Chapter 1

Diameter of some monomial digraphs.

A. Kodess

University of Rhode Island, Kingston, RI, USA `kodess@uri.edu`

F. Lazebnik

University of Delaware, Newark, DE, USA `fellaz@udel.edu`

S. Smith

University of Delaware, Newark, DE, USA `smithsj@udel.edu`

J. Sporre

University of Delaware, Newark, DE, USA `jsporre@udel.edu`

1.1 Introduction

For all terms related to digraphs and not defined below, see Bang-Jensen and Gutin [1]. In this paper, by a *directed graph* (or simply *digraph)* D we mean a pair (V, A), where $V = V(D)$ is the set of vertices and $A = A(D) \subseteq V \times V$ is the set of arcs. For an arc (u, v), the first vertex u is called its *tail* and the second vertex v is called its *head*; we also denote such an arc by $u \to v$. If (u, v) is an arc, we call v an *out-neighbor* of u, and u – an *in-neighbor* of v. The number of out-neighbors of u is called the *out-degree* of u, and the number of in-neighbors of u — the *in-degree* of u. For an integer $k \geq 2$, a *walk* W *from* x_1 *to* x_k in D is an alternating sequence $W = x_1 a_1 x_2 a_2 x_3 \ldots x_{k-1} a_{k-1} x_k$ of vertices $x_i \in V$ and arcs $a_j \in A$ such that the tail of a_i is x_i and the head of a_i is x_{i+1} for every i, $1 \leq i \leq k-1$. Whenever the labels of the arcs of a walk are not important, we use the notation $x_1 \to x_2 \to \cdots \to x_k$ for the walk, and say that we have an x_1x_k-walk. In a digraph D, a vertex y is *reachable* from a vertex x if D has a walk from x to y. In particular, a vertex is reachable from itself. A digraph D is *strongly connected* (or, just *strong*) if, for every pair x, y of distinct vertices in D, y is reachable from x and x is reachable from y. A *strong component* of a digraph D is a maximal induced subdigraph of D that is strong. If x and y are vertices of a digraph D, then the *distance from x to y* in D, denoted $\operatorname{dist}(x, y)$, is the minimum length of an xy-walk, if y is reachable from x, and otherwise $\operatorname{dist}(x, y) = \infty$. The *distance from a set X to a set Y* of vertices in D is

$$\operatorname{dist}(X, Y) = \max\{\operatorname{dist}(x, y) \colon x \in X, y \in Y\}.$$

The *diameter* of D is $\operatorname{diam}(D) = \operatorname{dist}(V, V)$.

Let p be a prime, e a positive integer, and $q = p^e$. Let $\mathbb{F}_q$ denote the finite field of q elements, and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$.

Let $\mathbb{F}_q^2$ to denote the Cartesian product $\mathbb{F}_q \times \mathbb{F}_q$, and let $f \colon \mathbb{F}_q^2 \to \mathbb{F}_q$ be an arbitrary function. We define a digraph $D = D(q; f)$ as follows: $V(D) = \mathbb{F}_q^2$, and there is an arc from a vertex $\mathbf{x} = (x_1, x_2)$ to a vertex $\mathbf{y} = (y_1, y_2)$ if and only if

$$x_2 + y_2 = f(x_1, y_1).$$

If $\mathbf{x} \to \mathbf{y}$ is an arc in D, then $\mathbf{y}$ is uniquely determined by $\mathbf{x}$ and y_1, and $\mathbf{x}$ is uniquely determined by $\mathbf{y}$ and x_1. Hence, each vertex of D has both its in-degree and out-degree equal to q.

By Lagrange's interpolation, f can be uniquely represented by a bivariate polynomial of degree at most $q - 1$ in each of the variables. If $f(x, y) = x^m y^n$, $1 \le m, n \le q - 1$, we call D a *monomial* digraph, and denote it also by $D(q; m, n)$. Digraph $D(3; 1, 2)$ is depicted in Fig. 1.1. It is clear, that $\mathbf{x} \to \mathbf{y}$ in $D(q; m, n)$ if and only if $\mathbf{y} \to \mathbf{x}$ in $D(q; n, m)$. Hence, one digraph is obtained from the other by reversing the direction of every arc. In general, these digraphs are not isomorphic, but if one of them is strong then so is the other and their diameters are equal. As this paper is concerned only with the diameter of $D(q; m, n)$, it is sufficient to assume that $1 \le m \le n \le q - 1$.

The digraphs $D(q; f)$ and $D(q; m, n)$ are directed analogues of some algebraically defined graphs, which have been studied extensively and have many applications. See Lazebnik and Woldar [18] and references therein; for some subsequent work see Viglione [24], Lazebnik and Mubayi [14], Lazebnik and Viglione [17], Lazebnik and Verstraëte [16], Lazebnik and Thomason [15], Dmytrenko, Lazebnik and Viglione [7], Dmytrenko, Lazebnik and

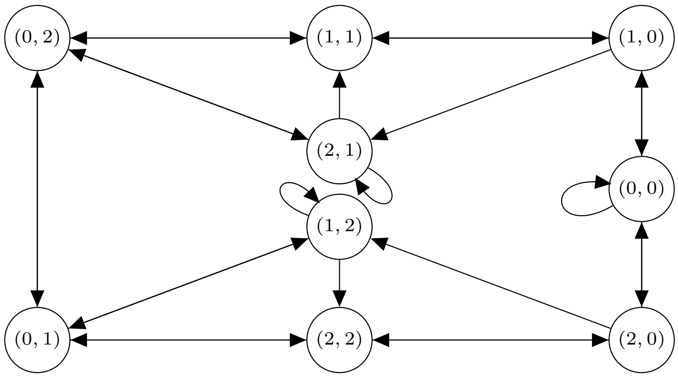

Fig. 1.1 The digraph $D(3; 1, 2)$: $x_2 + y_2 = x_1 y_1^2$.

Williford [8], Ustimenko [23], Viglione [25], Terlep and Williford [22], Kronenthal [13], Cioabă, Lazebnik and Li [3], Kodess [11], and Kodess and Lazebnik [12].

The questions of strong connectivity of digraphs $D(q; f)$ and $D(q; m, n)$ and descriptions of their components were completely answered in [12]. Determining the diameter of a component of $D(q; f)$ for an arbitrary prime power q and an arbitrary f seems to be out of reach, and most of our results below are concerned with some instances of this problem for strong monomial digraphs. The following theorems are the main results of this paper.

Theorem 1.1.1. *Let p be a prime, e, m, n be positive integers, $q = p^e$, $1 \le m \le n \le q-1$, and $D_q = D(q; m, n)$. Then the following statements hold.*

(1) If D_q is strong, then $\mathrm{diam}(D_q) \ge 3$.
(2) If D_q is strong, then
  - *for $e = 2$,* $\mathrm{diam}(D_q) \le 96\sqrt{n+1} + 1$*;*
  - *for $e \ge 3$,* $\mathrm{diam}(D_q) \le 60\sqrt{n+1} + 1$.

(3) If $\gcd(m, q-1) = 1$ *or* $\gcd(n, q-1) = 1$*, then* $\mathrm{diam}(D_q) \le 4$*. If* $\gcd(m, q-1) = \gcd(n, q-1) = 1$*, then* $\mathrm{diam}(D_q) = 3$.
(4) If p does not divide n, and $q > (n^2-n+1)^2$, then $\mathrm{diam}(D(q; 1, n)) = 3$.
(5) If D_q is strong, then:
  (a) If $q > n^2$, then $\mathrm{diam}(D_q) \le 49$.
  (b) If $q > (m-1)^4$, then $\mathrm{diam}(D_q) \le 13$.

(c) *If* $q > (n-1)^4$*, then* $\mathrm{diam}(D(q;n,n)) \le 9$.

Remark 1. The converse to either of the statements in part (3) of Theorem 1.1.1 is not true. Consider, for instance, $D(9;2,2)$ of diameter 4, or $D(29;7,12)$ of diameter 3.

Remark 2. The result of part 5a can hold for some $q \le m^2$.

For prime q, some of the results of Theorem 1.1.1 can be strengthened.

Theorem 1.1.2. *Let* p *be a prime,* $1 \le m \le n \le p-1$*, and* $D_p = D(p;m,n)$*. Then* D_p *is strong and the following statements hold.*

(1) $\mathrm{diam}(D_p) \le 2p-1$ *with equality if and only if* $m = n = p-1$.
(2) *If* $(m,n) \notin \{((p-1)/2,(p-1)/2),((p-1)/2,p-1),(p-1,p-1)\}$*, then* $\mathrm{diam}(D_p) \le 120\sqrt{m}+1$.
(3) *If* $p > (m-1)^3$*, then* $\mathrm{diam}(D_p) \le 19$.

The paper is organized as follows. In section 1.2 we present all results which are needed for our proofs of Theorems 1.1.1 and 1.1.2 in sections 1.3 and 1.4, respectively. Section 1.5 contains concluding remarks and open problems.

1.2 Preliminary results.

We begin with a general result that gives necessary and sufficient conditions for a digraph $D(q;m,n)$ to be strong.

Theorem 1.2.1. [[12], Theorem 2] $D(q;m,n)$ *is strong if and only if* $\gcd(q-1,m,n)$ *is not divisible by any* $q_d = (q-1)/(p^d-1)$ *for any positive divisor* d *of* e*,* $d < e$*. In particular,* $D(p;m,n)$ *is strong for any* m,n.

Every walk of length k in $D = D(q;m,n)$ originating at (a,b) is of the form

$$\begin{aligned}(a,b) &\to (x_1, -b + a^m x_1^n)\\ &\to (x_2, b - a^m x_1^n + x_1^m x_2^n)\\ &\to \cdots\\ &\to (x_k, x_{k-1}^m x_k^n - x_{k-2}^m x_{k-1}^n + \cdots + (-1)^{k-1} a^m x_1^n + (-1)^k b).\end{aligned}$$

Therefore, in order to prove that $\mathrm{diam}(D) \le k$, one can show that for any choice of $a,b,u,v \in \mathbb{F}_q$, there exists $(x_1,\dots,x_k) \in \mathbb{F}_q^k$ so that

$$(u,v) = (x_k, x_{k-1}^m x_k^n - \cdots + (-1)^{k-1} a^m x_1^n + (-1)^k b). \qquad (1.1)$$

In order to show that $\mathrm{diam}(D) \geq l$, one can show that there exist $a, b, u, v \in \mathbb{F}_q$ such that (1.1) has no solution in $\mathbb{F}_q^k$ for any $k < l$.

1.2.1 *Waring's Problem*

In order to obtain an upper bound on $\mathrm{diam}(D(q; m, n))$ we will use some results concerning Waring's problem over finite fields.

Waring's number $\gamma(r, q)$ over $\mathbb{F}_q$ is defined as the smallest positive integer s (should it exist) such that the equation

$$x_1^r + x_2^r + \cdots + x_s^r = a$$

has a solution $(x_1, \ldots, x_s) \in \mathbb{F}_q^s$ for any $a \in \mathbb{F}_q$. Similarly, $\delta(r, q)$ is defined as the smallest positive integer s (should it exist) such that for any $a \in \mathbb{F}_q$, there exists $(\epsilon_1, \ldots, \epsilon_s)$, each $\epsilon_i \in \{-1, 1\} \subseteq \mathbb{F}_q$, for which the equation

$$\epsilon_1 x_1^r + \epsilon_2 x_2^r + \cdots + \epsilon_s x_s^r = a$$

has a solution $(x_1, \ldots, x_s) \in \mathbb{F}_q^s$. It is easy to argue that $\delta(r, q)$ exists if and only if $\gamma(r, q)$ exists, and in this case $\delta(r, q) \leq \gamma(r, q)$.

A criterion on the existence of $\gamma(r, q)$ is the following theorem by Bhashkaran [2].

Theorem 1.2.2. [[2], Theorem G] *Waring's number $\gamma(r, q)$ exists if and only if r is not divisible by any $q_d = (q-1)/(p^d - 1)$ for any positive divisor d of e, $d < e$.*

The study of various bounds on $\gamma(r, q)$ has drawn considerable attention. We will use the following two upper bounds on Waring's number due to J. Cipra [5].

Theorem 1.2.3. [[5], Theorem 4] *If $e = 2$ and $\gamma(r, q)$ exists, then $\gamma(r, q) \leq 16\sqrt{r+1}$. Also, if $e \geq 3$ and $\gamma(r, q)$ exists, then $\gamma(r, q) \leq 10\sqrt{r+1}$.*

Corollary 1.2.1. [[5], Corollary 7] *If $\gamma(r, q)$ exists and $r < \sqrt{q}$, then $\gamma(r, q) \leq 8$.*

For the case $q = p$, the following bound will be of interest.

Theorem 1.2.4. [Cochrane, Pinner [6], Corollary 10.3] *If $|\{x^k : x \in \mathbb{F}_p^*\}| > 2$, then $\delta(k, p) \leq 20\sqrt{k}$.*

The next two statements concerning very strong bounds on Waring's number in large fields follow from the work of Weil [26], and Hua and Vandiver [10].

Theorem 1.2.5. [Small [20]] *If $q > (k-1)^4$, then $\gamma(k,q) \le 2$.*

Theorem 1.2.6. [Cipra [4], p. 4] *If $p > (k-1)^3$, then $\gamma(k,p) \le 3$.*

For a survey on Waring's number over finite fields, see Castro and Rubio (Section 7.3.4, p. 211), and Ostafe and Winterhof (Section 6.3.2.3, p. 175) in Mullen and Panario [19]. See also Cipra [4].

We will need the following technical lemma.

Lemma 1.2.1. *Let $\delta = \delta(r,q)$ exist, and $k \ge 2\delta$. Then for every $a \in \mathbb{F}_q$ the equations*

$$x_1^r - x_2^r + x_3^r - \cdots + (-1)^{k+1}x_k^r = a \tag{1.2}$$

has a solution $(x_1, \ldots, x_k) \in \mathbb{F}_q^k$.

Proof. Let $a \in \mathbb{F}_q$ be arbitrary. There exist $\varepsilon_1, \ldots, \varepsilon_\delta$, each $\varepsilon_i \in \{-1,1\} \subseteq \mathbb{F}_q$, such that the equation $\sum_{i=1}^{\delta} \varepsilon_i y_i^r = a$ has a solution $(y_1, \ldots, y_\delta) \in \mathbb{F}_q^\delta$. As $k \ge 2\delta$, the alternating sequence $1, -1, 1, \ldots, (-1)^k$ with k terms contains the sequence $\varepsilon_1, \ldots, \varepsilon_\delta$ as a subsequence. Let the indices of this subsequence be $j_1, j_2, \ldots, j_\delta$. For each l, $1 \le l \le k$, let $x_l = 0$ if $l \ne j_i$ for any i, and $x_l = y_i$ for $l = j_i$. Then $(x_1, \ldots, x_k)$ is a solution of (1.2). □

1.2.2 *The Hasse-Weil bound*

In the next section we will use the Hasse-Weil bound, which provides a bound on the number of $\mathbb{F}_q$-points on a plane non-singular absolutely irreducible projective curve over a finite field $\mathbb{F}_q$. If the number of points on the curve C of genus g over the finite field $\mathbb{F}_q$ is $|C(\mathbb{F}_q)|$, then

$$||C(\mathbb{F}_q)| - q - 1| \le 2g\sqrt{q}. \tag{1.3}$$

It is also known that for a non-singular curve defined by a homogeneous polynomial of degree k, $g = (k-1)(k-2)/2$. Discussion of all related notions and a proof of this result can be found in Hirschfield, Korchmáros, Torres [9] (Theorem 9.18, p. 343) or in Szőnyi [21] (p. 197).

1.3 Proof of Theorem 1.1.1

(1). As there is a loop at $(0,0)$, and there are arcs between $(0,0)$ and $(x,0)$ in either direction, for every $x \in \mathbb{F}_q^*$, the number of vertices in D_q which are at distance at most 2 from $(0,0)$ is at most $1 + (q-1) + (q-1)^2 < q^2$. Thus, there are vertices in D_q which are at distance at least 3 from $(0,0)$, and so $\mathrm{diam}(D_q) \ge 3$.

(2). As D_q is strong, by Theorem 1.2.1, for any positive divisor d of e, $d < e$, $q_d \not| \gcd(p^e - 1, m, n)$. As, clearly, $q_d \,|\, (p^e - 1)$, then either $q_d \not| m$ or $q_d \not| n$. This implies by Theorem 1.2.2 that either $\gamma(m, q)$ or $\gamma(n, q)$ exists.

Let (a, b) and (u, v) be arbitrary vertices of D_q. By (1.1), there exists a walk of length at most k from (a, b) to (u, v) if the equation

$$v = x_{k-1}^m u^n - x_{k-2}^m x_{k-1}^n + \cdots + (-1)^{k-1} a^m x_1^n + (-1)^k b \tag{1.4}$$

has a solution $(x_1, \ldots, x_k) \in \mathbb{F}_q^k$.

Assume first that $\gamma_m = \gamma(m, q)$ exists. Taking $k = 6\gamma_m + 1$, and $x_i = 0$ for $i \equiv 1 \mod 3$, and $x_i = 1$ for $i \equiv 0 \mod 3$, we have that (1.4) is equivalent to

$$-x_{k-2}^m + x_{k-5}^m - \cdots + (-1)^k x_5^m + (-1)^{k-1} x_2^m = v - (-1)^k b - u^n.$$

As the number of terms on the left is $(k-1)/3 = 2\gamma_m$, this equation has a solution in $\mathbb{F}_q^{2\gamma_m}$ by Lemma 1.2.1. Hence, (1.4) has a solution in $\mathbb{F}_q^k$.

If $\gamma_n = \gamma(n, q)$ exists, then the argument is similar: take $k = 6\gamma_n + 1$, $x_i = 0$ for $i \equiv 0 \mod 3$, and $x_i = 1$ for $i \equiv 1 \mod 3$.

The result now follows from the bounds on $\gamma(r, q)$ in Theorem 1.2.3.

Remark 3. As $m \le n$, if $\gamma(m, q)$ exists, the upper bounds in Theorem 1.1.1, part **(2)**, can be improved by replacing n by m. Also, if a better upper bound on $\delta(m, q)$ than $\gamma(m, q)$ (respectively, on $\delta(n, q)$ than $\gamma(n, q)$) is known, the upper bounds in Theorem 1.1.1, **(2)**, can be further improved: use $k = 6\delta(m, q) + 1$ (respectively, $k = 6\delta(n, q) + 1$) in the proof. Similar comments apply to other parts of Theorem 1.1.1 as well as Theorem 1.1.2.

(3). Recall the basic fact $\gcd(r, q-1) = 1 \Leftrightarrow \{x^r : x \in \mathbb{F}_q\} = \mathbb{F}_q$.

Let $k = 4$. If $\gcd(m, q-1) = 1$, a solution to (1.1) of the form $(0, x_2, 1, u)$ is seen to exist for any choice of $a, b, u, v \in \mathbb{F}_q$. If $\gcd(n, q-1) = 1$, there exists a solution of the form $(1, x_2, 0, u)$. Hence, $\mathrm{diam}(D_q) \le 4$.

Let $k = 3$, and $\gcd(m, q-1) = \gcd(n, q-1) = 1$. If $a = 0$, then a solution to (1.1) of the form $(x_1, 1, u)$ exists. If $a \ne 0$, a solution of the form $(x_1, 0, u)$ exists. Hence, D_q is strong and $\mathrm{diam}(D_q) \le 3$. Using the lower bound from part **(1)**, we conclude that $\mathrm{diam}(D_q) = 3$.

(4). As was shown in part 3, for any n, $\mathrm{diam}(D(q; 1, n)) \le 4$. If, additionally, $\gcd(n, q-1) = 1$, then $\mathrm{diam}(D(q; 1, n)) = 3$. It turns out that if p does not divide n, then only for finitely many q is the diameter of $D(q; 1, n)$ actually 4.

For $k = 3$, (1.1) is equivalent to

$$(u, v) = (x_3, x_2 x_3^n - x_1 x_2^n + a x_1^n - b), \tag{1.5}$$

which has solution $(x_1, x_2, x_3) = (0, u^{-n}(b + v), u)$, provided $u \neq 0$.

Suppose now that $u = 0$. Aside from the trivial case $a = 0$, the question of the existence of a solution to (1.5) shall be resolved if we prove that the equation

$$ax^n - xy^n + c = 0 \tag{1.6}$$

has a solution for any $a, c \in \mathbb{F}_q^*$ (for $c = 0$, (1.6) has solutions). The projective curve corresponding to this equation is the zero locus of the homogeneous polynomial

$$F(X, Y, Z) = aX^n Z - XY^n + cZ^{n+1}.$$

It is easy to see that, provided p does not divide n,

$$F = F_X = F_Y = F_Z = 0 \quad \Leftrightarrow \quad X = Y = Z = 0,$$

and thus the curve has no singularities and is absolutely irreducible.

Counting the two points $[1 : 0 : 0]$ and $[0 : 1 : 0]$ on the line at infinity $Z = 0$, we obtain from (1.3), the inequality $N \geq q - 1 - 2g\sqrt{q}$, where $N = N(c)$ is the number of solutions of (1.6). As $g = n(n-1)/2$, solving the inequality $q - 1 - n(n-1)\sqrt{q} > 0$ for q, we obtain a lower bound on q for which $N \geq 1$.

(5a). The result follows from Corollary 1.2.1 by an argument similar to that of the proof of part **(2)**.

(5b). For $k = 13$, (1.1) is equivalent to

$$(u, v) = (x_{13}, -b + a^m x_1^n - x_1^m x_2^n + x_2^m x_3^n - \cdots - x_{11}^m x_{12}^n + x_{12}^m x_{13}^n).$$

If $q > (n-1)^4$, set $x_1 = x_4 = x_7 = x_{10} = 1$, $x_3 = x_6 = x_9 = x_{12} = 0$. Then $v - a^m + b = x_{11}^n - x_8^n + x_5^n - x_2^n$, which has a solution $(x_2, x_5, x_8, x_{11}) \in \mathbb{F}_q^4$ by Theorem 1.2.5 and Lemma 1.2.1.

(5c). For $k = 9$, (1.1) is equivalent to

$$(u, v) = (x_9, -b + a^n x_1^n - x_1^n x_2^n + x_2^n x_3^n - \cdots - x_7^m x_8^n + x_8^n x_9^n).$$

If $q > (n-1)^4$, set $x_1 = x_4 = x_5 = x_8 = 0$, $x_3 = x_7 = 1$. Then $v + b = x_2^n + x_6^n$, which has a solution $(x_2, x_6) \in \mathbb{F}_q^2$ by Theorem 1.2.5.

1.4 Proofs of Theorem 1.1.2

Lemma 1.4.1. *Let $D = D(q; m, n)$. Then, for any $\lambda \in \mathbb{F}_q^*$, the function $\phi : V(D) \to V(D)$ given by $\phi((a, b)) = (\lambda a, \lambda^{m+n} b)$ is a digraph automorphism of D.*

The proof of the lemma is straightforward. It amounts to showing that ϕ is a bijection and that it preserves adjacency: $\mathbf{x} \to \mathbf{y}$ if and only if $\phi(\mathbf{x}) \to \phi(\mathbf{y})$. We omit the details. Due to Lemma 1.4.1, any walk in D initiated at a vertex (a, b) corresponds to a walk initiated at a vertex $(0, b)$ if $a = 0$, or at a vertex $(1, b')$, where $b' = a^{-m-n}b$, if $a \neq 0$. This implies that if we wish to show that $\mathrm{diam}(D_p) \leq 2p-1$, it is sufficient to show that the distance from any vertex $(0, b)$ to any other vertex is at most $2p - 1$, and that the distance from any vertex $(1, b)$ to any other vertex is at most $2p - 1$.

First we note that by Theorem 1.2.1, $D_p = D(p; m, n)$ is strong for any choice of m, n.

For $a \in \mathbb{F}_p$, let integer $\overline{a}$, $0 \leq \overline{a} \leq p - 1$, be the representative of the residue class a.

It is easy to check that $\mathrm{diam}(D(2; 1, 1)) = 3$. Therefore, for the remainder of the proof, we may assume that p is odd.

(1). In order to show that $\mathrm{diam}(D_p) \leq 2p-1$, we use (1.1) with $k = 2p-1$, and prove that for any two vertices (a, b) and (u, v) of D_p there is always a solution $(x_1, \ldots, x_{2p-1}) \in \mathbb{F}_q^{2p-1}$ of

$$(u, v) = (x_{2p-1}, -b + a^m x_1^n - x_1^m x_2^n + x_2^m x_3^n - \cdots - x_{2p-3}^m x_{2p-2}^n + x_{2p-2}^m x_{2p-1}^n),$$

or, equivalently, a solution $\mathbf{x} = (x_1, \ldots, x_{2p-2}) \in \mathbb{F}_q^{2p-2}$ of

$$a^m x_1^n - x_1^m x_2^n + x_2^m x_3^n - \cdots - x_{2p-3}^m x_{2p-2}^n + x_{2p-2}^m u^n = b + v. \tag{1.7}$$

As the upper bound $2p - 1$ on the diameter is exact and holds for all p, we need a more subtle argument compared to the ones we used before. The only way we can make it is (unfortunately) by performing a case analysis on $\overline{b+v}$ with a nested case structure. In most of the cases we just exhibit a solution $\mathbf{x}$ of (1.7) by describing its components x_i. It is always a straightforward verification that $\mathbf{x}$ satisfies (1.7), and we will suppress our comments as cases proceed.

Our first observation is that if $\overline{b+v} = 0$, then $\mathbf{x} = (0, \ldots, 0)$ is a solution to (1.7). We may assume now that $\overline{b+v} \neq 0$.

Case 1.1: $\overline{b+v} \geq \frac{p-1}{2} + 2$
We define the components of $\mathbf{x}$ as follows:

if $1 \leq i \leq 4(p - (\overline{b+v}))$, then $x_i = 0$ for $i \equiv 1, 2 \mod 4$, and $x_i = 1$ for $i \equiv 0, 3 \mod 4$;

if $4(p - (\overline{b+v})) < i \leq 2p - 2$, then $x_i = 0$.

Note that $x_i^m x_{i+1}^n = 0$ unless $i \equiv 3 \mod 4$, in which case $x_i^m x_{i+1}^n = 1$. If we group the terms in groups of four so that each group is of the form

$$-x_i^m x_{i+1}^n + x_{i+1}^m x_{i+2}^n - x_{i+2}^m x_{i+3}^n + x_{i+3}^m x_{i+4}^n,$$

where $i \equiv 1 \mod 4$, then assuming i, $i+1$, $i+2$, $i+3$, and $i+4$ are within the range of $1 \leq i < i+4 \leq 4(\overline{b+v})$, it is easily seen that one group contributes -1 to

$$a^m x_1^n - x_1^m x_2^n + x_2^m x_3^n - \cdots - x_{2p-3}^m x_{2p-2}^n + x_{2p-2}^m x_{2p-1}^n.$$

There are $\frac{4(p-(\overline{b+v}))}{4} = p-(\overline{b+v})$ such groups, and so the solution provided adds -1 exactly $p - (\overline{b+v})$ times. Hence, $\mathbf{x}$ is a solution to (1.7).

For the remainder of the proof, solutions to (1.7) will be given without justification as the justification is similar to what's been done above.

Case 1.2: $\overline{b+v} \leq \frac{p-1}{2}$
We define the components of $\mathbf{x}$ as follows:

if $1 \leq i \leq 4(\overline{b+v}) - 1$, then $x_i = 0$ for $i \equiv 0, 1 \mod 4$, and $x_i = 1$ for $i \equiv 2, 3 \mod 4$;

if $4(\overline{b+v}) - 1 < i \leq 2p - 2$, then $x_i = 0$.

Case 1.3: $\overline{b+v} = \frac{p-1}{2} + 1$

This case requires several nested subcases.

Case 1.3.1: $u = x_{2p-1} = 0$

Here, there is no need to restrict x_{2p-2} to be 0. The components of a solution $\mathbf{x}$ of (1.7) are defined as:

if $1 \leq i \leq 2p-2$, then $x_i = 0$ for $i \equiv 1, 2 \mod 4$, and $x_i = 1$ for $i \equiv 0, 3 \mod 4$.

Case 1.3.2: $a = 0$

Here, there is no need to restrict x_1 to be 0. Therefore, the components of a solution $\mathbf{x}$ of (1.7) are defined as:

if $1 \leq i \leq 2p-2$, then $x_i = 0$ for $i \equiv 0, 3 \mod 4$, and $x_i = 1$ for $i \equiv 1, 2 \mod 4$.

Case 1.3.3: $u \neq 0$ and $a \neq 0$

Because of Lemma 1.4.1, we may assume without loss of generality that $a = 1$. Let $x_{2p-2} = 1$, so that $x_{2p-2}^m u^n = u^n \neq 0$ and let $t = \overline{b + v - u^n}$. Note that $t \neq \frac{p-1}{2} + 1$.

Case 1.3.3.1: $t = 0$

The components of a solution $\mathbf{x}$ of (1.7) are defined as: $x_{2p-2} = 1$, and if $1 \leq i < 2p - 2$, then $x_i = 0$.

Case 1.3.3.2: $0 < t \leq \frac{p-1}{2}$

The components of a solution $\mathbf{x}$ of (1.7) are defined as: $x_{2p-2} = 1$, and if $1 \leq i \leq 4(t-1)+1$, then $x_i = 0$ for $i \equiv 2, 3 \mod 4$, and $x_i = 1$ for $i \equiv 0, 1 \mod 4$;

if $4(t-1)+1 < i < 2p-2$, then $x_i = 0$.

Case 1.3.3.3: $t \geq \frac{p-1}{2} + 2$

The components of a solution $\mathbf{x}$ of (1.7) are defined as: $x_{2p-2} = 1$, and if $1 \leq i \leq 4(p-t)$, then $x_i = 0$ for $i \equiv 1, 2 \mod 4$, and $x_i = 1$ for $i \equiv 0, 3 \mod 4$;

if $4(p-t) < i < 2p-2$, then $x_i = 0$.

The whole range of possible values $\overline{b + v}$ has been checked. Hence, $\mathrm{diam}(D) \leq 2p - 1$.

We now show that if $\mathrm{diam}(D) = 2p - 1$, then $m = n = p - 1$. To do so, we assume that $m \neq p - 1$ or $n \neq p - 1$ and prove the contrapositive. Specifically, we show that $\mathrm{diam}(D) \leq 2p - 2 < 2p - 1$ by again using (1.1) but with $k = 2p - 2$. We prove that for any two vertices (a, b) and (u, v) of D_p there is always a solution $(x_1, \ldots, x_{2p-2}) \in \mathbb{F}_q^{2p-2}$ of

$$(u, v) = (x_{2p-2}, b - a^m x_1^n + x_1^m x_2^n - \cdots - x_{2p-4}^m x_{2p-3}^n + x_{2p-3}^m x_{2p-2}^n),$$

or, equivalently, a solution $\mathbf{x} = (x_1, \ldots, x_{2p-3}) \in \mathbb{F}_q^{2p-3}$ of

$$-a^m x_1^n + x_1^m x_2^n - x_2^m x_3^n + \cdots - x_{2p-4}^m x_{2p-3}^n + x_{2p-3}^m u^n = -b + v. \quad (1.8)$$

We perform a case analysis on $\overline{-b + v}$.

Our first observation is that if $\overline{-b + v} = 0$, then $\mathbf{x} = (0, \ldots, 0)$ is a solution to (1.8). We may assume for the remainder of the proof that $\overline{-b + v} \neq 0$.

Case 2.1: $\overline{-b + v} \leq \frac{p-1}{2} - 1$

We define the components of $\mathbf{x}$ as follows:

if $1 \le i \le 4(\overline{-b+v})$, then $x_i = 0$ for $i \equiv 1,2 \mod 4$, and $x_i = 1$ for $i \equiv 0,3 \mod 4$;

if $4(\overline{-b+v}) < i \le 2p-3$, then $x_i = 0$.

<u>Case 2.2</u>: $\overline{-b+v} \ge \frac{p-1}{2} + 2$

We define the components of $\mathbf{x}$ as follows:

if $1 \le i \le 4(p - (\overline{-b+v})) - 1$, then $x_i = 0$ for $i \equiv 0,1 \mod 4$, and $x_i = 1$ for $i \equiv 2,3 \mod 4$;

if $4(p - (\overline{-b+v})) - 1 < i \le 2p-3$, then $x_i = 0$.

<u>Case 2.3</u>: $\overline{-b+v} = \frac{p-1}{2}$

<u>Case 2.3.1</u>: $a = 0$

We define the components of $\mathbf{x}$ as:

if $1 \le i \le 2p-3$, then $x_i = 0$ for $i \equiv 0,3 \mod 4$, and $x_i = 1$ for $i \equiv 1,2 \mod 4$.

<u>Case 2.3.2</u>: $a \ne 0$

Here, we may assume without loss of generality that $a = 1$ by Lemma (1.4.1).

<u>Case 2.3.2.1</u>: $n \ne p-1$

If $n \ne p-1$, then there exists $\beta \in \mathbb{F}_p^*$ such that $\beta^n \notin \{0,1\}$. For such a β, let $x_1 = \beta$ and consider $t = \overline{-b+v+a^m x_1^n} = \overline{-b+v+\beta^n} \notin \{\frac{p-1}{2}, \frac{p-1}{2}+1\}$.

<u>Case 2.3.2.1.1</u>: $t = 0$

We define the components of $\mathbf{x}$ as: $x_1 = \beta$ and

if $2 \le i \le 2p-3$, then $x_i = 0$.

<u>Case 2.3.2.1.2</u>: $t \le \frac{p-1}{2} - 1$

We define the components of $\mathbf{x}$ as: $x_1 = \beta$ and

if $2 \le i \le 4t$, then $x_i = 0$ for $i \equiv 1,2 \mod 4$, and $x_i = 1$ for $i \equiv 0,3 \mod 4$;

if $4t < i \le 2p-3$, then $x_i = 0$.

<u>Case 2.3.2.1.3</u>: $t \ge \frac{p-1}{2} + 2$

We define the components of $\mathbf{x}$ as: $x_1 = \beta$ and

if $2 \le i \le 4(p-t)+1$, then $x_i = 0$ for $i \equiv 2,3 \mod 4$, and $x_i = 1$ for $i \equiv 0,1 \mod 4$;

if $4(p-t)+1 < i \le 2p-3$, then $x_i = 0$.

Case 2.3.2.2: $n = p - 1$

Case 2.3.2.2.1: $u \in \mathbb{F}_p^*$

Here, we have that $u^n = 1$, so that the components of a solution $\mathbf{x}$ of (1.8) are defined as:

if $1 \le i \le 2p-3$, then $x_i = 0$ for $i \equiv 1, 2 \mod 4$, and $x_i = 1$ for $i \equiv 0, 3 \mod 4$.

Case 2.3.2.2.2: $u = 0$

Since $n = p - 1$, it must be the case that $m \ne p - 1$ so that there exists $\alpha \in \mathbb{F}_p^*$ such that $\alpha^m \notin \{0.1\}$. For such an α, let $x_2 = \alpha, x_3 = 1$ and consider $t = \overline{-b + v + x_2^m x_3^n} = \overline{-b + v + \alpha^m} \notin \{\frac{p-1}{2}, \frac{p-1}{2} + 1\}$.

Case 2.3.2.2.2.1: $t = 0$

We define the components of $\mathbf{x}$ as: $x_1 = 0, x_2 = \alpha, x_3 = 1$ and

if $4 \le i \le 2p - 3$, then $x_i = 0$.

Case 2.3.2.2.2.2: $t \le \frac{p-1}{2} - 1$

We define the components of $\mathbf{x}$ as: $x_1 = 0, x_2 = \alpha, x_3 = 1$ and

if $4 \le i \le 4t$, then $x_i = 0$ for $i \equiv 1, 2 \mod 4$, and $x_i = 1$ for $i \equiv 0, 3 \mod 4$;

if $4t < i \le 2p - 3$, then $x_i = 0$.

Case 2.3.2.2.2.3: $t \ge \frac{p-1}{2} + 2$

We define the components of $\mathbf{x}$ as: $x_1 = 0, x_2 = \alpha, x_3 = 1$ and

if $4 \le i \le 4(p - t) + 3$, then $x_i = 0$ for $i \equiv 0, 1 \mod 4$, and $x_i = 1$ for $i \equiv 2, 3 \mod 4$;

if $4(p - t) + 3 < i \le 2p - 3$, then $x_i = 0$.

Case 2.4: $\overline{-b + v} = \frac{p-1}{2} + 1$

Case 2.4.1: $u = 0$

We define the components of $\mathbf{x}$ as:

if $1 \le i \le 2p-3$, then $x_i = 0$ for $i \equiv 0, 1 \mod 4$, and $x_i = 1$ for $i \equiv 2, 3 \mod 4$.

Case 2.4.2: $u \ne 0$

Here, we may assume without loss of generality that $u = 1$ by Lemma (1.4.1).

Case 2.4.2.1: $m \ne p - 1$

If $m \ne p - 1$, then there exists $\alpha \in \mathbb{F}_p^*$ such that $\alpha^m \notin \{0, 1\}$. For such an α, let $x_{2p-3} = \alpha$ and consider $t = \overline{-b + v - x_{2p-3}^m u^n} = \overline{-b + v - \alpha^m} \notin \{\frac{p-1}{2}, \frac{p-1}{2} + 1\}$.

Case 2.4.2.1.1: $t = 0$
We define the components of $\mathbf{x}$ as: $x_{2p-3} = \alpha$ and
if $1 \le i \le 2p-4$, then $x_i = 0$.

Case 2.4.2.1.2: $t \le \frac{p-1}{2} - 1$
We define the components of $\mathbf{x}$ as: $x_{2p-3} = \alpha$ and
if $1 \le i \le 4t$, then $x_i = 0$ for $i \equiv 1, 2 \mod 4$, and $x_i = 1$ for $i \equiv 0, 3 \mod 4$;
if $4t < i \le 2p-4$, then $x_i = 0$.

Case 2.4.2.1.3: $t \ge \frac{p-1}{2} + 2$
We define the components of $\mathbf{x}$ as: $x_{2p-3} = \alpha$ and
if $1 \le i \le 4(p-t) - 1$, then $x_i = 0$ for $i \equiv 0, 1 \mod 4$, and $x_i = 1$ for $i \equiv 2, 3 \mod 4$;
if $4(p-t) - 1 < i \le 2p-4$, then $x_i = 0$.

Case 2.4.2.2: $m = p-1$

Case 2.4.2.2.1: $a \in \mathbb{F}_p^*$
Here, we have that $a^m = 1$, so that the components of a solution $\mathbf{x}$ of (1.8) are defined as:
if $1 \le i \le 2p-5$, then $x_i = 0$ for $i \equiv 2, 3 \mod 4$, and $x_i = 1$ for $i \equiv 0, 1 \mod 4$.

Case 2.4.2.2.2: $a = 0$
Since $m = p-1$, it must be the case that $n \ne p-1$ so that there exists $\beta \in \mathbb{F}_p^*$ such that $\beta^n \notin \{0.1\}$. For such a β, let $x_{2p-5} = 1, x_{2p-4} = \beta$ and consider $t = \overline{-b + v - x_{2p-5}^m x_{2p-4}^n} = \overline{-b + v - \beta^n} \notin \{\frac{p-1}{2}, \frac{p-1}{2} + 1\}$.

Case 2.4.2.2.2.1: $t = 0$
We define the components of $\mathbf{x}$ as: $x_{2p-5} = 1, x_{2p-4} = \beta, x_{2p-3} = 0$ and
if $1 \le i \le 2p-6$, then $x_i = 0$.

Case 2.4.2.2.2.2: $t \le \frac{p-1}{2} - 1$
We define the components of $\mathbf{x}$ as: $x_{2p-5} = 1, x_{2p-4} = \beta, x_{2p-3} = 0$ and
if $1 \le i \le 4t-2$, then $x_i = 0$ for $i \equiv 0, 3 \mod 4$, and $x_i = 1$ for $i \equiv 1, 2 \mod 4$;
if $4t - 2 < i \le 2p-6$, then $x_i = 0$.

<u>Case 2.4.2.2.2.3</u>: $t \geq \frac{p-1}{2} + 2$
We define the components of $\mathbf{x}$ as: $x_{2p-5} = 1, x_{2p-4} = \beta, x_{2p-3} = 0$ and

if $1 \leq i \leq 4(p-t) - 1$, then $x_i = 0$ for $i \equiv 0, 1 \mod 4$, and $x_i = 1$ for $i \equiv 2, 3 \mod 4$;

if $4(p-t) - 1 < i \leq 2p - 6$, then $x_i = 0$.

All cases have been checked, so if $m \neq p-1$ or $n \neq p-1$, then $\operatorname{diam}(D) < 2p - 1$.

We now prove that if $m = n = p - 1$, then $d := \operatorname{diam}(D(p; m, n)) = 2p - 1$. In order to do this, we explicitly describe the structure of the digraph $D(p; p-1, p-1)$, from which the diameter becomes clear. In this description, we look at sets of vertices of a given distance from the vertex $(0, 0)$, and show that some of them are at distance $2p - 1$. We recall the following important general properties of our digraphs that will be used in the proof.

- Every out-neighbor (u, v) of a vertex (a, b) of $D(q; m, n)$ is completely determined by its first component u.
- Every vertex of $D(q; m, n)$ has its out-degree and in-degree equal q.
- In $D(q; m, m)$, $\mathbf{x} \to \mathbf{y}$ if and only if $\mathbf{y} \to \mathbf{x}$

In $D(p; p-1, p-1)$, we have that $(x_1, y_1) \to (x_2, y_2)$ if and only if

$$y_1 + y_2 = x_1^{p-1} x_2^{p-1} = \begin{cases} 0 & \text{if } x_1 = 0 \text{ or } x_2 = 0, \\ 1 & \text{if } x_1 \text{ and } x_2 \text{ are non-zero.} \end{cases}$$

For notational convenience, we set

$$(*, a) = \{(x, a) : x \in \mathbb{F}_p^*\}$$

and, for $1 \leq k \leq d$, let

$$N_k = \{v \in V(D(p; m, n)) : \operatorname{dist}((0, 0), v) = k\}.$$

We assume that $N_0 = \{(0, 0)\}$. It is clear from this definition that these $d+1$ sets N_k partition the vertex set of $D(p; p-1, p-1)$; for every k, $1 \leq k \leq d-1$, every out-neighbor of a vertex from N_k belongs to $N_{k-1} \cup N_k \cup N_{k+1}$, and N_{k+1} is the set of all out-neighbors of all vertices from N_k which are not in $N_{k-1} \cup N_k$.

Thus we have $N_0 = \{(0, 0)\}$, $N_1 = (*, 0)$, $N_2 = (*, 1)$, $N_3 = \{(0, -1)\}$. If $p > 2$, $N_4 = \{(0, 1)\}$, $N_5 = (*, -1)$. As there exist two (opposite) arcs between each vertex of $(*, x)$ and each vertex $(*, -x + 1)$, these subsets of vertices induce the complete bipartite subdigraph $\overrightarrow{K}_{p-1,p-1}$ if $x \neq -x+1$, and the complete subdigraph $\overrightarrow{K}_{p-1}$ if $x = -x+1$. Note that our $\overrightarrow{K}_{p-1,p-1}$ has no loops, but $\overrightarrow{K}_{p-1}$ has a loop on every vertex. Digraph $D(5;4,4)$ is depicted in Fig. 1.2.

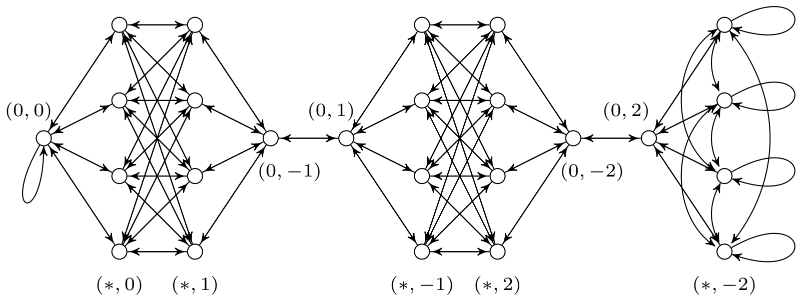

Fig. 1.2 The digraph $D(5;4,4)$: $x_2 + y_2 = x_1^4 y_1^4$.

The structure of $D(p;p-1,p-1)$ for any other prime p is similar. We can describe it as follows: for each $t \in \{0,1,\ldots,(p-1)/2\}$, let

$$N_{4\bar{t}} = \{(0,t)\}, \;\; N_{4\bar{t}+1} = (*,-t),$$

and for each $t \in \{0,1,\ldots,(p-3)/2\}$, let

$$N_{4\bar{t}+2} = (*,t+1), \; N_{4\bar{t}+3} = \{(0,-t-1)\}.$$

Note that for $0 \le \bar{t} < (p-1)/2$, $N_{4\bar{t}+1} \neq N_{4\bar{t}+2}$, and for $\bar{t} = (p-1)/2$, $N_{2p-1} = (*,(p+1)/2)$. Therefore, for $p \ge 3$, $D(p;p-1,p-1)$ contains $(p-1)/2$ induced copies of $\overrightarrow{K}_{p-1,p-1}$ with partitions $N_{4\bar{t}+1}$ and $N_{4\bar{t}+2}$, and a copy of $\overrightarrow{K}_{p-1}$ induced by N_{2p-1}. The proof is a trivial induction on $\bar{t}$. Hence, $\mathrm{diam}(D(p;p-1,p-1)) = 2p-1$. This ends the proof of Theorem 1.1.2 (1).

(2). We follow the argument of the proof of Theorem 1.1.1, part **(2)** and use Lemma 1.2.1, with $k = 6\delta(m,p)+1$. We note, additionally, that if $m \notin \{p,(p-1)/2\}$, then $\gcd(m,p-1) < (p-1)/2$, which implies $|\{x^m : x \in \mathbb{F}_p^*\}| > 2$. The result then follows from Theorem 1.2.4.

(3). We follow the argument of the proof of Theorem 1.1.1, part **(5b)** and use Lemma 1.2.1 and Theorem 1.2.6.

This ends the proof of Theorem 1.1.2.

1.5 Concluding remarks.

Many results in this paper follow the same pattern: if Waring's number $\delta(r,q)$ exists and is bounded above by δ, then one can show that $\mathrm{diam}(D(q;m,n)) \leq 6\delta+1$. Determining the exact value of $\delta(r,q)$ is an open problem, and it is likely to be very hard. Also, the upper bound $6\delta+1$ is not exact in general. Out of all partial results concerning $\delta(r,q)$, we used only those ones which helped us deal with the cases of the diameter of $D(q;m,n)$ that we considered, especially where the diameter was small. We left out applications of all asymptotic bounds on $\delta(r,q)$. Our computer work demonstrates that some upper bounds on the diameter mentioned in this paper are still far from being tight. Here we wish to mention only a few strong patterns that we observed but have not been able to prove so far. We state them as problems.

Problem 1. Let p be prime, $q=p^e$, $e\geq 2$, and suppose $D(q;m,n)$ is strong. Let r be the largest divisor of $q-1$ not divisible by any $q_d = (p^e-1)/(q^d-1)$ where d is a positive divisor of e smaller than e. Is it true that

$$\max_{1\leq m\leq n\leq q-1}\{\mathrm{diam}(D(q;m,n))\} = \mathrm{diam}(D(q;r,r))?$$

Find an upper bound on $\mathrm{diam}(D(q;r,r))$ better than the one of Theorem 1.1.1, part **(5c)**.

Problem 2. Is it true that for every prime p and $1\leq m\leq n$, $(m,n)\neq(p-1,p-1))$, $\mathrm{diam}(D(p;m,n))\leq (p+3)/2$ with the equality if and only if $(m,n)=((p-1)/2,(p-1)/2)$ or $(m,n)=((p-1)/2,p-1)$?

Problem 3. Is it true that for every prime p, $\mathrm{diam}(D(p;m,n))$ takes only one of two consecutive values which are completely determined by $\gcd((p-1,m,n)$?

1.6 Acknowledgement

The authors are thankful to the anonymous referee whose careful reading and thoughtful comments led to a number of significant improvements in the paper.

Bibliography

[1] J. Bang-Jensen, G. Gutin, Digraphs: Theory, Algorithms and Applications, Springer 2009.

[2] M. Bhaskaran, Sums of m-th powers in algebraic and abelian number fields, Arch. Math. (Basel) 17 (1966), 497-504; Correction, ibid. 22 (1972), 370-371.

[3] S.M. Cioabă, F. Lazebnik and W. Li, On the Spectrum of Wenger Graphs, J. Combin. Theory Ser. B 107: (2014), 132–139.

[4] J. Cipra, Waring's number in finite fields, Doctoral Thesis, Kansas State University, 2010.

[5] J. Cipra. Waring's number in a finite field, Integers 8 2009.

[6] T. Cochrane, C. Pinner, Sum-product estimates applied to Waring's problem mod p, Integers 8 (2008), A46.

[7] V. Dmytrenko, F. Lazebnik and R. Viglione, An Isomorphism Criterion for Monomial Graphs, J. Graph Theory 48 (2005), 322–328.

[8] V. Dmytrenko, F. Lazebnik and J. Williford, On monomial graphs of girth eight, Finite Fields Appl. 13 (2007), 828–842.

[9] J.W.P. Hirschfield, G. Korchmáros, F. Torres, Algebraic Curves over a Finite Field, Princeton Series in Applied Mathematics, 2008.

[10] L.K. Hua, H.S. Vandiver, Characters over certain types of rings with applications to the theory of equations in a finite field, Proc. Natl. Acad. Sci. U.S.A. 35 (1949), 94–99.

[11] A. Kodess, Properties of some algebraically defined digraphs, Doctoral Thesis, University of Delaware, 2014.

[12] A. Kodess, F. Lazebnik, Connectivity of some algebraically defined digraphs, Electron. J. Combin, 22(3) (2015), #P3.27, 1–11.

[13] B.G. Kronenthal, Monomial graphs and generalized quadrangles, Finite Fields Appl. 18 (2012), 674–684.

[14] F. Lazebnik, D. Mubayi, New lower bounds for Ramsey numbers of graphs and hypergraphs, Adv. Appl. Math. 8 (3/4) (2002), 544–559.

[15] F. Lazebnik, A. Thomason, Orthomorphisms and the construction of projective planes, Math. Comp. 73 (247) (2004), 1547–1557.

[16] F. Lazebnik, J. Verstraëte, On hypergraphs of girth five, Electron. J. Combin. 10 (R25) (2003), 1–15.

[17] F. Lazebnik, R. Viglione, An infinite series of regular edge- but not vertex-transitive graphs, J. Graph Theory 41 (2002), 249–258.

[18] F. Lazebnik, A.J. Woldar, General properties of some families of graphs defined by systems of equations, J. Graph Theory 38 (2) (2001), 65–86.

[19] G.L. Mullen and D. Panario, Handbook of Finite Fields, CRC Press, Taylor & Francis Group, 2013.

[20] C. Small, Sums of powers in large fields, Proc. Amer. Math. Soc. 65 (1977), p. 3535.

[21] T. Szőnyi, Some applications of algebraic curves in finite geometry and combinatorics. In Surveys in Combinatorics, Edited by R.A. Bailey, pp. 197–236, 1997 (London), vol. 241 of London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, Cambridge, 1997.

[22] T.A. Terlep, J. Williford, Graphs from generalized Kac-Moody algebras, SIAM J. Discrete Math. 26 no. 3 (2012), 1112–1120.

[23] V.A. Ustimenko, On the extremal regular directed graphs without commutative diagrams and their applications in coding theory and cryptography, *Albanian J. Math.* 1 (01/2007), 283–295.

[24] R. Viglione, Properties of some algebraically defined graphs, Doctoral Thesis, University of Delaware, 2002.

[25] R. Viglione, On Diameter of Wenger Graphs, Acta Appl. Math. 104 (2) (11/2008), 173–176.

[26] A. Weil, Number of solutions of equations in finite fields, Bull. Amer. Math. Soc. 55 (1949), 497–508.