 (1993) 71–74. <209, 210, 222>

[1924] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson Polynomials*, volume 65 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*, Longman Scientific & Technical, Harlow, 1993. <29, 30, 222, 231, 233, 275, 276, 281, 282, 286, 290, 295, 326, 329>

[1925] R. Lidl and H. Niederreiter, On orthogonal systems and permutation polynomials in several variables, *Acta Arith.* 22 (1972/73) 257–265. <223, 224, 225>

[1926] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, Cambridge, revised edition, 1994. <11, 29, 30, 66, 69, 305, 310, 386, 394>

[1927] R. Lidl and H. Niederreiter, *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*, Cambridge University Press, Cambridge, second edition, 1997. <2, 10, 11, 22, 25, 29, 30, 35, 46, 56, 57, 58, 61, 62, 66, 69, 82, 85, 165, 167, 169, 173, 177, 179, 196, 200, 201, 203, 207, 208, 209, 210, 220, 222, 225, 228, 229, 231, 233, 246, 254, 275, 279, 282, 311, 317, 318, 320, 329, 342, 356, 358, 367, 370, 373, 386, 387, 394, 502>

[1928] R. Lidl and C. Wells, Chebyshev polynomials in several variables, *J. Reine Angew. Math.* 255 (1972) 104–111. <224, 225>

[1929] C. H. Lim and P. J. Lee, More flexible exponentiation with precomputation, In *Advances in Cryptology—CRYPTO '94*, volume 839 of *Lecture Notes in Comput. Sci.*, 95–107, Springer, Berlin, 1994. <349, 356>

[1930] S. Lin, On a class of cyclic codes, In *Error Correcting Codes*, 131–148, John Wiley, New York, 1968. <680, 687, 693, 694>

[1931] S. Lin and D. Costello, *Error Control Coding*, Prentice-Hall, Saddle River, NJ, second edition, 2004. <29, 30, 652, 683, 694>

[1932] J. Lindholm, An analysis of the pseudo-randomness properties of subsequences of long m-sequences, *IEEE Transactions on Information Theory* 14 (1968) 569–576. <621, 633>

[1933] S. Ling and C. Xing, *Coding Theory: A First Course*, Cambridge University Press, Cambridge, 2004. <29, 30, 652, 666, 671, 676, 694>

[1934] P. Lisoněk and M. Moisio, On zeros of Kloosterman sums, *Des. Codes Cryptogr.* 59 (2011) 223–230. <148, 155>

[1935] C. Liu, Twisted higher moments of Kloosterman sums, *Proc. Amer. Math. Soc.* 130 (2002) 1887–1892. <152, 155>

[1936] C. Liu, The L-functions of twisted Witt extensions, *J. Number Theory* 125 (2007) 267–284. <476, 480>

[1937] C. Liu and D. Wan, T-adic exponential sums over finite fields, *Algebra Number Theory* 3 (2009) 489–509. <476, 480>

[1938] C. Liu and D. Wei, The L-functions of Witt coverings, *Math. Z.* 255 (2007) 95–115. <476, 480>

[1939] P. Loidreau, On the factorization of trinomials over $\mathbb{F}_3$, INRIA rapport de recherche 3918, 2000. <65, 66>

[1940] A. F. Long, Jr., Classification of irreducible factorable polynomials over a finite field, *Acta Arith.* 12 (1967) 301–313. <59, 61>

[1941] A. F. Long, Jr., Factorization of irreducible polynomials over a finite field with the substitution $x^{p^r} - x$ for x, *Duke Math. J* 40 (1973) 63–76. <56, 59, 61>

[1942] A. F. Long, Jr., Factorization of irreducible polynomials over a finite field with the substitution $x^{p^r} - x$ for x, *Acta Arith.* 25 (1973/74) 65–80. <56, 59, 61>

[1943] A. F. Long, Jr., A theorem on factorable irreducible polynomials in several variables over a finite field with the substitution $x_i^{p^r} - x_i$ for x_i, *Math. Nachr.* 63 (1974) 123–130. <59, 61>

[1944] A. F. Long, Jr. and T. P. Vaughan, Factorization of $q(h(t)(x))$ over a finite field, where $q(x)$ is irreducible and $h(x)$ is linear II, *Linear Algebra Appl.* 11 (1975) 53–72. <59, 61>

[1945] A. F. Long, Jr. and T. P. Vaughan, Factorization of $q(h(t)(x))$ over a finite field, where $q(x)$ is irreducible and $h(x)$ is linear I, *Linear Algebra Appl.* 13 (1976) 207–221. <59, 61>

[1946] D. Lorenzini, *An Invitation to Arithmetic Geometry*, volume 9 of *Graduate Studies in Mathematics*, American Mathematical Society, Providence, RI, 1996. <452, 456>

[1947] S. R. Louboutin, Efficient computation of root numbers and class numbers of parametrized families of real abelian number fields, *Math. Comp.* 76 (2007) 455–473. <137, 155>

[1948] L. Lovász and A. Schrijver, Remarks on a theorem of Rédei, *Studia Sci. Math. Hungar.* 16 (1983) 449–454. <550, 555>

[1949] R. Lowe and D. Zelinsky, Which Galois fields are pure extensions?, *Math. Student* 21 (1953) 37–41. <57, 61>

[1950] H.-F. Lu and P. V. Kumar, Rate-diversity tradeoff of space-time codes with fixed alphabet and optimal constructions of PSK modulation, *IEEE Trans. Inform. Theory* 49 (2003) 2747–2751. <837, 839>

[1951] H.-F. Lu and P. V. Kumar, A unified construction of space-time codes with optimal rate-diversity tradeoff, *IEEE Trans. Inform. Theory* 51 (2005) 1709–1730. <837, 839>

[1952] Y. Lu and L. Zhu, On the existence of triplewhist tournaments TWh(v), *J. Combin. Des.* 5 (1997) 249–256. <610>

[1953] F. Lübeck, Conway polynomials for finite fields, 2008, `http://www.math.rwth-aachen.de:8001/~Frank.Luebeck/data/ConwayPol`. <395, 397>

[1954] A. Lubotzky, *Discrete Groups, Expanding Graphs and Invariant Measures*, volume 125 of *Progress in Mathematics*, Birkhäuser Verlag, Basel, 1994. <634, 639, 640, 649>

[1955] A. Lubotzky, Expander Graphs in Pure and Applied Mathematics, *ArXiv e-prints* (2011). <634, 640, 643, 649>

[1956] A. Lubotzky, R. Phillips, and P. Sarnak, Ramanujan graphs, *Combinatorica* 8 (1988) 261–277. <643, 644, 645, 646, 649>

[1957] A. Lubotzky and B. Weiss, Groups and expanders, In *Expanding Graphs*, volume 10 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, 95–109, Amer. Math. Soc., Providence, RI, 1993. <642, 649>

[1958] M. G. Luby, LT codes, In *Proc. Forty Third Ann. IEEE Symp. Foundations of Comput. Sci.*, 271–280, 2002. <722, 723, 724, 725>

[1959] M. G. Luby, M. Mitzenmacher, and M. A. Shokrollahi, Analysis of random processes via And-Or tree evaluation, In *Proceedings of the Ninth Annual ACM-SIAM Symposium on Discrete Algorithms*, 364–373, ACM, New York, 1998. <719,

720, 721, 725>

[1960] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. Spielman, Analysis of low density codes and improved designs using irregular graphs, In *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing*, 249–258, ACM, New York, 1998. <719, 725>

[1961] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, D. Spielman, and V. Stenman, Practical loss-resilient codes, In *Proceedings of the Twenty Ninth Annual ACM Symposium on the Theory of Computing*, 150–159, ACM, New York, 1997. <719, 721, 725>

[1962] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, Efficient erasure correcting codes, *IEEE Trans. Inform. Theory* 47 (2001) 569–584. <719, 720, 721, 725>

[1963] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, Improved low-density parity-check codes using irregular graphs, *IEEE Trans. Inform. Theory* 47 (2001) 585–598. <720, 725>

[1964] G. Lunardon, Normal spreads, *Geom. Dedicata* 75 (1999) 245–261. <552, 555>

[1965] G. Lunardon and O. Polverino, Blocking sets of size $q^t + q^{t-1} + 1$, *J. Combin. Theory, Ser. A* 90 (2000) 148–158. <552, 555>

[1966] H. Lüneburg, Über projektive Ebenen, in denen jede Fahne von einer nicht-trivialen Elation invariant gelassen wird, *Abh. Math. Sem. Univ. Hamburg* 29 (1965) 37–76. <560, 565>

[1967] H. Lüneburg, *Translation Planes*, Springer-Verlag, Berlin, 1980. <558, 565>

[1968] J. Luo and K. Feng, On the weight distributions of two classes of cyclic codes, *IEEE Trans. Inform. Theory* 54 (2008) 5332–5344. <199, 200>

[1969] Y. Luo, Q. Chai, G. Gong, and X. Lai, Wg-7, a lightweight stream cipher with good cryptographic properties, In *Proceedings of IEEE Global Communications Conference (GLOBECOM'10)*, 2010. <748, 754>

[1970] K. Ma and J. von zur Gathen, The computational complexity of recognizing permutation functions, *Comput. Complexity* 5 (1995) 76–97. <210, 222, 385, 386>

[1971] K. Ma and J. von zur Gathen, Tests for permutation functions, *Finite Fields Appl.* 1 (1995) 31–56. <210, 222>

[1972] F. S. Macaulay, *The Algebraic Theory of Modular Systems*, Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1994. <772, 774>

[1973] C. R. MacCluer, On a conjecture of Davenport and Lewis concerning exceptional polynomials, *Acta Arith* 12 (1966/1967) 289–299. <285, 295>

[1974] D. J. C. MacKay, Good error-correcting codes based on very sparse matrices, *IEEE Trans. Inform. Theory* 45 (1999) 399–431. <704, 706, 707, 710>

[1975] H. F. MacNeish, Euler squares, *Ann. of Math., 2nd Ser.* 23 (1922) 221–227. <544, 547>

[1976] F. J. MacWilliams, Orthogonal matrices over finite fields, *Amer. Math. Monthly* 76 (1969) 152–164. <497, 499, 502>

[1977] F. J. MacWilliams, Orthogonal circulant matrices over finite fields, and how to find them., *J. Combin. Theory, Ser. A* 10 (1971) 1–17. <109, 110, 498, 502>

[1978] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes. I*, North-Holland Mathematical Library, Vol. 16, North-Holland Publishing Co., Amsterdam, 1977. <29, 30, 173, 179, 199, 200, 252, 254, 259, 265, 578, 580, 652, 675, 682, 692, 694>

[1979] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes. II*, North-Holland Mathematical Library, Vol. 16, North-Holland Publishing Co., Amsterdam, 1977. <236, 237, 238, 239, 244, 245>

[1980] H. Mahdavifar and A. Vardy, Achieving the secrecy capacity of wiretap channels using polar codes, *IEEE Trans. Inform. Theory* 57 (2011) 6428–6443. <730>

[1981] S. Maitra, K. C. Gupta, and A. Venkateswarlu, Results on multiples of primitive polynomials and their products over GF(2), *Theoret. Comput. Sci.* 341 (2005) 311–343. <92, 93, 625, 626, 633>

[1982] C. Malvenuto and F. Pappalardi, Enumerating permutation polynomials I: Permutations with non-maximal degree, *Finite Fields Appl.* 8 (2002) 531–547. <213, 222>

[1983] C. Malvenuto and F. Pappalardi, Enumerating permutation polynomials II: k-cycles with minimal degree, *Finite Fields Appl.* 10 (2004) 72–96. <213, 222>

[1984] C. Malvenuto and F. Pappalardi, Corrigendum to: "Enumerating permutation polynomials I: Permutations with non-maximal degree" [Finite Fields Appl. 8 (2002), no. 4, 531–547; MR1933624], *Finite Fields Appl.* 13 (2007) 171–174. <213, 222>

[1985] F. Manganiello, E. Gorla, and J. Rosenthal, Spread codes and spread decoding in network coding, In *Proc. Int. Symp. Inform. Theory*, 881–885, 2008. <838, 839>

[1986] J. I. Manin, The Hasse-Witt matrix of an algebraic curve, *Izv. Akad. Nauk SSSR Ser. Mat.* 25 (1961) 153–172. <479, 480>

[1987] Y. Mansury, M. Kimura, J. Lobo, and T. S. Deisboeck, Emerging patterns in tumor systems: Simulating the dynamics of multicellular clusters with an agent-based spatial agglomeration model, *Journal of Theoretical Biology* 219 (2002) 343–370. <821, 824>

[1988] I. Mantin, *Analysis of the Stream Cipher RC4*, Master's dissertation, The Weizmann Institute of Science, Rehovot, 76100, Israel, 2001. <741, 743, 754>

[1989] Maplesoft^{TM}, Maplesoft - Technical Computing Software for Engineers, Mathematicians, Scientists, Intructors and Students, `http://www.maplesoft.com/`, as viewed in July 2012. <45, 46>

[1990] J. E. Marcos, Specific permutation polynomials over finite fields, *Finite Fields Appl.* 17 (2011) 105–112. <214, 217, 218, 222>

[1991] D. A. Marcus, *Number Fields*, Universitext, Springer-Verlag, New York, 1977. <837, 839>

[1992] G. A. Margulis, Explicit constructions of expanders, *Problemy Peredači Informacii* 9 (1973) 71–80. <640, 649>

[1993] G. A. Margulis, Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators, *Problemy Peredachi Informatsii* 24 (1988) 51–60. <644, 646, 649>

[1994] W. J. Martin and D. R. Stinson, A generalized Rao bound for ordered orthogonal arrays and (t, m, s)-nets, *Canad. Math. Bull.* 42 (1999) 359–370. <612, 621>

[1995] W. J. Martin and D. R. Stinson, Association schemes for ordered orthogonal arrays and (T, M, S)-nets, *Canad. J. Math.* 51 (1999) 326–346. <612, 621>

[1996] W. J. Martin and T. I. Visentin, A dual Plotkin bound for (T, M, S)-nets, *IEEE Trans. Inform. Theory* 53 (2007) 411–415. <612, 621>

[1997] J. L. Massey, *Threshold Decoding*, Massachusetts Institute of Technology, Research Laboratory of Electronics, Tech. Rep. 410, Cambridge, Mass., 1963. <687,

694>

[1998] J. L. Massey, Shift-register synthesis and BCH decoding, *IEEE Trans. Information Theory* IT-15 (1969) 122–127. <239, 245, 307, 310, 318, 329, 343, 356, 684, 693, 694>

[1999] J. L. Massey and J. K. Omura, Computational methods and apparatus for finite field arithmetic, *US Patent No. 4,587,627, to OMNET Assoc., Sunnyvale CA, Washington, D.C.: Patent and Trademark Office* (1986). <809, 811, 814>

[2000] J. L. Massey and S. Serconek, Linear complexity of periodic sequences: a general theory, In *Advances in Cryptology—CRYPTO '96*, volume 1109 of *Lecture Notes in Comput. Sci.*, 358–371, Springer, Berlin, 1996. <301, 303, 321, 329>

[2001] E. D. Mastrovito, VLSI designs for multiplication over finite field $GF(2^m)$, In *Proc. Sixth International Conference on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-6)*, 297–309, 1988. <807, 814>

[2002] A. Masuda and D. Panario, Sequences of consecutive smooth polynomials over a finite field, *Proc. Amer. Math. Soc.* 135 (2007) 1271–1277. <492>

[2003] A. Masuda, D. Panario, and Q. Wang, The number of permutation binomials over $\mathbb{F}_{4p+1}$ where p and $4p+1$ are primes, *Electron. J. Combin.* 13 (2006) Research Paper 65, 15 pp. <210, 211, 216, 222>

[2004] A. M. Masuda, L. Moura, D. Panario, and D. Thomson, Low complexity normal elements over finite fields of characteristic two, *IEEE Trans. Comput.* 57 (2008) 990–1001. <36, 37, 46, 111, 117, 122>

[2005] A. M. Masuda and D. Panario, *Tópicos de Corpos Finitos com Aplicações em Criptografia e Teoria de Códigos*, Publicações Matemáticas do IMPA. [IMPA Mathematical Publications]. Instituto Nacional de Matemática Pura e Aplicada (IMPA), Rio de Janeiro, 2007, 26o Colóquio Brasileiro de Matemática. [26th Brazilian Mathematics Colloquium]. <11, 29, 30>

[2006] A. M. Masuda and M. E. Zieve, Nonexistence of permutation binomials of certain shapes, *Electron. J. Combin.* 14 (2007) Note 12, 5 pp. <211, 222>

[2007] A. M. Masuda and M. E. Zieve, Permutation binomials over finite fields, *Trans. Amer. Math. Soc.* 361 (2009) 4169–4180. <211, 216, 222>

[2008] E. Mathieu, Nombre de valeurs que peut acquérir une fonction quand on y permute ses variables de toutes les manières possibles, *J. Math.* 5 (1860) 9–42. <9, 10>

[2009] E. Mathieu, Mémoire sur l'étude des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariables, *J. Math. Pures Appl.* 6 (1861) 241–323. <58, 61>

[2010] R. Mathon, Symmetric conference matrices of order pq^2+1, *Canad. J. Math.* 30 (1978) 321–331. <601, 610>

[2011] R. Mathon, New maximal arcs in Desarguesian planes, *J. Combin. Theory, Ser. A* 97 (2002) 353–368. <564, 565>

[2012] R. Mathon and G. F. Royle, The translation planes of order 49, *Des. Codes Cryptogr.* 5 (1995) 57–72. <267, 270>

[2013] M. Matsui, Linear cryptoanalysis method for DES cipher, In *EUROCRYPT*, volume 765 of *Lecture Notes in Comput. Sci.*, 386–397, Springer, Berlin, 1993. <246, 254>

[2014] R. Matsumoto, Improvement of Ashikhmin-Litsyn-Tsfasman bound for quantum codes, *IEEE Transactions on Information Theory* 48 (2002) 2122–2124. <828, 831>

[2015] T. Matsumoto and H. Imai, Public quadratic polynomial-tuples for efficient

signature-verification and message-encryption, In *Advances in Cryptology—EUROCRYPT '88*, volume 330 of *Lecture Notes in Comput. Sci.*, 419–453, Springer, Berlin, 1988. <755, 760, 774>

[2016] T. Matsumoto, H. Imai, H. Harashima, and H. Miyakawa, A cryptographically useful theorem on the connection between uni and multivariate polynomials, *Transactions of the IECE of Japan* 68 (1985) 139–146. <755, 758, 774>

[2017] S. Mattarei, On a bound of Garcia and Voloch for the number of points of a Fermat curve over a prime field, *Finite Fields Appl.* 13 (2007) 773–777. <206, 207>

[2018] R. Matthews, Permutation polynomials over algebraic number fields, *J. Number Theory* 18 (1984) 249–260. <295>

[2019] R. Matthews, Some results on permutation polynomials over finite fields, *Appl. Algebra Engrg. Comm. Comput.* 3 (1992) 63–65. <223, 225>

[2020] R. Matthews, Permutation properties of the polynomials $1 + x + \cdots + x^k$ over a finite field, *Proc. Amer. Math. Soc.* 120 (1994) 47–51. <216, 222>

[2021] R. W. Matthews, *Permutation Polynomials in One and Several Variables*, PhD thesis, University of Tasmania, Hobart, Tasmania, Australia, 1982. <219, 222, 266, 270>

[2022] H. F. Mattson and G. Solomon, A new treatment of Bose-Chaudhuri codes, *J. Soc. Indust. Appl. Math.* 9 (1961) 654–669. <669, 693, 694>

[2023] C. Mauduit, H. Niederreiter, and A. Sárközy, On pseudorandom $[0, 1)$ and binary sequences, *Publ. Math. Debrecen* 71 (2007) 305–324. <329>

[2024] C. Mauduit and A. Sárközy, On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the Legendre symbol, *Acta Arith.* 82 (1997) 365–377. <176, 179, 328, 329, 832, 839>

[2025] U. M. Maurer, Fast generation of prime numbers and secure public-key cryptographic parameters, *J. Cryptology* 8 (1995) 123–155. <340, 356>

[2026] U. M. Maurer and S. Wolf, The Diffie-Hellman protocol: towards a quarter-century of public key cryptography, *Des. Codes Cryptogr.* 19 (2000) 147–171. <736, 740>

[2027] J. P. May, D. Saunders, and Z. Wan, Efficient matrix rank computation with application to the study of strongly regular graphs, In *ISSAC 2007*, 277–284, ACM, New York, 2007. <526, 527>

[2028] B. Mazur, Frobenius and the Hodge filtration (estimates), *Ann. of Math., 2nd Ser.* 98 (1973) 58–95. <474, 480>

[2029] O. D. Mbodj, Quadratic Gauss sums, *Finite Fields Appl.* 4 (1998) 347–361. <144, 155>

[2030] K. McCann and K. S. Williams, The distribution of the residues of a quartic polynomial, *Glasgow Math. J.* 8 (1967) 67–88. <227, 229>

[2031] K. S. McCurley, Cryptographic key distribution and computation in class groups, In *Number Theory and Applications*, volume 265 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, 459–479, Kluwer Acad. Publ., Dordrecht, 1989. <387, 394>

[2032] B. R. McDonald, *Finite Rings with Identity*, Pure and Applied Mathematics, Vol. 28. Marcel Dekker Inc., New York, 1974. <27, 29>

[2033] R. J. McEliece, Table of polynomials of period e over GF(p), *Math. Comp.* 23 (1969) C1–C6. <58, 61>

[2034] R. J. McEliece, *The Theory of Information and Coding*, Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1977. <652, 675, 676, 685, 694>

[2035] R. J. McEliece, A public-key cryptosystem based on algebraic coding theory, DSN progress report #42-44, Jet Propulsion Laboratory, Pasadena, California, 1978. <739, 740>

[2036] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*, The Kluwer International Series in Engineering and Computer Science, 23. Kluwer Academic Publishers, Boston, MA, 1987. <11, 29, 30>

[2037] R. J. McEliece, E. R. Rodemich, H. Rumsey, Jr., and L. R. Welch, New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities, *IEEE Trans. Information Theory* IT-23 (1977) 157–166. <664, 665, 694>

[2038] R. L. McFarland, A family of difference sets in non-cyclic groups, *J. Combin. Theory, Ser. A* 15 (1973) 1–10. <259, 265, 596, 598>

[2039] G. McGuire, G. L. Mullen, D. Panario, and I. E. Shparlinski, editors, *Finite Fields: Theory and Applications*, volume 518 of *Contemporary Mathematics*, American Mathematical Society, Providence, RI, 2010. <30>

[2040] B. D. McKay and I. M. Wanless, On the number of Latin squares, *Ann. Comb.* 9 (2005) 335–344. <542, 547>

[2041] H. McKean and V. Moll, *Elliptic Curves: Function Theory, Geometry, Arithmetic*, Cambridge University Press, Cambridge, 1997. <29, 30, 416, 433>

[2042] P. K. Meher, Systolic and super-systolic multipliers for finite field $GF(2^m)$ based on irreducible trinomials, *IEEE Transactions on Circuits and Systems I: Regular Papers* 55 (2008) 1031–1040. <806, 814>

[2043] W. Meidl, Linear complexity and k-error linear complexity for p^n-periodic sequences, In *Coding, Cryptography and Combinatorics*, volume 23 of *Progr. Comput. Sci. Appl. Logic*, 227–235, Birkhäuser, Basel, 2004. <322, 329>

[2044] W. Meidl, Reducing the calculation of the linear complexity of $u2^v$-periodic binary sequences to Games-Chan algorithm, *Des. Codes Cryptogr.* 46 (2008) 57–65. <322, 329>

[2045] W. Meidl and H. Niederreiter, Counting functions and expected values for the k-error linear complexity, *Finite Fields Appl.* 8 (2002) 142–154. <324, 329>

[2046] W. Meidl and H. Niederreiter, Linear complexity, k-error linear complexity, and the discrete Fourier transform, *J. Complexity* 18 (2002) 87–103. <324, 329>

[2047] W. Meidl and H. Niederreiter, On the expected value of the linear complexity and the k-error linear complexity of periodic sequences, *IEEE Trans. Inform. Theory* 48 (2002) 2817–2825. <324, 329>

[2048] W. Meidl and H. Niederreiter, The expected value of the joint linear complexity of periodic multisequences, *J. Complexity* 19 (2003) 61–72. <321, 324, 329>

[2049] W. Meidl and H. Niederreiter, Periodic sequences with maximal linear complexity and large k-error linear complexity, *Appl. Algebra Engrg. Comm. Comput.* 14 (2003) 273–286. <324, 329>

[2050] W. Meidl, H. Niederreiter, and A. Venkateswarlu, Error linear complexity measures for multisequences, *J. Complexity* 23 (2007) 169–192. <324, 329>

[2051] W. Meidl and F. Özbudak, Linear complexity over $\mathbb{F}_q$ and over $\mathbb{F}_{q^m}$ for linear recurring sequences, *Finite Fields Appl.* 15 (2009) 110–124. <318, 329>

[2052] W. Meidl and A. Winterhof, Lower bounds on the linear complexity of the discrete logarithm in finite fields, *IEEE Trans. Inform. Theory* 47 (2001) 2807–2811. <327, 329>

[2053] W. Meidl and A. Winterhof, Linear complexity and polynomial degree of a function over a finite field, In *Finite Fields with Applications to Coding Theory,*

Cryptography and Related Areas, 229–238, Springer, Berlin, 2002. <322, 329>

[2054] W. Meidl and A. Winterhof, On the linear complexity profile of explicit nonlinear pseudorandom numbers, *Inform. Process. Lett.* 85 (2003) 13–18. <325, 329>

[2055] W. Meidl and A. Winterhof, On the autocorrelation of cyclotomic generators, In *Finite Fields and Applications*, volume 2948 of *Lecture Notes in Comput. Sci.*, 1–11, Springer, Berlin, 2004. <166, 179>

[2056] W. Meidl and A. Winterhof, On the linear complexity profile of some new explicit inversive pseudorandom numbers, *J. Complexity* 20 (2004) 350–355. <325, 329>

[2057] W. Meidl and A. Winterhof, On the joint linear complexity profile of explicit inversive multisequences, *J. Complexity* 21 (2005) 324–336. <325, 329>

[2058] W. Meidl and A. Winterhof, Some notes on the linear complexity of Sidel′nikov-Lempel-Cohn-Eastman sequences, *Des. Codes Cryptogr.* 38 (2006) 159–178. <327, 329>

[2059] W. Meidl and A. Winterhof, On the linear complexity profile of nonlinear congruential pseudorandom number generators with Rédei functions, *Finite Fields Appl.* 13 (2007) 628–634. <326, 329>

[2060] W. Meier and O. Staffelbach, Fast correlation attacks on stream ciphers, In D. Barstow, W. Brauer, P. Brinch Hansen, D. Gries, D. Luckham, C. Moler, A. Pnueli, G. Seegmüller, J. Stoer, N. Wirth, and C. Günther, editors, *Advances in Cryptology—EUROCRYPT'88*, volume 330 of *Lecture Notes in Computer Science*, 301–314, Springer, Berlin, 1988. <621, 633>

[2061] W. Meier and O. Staffelbach, Fast correlation attacks on certain stream ciphers, *J. Cryptology* 1 (1989) 159–176. <240, 245>

[2062] A. Menezes, *Elliptic Curve Public Key Cryptosystems*, The Kluwer International Series in Engineering and Computer Science, 234. Kluwer Academic Publishers, Boston, MA, 1993. <29, 30>

[2063] A. Menezes, I. Blake, X.-H. Gao, R. Mullin, S. Vanstone, and T. Yaghoobian, *Applications of Finite Fields*, The Springer International Series in Engineering and Computer Science, Vol. 199, Springer, 1993. <11, 29, 30, 56, 59, 60, 61, 66, 67, 69, 107, 110>

[2064] A. Menezes and M. Qu, Analysis of the Weil descent attack of Gaudry, Hess and Smart, In *Topics in Cryptology—CT-RSA 2001*, volume 2020 of *Lecture Notes in Comput. Sci.*, 308–318, Springer, Berlin, 2001. <801, 802>

[2065] A. J. Menezes, T. Okamoto, and S. A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Trans. Inform. Theory* 39 (1993) 1639–1646. <433, 784, 787>

[2066] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. <29, 30, 44, 46, 339, 340, 344, 345, 355, 356, 386, 394, 740, 748, 754, 775, 787, 813, 814>

[2067] G. Menichetti, On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field, *J. Algebra* 47 (1977) 400–410. <269, 270>

[2068] G. Menichetti, n-dimensional algebras over a field with a cyclic extension of degree n, *Geom. Dedicata* 63 (1996) 69–94. <269, 270>

[2069] P. Merkey and E. Posner, Optimum cyclic redundancy codes for noisy channels, *IEEE Trans. Inform. Theory* 30 (1984) 865–867. <624, 626, 629, 630, 633>

[2070] "Mersenne Research, Inc.", GIMPS Home, `http://www.mersenne.org`, as viewed

in July, 2012. <44, 46>

[2071] S. Mesnager, Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity, *IEEE Trans. Inform. Theory* 54 (2008) 3656–3662. <241, 245>

[2072] S. Mesnager, A new class of bent and hyper-bent Boolean functions in polynomial forms, *Des. Codes Cryptogr.* 59 (2011) 265–279. <148, 155>

[2073] J.-F. Mestre, Construction des courbes de genre 2 à partir de leurs modules, *Progress in Mathematics* 94 (1991) 313–334. <794>

[2074] J.-F. Mestre, Lettre adressée à Gaudry et Harley, `http://www.math.jussieu.fr/~mestre/lettreGaudryHarley.ps`, 2000. <779, 787>

[2075] J.-F. Mestre, Algorithmes pur compter des point de courbes en petite charactéristique et en petit genres, Available at `http://www.math.jussieu.fr/~mestre/`, 2002. <447, 449>

[2076] P. Meyer, Eine Charakterisierung vollständig regulärer, abelscher Erweiterungen, *Abh. Math. Sem. Univ. Hamburg* 68 (1998) 199–223. <123, 124, 132>

[2077] H. Meyn, On the construction of irreducible self-reciprocal polynomials over finite fields, *Appl. Algebra Engrg. Comm. Comput.* 1 (1990) 43–53. <53, 55, 56, 60, 61, 278, 282>

[2078] P. Michel, Some recent applications of Kloostermania, In *Physics and Number Theory*, volume 10 of *IRMA Lect. Math. Theor. Phys.*, 225–251, Eur. Math. Soc., Zürich, 2006. <151, 155>

[2079] T. Migler, K. E. Morrison, and M. Ogle, How much does a matrix of rank k weigh?, *Math. Mag.* 79 (2006) 262–271. <493, 502>

[2080] M. Mignotte and C. Schnorr, Calcul des racines d-ièmes dans un corps fini, *Comptes Rendus de l'Académie des Sciences Paris* 290 (1988) 205–206. <374, 375>

[2081] P. Mihăilescu, Fast generation of provable primes using search in arithmetic progressions, In *Advances in Cryptology—CRYPTO '94*, volume 839 of *Lecture Notes in Comput. Sci.*, 282–293, Springer, Berlin, 1994. <340, 356>

[2082] P. Mihăilescu, Optimal Galois field bases which are not normal, 1997, Presented at the Workshop on Fast Software Encryption in Haifa. <346, 356>

[2083] P. Mihăilescu, Medium Galois Fields, their Bases and Arithmetic, 2000, `http://grouper.ieee.org/groups/1363/P1363a/NumThAlgs.html`. <351, 356>

[2084] P. Mihăilescu, F. Morain, and E. Schost, Computing the eigenvalue in the Schoof–Elkies–Atkin algorithm using abelian lifts, In C. W. Brown, editor, *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation—ISSAC 2007*, 285–292, ACM, New York, 2007. <778, 787>

[2085] G. L. Miller, Riemann's hypothesis and tests for primality, *J. Comput. System Sci.* 13 (1976) 300–317. <339, 356>

[2086] R. L. Miller, Necklaces, symmetries and self-reciprocal polynomials, *Discrete Math.* 22 (1978) 25–33. <278, 282>

[2087] S. J. Miller and M. R. Murty, Effective equidistribution and the Sato-Tate law for families of elliptic curves, *J. Number Theory* 131 (2011) 25–44. <423, 433>

[2088] V. S. Miller, Use of elliptic curves in cryptography, In *Advances in Cryptology—CRYPTO '85*, volume 218 of *Lecture Notes in Comput. Sci.*, 417–426, Springer, Berlin, 1986. <736, 740, 774, 787>

[2089] D. Mills, Factorizations of root-based polynomial compositions, *Discrete Math.* 240 (2001) 161–173. <63, 66>

[2090] D. Mills, Existence of primitive polynomials with three coefficients prescribed, *JP J. Algebra Number Theory Appl.* 4 (2004) 1–22. <88, 90>

[2091] W. H. Mills, Polynomials with minimal value sets, *Pacific J. Math.* 14 (1964) 225–241. <226, 229>

[2092] W. H. Mills and R. C. Mullin, Coverings and packings, In *Contemporary Design Theory*, Wiley-Intersci. Ser. Discrete Math. Optim., 371–399, Wiley, New York, 1992. <589, 590>

[2093] J. S. Milne, *Elliptic Curves*, BookSurge Publishers, Charleston, SC, 2006. <29, 30, 416, 433>

[2094] R. Mines, F. Richman, and W. Ruitenburg, *A Course in Constructive Algebra*, Universitext. Springer-Verlag, 1988. <376, 386>

[2095] M. Minzlaff, Computing zeta functions of superelliptic curves in larger characteristic, *Math. Comput. Sci.* 3 (2010) 209–224. <482, 484>

[2096] Y. Miyamoto, H. Doi, K. Matsuo, J. Chao, and S. Tsuji, A fast addition algorithm of genus two hyperelliptic curve, In *Proc. of SCIS2002, IEICE Japan*, 497–502, 2002, in Japanese. <789, 794>

[2097] R. T. Moenck, Another polynomial homomorphism, *Acta Informat.* 6 (1976) 153–169. <344, 356>

[2098] R. T. Moenck, On the efficiency of algorithms for polynomial factoring, *Mathematics of Computation* 31 (1977) 235–250. <374, 375>

[2099] T. Moh, A public key system with signature and master key functions, *Comm. Algebra* 27 (1999) 2207–2222. <765, 773, 774>

[2100] M. S. E. Mohamed, D. Cabarcas, J. Ding, J. Buchmann, and S. Bulygin, MXL_3: an efficient algorithm for computing Gröbner bases of zero-dimensional ideals, In *Information Security and Cryptology—ICISC 2009*, volume 5984 of *Lecture Notes in Comput. Sci.*, 87–100, Springer, Berlin, 2010. <772, 774>

[2101] M. S. E. Mohamed, J. Ding, J. Buchmann, and F. Werner, Algebraic attack on the MQQ public key cryptosystem, In *Eighth International Conference on Cryptology and Network Security*, volume 5888 of *Lecture Notes in Comput. Sci.*, 392–401, 2009. <766, 774>

[2102] M. S. E. Mohamed, W. S. A. E. Mohamed, J. Ding, and J. Buchmann, MXL2: Solving polynomial equations over GF(2) using an improved mutant strategy, In J. Buchmann and J. Ding, editors, *PQCrypto*, volume 5299 of *Lecture Notes in Comput. Sci.*, 203–215. Springer, 2008. <772, 774>

[2103] B. Mohar, Isoperimetric numbers of graphs, *J. Combin. Theory, Ser. B* 47 (1989) 274–291. <640, 649>

[2104] B. Mohar, A strengthening and a multipartite generalization of the Alon-Boppana-Serre theorem, *Proc. Amer. Math. Soc.* 138 (2010) 3899–3909. <638, 639, 649>

[2105] M. Moisio, The moments of a Kloosterman sum and the weight distribution of a Zetterberg-type binary cyclic code, *IEEE Trans. Inform. Theory* 53 (2007) 843–847. <151, 155>

[2106] M. Moisio, On the number of rational points on some families of Fermat curves over finite fields, *Finite Fields Appl.* 13 (2007) 546–562. <202, 207>

[2107] M. Moisio, Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm, *Acta Arith.* 132 (2008) 329–350. <71, 75, 263, 265>

[2108] M. Moisio, On the moments of Kloosterman sums and fibre products of Kloosterman

curves, *Finite Fields Appl.* 14 (2008) 515–531. <151, 155>

[2109] M. Moisio and K. Ranto, Elliptic curves and explicit enumeration of irreducible polynomials with two coefficients prescribed, *Finite Fields Appl.* 14 (2008) 798–815. <75>

[2110] M. Moisio, K. Ranto, M. Rinta-Aho, and K. Väänänen, On the weight distribution of cyclic codes with one or two zeros, *Adv. Appl. Discrete Math.* 3 (2009) 125–150. <148, 155>

[2111] M. Moisio and D. Wan, On Katz's bound for the number of elements with given trace and norm, *J. Reine Angew. Math.* 638 (2010) 69–74. <190, 195>

[2112] F. Möller, Exceptional polynomials with 2-transitive affine monodromy groups, *Finite Fields Appl.* 18 (2012) 445–457. <231, 233>

[2113] R. A. Mollin and C. Small, On permutation polynomials over finite fields, *Internat. J. Math. Math. Sci.* 10 (1987) 535–543. <216, 222>

[2114] R. Moloney, *Divisibility Properties of Kloosterman Sums and Division Polynomials for Edwards Curves*, PhD dissertation, University College Dublin, College of Engineering, Mathematical and Physical Sciences, 2011. <148, 155>

[2115] M. Monagan and R. Pearce, Polynomial division using dynamic arrays, heaps, and packed exponent vectors, In *Proc. of CASC 2007*, 295–315. Springer-Verlag, 2007. <375, 386>

[2116] M. Monagan and R. Pearce, Parallel sparse polynomial multiplication using heaps, In *ISSAC '09: Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation*, 263–270, ACM, New York, NY, USA, 2009. <375, 386>

[2117] M. Monagan and R. Pearce, Sparse polynomial multiplication and division in Maple 14, *ACM Communications in Computer Algebra* 44 (2010) 183–220. <375, 386>

[2118] P. L. Montgomery, Modular multiplication without trial division, *Math. Comp.* 44 (1985) 519–521. <344, 353, 356, 813, 814>

[2119] P. L. Montgomery, Speeding the Pollard and elliptic curve methods of factorization, *Math. Comp.* 48 (1987) 243–264. <352, 356, 434, 436, 440>

[2120] P. L. Montgomery, A block Lanczos algorithm for finding dependencies over GF(2), In *Advances in Cryptology—EUROCRYPT '95*, volume 921 of *Lecture Notes in Comput. Sci.*, 106–120, Springer, Berlin, 1995. <393, 394>

[2121] J. W. Moon and L. Moser, On the correlation function of random binary sequences, *SIAM J. Appl. Math.* 16 (1968) 340–343. <832>

[2122] T. Moon, *Error Correction Coding: Mathematical Methods and Algorithms*, John Wiley and Sons, Hoboken, NJ, 2005. <652, 683, 694>

[2123] Y. Moon, J. B. Lee, and Y. H. Park, Counting formula for solutions of diagonal equations, *Bull. Korean Math. Soc.* 37 (2000) 803–810. <207>

[2124] C. Moore, D. Rockmore, A. Russell, and L. J. Schulman, The hidden subgroup problem in affine groups: basis selection in Fourier sampling, preprint available, `http://arxiv.org/abs/quant-ph/0211124`, 2003. <830, 831>

[2125] E. H. Moore, A doubly-infinite system of simple groups, In E. H. Moore *et al.*, editor, *Mathematical Papers Read at the International Mathematics Congress Held in Connection with the World's Columbian Exposition*, 208–242, New York: Macmillan & Co., 1896. <2, 9, 10>

[2126] E. H. Moore, A two-fold generalization of Fermat's theorem, *Bull. Amer. Math. Soc.* 2 (1896) 189–199. <501, 502>

[2127] F. Morain, Implementing the asymptotically fast version of the elliptic curve primality proving algorithm, *Math. Comp.* 76 (2007) 493–505. <340, 356>

[2128] D. J. M. Morales, An analysis of the infrastructure in real function fields, preprint available, `http://eprint.iacr.org/2008/299`, 2008. <449>

[2129] L. J. Mordell, On a sum analogous to a Gauss sum, *Quart. J. Math.* 3 (1932) 161–162. <184, 186>

[2130] C. Moreno, *Algebraic Curves over Finite Fields*, volume 97 of *Cambridge Tracts in Mathematics*, Cambridge University Press, Cambridge, 1991. <30, 202, 207>

[2131] O. Moreno, Discriminants and the irreducibility of a class of polynomials in a finite field of arbitrary characteristic, *J. Number Theory* 28 (1988) 62–65. <62, 66>

[2132] O. Moreno and F. N. Castro, Divisibility properties for covering radius of certain cyclic codes, *IEEE Trans. Inform. Theory* 49 (2003) 3299–3303. <207>

[2133] O. Moreno and F. N. Castro, On the covering radius of certain cyclic codes, In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 2643 of *Lecture Notes in Comput. Sci.*, 129–138, Springer, Berlin, 2003. <207>

[2134] O. Moreno and F. N. Castro, On the calculation and estimation of Waring number for finite fields, In *Arithmetic, Geometry and Coding Theory (AGCT 2003)*, volume 11 of *Sémin. Congr.*, 29–40, Soc. Math. France, Paris, 2005. <205, 207>

[2135] O. Moreno and F. N. Castro, Optimal divisibility for certain diagonal equations over finite fields, *J. Ramanujan Math. Soc.* 23 (2008) 43–61. <204, 205, 207>

[2136] O. Moreno, F. N. Castro, and H. F. Mattson, Jr., Correction to: "Divisibility properties for covering radius of certain cyclic codes" [IEEE Trans. Inform. Theory 49 (2003), no. 12, 3299–3303; MR2045808] by Moreno and Castro, *IEEE Trans. Inform. Theory* 52 (2006) 1798–1799. <207>

[2137] O. Moreno and C. J. Moreno, Improvements of the Chevalley-Warning and the Ax-Katz theorems, *Amer. J. Math.* 117 (1995) 241–244. <194, 195, 201, 204, 207, 474, 480>

[2138] O. Moreno and I. Rubio, Cyclic decomposition of monomial permutations, *Congr. Numer.* 73 (1990) 147–158. <221, 222>

[2139] O. Moreno, K. W. Shum, F. N. Castro, and P. V. Kumar, Tight bounds for Chevalley-Warning-Ax-Katz type estimates, with improved applications, *Proc. London Math. Soc., 3rd Ser.* 88 (2004) 545–564. <474, 480>

[2140] M. Morf, Doubling algorithms for Toeplitz and related equations, In *Proc. 1980 Int'l Conf. Acoustics Speech and Signal Processing*, 954–959, Denver, Colo., 1980. <526, 527>

[2141] I. H. Morgan, Construction of complete sets of mutually equiorthogonal frequency hypercubes, *Discrete Math.* 186 (1998) 237–251. <545, 547>

[2142] I. H. Morgan and G. L. Mullen, Primitive normal polynomials over finite fields, *Math. Comp.* 63 (1994) 759–765, S19–S23. <83, 85>

[2143] I. H. Morgan and G. L. Mullen, Completely normal primitive basis generators of finite fields, *Utilitas Math.* 49 (1996) 21–43. <84, 85, 90, 130, 131, 132>

[2144] I. H. Morgan, G. L. Mullen, and M. Živković, Almost weakly self-dual bases for finite fields, *Appl. Algebra Engrg. Comm. Comput.* 8 (1997) 25–31. <84, 85, 101, 103>

[2145] J. P. Morgan, Nested designs, In *Design and Analysis of Experiments*, volume 13 of *Handbook of Statist.*, 939–976, North-Holland, Amsterdam, 1996. <586, 587, 590>

[2146] M. Morgenstern, Existence and explicit constructions of $q+1$ regular Ramanujan graphs for every prime power q, *J. Combin. Theory, Ser. B* 62 (1994) 44–62. <646, 649>

[2147] R. Mori and T. Tanaka, Performance and construction of polar codes on symmetric binary-input memoryless channels, In *Proc. IEEE Int. Symp. Information Theory ISIT 2009*, 1496–1500, 2009. <726, 729, 730>

[2148] R. Mori and T. Tanaka, Performance of polar codes with the construction using density evolution, *IEEE Comm. Letters* 13 (2009) 519–521. <730>

[2149] R. Mori and T. Tanaka, Non-binary polar codes using Reed-Solomon codes and algebraic geometry codes, 2010. <730>

[2150] M. Morii and M. Kasahara, Generalized key-equation of remainder decoding algorithm for Reed-Solomon codes, *IEEE Trans. Inform. Theory* 38 (1992) 1801–1807. <686, 694>

[2151] B. Morlaye, Équations diagonales non homogènes sur un corps fini, *C. R. Acad. Sci. Paris, Sér. A-B* 272 (1971) A1545–A1548. <202, 207>

[2152] K. E. Morrison, Integer sequences and matrices over finite fields, *J. Integer Seq.* 9 (2006) Article 06.2.1, 28 pp. <494, 502>

[2153] E. Mortenson, Modularity of a certain Calabi-Yau threefold and combinatorial congruences, *Ramanujan J.* 11 (2006) 5–39. <135, 155>

[2154] M. J. Mossinghoff, Wieferich pairs and Barker sequences, *Des. Codes Cryptogr.* 53 (2009) 149–163. <595, 598>

[2155] C. Mulcahy, Card colm, Mathematical Association of America Online, `http://www.maa.org/columns/colm/cardcolm.html`. <623, 633>

[2156] T. Mulders and A. Storjohann, Rational solutions of singular linear systems, In *Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation*, 242–249, ACM, New York, 2000. <520, 527>

[2157] G. Mullen and H. Stevens, Polynomial functions (mod m), *Acta Math. Hungar.* 44 (1984) 237–241. <222>

[2158] G. L. Mullen, Permutation polynomials in several variables over finite fields, *Acta Arith.* 31 (1976) 107–111. <223, 225>

[2159] G. L. Mullen, Polynomial representation of complete sets of mutually orthogonal frequency squares of prime power order, *Discrete Math.* 69 (1988) 79–84. <544, 545, 547>

[2160] G. L. Mullen, Permutation polynomials and nonsingular feedback shift registers over finite fields, *IEEE Trans. Inform. Theory* 35 (1989) 900–902. <224, 225>

[2161] G. L. Mullen, Dickson polynomials over finite fields, *Adv. in Math. (China)* 20 (1991) 24–32. <219, 222>

[2162] G. L. Mullen, Permutation polynomials over finite fields, In *Finite Fields, Coding Theory, and Advances in Communications and Computing*, volume 141 of *Lecture Notes in Pure and Appl. Math.*, 131–151, Dekker, New York, 1993. <209, 210, 222>

[2163] G. L. Mullen, A candidate for the "next Fermat problem", *Math. Intelligencer* 17 (1995) 18–22. <543, 547>

[2164] G. L. Mullen, Permutation polynomials: a matrix analogue of Schur's conjecture and a survey of recent results, *Finite Fields Appl.* 1 (1995) 242–258. <209, 221, 222>

[2165] G. L. Mullen and C. Mummert, *Finite Fields and Applications*, volume 41 of *Student Mathematical Library*, American Mathematical Society, Providence, RI, 2007.

<11, 29, 30>

[2166] G. L. Mullen and D. Panario, Handbook of Finite Fields (web resource), `http://www.crcpress.com/`, as viewed in July, 2012. <30, 46>

[2167] G. L. Mullen, D. Panario, and I. E. Shparlinski, editors, *Finite Fields and Applications*, volume 461 of *Contemporary Mathematics*, American Mathematical Society, Providence, RI, 2008. <30>

[2168] G. L. Mullen, A. Poli, and H. Stichtenoth, editors, *Finite Fields and Applications*, volume 2948 of *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, 2004. <30>

[2169] G. L. Mullen and W. C. Schmid, An equivalence between (t, m, s)-nets and strongly orthogonal hypercubes, *J. Combin. Theory, Ser. A* 76 (1996) 164–174. <612, 621>

[2170] G. L. Mullen and P. J.-S. Shiue, editors, *Finite Fields, Coding Theory, and Advances in Communications and Computing*, volume 141 of *Lecture Notes in Pure and Applied Mathematics*, Marcel Dekker Inc., New York, 1993. <30>

[2171] G. L. Mullen and P. J.-S. Shiue, editors, *Finite Fields: theory, applications, and algorithms*, volume 168 of *Contemporary Mathematics*, American Mathematical Society, Providence, RI, 1994. <30>

[2172] G. L. Mullen and I. E. Shparlinski, Open problems and conjectures in finite fields, In *Finite Fields and Applications*, volume 233 of *London Math. Soc. Lecture Note Ser.*, 243–268, Cambridge Univ. Press, Cambridge, 1996. <68, 69, 83, 84, 85, 91, 93>

[2173] G. L. Mullen, H. Stichtenoth, and H. Tapia-Recillas, editors, *Finite Fields with Applications to Coding Theory, Cryptography and Related Areas*, Springer-Verlag, Berlin, 2002. <30>

[2174] G. L. Mullen, D. Wan, and Q. Wang, Value sets of polynomials maps over finite fields, Quarterly J. of Math., to appear, 2012. <225>

[2175] G. L. Mullen and D. White, A polynomial representation for logarithms in GF(q), *Acta Arith.* 47 (1986) 255–261. <389, 394>

[2176] P. Müller, New examples of exceptional polynomials, In *Finite Fields: Theory, Applications, and Algorithms*, volume 168 of *Contemp. Math.*, 245–249, Amer. Math. Soc., Providence, RI, 1994. <232, 233>

[2177] P. Müller, Primitive monodromy groups of polynomials, In *Recent Developments in the Inverse Galois Problem*, volume 186 of *Contemp. Math.*, 385–401, Amer. Math. Soc., Providence, RI, 1995. <293, 295>

[2178] P. Müller, A Weil-bound free proof of Schur's conjecture, *Finite Fields Appl.* 3 (1997) 25–32. <220, 222, 230, 231, 233>

[2179] P. Müller, Arithmetically exceptional functions and elliptic curves, In *Aspects of Galois Theory*, volume 256 of *London Math. Soc. Lecture Note Ser.*, 180–201, Cambridge Univ. Press, Cambridge, 1999. <232, 233>

[2180] S. Müller, On the computation of square roots in finite fields, *Des. Codes Cryptogr.* 31 (2004) 301–312. <353, 356>

[2181] V. Müller, Fast multiplication on elliptic curves over small fields of characteristic two, *Journal of Cryptology* 11 (1998) 219–234. <792, 794>

[2182] R. Mullin, I. Onyszchuk, S. Vanstone, and R. Wilson, Optimal normal bases in $GF(p^n)$, *Discrete Appl. Math.* 22 (1988/89) 149–161. <809, 810, 814>

[2183] R. C. Mullin and G. L. Mullen, editors, *Finite Fields: Theory, Applications, and Algorithms*, volume 225 of *Contemporary Mathematics*, American Mathematical

Society, Providence, RI, 1999. <30>

[2184] R. C. Mullin and E. Nemeth, An existence theorem for room squares, *Canad. Math. Bull.* 12 (1969) 493–497. <605, 610>

[2185] R. C. Mullin, I. M. Onyszchuk, S. A. Vanstone, and R. M. Wilson, Optimal normal bases in GF(p^n), *Discrete Appl. Math.* 22 (1988/89) 149–161. <111, 122>

[2186] R. C. Mullin, J. L. Yucas, and G. L. Mullen, A generalized counting and factoring method for polynomials over finite fields, *J. Combin. Math. Combin. Comput.* 72 (2010) 121–143. <53, 54, 55>

[2187] D. Mumford, An algebro-geometric construction of commuting operators and of solutions to the Toda lattice equation, Korteweg deVries equation and related nonlinear equation, In *Proceedings of the International Symposium on Algebraic Geometry*, 115–153, Kinokuniya Book Store, Tokyo, 1978. <537, 538>

[2188] D. Mumford, *Algebraic Geometry. I*, Classics in Mathematics. Springer-Verlag, Berlin, 1995. <380, 386>

[2189] D. Mumford, *The Red Book of Varieties and Schemes*, volume 1358 of *Lecture Notes in Mathematics*, Springer-Verlag, Berlin, expanded edition, 1999. <283, 284, 290, 295>

[2190] A. Munemasa, Orthogonal arrays, primitive trinomials, and shift-register sequences, *Finite Fields Appl.* 4 (1998) 252–260. <85, 622, 629, 633>

[2191] A. Muratović-Ribić, A note on the coefficients of inverse polynomials, *Finite Fields Appl.* 13 (2007) 977–980. <221, 222>

[2192] A. Muratović-Ribić, Inverse of some classes of permutation binomials, *J. Concr. Appl. Math.* 7 (2009) 47–53. <221, 222>

[2193] M. R. Murty, *Problems in Analytic Number Theory*, volume 206 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 2001. <641, 649>

[2194] M. R. Murty, Ramanujan graphs, *J. Ramanujan Math. Soc.* 18 (2003) 33–52. <634, 642, 649>

[2195] D. R. Musser, Multivariate polynomial factorization, *J. Assoc. Comput. Mach.* 22 (1975) 291–308. <378, 386>

[2196] M. Muzychuk, On Skew Hadamard difference sets, arXiv:1012.2089v1, 2010. <595, 598>

[2197] K.-i. Nagao, Improving group law algorithms for Jacobians of hyperelliptic curves, In *Proceedings of the Fourth International Symposium of Algorithmic Number Theory— ANTS-IV*, volume 1838 of *Lecture Notes in Comput. Sci.*, 439–448, Springer, Berlin, 2000. <790, 794>

[2198] K.-i. Nagao, Index calculus attack for Jacobian of hyperelliptic curves of small genus using two large primes, *Japan J. Indust. Appl. Math.* 24 (2007) 289–305. <789, 790, 794>

[2199] M. Nagata, *On Automorphism Group of* $k[x, y]$, Kinokuniya Book-Store Co. Ltd., Department of Mathematics, Kyoto University, Lectures in Mathematics, No. 5, Tokyo, 1972. <759, 774>

[2200] S. Najib, Une généralisation de l'inégalité de Stein-Lorenzini, *J. Algebra* 292 (2005) 566–573. <79, 81>

[2201] A. Naldi, D. Thieffry, and C. Chaouiya, Decision diagrams for the representation and analysis of logical models of genetic networks, In *CMSB'07: Proceedings of the 2007 International Conference on Computational Methods in Systems Biology*, 233–247, Springer-Verlag, Berlin, Heidelberg, 2007. <817, 824>

[2202] A. H. Namin, H. Wu, and M. Ahmadi, A new finite field multiplier using redundant

representation, *IEEE Trans. Comput.* 57 (2008) 716–720. <813, 814>

[2203] Y. Nawaz and G. Gong, The WG stream cipher, 2005, preprint available at `http://www.cacr.math.uwaterloo.ca/techreports/2005/cacr2005-15.pdf`. <741, 745, 746, 747, 754>

[2204] M. Nazarathy, S. Newton, R. Giffard, D. Moberly, F. Sischka, W. Trutna, Jr., and S. Foster, Real-time long range complementary correlation optical time domain reflectometer, *IEEE J. Lightwave Technology* 7 (1989) 24–38. <833, 839>

[2205] V. I. Nechaev, On the complexity of a deterministic algorithm for a discrete logarithm, *Mat. Zametki* 55 (1994) 91–101, 189. <388, 394>

[2206] NESSIE: New European Schemes for Signatures, Integrity, and Encryption. Information Society Technologies programme of the European commission (IST-1999-12324), `http://www.cryptonessie.org/`. <763, 774>

[2207] J. C. Néto, A. F. Tenca, and W. V. Ruggiero, A parallel k-partition method to perform Montgomery multiplication, In *Proc. ASAP-2011*, 251–254, 2011. <813, 814>

[2208] E. Netto, Zur Theorie der Tripelsysteme, *Math. Ann.* 42 (1893) 143–152. <582, 590>

[2209] P. M. Neumann, *The Mathematical Writings of Evariste Galois*, European Mathematical Society, Zurich, 2011. <12, 30>

[2210] T. Neumann, *Bent Functions*, PhD thesis, Department of Mathematics, University of Kaiserslautern, Germany, 2006. <265>

[2211] D. K. Nguyen and B. Schmidt, Fast computation of Gauss sums and resolution of the root of unity ambiguity, *Acta Arith.* 140 (2009) 205–232. <135, 155>

[2212] X. Nie, L. Hu, J. Li, C. Updegrove, and J. Ding, Breaking a new instance of ttm cryptosystems., In J. Zhou, M. Yung, and F. Bao, editors, *ACNS*, volume 3989 of *Lecture Notes in Computer Science*, 210–225, 2006. <765, 774>

[2213] H. Niederreiter, Permutation polynomials in several variables over finite fields, *Proc. Japan Acad.* 46 (1970) 1001–1005. <224, 225>

[2214] H. Niederreiter, Orthogonal systems of polynomials in finite fields, *Proc. Amer. Math. Soc.* 28 (1971) 415–422. <223, 224, 225>

[2215] H. Niederreiter, Permutation polynomials in several variables, *Acta Sci. Math. (Szeged)* 33 (1972) 53–58. <224, 225>

[2216] H. Niederreiter, On the distribution of pseudo-random numbers generated by the linear congruential method. II, *Math. Comp.* 28 (1974) 1117–1132. <168, 179>

[2217] H. Niederreiter, On the cycle structure of linear recurring sequences, *Math. Scand.* 38 (1976) 53–77. <309, 310>

[2218] H. Niederreiter, Weights of cyclic codes, *Information and Control* 34 (1977) 130–140. <310>

[2219] H. Niederreiter, Distribution properties of feedback shift register sequences, *Problems Control Inform. Theory* 15 (1986) 19–34. <309, 310>

[2220] H. Niederreiter, Low-discrepancy point sets, *Monatsh. Math.* 102 (1986) 155–167. <613, 621>

[2221] H. Niederreiter, Continued fractions for formal power series, pseudorandom numbers, and linear complexity of sequences, In *Contributions to General Algebra, 5*, 221–233, Hölder-Pichler-Tempsky, Vienna, 1987. <323, 329>

[2222] H. Niederreiter, Point sets and sequences with small discrepancy, *Monatsh. Math.* 104 (1987) 273–337. <611, 612, 613, 617, 619, 621>

[2223] H. Niederreiter, A simple and general approach to the decimation of feedback shift-register sequences, *Problems Control Inform. Theory* 17 (1988) 327–331. <306, 310>

[2224] H. Niederreiter, Low-discrepancy and low-dispersion sequences, *J. Number Theory* 30 (1988) 51–70. <617, 618, 619, 621>

[2225] H. Niederreiter, The probabilistic theory of linear complexity, In *Advances in Cryptology—EUROCRYPT '88*, volume 330 of *Lecture Notes in Comput. Sci.*, 191–209, Springer, Berlin, 1988. <322, 323, 329>

[2226] H. Niederreiter, Sequences with almost perfect linear complexity profile, In *Advances in Cryptology—EUROCRYPT '87*, volume 304 of *Lecture Notes in Comput. Sci.*, 37–51, Springer, Berlin, 1988. <321, 322, 323, 329>

[2227] H. Niederreiter, Some new cryptosystems based on feedback shift register sequences, *Math. J. Okayama Univ.* 30 (1988) 121–149. <309, 310>

[2228] H. Niederreiter, A combinatorial approach to probabilistic results on the linear-complexity profile of random sequences, *J. Cryptology* 2 (1990) 105–112. <323, 329>

[2229] H. Niederreiter, Keystream sequences with a good linear complexity profile for every starting point, In *Advances in Cryptology—EUROCRYPT '89*, volume 434 of *Lecture Notes in Comput. Sci.*, 523–532, Springer, Berlin, 1990. <323, 329>

[2230] H. Niederreiter, A short proof for explicit formulas for discrete logarithms in finite fields, *Appl. Algebra Engrg. Comm. Comput.* 1 (1990) 55–57. <389, 394>

[2231] H. Niederreiter, The distribution of values of Kloosterman sums, *Arch. Math. (Basel)* 56 (1991) 270–277. <151, 155>

[2232] H. Niederreiter, The linear complexity profile and the jump complexity of keystream sequences, In *Advances in Cryptology—EUROCRYPT '90*, volume 473 of *Lecture Notes in Comput. Sci.*, 174–188, Springer, Berlin, 1991. <322, 323, 329>

[2233] H. Niederreiter, Low-discrepancy point sets obtained by digital constructions over finite fields, *Czechoslovak Math. J.* 42 (1992) 143–166. <614, 615, 621>

[2234] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, volume 63 of *CBMS-NSF Regional Conference Series in Applied Mathematics*, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1992. <168, 179, 310, 611, 613, 618, 621>

[2235] H. Niederreiter, A new efficient factorization algorithm for polynomials over small finite fields, *Appl. Algebra Engrg. Comm. Comput.* 4 (1993) 81–87. <307, 310, 374, 375>

[2236] H. Niederreiter, Factoring polynomials over finite fields using differential equations and normal bases, *Mathematics of Computation* 62 (1994) 819–830. <374, 375>

[2237] H. Niederreiter, Constructions of (t, m, s)-nets, In *Monte Carlo and Quasi-Monte Carlo Methods*, 70–85, Springer-Verlag, Berlin, 2000. <616, 621>

[2238] H. Niederreiter, editor, *Coding Theory and Cryptology*, volume 1 of *Lecture Notes Series, Institute for Mathematical Sciences, National University of Singapore*, World Scientific Publishing Co. Inc., River Edge, NJ, 2002. <29, 30>

[2239] H. Niederreiter, Linear complexity and related complexity measures for sequences, In *Progress in Cryptology—INDOCRYPT 2003*, volume 2904 of *Lecture Notes in Comput. Sci.*, 1–17, Springer, Berlin, 2003. <323, 329>

[2240] H. Niederreiter, Periodic sequences with large k-error linear complexity, *IEEE Trans. Inform. Theory* 49 (2003) 501–505. <324, 329>

[2241] H. Niederreiter, Digital nets and coding theory, In *Coding, Cryptography and Combinatorics*, volume 23 of *Progr. Comput. Sci. Appl. Logic*, 247–257, Birkhäuser, Basel, 2004. <615, 621>

[2242] H. Niederreiter, Constructions of (t, m, s)-nets and (t, s)-sequences, *Finite Fields Appl.* 11 (2005) 578–600. <616, 621>

[2243] H. Niederreiter, The probabilistic theory of the joint linear complexity of multisequences, In *Sequences and Their Applications—SETA 2006*, volume 4086 of *Lecture Notes in Comput. Sci.*, 5–16, Springer, Berlin, 2006. <323, 329>

[2244] H. Niederreiter, Nets, (t, s)-sequences, and codes, In *Monte Carlo and Quasi-Monte Carlo Methods*, 83–100, Springer-Verlag, Berlin, 2008. <614, 619, 621>

[2245] H. Niederreiter, Quasi-Monte Carlo methods, In *Encyclopedia of Quantitative Finance*, 1460–1472, John Wiley and Sons, Chichester, 2010. <611, 621>

[2246] H. Niederreiter and R. Göttfert, Factorization of polynomials over finite fields and characteristic sequences, *J. Symbolic Comput.* 16 (1993) 401–412. <307, 310>

[2247] H. Niederreiter and F. Özbudak, Constructions of digital nets using global function fields, *Acta Arith.* 105 (2002) 279–302. <615, 621>

[2248] H. Niederreiter and F. Özbudak, Constructive asymptotic codes with an improvement on the Tsfasman-Vlăduţ-Zink and Xing bounds, In *Coding, Cryptography and Combinatorics*, volume 23 of *Progr. Comput. Sci. Appl. Logic*, 259–275, Birkhäuser, Basel, 2004. <703>

[2249] H. Niederreiter and F. Özbudak, Matrix-product constructions of digital nets, *Finite Fields Appl.* 10 (2004) 464–479. <616, 621>

[2250] H. Niederreiter and F. Özbudak, Further improvements on asymptotic bounds for codes using distinguished divisors, *Finite Fields Appl.* 13 (2007) 423–443. <703>

[2251] H. Niederreiter and F. Özbudak, Improved asymptotic bounds for codes using distinguished divisors of global function fields, *SIAM J. Discrete Math.* 21 (2007) 865–899. <703>

[2252] H. Niederreiter and F. Özbudak, Low-discrepancy sequences using duality and global function fields, *Acta Arith.* 130 (2007) 79–97. <620, 621>

[2253] H. Niederreiter and G. Pirsic, Duality for digital nets and its applications, *Acta Arith.* 97 (2001) 173–182. <614, 621>

[2254] H. Niederreiter and K. H. Robinson, Complete mappings of finite fields, *J. Austral. Math. Soc., Ser. A* 33 (1982) 197–212. <221, 222>

[2255] H. Niederreiter and I. E. Shparlinski, On the distribution and lattice structure of nonlinear congruential pseudorandom numbers, *Finite Fields Appl.* 5 (1999) 246–253. <333, 337>

[2256] H. Niederreiter and I. E. Shparlinski, On the distribution of inversive congruential pseudorandom numbers in parts of the period, *Math. Comp.* 70 (2001) 1569–1574. <174, 179, 333, 337>

[2257] H. Niederreiter and I. E. Shparlinski, Dynamical systems generated by rational functions, In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 2643 of *Lecture Notes in Comput. Sci.*, 6–17, Springer, Berlin, 2003. <330, 331, 337>

[2258] H. Niederreiter and I. E. Shparlinski, On the distribution of power residues and primitive elements in some nonlinear recurring sequences, *Bull. London Math. Soc.* 35 (2003) 522–528. <334, 337>

[2259] H. Niederreiter and I. E. Shparlinski, Periodic sequences with maximal linear com-

plexity and almost maximal k-error linear complexity, In *Cryptography and Coding*, volume 2898 of *Lecture Notes in Comput. Sci.*, 183–189, Springer, Berlin, 2003. <324, 329>

[2260] H. Niederreiter and A. Venkateswarlu, Periodic multisequences with large error linear complexity, *Des. Codes Cryptogr.* 49 (2008) 33–45. <324, 329>

[2261] H. Niederreiter and L.-P. Wang, Proof of a conjecture on the joint linear complexity profile of multisequences, In *Progress in Cryptology—INDOCRYPT 2005*, volume 3797 of *Lecture Notes in Comput. Sci.*, 13–22, Springer, Berlin, 2005. <323, 330>

[2262] H. Niederreiter and L.-P. Wang, The asymptotic behavior of the joint linear complexity profile of multisequences, *Monatsh. Math.* 150 (2007) 141–155. <323, 330>

[2263] H. Niederreiter and A. Winterhof, Multiplicative character sums for nonlinear recurring sequences, *Acta Arith.* 111 (2004) 299–305. <334, 337>

[2264] H. Niederreiter and A. Winterhof, Cyclotomic R-orthomorphisms of finite fields, *Discrete Math.* 295 (2005) 161–171. <165, 179, 214, 221, 222>

[2265] H. Niederreiter and A. Winterhof, Exponential sums for nonlinear recurring sequences, *Finite Fields Appl.* 14 (2008) 59–64. <333, 337>

[2266] H. Niederreiter and C. Xing, *Rational Points on Curves over Finite Fields: Theory and Applications*, volume 285 of *London Mathematical Society Lecture Note Series*, Cambridge University Press, Cambridge, 2001. <30, 399, 415, 453, 456, 457, 461, 462, 538, 699, 701, 703>

[2267] H. Niederreiter and C. Xing, *Algebraic Geometry in Coding Theory and Cryptography*, Princeton University Press, Princeton, NJ, 2009. <29, 30, 399, 414, 415, 696, 698, 703>

[2268] H. Niederreiter and C. P. Xing, Low-discrepancy sequences and global function fields with many rational places, *Finite Fields Appl.* 2 (1996) 241–273. <620, 621>

[2269] H. Niederreiter and C. P. Xing, Quasirandom points and global function fields, In *Finite Fields and Applications*, volume 233 of *London Math. Soc. Lecture Note Ser.*, 269–296, Cambridge University Press, Cambridge, 1996. <617, 621>

[2270] H. Niederreiter and C. P. Xing, Towers of global function fields with asymptotically many rational places and an improvement on the Gilbert-Varshamov bound, *Math. Nachr.* 195 (1998) 171–186. <702, 703>

[2271] H. Niederreiter, C. P. Xing, and K. Y. Lam, A new construction of algebraic-geometry codes, *Appl. Algebra Engrg. Comm. Comput.* 9 (1999) 373–381. <696, 697, 703>

[2272] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000. <824, 831>

[2273] Y. Niho, *Multi-Valued Cross-Correlation functions Between two Maximal Linear Recursive Sequences*, PhD thesis, Univ. Southern California, 1972. <254>

[2274] Y. Niitsuma, Counting points of the curve $y^2 = x^{12} + a$ over a finite field, *Tokyo J. Math.* 31 (2008) 59–94. <143, 155>

[2275] A. Nilli, On the second eigenvalue of a graph, *Discrete Math.* 91 (1991) 207–210. <637, 649>

[2276] A. Nilli, Tight estimates for eigenvalues of regular graphs, *Electron. J. Combin.* 11 (2004) Note 9, 4 pp. <637, 638, 649>

[2277] A. Nimbalker, T. K. Blankenship, B. Classon, T. E. Fuja, and D. J. Costello, Jr.,

Contention-free interleavers, In *Proc. 2004 IEEE International Symposium on Information Theory*, 54, Chicago, IL, 2004. <717, 718>

[2278] NIST, Digital signature standard (DSS), Federal Information Processing Standards Publication 186-3, National Institute of Standards and Technology, 2009. <776, 778, 787>

[2279] I. Niven, Fermat's theorem for matrices, *Duke Math. J.* 15 (1948) 823–826. <493, 502>

[2280] J.-S. No, S. W. Golomb, G. Gong, H.-K. Lee, and P. Gaal, Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation, *IEEE Transactions on Information Theory* 44 (1998) 814–817. <745, 746, 754>

[2281] J. S. No and P. V. Kumar, A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span, *IEEE Trans. Inform. Theory* IT-35 (1989) 371–379. <314, 317>

[2282] W. Nöbauer, On the length of cycles of polynomial permutations, In *Contributions to General Algebra, 3*, 265–274, Hölder-Pichler-Tempsky, Vienna, 1985. <221, 222>

[2283] E. Noether, Normalbasis bei Körpen ohne höhere Verzweigung, *J. Reine Angew. Math.* 167 (1932) 147–152. <104, 110>

[2284] A. W. Nordstrom and J. P. Robinson, An optimum nonlinear code, *Information and Control* 11 (1967) 613–616. <692, 693, 694>

[2285] M. Noro and K. Yokoyama, Yet another practical implementation of polynomial factorization over finite fields, In *ISSAC '02: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, 200–206. ACM, 2002. <380, 386>

[2286] A. Nowicki, W. Secomski, J. Litniewski, I. Trots, and P. A. Lewin, On the application of signal compression using Golay's codes sequences in ultrasonic diagnostic, *Arch. Acoustics* 28 (2003) 313–324. <833, 839>

[2287] M. Nüsken and M. Ziegler, Fast multipoint evaluation of bivariate polynomials, In *Twelfth Annual European Symposium on Algorithms (ESA)*, volume 3221 of *Lecture Notes in Comput. Sci.*, 544–555, Springer, Berlin, 2004. <374, 375>

[2288] K. Nyberg, Perfect nonlinear S-boxes, In *Advances in Cryptology—EUROCRYPT '91*, volume 547 of *Lecture Notes in Comput. Sci.*, 378–386, Springer, Berlin, 1991. <247, 254, 265>

[2289] K. Nyberg, Differentially uniform mappings for cryptography, In *Advances in Cryptology—EUROCRYPT '93*, volume 765 of *Lecture Notes in Comput. Sci.*, 55–64, Springer, Berlin, 1994. <249, 252, 254>

[2290] K. Nyberg and L. R. Knudsen, Provable security against differential cryptanalysis, In *Advances in Cryptology—CRYPTO '92*, volume 740 of *Lecture Notes in Comput. Sci.*, 566–574, Springer, Berlin, 1993. <247, 248, 254>

[2291] L. O'Connor, An analysis of exponentiation based on formal languages, In *Advances in Cryptology—EUROCRYPT '99*, volume 1592 of *Lecture Notes in Comput. Sci.*, 375–388, Springer, Berlin, 1999. <350, 356>

[2292] A. Odlyzko, Discrete logarithms: the past and the future, *Des. Codes Cryptogr.* 19 (2000) 129–145. <386, 394>

[2293] A. M. Odlyzko, Discrete logarithms in finite fields and their cryptographic significance, In *Advances in Cryptology*, volume 209 of *Lecture Notes in Comput. Sci.*, 224–314, Springer, Berlin, 1985. <341, 356, 358, 363, 367, 386, 391, 392, 394>

[2294] A. M. Odlyzko, Asymptotic enumeration methods, In *Handbook of Combinatorics, Vol. 2*, 1063–1229, Elsevier, Amsterdam, 1995. <360, 367>

[2295] A. P. Ogg, Abelian curves of small conductor, *J. Reine Angew. Math.* 226 (1967) 204–215. <292, 295>

[2296] A. P. Ogg, Rational points of finite order on elliptic curves, *Invent. Math.* 12 (1971) 105–111. <291, 295>

[2297] E. Okamoto and K. Nakamura, Evaluation of public key cryptosystems proposed recently, In *Proc. 1986 Symposium of Cryptography and Information Security*, volume D1, 1986. <758, 774>

[2298] C. M. O'Keefe and T. Penttila, Ovoids of PG(3, 16) are elliptic quadrics, *J. Geom.* 38 (1990) 95–106. <580>

[2299] C. M. O'Keefe and T. Penttila, Ovoids of PG(3, 16) are elliptic quadrics II, *J. Geom.* 44 (1992) 140–159. <580>

[2300] C. M. O'Keefe, T. Penttila, and G. F. Royle, Classification of ovoids in PG(3, 32), *J. Geom.* 50 (1994) 143–150. <580>

[2301] M. Olofsson, *VLSI Aspects on Inversion in Finite Fields*, PhD thesis, Department of Electrical Engineering, Linkopings Universitet, 2002. <807, 814>

[2302] J. D. Olsen, R. A. Scholtz, and L. R. Welch, Bent-function sequences, *IEEE Trans. Inform. Theory* 28 (1982) 858–864. <245>

[2303] B. Omidi Koma, D. Panario, and Q. Wang, The number of irreducible polynomials of degree n over $\mathbb{F}_q$ with given trace and constant terms, *Discrete Math.* 310 (2010) 1282–1292. <71, 72, 75>

[2304] R. Omrani, O. Moreno, and P. V. Kumar, Improved Johnson bounds for optical orthogonal codes with $\lambda > 1$ and some optimal constructions, In *Proc. Int. Symp. Inform. Theory*, 259–263, 2005. <834, 839>

[2305] H. Ong, C. Schnorr, and A. Shamir, Signatures through approximate representations by quadratic forms, In *Advances in Cryptology—CRYPTO 1983*, 117–131. Plenum Publ., 1984. <755, 758, 774>

[2306] H. Ong, C.-P. Schnorr, and A. Shamir, Efficient signature schemes based on polynomial equations, In *Advances in Cryptology*, volume 196 of *Lecture Notes in Comput. Sci.*, 37–46, Springer, Berlin, 1985. <758, 774>

[2307] F. Oort, Moduli of abelian varieties and Newton polygons, *C. R. Acad. Sci. Paris, Sér. I, Math.* 312 (1991) 385–389. <479, 480>

[2308] O. Ore, Über die reduzibilität von algebraischen gleichungen, *Skrifter Norsk Vid. Akad. Oslo* (1923). <58, 61>

[2309] O. Ore, Contributions to the theory of finite fields, *Trans. Amer. Math. Soc.* 36 (1934) 243–274. <56, 59, 61, 62, 66, 67, 69, 106, 110>

[2310] B. Ors, L. Batina, B. Preneel, and J. Vandewalle, Hardware implementation of an elliptic curve processor over $GF(p)$ with Montgomery modular multiplier, *International Journal of Embedded Systems* 3 (2008) 229–240. <813, 814>

[2311] A. Ostafe, Multivariate permutation polynomial systems and nonlinear pseudorandom number generators, *Finite Fields Appl.* 16 (2010) 144–154. <225, 334, 335, 337>

[2312] A. Ostafe, Pseudorandom vector sequences derived from triangular polynomial systems with constant multipliers, In *Arithmetic of Finite Fields*, volume 6087 of *Lecture Notes in Comput. Sci.*, 62–72, Springer, Berlin, 2010. <334, 335, 337>

[2313] A. Ostafe, Pseudorandom vector sequences of maximal period generated by trian-

gular polynomial dynamical systems, *Des. Codes Cryptogr.* 63 (2012) 59–72. <332, 335, 337>

[2314] A. Ostafe, E. Pelican, and I. E. Shparlinski, On pseudorandom numbers from multivariate polynomial systems, *Finite Fields Appl.* 16 (2010) 320–328. <331, 332, 333, 337>

[2315] A. Ostafe and I. E. Shparlinski, On the degree growth in some polynomial dynamical systems and nonlinear pseudorandom number generators, *Math. Comp.* 79 (2010) 501–511. <332, 334, 335, 337>

[2316] A. Ostafe and I. E. Shparlinski, On the length of critical orbits of stable quadratic polynomials, *Proc. Amer. Math. Soc.* 138 (2010) 2653–2656. <172, 179, 335, 336, 337>

[2317] A. Ostafe and I. E. Shparlinski, Pseudorandom numbers and hash functions from iterations of multivariate polynomials, *Cryptogr. Commun.* 2 (2010) 49–67. <332, 334, 335, 337>

[2318] A. Ostafe and I. E. Shparlinski, Degree growth, linear independence and periods of a class of rational dynamical systems, Preprint, 2011. <332, 334, 335, 337>

[2319] A. Ostafe and I. E. Shparlinski, On the Waring problem with Dickson polynomials in finite fields, *Proc. Amer. Math. Soc.* 139 (2011) 3815–3820. <186, 207>

[2320] A. Ostafe and I. E. Shparlinski, On the power generator and its multivariate analogue, *J. Complexity* 28 (2012) 238–249. <332, 333, 337>

[2321] A. Ostafe, I. E. Shparlinski, and A. Winterhof, On the generalized joint linear complexity profile of a class of nonlinear pseudorandom multisequences, *Adv. Math. Commun.* 4 (2010) 369–379. <334, 335, 337>

[2322] A. Ostafe, I. E. Shparlinski, and A. Winterhof, Multiplicative character sums of a class of nonlinear recurrence vector sequences, *Int. J. Number Theory* 7 (2011) 1557–1571. <334, 335, 337>

[2323] A. M. Ostrowski, Über die Bedeutung der Theorie der konvexen Polyeder für die formale Algebra, *Jahresber. Deutsch. Math.-Verein.* 30 (1921) 98–99. <381, 386, 963>

[2324] A. M. Ostrowski, On the significance of the theory of convex polyhedra for formal algebra, *ACM SIGSAM Bull.* 33 (1999) 5, Translated from [2323]. <381, 386>

[2325] P. Oswald and A. Shokrollahi, Capacity-achieving sequences for the erasure channel, *IEEE Trans. Inform. Theory* 48 (2002) 3017–3028. <720, 725>

[2326] F. Özbudak, On maximal curves and linearized permutation polynomials over finite fields, *J. Pure Appl. Algebra* 162 (2001) 87–102. <232, 233>

[2327] C. Paar, A new architecture for a parallel finite field multiplier with low complexity based on composite fields, *IEEE Trans. Comput.* 45 (1996) 856–861. <804, 805, 814>

[2328] L. J. Paige, Neofields, *Duke Math. J.* 16 (1949) 39–60. <26, 30>

[2329] R. Paley, On orthogonal matrices., *J. Math. Phys., Mass. Inst. Techn.* 12 (1933) 311–320. <164, 179>

[2330] R. E. A. C. Paley, On orthogonal matrices, *J. Math. Phys* 12 (1933) 311–320. <600, 610>

[2331] V. Y. Pan, *Structured Matrices and Polynomials: Unified Superfast Algorithms*, Birkhäuser Boston Inc., Boston, MA, 2001. <525, 527>

[2332] D. Panario, What do random polynomials over finite fields look like?, In *Finite Fields and Applications*, volume 2948 of *Lecture Notes in Comput. Sci.*, 89–108, Springer, Berlin, 2004. <358, 367>

[2333] D. Panario, X. Gourdon, and P. Flajolet, An analytic approach to smooth polynomials over finite fields, In *Algorithmic Number Theory*, volume 1423 of *Lecture Notes in Comput. Sci.*, 226–236, Springer, Berlin, 1998. <392, 394>

[2334] D. Panario, B. Pittel, B. Richmond, and A. Viola, Analysis of Rabin's irreducibility test for polynomials over finite fields, *Random Structures Algorithms* 19 (2001) 525–551. <362, 367, 369, 373>

[2335] D. Panario and B. Richmond, Analysis of Ben-Or's polynomial irreducibility test, *Random Structures Algorithms* 13 (1998) 439–456. <362, 367, 370, 373>

[2336] D. Panario and B. Richmond, Exact largest and smallest size of components, *Algorithmica* 31 (2001) 413–432. <364, 366, 367>

[2337] D. Panario and B. Richmond, Smallest components in decomposable structures: exp-log class, *Algorithmica* 29 (2001) 205–226. <364, 367>

[2338] D. Panario, A. Sakzad, B. Stevens, and Q. Wang, Two new measures for permutations: ambiguity and deficiency, *IEEE Trans. Inform. Theory* 57 (2011) 7648–7657. <222>

[2339] D. Panario, O. Sosnovski, B. Stevens, and Q. Wang, Divisibility of polynomials over finite fields and combinatorial applications, *Des. Codes Cryptogr.* 63 (2012) 425–445. <622, 632, 633>

[2340] D. Panario, B. Stevens, and Q. Wang, Ambiguity and deficiency in Costas arrays and APN permutations, In *LATIN 2010: Theoretical Informatics*, volume 6034 of *Lecture Notes in Computer Science, 2010*, 397–406, Dekker, New York, 2010. <222>

[2341] D. Panario and D. Thomson, Efficient pth root computations in finite fields of characteristic p, *Des. Codes Cryptogr.* 50 (2009) 351–358. <35, 46, 66, 69>

[2342] D. Panario and A. Viola, Analysis of Rabin's polynomial irreducibility test, In *LATIN'98: theoretical informatics (Campinas, 1998)*, volume 1380 of *Lecture Notes in Comput. Sci.*, 1–10, Springer, Berlin, 1998. <369, 373>

[2343] G. Panella, Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito, *Boll. Un. Mat. Ital. Ser. III* 10 (1955) 507–513. <579, 580>

[2344] Y. H. Park and J. B. Lee, Permutation polynomials and group permutation polynomials, *Bull. Austral. Math. Soc.* 63 (2001) 67–74. <214, 222>

[2345] K. R. Parthasarathy, *Quantum Computation, Quantum Error Correcting Codes and Information Theory*, Published for the Tata Institute of Fundamental Research, Mumbai, 2006. <824, 831>

[2346] F. Parvaresh and A. Vardy, Correcting errors beyond the Guruswami-Sudan radius in polynomial time, In *Proceedings of the Forty Sixth Annual IEEE Symposium on Foundations of Computer Science, 2005*, 285–294, 2005. <690, 694>

[2347] E. Pasalic, On cryptographically significant mappings over GF(2^n), In *Arithmetic of Finite Fields*, volume 5130 of *Lecture Notes in Comput. Sci.*, 189–204, Springer, Berlin, 2008. <219, 222>

[2348] E. Pasalic and P. Charpin, Some results concerning cryptographically significant mappings over GF(2^n), *Des. Codes Cryptogr.* 57 (2010) 257–269. <219, 222>

[2349] J. Patarin, The oil and vinegar signature scheme, Dagstuhl Workshop on Cryptography, September 1997. <761, 774>

[2350] J. Patarin, Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt '88, In *Advances in Cryptology—CRYPTO '95*, volume 963 of *Lecture Notes in Comput. Sci.*, 248–261, Springer, Berlin, 1995. <760, 767, 774>

[2351] J. Patarin, Asymmetric cryptography with a hidden monomial and a candidate algorithm for $\simeq$ 64 bits asymmetric signatures, In *Advances in Cryptology—CRYPTO '96*, volume 1109 of *Lecture Notes in Comput. Sci.*, 45–60, Springer, Berlin, 1996. <757, 774>

[2352] J. Patarin, Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms, In *1996*, volume 1070 of *Lecture Notes in Computer Science*, 33–48. Ueli Maurer, ed., 1996, Extended Version: `http://www.minrank.org/hfe.pdf`. <758, 774>

[2353] J. Patarin, N. T. Courtois, and L. Goubin, FLASH, a fast multivariate signature algorithm, In *Topics in Cryptology—CT-RSA 2001*, volume 2020 of *Lecture Notes in Comput. Sci.*, 298–307, Springer, Berlin, 2001. <763, 774>

[2354] J. Patarin, N. T. Courtois, and L. Goubin, QUARTZ, 128-bit long digital signatures, In *Topics in Cryptology—CT-RSA 2001*, volume 2020 of *Lecture Notes in Comput. Sci.*, 282–297, Springer, Berlin, 2001. <761, 774>

[2355] J. Patarin, L. Goubin, and N. T. Courtois, C^*_{-+} and HM: Variations around two schemes of T. Matsumoto and H. Imai, In *Asiacrypt 1998*, volume 1514 of *LNCS*, 35–49. Kazuo Ohta and Dingyi Pei, editors, Springer, 1998, Extended Version: `http://citeseer.nj.nec.com/patarin98plusmn.html`. <763, 768, 774>

[2356] J. Patarin, L. Goubin, and N. T. Courtois, Improved algorithms for Isomorphisms of Polynomials, In *1998*, volume 1403 of *Lecture Notes in Computer Science*, 184–200. Kaisa Nyberg, ed., 1998, Extended Version: `http://www.minrank.org/ip6long.ps`. <758, 774>

[2357] K. G. Paterson, Applications of exponential sums in communications theory, In *Cryptography and Coding*, volume 1746 of *Lecture Notes in Comput. Sci.*, 1–24, Springer, Berlin, 1999. <173, 174, 179>

[2358] S. Paulus and H.-G. Rück, Real and imaginary quadratic representations of hyperelliptic function fields, *Math. Comp.* 68 (1999) 1233–1241. <441, 444, 445, 449>

[2359] S. E. Payne, Spreads, flocks, and generalized quadrangles, *J. Geom.* 33 (1988) 113–128. <559, 565>

[2360] F. Pellarin, Values of certain l-series in positive characteristic, preprint available, `http://arxiv.org/abs/1107.4511`, 2011. <538>

[2361] A. Pellet, Sur les fonctions irréducibles suivant un module premier, *C.R. Acad. Sci. Paris* 93 (1881) 1065–1066. <56, 61>

[2362] A. Pellet, Sur les fonctions réduites suivant un module premier, *Bull. Soc. Math. France* 17 (1889) 156–167. <59, 61>

[2363] A. E. Pellet, Sur les fonctions irréductibles suivant un module premier et une fonction modulaire., *C. R. Acad. Sci. Paris.* 70 (1870) 328–330. <58, 59, 61, 67, 69>

[2364] A. E. Pellet, Sur la décomposition d'une fonction entière en facteurs irréductibles suivant un module premier., *C. R. Acad. Sci. Paris.* 86 (1878) 1071–1072. <62, 63, 66>

[2365] R. Pellikaan, B.-Z. Shen, and G. J. M. van Wee, Which linear codes are algebraic-geometric?, *IEEE Trans. Inform. Theory* 37 (1991) 583–602. <701, 703>

[2366] J. Pelzl, T. Wollinger, and C. Paar, High performance arithmetic for hyperelliptic curve cryptosystems of genus two, *Information Technology: Coding and Computing (ITCC)* 2 (2004) 513–517. <790, 794>

[2367] T. Penttila and G. F. Royle, Sets of type (m, n) in the affine and projective planes of order nine, *Des. Codes Cryptogr.* 6 (1995) 229–245. <563, 565>

[2368] T. Penttila and B. Williams, Ovoids of parabolic spaces, *Geom. Dedicata* 82 (2000) 1–19. <274>

[2369] G. I. Perel′muter, Estimate of a sum along an algebraic curve, *Mat. Zametki* 5 (1969) 373–380. <162, 163>

[2370] S. Perlis, Normal bases of cyclic fields of prime-power degree, *Duke Math J.* 9 (1942) 507–517. <106, 110>

[2371] C. Pernet and A. Storjohann, Faster algorithms for the characteristic polynomial, In *ISSAC 2007*, 307–314, ACM, New York, 2007. <522, 527>

[2372] L. Perret, A fast cryptanalysis of the isomorphism of polynomials with one secret problem, In *Advances in Cryptology—EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Comput. Sci.*, 354–370, Springer, Berlin, 2005. <758, 774>

[2373] O. Perron, Bemerkungen über die Verteilung der quadratischen Reste, *Math. Z.* 56 (1952) 122–130. <312, 317>

[2374] W. W. Peterson, *Error-Correcting Codes*, The M.I.T. Press, Cambridge, Mass., 1961. <652, 665, 683, 694>

[2375] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, The M.I.T. Press, Cambridge, Mass., second edition, 1972. <309, 310, 652, 664, 665, 672, 677, 679, 683, 684, 687, 688, 694>

[2376] K. Petr, Über die Reduzibilität eines Polynoms mit ganzzahligen Koeffizienten nach einem Primzahlmodul, *Časopis pro pěstování matematiky a fysiky* 66 (1937) 85–94. <368, 373, 374, 375>

[2377] E. Petterson, Über die Irreduzibilität ganzzahliger Polynome nach einem Primzahlmodul, *J. Reine Angew. Math.* 175 (1936) 209–220. <56, 58, 61>

[2378] D. Pierce and M. J. Kallaher, A note on planar functions and their planes, *Bull. Inst. Combin. Appl.* 42 (2004) 53–75. <272, 274>

[2379] J. Pila, Frobenius maps of abelian varieties and finding roots of unity in finite fields, *Math. Comp.* 55 (1990) 745–763. <483, 484, 794>

[2380] A. Pincin, Bases for finite fields and a canonical decomposition for a normal basis generator, *Comm. Algebra* 17 (1989) 1337–1352. <105, 110>

[2381] N. Pippenger, On the evaluation of powers and monomials, *SIAM J. Comput.* 9 (1980) 230–250. <349, 356>

[2382] F. Piroi and A. Winterhof, Quantum period reconstruction of binary sequences, In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 3857 of *Lecture Notes in Comput. Sci.*, 60–67, Springer, Berlin, 2006. <829, 831>

[2383] G. Pirsic, J. Dick, and F. Pillichshammer, Cyclic digital nets, hyperplane nets, and multivariate integration in Sobolev spaces, *SIAM J. Numer. Anal.* 44 (2006) 385–411. <616, 621>

[2384] N. L. Pitcher, *Efficient Point-Counting on Genus-2 Hyperelliptic Curves*, ProQuest LLC, Ann Arbor, MI, 2009, Thesis (Ph.D.)–University of Illinois at Chicago. <447, 449>

[2385] D. A. Plaisted, New NP-hard and NP-complete polynomial and integer divisibility problems, *Theoret. Comput. Sci.* 13 (1984) 125–138. <383, 386>

[2386] M. Planat, H. C. Rosu, and S. Perrine, A survey of finite algebraic geometrical structures underlying mutually unbiased quantum measurements, *Found. Phys.* 36 (2006) 1662–1680. <825, 831>

[2387] V. Pless, Q-codes, *J. Combin. Theory, Ser. A* 43 (1986) 258–276. <673, 694>

[2388] V. Pless, Duadic codes and generalizations, In *Eurocode '92*, volume 339 of *CISM Courses and Lectures*, 3–15, Springer, Vienna, 1993. <673, 694>

[2389] V. Pless, *Introduction to the Theory of Error-Correcting Codes*, Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons Inc., New York, third edition, 1998. <29, 30>

[2390] V. S. Pless, W. C. Huffman, and R. A. Brualdi, editors, *Handbook of Coding Theory. Vol. I, II*, North-Holland, Amsterdam, 1998. <29, 30, 652, 674, 681, 682, 694>

[2391] S. C. Pohlig and M. E. Hellman, An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance, *IEEE Trans. Information Theory* 24 (1978) 106–110. <389, 394, 791, 793, 794>

[2392] L. Poinsot, Réflexions sur les principes fondamentaux de la théorie des nombres, *Journal de mathématiques pures et appliquées* 10 (1845) 1–101. <66, 69>

[2393] P. Polito and O. Polverino, Linear blocking sets in $\mathrm{PG}(2, q^4)$, *Australas. J. Combin.* 26 (2002) 41–48. <552, 555>

[2394] P. Pollack, An explicit approach to hypothesis H for polynomials over a finite field, In *Anatomy of Integers*, volume 46 of *CRM Proc. Lecture Notes*, 259–273, Amer. Math. Soc., Providence, 2008. <488, 492>

[2395] P. Pollack, A polynomial analogue of the twin primes conjecture, *Proc. Amer. Math. Soc.* 136 (2008) 3775–3784. <488, 492>

[2396] P. Pollack, Simultaneous prime specializations of polynomials over finite fields, *Proc. Lond. Math. Soc.* 97 (2008) 545–567. <488, 492>

[2397] P. Pollack, Revisiting Gauss's analogue of the prime number theorem for polynomials over finite fields, *Finite Fields Appl.* 16 (2010) 290–299. <486, 492>

[2398] J. M. Pollard, Monte Carlo methods for index computation (mod p), *Math. Comp.* 32 (1978) 918–924. <390, 394, 736, 740>

[2399] J. M. Pollard, Kangaroos, Monopoly and discrete logarithms, *J. Cryptology* 13 (2000) 437–447. <390, 394>

[2400] J. M. Pollard and C.-P. Schnorr, An efficient solution of the congruence $x^2+ky^2 = m$ (mod n), *IEEE Trans. Inform. Theory* 33 (1987) 702–709. <758, 774>

[2401] O. Polverino, Small minimal blocking sets and complete k-arcs in $\mathrm{PG}(2, p^3)$, *Discrete Math.* 208/209 (1999) 469–476. <554, 555>

[2402] O. Polverino, Small blocking sets in $\mathrm{PG}(2, p^3)$, *Des. Codes Cryptogr.* 20 (2000) 319–324. <552, 554, 555>

[2403] O. Polverino and L. Storme, Small minimal blocking sets in $\mathrm{PG}(2, q^3)$, *European J. Combin.* 23 (2002) 83–92. <554, 555>

[2404] B. Poonen, Local height functions and the Mordell-Weil theorem for Drinfeld modules, *Compositio Math.* 97 (1995) 349–368. <532, 538>

[2405] A. D. Porto, F. Guida, and E. Montolivo, Fast algorithm for finding primitive polynomials over $GF(q)$, *Electron. Lett.* 28 (1992) 118–120. <343, 356>

[2406] A. G. Postnikov, *Ergodic Problems in the Theory of Congruences and of Diophantine Approximations*, Proceedings of the Steklov Institute of Mathematics, No. 82 (1966). American Mathematical Society, Providence, RI, 1967. <330, 337>

[2407] A. Pott, On the complexity of normal bases, *Bull. Inst. Combin. Appl.* 4 (1992) 51–52. <117, 122>

[2408] A. Pott, *Finite Geometry and Character Theory*, volume 1601 of *Lecture Notes in Mathematics*, Springer-Verlag, Berlin, 1995. <258, 261, 265>

[2409] A. Pott, Y. Tan, T. Feng, and S. Ling, Association schemes arising from bent functions, *Des. Codes Cryptogr.* 59 (2011) 319–331. <258, 265>

[2410] A. Pott and Y. Zhou, A new family of semifields with 2 parameters, submitted. <274>

[2411] B. Preneel et al., NESSIE security report, Technical Report D20-v2, New European Schemes for Signatures, Integrity, and Encryption, 2003. <775, 787>

[2412] F. P. Preparata, A class of optimum nonlinear double-error-correcting codes, *Information and Control* 13 (1968) 378–400. <692, 693, 694>

[2413] N. Presman, O. Shapira, and S. Litsyn, Binary polar code kernels from code decompositions, 2011, preprint available, `http://arxiv.org/abs/1101.0764`. <730>

[2414] N. Presman, O. Shapira, and S. Litsyn, Polar codes with mixed kernels, In *Proceedings of the 2011 Symposium on Information Theory*, 6–10, 2011. <730>

[2415] R. Pries and H. J. Zhu, p-rank stratification of Artin-Schreier curves, *Ann. Inst. Fourier* to appear . <480>

[2416] M. Ptashne, *A Genetic Switch: Phage Lambda and Higher Organisms*, Blackwell Publishers, 1992. <819, 824>

[2417] S. Qi, On diagonal equations over finite fields, *Finite Fields Appl.* 3 (1997) 175–179. <202, 207>

[2418] G. Quenell, Spectral diameter estimates for k-regular graphs, *Adv. Math.* 106 (1994) 122–148. <636, 649>

[2419] M. Rabin, Probabilistic algorithms in finite fields, *SIAM Journal on Computing* 9 (1980) 273–280. <368, 369, 373>

[2420] M. O. Rabin, Probabilistic algorithm for testing primality, *J. Number Theory* 12 (1980) 128–138. <339, 356>

[2421] R. Raghavendran, Finite associative rings, *Compositio Math.* 21 (1969) 195–229. <27>

[2422] J. Rajsski and J. Tyszer, Primitive polynomials over GF(2) of degree up to 660 with uniformly distributed coefficients, *J. Elect. Testing* 19 (2003) 645–657. <91, 93>

[2423] J. Ray and P. Koopman, Efficient high Hamming distance CRCs for embedded networks, In *Dependable Systems and Networks DSN*, 3–12, 2006. <626, 633>

[2424] D. K. Ray-Chaudhuri and R. M. Wilson, Solution of Kirkman's schoolgirl problem, In *Proc. Sympos. Pure Math., Vol. XIX: Combinatorics*, 187–203, Amer. Math. Soc., Providence, RI, 1971. <583, 590>

[2425] C. Rebeiro, S. S. Roy, D. S. Reddy, and D. Mukhopadhyay, Revisiting the Itoh-Tsujii inversion algorithm for FPGA platforms, *IEEE Transactions on VLSI Systems* 19 (2011) 1508–1512. <809, 814>

[2426] L. Rédei, A short proof of a theorem of Št. Schwarz concerning finite fields, *Časopis Pěst. Mat. Fys.* 75 (1950) 211–212. <58, 61>

[2427] L. Rédei, *Algebra. Vol 1*, International Series of Monographs in Pure and Applied Mathematics. Pergamon Press, Oxford, 1967. <57, 61>

[2428] L. Rédei, *Lückenhafte Polynome über endlichen Körpern*, Birkhäuser Verlag, Basel, 1970, Lehrbücher und Monographien aus dem Gebiete der exakten Wissenschaften, Mathematische Reihe, Band 42. <548, 555>

[2429] L. Rédei, *Lacunary Polynomials over Finite Fields*, North-Holland Publishing Co., Amsterdam, 1973. <29, 30, 548, 550, 555>

[2430] R. Ree, Proof of a conjecture of S. Chowla, *J. Number Theory* 3 (1971) 210–212. <67, 69>

[2431] I. S. Reed and G. Solomon, Polynomial codes over certain finite fields, *J. Soc. Indust. Appl. Math.* 8 (1960) 300–304. <670, 693, 694>

[2432] O. Reingold, S. Vadhan, and A. Wigderson, Entropy waves, the zig-zag graph product, and new constant-degree expanders, *Ann. of Math., 2nd Ser.* 155 (2002) 157–187. <646, 649>

[2433] D. Ren, Q. Sun, and P. Yuan, Number of zeros of diagonal polynomials over finite fields, *Finite Fields Appl.* 7 (2001) 197–204. <203, 207>

[2434] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, Symmetric informationally complete quantum measurements, *J. Math. Phys.* 45 (2004) 2171–2180. <826, 831>

[2435] A. Reyhani-Masoleh and M. A. Hasan, A new construction of Massey-Omura parallel multiplier over $GF(2^m)$, *IEEE Trans. Comput.* 51 (2002) 511–520. <810, 811, 812, 814>

[2436] A. Reyhani-Masoleh and M. A. Hasan, Efficient multiplication beyond optimal normal bases, *IEEE Trans. Comput.* 52 (2003) 428–439. <810, 811, 814>

[2437] A. Reyhani-Masoleh and M. A. Hasan, Low complexity bit parallel polynomial basis multiplication over $GF(2^m)$, *IEEE Trans. Comput.* 53 (2004) 945–959. <813, 814>

[2438] G. Rhin, Répartition modulo 1 dans un corps de séries formelles sur un corps fini, *Dissertationes Math. (Rozprawy Mat.)* 95 (1972) 75. <72, 75>

[2439] T. Richardson and R. Urbanke, *Modern Coding Theory*, Cambridge University Press, Cambridge, 2008. <705, 707, 708, 710>

[2440] T. J. Richardson, Error floors of LDPC codes, In *Proceedings of the Forty-First Annual Allerton Conference on Communication, Control and Computing*, (2003) 1426–1435. <710>

[2441] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, Design of capacity-approaching irregular low-density parity-check codes, *IEEE Trans. Inform. Theory* 47 (2001) 619–637. <704, 710, 720, 721, 725>

[2442] T. J. Richardson and R. L. Urbanke, The capacity of low-density parity-check codes under message-passing decoding, *IEEE Trans. Inform. Theory* 47 (2001) 599–618. <709, 710, 725>

[2443] C. Ritzenthaler, Optimal curves of genus 1, 2 and 3, *Publ. Math. Besancon (PMB)* (2011), preprint available, `http://arxiv.org/abs/1101.5871`. <453, 456>

[2444] R. L. Rivest, Permutation polynomials modulo 2^w, *Finite Fields Appl.* 7 (2001) 287–292. <222>

[2445] R. L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Yin, The RC6 block cipher, 1998. <741, 749, 750, 754>

[2446] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Comm. ACM* 21 (1978) 120–126. <734, 740>

[2447] A. M. Robert, The Gross-Koblitz formula revisited, *Rend. Sem. Mat. Univ. Padova* 105 (2001) 157–170. <147, 155>

[2448] J. A. G. Roberts and F. Vivaldi, A combinatorial model for reversible rational maps over finite fields, *Nonlinearity* 22 (2009) 1965–1982. <330, 337>

[2449] F. Rodríguez-Henríquez and Ç. K. Koç, Parallel multipliers based on special irreducible pentanomials, *IEEE Trans. Comput.* 52 (2003) 1535–1542. <813, 814>

[2450] F. Rodríguez-Henríquez, G. Morales-Luna, N. A. Saqib, and N. C. Cortés, Parallel Itoh-Tsujii multiplicative inversion algorithm for a special class of trinomials, *Des. Codes Cryptogr.* 45 (2007) 19–37. <809, 814>

[2451] M. Roitman, On Zsigmondy primes, *Proc. Amer. Math. Soc.* 125 (1997) 1913–1919. <71, 75>

[2452] A. Rojas-León, Estimates for singular multiplicative character sums, *Int. Math. Res. Not.* (2005) 1221–1234. <160, 161, 163, 193, 195>

[2453] A. Rojas-León, Purity of exponential sums on $\mathbb{A}^n$, *Compos. Math.* 142 (2006) 295–306. <157, 163>

[2454] A. Rojas-Leon, Rationality of trace and norm L-functions, *Duke Math. J.* (2012, to appear), preprint available, `http://arxiv.org/abs/1007.5324`. <193, 195>

[2455] A. Rojas-Leon and D. Wan, Moment zeta functions for toric Calabi-Yau hypersurfaces, *Commun. Number Theory Phys.* 1 (2007) 539–578. <190, 192, 195>

[2456] A. Rojas-Leon and D. Wan, Improvements of the Weil bound for Artin-Schreier curves, *Math. Ann.* 351 (2011) 417–442. <191, 195>

[2457] S. Roman, *Field Theory*, volume 158 of *Graduate Texts in Mathematics*, Springer, New York, second edition, 2006. <342, 356>

[2458] S. Rønjom and T. Helleseth, A new attack on the filter generator, *IEEE Trans. Inform. Theory* 53 (2007) 1752–1758. <239, 245>

[2459] C. Ronse, *Feedback Shift Registers*, volume 169 of *Lecture Notes in Computer Science*, Springer, Berlin, 1984. <305, 310>

[2460] L. Rónyai, Factoring polynomials over finite fields, In *Proceedings of the 28th Annual IEEE Symposium on Foundations of Computer Science,* Los Angeles CA, 132–137, IEEE Computer Society Press, Washington DC, 1987. <374, 375>

[2461] L. Rónyai, Factoring polynomials over finite fields, *Journal of Algorithms* 9 (1988) 391–400. <374, 375>

[2462] L. Rónyai, Factoring polynomials modulo special primes, *Combinatorica* 9 (1989) 199–206. <374, 375>

[2463] L. Rónyai, Galois groups and factoring polynomials over finite fields, *SIAM Journal on Discrete Mathematics* 5 (1992) 345–365. <374, 375>

[2464] L. Rónyai and Á. Szántó, Prime-field-complete functions and factoring polynomials over finite fields, *Computers and Artificial Intelligence* 15 (1996) 571–577. <374, 375>

[2465] L. Rónyai and T. Szőnyi, Planar functions over finite fields, *Combinatorica* 9 (1989) 315–320. <273, 274>

[2466] L. A. Rosati, Unitals in Hughes planes, *Geom. Dedicata* 27 (1988) 295–299. <563, 565>

[2467] M. Y. Rosenbloom and M. A. Tsfasman, Codes for the m-metric, *Problems Inform. Transmission* 33 (1997) 45–52. <613, 621>

[2468] R. Roth, *Introduction to Coding Theory*, Cambridge University Press, Cambridge, 2006. <652, 671, 675, 683, 694>

[2469] R. M. Roth, Maximum-rank array codes and their application to crisscross error correction, *IEEE Trans. Inform. Theory* 37 (1991) 328–336. <836, 839>

[2470] O. S. Rothaus, On "bent" functions, *J. Combin. Theory, Ser. A* 20 (1976) 300–305. <256, 257, 258, 265>

[2471] M. Rötteler, Quantum algorithms to solve the hidden shift problem for quadratics and for functions of large Gowers norm, In *Mathematical Foundations of Com-*

puter Science 2009, volume 5734 of *Lecture Notes in Comput. Sci.*, 663–674, Springer, Berlin, 2009. <830, 831>

[2472] M. Rötteler, Quantum algorithms for highly non-linear Boolean functions, In *Proceedings of the Twenty First Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 448–457, 2010. <830, 831>

[2473] S. S. Roy, C. Rebeiro, and D. Mukhopadhyay, Generalized high speed Itoh-Tsujii multiplicative inversion architecture for FPGAs, *Integration* 45 (2012) 307–315. <809, 814>

[2474] I. F. Rúa, Primitive and non primitive finite semifields, *Comm. Algebra* 32 (2004) 793–803. <270>

[2475] I. F. Rúa, E. F. Combarro, and J. Ranilla, Determination of division algebras with 243 elements, submitted. <268, 270>

[2476] I. F. Rúa, E. F. Combarro, and J. Ranilla, Classification of semifields of order 64, *J. Algebra* 322 (2009) 4011–4029. <268, 270>

[2477] K. Rubin and A. Silverberg, Supersingular abelian varieties in cryptology, In *Advances in Cryptology—CRYPTO 2002*, volume 2442 of *Lecture Notes in Comput. Sci.*, 336–353, Springer, Berlin, 2002. <448, 449>

[2478] K. Rubin and A. Silverberg, Using abelian varieties to improve pairing-based cryptography, *J. Cryptology* 22 (2009) 330–364. <802>

[2479] I. M. Rubio and C. J. Corrada-Bravo, Cyclic decomposition of permutations of finite fields obtained using monomials, In *Finite Fields and Applications*, volume 2948 of *Lecture Notes in Comput. Sci.*, 254–261, Springer, Berlin, 2004. <221, 222, 718>

[2480] I. M. Rubio, G. L. Mullen, C. Corrada, and F. N. Castro, Dickson permutation polynomials that decompose in cycles of the same length, In *Finite Fields and Applications*, volume 461 of *Contemp. Math.*, 229–239, Amer. Math. Soc., Providence, RI, 2008. <221, 222, 718>

[2481] H.-G. Rück, A note on elliptic curves over finite fields, *Math. Comp.* 49 (1987) 301–304. <424, 433, 784, 787>

[2482] H.-G. Rück, On the discrete logarithm in the divisor class group of curves, *Math. Comp.* 68 (1999) 805–806. <449>

[2483] H.-G. Rück and H. Stichtenoth, A characterization of Hermitian function fields over finite fields, *J. Reine Angew. Math.* 457 (1994) 185–188. <202, 207, 454, 456>

[2484] M. Rudnev, An improved sum-product inequality in fields of prime order, *Int. Math. Res. Notices* 2012 (2012) 3693–3705. <181, 186>

[2485] A. Rudra, Limits to list decoding of random codes, *IEEE Trans. Information Theory* IT-57 (2011) 1398–1408. <690, 694>

[2486] R. A. Rueppel, *Analysis and Design of Stream Ciphers*, Communications and Control Engineering Series. Springer-Verlag, Berlin, 1986. <318, 319, 322, 323, 330>

[2487] R. A. Rueppel, Stream ciphers, In *Contemporary Cryptology*, 65–134, IEEE, New York, 1992. <318, 319, 321, 330>

[2488] W. M. Ruppert, Reduzibilität ebener Kurven, *J. Reine Angew. Math.* 369 (1986) 167–191. <379, 380, 386>

[2489] W. M. Ruppert, Reducibility of polynomials $f(x, y)$ modulo p, *J. Number Theory* 77 (1999) 62–70. <379, 386>

[2490] J. J. Rushanan, *Topics in Integral Matrices and Abelian Group Codes: Generalized Q-Codes*, ProQuest LLC, Ann Arbor, MI, 1986, Thesis (Ph.D.)–California

Institute of Technology. <673, 694>

[2491] F. Ruskey, The Object Server Home Page (COS), `http://theory.cs.uvic.ca`, as viewed in July 2012. <44, 46>

[2492] F. Ruskey, C. R. Miers, and J. Sawada, The number of irreducible polynomials and Lyndon words with given trace, *SIAM J. Discrete Math.* 14 (2001) 240–245. <50, 55>

[2493] A. Russell and I. E. Shparlinski, Classical and quantum function reconstruction via character evaluation, *J. Complexity* 20 (2004) 404–422. <829, 831>

[2494] I. Z. Ruzsa, Essential components, *Proc. London Math. Soc., 3rd Ser.* 54 (1987) 38–56. <178, 179>

[2495] W. E. Ryan and S. Lin, *Channel Codes: Classical and Modern*, Cambridge University Press, Cambridge, 2009. <652, 694>

[2496] A. Sackmann, M. Heiner, and I. Koch, Application of petri net based analysis techniques to signal transduction pathways, *BMC Bioinformatics* 7 (2006) 482. <817, 824>

[2497] H. R. Sadjadpour, N. J. A. Sloane, M. Salehi, and G. Nebe, Interleaver design for turbo codes, *IEEE J. Select. Areas Commun.* 19 (2001) 831–837. <621, 625, 633, 717, 718>

[2498] J. Saez-Rodriguez, L. G. Alexopoulos, J. Epperlein, R. Samaga, D. A. Lauffenburger, S. Klamt, and P. K. Sorger, Discrete logic modelling as a means to link protein signalling networks with functional analysis of mammalian signal transduction, *Molecular Systems Biology* 5:331 (2009). <815, 824>

[2499] O. Sahin, H. Frohlich, C. Lobke, U. Korf, S. Burmester, M. Majety, J. Mattern, I. Schupp, C. Chaouiya, D. Thieffry, A. Poustka, S. Wiemann, T. Beissbarth, and D. Arlt, Modeling erbb receptor-regulated g1/s transition to find novel targets for de novo trastuzumab resistance, *BMC Systems Biology* 3 (2009) 1. <815, 824>

[2500] S. Sakata, n-dimensional Berlekamp-Massey algorithm for multiple arrays and construction of multivariate polynomials with preassigned zeros, In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 357 of *Lecture Notes in Comput. Sci.*, 356–376, Springer, Berlin, 1989. <322, 330>

[2501] S. Sakata, Extension of the Berlekamp-Massey algorithm to N dimensions, *Inform. and Comput.* 84 (1990) 207–239. <322, 330>

[2502] A. Sakzad, M.-R. Sadeghi, and D. Panario, Codes with girth 8 Tanner graph representation, *Des. Codes Cryptogr.* 57 (2010) 71–81. <709, 710>

[2503] A. Sakzad, M. R. Sadeghi, and D. Panario, Cycle structure of permutation functions over finite fields and their applications, *Adv. Math. Commun.* 6 (2012) 347–361. <221, 222, 718>

[2504] A. Sălăgean, On the computation of the linear complexity and the k-error linear complexity of binary sequences with period a power of two, *IEEE Trans. Inform. Theory* 51 (2005) 1145–1150. <322, 330>

[2505] R. Sandler, The collineation groups of some finite projective planes, *Portugal. Math.* 21 (1962) 189–199. <268, 270>

[2506] P. Sarnak, *Some Applications of Modular Forms*, volume 99 of *Cambridge Tracts in Mathematics*, Cambridge University Press, Cambridge, 1990. <635, 649>

[2507] P. Sarnak, Kloosterman, quadratic forms and modular forms, *Nieuw Arch. Wiskd.* 1 (2000) 385–389. <148, 155>

[2508] P. Sarnak, What is... an expander?, *Notices Amer. Math. Soc.* 51 (2004) 762–763.

<634, 637, 649>

[2509] D. Sarwate and M. Pursley, Crosscorrelation properties of pseudorandom and related sequences, *Proceedings of the IEEE* 68 (1980) 593–619. <310, 317>

[2510] D. V. Sarwate, An upper bound on the aperiodic autocorrelation function for a maximal-length sequence, *IEEE Trans. Inform. Theory* 30 (1984) 685–687. <831, 839>

[2511] T. Sasaki, T. Saito, and T. Hilano, Analysis of approximate factorization algorithm. I, *Japan J. Indust. Appl. Math.* 9 (1992) 351–368. <378, 386>

[2512] T. Sasaki and M. Sasaki, A unified method for multivariate polynomial factorizations, *Japan J. Indust. Appl. Math.* 10 (1993) 21–39. <378, 386>

[2513] T. Sasaki, M. Suzuki, M. Kolář, and M. Sasaki, Approximate factorization of multivariate polynomials and absolute irreducibility testing, *Japan J. Indust. Appl. Math.* 8 (1991) 357–375. <378, 386>

[2514] E. Sasoglu, E. Telatar, and E. Arikan, Polarization for arbitrary discrete memoryless channels, preprint available, `http://arxiv.org/abs/0908.0302`, 2009. <730>

[2515] E. Sasoglu, E. Telatar, and E. Yeh, Polar codes for the two-user binary-input multiple-access channel, In *Proc. IEEE Information Theory Workshop (ITW)*, 1–5, 2010. <730>

[2516] T. Satoh, The canonical lift of an ordinary elliptic curve over a finite field and its point counting, *J. Ramanujan Math. Soc.* 15 (2000) 247–270. <484, 779, 787>

[2517] T. Satoh, Generating genus two hyperelliptic curves over large characteristic finite fields, In *Advances in Cryptology - EUROCRYPT 2009*, volume 5479 of *Lecture Notes in Comput. Sci.*, 536–553, Springer, Berlin, 2009. <794>

[2518] T. Satoh and K. Araki, Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves, *Comment. Math. Univ. St. Paul.* 47 (1998) 81–92. <433, 775>

[2519] E. Savas and Ç. K. Koç, The Montgomery modular inverse—revisited, *IEEE Trans. Comput.* 49 (2000) 763–766. <353, 356>

[2520] A. Scheerhorn, Trace and norm-compatible extensions of finite fields, *Appl. Algebra Engrg. Comm. Comput.* 3 (1992) 199–209. <124, 132>

[2521] A. Scheerhorn, Iterated constructions of normal bases over finite fields, In *Finite Fields: Theory, Applications, and Algorithms*, volume 168 of *Contemp. Math.*, 309–325, Amer. Math. Soc., Providence, RI, 1994. <124, 132, 278, 282>

[2522] A. Scheerhorn, Dickson polynomials and completely normal elements over finite fields, In *Applications of Finite Fields*, volume 59 of *Inst. Math. Appl. Conf. Ser. (New Ser.)*, 47–55, Oxford Univ. Press, New York, 1996. <131, 132>

[2523] A. Scheerhorn, Dickson polynomials, completely normal polynomials and the cyclic module structure of specific extensions of finite fields, *Des. Codes Cryptogr.* 9 (1996) 193–202. <131, 132>

[2524] D. M. Schinianakis, A. P. Fournaris, H. E. Michail, A. P. Kakarountas, and T. Stouraitis, An RNS implementation of an F_p elliptic curve point multiplier, *IEEE Transactions on Circuits and Systems I: Regular Papers* 56 (2009) 1202–1213. <813, 814>

[2525] A. Schinzel, *Polynomials with Special Regard to Reducibility*, volume 77 of *Encyclopedia of Mathematics and its Applications*, Cambridge University Press, 2000. <379, 386>

[2526] O. Schirokauer, The special function field sieve, *SIAM J. Discrete Math.* 16 (2002)

81–98. <392, 394>

[2527] O. Schirokauer, The impact of the number field sieve on the discrete logarithm problem in finite fields, In *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, 397–420, Cambridge Univ. Press, Cambridge, 2008. <392, 394>

[2528] O. Schirokauer, The number field sieve for integers of low weight, *Math. Comp.* 79 (2010) 583–602. <392, 394>

[2529] B. Schmidt, *Characters and Cyclotomic Fields in Finite Geometry*, volume 1797 of *Lecture Notes in Mathematics*, Springer-Verlag, Berlin, 2002. <591, 592, 598>

[2530] K. Schmidt, *Dynamical Systems of Algebraic Origin*, volume 128 of *Progress in Mathematics*, Birkhäuser Verlag, Basel, 1995. <330, 337>

[2531] W. M. Schmidt, *Equations over Finite Fields. An Elementary Approach*, Lecture Notes in Mathematics, Vol. 536. Springer-Verlag, Berlin, 1976. <29, 30, 170, 179, 187, 188, 193, 195>

[2532] W. M. Schmidt, Construction and estimation of bases in function fields, *J. Number Theory* 39 (1991) 181–224. <323, 330>

[2533] T. Schoen and I. Shkredov, Additive properties of multiplicative subgroups of $\mathbb{F}_p$, *Quart. J. Math.* 63 (2012) 713–822. <206, 207>

[2534] J. Scholten and H. J. Zhu, Families of supersingular curves in characteristic 2, *Math. Res. Lett.* 9 (2002) 639–650. <480>

[2535] J. Scholten and H. J. Zhu, Hyperelliptic curves in characteristic 2, *Int. Math. Res. Not.* (2002) 905–917. <477, 480, 790, 794>

[2536] J. Scholten and H. J. Zhu, Slope estimates of Artin-Schreier curves, *Compositio Math.* 137 (2003) 275–292. <477, 480>

[2537] R. A. Scholtz, The spread spectrum concept, *IEEE Trans. Commun.* COM-25 (1977) 748–755. <832, 835, 839>

[2538] R. A. Scholtz and L. R. Welch, GMW sequences, *IEEE Trans. Inform. Theory* 30 (1984) 548–553. <311, 317>

[2539] T. Schönemann, Grundzüge einer allgemeinen theorie der höheren congruenzen, deren modul eine reele primzahl ist, *J. Reine Agnew. Math.* 31 (1845) 269–325. <8, 10>

[2540] A. Schönhage, Schnelle berechnung von kettenbruchentwicklungen, *Acta Inf.* 1 (1971) 139–144. <352, 356>

[2541] A. Schönhage, Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2, *Acta Informatica* 7 (1977) 395–398. <373, 375>

[2542] A. Schönhage and V. Strassen, Schnelle Multiplikation grosser Zahlen, *Computing (Arch. Elektron. Rechnen)* 7 (1971) 281–292. <348, 351, 356, 373, 375>

[2543] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.* 44 (1985) 483–494. <483, 484, 778, 787>

[2544] R. Schoof, Algebraic curves over $\mathbf{F}_2$ with many rational points, *J. Number Theory* 41 (1992) 6–14. <457, 462>

[2545] B. Schumacher and M. D. Westmoreland, Modal quantum theory, In *QPL 2010, 7th Workshop on Quantum Physics and Logic*, 145–149, 2010. <830, 831>

[2546] I. Schur, Über den Zusammenhang zwischen einem Problem der Zahlentheorie und einem Satz über algebraische Funktionen, *S.-B. Preuss. Akad. Wiss. Phys.-Math. Klasse* (1923) 123–134. <231, 232, 233>

[2547] I. Schur, Zur theorie der einfach transitiven permutationgruppen, *S.-B. Preuss.*

Akad. Wiss. Phys.-Math. Klasse (1933) 598–623. <231, 233>

[2548] R. Schürer, A new lower bound on the t-parameter of (t, s)-sequences, In *Monte Carlo and Quasi-Monte Carlo Methods*, 623–632, Springer-Verlag, Berlin, 2008. <617, 621>

[2549] M. P. Schützenberger, A non-existence theorem for an infinite family of symmetrical block designs, *Ann. Eugenics* 14 (1949) 286–287. <591, 598>

[2550] Š. Schwarz, Contribution à la recluctibilité des polynômes dans la théorie des congruences, *Věstnik Knálovskè českè spol. nauk.* (1939) 1–7. <368, 373>

[2551] Š. Schwarz, A contribution to the reducibility of binomial congruences (Slovak), *Časopis Pěst. Mat. Fys.* 71 (1946) 21–31. <57, 58, 61>

[2552] Š. Schwarz, On the reducibility of binomial congruences and on the bound of the least integer belonging to a given exponent mod p, *Časopis Pěst. Mat. Fys.* 74 (1949) 1–16. <58, 61>

[2553] Š. Schwarz, On the reducibility of polynomials over a finite field, *Quart. J. Math. Oxford* 2 (1956) 110–124. <368, 373>

[2554] Š. Schwarz, On a class of polynomials over a finite field (Russian), *Mat.-Fyz. Časopis. Slovensk. Akad.* 10 (1960) 68–80. <59, 61>

[2555] J. Schwinger, Unitary operator bases, *Proc. Nat. Acad. Sci. U.S.A.* 46 (1960) 570–579. <825, 831>

[2556] M. Scott, Optimal irreducible polynomials for GF(2^m) arithmetic, In *Software Performance Enhancement for Encryption and Decryption (SPEED 2007)*, 2007, Available online (July 2011) `http://www.hyperelliptic.org/SPEED/start07.html`. <31, 46>

[2557] M. Scott, Optimal irreducible polynomials for GF(2^m) arithmetic, *IACR Cryptology ePrint Archive* 2007 (2007) 192. <346, 356>

[2558] E. J. Scourfield, On ideals free of large prime factors, *J. Théor. Nombres Bordeaux* 16 (2004) 733–772. <392, 394>

[2559] B. Segre, Ovals in a finite projective plane, *Canad. J. Math.* 7 (1955) 414–416. <576, 580>

[2560] B. Segre, On complete caps and ovaloids in three-dimensional Galois spaces of characteristic two, *Acta Arith.* 5 (1959) 315–332 (1959). <579, 580>

[2561] B. Segre, Introduction to Galois geometries, *Atti Accad. Naz. Lincei Mem. Cl. Sci. Fis. Mat. Natur. Sez. I Ser. XIII* 8 (1967) 133–236. <576, 580>

[2562] G. E. Séguin, Low complexity normal bases for $F_{2^{mn}}$, *Discrete Appl. Math.* 28 (1990) 309–312. <113, 122>

[2563] E. S. Selmer, *Linear Recurrence Relations over Finite Fields*, University of Bergen, Bergen (Norway), 1966. <305, 310>

[2564] I. Semaev, Construction of polynomials, irreducible over a finite field, with linearly independent roots, *Mat. Sbornik* 135 (1988) 520–532, In Russian; English translation in Math. USSR-Sbornik, 63:507-519, 1989. <105, 110, 113, 122, 371, 373>

[2565] I. A. Semaev, Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p, *Math. Comp.* 67 (1998) 353–356. <433, 775>

[2566] G. Seroussi, Table of low-weight binary irreducible polynomials, Technical Report HP-98-135, Computer Systems Laboratory, Hewlett Packard, 1998. <31, 33, 46, 341, 356>

[2567] G. Seroussi and A. Lempel, Factorization of symmetric matrices and trace-

orthogonal bases in finite fields, *SIAM J. Comput.* 9 (1980) 758–767. <97, 103>

[2568] G. Seroussi and A. Lempel, On symmetric representations of finite fields, *SIAM J. Algebraic Discrete Methods* 4 (1983) 14–21. <495, 496, 502>

[2569] J.-P. Serre, Géométrie algébrique et géométrie analytique, *Ann. Inst. Fourier, Grenoble* 6 (1955–1956) 1–42. <529, 538>

[2570] J.-P. Serre, *Abelian l-adic Representations and Elliptic Curves*, McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. W. A. Benjamin, Inc., New York-Amsterdam, 1968. <291, 292, 295>

[2571] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* 15 (1972) 259–331. <292, 295>

[2572] J.-P. Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1973, Graduate Texts in Mathematics, No. 7. <27>

[2573] J.-P. Serre, Majorations de sommes exponentielles, In *Journées Arithmétiques de Caen*, 111–126, Astérisque No. 41–42, Soc. Math. France, Paris, 1977. <163, 641, 649>

[2574] J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, *Inst. Hautes Études Sci. Publ. Math.* (1981) 323–401. <292, 295, 431, 433>

[2575] J.-P. Serre, Nombres de points des courbes algébriques sur $\mathbf{F}_q$, In *Seminar on Number Theory*, Exp. No. 22, 8, Univ. Bordeaux I, Talence, 1983. <452, 453, 456>

[2576] J.-P. Serre, Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, *C. R. Acad. Sci. Paris, Sér. I, Math.* 296 (1983) 397–402. <453, 456, 457, 462>

[2577] J.-P. Serre, Quel est le nombre maximum de points rationnels que peut avoir une courbe algébrique de genre g sur un corps fini?, *Annuaire du Collége de France* 84 (1984) 397–402. <454, 456>

[2578] J.-P. Serre, Répartition asymptotique des valeurs propres de l'opérateur de Hecke T_p, *J. Amer. Math. Soc.* 10 (1997) 75–102. <638, 649>

[2579] J.-P. Serre, On a theorem of Jordan, *Bull. Amer. Math. Soc. (New Ser.)* 40 (2003) 429–440. <292, 295>

[2580] J. A. Serret, Mémoire sur la théorie des congruences suivant un module premier et suivant une fonction modularie irréductible, *Mém. Acad. Sci., Inst. de France* 1 (1866) 617–688. <56, 58, 61>

[2581] J. A. Serret, Détermination des fonctions entières irréductiblles, suivant un module premier, dans le cas où le degrè est ègal au module, *J. Math. Pures Appl.* 18 (1873) 301–304. <59, 61>

[2582] J. A. Serret, Sur les fonctions enti'eres irréductiblles, suivant un module premier, dans le cas où le degrè est une puissance du module, *J. Math. Pures Appl.* 18 (1873) 437–451. <59, 61>

[2583] J.-A. Serret, *Cours d'Algèbre Supérieure. Tome I*, Les Grands Classiques Gauthier-Villars. [Gauthier-Villars Great Classics]. Éditions Jacques Gabay, Sceaux, 1992, Reprint of the fourth (1877) edition. <7, 10, 56, 57, 58, 61, 66, 69, 374, 375>

[2584] H. Shacham and B. Waters, editors, *Pairing-Based Cryptography — Pairing 2009*, volume 5671 of *Lecture Notes in Computer Science*, Berlin, 2009. Springer-Verlag. <779, 787>

[2585] I. R. Shafarevich, *Basic Algebraic Geometry 1: Varieties in Projective Space*,

Springer-Verlag, second edition, 1994. <379, 386>

[2586] R. Shaheen and A. Winterhof, Permutations of finite fields for check digit systems, *Des. Codes Cryptogr.* 57 (2010) 361–371. <222>

[2587] A. Shallue and C. E. van de Woestijne, Construction of rational points on elliptic curves over finite fields, In F. Hess, S. Pauli, and M. Pohst, editors, *Algorithmic Number Theory—ANTS-VII*, volume 4076 of *Lecture Notes in Computer Science*, 510–524, Springer-Verlag, Berlin, 2006. <787>

[2588] A. Shamir, Efficient signature schemes based on birational permutations, In *Crypto*, volume 773 of *Lecture Notes in Computer Science*, 1–12, Springer, Berlin, 1993. <759, 763, 765, 774>

[2589] D. Shanks, Class number, a theory of factorization, and genera, In *1969 Number Theory Institute*, 415–440, Amer. Math. Soc., Providence, RI, 1971. <389, 394>

[2590] C. E. Shannon, A mathematical theory of communication, *Bell System Tech. J.* 27 (1948) 379–423, 623–656. <652, 675, 694, 717, 718>

[2591] C. E. Shannon, Communication theory of secrecy systems, *Bell System Tech. J.* 28 (1949) 656–715. <733, 740>

[2592] R. T. Sharifi, On norm residue symbols and conductors, *J. Number Theory* 86 (2001) 196–209. <140, 155>

[2593] J. T. Sheats, The Riemann hypothesis for the Goss zeta function for $\mathbb{F}_q[t]$, *J. Number Theory* 71 (1998) 121–157. <536, 538>

[2594] G. B. Sherwood, S. S. Martirosyan, and C. J. Colbourn, Covering arrays of higher strength from permutation vectors, *J. Combin. Des.* 14 (2006) 202–213. <601, 610>

[2595] I. P. Shestakov and U. U. Umirbaev, The Nagata automorphism is wild, *Proc. Natl. Acad. Sci. USA* 100 (2003) 12561–12563. <759, 774>

[2596] G. Shimura and Y. Taniyama, *Complex Multiplication of Abelian Varieties and its Applications to Number Theory*, volume 6 of *Publications of the Mathematical Society of Japan*, The Mathematical Society of Japan, Tokyo, 1961. <291, 295>

[2597] K. Shiratani and M. Yamada, On rationality of Jacobi sums, *Colloq. Math.* 73 (1997) 251–260. <140, 155>

[2598] S. G. Shiva and P. Allard, A few useful details about a known technique for factoring $1 + X^{2q-1}$, *IEEE Trans. Inform. Theory* IT-16 (1970) 234–235. <58, 61>

[2599] I. Shmulevich, E. R. Dougherty, S. Kim, and W. Zhang, Probabilistic Boolean networks: a rule-based uncertainty model for gene regulatory networks, *Bioinformatics* 18 (2002) 261–274. <817, 824>

[2600] A. Shokrollahi, Raptor codes, *IEEE Trans. Inform. Theory* 52 (2006) 2551–2567. <723, 724, 725>

[2601] A. Shokrollahi and M. Luby, Raptor codes, In *Foundations and Trends in Communications and Information Theory*, volume 6, 213 – 322, NOW Publishers, 2009. <725>

[2602] M. A. Shokrollahi, New sequences of linear time erasure codes approaching the channel capacity, In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 1719 of *Lecture Notes in Comput. Sci.*, 65–76, Springer, Berlin, 1999. <720, 721, 725>

[2603] M. A. Shokrollahi, Codes and graphs, In *STACS 2000*, volume 1770 of *Lecture Notes Comput. Sci.*, 1–12. Springer, 2000. <719, 721, 725>

[2604] M. A. Shokrollahi, Capacity-achieving sequences, In *Codes, Systems, and Graphical Models*, volume 123 of *IMA Vol. Math. Appl.*, 153–166, Springer, New York, 2001. <720, 721, 725>

[2605] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Comput.* 26 (1997) 1484–1509. <388, 394, 739, 740, 829, 831>

[2606] V. Shoup, *Removing Randomness From Computational Number Theory*, PhD thesis, University of Wisconsin, Madison, 1989. <372, 373>

[2607] V. Shoup, *Removing Randomness from Computational Number Theory*, PhD dissertation, University of Wisconsin, 1989. <374>

[2608] V. Shoup, New algorithms for finding irreducible polynomials over finite fields, *Mathematics of Computation* 54 (1990) 435–447. <371, 372, 373>

[2609] V. Shoup, On the deterministic complexity of factoring polynomials over finite fields, *Inform. Process. Lett.* 33 (1990) 261–267. <176, 179>

[2610] V. Shoup, Searching for primitive roots in finite fields, In *Symposium on the Theory of Computing – STOC 1990*, 546–554. ACM, 1990. <341, 356>

[2611] V. Shoup, Searching for primitive roots in finite fields, *Math. Comp.* 58 (1992) 369–380. <341, 356>

[2612] V. Shoup, Fast construction of irreducible polynomials over finite fields, *Journal of Symbolic Computation* 17 (1994) 371–391. <371, 373>

[2613] V. Shoup, Lower bounds for discrete logarithms and related problems, In *Advances in Cryptology—EUROCRYPT '97*, volume 1233 of *Lecture Notes in Comput. Sci.*, 256–266, Springer, Berlin, 1997. <388, 394>

[2614] V. Shoup, Efficient computation of minimal polynomials in algebraic extensions of finite fields, In *Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation*, 53–58, ACM, New York, 1999. <343, 356>

[2615] V. Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press, Cambridge, second edition, 2009. <29, 30, 339, 340, 342, 356>

[2616] V. Shoup, NTL: A Library for doing Number Theory, version 5.5.2, 2009, available at `http://www.shoup.net/ntl`. <30, 45, 46, 339, 350, 356>

[2617] I. E. Shparlinski, On primitive polynomials, *Problemy Peredachi Informatsii* 23 (1987) 100–103. <68, 69, 91, 93>

[2618] I. E. Shparlinski, Distribution of values of recurrent sequences, *Problems Inform. Transmission* 25 (1989) 120–125. <309, 310>

[2619] I. E. Shparlinski, Some problems in the theory of finite fields, *Uspekhi Mat. Nauk* 46 (1991) 165–200, 240. <372, 373>

[2620] I. E. Shparlinski, *Computational and Algorithmic Problems in Finite Fields*, volume 88 of *Mathematics and its Applications (Soviet Series)*, Kluwer Academic Publishers Group, Dordrecht, 1992. <29, 30, 374, 375>

[2621] I. E. Shparlinski, A deterministic test for permutation polynomials, *Comput. Complexity* 2 (1992) 129–132. <210, 222>

[2622] I. E. Shparlinski, Finding irreducible and primitive polynomials, *Applicable Algebra in Engineering, Communication and Computing* 4 (1993) 263–268. <372, 373>

[2623] I. E. Shparlinski, On finding primitive roots in finite fields, *Theoret. Comput. Sci.* 157 (1996) 273–275. <341, 356>

[2624] I. E. Shparlinski, *Finite Fields: Theory and Computation*, volume 477 of *Mathematics and its Applications*, Kluwer Academic Publishers, Dordrecht, 1999. <29,

30, 374, 375>

[2625] I. E. Shparlinski, On the linear complexity of the power generator, *Des. Codes Cryptogr.* 23 (2001) 5–10. <326, 330>

[2626] I. E. Shparlinski, On a question of Erdős and Graham, *Arch. Math. (Basel)* 78 (2002) 445–448. <207>

[2627] I. E. Shparlinski, *Cryptographic Applications of Analytic Number Theory: Complexity Lower Bounds and Pseudorandomness*, volume 22 of *Progress in Computer Science and Applied Logic*, Birkhäuser Verlag, Basel, 2003. <29, 30, 170, 179, 327, 330>

[2628] I. E. Shparlinski, Bounds of Gauss sums in finite fields, *Proc. Amer. Math. Soc.* 132 (2004) 2817–2824. <135, 155>

[2629] I. E. Shparlinski, On the number of zero trace elements in polynomial bases for $\mathbb{F}_{2^n}$, *Rev. Mat. Complut.* 18 (2005) 177–180. <101, 103>

[2630] I. E. Shparlinski, Playing 'hide-and-seek' with numbers: the hidden number problem, lattices and exponential sums, In *Public-Key Cryptography*, volume 62 of *Proc. Sympos. Appl. Math.*, 153–177, Amer. Math. Soc., Providence, RI, 2005. <170, 179>

[2631] I. E. Shparlinski, On some dynamical systems in finite fields and residue rings, *Discrete Contin. Dyn. Syst.* 17 (2007) 901–917. <330, 337>

[2632] I. E. Shparlinski, On the distribution of angles of the Salié sums, *Bull. Austral. Math. Soc.* 75 (2007) 221–227. <151, 155>

[2633] I. E. Shparlinski, On the distribution of Kloosterman sums, *Proc. Amer. Math. Soc.* 136 (2008) 419–425. <151, 155>

[2634] I. E. Shparlinski, On the exponential sum-product problem, *Indag. Math. (New Ser.)* 19 (2008) 325–331. <182, 186>

[2635] I. E. Shparlinski, On the distribution of arguments of Gauss sums, *Kodai Math. J.* 32 (2009) 172–177. <134, 155>

[2636] I. E. Shparlinski, On the average distribution of pseudorandom numbers generated by nonlinear permutations, *Math. Comp.* 80 (2011) 1053–1061. <334, 337>

[2637] I. E. Shparlinski, On the distribution of irreducible trinomials, *Canad. Math. Bull.* 54 (2011) 748–756. <83, 85>

[2638] I. E. Shparlinski and A. Winterhof, Noisy interpolation of sparse polynomials in finite fields, *Appl. Algebra Engrg. Comm. Comput.* 16 (2005) 307–317. <170, 179>

[2639] I. E. Shparlinski and A. Winterhof, Constructions of approximately mutually unbiased bases, In *LATIN 2006: Theoretical Informatics*, volume 3887 of *Lecture Notes in Comput. Sci.*, 793–799, Springer, Berlin, 2006. <825, 831>

[2640] I. E. Shparlinski and A. Winterhof, Quantum period reconstruction of approximate sequences, *Inform. Process. Lett.* 103 (2007) 211–215. <829, 831>

[2641] F. Shuqin and H. Wenbao, Primitive polynomials over finite fields of characteristic two, *Appl. Algebra Engrg. Comm. Comput.* 14 (2004) 381–395. <88, 90>

[2642] V. M. Sidel′nikov, Some k-valued pseudo-random sequences and nearly equidistant codes, *Problemy Peredači Informacii* 5 (1969) 16–22. <312, 317>

[2643] V. M. Sidel′nikov, On mutual correlation of sequences, *Soviet Math. Dokl.* 12 (1971) 197–201. <313, 317>

[2644] V. M. Sidel′nikov, On the cross correlation of sequences, *Problemy Kibernet.* (1971) 15–42. <314, 317>

[2645] V. M. Sidel'nikov, Estimates for the number of appearances of elements on an interval of a recurrent sequence over a finite field, *Discrete Math. Appl.* 2 (1992) 473–481. <309, 310>

[2646] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, *IEEE Trans. Inform. Theory* 30 (1984) 776–780. <240, 245>

[2647] M. Sieveking, An algorithm for division of powerseries, *Computing* 10 (1972) 153–156. <373, 375>

[2648] D. Silva and F. R. Kschischang, Universal secure network coding via rank-metric codes, *IEEE Trans. Inform. Theory* 57 (2011) 1124–1135. <115, 122>

[2649] D. Silva, F. R. Kschischang, and R. Kötter, A rank-metric approach to error control in random network coding, *IEEE Trans. Inform. Theory* 54 (2008) 3951–3967. <838, 839>

[2650] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1994. <29, 30, 416, 433>

[2651] J. H. Silverman, *The Arithmetic of Dynamical Systems*, volume 241 of *Graduate Texts in Mathematics*, Springer, New York, 2007. <330, 331, 337>

[2652] J. H. Silverman, Variation of periods modulo p in arithmetic dynamics, *New York J. Math.* 14 (2008) 601–616. <335, 337>

[2653] J. H. Silverman, *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, second edition, 2009. <29, 30, 416, 417, 418, 419, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 433>

[2654] J. H. Silverman, A survey of local and global pairings on elliptic curves and abelian varieties, In *Pairing-Based Cryptography (PAIRING 2010)*, volume 6478 of *Lecture Notes in Comput. Sci.*, 377–396, Springer, Berlin, 2010. <428, 433>

[2655] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992. <29, 30, 416, 433>

[2656] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*, McGraw-Hill, Inc., 1994. <310, 317>

[2657] J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* 43 (1938) 377–385. <593, 598>

[2658] M. Skałba, Points on elliptic curves over finite fields, *Acta Arithmetica* 117 (2005) 293–301. <787>

[2659] C. Small, Solution of Waring's problem mod n, *Amer. Math. Monthly* 84 (1977) 356–359. <205, 207>

[2660] C. Small, Sums of powers in large finite fields, *Proc. Amer. Math. Soc.* 65 (1977) 35–36. <205, 207>

[2661] C. Small, Waring's problem mod n, *Amer. Math. Monthly* 84 (1977) 12–25. <205, 207>

[2662] C. Small, Diagonal equations over large finite fields, *Canad. J. Math.* 36 (1984) 249–262. <201, 203, 207>

[2663] C. Small, Permutation binomials, *Internat. J. Math. Math. Sci.* 13 (1990) 337–342. <216, 222>

[2664] C. Small, *Arithmetic of Finite Fields*, volume 148 of *Monographs and Textbooks in Pure and Applied Mathematics*, Marcel Dekker Inc., New York, 1991. <29, 30, 200, 201, 207, 216, 222>

[2665] N. P. Smart, The discrete logarithm problem on elliptic curves of trace one, *J. Cryptology* 12 (1999) 193–196. <433, 775>

[2666] N. P. Smart, The exact security of ECIES in the generic group model, In B. Honary, editor, *Cryptography and Coding*, volume 2260 of *Lecture Notes in Computer Science*, 73–84, Springer-Verlag, Berlin, 2001. <776, 787>

[2667] N. Smart (ed.), ECRYPT II yearly report on algorithms and keysizes (2009-2010), Technical Report D.SPA.13, European Network of Excellence in Cryptology II, 2010. <775, 784, 787>

[2668] B. Smeets, The linear complexity profile and experimental results on a randomness test of sequences over the field $\mathbf{F}_q$, presented at IEEE Int. Symp. on Information Theory 1988, June 19–24. <323, 330>

[2669] B. Smeets and W. Chambers, Windmill generators: a generalization and an observation of how many there are, In *Advances in Cryptology—EUROCRYPT'88*, volume 330 of *Lecture Notes in Comput. Sci.*, 325–330, Springer, Berlin, 1988. <65, 66>

[2670] M. H. M. Smid, Duadic codes, *IEEE Trans. Inform. Theory* 33 (1987) 432–433. <673, 694>

[2671] B. A. Smith, Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves, *J. Cryptology* 22 (2009) 505–529. <789, 794>

[2672] S. L. Snover, *The Uniqueness of the Nordstrom-Robinson and the Golay Binary Codes*, ProQuest LLC, Ann Arbor, MI, 1973, Thesis (Ph.D.)–Michigan State University. <692, 694>

[2673] I. M. Sobol', Distribution of points in a cube and approximate evaluation of integrals (Russian), *Ž. Vyčisl. Mat. i Mat. Fiz.* 7 (1967) 784–802. <611, 617, 619, 621>

[2674] M. Sodestrand, W. Jenkins, G. A. Jullien, and F. J. Taylor, *Residue Number System Arithmetic: Modern Applications in Digital Signal Processing*, IEEE Press, 1986. <813, 814>

[2675] P. Solé, A quaternary cyclic code, and a family of quadriphase sequences with low correlation properties, In *Coding Theory and Applications*, volume 388 of *Lecture Notes in Comput. Sci.*, 193–201, Springer, New York, 1989. <315, 317>

[2676] J. A. Solinas, Generalized Mersenne numbers, Combinatorics and Optimization Research Report CORR 99-39, University of Waterloo, 1999, available at `http://www.cacr.math.uwaterloo.ca/techreports/1999/corr99-39.ps`. <345, 356>

[2677] R. Solovay and V. Strassen, A fast Monte-Carlo test for primality, *SIAM J. Comput.* 6 (1977) 84–85. <339, 356, 374, 375>

[2678] L. Song and K. K. Parhi, Low-energy digit-serial/parallel finite field multipliers, *The Journal of VLSI Signal Processing* 19 (1998) 149–166. <806, 814>

[2679] A. B. Sørensen, Projective Reed-Muller codes, *IEEE Trans. Inform. Theory* 37 (1991) 1567–1576. <678, 694>

[2680] K. W. Spackman, Simultaneous solutions to diagonal equations over finite fields, *J. Number Theory* 11 (1979) 100–115. <207>

[2681] S. Sperber, On the p-adic theory of exponential sums, *Amer. J. Math.* 108 (1986) 255–296. <163, 204, 207, 474, 480>

[2682] W. Stahnke, Primitive binary polynomials, *Math. Comp.* 27 (1973) 977–980. <91, 93>

[2683] M. Stamp and C. F. Martin, An algorithm for the k-error linear complexity of binary

sequences with period 2^n, *IEEE Trans. Inform. Theory* 39 (1993) 1398–1401. <319, 322, 330>

[2684] H. M. Stark and A. A. Terras, Zeta functions of finite graphs and coverings, *Adv. Math.* 121 (1996) 124–165. <649>

[2685] A. Steane, Multiple-particle interference and quantum error correction, *Proc. Roy. Soc. London Ser. A* 452 (1996) 2551–2577. <828, 831>

[2686] A. Steel, Conquering inseparability: primary decomposition and multivariate factorization over algebraic function fields of positive characteristic, *J. Symbolic Comput.* 40 (2005) 1053–1075. <380, 386>

[2687] L. J. Steggles, R. Banks, O. Shaw, and A. Wipat, Qualitatively modelling and analysing genetic regulatory networks: a Petri net approach, *Bioinformatics* 23 (2007) 336–343. <817, 824>

[2688] D. Stehlé and P. Zimmermann, A binary recursive GCD algorithm, In *Algorithmic Number Theory*, volume 3076 of *Lecture Notes in Comput. Sci.*, 411–425, Springer, Berlin, 2004. <352, 356>

[2689] A. Stein, Sharp upper bounds for arithmetic in hyperelliptic function fields, *J. Ramanujan Math. Soc.* 16 (2001) 119–203. <446, 449>

[2690] A. Stein, Explicit infrastructure for real quadratic function fields and real hyperelliptic curves, *Glas. Mat. Ser. III* 44(64) (2009) 89–126. <445, 449>

[2691] A. Stein and E. Teske, Optimized baby step–giant step methods, *J. Ramanujan Math. Soc.* 20 (2005) 27–58. <390, 394>

[2692] W. A. Stein et al., Sage Mathematics Software (Version 5.0), The Sage Development Team. Available at `http://www.sagemath.org/`, 2012. <45, 46, 339, 356>

[2693] S. A. Stepanov, On the number of polynomials of a given form that are irreducible over a finite field, *Mat. Zametki* 41 (1987) 289–295, 456. <73, 75>

[2694] S. A. Stepanov, *Arithmetic of Algebraic Curves*, Monographs in Contemporary Mathematics. Consultants Bureau, New York, 1994. <29, 30, 171, 179>

[2695] J. Stern, D. Pointcheval, J. Malone-Lee, and N. Smart, Flaws in applying proof methodologies to signature schemes, In M. Yung, editor, *Advances in Cryptology—CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, 93–110, Berlin, 2002, Springer-Verlag. <776, 787>

[2696] H. Stichtenoth, Transitive and self-dual codes attaining the Tsfasman-Vlăduţ-Zink bound, *IEEE Trans. Inform. Theory* 52 (2006) 2218–2224. <461, 462>

[2697] H. Stichtenoth, *Algebraic Function Fields and Codes*, volume 254 of *Graduate Texts in Mathematics*, Springer-Verlag, Berlin, second edition, 2009. <29, 30, 202, 207, 399, 400, 401, 402, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 415, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 462, 696, 703>

[2698] H. Stichtenoth and C. P. Xing, Excellent nonlinear codes from algebraic function fields, *IEEE Trans. Inform. Theory* 51 (2005) 4044–4046. <703>

[2699] L. Stickelberger, On a new property of the discriminants of algebraic number fields. (Ueber eine neue Eigenschaft der Discriminanten algebraischer Zahlkörper.), *Verh. d. intern. Math.-Congr.* 1 (1897) 182–193. <62, 63, 66>

[2700] B. Stigler, Polynomial dynamical systems in systems biology, In *Modeling and Simulation of Biological Networks*, volume 64 of *Proc. Sympos. Appl. Math.*, 53–84, Amer. Math. Soc., Providence, RI, 2007. <330, 337>

[2701] D. R. Stinson, On bit-serial multiplication and dual bases in GF(2^m), *IEEE Trans. Inform. Theory* 37 (1991) 1733–1736. <101, 103>

[2702] D. R. Stinson, *Combinatorial Designs: Constructions and Analysis*, Springer-Verlag,

New York, 2004. <29, 30, 590, 610>

[2703] D. R. Stinson, *Cryptography: Theory and Practice*, Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton, FL, third edition, 2006. <29, 30, 386, 394, 740>

[2704] D. R. Stinson, R. Wei, and L. Zhu, New constructions for perfect hash families and related structures using combinatorial designs and codes, *J. Combin. Des.* 8 (2000) 189–200. <604, 610>

[2705] K.-O. Stöhr and J. F. Voloch, Weierstrass points and curves over finite fields, *Proc. London Math. Soc., 3rd Ser.* 52 (1986) 1–19. <455, 456>

[2706] T. Stoll, Complete decomposition of Dickson-type polynomials and related Diophantine equations, *J. Number Theory* 128 (2008) 1157–1181. <280, 282>

[2707] R. Stong, The average order of a permutation, *Electron. J. Combin.* 5 (1998) Research Paper 41, 6 pp. <366, 367>

[2708] T. Storer, *Cyclotomy and Difference Sets*, Lectures in Advanced Mathematics, No. 2. Markham Publishing Co., Chicago, IL, 1967. <595, 598>

[2709] A. Storjohann, Deterministic computation of the Frobenius form (extended abstract), In *Forty Second IEEE Symposium on Foundations of Computer Science*, 368–377, IEEE Computer Soc., Los Alamitos, CA, 2001. <522, 527>

[2710] A. Storjohann and G. Villard, Algorithms for similarity transforms, Technical report, Rhine Workshop on Computer Algebra, 2000. <522, 527>

[2711] A. J. Stothers, *On the Complexity of Matrix Multiplication*, PhD thesis, University of Edinburgh, 2010. <513, 527>

[2712] W. W. Stothers, On permutation polynomials whose difference is linear, *Glasgow Math. J.* 32 (1990) 165–171. <221, 222>

[2713] D. R. Stoutemyer, Which polynomial representation is best?, In *Proceedings of the 1984 MACSYMA Users' Conference*, 221–243, 1984. <375, 386>

[2714] V. Strassen, Gaussian elimination is not optimal, *Numer. Math.* 13 (1969) 354–356. <351, 356>

[2715] V. Strassen, Evaluation of rational functions, In R. E. Miller and J. W. Thatcher, editors, *Complexity of Computer Computations*, Plenum Press, 1972. <374, 375>

[2716] V. Strassen, Vermeidung von Divisionen, *J. Reine Angew. Math.* 264 (1973) 182–202. <384, 386>

[2717] V. Strassen, Algebraische berechnungskomplexität, In *Perspectives in Mathematics, Anniversary of Oberwolfach 1984*, 509–550, Birkhäuser Verlag, Basel, 1984. <373, 375>

[2718] M. Streng, Computing Igusa class polynomials, preprint available, `http://arxiv.org/abs/0903.4766`, 2012. <794>

[2719] S. J. Suchower, Subfield permutation polynomials and orthogonal subfield systems in finite fields, *Acta Arith.* 54 (1990) 307–315. <224, 225>

[2720] S. J. Suchower, Polynomial representations of complete sets of frequency hyperrectangles with prime power dimensions, *J. Combin. Theory, Ser. A* 62 (1993) 46–65. <546, 547>

[2721] B. Sudakov, E. Szemerédi, and V. H. Vu, On a question of Erdős and Moser, *Duke Math. J.* 129 (2005) 129–155. <182, 186>

[2722] M. Sudan, Decoding of Reed Solomon codes beyond the error-correction bound, *J. Complexity* 13 (1997) 180–193. <689, 690, 694>

[2723] M. Sugita, M. Kawazoe, and H. Imai, Gröbner basis based cryptanalysis of sha-1, Cryptology ePrint Archive, Report 2006/098, 2006, http://eprint.iacr.org/. <773, 774>

[2724] Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa, A method for solving key equation for decoding Goppa codes, *Information and Control* 27 (1975) 87–99. <685, 694>

[2725] J. Sun and O. Y. Takeshita, Interleavers for turbo codes using permutation polynomials over integer rings, *IEEE Trans. Inform. Theory* 51 (2005) 101–119. <221, 222, 716, 717, 718>

[2726] Q. Sun, The number of solutions of certain diagonal equations over finite fields, *Sichuan Daxue Xuebao* 34 (1997) 395–398. <203, 207>

[2727] Q. Sun and D. Q. Wan, On the solvability of the equation $\sum_{i=1}^{n} x_i/d_i \equiv 0 \pmod 1$ and its application, *Proc. Amer. Math. Soc.* 100 (1987) 220–224. <202, 203, 207>

[2728] Q. Sun and D. Q. Wan, On the Diophantine equation $\sum_{i=1}^{n} x_i/d_i \equiv 0 \pmod 1$, *Proc. Amer. Math. Soc.* 112 (1991) 25–29. <203, 207>

[2729] Z.-W. Sun, On value sets of polynomials over a field, *Finite Fields Appl.* 14 (2008) 470–481. <204, 207, 228, 229>

[2730] B. Sunar, A generalized method for constructing subquadratic complexity $GF(2^k)$ multipliers, *IEEE Trans. Comput.* 53 (2004) 1097–1105. <805, 814>

[2731] B. Sunar, A Euclidean algorithm for normal bases, *Acta Appl. Math.* 93 (2006) 57–74. <353, 356>

[2732] B. Sunar and Ç. K. Koç, Mastrovito multiplier for all trinomials, *IEEE Trans. Comput.* 48 (1999) 522–527. <813, 814>

[2733] B. Sunar and Ç. K. Koç, An efficient optimal normal basis type II multiplier, *IEEE Trans. Comput.* 50 (2001) 83–87. <812, 814>

[2734] A. V. Sutherland, Genus 1 point counting in essentially quartic time and quadratic space, 2010, Slides, http://math.mit.edu/~drew/NYU0910.pdf. <778, 787>

[2735] A. V. Sutherland, Genus 1 point-counting record modulo a 5000+ digit prime, 2010, Posting to the Number Theory List, http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1007&L=nmbrthry&T=0&F=&S=&P=287. <778, 787>

[2736] R. G. Swan, Factorization of polynomials over finite fields, *Pacific J. Math.* 12 (1962) 1099–1106. <33, 46, 63, 64, 66, 91, 93>

[2737] N. Szabo and R. I. Tanaka, *Residue Arithmetic and its Application to Computer Technology*, McGraw-Hill, 1967. <345, 356>

[2738] P. Sziklai, On small blocking sets and their linearity, *J. Combin. Theory, Ser. A* 115 (2008) 1167–1182. <552, 555>

[2739] T. Szőnyi, On the number of directions determined by a set of points in an affine Galois plane, *J. Combin. Theory, Ser. A* 74 (1996) 141–146. <549, 555>

[2740] T. Szőnyi, Blocking sets in Desarguesian affine and projective planes, *Finite Fields Appl.* 3 (1997) 187–202. <552, 555>

[2741] T. Szőnyi, Around Rédei's theorem, *Discrete Math.* 208/209 (1999) 557–575. <554, 555>

[2742] P. Szüsz, On a problem in the theory of uniform distribution, *Comptes Rendus Premier Congrès Hongrois* (1952) 461–472, (in Hungarian). <333, 337>

[2743] L. Taelman, Special L-values of t-motives: a conjecture, *Int. Math. Res. Not. IMRN*

(2009) 2957–2977. <532, 533, 538>

[2744] L. Taelman, A Dirichlet unit theorem for Drinfeld modules, *Math. Ann.* 348 (2010) 899–907. <532, 533, 538>

[2745] L. Taelman, The Carlitz shtuka, *J. Number Theory* 131 (2011) 410–418. <533, 538>

[2746] L. Taelman, Special L-values of Drinfeld modules, To appear in Ann. of Math., preprint available `http://arxiv.org/abs/1004.4304`, 2011. <535, 538>

[2747] L. Taelman, A Herbrand-Ribet theorem for function fields, *Inventiones Mathematicae* 188 (2012) 253–275. <535, 538>

[2748] Y. Taguchi, The Tate conjecture for t-motives, *Proc. Amer. Math. Soc.* 123 (1995) 3285–3287. <532, 538>

[2749] T. Takagi, T. Okamoto, E. Okamoto, and T. Okamoto, editors, *Pairing-Based Cryptography — Pairing 2007*, volume 4575 of *Lecture Notes in Computer Science*, Berlin, 2007. Springer-Verlag. <779, 787>

[2750] T. Takahashi, Good reduction of elliptic modules, *J. Math. Soc. Japan* 34 (1982) 475–487. <532, 538>

[2751] O. Y. Takeshita, On maximum contention-free interleavers and permutation polynomials over integer rings, *IEEE Trans. Inform. Theory* 52 (2006) 1249–1253. <716, 717, 718>

[2752] O. Y. Takeshita, Permutation polynomial interleavers: an algebraic-geometric perspective, *IEEE Trans. Inform. Theory* 53 (2007) 2116–2132. <221, 222>

[2753] O. Y. Takeshita and D. J. Costello, Jr., On deterministic linear interleavers for turbo-codes, In *Proc. 35th Annual Allerton Conference on Communication, Control, and Computing*, 711–712, 1997. <717, 718>

[2754] O. Y. Takeshita and D. J. Costello, Jr., New deterministic interleaver designs for turbo codes, *IEEE Trans. Inform. Theory* 46 (2000) 1988–2006. <717, 718>

[2755] I. Tal and A. Vardy, List decoding of polar codes, In *Proc. IEEE Int. Symp. Information Theory (ISIT)*, 1–5, 2011. <730>

[2756] A. Tamagawa, The Tate conjecture and the semisimplicity conjecture for t-modules, *Sūrikaisekikenkyūsho Kōkyūroku* (1995) 89–94. <532, 538>

[2757] L. Tan and W.-F. Qi, On the k-error linear complexity of l-sequences, *Finite Fields Appl.* 16 (2010) 420–435. <329, 330>

[2758] Y. Tan, A. Pott, and T. Feng, Strongly regular graphs associated with ternary bent functions, *J. Combin. Theory, Ser. A* 117 (2010) 668–682. <258, 265>

[2759] T. Tanaka and R. Mori, Refined rate of channel polarization, preprint available, `http://arxiv.org/abs/1001.2067`, 2010. <730>

[2760] X. Tang, P. Fan, and S. Matsufuji, Lower bound on correlation of spreading sequence set with low or zero correlation, *Electronics Letters* 36 (2000) 551–552. <316, 317>

[2761] R. M. Tanner, A recursive approach to low complexity codes, *IEEE Trans. Inform. Theory* 27 (1981) 533–547. <705, 710>

[2762] T. Tao, *Structure and Randomness*, American Mathematical Society, Providence, RI, 2008. <303>

[2763] T. Tao and V. Vu, *Additive Combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*, Cambridge University Press, Cambridge, 2006. <29, 30, 182, 186>

[2764] V. Tarokh, N. Seshadri, and A. R. Calderbank, Space-time codes for high data rate

wireless communication: performance criterion and code construction, *IEEE Trans. Inform. Theory* 44 (1998) 744–765. <837, 839>

[2765] J. Tate, Endomorphisms of abelian varieties over finite fields, *Invent. Math.* 2 (1966) 134–144. <424, 426, 433, 452, 456, 797, 802>

[2766] J. Tate, The arithmetic of elliptic curves, *Invent. Math.* 23 (1974) 179–206. <416, 433>

[2767] W. Tautz, J. Top, and A. Verberkmoes, Explicit hyperelliptic curves with real multiplication and permutation polynomials, *Canad. J. Math.* 43 (1991) 1055–1064. <232, 233>

[2768] D. E. Taylor, *The Geometry of the Classical Groups*, volume 9 of *Sigma Series in Pure Mathematics*, Heldermann Verlag, Berlin, 1992. <505, 506, 507, 510, 512, 513>

[2769] A. F. Tenca and Ç. K. Koç, A scalable architecture for Montgomery multiplication, In *Proc. Cryptographic Hardware and Embedded Systems (CHES)*, volume 1717 of *Lecture Notes Comput. Sci.*, 94–108, Springer, Berlin, 1999. <813, 814>

[2770] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, volume 46 of *Cambridge Studies in Advanced Mathematics*, Cambridge University Press, Cambridge, 1995. <362, 363, 367>

[2771] A. Terras, *Fourier Analysis on Finite Groups and Applications*, volume 43 of *London Mathematical Society Student Texts*, Cambridge University Press, Cambridge, 1999. <298, 300, 301, 303, 635, 649>

[2772] E. Teske, Square-root algorithms for the discrete logarithm problem (a survey), In *Public-Key Cryptography and Computational Number Theory*, 283–301, de Gruyter, Berlin, 2001. <390, 394>

[2773] F. Thaine, On Gaussian periods that are rational integers, *Michigan Math. J.* 50 (2002) 313–337. <135, 155>

[2774] D. Thakur, Multizeta in function field arithmetic, In *Proceedings of Banff Workshop*, European Mathematical Society (EMS), Zürich. <535, 536, 538>

[2775] D. S. Thakur, *Function Field Arithmetic*, World Scientific Publishing Co. Inc., River Edge, NJ, 2004. <29, 30, 528, 538>

[2776] J. A. Thas, Normal rational curves and k-arcs in Galois spaces, *Rend. Mat. (6)* 1 (1968) 331–334. <577, 580>

[2777] J. A. Thas, The affine plane AG$(2, q)$, q odd, has a unique one point extension, *Invent. Math.* 118 (1994) 133–139. <580>

[2778] "The GAP Group", GAP system for computational discrete algebra, `http://www.gap-system.org`, as viewed in July, 2012. <45, 46>

[2779] "The GNU Project", The GNU MP Bignum library, `http://www.gmplib.org/`, as viewed in July, 2012. <30, 45, 46>

[2780] The Magma computational algebra system for algebra, number theory and geometry, version 2.18-3, 2012. <339, 356, 772, 774>

[2781] "The Mathworks Inc.", MATLAB - The Language of Technical Computing, `http://www.mathworks.com/products/matlab/`, as viewed in July 2012. <45, 46>

[2782] "The OEIS Foundation Inc.", The on-line encyclopedia of integer sequences^{TM}(OEIS^{TM}), `http://www.oeis.org`, as viewed in July, 2012. <44, 46>

[2783] "The PARI Group", PARI/GP Development Center, http://pari.math.u-bordeaux.fr/, as viewed in July, 2012. <45, 46>

[2784] N. Thériault, Index calculus attack for hyperelliptic curves of small genus, In *Advances in Cryptology—ASIACRYPT 2003*, volume 2894 of *Lecture Notes in Comput. Sci.*, 75–92, Springer, Berlin, 2003. <449, 789, 794>

[2785] J. J. Thomas, J. M. Keller, and G. N. Larsen, The calculation of multiplicative inverses over GF(P) efficiently where P is a Mersenne prime, *IEEE Trans. Comput.* 35 (1986) 478–482. <352, 356>

[2786] E. Thomé, Fast computation of linear generators for matrix sequences and application to the block Wiedemann algorithm, In *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation*, 323–331, ACM, New York, 2001. <527>

[2787] T. M. Thompson, *From Error-Correcting Codes Through Sphere Packings to Simple Groups*, volume 21 of *Carus Mathematical Monographs*, Mathematical Association of America, Washington, DC, 1983. <682, 694>

[2788] T. Tian and W. F. Qi, Primitive normal element and its inverse in finite fields, *Acta Math. Sinica (Chin. Ser.)* 49 (2006) 657–668. <110>

[2789] T. Tian and W.-F. Qi, Typical primitive polynomials over integer residue rings, *Finite Fields Appl.* 15 (2009) 796–807. <85>

[2790] A. Tietäväinen, On systems of linear and quadratic equations in finite fields, *Ann. Acad. Sci. Fenn. Ser. A I No.* 382 (1965) 5. <204, 207>

[2791] A. Tietäväinen, On diagonal forms over finite fields, *Ann. Univ. Turku. Ser. A I No.* 118 (1968) 10. <201, 207>

[2792] A. Tietäväinen, On the nonexistence of perfect codes over finite fields, *SIAM J. Appl. Math.* 24 (1973) 88–96. <663, 675, 694>

[2793] A. Tietäväinen, A short proof for the nonexistence of unknown perfect codes over GF(q), $q > 2$, *Ann. Acad. Sci. Fenn. Ser. A I* (1974) 6. <663, 693, 694>

[2794] R. A. H. Toledo, Linear finite dynamical systems, *Comm. Algebra* 33 (2005) 2977–2989. <824>

[2795] A. Tonelli, Bemerkung über die Auflösung quadratischer Congruenzen, *Nachrichten von der Königl. Gesellschaft der Wissenschaften und der Georg-Augusts-Universität zu Göttingen* (1891) 344–346. <787>

[2796] A. Topuzoğlu and A. Winterhof, Pseudorandom sequences, In *Topics in Geometry, Coding Theory and Cryptography*, volume 6 of *Algebr. Appl.*, 135–166, Springer, Dordrecht, 2007. <330, 331, 337>

[2797] Á. Tóth, On the evaluation of Salié sums, *Proc. Amer. Math. Soc.* 133 (2005) 643–645. <154, 155>

[2798] J. Tromp, L. Zhang, and Y. Zhao, Small weight bases for Hamming codes, In *Computing and Combinatorics*, volume 959 of *Lecture Notes in Comput. Sci.*, 235–243, Springer, Berlin, 1995. <84, 85>

[2799] T. T. Truong, Degree complexity of a family of birational maps. II. Exceptional cases, *Math. Phys. Anal. Geom.* 12 (2009) 157–180. <331, 337>

[2800] B. Tsaban and U. Vishne, Efficient linear feedback shift registers with maximal period, *Finite Fields Appl.* 8 (2002) 256–267. <65, 66>

[2801] M. Tsfasman, S. Vlăduţ, and D. Nogin, *Algebraic Geometric Codes: Basic Notions*, volume 139 of *Mathematical Surveys and Monographs*, American Mathematical Society, Providence, RI, 2007. <29, 30>

[2802] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-Geometric Codes*, volume 58 of *Mathematics and its Applications (Soviet Series)*, Kluwer Academic Publishers Group, Dordrecht, 1991. <29, 30, 701, 703>

[2803] M. A. Tsfasman, S. G. Vlăduţ, and T. Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, *Math. Nachr.* 109 (1982) 21–28. <456, 457, 462, 702, 703>

[2804] S. Tsujii, A. Fujioka, and T. Itoh, Generalization of the public key cryptosystem based on the difficulty of solving a system of non-linear equations, In *Proc. Tenth Symposium on Information Theory and Its Applications*, JA5–3, 1987. <755, 759, 774>

[2805] S. Tsujii, K. Kurosawa, T. Itoh, A. Fujioka, and T. Matsumoto, A public key cryptosystem based on the difficulty of solving a system of nonlinear equations, *ICICE Transactions (D) J69-D* 12 (1986) 1963–1970. <755, 759, 774>

[2806] W. J. Turner, *Black Box Linear Algebra with the Linbox Library*, PhD thesis, 2002. <523, 527>

[2807] G. Turnwald, Permutation polynomials of binomial type, In *Contributions to General Algebra, 6*, 281–286, Hölder-Pichler-Tempsky, Vienna, 1988. <211, 216, 222>

[2808] G. Turnwald, A new criterion for permutation polynomials, *Finite Fields Appl.* 1 (1995) 64–82. <210, 221, 222, 226, 227, 228, 229>

[2809] G. Turnwald, On Schur's conjecture, *J. Austral. Math. Soc., Ser. A* 58 (1995) 312–357. <221, 222, 231, 233>

[2810] R. Turyn and J. Storer, On binary sequences, *Proc. Amer. Math. Soc.* 12 (1961) 394–399. <316, 317>

[2811] R. J. Turyn, The linear generation of Legendre sequence, *J. Soc. Indust. Appl. Math.* 12 (1964) 115–116. <326, 330>

[2812] R. J. Turyn, Character sums and difference sets, *Pacific J. Math.* 15 (1965) 319–346. <596, 597, 598>

[2813] R. J. Turyn, An infinite class of Williamson matrices, *J. Combin. Theory, Ser. A* 12 (1972) 319–321. <601, 610>

[2814] R. J. Turyn, Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings, *J. Combin. Theory, Ser. A* 16 (1974) 313–333. <833, 839>

[2815] S. Uchiyama, Note on the mean value of $V(f)$. II, *Proc. Japan Acad.* 31 (1955) 321–323. <361, 367>

[2816] S. Uchiyama, Sur les polynômes irréductibles dans un corps fini. II, *Proc. Japan Acad.* 31 (1955) 267–269. <69, 75>

[2817] D. Ulmer, Jacobi sums, Fermat Jacobians, and ranks of abelian varieties over towers of function fields, *Math. Res. Lett.* 14 (2007) 453–467, `http://people.math.gatech.edu/~ulmer/research/papers/2007c-correction.pdf`. <140, 155>

[2818] C. Umans, Fast polynomial factorization and modular composition in small characteristic, In *STOC'08*, 481–490, ACM, New York, 2008. <351, 356>

[2819] A. Valette, Graphes de Ramanujan et applications, *Astérisque* (1997) Exp. No. 829, 4, 247–276, Séminaire Bourbaki, Vol. 1996/97. <634, 649>

[2820] E. R. van Dam and D. Fon-Der-Flaass, Codes, graphs, and schemes from nonlinear functions, *European J. Combin.* 24 (2003) 85–98. <252, 254>

[2821] E. R. van Dam and W. H. Haemers, Eigenvalues and the diameter of graphs, *Linear and Multilinear Algebra* 39 (1995) 33–44. <636, 649>

[2822] W. van Dam, S. Hallgren, and L. Ip, Quantum algorithms for some hidden shift problems, In *Proceedings of the Fourteenth Annual ACM-SIAM Symposium on Discrete Algorithms (Baltimore, MD, 2003)*, 489–498, New York, 2003, ACM.

<830, 831>

[2823] W. van Dam and I. E. Shparlinski, Classical and quantum algorithms for exponential congruences, In *Theory of Quantum Computation, Communication, and Cryptography*, volume 5106 of *Lecture Notes in Comput. Sci.*, 1–10, Springer, Berlin, 2008. <830, 831>

[2824] G. van der Geer and M. van der Vlugt, Reed-Muller codes and supersingular curves. I, *Compositio Math.* 84 (1992) 333–367. <480>

[2825] G. van der Geer and M. van der Vlugt, On the existence of supersingular curves of given genus, *J. Reine Angew. Math.* 458 (1995) 53–61. <479, 480>

[2826] G. van der Geer and M. van der Vlugt, Quadratic forms, generalized Hamming weights of codes and curves with many points, *J. Number Theory* 59 (1996) 20–36. <199, 200>

[2827] G. van der Geer and M. van der Vlugt, An asymptotically good tower of curves over the field with eight elements, *Bull. London Math. Soc.* 34 (2002) 291–300. <461, 462>

[2828] G. van der Geer and M. van der Vlugt, Tables of curves with many points, 2009, `http://www.science.uva.nl/~geer/tables-mathcomp21.pdf`. <453, 456>

[2829] M. van der Put, A note on p-adic uniformization, *Nederl. Akad. Wetensch. Indag. Math.* 49 (1987) 313–318. <536, 538>

[2830] B. L. van der Waerden, *A History of Algebra: From al-Khwārizmī to Emmy Noether*, Springer-Verlag, Berlin, 1985. <2, 10>

[2831] J. H. van Lint, *Introduction to Coding Theory*, volume 86 of *Graduate Texts in Mathematics*, Springer-Verlag, Berlin, third edition, 1999. <29, 30, 578, 580, 652, 654, 659, 661, 662, 663, 664, 665, 674, 675, 676, 677, 680, 681, 694>

[2832] J. H. van Lint and A. Schrijver, Construction of strongly regular graphs, two-weight codes and partial geometries by finite fields, *Combinatorica* 1 (1981) 63–73. <608, 610>

[2833] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, Cambridge University Press, Cambridge, 1992. <29, 30, 600, 610>

[2834] P. C. van Oorschot and M. J. Wiener, Parallel collision search with cryptanalytic applications, *J. Cryptology* 12 (1999) 1–28. <390, 394, 736, 740>

[2835] T. van Trung and S. Martirosyan, New constructions for IPP codes, *Des. Codes Cryptogr.* 35 (2005) 227–239. <604, 610>

[2836] P. van Wamelen, New explicit multiplicative relations between Gauss sums, *Int. J. Number Theory* 3 (2007) 275–292. <140, 155>

[2837] R. Varshamov, Estimate of the number of signals in error correcting codes, *Dokl. Akad. Nauk. SSSR* 117 (1957) 739–741. <662, 693, 694>

[2838] R. Varshamov, A general method of synthesizing irreducible polynomials over Galois fields, *Soviet Math. Dokl.* 29 (1984) 334–336. <371, 373>

[2839] R. R. Varshamov, A certain linear operator in a Galois field and its applications (Russian), *Studia, Sci. Math. Hunger.* 8 (1973) 5–19. <58, 61>

[2840] R. R. Varshamov, Operator substitutions in a Galois field, and their applications (Russian), *Dokl. Akad. Nauk SSSR;* 211 (1973) 768–771. <58, 61>

[2841] R. R. Varshamov, A general method of synthesis for irreducible polynomials over Galois fields, *Dokl. Akad. Nauk SSSR* 275 (1984) 1041–1044. <59, 60, 61, 107, 110>

[2842] R. R. Varshamov and G. Ananiashvili, The theory of polynomial reducibility in

finite fields (Russian), In *Abstract and Structual Theory of the Construction of Swithching Circuits (Russian) (M.A. Gavrilov, ed.)*, 134–138, Nauka, Moscow, 1966. <56, 61>

[2843] R. R. Varshamov and G. Garakov, On the theory of self-dual polynomials over a Galois field (Russian), *Bull. Math. Soc. Sci. Math. R. S. Roumania (New Ser.)* 13 (1969) 403–415. <56, 61>

[2844] R. C. Vaughan and T. D. Wooley, Waring's problem: a survey, In *Number Theory for the Millennium*, volume III, 301–340, A. K. Peters, Natick, MA, 2002. <491, 492>

[2845] T. Vaughan, Polynomials and linear transformations over finite fields, *J. Reine Angew. Math.* 267 (1974) 179–206. <58, 61>

[2846] A. Veliz-Cuba, A. S. Jarrah, and R. Laubenbacher, Polynomial algebra of discrete models in systems biology, *Bioinformatics* 26 (2010) 1637–1643. <816, 817, 820, 821, 824>

[2847] J. Vélu, Isogénies entre courbes elliptiques, *C. R. Acad. Sci. Paris, Sér. A-B* 273 (1971) A238–A241. <115, 122>

[2848] A. Venkateswarlu and H. Niederreiter, Improved results on periodic multisequences with large error linear complexity, *Finite Fields Appl.* 16 (2010) 463–476. <324, 330>

[2849] F. Vercauteren, Computing zeta functions of hyperelliptic curves over finite fields of characteristic 2, In *Advances in Cryptology—CRYPTO 2002*, volume 2442 of *Lecture Notes in Comput. Sci.*, 369–384, Springer, Berlin, 2002. <447, 449>

[2850] F. Vercauteren, Optimal pairings, *IEEE Transactions on Information Theory* 56 (2010) 455–461. <782, 787>

[2851] E. R. Verheul, Evidence that XTR is more secure than supersingular elliptic curve cryptosystems, *Journal of Cryptology* 17 (2004) 277–296. <781, 787>

[2852] C.-M. Viallet, Algebraic dynamics and algebraic entropy, *Int. J. Geom. Methods Mod. Phys.* 5 (2008) 1373–1391. <330, 331, 337>

[2853] C. M. Viallet, Integrable lattice maps: Q_V, a rational version of Q_4, *Glasgow Math. J.* 51 (2009) 157–163. <330, 331, 337>

[2854] G. D. Villa Salvador, *Topics in the Theory of Algebraic Function Fields*, Mathematics: Theory & Applications. Birkhäuser Boston Inc., Boston, MA, 2006. <399, 415>

[2855] G. Villard, Further analysis of Coppersmith's block Wiedemann algorithm for the solution of sparse linear systems, In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation*, ISSAC '97, 32–39, ACM, New York, NY, USA, 1997. <527>

[2856] G. Villard, Computing the Frobenius normal form of a sparse matrix, In *Computer Algebra in Scientific Computing*, 395–407, Springer, Berlin, 2000. <523, 524, 527>

[2857] G. Villard, *Algorithmique en Algèbre Linéaire Exacte*, Mémoire d'habilitation, Université Claude Bernard Lyon 1, 2003. <523, 527>

[2858] L. A. Vinh, The Szemerédi-Trotter type theorem and the sum-product estimate in finite fields, *Eur. J. Combinatorics* 32 (2011) 1177–1181. <185, 186>

[2859] I. M. Vinogradov, Representation of an odd number as a sum of three primes, *Comptes Rendus (Doklady)* 15 (1937) 191–294. <489, 492>

[2860] U. Vishne, Factorization of trinomials over Galois fields of characteristic 2, *Finite Fields Appl.* 3 (1997) 370–377. <64, 66>

[2861] A. J. Viterbi, Error bounds for convolutional codes and an asymptotically optimum decoding algorithm, *IEEE Trans. Inform. Theory* 13 (1967) 260–269. <712, 718>

[2862] A. J. Viterbi, *CDMA: Principles of Spread Spectrum Communication*, Addison-Wesley, Reading, MA, 1995. <310>

[2863] S. G. Vlèduts and Y. I. Manin, Linear codes and modular curves, In *Current Problems in Mathematics, Vol. 25*, Itogi Nauki i Tekhniki, 209–257, Akad. Nauk SSSR Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1984. <538>

[2864] S. G. Vlăduţ and V. G. Drinfeld, The number of points of an algebraic curve, *Funktsional. Anal. i Prilozhen.* 17 (1983) 68–69. <455, 456>

[2865] J. F. Voloch, Diagonal equations over function fields, *Bol. Soc. Brasil. Mat.* 16 (1985) 29–39. <207>

[2866] J. F. Voloch, On the order of points on curves over finite fields, *Integers* 7 (2007) A49, 4. <93, 94>

[2867] J. F. Voloch, Symmetric cryptography and algebraic curves, In *Algebraic Geometry and its Applications*, volume 5 of *Ser. Number Theory Appl.*, 135–141, World Sci. Publ., Hackensack, NJ, 2008. <248, 254>

[2868] J. F. Voloch, Elements of high order on finite fields from elliptic curves, *Bull. Aust. Math. Soc.* 81 (2010) 425–429. <94>

[2869] C. H. Waddington, Canalisation of development and the inheritance of acquired characters, *Nature* 150 (1942) 563–564. <822, 824>

[2870] L. I. Wade, Certain quantities transcendental over $GF(p^n, x)$, *Duke Math. J.* 8 (1941) 701–720. <538>

[2871] A. Wagner, On finite affine line transitive planes, *Math. Z.* 87 (1965) 1–11. <560, 565>

[2872] S. S. Wagstaff, Jr., The Cunningham project, `http://homes.cerias.purdue.edu/~ssw/cun/`, as viewed in July, 2012. <44, 46>

[2873] R. J. Walker, Determination of division algebras with 32 elements, In *Proc. Sympos. Appl. Math., Vol. XV*, 83–85, Amer. Math. Soc., Providence, RI, 1963. <268, 270>

[2874] D. Wan, On the Riemann hypothesis for the characteristic p zeta function, *J. Number Theory* 58 (1996) 196–212. <536, 538>

[2875] D. Wan, Generators and irreducible polynomials over finite fields, *Math. Comp.* 66 (1997) 1195–1212. <70, 71, 75, 162, 163>

[2876] D. Wan, Computing zeta functions over finite fields, In *Finite Fields: Theory, Applications, and Algorithms*, volume 225 of *Contemp. Math.*, 131–141, Amer. Math. Soc., Providence, RI, 1999. <483, 484>

[2877] D. Wan, Dwork's conjecture on unit root zeta functions, *Ann. of Math., 2nd Ser.* 150 (1999) 867–927. <472, 480>

[2878] D. Wan, Higher rank case of Dwork's conjecture, *J. Amer. Math. Soc.* 13 (2000) 807–852. <472, 480>

[2879] D. Wan, Rank one case of Dwork's conjecture, *J. Amer. Math. Soc.* 13 (2000) 853–908. <472, 480>

[2880] D. Wan, Rationality of partial zeta functions, *Indag. Math. (New Ser.)* 14 (2003) 285–292. <192, 195>

[2881] D. Wan, Variation of p-adic Newton polygons for L-functions of exponential sums, *Asian J. Math.* 8 (2004) 427–471. <476, 478, 480>

[2882] D. Wan, Mirror symmetry for zeta functions, In *Mirror Symmetry V*, volume 38 of *AMS/IP Stud. Adv. Math.*, 159–184, Amer. Math. Soc., Providence, RI, 2006. <190, 194, 195>

[2883] D. Wan, Algorithmic theory of zeta functions over finite fields, In *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, 551–578, Cambridge Univ. Press, Cambridge, 2008. <484>

[2884] D. Wan, Lectures on zeta functions over finite fields, In *Higher-Dimensional Geometry over Finite Fields*, volume 16 of *NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur.*, 244–268, IOS, Amsterdam, 2008. <187, 190, 195>

[2885] D. Wan, Modular counting of rational points over finite fields, *Found. Comput. Math.* 8 (2008) 597–605. <482, 484>

[2886] D. Q. Wan, On a problem of Niederreiter and Robinson about finite fields, *J. Austral. Math. Soc., Ser. A* 41 (1986) 336–338. <221, 222>

[2887] D. Q. Wan, Permutation polynomials over finite fields, *Acta Math. Sinica (New Ser.)* 3 (1987) 1–5. <211, 216, 222>

[2888] D. Q. Wan, Zeros of diagonal equations over finite fields, *Proc. Amer. Math. Soc.* 103 (1988) 1049–1052. <203, 204, 207>

[2889] D. Q. Wan, An elementary proof of a theorem of Katz, *Amer. J. Math.* 111 (1989) 1–8. <193, 195>

[2890] D. Q. Wan, Permutation polynomials and resolution of singularities over finite fields, *Proc. Amer. Math. Soc.* 110 (1990) 303–309. <211, 222>

[2891] D. Q. Wan, A generalization of the Carlitz conjecture, In *Finite Fields, Coding Theory, and Advances in Communications and Computing*, volume 141 of *Lecture Notes in Pure and Appl. Math.*, 431–432, Dekker, New York, 1993. <211, 222>

[2892] D. Q. Wan, Newton polygons of zeta functions and L functions, *Ann. of Math., 2nd Ser.* 137 (1993) 249–293. <476, 480>

[2893] D. Q. Wan, A p-adic lifting lemma and its applications to permutation polynomials, In *Finite Fields, Coding Theory, and Advances in Communications and Computing*, volume 141 of *Lecture Notes in Pure and Appl. Math.*, 209–216, Dekker, New York, 1993. <210, 222, 226, 229>

[2894] D. Q. Wan, A classification conjecture about certain permutation polynomials, In *Finite Fields: Theory, Applications and Algorithms*, volume 168 of *Contemporary Math.*, 401–402, American Mathematical Society, Providence, RI, 1994. <221, 222>

[2895] D. Q. Wan, Permutation binomials over finite fields, *Acta Math. Sinica (New Ser.)* 10 (1994) 30–35. <211, 216, 222>

[2896] D. Q. Wan, A Chevalley-Warning approach to p-adic estimates of character sums, *Proc. Amer. Math. Soc.* 123 (1995) 45–54. <193, 195>

[2897] D. Q. Wan, Minimal polynomials and distinctness of Kloosterman sums, *Finite Fields Appl.* 1 (1995) 189–203. <149, 155>

[2898] D. Q. Wan and R. Lidl, Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure, *Monatsh. Math.* 112 (1991) 149–163. <214, 222>

[2899] D. Q. Wan, G. L. Mullen, and P. J.-S. Shiue, Erratum: "The number of permutation polynomials of the form $f(x) + cx$ over a finite field", *Proc. Edinburgh Math. Soc., Ser. II* 38 (1995) 133. <546, 547>

[2900] D. Q. Wan, G. L. Mullen, and P. J.-S. Shiue, The number of permutation poly-

nomials of the form $f(x) + cx$ over a finite field, *Proc. Edinburgh Math. Soc., Ser. II* 38 (1995) 133–149. <221, 222, 546, 547>

[2901] D. Q. Wan, P. J.-S. Shiue, and C. S. Chen, Value sets of polynomials over finite fields, *Proc. Amer. Math. Soc.* 119 (1993) 711–717. <210, 222, 227, 229>

[2902] Z.-X. Wan, *Geometry of Classical Groups over Finite Fields*, Science Press, Beijing, second edition, 2002. <29, 30, 504, 506, 508, 511, 512, 513>

[2903] Z.-X. Wan, *Lectures on Finite Fields and Galois Rings*, World Scientific Publishing Co. Inc., River Edge, NJ, 2003. <11, 27, 29, 30>

[2904] Z.-X. Wan, A shorter proof for an explicit formula for discrete logarithms in finite fields, *Discrete Math.* 308 (2008) 4914–4915. <389, 394>

[2905] Z.-X. Wan, *Finite Fields and Galois Rings*, World Scientific Publishing Co. Inc., Singapore, 2012. <29, 30>

[2906] Z.-X. Wan and K. Zhou, On the complexity of the dual basis of a type I optimal normal basis, *Finite Fields Appl.* 13 (2007) 411–417. <119, 122>

[2907] C. C. Wang, An algorithm to design finite field multipliers using a self-dual normal basis, *IEEE Trans. Comput.* 38 (1989) 1457–1460. <37, 46>

[2908] C. C. Wang, T. K. Truong, H. M. Shao, L. J. Deutsch, J. K. Omura, and I. S. Reed, VLSI architectures for computing multiplications and inverses in $GF(2^m)$, *IEEE Trans. Comput.* 34 (1985) 709–716. <810, 811, 814>

[2909] L. Wang, On permutation polynomials, *Finite Fields Appl.* 8 (2002) 311–322. <215, 222>

[2910] L. Wang and Y. Zhu, $F[x]$-lattice basis reduction algorithm and multisequence synthesis, *Sci. China, Ser. F* 44 (2001) 321–328. <323, 330>

[2911] L.-C. Wang and F.-H. Chang, Tractable rational map cryptosystem (version 2), `http://eprint.iacr.org/2004/046`, ver. 20040221:212731. <765, 774>

[2912] L.-C. Wang and F.-H. Chang, Tractable rational map cryptosystem (version 4), `http://eprint.iacr.org/2004/046`, ver. 20060203:065450. <765, 774>

[2913] L.-C. Wang, Y.-H. Hu, F. Lai, C.-Y. Chou, and B.-Y. Yang, Tractable rational map signature, In *Public Key Cryptography—PKC 2005*, volume 3386 of *Lecture Notes in Comput. Sci.*, 244–257, Springer, Berlin, 2005. <763, 774>

[2914] L.-C. Wang, B.-Y. Yang, Y.-H. Hu, and F. Lai, A "medium-field" multivariate public-key encryption scheme, In *Topics in Cryptology—CT-RSA 2006*, volume 3860 of *Lecture Notes in Comput. Sci.*, 132–149, Springer, Berlin, 2006. <765, 768, 774>

[2915] L.-P. Wang and H. Niederreiter, Enumeration results on the joint linear complexity of multisequences, *Finite Fields Appl.* 12 (2006) 613–637. <323, 330>

[2916] L.-P. Wang, Y.-F. Zhu, and D.-Y. Pei, On the lattice basis reduction multisequence synthesis algorithm, *IEEE Trans. Inform. Theory* 50 (2004) 2905–2910. <323, 330>

[2917] M. Wang, Linear complexity profiles and continued fractions, In *Advances in Cryptology—EUROCRYPT '89*, volume 434 of *Lecture Notes in Comput. Sci.*, 571–585, Springer, Berlin, 1990. <322, 330>

[2918] M. Wang and I. F. Blake, Bit serial multiplication in finite fields, *SIAM J. Discrete Math.* 3 (1990) 140–148. <99, 103>

[2919] M. Z. Wang, Linear complexity profiles and jump complexity, *Inform. Process. Lett.* 61 (1997) 165–168. <322, 330>

[2920] P. S. Wang, An improved multivariate polynomial factoring algorithm, *Math. Comp.*

32 (1978) 1215–1231. <378, 386>

[2921] P. S. Wang and L. P. Rothschild, Factoring multivariate polynomials over the integers, *Math. Comp.* 29 (1975) 935–950. <378, 386>

[2922] Q. Wang, Cyclotomic mapping permutation polynomials over finite fields, In *Sequences, Subsequences, and Consequences*, volume 4893 of *Lecture Notes in Comput. Sci.*, 119–128, Springer, Berlin, 2007. <214, 215, 222>

[2923] Q. Wang, On inverse permutation polynomials, *Finite Fields Appl.* 15 (2009) 207–213. <222>

[2924] Q. Wang, On generalized Lucas sequences, *Contemporary Math.* 531 (2010) 127–141. <215, 221, 222>

[2925] Q. Wang, K. Wang, and Z. Dai, Implementation of multi-continued fraction algorithm and application to multi-sequence linear synthesis, In *Sequences and Their Applications—SETA 2006*, volume 4086 of *Lecture Notes in Comput. Sci.*, 248–258, Springer, Berlin, 2006. <322, 330>

[2926] Q. Wang and J. L. Yucas, Dickson polynomials over finite fields, *Finite Fields Appl.* 18 (2012) 814–831. <277, 280, 281, 282>

[2927] Y. Wang, Linear complexity versus pseudorandomness: on Beth and Dai's result, In *Advances in Cryptology—ASIACRYPT'99*, volume 1716 of *Lecture Notes in Comput. Sci.*, 288–298, Springer, Berlin, 1999. <328, 330>

[2928] K. L. Wantz, A new class of unitals in the Hughes plane, *Geom. Dedicata* 70 (1998) 125–138. <563, 565>

[2929] L. C. Washington, *Introduction to Cyclotomic Fields*, volume 83 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, second edition, 1997. <137, 146, 155>

[2930] L. C. Washington, *Elliptic Curves*, Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton, FL, 2003. <29, 30>

[2931] L. C. Washington, *Elliptic Curves*, Discrete Mathematics and Its Applications. Chapman & Hall/CRC, Boca Raton, FL, second edition, 2008. <29, 30, 416, 433>

[2932] A. Wassermann, Konstruktion von Normalbasen, *Bayreuth. Math. Schr.* (1990) 155–164. <114, 122>

[2933] A. Wassermann, Zur Arithmetik in endlichen Körpern, *Bayreuth. Math. Schr.* (1993) 147–251, Dissertation, Universität Bayreuth, Bayreuth, 1992. <114, 122>

[2934] Y. Watanabe, N. Takagi, and K. Takagi, A VLSI algorithm for division in $GF(2^m)$ based on extended binary GCD algorithm, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* E85-A (2002) 994–999. <807, 814>

[2935] W. C. Waterhouse, Abelian varieties over finite fields, *Ann. Sci. École Norm. Sup. IVe Ser.* 2 (1969) 521–560. <424, 429, 433>

[2936] W. A. Webb, Waring's problem in GF[q,x], *Acta Arith.* 22 (1973) 207–220. <491, 492>

[2937] C. Wei and Q. Sun, The least integer represented by $\sum_{i=1}^{n} x_i/d_i$ and its application, *Acta Math. Sinica (Chin. Ser.)* 49 (2006) 1021–1026. <203, 207>

[2938] Q. Wei and Q. Zhang, On strong orthogonal systems and weak permutation polynomials over finite commutative rings, *Finite Fields Appl.* 13 (2007) 113–120. <225>

[2939] S. Wei, G. Chen, and G. Xiao, A fast algorithm for determining the linear complexity

of periodic sequences, In *Information Security and Cryptology*, volume 3822 of *Lecture Notes in Comput. Sci.*, 202–209, Springer, Berlin, 2005. <322, 330>

[2940] S. Wei, G. Xiao, and Z. Chen, A fast algorithm for determining the linear complexity of a binary sequence with period $2^n p^m$, *Sci. China, Ser. F* 44 (2001) 453–460. <322, 330>

[2941] S. Wei, G. Xiao, and Z. Chen, A fast algorithm for determining the minimal polynomial of a sequence with period $2p^n$ over GF(q), *IEEE Trans. Inform. Theory* 48 (2002) 2754–2758. <322, 330>

[2942] A. Weil, On some exponential sums, *Proc. Nat. Acad. Sci. U. S. A.* 34 (1948) 204–207. <156, 163>

[2943] A. Weil, *Sur les Courbes Algébriques et les Variétés qui s'en dÉduisent*, Actualités Sci. Ind., no. 1041; Publ. Inst. Math. Univ. Strasbourg 7 (1945). Hermann et Cie., Paris, 1948. <156, 163, 489, 492>

[2944] A. Weimerskirch and C. Paar, Generalizations of the Karatsuba algorithm for efficient implementations, 2006, preprint available, `http://eprint.iacr.org/2006/224`. <804, 814>

[2945] L. Welch, Lower bounds on the maximum cross correlation of signals, *IEEE Trans. Inform. Theory* 20 (1974) 397–399. <313, 317>

[2946] L. R. Welch and E. R. Berlekamp, Error Correction for Algebraic Block Codes, U. S. Patent 4,633,470 (1986). <686, 694>

[2947] E. J. Weldon, Jr., Euclidean geometry cyclic codes, In *Combinatorial Mathematics and its Applications*, 377–387, Univ. North Carolina Press, Chapel Hill, N.C., 1969. <680, 687, 694>

[2948] C. Wells, The degrees of permutation polynomials over finite fields, *J. Combinatorial Theory* 7 (1969) 49–55. <212, 213, 222>

[2949] A. Wells Jr, A polynomial form for logarithms modulo a prime, *IEEE Trans. Inf. Theory* 30 (1984) 845–846. <389, 394>

[2950] G. P. Wene, On the multiplicative structure of finite division rings, *Aequationes Math.* 41 (1991) 222–233. <270>

[2951] A. Weng, *Konstruktion kryptographisch geeigneter Kurven mit komplexer Multiplikation*, PhD thesis, Universität Gesamthochschule Essen, 2001. <794>

[2952] A. Weng, Constructing hyperelliptic curves of genus 2 suitable for cryptography, *Math. Comput.* 72 (2003) 435–458. <794>

[2953] G. Weng, W. Qiu, Z. Wang, and Q. Xiang, Pseudo-Paley graphs and skew Hadamard difference sets from presemifields, *Des. Codes Cryptogr.* 44 (2007) 49–62. <274>

[2954] G. Weng and X. Zeng, Further results on planar DO functions and commutative semifields, *Des. Codes Cryptog.* 63 (2012) 413–423. <274>

[2955] R. C. Whaley, A. Petitet, and J. J. Dongarra, Automated empirical optimizations of software and the ATLAS project, *Parallel Computing* 27 (2001) 3–35. <515, 527>

[2956] A. L. Whiteman, An infinite family of Hadamard matrices of Williamson type, *J. Combin. Theory, Ser. A* 14 (1973) 334–340. <601, 610>

[2957] D. H. Wiedemann, Solving sparse linear equations over finite fields, *IEEE Trans. Inform. Theory* 32 (1986) 54–62. <343, 356, 393, 394, 522, 527>

[2958] D. Wiedermann, An iterated quadratic extension of GF(2), *Fibonacci Quart.* 26 (1988) 290–295. <60, 61>

[2959] M. J. Wiener and R. J. Zuccherato, Faster attacks on elliptic curve cryptosystems, In S. Tavares and H. Meijer, editors, *Selected Areas in Cryptography—SAC '98*, volume 1556 of *Lecture Notes in Computer Science*, 190–100, Springer-Verlag, Berlin, 1999. <776, 787>

[2960] M. L. H. Willems and J. A. Thas, A note on the existence of special Laguerre i-structures and optimal codes, *European J. Combin.* 4 (1983) 93–96. <578, 580>

[2961] M. Willett, Matrix fields over GF(q), *Duke Math. J.* 40 (1973) 701–704. <495, 502>

[2962] K. S. Williams, On general polynomials, *Canad. Math. Bull.* 10 (1967) 579–583. <226, 229>

[2963] K. S. Williams, On exceptional polynomials, *Canad. Math. Bull.* 11 (1968) 279–282. <226, 229>

[2964] K. S. Williams, Polynomials with irreducible factors of specified degree, *Canad. Math. Bull.* 12 (1969) 221–223. <361, 367>

[2965] V. V. Williams, Breaking the Coppersmith–Winograd barrier, 2011, preprint available at `http:cs.berkeley.edu/~virgi/matrixmult.pdf`. <351, 356, 373, 375>

[2966] V. V. Williams, Multiplying matrices faster than Coppersmith-Winograd, In *Proceedings of the Forty Fourth Symposium on Theory of Computing*, STOC '12, 887–898, New York, NY, USA, 2012, ACM. <351, 356, 367, 373, 513, 527>

[2967] R. M. Wilson, Cyclotomy and difference families in elementary abelian groups, *J. Number Theory* 4 (1972) 17–47. <585, 590>

[2968] S. Winograd, On multiplication of 2×2 matrices, *Linear Algebra and Appl.* 4 (1971) 381–388. <516, 527>

[2969] S. Winograd, *Arithmetic Complexity of Computations*, SIAM, 1980. <805, 807, 808, 814>

[2970] A. Winterhof, On the distribution of powers in finite fields, *Finite Fields Appl.* 4 (1998) 43–54. <175, 179>

[2971] A. Winterhof, On Waring's problem in finite fields, *Acta Arith.* 87 (1998) 171–177. <169, 179, 206, 207>

[2972] A. Winterhof, Incomplete additive character sums and applications, In *Finite Fields and Applications*, 462–474, Springer, Berlin, 2001. <175, 179>

[2973] A. Winterhof, A note on Waring's problem in finite fields, *Acta Arith.* 96 (2001) 365–368. <206, 207>

[2974] A. Winterhof, Some estimates for character sums and applications, *Des. Codes Cryptogr.* 22 (2001) 123–131. <175, 179>

[2975] A. Winterhof, A note on the linear complexity profile of the discrete logarithm in finite fields, In *Coding, Cryptography and Combinatorics*, volume 23 of *Progr. Comput. Sci. Appl. Logic*, 359–367, Birkhäuser, Basel, 2004. <327, 330>

[2976] A. Winterhof and C. van de Woestijne, Exact solutions to Waring's problem for finite fields, *Acta Arith.* 141 (2010) 171–190. <206, 207>

[2977] E. Wirsing, Thin essential components, In *Topics in Number Theory*, 429–442. Colloq. Math. Soc. János Bolyai, Vol. 13, North-Holland, Amsterdam, 1976. <178, 179>

[2978] E. Witt, Über steinersche systeme, *Abh. Math. Sem. Univ. Hamburg* 12 (1938) 265–275. <580>

[2979] C. Wolf, A. Braeken, and B. Preneel, Efficient cryptanalysis of RSE(2)PKC and RSSE(2)PKC, In *2004*, volume 3352 of *Lecture Notes in Computer Science*, 294–309, Sept. 8–10 2004, Extended version: `http://eprint.iacr.org/2004/237`. <762, 774>

[2980] J. K. Wolf, Adding two information symbols to certain nonbinary BCH codes and some applications, *Bell System Tech. J.* 48 (1969) 2405–2424. <672, 694>

[2981] J. Wolfmann, Formes quadratiques et codes à deux poids, *C. R. Acad. Sci. Paris, Sér. A-B* 281 (1975) Aii, A533–A535. <199, 200>

[2982] J. Wolfmann, The number of solutions of certain diagonal equations over finite fields, *J. Number Theory* 42 (1992) 247–257. <202, 207>

[2983] J. Wolfmann, New results on diagonal equations over finite fields from cyclic codes, In *Finite Fields: Theory, Applications, and Algorithms*, volume 168 of *Contemp. Math.*, 387–395, Amer. Math. Soc., Providence, RI, 1994. <207>

[2984] J. Wolfmann, Some systems of diagonal equations over finite fields, *Finite Fields Appl.* 4 (1998) 29–37. <207>

[2985] "Wolfram Research", Wolfram Research: Mathematica, technical and scientific software, `http://www.wolfram.com/`, as viewed in July, 2012. <45, 46>

[2986] W. K. Wootters and B. D. Fields, Optimal state-determination by mutually unbiased measurements, *Ann. Physics* 191 (1989) 363–381. <825, 831>

[2987] H. Wu, Low complexity bit-parallel finite field arithmetic using polynomial basis, In *Proc. Cryptographic Hardware and Embedded Systems (CHES)*, volume 1717 of *Lecture Notes Comput. Sci.*, 280–291, Springer, Berlin, 1999. <805, 814>

[2988] H. Wu, Bit-parallel finite field multiplier and squarer using polynomial basis, *IEEE Trans. Comput.* 51 (2002) 750–758. <806, 814>

[2989] H. Wu, M. A. Hasan, and I. F. Blake, New low-complexity bit-parallel finite field multipliers using weakly dual bases, *IEEE Trans. Comput.* 47 (1998) 1223–1234. <813, 814>

[2990] H. Wu, M. A. Hasan, I. F. Blake, and S. Gao, Finite field multiplier using redundant representation, *IEEE Trans. Comput.* 51 (2002) 1306–1316. <344, 356, 813, 814>

[2991] M. Wu, X. Yang, and C. Chan, A dynamic analysis of irs-pkr signaling in liver cells: A discrete modeling approach, *PLoS ONE* 4 (2009) e8040. <815, 824>

[2992] P.-C. Wu, Random number generation with primitive pentanomials, *ACM Trans. Modeling and Computer Simulation* 11 (2001) 346–351. <91, 92, 93>

[2993] Q. Xiang, Maximally nonlinear functions and bent functions, *Des. Codes Cryptogr.* 17 (1999) 211–218. <232, 233>

[2994] G. Xiao and S. Wei, Fast algorithms for determining the linear complexity of period sequences., In *Progress in Cryptology—INDOCRYPT 2002*, volume 2551 of *Lecture Notes in Comput. Sci.*, 12–21, Springer, Berlin, 2002. <322, 330>

[2995] G. Xiao, S. Wei, K. Y. Lam, and K. Imamura, A fast algorithm for determining the linear complexity of a sequence with period p^n over GF(q), *IEEE Trans. Inform. Theory* 46 (2000) 2203–2206. <322, 330>

[2996] G. Z. Xiao and J. L. Massey, A spectral characterization of correlation-immune combining functions, *IEEE Trans. Inform. Theory* 34 (1988) 569–571. <240, 245>

[2997] C. Xing and Y. Ding, Multisequences with large linear and k-error linear complexity from Hermitian function fields, *IEEE Trans. Inform. Theory* 55 (2009) 3858–3863. <324, 330>

[2998] C. P. Xing, Goppa geometric codes achieving the Gilbert-Varshamov bound, *IEEE Trans. Inform. Theory* 51 (2005) 259–264. <702, 703>

[2999] C. P. Xing and H. Niederreiter, A construction of low-discrepancy sequences using global function fields, *Acta Arith.* 73 (1995) 87–102. <620, 621>

[3000] C. P. Xing, H. Niederreiter, and K. Y. Lam, A generalization of algebraic-geometry codes, *IEEE Trans. Inform. Theory* 45 (1999) 2498–2501. <698, 703>

[3001] C. P. Xing and S. L. Yeo, New linear codes and algebraic function fields over finite fields, *IEEE Trans. Inform. Theory* 53 (2007) 4822–4825. <698, 703>

[3002] T. Yan, The geobucket data structure for polynomials, *J. Symbolic Comput.* 25 (1998) 285–293. <375, 386>

[3003] B.-Y. Yang and J.-M. Chen, All in the XL family: theory and practice, In *Information Security and Cryptology—ICISC 2004*, volume 3506 of *Lecture Notes in Comput. Sci.*, 67–86, Springer, Berlin, 2005. <773, 774>

[3004] B.-Y. Yang and J.-M. Chen, Building secure tame-like multivariate public-key cryptosystems: The new TTS, In *ACISP 2005*, volume 3574 of *Lecture Notes in Computer Science*, 518–531. Springer, 2005. <763, 764, 770, 774>

[3005] B.-Y. Yang, J.-M. Chen, and Y.-H. Chen, TTS: High-speed signatures on a low-cost smart card, In *Proceedings of the Sixth International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 3156 of *Lecture Notes in Computer Science*, 371–385. Springer, 2004. <763, 774>

[3006] J. Yang and Z. Dai, Linear complexity of periodically repeated random sequences, *Acta Math. Sinica (New Ser.)* 11 (1995) 1–7. <324, 330>

[3007] J. Yang, S. X. Luo, and K. Q. Feng, Gauss sum of index 4. II. Non-cyclic case, *Acta Math. Sin. (Engl. Ser.)* 22 (2006) 833–844. <144, 155>

[3008] J. Yang and L. Xia, Complete solving of explicit evaluation of Gauss sums in the index 2 case, *Sci. China Math.* 53 (2010) 2525–2542. <144, 155>

[3009] R. Yang, Newton polygons of L-functions of polynomials of the form $x^d + \lambda x$, *Finite Fields Appl.* 9 (2003) 59–88. <477, 480>

[3010] S. M. Yang and L. L. Qi, On improved asymptotic bounds for codes from global function fields, *Des. Codes Cryptogr.* 53 (2009) 33–43. <703>

[3011] T. Yanik, E. Savas, and C. Koc, Incomplete reduction in modular arithmetic, *Computers and Digital Techniques, IEE Proceedings* - 149 (2002) 46 –52. <343, 356>

[3012] M. Yannakakis, Computing the minimum fill-in is NP-complete, *SIAM J. Algebraic Discrete Methods* 2 (1981) 77–79. <525, 527>

[3013] A. C. C. Yao, On the evaluation of powers, *SIAM J. Comput.* 5 (1976) 100–103. <349, 356>

[3014] C. K. Yap, *Fundamental Problems of Algorithmic Algebra*, Oxford University Press, New York, 2000. <352, 356>

[3015] Y. Ye, A hyper-Kloosterman sum identity, *Sci. China, Ser. A* 41 (1998) 1158–1162. <149, 155>

[3016] C. S. Yeh, I. S. Reed, and T. K. Troung, Systolic multipliers for finite fields $GF(2^m)$, *IEEE Trans. Comput.* 33 (1984) 357–360. <806, 814>

[3017] B. Young and D. Panario, Low complexity normal bases in $\mathbb{F}_{2^n}$, *Finite Fields Appl.* 10 (2004) 53–64. <36, 46, 113, 122>

[3018] H. P. Young, Affine triple systems and matroid designs, *Math. Z.* 132 (1973) 343–359. <602, 610>

[3019] A. M. Youssef and G. Gong, Hyper-bent functions, In *Advances in Cryptology—EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Comput. Sci.*, 406–419, Springer, Berlin, 2001. <257, 265>

[3020] J. Yu, Transcendence and Drinfel'd modules, *Invent. Math.* 83 (1986) 507–517. <538>

[3021] J. Yu, On periods and quasi-periods of Drinfel'd modules, *Compositio Math.* 74 (1990) 235–245. <538>

[3022] J.-D. Yu, Variation of the unit root along the Dwork family of Calabi-Yau varieties, *Math. Ann.* 343 (2009) 53–78. <472, 480>

[3023] J. Yuan, C. Carlet, and C. Ding, The weight distribution of a class of linear codes from perfect nonlinear functions, *IEEE Trans. Inform. Theory* 52 (2006) 712–717. <264, 265>

[3024] J. Yuan and C. Ding, Four classes of permutation polynomials of $\mathbb{F}_{2^m}$, *Finite Fields Appl.* 13 (2007) 869–876. <219, 222>

[3025] J. Yuan, C. Ding, H. Wang, and J. Pieprzyk, Permutation polynomials of the form $(x^p - x + \delta)^s + L(x)$, *Finite Fields Appl.* 14 (2008) 482–493. <219, 222>

[3026] P. Yuan, More explicit classes of permutation polynomials of $\mathbb{F}_{3^{3m}}$, *Finite Fields Appl.* 16 (2010) 88–95. <219, 222>

[3027] P. Yuan and X. Zeng, A note on linear permutation polynomials, *Finite Fields Appl.* 17 (2011) 488–491. <209, 222>

[3028] J. L. Yucas, Irreducible polynomials over finite fields with prescribed trace/prescribed constant term, *Finite Fields Appl.* 12 (2006) 211–221. <50, 55>

[3029] J. L. Yucas and G. L. Mullen, Irreducible polynomials over GF(2) with prescribed coefficients, *Discrete Math.* 274 (2004) 265–279. <51, 52, 55, 75>

[3030] D. Y. Y. Yun, Fast algorithm for rational function integration, In B. Gilchrist, editor, *Information Processing 77—Proceedings of the IFIP Congress 77*, 493–498, North-Holland, Amsterdam, 1977. <373, 375>

[3031] H. Zassenhaus, On Hensel factorization I, *J. Number Theory* 1 (1969) 291–311. <378, 386>

[3032] H. Zassenhaus, Polynomial time factoring of integral polynomials, *ACM SIGSAM Bull.* 15 (1981) 6–7. <380, 386>

[3033] G. Zeng, Y. Yang, W. Han, and S. Fan, Reducible polynomial over $\mathbb{F}_2$ constructed by trinomial σ-lfsr, In *Information Security and Cryptology*, volume 5487 of *Lecture Notes in Comput. Sci.*, 192–200, Springer, Berlin, 2009. <65, 66>

[3034] L. Zeng, L. Lan, Y. Y. Tai, S. Song, S. Lin, and K. Abdel-Ghaffar, Constructions of nonbinary quasi-cyclic LDPC codes: a finite field approach, *IEEE Trans. Communications* 56 (2008) 545–554. <709, 710>

[3035] X. Zeng, X. Zhu, and L. Hu, Two new permutation polynomials with the form $(x^{2^k} + x + \delta)^s + x$ over $\mathbb{F}_{2^n}$, *Appl. Algebra Engrg. Comm. Comput.* 21 (2010) 145–150. <219, 222>

[3036] Z. Zha, G. M. Kyureghyan, and X. Wang, Perfect nonlinear binomials and their semifields, *Finite Fields Appl.* 15 (2009) 125–133. <274>

[3037] Z. Zha and X. Wang, New families of perfect nonlinear polynomial functions, *J. Algebra* 322 (2009) 3912–3918. <274>

[3038] L. Zhang, Q. Huang, S. Lin, K. Abdel-Ghaffar, and I. Blake, Quasi-cyclic LDPC codes: an algebraic construction, rank analysis, and codes on Latin squares,

IEEE Trans. Communications 58 (2010) 3126–3139. <709, 710>

[3039] Q. Zhang, Polynomial functions and permutation polynomials over some finite commutative rings, *J. Number Theory* 105 (2004) 192–202. <222, 225>

[3040] Z. Zhao and X. Cao, A note on the reducibility of binary affine polynomials, *Des. Codes Cryptogr.* 57 (2010) 83–90. <65, 66>

[3041] G. Zhou and H. Michalik, Comments on 'A new architecture for a parallel finite field multiplier with low complexity based on composite field', *IEEE Trans. Comput.* 59 (2010) 1007–1008. <804, 805, 814>

[3042] K. Zhou, A remark on linear permutation polynomials, *Finite Fields Appl.* 14 (2008) 532–536. <209, 223>

[3043] G. Zhu and D. Wan, An asmptotic formula for counting subset sums over subgroups of finite fields, *Finite Fields Appl.* 18 (2012) 192–209. <207>

[3044] H. J. Zhu, p-adic variation of L functions of one variable exponential sums. I, *Amer. J. Math.* 125 (2003) 669–690. <477, 480>

[3045] H. J. Zhu, Asymptotic variation of L functions of one-variable exponential sums, *J. Reine Angew. Math.* 572 (2004) 219–233. <477, 480>

[3046] H. J. Zhu, L-functions of exponential sums over one-dimensional affinoids: Newton over Hodge, *Int. Math. Res. Not.* (2004) 1529–1550. <475, 477, 480>

[3047] N. Zierler, Linear recurring sequences, *J. Soc. Indust. Appl. Math.* 7 (1959) 31–48. <305, 310>

[3048] N. Zierler, Primitive trinomials whose degree is a Mersenne exponent, *Information and Control* 15 (1969) 67–69. <91, 93>

[3049] N. Zierler and W. H. Mills, Products of linear recurring sequences, *J. Algebra* 27 (1973) 147–157. <306, 310>

[3050] M. Zieve, Bivariate factorizations via Galois theory, with application to exceptional polynomials, *J. Algebra* 210 (1998) 670–689. <232, 233>

[3051] M. E. Zieve, On a theorem of Carlitz, arXiv:0810.2834, 2008. <231, 233>

[3052] M. E. Zieve, Some families of permutation polynomials over finite fields, *Int. J. Number Theory* 4 (2008) 851–857. <216, 223>

[3053] M. E. Zieve, On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$, *Proc. Amer. Math. Soc.* 137 (2009) 2209–2216. <214, 216, 223>

[3054] M. E. Zieve, Classes of permutation polynomials based on cyclotomy and an additive analogue, In *Additive Number Theory*, 355–361, Springer, 2010. <214, 217, 223>

[3055] P. Zimmermann, Avoiding adjustments in modular computations, 2012, preprint available at `http:www.loria.fr/~zimmerma/papers/norm.pdf`. <347, 356>

[3056] T. Zink, Degeneration of Shimura surfaces and a problem in coding theory, In *Fundamentals of Computation Theory*, volume 199 of *Lecture Notes in Comput. Sci.*, 503–511, Springer, Berlin, 1985. <456>

[3057] R. Zippel, Probabilistic algorithms for sparse polynomials, In *EUROSAM '79: Proceedings of the International Symposium on Symbolic and Algebraic Computation*, number 72 in Lecture Notes in Comput. Sci., 216–226. Springer-Verlag, 1979. <384, 386>

[3058] R. Zippel, Newton's iteration and the sparse Hensel algorithm (Extended Abstract), In *SYMSAC '81: Proceedings of the fourth ACM Symposium on Symbolic and Algebraic Computation*, 68–72, ACM, New York, 1981. <384, 386>

[3059] Z. Zlatev, *Computational Methods for General Sparse Matrices*, volume 65 of *Math-*

ematics and its Applications, Kluwer Academic Publishers Group, Dordrecht, 1991. <525, 527>

[3060] K. Zsigmondy, Über die Anzahl derjenigen ganzen ganzzahligen Functionen $n$ten Grades von x, welche in Bezug auf einen gegebenen Primzahlmodul eine vorgeschriebene Anzahl von Wurzeln besitzen., *Sitzungsber. Wien Abt II* 103 (1894) 135–144. <357, 361, 367>

[3061] D. Zywina, Explicit class field theory for global function fields, preprint, 2011. <530, 538>

Index

AB function, 248
Abelian subvariety, 795
Abelian variety, 795
  absolutely simple, 795
  discrete logarithm problem, 799
  has $\mathbb{F}_q$ point, 418
  isogenous, 795
  Newton polygon, 797
  ordinary, 797
  simple, 795
  supersingular, 797
  zeta function, 796
adder, 607
addition chain, 780
additive white Gaussian noise channel, 651, 704, 706
AES (Advanced Encryption Standard), 750
affine plane, 546, 556
  classical, 556
  Desarguesian, 549, 556
affine space, 568
agent-based model, 821
agreeable decomposition, 127
algebraic curve
  $X_0(n)$, 291
  $Y_0(n)$, 291
  modular, 291
  normalization, 283
algebraic dynamical system, 330
algebraic entropy, 331
algebraic set
  absolutely irreducible, 283
  component, 283
  definition field, 283
  variety, 283
algebraic-geometry code, 695
algorithm
  baby steps–giant steps, 389
  Berlekamp-Massey, 307
  compressed dot product, 515
  discrete logarithm, 390
  elliptic curve addition, 419
  Gaussian elimination, 524
  generic matrix multiplication, 516
  Greasing, 514
  Hales and Hallgren, 829
  index calculus, 390, 789
  Lanczos system solving, 524
  Las-Vegas, 520
  Monte-Carlo, 520
  Niederreiter, 307
  nullspace vector, 527
  packed matrix multiplication, 515
  PLE decomposition, 519
  Pollard rho, 390
  REDQ, 514
  REDQ Compression, 515
  REDQ Correction, 515
  reduced row echelon, 519
  row echelon, 519
  Strassen-Winograd, 516
  triangular matrix inversion, 518
  triangular matrix multiplication, 518
  triangular system, 517
  upper-lower triangular, 518
  Wiedemann, 522
almost irreducible trinomial, 346
almost perfect nonlinear (APN), 220, 232, 248
analytic combinatorics, 358
anomalous elliptic curve, 433
APN function, 232
approximately symmetric informationally complete positive operator-valued measure (ASIC-POVM), 826
approximation theorem, 402
arc, 563
  k-, 575
    complete, 575
    secant, 576
    tangent, 576
  maximal, 563
  trivial, 563
arithmetic
  normal basis, 808
  optimal normal basis, 810
  polynomial basis, 803
Artin's conjecture, 68
association scheme, 258, 599
  cyclotomic, 599
  Hamming, 599
asymptotic bounds, 664
asymptotic Gilbert-Varshamov bound, 702
asymptotic normalized rate, 664

ate pairing, 782
Aut(E), 420
autocorrelation, 166, 232, 829
autocorrelation function, 308
automorphic collineation, 568
automorphism, 557
automorphism group, 557
  of a BIBD, 582, 584
  of elliptic curve, 420, 422, 428

Baer subplane, 561
  partition, 562
    classical, 562
    perfect, 562
balanced incomplete block design
  automorphism group, 582, 584
  blocksize, 581
  complete, 581
  cyclic, 584
  decomposable, 581
  derived, 581
  difference family, 584
  G-orbit, 584
  G-stabilizer, 584
  generated by a difference family, 584
  index, 581
  isomorphic, 582
  m-multiple, 581
  nested, 586
  nested row-column, 587
  nontrivial, 581
  order, 581
  quasi-symmetric, 581
  replication number, 581
  simple, 581
  starter blocks, 582
  symmetric, *see* symmetric design
Barrett reduction, 344
bases
  almost self-dual, 98
  almost weakly self-dual, 102
  almost weakly self-dual polynomial, 102
  characterization, 20
  complementary, 96
  discriminant, 20
  dual, 21, 96
  mutually unbiased, 825
  normal, 20, 96, 808
  number of, 20
  optimal normal, 809
  polynomial, 20, 97, 803
  primitive normal, 21
  self-dual, 21, 96, 98
  trace-orthogonal, 96
  weakly self-dual, 98
  weakly self-dual polynomial, 99
  weakly self-dual polynomial over $\mathbb{F}_2$, 99
bent function, 148, 232, 595
  Maiorana-McFarland, 596
Berlekamp algorithm, 760
Berlekamp-Massey algorithm, 307
Bernoulli-Carlitz elements, 534
Bertini theorem, 379
BIBD, *see* balanced incomplete block design
big-field, 760
binary
  complement, 307
  erasure channel, 651, 707
  field
    quadratic equation, 356
  symmetric channel, 651, 705, 706
binomial, 66, 341
binomial coefficients
  congruences, 136
bipartite graph, 719
biquadratic reciprocity law, 167
birational permutation, 759
bit-packing, 513, 514
bit-slicing, 514
black box, 383, 384
Blahut's theorem, 321
block cipher, 246, 733
block weight, 700
blocking set, 551, 565
  t-fold, 554
  small linear, 565
Boolean function, 235, 246, 830
  affine, 238
  algebraic degree, 237
  algebraic immunity, 240
  algebraic normal form, 235
  annihilator, 240
  balanced, 238
  bent, 238, 256
    $\mathcal{PS}^+$ and $\mathcal{PS}^-$ classes of, 260
    $\mathcal{PS}_{ap}$ class of, 261
    class $\mathcal{H}$ of, 262
    degree of, 260, 261
    dual of, 261, 262
    equivalent, 258
    from regular spreads, 260
    Maiorana-McFarland, 261

monomial, 261
Niho, 261, 262
of Dillon type, 263
of partial spread type, 260
quadratic, 256, 259, 261
correlation immune, 240
derivative, 239
EA-equivalent, 239
EA-invariant, 239
formally self-dual, 256
Hamming distance, 238
Hamming weight, 238
hyper bent, 257, 260
inverse Walsh transform, 237
Kerdock code, 244
maximum nonlinear, 258
nonlinearity, 238
Parseval's relation, 237
plateaued, 246
propagation criterion, 241
quadratic, 238
Reed-Muller code, 244
resilient, 240
self-dual bent, 256
semi-bent, 246
sign function, 236
strict avalanche criterion, 241
trace representation, 236
Walsh support, 236
Walsh transform, 236
Boolean network model, 819
bound, 661–665
asymptotic, 664
asymptotic Gilbert-Varshamov, 702
Drinfeld–Vlăduţ, 455
Elias, 664
Griesmer, 663
Hamming, 663
Johnson
first, 590
second, 590
linear programming, 664
MRRW, 665
Niederreiter-Özbudak, 703
Plotkin, 663
Schönheim, 589
Singleton, 663, 695
sphere covering bound, 662
sphere packing, 663
TVZ, 702
Varshamov-Gilbert, 662
Weil, 253
Brewer sums, 136, 141
Buchstab function, 363

Cameron-Liebler line class, 565
canalyzing function, 822
nested, 822
parametrization of nested, 823
Carmichael number, 128
Cartesian group, 266
Cauchy matrix, 526
Cayley graph, 149, 185, 640
CDMA, 310
channel capacity, 652
character, 297
Hecke, 140
lifted, 139
multiplicative, 134
order, 134
power residue, 137, 146
quadratic, 134, 832
restriction, 136
trivial, 134
character table of a group, 300
characteristic function, 303
characteristic polynomial, 304
of sequence, 317
characteristic sequence, 306, 307
Chebychev polynomial, 152
check digit system, 165
chromatic number, 636
circle, 559
geometry, 589
method, 490
circulant matrix, 105
class
group, 146
number, 137
of a function field, 451
polynomial, 777
Clifford's theorem, 405
code, 651–693
$\mathbb{Z}_4$, 690
Gray image, 690
Lee distance, 691
Lee weight, 691
residue, 690
torsion, 690
type, 691
algebraic-geometry, 695
alternant, 675

asymptotically good, 677
BCH, 200, 251, 669
  designed distance, 669
  narrow sense, 669
  primitive, 669
concatenated, 661, 711
constant-dimension, 838
constituent, 711
convolutional, 712
CSS, 828
cyclic, 251, 309, 666–680
  defining set, 669
  generator matrix, 667
  generator polynomial, 666
  parity check matrix, 667
  with two zeros, 253
decoding, 728
density evolution, 710
direct sum, 661
distance distribution, 655
distance invariant, 656
doubly even, 682
duadic, 673
  splitting, 673
dual, 653
encoding, 656
Euclidean geometry, 679
even, 682
even-like, 672
external distance, 656
finite geometry, 678
formally self-dual, 682
fountain, 721
four fundamental parameters, 656
function-field, 699
Gallager, 704
  bit-flipping decoding algorithm, 705
  encoding, 708
  irregular, 704
  message passing decoding algorithm for a BEC, 707
  message passing sum-product decoding algorithm, 706
  pseudocodeword, 709
  regular, 704
generalized Reed-Muller (GRM), 677
generalized RS (GRS), 671
generator matrix, 653
Golay binary, 674, 682
Golay ternary, 674, 682
Goppa, 675
graph, 719
graph construction, 719
graph decoding, 719
Hamming, 657
Hermitian, 696
information set, 671
Justesen, 680
Kerdock, 200, 692
Kloosterman, 174
linear, 251, 652–656
low density parity check (LDPC), 704
  Bit-Flipping Decoding Algorithm, 705
  computation tree, 709
  encoding, 708
  error floor, 710
  Message Passing Decoding Algorithm for a BEC, 707
  Message Passing Sum-Product Decoding Algorithm, 706
  pseudocodeword, 709
  trapping sets, 710
LT, 721
  decoding, 722
  encoding, 722
maximum distance separable (MDS), 663
MDS, 578
Melas, 253
minimum distance, 651
minimum distance decoding, 656
modifying, 660
nonlinear, 651
NXL, 697
octacode, 692
odd-like, 672
optical orthogonal, 834
  optimal, 834
parallel-concatenated, 712
parity check matrix, 653
perfect, 663
polar, 726
polynomial, 680
Preparata, 692
product, 661
projective geometry, 679
quadratic residue (QR), 673
quantum error-correcting, 827
quantum Goppa, 828
quantum MDS, 828
quantum Reed-Solomon, 828

rank distance, 836
raptor, 724
precode, 724
precode only, 725
rate, 651
Reed-Muller, 200, 252, 658, 833
Reed-Solomon, 670, 695, 726
self-dual, 653, 682
self-orthogonal, 653
serially-concatenated, 712
simplex, 658
space-time, 837
stabilizer, 827
subfield, 659
Tanner graph of, 705, 719, 722
tornado, 719, 721
trace, 659
turbo, 704, 710
universal rateless, 722
XNL, 698
coding theory, 137, 146, 148
coefficient
i-th, 69
first, 50, 69
last, 50, 69
cogredient, 505
collineation, 557, 568
automorphic, 568
group, 557
complete cyclotomic generator theorem, 126
complete decomposition theorem, 127
complete generator, 126
complete mapping, 165
complete normal basis theorem, 123
complete universal generator, 131
completely basic extension, 124
completely free element, 123
completely normal element, 122
complex multiplication, 446, 777
complexity
linear, 309
computation tree, 709
computational Diffie–Hellman problem, 432, 449
concatenated code, 711
conductor, 428
conference matrix, 600
normalized, 600
skew-symmetric, 600
symmetric, 600
conic, 571
conjecture
Artin's, 68
Barker sequence, 595
circulant Hadamard, 595
Lander, 594
Ryser, 594
conjugates, 18
connection polynomial, 304
conorm (of a divisor), 407
constituent code, 711
convex-dense factorization, 382
convolution of polynomials, 298
convolutional code, 712
coordinate frame, 569
coordinate vector
of a hyperplane, 567
of a point, 566
coordinates
dual, 96
primal, 96
correlation, 569
aperiodic, 315, 831, 832
Hamming, 316, 835
mean-square, 317
measure of order k, 328
partial-period, 317
periodic, 310, 832
Costas array, 599
Golomb construction, 599
Lempel construction, 599
Welch construction, 599
cover
branch points, 285
branched, 232
elliptic curve isogeny, 232, 291
exceptional, 232, 285
pr-exceptional, 293
properties, 285
ramified point, 285
covering
t-(v, k, λ), 589
covering array, 601
degree, 601
index, 601
number, 601
optimal, 601
order, 601
strength of, 601
covering radius, 170
of Reed-Muller code, 258
critical orbit, 172

critical path, 803
cryptanalysis
  differential, 246
  linear, 246
cryptographic pairing, 779
cryptography
  pairing-based, 737
  post-quantum, 739
  public-key, 734
  symmetric-key, 732
cryptosystem
  FSR, 309
  hyperelliptic curve discrete logarithm, 788
  multivariate public key, 754
  pairings based, 801
  symmetric, 246
  tame transformation method (TTM), 773
CSS Code, 828
cubic reciprocity law, 167
cubic twist, 424
curve
  algebraic curve, 414
  Artin-Schreier, 200
  elliptic, 140
  Hermitian, 563
  hyperelliptic, 143
  maximal, 232
  Newton polygon, 478
  non-singular curve, 415
  ordinary, 479
  projective curve, 415
  supersingular, 479
cyclic code, 151, 309
cyclic digital net, 616
cyclic projectivity, 574
cyclotomic
  coset, 165, 668
  decomposition, 126
  module, 126
    exceptional, 129
    non-exceptional, 129
    regular, 128
  number, 114, 141, 594
  reduction theorem, 126
cyclotomy, 594

Davenport pair, 232
  over $\mathbb{F}_q$, 293
  over a number field, 293
de Bruijn sequence, 309
de Jonquières map, 759
decimated sequence, 306
decimation, 306
decisional Diffie–Hellman problem, 432
decoder
  maximum a posteriori, 651
  maximum likelihood, 651
  minimum distance, 652
decoding, 683–690
  BCH code, 683
  Berlekamp-Massey, 684
  error evaluator polynomial, 685
  error locator polynomial, 683
  extended Euclidean, 685
  Gallager bit-flipping, 705
  Gallager message passing sum-product, 706
  generalized minimum distance, 687
  key equation, 685
  list, 689
  majority logic, 687
  message passing for a BEC, 707
  Peterson-Gorenstein-Zierler, 683
  standard array, 656, 657
  syndrome, 683
  Welch-Berlekamp, 686
decomposition
  agreeable, 127
  cyclotomic, 126
Dedekind eta function, 152
Dedekind's different theorem, 409
degree
  of a field element, 93
  of an isogeny, 421
degree zero divisor class group, 443
degree zero divisor class number, 443
Deligne's theorem, 465, 469
denominator elimination, 781, 782
dense polynomial representation, 376, 482
density evolution, 710
density of primes, 486
dependency graph, 816
derivation, 412
Desarguesian, 547
design, 259, 681
  t-(v, k, λ), 589
  Assmus-Mattson theorem, 681
  group divisible, 588
  linked symmetric, 200
  order, 602

pairwise balanced, 587
symmetric, 591
determinant, 501
Hankel, 307
Moore, 501
diagonal equations, 137
Dickman function, 362
Dickson polynomial, 150, 228, 286
see polynomial, 275
Dickson polynomial vector, 281
Dickson system, 281
difference families
multiplier, 585
radical, 585
relative, 588
difference field, 231
difference set, 146, 253, 258–260, 312, 590
Abelian, 590
character sum, 597
cyclic, 590
cyclotomy, 594
development of, 591
equivalent, 258, 592
Gordon-Mills-Welch, 593
Hadamard, 592
isomorphic, 592
multiplier, 597
Paley, 592
partial, 258
planar, 592
relative, 258
Singer, 232, 312, 592
skew symmetric, 595
different (of a field extension), 409
different exponent, 409
differential
module, 412
of a function field, 412
divisor of a differential, 413
uniformity, 248
Diffie-Hellman triple, 177
digital
(t, m, s)-net, 612
(t, m, s)-net over R, 612
(t, s)-sequence, 618
(t, s)-sequence over R, 618
$(\mathbf{T}, s)$-sequence, 618
$(\mathbf{T}, s)$-sequence over R, 618
method, 612, 617
multistep method, 310
signature, 776
strict (t, m, s)-net, 612
strict (t, m, s)-net over R, 612
strict (t, s)-sequence, 618
strict (t, s)-sequence over R, 618
strict $(\mathbf{T}, s)$-sequence, 618
strict $(\mathbf{T}, s)$-sequence over R, 618
dimension
translation plane, 557
Dirichlet character, 488
discrepancy, 168, 329
discrete Fourier transform, 178, 301, 321, 828
discrete logarithm, 386
discrete logarithm cryptosystem, 137, 735
discrete memoryless channel, 650
discrete model, 815
discriminant, 25, 416
distinct degree factorization
multivariate, 380
distortion map, 781
distribution
capacity achieving, 720
degree, 719
heavy tail/Poisson, 721
soliton, 723
tornado, 721
division polynomial, 425
divisor, 780
balanced, 444
Cantor's algorithm, 445
defined over L, 443
finitely effective, 444
Mumford representation, 444
NUCOMP, 445
reduced, 444
semi-reduced, 444
divisor (of a function field), 402
canonical class, 404
canonical divisor, 404, 413
class group $\mathrm{Cl}^0(F)$, 451
degree of a divisor, 402
dimension of a divisor, $\ell(A)$, 404
divisor class $[D]$, 403
divisor class group $\mathrm{Cl}(F)$, 403
divisor group $\mathrm{Div}(F)$, 402
divisor of a differential, 413
divisor of poles $(x)_\infty$, 403
equivalent divisors, 403
positive divisor, 402
prime divisor, 402
principal divisor, 403

principal divisor $\mathrm{div}(x)$, 403
zero divisor $(x)_0$, 403
divisor group of elliptic curve, 423
DO polynomial, 264, 272
DSA (digital signature algorithm), 736
dual basis, 108
dual basis multiplier, 99
dual isogeny, 421, 422
Frobenius map, 429
dual space chain, 619
duality theory, 619
duplication formula, 419

ECDHP, 432
ECDLP, 432
ECDSA, 776
ECIES, 775
Eisenstein sum, 136
elation
projective plane, 557
elliptic curve, 140, 416
GL_2-type, 291
addition algorithm, 419
anomalous, 433
ate pairing, 782
automorphism, 420
automorphism group, 422, 428
CM-type, 291
complex multiplication, 291, 777
Diffie–Hellman problem, 432
digital signature algorithm, 776
discrete logarithm problem, 432
division polynomial, 425
divisor group, 423
dual isogeny, 421
duplication formula, 419
ECDHP, 432
ECDLP, 432
ECDSA, 776
ECIES, 775
Edwards curve, non-binary, 434
endomorphism, 420
endomorphism ring, 422, 428
eta pairing, 781
explicit formulas, 436
formal group, 429
Frobenius map, 421
group law, 418
hash function, 786
Hasse Weil estimate, 431
Hasse-Weil estimate, 423
Hessian curve, 434
integrated encryption scheme, 775
isogeny, 232, 420
isogeny of degree 2, 421
isogeny theorem, 424, 426
isomorphic, 417, 418, 783
kernel of multiplication-by-m, 420, 425
mass formula, 431
Montgomery curve, 434
Montgomery ladder, 436
multiplication-by-m map, 420
nonsingular projective genus one, 416
number of points, 423, 425, 431
optimal pairing, 782
ordinary, 429
over $\mathbb{F}_2$, 418
pairing-friendly, 784
Picard group, 423
point at infinity, 416
point counting, 778
points defined over a field, 416
short Weierstrass curve, non-binary, 433
short Weierstrass curve, ordinary binary, 433
supersingular, 429, 776, 781
Tate module, 425
Tate pairing, 427, 781
torsion subgroup, 420, 425
transformation of coordinates, 417
twist, 424
twisted ate pairing, 782
twisted Edwards curve, non-binary, 434
Weil pairing, 426, 781
zeta function, 431
elliptic period, 116
embedding degree, 432, 779, 784, 785
encryption, 775
$\mathrm{End}(E)$, 420
endomorphism, 446
of elliptic curve, 420
endomorphism ring, 446
of elliptic curve, 422, 428
entropy function, 664, 701
equation
Artin-Schreier, 171
diagonal, 169, 200
hyperelliptic, 171
Kloosterman, 173
superelliptic, 171
Equidistribution

Kloosterman angles, 151
Salié angles, 151
Erdös-Turan inequality, 168
error evaluator polynomial, 685
error floor, 710
error locator polynomial, 683
error-rate exponent, 652
eta pairing, 781
Euclidean algorithm, 806
Euclidean geometry, 679
exceptional cover, 232
MacCluer's theorem, 285
Serre's OIT theorem, 292
exceptional cyclotomic module, 129
exceptional tower, 289
arithmetic monodromy, 289
cryptographic subtower, 290
Dickson subtower, 290
Redei subtower, 290
subtower, 290
exceptionality set
number field, 286
over $\mathbb{F}_q$, 286
excess of a matrix, 100
exponential
Carlitz, 530
Drinfeld, 530
extended Euclidean algorithm, 351, 685
binary method, 352
plus-minus method, 352
extension
algebraic, 16
completely basic, 124
finite, 16
regular, 128
simple, 16
extension (of function fields), 405
Artin–Schreier extension, 411
constant field extension, 411
Kummer extension, 410
external distance, 656

factor of a symmetric matrix, 499
factorization
Berlekamp's algorithm, 373
Cantor and Zassenhaus' algorithm, 373
convex-dense, 382
distinct degree
multivariate, 380
irreducible
bivariate, 232, 377
multivariate, 379
separable, 375
sparse, 380
squarefree
multivariate, 376
univariate polynomials, 373
Faure sequence, 619
Feistel structure, 748
fewnomial, 66
fiber product, 285
absolute components, 288
complementary components, 288
in $\mathcal{T}_{Z,\mathbb{F}_q}$, 289
normalized, 287
set theoretic, 287
field
cardinality, 12
cyclotomic, 530
definition, 11
difference, 231
existence and uniqueness, 14
extension
separable, 287
number, 837
prime, 12
skew, 11
splitting, 14
subfield criterion, 14
field-like structures
difference field, 231
division semiring, 26
nearfield, 26
neofield, 26
prequasifield, 25
presemifield, 26
quasifield, 26
semifield, 26
figure of merit, 614
finite field
arithmetic
addition, 347
exponentiation, 349
inversion, 351
modular reduction, 344
multiplication, 347
square root, 353, 355
squaring, 349
embedding degree, 432
fixed point, 816
flock quadratic cone, 565
form

algebraic normal, 833
modular, 537
quadratic, 195
quadratic equivalent, 195
trace, 198
formal group, 429
four fundamental parameters, 656
four Russians method, 513
Fourier
coefficients, 174
matrix, 300
transform, 297
of a function, 299
frequency square, 544
orthogonal, 544
Frobenius
automorphism, 18
eigenvalues, 150
endomorphism, 446
(acting on the Tate module), 452
map, 262, 421
dual of, 429
is purely inseparable, 421
isogeny factors through, 422
normal form, 521
FSR cryptosystem, 309
function
(n, m)-, 246
L-, 467, 534
p-ary
s-plateaued, 264
complete class of, 256
degree of, 255, 257
EA-equivalent, 256
Walsh transform of, 255
p-ary bent, 256
complete class of, 257
Coulter-Matthews, 257
degree of, 257, 259, 264
dual of, 256, 257, 259, 263
EA-equivalent, 257
equivalent, 257, 259
Maiorana-McFarland, 257, 259
non weakly regular, 257, 264
of Dillon type, 263
primary constructions, 260
propagation criterion, 258
quadratic, 256–259, 262
recursive construction, 260
regular, 256, 257, 259, 263
secondary constructions, 260
Walsh transform of, 257, 262–264
weakly regular, 256–259, 262–264
absolute trace, 246
almost bent, 248
almost perfect nonlinear, 232, 248
balanced, 246
bent, 232, 247, 595
Buchstab, 363
CCZ-equivalent, 250
component, 246
crooked, 252
Dickman, 362
Dobbertin, 254
EA-equivalent, 250
Euler's Φ, 523
Euler's ϕ , 15
exponential, 530
Gold, 252
inverse, 249
Möbius, 13
perfect nonlinear, 247
planar, 247, 271
polynomial Euler's Φ, 22
Rédei, 276
Welch, 254
function field, 399, 828
constant field, 399
elliptic function field, 400, 413
Fermat function field, 454
Giulietti–Korchmáros function field, 455
Hermitian, 454, 695
hyperelliptic function field, 400, 413
maximal function field, 454
rational function field, 399, 401
function-field code, 699
functional equation, 463, 465, 471
fundamental theorem of projective geometry, 569
fundamental unit, 443

Galois
Évariste, 12
field, 12
group, 18
ring, 27
theory, 18
Galois's Sur la théorie des nombres, 5
Gauss multiplication formula for gamma functions, 140
Gauss periods, 113, 135

cubic, 144
duodecic, 145
of type (n, k), 115
quartic, 145
sextic, 144
Gauss sum, 303
absolute value, 134
cubic, 144
equidistribution, 134, 144
estimates, 135
generalized quadratic, 153
Hecke, 154
in multi-quadratic field, 144
lifted, 139
of first kind, 166
of second kind, 166
prime ideal factorization, 146
primitive, 154
pure, 139
quadratic, 144
quadratic over $\mathbb{Z}/k\mathbb{Z}$, 153
quartic, 145
quintic, 143
reciprocity, 153
reduction formula, 154
uniform distribution, 134
with character over $\mathbb{F}_q$, 134
Gauss's Disquisitiones Arithmeticae, 3
Gauss's Disquisitiones Generales de Congruentiis, 4
Gaussian coefficients, 493
generalized bent function, *see* p-ary bent function
generalized cyclotomic polynomial, 125
canonical decomposition of, 126
generalized dual coordinates, 100
generalized quadrangle, 565
generalized Riemann hypothesis, 488
generating matrices, 612, 618
generator
cyclotomic, 166
inversive, 174
linear congruential, 168
generator matrix, 653
genus
of a function field, 404
of a plane curve, 405
one curve, 416
has $\mathbb{F}_q$ point, 418
geometric Frobenius, 467
geometric Frobenius correspondence, 464
geometry
affine, 834
projective, 834
GFSR method, 310
Gold exponents, 252
Goldbach problem, 489
Gowers norm, 830
Gröbner basis, 80
Gröbner fan, 821
graph, 634
adjacency matrix, 634
adjacent vertices, 634
bipartite, 635, 719
Cayley, 185
complete, 634
complete bipartite, 635
connected, 635
cycle, 635
degree, 634
diameter of, 185, 635
distance, 635
edge set, 634
eigenvalue, 634
loop, 634
path, 635
Ramanujan, 633
regular, 634
simple, 634
spectrum, 634
strongly regular, 581, 608
Tanner, 705, 719, 722
vertex set, 634
Gray map, 690
greatest common divisor (gcd), 15, 364
Gross-Koblitz formula
for Gauss sums, 147
for Jacobi sums, 148
Grothendieck trace formula, 468
Grothendieck's formula
L-function, 468
zeta function, 464
Grothendieck-Ogg-Shafarevich formula, 471
group
Abelian, 11
doubly transitive, 285
general linear, 492, 502
law (on elliptic curve), 418
multiplicative is cyclic, 14
orthogonal, 509
primitive, 285
projective general linear, 503

projective orthogonal, 510
projective proper orthogonal, 232, 510
projective special linear, 503
projective special unitary, 507
projective symplectic, 232, 506
projective unitary, 507
proper orthogonal, 510
regular automorphism, 591
special linear, 492, 502
special unitary, 507
symplectic, 505
unitary, 507

Hadamard design, 581
Hadamard matrix, 143, 164, 595
Hall triple system (HTS), 602
Hammersley net, 611, 613
Hamming
distance, 578, 651
space, 613
weight, 651
Handshaking Lemma, 634
Hankel
determinant, 307
matrix, 526
hash function, 786
Hasse-Davenport
product formula for Gauss sums, 140, 149
theorem on lifted Gauss sums, 139
theorem on lifted Jacobi sums, 139
Hasse-Weil
bound, 452
estimate, 423, 431, 447
theorem, 452
HCDHP, 449
HCDLP, 448
Hecke
L-function, 154
characters, 140
Hensel lifting (sparse), 381
Hermite/Dickson criterion, 227, 232
Hermitian
code, 696
curve, 562, 571
function field, 695
matrix, 507
surface, 571
variety, 571
Hessenberg form, 521
HFE system, 760
hidden shift problem, 830
hidden subgroup problem, 830
higher-order linearization equation (HOLE), 767
Hilbert theorem, 379
$\mathrm{Hom}(E_1, E_2)$, 420
homogeneous coordinates, 555
Hurwitz genus formula, 409
hyper-Kloosterman sum, 149
hyperbolic fibration, 565
agrees on a line, 565
regular, 565
hypercube, 545
orthogonal, 545
hyperelliptic curve, 143, 440
baby step, 446
balanced divisor, 444
Cantor's algorithm, 445
complex multiplication, 446
degree zero divisor class group, 443
degree zero divisor class number, 443
Diffie–Hellman problem, 449
discrete logarithm problem, 448
distance, 445
divisor defined over L, 443
endomorphism, 446
endomorphism ring, 232, 446
finite points, 441
finitely effective divisor, 444
Frobenius endomorphism, 446
fundamental unit, 443
giant step, 446
Hasse-Weil interval, 447
HCDHP, 449
HCDLP, 448
IDLP, 449
imaginary, 441
index-calculus, 448, 449
inert, 441
infinite places, 441
infrastructure, 445
discrete logarithm problem, 449
Jacobian, 443
Miller's algorithm, 448
modified Tate-Lichtenbaum pairing, 448, 449
Mumford representation, 444
NUCOMP, 445
points, 441
points at infinity, 441
ramified, 441

real, 441
reduced divisor, 444
regulator, 443
semi-reduced divisor, 444
split, 441
supersingular, 447, 449
Tate-Lichtenbaum pairing, 447
unusual, 441
zeta function, 447
hyperelliptic curve point counting, 793
hyperelliptic equation, 440
hyperelliptic involution, 441
hyperelliptic Koblitz curve, 792
hypergeometric character sums, 140, 141
hypergraph, 639
hyperoval, 262, 563, 576
hyperplane at infinity, 568
hyperplane coordinates, 567
hyperplane net, 616
hypersurface
affine, 187
affine smooth, 188
affine toric, 190
Artin-Schreier, 191
Kummer, 193
projective, 189

ideal, 666
principal, 666
IDLP, 449
Ihara's bound, 454
Ihara's quantity $A(q)$, 455
impulse response sequence, 305
independence number, 636
independent set, 635
index calculus algorithm, 363, 789
infinity
line, 556
point, 556
infrastructure, 445
baby step, 446
discrete logarithm problem, 449
distance, 445
giant step, 446
initial values, 304
inseparability degree, 421
inseparable isogeny, 421
integer (Weil), 156
integer factorization, 44
integral
basis, 408
closure, 407
domain, 11
equation, 407
interleaver, 715
intrinsic rank, 761
invariant
σ-, 105
inversive plane, 559, 580, 589
circle, 580
classical, 580
egglike, 580
Miquelian, 559, 580
involution, 506
IP problem, 757
irreducibility test
Ben-Or's algorithm, 370
deterministic algorithms, 371
multivariate, 381
Rabin's algorithm, 368
randomized algorithms, 369
Shoup's algorithm, 371
univariate polynomials, 368
irreducible factorization
bivariate, 377
multivariate, 379
isogenous, 420
isogeny, 420
defined over K, 420
degree of, 421
Drinfeld, 530
dual, 422
factors through Frobenius, 422
inseparable, 421
is a homomorphism, 422
is constant or surjective, 421
is unramified, 422
of degree 2, 421
product of, 422
separable, 421
sum of, 422
theorem, 424, 426
zero, 421
isomorphism, 557
of elliptic curves, 417, 418, 783
of polynomials, 757
isotopism, 267
iterative decoding, 705–707

Jacobi logarithms, 25
Jacobi sum, 136, 166
congruences, 141

cubic, 142
duodecic, 143
equidistribution, 138
lifted, 139
multiple, 137
octic, 143
prime ideal factorization, 147
pure, 139
quadratic, 143
quartic, 142
quintic, 143
reduction formula, 138
sextic, 142
uniform distribution, 138
Jacobian, 443
Jacobian (of a curve), 232, 451
Jacobsthal sum, 141
j-invariant, 416, 777
equal iff isomorphic, 417
joint linear complexity, 319
k-error, 320
nth, 319
profile, 319

k-cap, 579
complete, 579
Karatsuba algorithm, 804
Karatsuba multiplication, 348
Kasami exponent, 251
Kerdock code, 265
kernel, 557
kernel of multiplication-by-m, 420, 425
key equation, 685
Kloosterman
angle, 150
code, 174
equation, 173
Kloosterman sum, 148, 173, 253, 261, 263
congruences, 148, 151
degree, 149
equidistribution, 151
estimates, 150, 153
lifted, 150
multiple, 149
over $\mathbb{Z}/k\mathbb{Z}$, 154
power moments, 151
reduction formula, 154
symmetric powers, 152
zeros, 148, 263
Koblitz curve
hyperelliptic, 792
Kolmogorov complexity, 327
Krawtchouk polynomials, 655
Kronecker
product, 544
construction, 616
substitution, 513
Krylov matrix, 521
Kummer's theorem, 408, 450

L-function, 467
L-polynomial (of a function field), 452
functional equation, 452
lacunary polynomial, 383
Lagrange Interpolation Formula, 24, 542
lambda phage, 819
largest prime survives
lps pair, 71
definition, 71
latin square, 542, 612
infinite, 543
isomorphic, 546
mateless, 543
mutually orthoognal, 543
orthogonal, 542
reduced, 542
lattice profile, 328
lattice test, 328
Laumon's product formula, 471
Laurent polynomial
non-degenerate, 159
law of quadratic reciprocity, 167
Lefschetz fixed point theorem, 464
Legendre
sequence, 176
symbol, 354, 829
symbol for polynomials, 355
LFSR sequence, 304
lifted character, 139
lifted Gauss sum, 139
lifted Jacobi sum, 139
lifted Kloosterman sums, 150
limit cycle, 816
linear
complexity, 176, 309, 318
$\mathbb{F}_q$-, 320
k-error, 319
n-th, 318
profile, 318
feedback shift register, 318, 805
recurrence relation, 304
recurring sequence, 304, 317

span, 309
translator, 218
linearity
of a function, 302
conjecture, 565
logical model, 819
loop number, 824

MacWilliams
identities, 654
transform, 655
mass formula, 431
matrix
alternate, 505
circulant, 496
circulant Hadamard, 595
companion, 495
generator, 653, 667
Hadamard, 164, 595
Hankel, 500
Hasse Witt, 479
involutory, 494
Mastrovito, 807
nilpotent, 494
orthogonal, 497, 510
orthogonal circulant, 498
parity check, 653, 667
proper orthogonal, 510
skew-symmetric, 499
symmetric, 499
systematic, 654
Toeplitz, 500
Vandermonde, 669
matrix field, 495
matrix representation, 495
symmetric, 496
matrix-product construction, 616
maximal partial spread, 565
maximal period sequence, 308
MDS code, 578
measure
R-valued, 535
correlation, 176
well distribution, 176
merit factor, 316
Mersenne prime, 44
message passing decoding, 705–707
Miller's algorithm, 448
Miller–Rabin test, 339
minihyper, 565
minimal polynomial, 305
joint, 319
of sequence, 318
minimal sampling algorithm, 821
minimal sets algorithms, 821
minimum block weight, 700
minimum distance, 578, 613
Minkowski sum, 381
Mobius
equivalence, 283
plane, 589
transformations, 283
modal quantum computing, 830
model for a finite field
algorithmic, 395
explicit, 394
standard, 395
model selection, 821
model space, 821
modified Tate-Lichtenbaum pairing, 448, 449
modular polynomial, 778
module
Carlitz, 530
character, 126
class, 533
cyclotomic, 126
Drinfeld, 530
Hayes, 530
Tate-Drinfeld, 531
Tate-Shafarevich, 533
monodromy group
arithmetic, 284
geometric, 284
monodromy precision
Davenport pairs, 293
exceptional polynomial, 285
general exceptional covers, 285
pr-exceptional covers, 293
monomial
APN, 253
Montgomery
reduction, 345
representation, 344
Morita's p-adic gamma function, 147
morphism
cover, 284
Drinfeld, 530
flat, 290
most significant bit map, 315
multigraph, 634
multinomial coefficients, 146

multiplication-by-m map, 420
multiplicative energy, 180
multiplier, 585, 597
multiply nested BIBD, 586
multisequence, 319
mutually unbiased bases, 825
  approximately, 825

N-polynomial, 103
nebentypus, 153
nest, 558
  plane, 559
  replaceable, 559
nested canalyzing function, 822
nested design
  multiply, 586
net
  (t, m, s)-, 611
  cyclic digital, 616
  digital (t, m, s)-, 612
  digital strict (t, m, s)-, 612
  Hammersley, 611, 613
  hyperplane, 616
  strict (t, m, s)-, 611
Netto triple system, 583
newform, 152
Newton
  polygon of Abelian variety, 797
  polyhedron, 159
  polytope, 190, 380
Niederreiter algorithm, 307
Niederreiter sequence, 619
Niederreiter-Özbudak bound, 703
Niederreiter-Xing sequence, 620
NIST, 777
non-exceptional cyclotomic module, 129
nonlinearity, 246
  of a function, 302
norm
  definition of, 19
  properties, 19
norm-compatible sequence, 123
normal
  k-, 54
normal basis
  complexity, 35, 39, 111
  dual, 118
  elliptic period, 115–117
  Gauss period, 38, 119–121
  multiplication table, 111
  optimal, 111, 119
  dual, 119
  self-dual, 37, 39, 117–119
    complexity, 117
  theorem, 104
normal element, 103
  completely, 122
  number, 106
  number of self-dual, 109
normal poynomial, 103
normal rational curve, 575
NP-complete, 755
NP-hardness, 383
NRT space, 613
NRT weight, 613
NXL code, 697

oil and vinegar scheme, 761
oil-vinegar map, 761
one-time pad, 741
operator
  hyperdifferential, 535
optical orthogonal code (OOC), 316
optimal extension field, 346
optimal pairing, 782
orbit, 504
  length, 172
order
  q^d-, 125
  affine plane, 556
  conductor of, 428
  elements with high order, 93
  in quadratic imaginary field, 428
  maximal, 428
  modulo n, 124
  of a finite field, 12
  of an element, 15, 93
  of LFSR sequence, 304
  of linear recurrence relation, 304
  projective plane, 555
ordered orthogonal array, 611
ordinary elliptic curve, 429
orthogonal array, 622
  s levels, 622
  index of, 622
  strength t, 622
orthogonal circulant matrices, 109
orthogonal system, 223
orthomorphism, 547
Ostrowski theorem, 381
oval, 576
  complete, 576

ovoid, 579
Tits, 579

p-adic gamma function, 147
p-density, 474
p-rank, 479
packing
t-(v, k, λ), 589
pairing
cryptographic, 779
eta, 781
Miller's algorithm, 448
modified Tate-Lichtenbaum, 448, 449
Tate, 781
Tate-Lichtenbaum, 447
Weil, 781
pairing-based cryptography, 737, 801
pairing-friendly elliptic curve, 784
Paley construction, 164
parallel-concatenated code, 712
parallelism, 556
parameter estimation, 821
parity check matrix, 653
partition
Baer subplane, 562
classical, 562
perfect, 562
Pauli group, 827
pentanomial, 66, 341
Mersenne, 92
perfect hash family, 604
linear, 604
optimal, 604
perfect nonlinear (PN), 247
period
Carlitz, 530
finding, 829
Fourier expansion, 135
polynomial, 135
periodic point, 816
permanent, 501
permutation
APN, 249
polynomial, 208–232, 546, 614
permutation model, 366
perpendicular array, 603
authentication, 603
perspectivity
projective plane, 557
elation, 557
Petr/Berklekamp matrix, 368
Petri net, 820
phase space, 816
Picard–Fuchs differential operator, 430
Picard group of elliptic curve, 423
place, 400
at infinity, 401
completely splitting place, 407
degree of a place, 401
extension of a place, 406
number of rational places $N(F)$, 450
pole of x, 402
prime element at a place, 400
ramification index, 406
ramified extension, 407
rational place, 401, 450
relative degree, 406
residue class field of a place, 401
residue class map, 401
totally ramified extension, 407
unramified extension, 407
zero of x, 402
planar equivalence, 272
planar function, 222
plane
affine, 556
flag-transitive, 559
André, 558
Hall, 558
inversive, 559
nest, 559
projective, 555
PLE decomposition, 518
Poincaré duality, 465, 471
Poincaré series, 149
point at infinity, 416
point counting
hyperelliptic curve, 793
problem, 481
point set, 611
points
special, 533
polar, 571
polarity, 569
Hermitian, 571
null, 571
ordinary, 571
orthogonal, 571
pseudo-, 571
symplectic, 571
unitary, 571
pole, 571

Polya-Vinogradov-Weil bound, 175
polygon
  generic, 476
  Hodge, 474
  Newton, 473
polynomial
  Δ-regular Laurent, 190
  κ-, 266
  a-cyclotomic, 279
  a-reciprocal, 277
  k-th fibred sum, 192
  n-th order transform, 54
  o-, 261
  s-sparse, 341
  t-, 53
  t-reciprocal, 54
  t-sedimentary, 341
  3-primes theorem, 490
  absolute value of, 486
  absolutely irreducible, 188, 229
  affine, 21
  all one, 68
  binomial
    irreducible, 35
  characteristic, 215, 304
  Chebychev, 152, 286
  Chebychev conjugate, 286
  complete mapping, 218
  completely normal, 90
  completely primitive normal, 83
  composed products, 63
  composition, 55
  connection, 304
  coprime, 358
  cyclotomic, 23
  Dembowski-Ostrom, 264, 272
  Dickson, 150, 228, 286
    $(k+1)$-st kind, 280
    first kind, 275
    multivariate, 281
    reverse $(k+1)$-st kind, 280
    second kind, 275
  Dirichlet L-function, 489
  discriminant, 25, 63
  dynamical system (PDS), 816
  equivalent, 224
  even, 490
  exceptional, 210, 229, 253
  excess, 84
  existence of irreducible, 16
  factorization pattern, 361
  feedback, 321
  fully reducible, 548
  generalized cyclotomic, 125
  generalized Riemann hypothesis, 489
  Hansen - Mullen Conjecture, 87
  Hasse, 476
  height, 83
  indecomposable, 79, 229
  interpolation problem, 689
  irreducible, 13, 31, 33, 34
    number of, 360
  kappa, 225
  lacunary, 548
  lattice, 614
  linearized, 21, 230
  Mattson-Solomon, 680
  minimal, 16, 305, 343, 668
  minimal value set, 226
  modular composition, 351
  monic original, 79
  multivariate quadratic, 754
  norm, 50, 69, 85
  normal, 86, 87, 103
  number of monic irreducibles, 13
  odd, 490
  pentanomial, 31, 33, 34
  permutation, 208, 224, 258, 262, 614
  permutation in several variables, 223
  planar, 271
  prime number theorem, 486
  primitive, 15, 33, 44, 69, 82, 342
  primitive normal, 82, 83
  Rédei, 549
  reciprocal, 15, 82
  recursive constructions, 59
  ring of, 13
  rough, 363
  sedimentary, 69
  self-reciprocal, 15
  set of directions, 548
  singular locus, 189
  smooth, 188, 363
  sparse, 66
  special, 534
  splitting degree, 365
  squarefree, 357
  stable, 171
  strict sum of, 491
  strong primitive normal, 90
  syndrome, 676
  trace, 50, 69, 85

trinomial, 31, 33, 34, 44
twin primes theorem, 488
Waring theorem, 491
weight of, 66
windmill, 84
with prescribed trace and norm, 137
post-quantum cryptography, 739
power residue
character, 137
symbol, 146
pre-Cartesian group, 266
prequasifield, 266
presemifield, 266
primality test
APRCL, 340
ECPP, 340
fastECPP, 340
primality testing, 137
prime ideal factorization of p, 146
prime number
generation, 340
largest Zsigmondy, 71
random search, 339
Zsigmondy, 71
prime power conjecture, 543
primes in arithmetic progression, 487
primitive element, 14, 82
random search, 341
primitive normal basis theorem, 109, 130
primitive part, 80
principal divisor
on elliptic curve, 423
principal ideal domain (PID), 666
principle of duality, 567
problem
hidden number, 170
sparse polynomial noisy interpolation, 170
Waring, 169
product set, 180
projective 1-space
F points, 283
j-line, 291
projective completion, 556
projective geometry, 678
projective plane, 546, 555
classical, 555
Desarguesian, 549, 555
projective space, 566–580
hyperplane, 566
line, 566
plane, 566
point, 566
solid, 566
subspace, 566
projectivity, 568
cyclic, 574
propagation rule, 616
pseudocodeword, 709
pseudorandom graph, 637
pseudorandom number generator, 330
pseudorandom numbers, 310
public-key cryptography, 734
pure number of weight w, 468
purely inseparable, 421

q-clan normalized, 565
quadratic imaginary field
order in, 428
quadratic nonresidue, 673
quadratic residue, 673
quadratic space, 195
Arf invariant, 196
non-degenerate, 196
radical, 196
rank, 197
quadratic twist, 424
quadric, 571
elliptic, 573
hyperbolic, 573
parabolic, 573
surface, 571
quadrinomial, 341
quality parameter, 611, 617
quantum
computer, 754
error-correcting code, 827
finite automata, 830
function reconstruction, 829
Goppa codes, 828
MDS codes, 828
Reed-Solomon codes, 828
Singleton bound, 828
quartic twist, 424
quasifield, 266, 547, 557
quaternion algebra, 428, 429

radical, 53, 86
rainbow structure sequence, 763
Ramanujan sum, 154
ramification
tame, 409

wild, 293, 409
ramification locus (of a tower), 458
rank of a matrix, 759
rational function
composition factor definition field, 292
composition factors, 283
cyclic conjugate, 290
Davenport pair, 293
decomposable, 283
exceptional over $\mathbb{F}_q$, 284
exceptional over a number field, 284
genus 0 problem, 293
permutation over $\mathbb{F}_q$, 287
Redei, 290
separable, 287
tame, 285
rational points
number of, 481
rational place, 450
RC4 algorithm, 743
RC6 algorithm, 749
reciprocity, 569
Redei polynomial, 549
reduction
good-Drinfeld, 532
potentially good, 532
stable-Drinfeld, 532
theorem, 123
Reed-Solomon code, 695
regular cyclotomic module, 128
regular extension, 128
regulator, 443
regulus, 558
opposite, 558
reordering, 524
replicator, 54
representation
bivariate, 262
matrix, 504
multivariate, 255
trace, 255
univariate, 255
residuacity, 141
resolvable BIBD, 581
reverse engineering, 821
Riemann
hypothesis, 463, 465, 469, 471
for function fields, 452
inequality, 405
theorem, 405
Riemann-Roch
space, 695
space $\mathcal{L}(A)$, 404
theorem, 404, 413, 416
ring, 11
characteristic, 12
commutative, 11
division, 11
Room square, 606
cyclic, 606
skew, 606
standardized, 606
roots of unity, 22
primitive, 22
RSA, 734

Salié angle, 151
Salié sum
equidistribution, 151
over $\mathbb{F}_q$, 149
over $\mathbb{Z}/k\mathbb{Z}$, 155
Sato-Tate measure, 151
Schoof–Elkies–Atkin algorithm, 778
Schur's conjecture, 231, 283
SEA, 778
Segre's problems, 575
self-dual basis, 108
semifield, 266
nuclei, 269
separable
factorization, 375
isogeny, 421
sequence, 310, 831
(t, s)-, 617
$(\mathbf{T}, s)$-, 617
m-, 253, 308, 311
r-shifted Legendre, 832
autocorrelation, 310
Barker, 315, 831
characteristic, 306, 307
crosscorrelation, 310
de Bruijn, 309
decimated, 306
digital (t, s)-, 618
digital $(\mathbf{T}, s)$-, 618
digital strict (t, s)-, 618
digital strict $(\mathbf{T}, s)$-, 618
elliptic curve congruential, 327
explicit inversive congruential, 325
family
$\mathcal{A}$, 315
Sidelnikov, 314

Faure, 619
frequency hopping, 835
generalized Lucas, 215
GMW, 311
Golay, 833
Gold, 313
ideal autocorrelation, 311
impulse response, 305
inversive, 326
Kasami, 314
Kerdock, 315
Legendre, 176, 312, 326, 832
LFSR, 304
linear recurring, 304
low correlation zone (LCZ), 316
maximal period, 308
maximal-length linear, *see* m-sequence
maximum length, 831
merit factor, 832
Niederreiter, 619
Niederreiter-Xing, 620
No, 314
nonlinear congruential, 326
norm-compatible, 123
optimal autocorrelation, 311
power, 326
quadratic exponential, 325
recursive nonlinear, 325
Sidelnikov, 312, 327
Sobol', 619
strict (t, s)-, 617
strict $(\mathbf{T}, s)$-, 617
trace-compatible, 123
van der Corput, 617, 618
serially-concatenated code, 712
Serre bound, 452
Serre's explicit formulas, 453
Serret's Cours d'algèbre supérieure, 7
sextic twist, 424
Shor's algorithm, 829
simplest cubic, 137
simplex of reference, 569
Singer
cycle, 494, 574
group, 574
subgroup, 494
Singleton bound, 695
singular point, 416
singularity analysis, 359
sliding window method, 349
small-field, 760
Sobol' sequence, 619
Solovay–Strassen test, 339
space
affine, 568
decomposition, 726
Hamming, 613
NRT, 613
projective, 566
Riemann-Roch, 695
sparse
factorization, 380
polynomial representation, 380
spectrum
Walsh, 246
sphere, 662
spherical geometry, 589
spin, 55
splitting, 673
splitting locus (of a tower), 458
spread, 260, 557, 573, 838
automorphism group, 557
partial, 260
maximal, 565
regular, 260, 558
subregular, 558
square-free divisor, 86
$W(r)$, 86
radical, 86
square-free part, 125
Stöhr–Voloch theory, 455
stabilizer code, 827
stable
σ-, 105
standard array, 657
starter, 605
block, 583
orthogonal, 605
Room frame, 606
skew, 605
strong, 605
state
space, 816
vector, 304
steady state, 816
Stein generator, 525
Steiner triple system
2-homogeneous, 583
Steinitz number, 123
Stickelberger's congruence for Gauss sums, 146
stopping set, 708

straight-line program, 383, 384
  without divisions, 384
stream cipher, 732
strict
  (t, m, s)-net, 611
  (t, s)-sequence, 617
  $(\mathbf{T}, s)$-sequence, 617
strong isotopism, 267
strongly regular graph, 258
  constructed from a quasi-symmetric design, 581
subfield curve, 792
subgeometry, 574
subplane, 561
  Baer, 561
subregular
  spread, 558
  translation plane, 558
substitution-permutation network, 749
sum
  Kloosterman, 253
sum set, 180
supersingular
  elliptic curve, 429, 776, 781
    mass formula, 431
  hyperelliptic curve, 447, 449
supersingularity, 140
supersparse polynomial, 383
Swan theorem, 63
Sylvester
  displacement operator, 525
  generator, 525
symmetric design, 581
symmetric differential, 771
symmetric-key cryptography, 732
symmetry, 510
syndrome, 676, 683
syndrome polynomial, 676

tangential coordinates, 567
Tanner graph, 705, 719, 722
  stopping set, 708
Tate
  module, 425
    Weil pairing on, 427
  pairing, 427, 781
Tate-Lichtenbaum pairing, 447
tetranomial, 66
tight set, 565
Tits ovoid, 579
Toeplitz
  matrix, 526, 807
  matrix-vector product, 808
torsion subgroup, 420, 425
total degree, 466
tower (of function fields), 457
  asymptotically bad tower, 458
  asymptotically good tower, 458
  limit of a tower, 458
  recursive tower, 459
  tame tower, 459
  wild tower, 460
trace, 659
  absolute, 18
  definition of, 18
  of a normal element, 119
  of the Frobenius map, 423, 426, 431
  polynomial, 108
  properties, 19
trace-compatible sequence, 123
trajectory, 330
  length, 334
translation
  affine plane, 557
  group, 557
  invariant, 54
  line, 557
  plane, 260
  projective plane, 557
transvection
  orthogonal, 512
  symplectic, 505
  unitary, 508
transversal, 558
  regulus, 558
trapping sets, 710
triangle inequality, 400
triangular map, 758
trinomial, 66, 341
  Mersenne, 91
triple system
  Netto, *see* Netto triple system
TRSM, 518
Tsfasman–Vlăduţ–Zink theorem, 456
turbo code, 710
TVZ bound, 702
twin primes, 487
twist, 424
  number of points, 425
twisted
  ate pairing, 782
  cubic, 575

Kloosterman sums, 830

uncertainty principle, 303
uniform distribution
Kloosterman angles, 151
Salié angles, 151
unital, 562
Buekenhout
nonsingular, 563
orthogonal, 563
embedded, 562
update schedule, 816

valuation, 400
corresponding to a place, 400
ring, 400
value set, 225
van der Corput sequence, 617, 618
Vandermonde matrix, 526
variety
Drinfeld module, 537
function field, 284
geometric point, 283
ordinary, 474
vector degree, 77
vectorial function
bent, 265
planar, 264
Coulter-Matthews, 264
Dembowski-Ostrom, 264
Walsh transform of, 256, 264
Vinogradov's formula, 177

walk, 635
closed, 635
Walsh
coefficient, 255
transform, 255
Waring's formula, 275
Waring's number, 205
existence, 205
Waring's problem, 490
Wedderburn, 12
Weierstrass $\wp$-function, 144
Weierstrass equation, 416
discriminant, 416
j-invariant, 416
nonsingular, 416
singular, 416
transformation of coordinates, 417
weight
distribution, 310
NRT, 613
of an error operator, 827
of matrix, 100
Weil
bound, 170, 231, 302
conjecture, 463
descent, 776, 800
pairing, 426, 781
formulas for, 427
restriction, 776
sum, 302
WG stream cipher, 744
Whist tournament, 609
$\mathbb{Z}$-cyclic, 609
triple, 610
wiring diagram, 816

XNL code, 698

Zech logarithm, 25, 343
zero isogeny, 421
zeta function, 462, 481
of a function field, 451
of a hyperelliptic curve, 447
of elliptic curve, 431
Poincaré duality, 431
Zsigmondy prime, 71
largest, 71