PROOF OF A CONJECTURE ON MONOMIAL GRAPHS

XIANG-DONG HOU, STEPHEN D. LAPPANO, AND FELIX LAZEBNIK

ABSTRACT. Let e be a positive integer, p be an odd prime, $q = p^e$, and $\mathbb{F}_q$ be the finite field of q elements. Let $f, g \in \mathbb{F}_q[X, Y]$. The graph $G_q(f, g)$ is a bipartite graph with vertex partitions $P = \mathbb{F}_q^3$ and $L = \mathbb{F}_q^3$, and edges defined as follows: a vertex $(p) = (p_1, p_2, p_3) \in P$ is adjacent to a vertex $[l] = [l_1, l_2, l_3] \in L$ if and only if $p_2+l_2 = f(p_1, l_1)$ and $p_3+l_3 = g(p_1, l_1)$. If $f = XY$ and $g = XY^2$, the graph $G_q(XY, XY^2)$ contains no cycles of length less than eight and is edge-transitive. Motivated by certain questions in extremal graph theory and finite geometry, people search for examples of graphs $G_q(f, g)$ containing no cycles of length less than eight and not isomorphic to the graph $G_q(XY, XY^2)$, even without requiring them to be edge-transitive. So far, no such graphs $G_q(f, g)$ have been found. It was conjectured that if both f and g are monomials, then no such graphs exist. In this paper we prove the conjecture.

1. INTRODUCTION

All graphs considered in this paper are finite, undirected, with no loops or multiple edges. All definitions of graph-theoretic terms that we omit can be found in Bollobás [1]. The *order* of a graph is the number of its vertices. The *degree* of a vertex of a graph is the number of vertices adjacent to it. A graph is called *r-regular* if degrees of all its vertices are equal to r. A graph is called *connected* if every pair of its distinct vertices is connected by a path. The *distance* between two distinct vertices in a connected graph is the length of the shortest path connecting them. The *girth* of a graph containing cycles is the length of a shortest cycle.

Let $k \geq 2$, and $g_k(n)$ denote the greatest number of edges in a graph of order n and girth at least $2k + 1$. The function $g_k(n)$ has been studied extensively; see the surveys by Bondy [3], and by Füredi and Simonovits [6]. It is known that for $2 \leq k \neq 5$, and sufficiently large n,

$$c'_k n^{1+\frac{2}{3k-3+\epsilon}} \leq g_k(n) \leq c_k n^{1+\frac{1}{k}}, \tag{1.1}$$

where $\epsilon = 0$ if k is odd, $\epsilon = 1$ if k is even, and c'_k and c_k are positive constants depending on k only. The upper bound is due to Bondy and Simonovits [2], and the lower bound was obtained via an explicit construction by Lazebnik, Ustimenko and Woldar [10]. (For many prior related results see the references in [2, 10].) For $k = 5$, a better lower bound is known, and it is of magnitude $n^{1+1/5}$. The only known values of k for which the lower bound for $g_k(n)$ is of (maximum) magnitude $n^{1+1/k}$

2000 *Mathematics Subject Classification.* 05C35, 11T06, 11T55, 51E12.

Key words and phrases. generalized quadrangle, girth eight, monomial graph, permutation polynomial, power sum.

This work was partially supported by a grant from the Simons Foundation (#426092, Felix Lazebnik).

are $k = 2, 3$, and 5. Several graphs of such extremal magnitude were constructed using polynomials over finite fields as we describe below.

Let q be a prime power, and let $\mathbb{F}_q$ be the finite field with q elements. For each $k = 2, 3, 5$, consider a bipartite graph $\Gamma_k(q)$ with vertex partitions $P_k = \mathbb{F}_q^k$ and $L_k = \mathbb{F}_q^k$, and edges defined as follows.

For $k = 2$, a vertex $(p) = (p_1, p_2) \in P_2$ is adjacent to a vertex $[l] = [l_1, l_2] \in L_2$ if and only if

$$p_2 + l_2 = p_1 l_1.$$

For $k = 3$, a vertex $(p) = (p_1, p_2, p_3) \in P_3$ is adjacent to a vertex $[l] = [l_1, l_2, l_3] \in L_3$ if and only if the following two equalities hold:

$$p_2 + l_2 = p_1 l_1, \;\; p_3 + l_3 = p_1 l_1^2.$$

For $k = 5$, a vertex $(p) = (p_1, p_2, p_3, p_4, p_5) \in P_5$ is adjacent to a vertex $[l] = [l_1, l_2, l_3, l_4, l_5] \in L_5$ if and only if the following four equalities hold:

$$p_2 + l_2 = p_1 l_1, \;\; p_3 + l_3 = p_1 l_1^2, \;\; p_4 + l_4 = p_1 l_1^3, \;\; p_5 + l_5 = p_4 l_1 - 2p_3 l_2 + p_2 l_3.$$

It is easy to see that for $k = 2, 3$ and 5, the graph $\Gamma_k(q)$ is q-regular, and it can be shown that the girth of $\Gamma_k(q)$ is $2(k + 1)$ (for $k = 5$ we have to assume that q is odd). For the origins and properties of these constructions, and their relation to generalized polygons (which we do not define here), see Lazebnik and Ustimenko [9], [10], Lazebnik and Woldar [11], and the references therein. The graphs described above are also related to Moore graphs and cages; see Miller and Širáň [16] and Exoo and Jajcay [5].

Similar constructions of hypergraphs turned out to be useful for some extremal problems for hypergraphs; see Lazebnik and Mubayi [12] and Lazebnik and Verstraëte [13].

In what follows we concentrate on a generalization of the construction of $\Gamma_3(q)$ above. Let $f, g \in \mathbb{F}_q[X, Y]$. The graph $G = G_q(f, g)$ is a bipartite graph with vertex partitions $P = \mathbb{F}_q^3$ and $L = \mathbb{F}_q^3$, and edges defined as follows: a vertex $(p) = (p_1, p_2, p_3) \in P$ is adjacent to a vertex $[l] = [l_1, l_2, l_3] \in L$ if and only if

$$p_2 + l_2 = f(p_1, l_1) \quad \text{and} \quad p_3 + l_3 = g(p_1, l_1).$$

It is clear that $\Gamma_3(q) = G_q(XY, XY^2)$, and as we already mentioned, the girth of this graph is eight. If f and g are monomials, we refer to $G_q(f, g)$ as a *monomial graph*.

For certain questions in extremal graph theory and finite geometry, it is desirable to have examples of graphs $G_q(f, g)$ containing no cycles of length less than eight and *not* isomorphic to the graph $G_q(XY, XY^2)$. Do they exist? So far, no such graphs $G_q(f, g)$ have been found for odd q. For even q, such examples exist, in particular, among monomial graphs. This motivated Dmytrenko, Lazebnik and Williford [4], and Kronenthal [8] to study monomial graphs $G_q(f, g)$ of girth at least eight for odd q; see these papers for more details and related references.

The results from [4] and [8] are described in the next section. They suggest that for odd q, monomial graphs of girth at least eight are isomorphic to $\Gamma_3(q)$. The main conjecture of [4] and [8] is the following.

Conjecture 1.1. *Let q be an odd prime power. Then every monomial graph of girth eight is isomorphic to $\Gamma_3(q)$.*

In an attempt to prove Conjecture 1.1, two more related conjectures were proposed in [4] and [8]. In order to state them we need the following definition. A *permutation polynomial* (PP) of $\mathbb{F}_q$ is a polynomial $h \in \mathbb{F}_q[X]$ such that the function defined by $a \mapsto h(a)$ is a bijection on $\mathbb{F}_q$. For more information on permutation polynomials, we refer the reader to a recent survey [7] by Hou and the references therein. For an integer $1 \le k \le q-1$, let

$$A_k = X^k\big[(X+1)^k - X^k\big] \in \mathbb{F}_q[X] \tag{1.2}$$

and

$$B_k = \big[(X+1)^{2k} - 1\big]X^{q-1-k} - 2X^{q-1} \in \mathbb{F}_q[X]. \tag{1.3}$$

Conjecture A. *Let q be a power of an odd prime p and $1 \le k \le q-1$. Then A_k is a PP of $\mathbb{F}_q$ if and only if k is a power of p.*

Conjecture B. *Let q be a power of an odd prime p and $1 \le k \le q-1$. Then B_k is a PP of $\mathbb{F}_q$ if and only if k is a power of p.*

The logical relation between the above three conjectures is as follows. It was proved in [4] that for odd q, every monomial graph of girth at least eight is isomorphic to $G_q(XY, X^kY^{2k})$, where $1 \le k \le q-1$ is an integer not divisible by p for which both A_k and B_k are PPs of $\mathbb{F}_q$. In particular, either of Conjectures A and B implies Conjecture 1.1.

In [4] and [8], the above conjectures were shown to be true under various additional conditions. The main objective of the present paper is to confirm Conjecture 1.1. This is achieved by making progress on Conjectures A and B. Our results fall short of establishing the claims of Conjectures A and B. However, when considered together, these partial results on Conjectures A and B turn out to be sufficient for proving Conjecture 1.1.

The paper is organized as follows. In Section 2, we review the prior status of the three conjectures and highlight the contributions of the present paper. The permutation property of a polynomial $f \in \mathbb{F}_q[X]$ is encoded in the power sums $\sum_{x\in\mathbb{F}_q} f(x)^s$, $1 \le s \le q-1$. In Section 3, we compute the power sums of A_k and B_k, from which we derive necessary and sufficient conditions for A_k and B_k to be PPs of $\mathbb{F}_q$. Further results on A_k and B_k are collected in Section 4. The results gathered in Section 4 are a bit more than we need in this paper but can be useful for further work on Conjectures A and B. Sections 5 and 6 deal with Conjectures A and B, respectively. We show that each of them is true under a simple additional condition. Finally, the proof of Conjecture 1.1 is given in Section 7.

Two well known facts about binomial coefficients are frequently used in the paper without further mentioning. Lucas' theorem (see Lucas [15]) states that for a prime p and integers $0 \le m_i, n_i \le p-1$, $0 \le i \le e$,

$$\binom{m_0 + m_1p + \cdots + m_ep^e}{n_0 + n_1p + \cdots + n_ep^e} \equiv \binom{m_0}{n_0}\cdots\binom{m_e}{n_e} \pmod p.$$

Consequently, for integers $0 \le n \le m$, $\binom{m}{n} \equiv 0 \pmod p$ if and only if the sum $n + (m-n)$ has at least one carry in base p.

Throughout the paper, for $a, b \in \mathbb{Q}$ whose denominators are not divisible by p, we write $a \equiv_p b$ to mean that $a \equiv b \pmod p$. When the variables of a sum are integers whose ranges are not specified, the ranges are understood to be such that

the variables produce nonzero contributions to the sum. For example, if $s \geq 0$ is an integer, then

$$\sum_{i,j} \binom{s}{i}\binom{i}{j} f(i,j) = \sum_{i=0}^{s}\sum_{j=0}^{i} \binom{s}{i}\binom{i}{j} f(i,j),$$

where $f(i,j)$ is some expression in i and j.

2. The Conjectures: Prior Status and New Contributions

Let $q = p^e$, where e is a positive integer. The "if" portions of Conjectures A and B are rather obvious. It is also clear that if Conjectures A (or B) is true for $k = k_0$, then it is also true for all k in the p-cyclotomic coset of k_0 modulo $q-1$, i.e., for all $k \equiv p^i k_0 \pmod{q-1}$, where $i \geq 0$. It was proved in [4] that Conjecture 1.1 is true for a given q if the k's for which both A_k and B_k are PPs of $\mathbb{F}_q$ are precisely the powers of p. In particular, either of Conjectures A and B implies Conjecture 1.1.

2.1. Prior Status of Conjecture 1.1.

For an integer $e > 1$, let $\mathrm{gpf}(e)$ denote the greatest prime factor of e, and additionally, define $\mathrm{gpf}(1) = 1$.

Theorem 2.1 ([4, Theorem 3])**.** *Conjecture 1.1 is true if one of the following occurs.*

(i) $q = p^e$, *where* $p \geq 5$ *and* $\mathrm{gpf}(e) \leq 3$.
(ii) $3 \leq q \leq 10^{10}$.

The above result was recently extended by Kronenthal [8] as follows.

Theorem 2.2 ([8, Theorem 4])**.** *For each prime* r *or* $r = 1$, *there is a positive integer* $p_0(r)$ *such that Conjecture 1.1 is true for* $q = p^e$ *with* $\mathrm{gfp}(e) \leq r$ *and* $p \geq p_0(r)$. *In particular, one can choose* $p_0(5) = 7$, $p_0(7) = 11$, $p_0(11) = 13$.

Remark 2.3. [4, Theorem 3] and the proof of [4, Theorem 1] allow one to choose $p_0(3) = 5$ and $p_0(1) = 3$. However, in general, the function $p_0(r)$ given in [8] is not explicit.

2.2. Prior Status of Conjecture A.

The proof of [4, Theorem 1] implies that Conjecture A is true for $q = p$.

2.3. Prior Status of Conjecture B.

For each odd prime p, let $\alpha(p)$ be the smallest positive even integer a such that

$$\binom{a}{a/2} \equiv_p (-1)^{a/2} 2^a.$$

The proof of [8, Theorem 4] implies the following.

Theorem 2.4. *Let* p *be an odd prime. If Conjecture B is true for* $q = p^e$, *then it is also true for* $q = p^{em}$ *whenever*

$$m \leq \frac{p-1}{\lfloor (p-1)/\alpha(p) \rfloor}.$$

Unfortunately, unlike Conjecture A, Conjecture B has not been established for $q = p$.

2.4. **Contributions of the Present Paper.**

We will prove the following results.

- Conjecture A is true for $q = p^e$, where p is an odd prime and $\mathrm{gpf}(e) \le p-1$ (Theorem 5.1). This implies that in Theorem 2.2, one can take $p_0(r) = r+1$ (Remark 5.3).
- Conjecture B is true for $q = p^e$, where $e > 0$ is arbitrary and p is an odd prime satisfying $\alpha(p) > (p-1)/2$ (Theorem 6.2).
- Conjecture 1.1 is true (Theorem 7.2).

Remark 2.5. Although Conjectures A and B were originally stated for an odd characteristic, their status also appears to be unsettled for $p = 2$.

3. Power Sums of A_k and B_k

Hermite's criterion (see Lidl and Niederreiter [14, Theorem 7.4]) states that a polynomial $f \in \mathbb{F}_q[X]$ is a PP of $\mathbb{F}_q$ if and only if

(i) 0 is the only root of f in $\mathbb{F}_q$, and
(ii) $\sum_{x\in\mathbb{F}_q} f(x)^s = 0$ for all $1 \le s \le q-2$.

Let q be any prime power (even or odd). For each integer $a > 0$, let $a^* \in \{1, \dots, q-1\}$ be such that $a^* \equiv a \pmod{q-1}$; we also define $0^* = 0$. Note that for all $a \ge 0$ and $x \in \mathbb{F}_q$, $x^a = x^{a^*}$. We always assume that $1 \le k \le q-1$; additional assumptions on k, when they apply, will be included in the context.

Lemma 3.1. *For $1 \le s \le q-1$,*

$$\sum_{x\in\mathbb{F}_q} A_k(x)^s = (-1)^{s+1} \sum_{i=0}^{s} (-1)^i \binom{s}{i} \binom{(ki)^*}{(2ks)^*}. \tag{3.1}$$

Proof. We have

$$\begin{aligned}
\sum_{x\in\mathbb{F}_q} A_k(x)^s &= \sum_{x\in\mathbb{F}_q^*} x^{ks}\left[(x+1)^k - x^k\right]^s \\
&= \sum_{x\in\mathbb{F}_q^*} x^{ks} \sum_i \binom{s}{i} (x+1)^{ki} (-x^k)^{s-i} \\
&= \sum_{x\in\mathbb{F}_q^*} \sum_i (-1)^{s-i} \binom{s}{i} x^{2ks-ki} (x+1)^{(ki)^*} \\
&= \sum_{x\in\mathbb{F}_q^*} \sum_i (-1)^{s-i} \binom{s}{i} x^{2ks-ki} \sum_j \binom{(ki)^*}{j} x^{(ki)^*-j} \\
&= \sum_{i,j} (-1)^{s-i} \binom{s}{i} \binom{(ki)^*}{j} \sum_{x\in\mathbb{F}_q^*} x^{2ks-j} \\
&= (-1)^{s+1} \sum_i (-1)^i \binom{s}{i} \sum_{j\equiv 2ks \,(\mathrm{mod}\, q-1)} \binom{(ki)^*}{j}.
\end{aligned}$$

If $2ks \not\equiv 0 \pmod{q-1}$,

$$\sum_{x\in\mathbb{F}_q} A_k(x)^s = (-1)^{s+1} \sum_i (-1)^i \binom{s}{i} \binom{(ki)^*}{(2ks)^*}.$$

If $2ks \equiv 0 \pmod{q-1}$,

$$\begin{aligned}\sum_{x\in\mathbb{F}_q} A_k(x)^s &= (-1)^{s+1}\sum_i (-1)^i \binom{s}{i}\Big[\binom{(ki)^*}{0} + \binom{(ki)^*}{q-1}\Big]\\ &= (-1)^{s+1}\sum_i (-1)^i \binom{s}{i}\binom{(ki)^*}{(2ks)^*}.\end{aligned}$$

Hence (3.1) always holds. □

Lemma 3.2. (i) *If q is even,*

$$\sum_{x\in\mathbb{F}_q} B_k(x)^s = \sum_{i=0}^{s}\binom{s}{i}\binom{(2ki)*}{(ks)^*}, \qquad 1\le s\le q-1. \tag{3.2}$$

(ii) *If q is odd,*

$$\sum_{x\in\mathbb{F}_q} B_k(x)^s = -(-2)^s\sum_{i,j} 2^{-i}(-1)^j\binom{s}{i}\binom{i}{j}\binom{(2kj)*}{(ki)^*}, \qquad 1\le s\le q-1. \tag{3.3}$$

Proof of (i). If $k = q-1$,

$$B_k(x) = (x+1)^{2(q-1)} - 1 = \begin{cases}1 & \text{if } x = 1,\\ 0 & \text{if } x\in\mathbb{F}_q\setminus\{1\},\end{cases}$$

so the left side of (3.2) is 1. On the other hand, the right side of (3.2) equals

$$\sum_{i=1}^{s}\binom{s}{i} \equiv_2 1,$$

and hence (3.2) holds.

Now assume that $1 \le k < q-1$. The calculation is identical to the proof of Lemma 3.1. We have

$$\begin{aligned}\sum_{x\in\mathbb{F}_q} B_k(x)^s &= \sum_{x\in\mathbb{F}_q^*}\Big(\big[(x+1)^{2k}+1\big]x^{-k}\Big)^s\\ &= \sum_{x\in\mathbb{F}_q^*} x^{-ks}\big[(x+1)^{2k}+1\big]^s\\ &= \sum_{x\in\mathbb{F}_q^*} x^{-ks}\sum_i\binom{s}{i}(x+1)^{(2ki)^*}\\ &= \sum_{x\in\mathbb{F}_q^*} x^{-ks}\sum_i\binom{s}{i}\sum_j\binom{(2ki)^*}{j}x^j\\ &= \sum_{i,j}\binom{s}{i}\binom{(2ki)^*}{j}\sum_{x\in\mathbb{F}_q^*} x^{j-ks}\\ &= \sum_i\binom{s}{i}\sum_{j\equiv ks\,(\mathrm{mod}\,q-1)}\binom{(2ki)^*}{j}.\end{aligned}$$

If $ks \not\equiv 0 \pmod{q-1}$,

$$\sum_{x\in\mathbb{F}_q} B_k(x)^s = \sum_i\binom{s}{i}\binom{(2ki)^*}{(ks)^*}.$$

If $ks \equiv 0 \pmod{q-1}$,

$$\sum_{x\in\mathbb{F}_q} B_k(x)^s = \sum_i \binom{s}{i}\Big[\binom{(2ki)^*}{0} + \binom{(2ki)^*}{q-1}\Big] \equiv_2 \sum_i \binom{s}{i}\binom{(2ki)^*}{(ks)^*}.$$

Proof of (ii). We have

$$\begin{aligned}
\sum_{x\in\mathbb{F}_q} B_k(x)^s &= \sum_{x\in\mathbb{F}_q^*} \Big(\big[(x+1)^{2k}-1\big]x^{-k}-2\Big)^s \\
&= \sum_{x\in\mathbb{F}_q^*}\sum_i \binom{s}{i}\big[(x+1)^{2k}-1\big]^i x^{-ki}(-2)^{s-i} \\
&= (-2)^s \sum_{x\in\mathbb{F}_q^*}\sum_i (-2)^{-i}\binom{s}{i}x^{-ki}\sum_j \binom{i}{j}(x+1)^{(2kj)^*}(-1)^{i-j} \\
&= (-2)^s \sum_{x\in\mathbb{F}_q^*}\sum_{i,j} 2^{-i}(-1)^j\binom{s}{i}\binom{i}{j}x^{-ki}\sum_l \binom{(2kj)^*}{l}x^l \\
&= (-2)^s \sum_{i,j,l} 2^{-i}(-1)^j\binom{s}{i}\binom{i}{j}\binom{(2kj)^*}{l}\sum_{x\in\mathbb{F}_q^*} x^{l-ki} \\
&= -(-2)^s \sum_{i,j}\sum_{l\equiv ki \,(\mathrm{mod}\, q-1)} 2^{-i}(-1)^j\binom{s}{i}\binom{i}{j}\binom{(2kj)^*}{l}.
\end{aligned}$$

Note that if $l \equiv ki \pmod{q-1}$ and $0 \le l \le (2kj)^*$, then either $l = (ki)^*$ or $i = 0$, $j > 0$ and $l = q-1$; in the latter case, $\binom{i}{j} = 0$. Therefore, we have

$$\sum_{x\in\mathbb{F}_q} B_k(x)^s = -(-2)^s \sum_{i,j} 2^{-i}(-1)^j\binom{s}{i}\binom{i}{j}\binom{(2kj)^*}{(ki)^*}.$$

□

Theorem 3.3. (i) *A_k is a PP of $\mathbb{F}_q$ if and only if* $\gcd(k, q-1) = 1$ *and*

$$\sum_i (-1)^i \binom{s}{i}\binom{(ki)^*}{(2ks)^*} \equiv_p 0 \quad \text{for all } 1 \le s \le q-2. \tag{3.4}$$

(ii) *B_k is a PP of $\mathbb{F}_q$ if and only if* $\gcd(k, q-1) = 1$ *and*

$$\sum_i (-1)^i \binom{s}{i}\binom{(2ki)^*}{(ks)^*} \equiv_p (-2)^s \quad \text{for all } 1 \le s \le q-2. \tag{3.5}$$

Proof of Theorem 3.3. We prove the claims using Hermite's criterion.

Proof of (i). Clearly, 0 is the only root of A_k in $\mathbb{F}_q$ if and only if $\gcd(k, q-1) = 1$. By (3.1), $\sum_{x\in\mathbb{F}_q} A_k(x)^s = 0$ for all $1 \le s \le q-2$ if and only if (3.4) holds.

Proof of (ii). We consider even and odd q's separately.

Case 1. Assume that q is even. We have $B_k = [(X+1)^{2k}-1]X^{q-1-k}$.

If $q = 2$, then $k = 1$ and $B_k = X^2$, which is a PP of $\mathbb{F}_2$. In this case, (3.5) is vacuously satisfied.

Now assume that $q > 2$. Clearly, 0 is the only root of B_k in $\mathbb{F}_q$ if and only if $\gcd(k, q-1) = 1$. By (3.2), $\sum_{x\in\mathbb{F}_q} B_k(x)^s = 0$ for all $1 \le s \le q-2$ if and only if (3.5) holds.

Case 2. Assume that q is odd.

1° We claim that if B_k is a PP of $\mathbb{F}_q$, then $\gcd(k, (q-1)/2) = 1$. Otherwise, $\gcd(2k, q-1) > 2$ and the equation $(x+1)^{2k} - 1 = 0$ has at least two distinct roots $x_1, x_2 \in \mathbb{F}_q^*$. Then $B_k(x_1) = -2 = B_k(x_2)$, which is a contradiction.

2° We claim that B_k is a PP of $\mathbb{F}_q$ if and only if $\gcd(k, (q-1)/2) = 1$ and (3.5) holds.

By 1° and (3.3), we only have to show that under the assumption that $\gcd(k, (q-2)/2) = 1$,

$$\sum_{i,j} 2^{-i}(-1)^j \binom{s}{i}\binom{i}{j}\binom{(2kj)^*}{(ki)^*} \equiv_p \begin{cases} 0 & \text{for } 1 \le s \le q-2, \\ 1 & \text{for } s = q-1, \end{cases} \tag{3.6}$$

if and only if (3.5) holds. Set

$$S_i = 2^{-i}\sum_j (-1)^j \binom{i}{j}\binom{(2kj)^*}{(ki)^*}, \qquad 0 \le i \le q-1.$$

Then (3.6) is equivalent to

$$\sum_i \binom{s}{i} S_i \equiv_p \begin{cases} 1 & \text{if } s = 0, \\ 0 & \text{if } 1 \le s \le q-2, \\ 1 & \text{if } s = q-1. \end{cases} \tag{3.7}$$

Equation (3.7) is a recursion for S_i, which has a unique solution

$$S_i \equiv_p \begin{cases} (-1)^i & \text{if } 0 \le i \le q-2, \\ 2 & \text{if } i = q-1. \end{cases}$$

Therefore, (3.6) is equivalent to

$$\sum_j (-1)^j \binom{i}{j}\binom{(2kj)^*}{(ki)^*} \equiv_p \begin{cases} (-2)^i & \text{if } 0 \le i \le q-2, \\ 2 & \text{if } i = q-1. \end{cases} \tag{3.8}$$

It remains to show that when $i = 0$ and $q-1$, (3.8) is automatically satisfied. When $i = 0$, (3.8) is clearly satisfied. When $i = q-1$,

$$\begin{aligned} \sum_j (-1)^j \binom{i}{j}\binom{(2kj)^*}{(ki)^*} &= \sum_{j=\frac{q-1}{2}, q-1} (-1)^j \binom{q-1}{j}\binom{(2kj)^*}{q-1} \\ &\equiv_p (-1)^{\frac{q-1}{2}}\binom{-1}{\frac{q-1}{2}} + (-1)^{q-1}\binom{-1}{q-1} = 2. \end{aligned}$$

3° To complete the proof of Case 2, it remains to show that if B_k is a PP of $\mathbb{F}_q$, then $\gcd(k, q-1) = 1$, that is, k must be odd. This is given by Lemma 4.7 later. □

Remark 3.4. In (3.5), we have

$$\binom{(2ki)^*}{(ks)^*} \equiv_p \binom{2ki}{ks} \qquad \text{if } 0 \le i \le s < \frac{q-1}{k}.$$

In fact, if $2ki \le q-1$, then $(2ki)^* = 2ki$. If $2ki \ge q$, then $(2ki)^* = 2ki-(q-1) < ki \le ks < q-1$, and hence $\binom{(2ki)^*}{(ks)^*} = 0$. On the other hand, the sum $ks+(2ki-ks)$ has a carry in base q, and hence we also have $\binom{2ki}{ks} \equiv_p 0$.

4. Facts about A_k and B_k

The permutation properties of A_k and B_k are encoded, respectively, in (3.4) and (3.5), which are not transparent in q and k. In this section, we extract from these equations some facts about A_k and B_k that are more explicit in q and k. The results collected here include both known and new. Slightly different proofs of the known results are provided for the reader's convenience.

Assume that $q > 2$ and $1 \le k \le q-1$, and let

$$a := \Big\lfloor \frac{q-1}{k} \Big\rfloor. \tag{4.1}$$

When $\gcd(k, q-1) = 1$, let $k', b \in \{1, \dots, q-1\}$ be such that

$$k'k \equiv 1 \pmod{q-1}, \qquad bk \equiv -1 \pmod{q-1}, \tag{4.2}$$

and set

$$c := \Big\lfloor \frac{q-1}{k'} \Big\rfloor. \tag{4.3}$$

Note that

$$\frac{q-1}{a+1} < k \le \frac{q-1}{a} \tag{4.4}$$

and

$$\frac{q-1}{c+1} < k' \le \frac{q-1}{c}. \tag{4.5}$$

The following obvious fact will be used frequently.

Fact 4.1. *A_k is a PP of $\mathbb{F}_q$ if and only if $A_{(pk)^*}$ is. The same is true for B_k.*

Lemma 4.2. *If $1 < k \le q-1$ and A_k is a PP of $\mathbb{F}_q$, then*

$$\binom{ka}{q-1-ka} \equiv_p 0, \tag{4.6}$$

$$\binom{2c}{c} \equiv_p 0. \tag{4.7}$$

Proof. **1°** We first prove (4.6). By Theorem 3.3 (i), $\gcd(k, q-1) = 1$, and hence (4.4) becomes

$$\frac{q-1}{a+1} < k < \frac{q-1}{a}. \tag{4.8}$$

Therefore

$$q-1 < k(a+1) \le 2ka < 2(q-1),$$

which implies that $(2ka)^* = 2ka - q + 1$. By (3.4),

$$\begin{aligned} 0 \equiv_p \sum_i (-1)^i \binom{a}{i} \binom{(ki)^*}{(2ka)^*} &= \sum_{2a-\frac{q-1}{k} \le i \le a} (-1)^i \binom{a}{i} \binom{ki}{2ka-q+1} \\ &= (-1)^a \binom{ka}{2ka-q+1} = (-1)^a \binom{ka}{q-1-ka}. \end{aligned}$$

(Note: in the above, $2a-(q-1)/k \le i \le a$ implies that $i=a$.)

2° We now prove (4.7). If $c > (q-1)/2$, (4.7) is automatically satisfied. So we assume that $c \le (q-1)/2$. Since $\gcd(k', q-1)=1$, (4.5) becomes

$$\frac{q-1}{c+1} < k' < \frac{q-1}{c}. \tag{4.9}$$

If $c=(q-1)/2$, then (4.9) implies that $k'=1$. It follows that $k=1$, which is a contradiction. Thus $c<(q-1)/2$. Set $s=(cb)^*$. Then

$$s = q-1-ck', \tag{4.10}$$

and

$$(2ks)^* = q-1-2c. \tag{4.11}$$

By (3.4),

$$0 \equiv_p \sum_i (-1)^i \binom{s}{i}\binom{(ki)^*}{(2ks)^*} = \sum_i (-1)^i \binom{s}{i}\binom{(ki)^*}{q-1-2c}. \tag{4.12}$$

For each $0 \le l \le 2c$, let $i(l) \in \{0,\dots,q-1\}$ be such that $(ki(l))^* = q-1-l$. Because of (4.9), we have

$$i(l) = \begin{cases} q-1-lk' & \text{if } 0 \le l \le c, \\ 2(q-1)-lk' & \text{if } c+1 \le l \le 2c. \end{cases}$$

When $0 \le l < c$,

$$i(l) = q-1-lk' > q-1-ck' = s.$$

When $c < l \le 2c$, we also have

$$i(l) = 2(q-1)-lk' > q-1-ck' = s.$$

When $l=c$, $i(l)=s$. Therefore (4.12) becomes

$$0 \equiv_p (-1)^s \binom{q-1-c}{q-1-2c} = (-1)^s \binom{q-1-c}{c} \equiv_p (-1)^s \binom{-1-c}{c} = (-1)^{s+c}\binom{2c}{c}.$$

□

Corollary 4.3. *Conjecture A is true for $q=p$.*

Proof. Let $1 < k \le p-1$. Since $0 \le p-1-ka \le ka \le p-1$, we have

$$\binom{ka}{p-1-ka} \not\equiv_p 0.$$

By Lemma 4.2, A_k is not a PP of $\mathbb{F}_q$. □

Remark 4.4. Equation (4.6) is contained in [4, Theorem 1], and Corollary 4.3 is implied by the proof of [4, Theorem 1].

Lemma 4.5. *Assume that A_k is a PP of $\mathbb{F}_q$. Then all the base p digits of k' are 0 or 1.*

Proof. We only have to consider the case when k is not a power of p. By (4.7), we have $c > (p-1)/2$. Write $k' = k'_0 p^0 + \cdots + k'_{e-1}p^{e-1}$, where $0 \le k'_i \le p-1$. Since

$$c \le \frac{q-1}{k'} \le \frac{p^e-1}{k'_{e-1}p^{e-1}},$$

we have

$$k'_{e-1}c \le p - \frac{1}{p^{e-1}},$$

and hence $k'_{e-1}c \le p-1$. It follows that $k'_{e-1} \le (p-1)/c < 2$. Replacing k' with $(p^{e-1-i}k')^*$ (and k with $(p^{1+i}k)^*$), we also have $k'_i < 2$. □

Lemma 4.6. *Assume that q is odd and B_k is a PP of $\mathbb{F}_q$. Then*

$$(-2)^{k-1} \equiv_p 1.$$

Proof. We first claim that $k \ne q-1$. If, to the contrary, $k = q-1$, since $\gcd(k, (q-1)/2) = 1$ (proof of Theorem 3.3, Case 2, 1°), we must have $q = 3$ and $k = 2$. But then $B_k = (X+1)^4 - 1 - 2X^2 \equiv 2X(X+1) \pmod{X^3 - X}$, which is not a PP of $\mathbb{F}_3$.

Since B_k is a PP of $\mathbb{F}_q$, $f := [(X+1)^{2k} - 1]/X^k$ is one-to-one on $\mathbb{F}_q^*$. Since $B_k(0) = 0$, we have $f(x) \ne 2$ for all $x \in \mathbb{F}_q^*$. Define $f(0) = 2$. Then $f : \mathbb{F}_q \to \mathbb{F}_q$ is a bijection with $f(-2) = 0$. Thus

(4.13)

$$-1 = \prod_{x \in \mathbb{F}_q \setminus \{-2\}} f(x) = 2 \prod_{x \in \mathbb{F}_q \setminus \{0,-2\}} \frac{(x+1)^{2k}-1}{x^k} = 2^{k+1} \prod_{x \in \mathbb{F}_q \setminus \{\pm 1\}} (x^k+1)(x^k-1).$$

Case 1. Assume that k is odd. Since $\gcd(k, (q-1)/2) = 1$, we have $\gcd(k, q-1) = 1$. Then,

$$\prod_{x \in \mathbb{F}_q \setminus \{\pm 1\}} (x^k + 1) = \prod_{y \in \mathbb{F}_q \setminus \{0,2\}} y = -\frac{1}{2},$$

$$\prod_{x \in \mathbb{F}_q \setminus \{\pm 1\}} (x^k - 1) = \prod_{y \in \mathbb{F}_q \setminus \{0,-2\}} y = \frac{1}{2}.$$

Therefore (4.13) gives

$$-1 \equiv_p 2^{k+1}\Big(-\frac{1}{2}\Big)\frac{1}{2},$$

that is, $2^{k-1} \equiv_p 1$.

Case 2. Assume that k is even. Then $(q-1)/2$ is odd and $\gcd(k, q-1) = 2$.

Let S denote the set of nonzero squares in $\mathbb{F}_q$. We have

$$\prod_{\alpha \in S} (X - \alpha) = X^{(q-1)/2} - 1. \tag{4.14}$$

Setting $X = -1$ in (4.14) gives $\prod_{\alpha \in S}(\alpha + 1) = 2$, that is,

$$\prod_{\alpha \in S \setminus \{1\}} (\alpha + 1) = 1. \tag{4.15}$$

By (4.14),

$$\prod_{\alpha \in S \setminus \{1\}} (X + 1 - \alpha) = \frac{(X+1)^{(q-1)/2} - 1}{X} = \sum_{i=1}^{(q-1)/2} \binom{(q-1)/2}{i} X^{i-1}. \tag{4.16}$$

Setting $X = 0$ on the left and right of (4.16) gives

$$\prod_{\alpha\in S\setminus\{1\}}(\alpha-1) = \frac{q-1}{2} \equiv_p -\frac{1}{2}. \tag{4.17}$$

By (4.15) and (4.17), respectively, we obtain the following.

$$\prod_{x\in\mathbb{F}_q\setminus\{\pm1\}}(x^k+1) = \prod_{x\in\mathbb{F}_q\setminus\{\pm1\}}(x^2+1) = \Big(\prod_{\alpha\in S\setminus\{1\}}(\alpha+1)\Big)^2 = 1,$$

$$\prod_{x\in\mathbb{F}_q\setminus\{\pm1\}}(x^k-1) = \Big(\prod_{\alpha\in S\setminus\{1\}}(\alpha-1)\Big)^2 = \frac{1}{4}.$$

Thus (4.13) becomes $2^{k-1} \equiv_p -1$. □

Lemma 4.7. *Assume that q is odd, $1 < k \le q-1$, and B_k is a PP of $\mathbb{F}_q$. Then k is odd, a and c are even, and*

$$2^{k-1} \equiv_p 1, \tag{4.18}$$

$$\binom{a}{\frac{a}{2}} \equiv_p (-1)^{\frac{a}{2}}2^a, \tag{4.19}$$

$$\binom{a-1}{\frac{a}{2}}\binom{ka}{k} \equiv_p (-1)^{\frac{a}{2}-1}2^{a-1}, \tag{4.20}$$

$$\binom{b}{\frac{q-1}{2}} \equiv_p (-1)^{b+\frac{q+1}{2}}2^b, \tag{4.21}$$

$$\binom{q-1-ck'}{\frac{1}{2}(q-1-ck')} \equiv_p (-1)^{\frac{c}{2}+\frac{q-1}{2}}2^{-ck'}, \tag{4.22}$$

$$(-c+1)\binom{q-1-(c-1)k'}{\frac{1}{2}[q-1-(c-2)k']} \equiv_p (-1)^{\frac{c}{2}+\frac{q-1}{2}}2^{-(c-1)k'}. \tag{4.23}$$

Proof. **1°** We first show that k is odd. This will imply (4.18) through Lemma 4.6 and also complete the proof of Theorem 3.3, Case 2, Step 3°. Recall from the proof of Theorem 3.3, Case 2, Step 2°, that $\gcd(k,(q-1)/2) = 1$ and (3.5) holds.

Assume to the contrary that k is even. Equation (3.5) with $s = (q-1)/2$ gives

$$\sum_i (-1)^i\binom{\frac{q-1}{2}}{i}\binom{(2ki)^*}{q-1} \equiv_p (-2)^{\frac{q-1}{2}}. \tag{4.24}$$

Since $\gcd(2k, q-1) = 2$, $(q-1)/2$ is odd. In the above,

$$\binom{\frac{q-1}{2}}{i}\binom{(2ki)^*}{q-1} \not\equiv_p 0$$

only if $i = (q-1)/2$. Hence (4.24) gives $2^{(q-1)/2} \equiv_p 1$. So the order of 2 in $\mathbb{F}_p^*$ is odd. However, by Lemma 4.6, $2^{k-1} \equiv_p -1$ has order 2, which is a contradiction.

2° We now prove that a is even and (4.19) and (4.20) hold. Since $\gcd(k,(q-1)/2) = 1$ and k is odd, we have $\gcd(k, q-1) = 1$. Thus (4.4) becomes

$$\frac{q-1}{a+1} < k < \frac{q-1}{a}.$$

By (3.5),

$$\sum_i (-1)^i \binom{a}{i} \binom{(2ki)^*}{ka} \equiv_p (-2)^a. \tag{4.25}$$

In the above, $(2ki)^* \geq ka$ only when $i \geq a/2$. When $a/2 < i \leq a$, $(2ki)^* = 2ki - (q-1) < ka$. Therefore, a must be even and (4.25) becomes

$$(-1)^{\frac{a}{2}} \binom{a}{\frac{a}{2}} \equiv_p (-2)^a,$$

which is (4.19). Also by (3.5),

$$\sum_i (-1)^i \binom{a-1}{i} \binom{(2ki)^*}{k(a-1)} \equiv_p (-2)^{a-1}. \tag{4.26}$$

In the above, $(2ki)^* \geq k(a-1)$ only when $i \geq (a-1)/2$, i.e., $i \geq a/2$ (since a is even). When $a/2 < i \leq a-1$, $(2ki)^* = 2ki - (q-1) < k(a-1)$. Hence (4.26) becomes

$$(-1)^{\frac{a}{2}} \binom{a-1}{\frac{a}{2}} \binom{ka}{k(a-1)} \equiv_p (-2)^{a-1},$$

which is (4.20).

3° Next, we prove (4.21). By (3.5),

$$(-2)^b \equiv_p \sum_i (-1)^i \binom{b}{i} \binom{(2ki)^*}{(kb)^*} = \sum_i (-1)^i \binom{b}{i} \binom{(2ki)^*}{q-2}. \tag{4.27}$$

In the above,

$$\binom{b}{i} \binom{(2ki)^*}{q-2} \not\equiv_p 0$$

only if $i = (q-1)/2$. Hence (4.27) gives

$$(-2)^b \equiv_p (-1)^{\frac{q-1}{2}} \binom{b}{\frac{q-1}{2}} \binom{q-1}{q-2} \equiv_p (-1)^{\frac{q+1}{2}} \binom{b}{\frac{q-1}{2}},$$

which is (4.21).

4° Finally, we prove that c is even and (4.22) and (4.2) hold.

In (4.5), if $k' = (q-1)/c$, since $\gcd(k', q-1) = 1$, we must have $k' = 1$. Then $k = 1$, which is a contradiction. Therefore (4.5) becomes

$$\frac{q-1}{c+1} < k' < \frac{q-1}{c}. \tag{4.28}$$

Let $s = (cb)^*$. Then we have

$$s = q - 1 - ck',$$
$$(ks)^* = q - 1 - c.$$

By (3.5),

$$\sum_i (-1)^i \binom{s}{i} \binom{(2ki)^*}{q-1-c} \equiv_p (-2)^s. \tag{4.29}$$

For $0 \leq l \leq c/2$, let $i \in \{0, \ldots, q-1\}$ be such that $(2ki)^* = q - 1 - 2l$. By (4.28),

$$i = q - 1 - lk' \quad \text{or} \quad \frac{1}{2}(q-1) - lk'.$$

If $i = q-1-lk'$, then $i > q-1-ck' = s$. If $i = \frac{1}{2}(q-1)-lk'$, then $i \le s$ only if $l = c/2$. In fact, $\frac{1}{2}(q-1)-lk' = i \le s = q-1-ck'$ implies that

$$k' \le \frac{q-1}{2(c-l)},$$

which, by (4.28), implies that $2(c-l) \le c$, i.e., $l \ge c/2$.

Therefore, the ith term of the sum in (4.29) is nonzero only if $i = \frac{1}{2}(q-1)-\frac{c}{2}k'$. Hence c must be even and (4.29) gives

$$(-1)^{\frac{1}{2}(q-1-ck')}\binom{q-1-ck'}{\frac{1}{2}(q-1-ck')} \equiv_p (-2)^{-ck'},$$

which is (4.22).

To prove (4.23), we choose $s = ((c-1)b)^*$. We have

$$s = q-1-(c-1)k',$$
$$(ks)^* = q-1-(c-1),$$

and (3.5) gives

$$\sum_i (-1)^i \binom{s}{i}\binom{(2ki)^*}{q-1-(c-1)} \equiv_p (-2)^s. \tag{4.30}$$

For $0 \le l \le c/2-1$, let $i \in \{0,\dots,q-1\}$ be such that $(2ki)^* = q-1-2l$. Then

$$i = q-1-lk' \quad \text{or} \quad \frac{1}{2}(q-1)-lk'.$$

If $i = q-1-lk'$, then $i > s$. If $i = \frac{1}{2}(q-1)-lk'$, then $i \le s$ only if $l = c/2-1$. In fact, $i \le s$ implies that

$$k' \le \frac{q-1}{2(c-1-l)},$$

which further implies that $2(c-1-l) \le c$, i.e., $l \ge c/2-1$. Therefore, the ith term of the sum in (4.30) is nonzero only if $i = \frac{1}{2}[q-1-(c-2)k']$. Hence (4.30) gives

$$\begin{aligned} -2^{-(c-1)k'} &\equiv_p (-1)^{\frac{c}{2}-1+\frac{q-1}{2}}\binom{q-1-(c-1)k'}{\frac{1}{2}[q-1-(c-2)k']}\binom{q-1-2(\frac{c}{2}-1)}{q-1-(c-1)} \\ &\equiv_p (-1)^{\frac{c}{2}-1+\frac{q-1}{2}}\binom{q-1-(c-1)k'}{\frac{1}{2}[q-1-(c-2)k']}(-c+1), \end{aligned}$$

which is (4.23). □

For each odd prime p, let

$$\alpha(p) = \min\Big\{u : u \text{ is a positive even integer, } \binom{u}{u/2} \equiv_p (-1)^{\frac{u}{2}}2^u\Big\}. \tag{4.31}$$

Remark 4.8. Since

$$\binom{p-1}{\frac{p-1}{2}} \equiv_p (-1)^{\frac{p-1}{2}},$$

we always have $\alpha(p) \le p-1$.

Lemma 4.9. *Assume that q is odd and $1 < k \le q-1$. If B_k is a PP of $\mathbb{F}_q$, then all the base p digits of k are $\le (p-1)/\alpha(p)$.*

Proof. By (4.19), $a = \lfloor (q-1)/k \rfloor \geq \alpha(p)$. Let $q = p^e$ and write $k = k_0 p^0 + \cdots + k_{e-1}p^{e-1}$, where $0 \leq k_i \leq p-1$. We first show that $k_{e-1} \leq (p-1)/\alpha(p)$. Assume that $k_{e-1} > 0$. Since

$$a \leq \frac{q-1}{k} \leq \frac{p^e - 1}{k_{e-1}p^{e-1}},$$

we have

$$k_{e-1}a \leq p - \frac{1}{p^{e-1}}.$$

Thus $k_{e-1}a \leq p-1$, and hence $k_{e-1} \leq (p-1)/a \leq (p-1)/\alpha(p)$.

Replacing k with $(p^{e-1-i}k)^*$, we conclude that $k_i \leq (p-1)/\alpha(p)$. □

We include a quick proof for Theorem 2.4.

Proof of Theorem 2.4. Let $q = p^e$. Assume that $1 < k \leq q^m - 1$ and B_k is a PP of $\mathbb{F}_{q^m}$. Write $k = k_0 q^0 + \cdots + k_{m-1}q^{m-1}$, $0 \leq k_i \leq q-1$. By Lemma 4.9, all the base p digits of k are $\leq \lfloor (p-1)/\alpha(p) \rfloor$. Hence

$$k_i \leq \Big\lfloor \frac{p-1}{\alpha(p)} \Big\rfloor \frac{q-1}{p-1}, \qquad 0 \leq i \leq m-1.$$

Since Conjecture B is assumed to be true for q, by Fact 4.1, we may assume that $k \equiv 1 \pmod{q-1}$, that is,

$$k_0 + \cdots + k_{m-1} \equiv 1 \pmod{q-1}.$$

However,

$$k_0 + \cdots + k_{m-1} \leq m \Big\lfloor \frac{p-1}{\alpha(p)} \Big\rfloor \frac{q-1}{p-1} \leq q-1.$$

So we must have $k_0 + \cdots + k_{m-1} = 1$. □

5. A Theorem on Conjecture A

Theorem 5.1. *Conjecture A is true for $q = p^e$, where p is an odd prime and* $\mathrm{gpf}(e) \leq p-1$.

Theorem 5.1 is an immediate consequence of Corollary 4.3 and the following lemma.

Lemma 5.2. *Let q be a power of an odd prime p and $1 \leq m \leq p-1$. If Conjecture A is true for q, it is also true for q^m.*

Proof. Assume that A_k is a PP of $\mathbb{F}_{q^m}$, where $1 \leq k \leq q^m - 2$. Let $k' \in \{1, \ldots, q^m - 2\}$ be such that $k'k \equiv 1 \pmod{q^m - 1}$. It suffices to show that k' is a power of p. Write $k' = k'_0 q^0 + \cdots + k'_{m-1}q^{m-1}$, $0 \leq k'_i \leq q-1$. Since A_k is a PP of $\mathbb{F}_q$ and since Conjecture A is true for q, we may assume that $k' \equiv 1 \pmod{q-1}$, that is,

$$k'_0 + \cdots + k'_{m-1} \equiv 1 \pmod{q-1}. \tag{5.1}$$

On the other hand, by Lemma 4.5, all base p digits of k' are ≤ 1. Hence

$$k'_i \leq \frac{q-1}{p-1}, \qquad 0 \leq i \leq m-1.$$

Therefore,

$$k'_0 + \cdots + k'_{m-1} \leq \frac{q-1}{p-1} m \leq q-1. \tag{5.2}$$

Combining (5.1) and (5.2) gives $k'_0 + \cdots + k'_{m-1} = 1$. □

Remark 5.3. In [8], the author commented that an avenue to improve Theorem 2.2 is to find a more explicit form for the function p_0 in that theorem. By Theorem 5.1, one can choose $p_0(r) = r + 1$.

6. Conjecture B with $\alpha(p) > (p-1)/2$

Our proof of Conjecture B under the condition $\alpha(p) > (p-1)/2$ follows a simple line of logic. Assume to the contrary that B_k is a PP of $\mathbb{F}_{p^e}$ for some $k \in \{1, \dots, p^e - 1\}$ which is not a power of p. Then with the help of Lemma 6.1, $a := \lfloor (p^e-1)/k \rfloor \equiv_p 0$. However, (4.20) dictates that $a \not\equiv_p 0$, hence a contradiction.

Lemma 6.1. *Let $p \geq 3$ be a prime. Let i, j, e be integers such that $0 < i < j \leq e - 1$, and let*

$$\begin{aligned} k &= k_0 p^0 + \cdots + k_{i-1} p^{i-1} + p^i + p^j, \quad k_0, \dots, k_{i-1} \in \{0, \dots, p-1\}, \\ a &= \Big\lfloor \frac{p^e - 1}{k} \Big\rfloor, \\ u &= \Big\lfloor \frac{e-j}{j-i} \Big\rfloor. \end{aligned}$$

Assume that a is even and

$$\frac{p^e - 1}{p^i + p^j} - \frac{p^e - 1}{k} \leq 1. \tag{6.1}$$

Then

$$a = \begin{cases} p^{e-j}\big[1 - p^{i-j} + \cdots + (-1)^{u(i-j)}\big] & \text{if } u \text{ is odd,} \\ p^{e-j}\big[1 - p^{i-j} + \cdots + (-1)^{u(i-j)}\big] - 1 & \text{if } u \text{ is even.} \end{cases} \tag{6.2}$$

Proof. Write $e - j = u(j-i) + r$, $0 \leq r < j - i$. We have

$$\begin{aligned} \frac{p^e - 1}{p^i + p^j} &= p^{e-j} \frac{1}{1 + p^{i-j}} - \frac{1}{p^i + p^j} \\ &= p^{e-j}\big[1 - p^{i-j} + p^{2(i-j)} - \cdots\big] - \frac{1}{p^i + p^j} \\ &= p^{e-j}\big[1 - p^{i-j} + \cdots + (-1)^u p^{u(i-j)}\big] \\ &\quad + (-1)^{u+1} p^{r+i-j}\big[1 - p^{i-j} + p^{2(i-j)} - \cdots\big] - \frac{1}{p^i + p^j} \\ &= p^{e-j}\big[1 - p^{i-j} + \cdots + (-1)^u p^{u(i-j)}\big] + (-1)^{u+1} p^{r+i-j} \frac{1}{1 + p^{i-j}} - \frac{1}{p^i + p^j} \\ &= p^{e-j}\big[1 - p^{i-j} + \cdots + (-1)^u p^{u(i-j)}\big] + \frac{1}{p^i + p^j}\big[(-1)^{u+1} p^{r+i} - 1\big]. \end{aligned}$$

Since $r + i < j$, we have

$$\begin{aligned} 0 < \frac{1}{p^i + p^j}\big[(-1)^{u+1} p^{r+i} - 1\big] < 1 \quad &\text{if } u \text{ is odd,} \\ -1 < \frac{1}{p^i + p^j}\big[(-1)^{u+1} p^{r+i} - 1\big] < 0 \quad &\text{if } u \text{ is even.} \end{aligned}$$

Thus

$$\Big\lfloor \frac{p^e - 1}{p^i + p^j} \Big\rfloor = \begin{cases} p^{e-j}\big[1 - p^{i-j} + \cdots + (-1)^u p^{u(i-j)}\big] & \text{if } u \text{ is odd,} \\ p^{e-j}\big[1 - p^{i-j} + \cdots + (-1)^u p^{u(i-j)}\big] - 1 & \text{if } u \text{ is even.} \end{cases} \tag{6.3}$$

Note that the right side of (6.3) is always even. Then (6.2) follows from (6.1), (6.3) and the assumption that a is even. □

Theorem 6.2. *Conjecture B is true for $q = p^e$, where p is an odd prime such that $\alpha(p) > (p-1)/2$.*

Proof. Assume to the contrary that there exists $k \in \{1, \dots, p^e - 1\}$, which is not a power of p, such that B_k is a PP of $\mathbb{F}_{p^e}$. Write

$$k = k_0 p^0 + \cdots + k_{e-1} p^{e-1}, \quad 0 \le k_i \le p-1.$$

Since $\alpha(p) > (p-1)/2$, by Lemma 4.9 we have $k_i \le 1$ for all i. Let

$$a = \Big\lfloor \frac{p^e - 1}{k} \Big\rfloor.$$

By Lemma 4.7, a is even, and by (4.20),

$$\binom{ka}{k} \not\equiv_p 0.$$

In particular, $a \not\equiv_p 0$.

Let d be the distance in $\mathbb{Z}/e\mathbb{Z}$ defined by

$$d([x],[y]) = \min\{|x-y|,\, e - |x-y|\}, \quad x, y \in \{0, \dots, e-1\}.$$

This is the arc distance with $[0], \dots, [e-1]$ evenly placed on a circle in that order. Let l be the shortest distance between two indices $i, j \in \mathbb{Z}/e\mathbb{Z}$ with $k_i = k_j = 1$. Then $1 \le l < e$. The 1's among $k_0, \dots, k_{e-1}$ cannot be evenly spaced. Otherwise, $\gcd(k, p^e - 1) = (p^e - 1)/(p^l - 1) > 1$, which is a contradiction. Therefore, we may write

$$(k_0, \dots, k_{e-1}) = (\overset{0}{*} \cdots * \overset{i}{1} \underbrace{0 \cdots 0}_{l-1} \overset{j}{1} \underbrace{0 \cdots \overset{e-1}{0}}_{l}),$$

where $j = e - 1 - l$, $i = j - l = e - 1 - 2l$. We have

$$u = \Big\lfloor \frac{e-j}{j-i} \Big\rfloor = \Big\lfloor \frac{l+1}{l} \Big\rfloor = \begin{cases} 2 & \text{if } l = 1, \\ 1 & \text{if } l \ge 2. \end{cases}$$

Case 1. Assume that $l = 1$. Since

$$k_0 p^0 + \cdots + k_i p^i \le p^0 + \cdots + p^i = \frac{p^j - 1}{p-1} < \frac{p^j}{p-1},$$

we have

$$\begin{aligned} \frac{p^e - 1}{p^i + p^j} - \frac{p^e - 1}{k} &= (p^e - 1)\Big[\frac{1}{p^i + p^j} - \frac{1}{k_0 p^0 + \cdots + k_i p^i + p^j}\Big] \\ &< (p^e - 1)\left[\frac{1}{p^i + p^j} - \frac{1}{\frac{p^j}{p-1} + p^j}\right] \\ &= (p^e - 1)\frac{1}{p^j}\Big[\frac{p}{p+1} - \frac{p-1}{p}\Big] \\ &= \frac{p^e - 1}{p^j p(p+1)} < p^{e-j-2} = 1. \end{aligned}$$

Thus by (6.2),

$$a = p^{e-j}\big[1 - p^{i-j} + \cdots + (-1)^u p^{u(i-j)}\big] - 1 = p^2(1 - p^{-1}) \equiv_p 0,$$

which is a contradiction.

Case 2. Assume that $l \geq 2$. Since the distance between the indices of any two consecutive 1's among $k_0, \ldots, k_{e-1}$ is $\geq l$, we have

$$k_0p^0 + \cdots + k_ip^i < p^i + p^{i-l} + p^{i-2l} + \cdots = p^i\frac{p^l}{p^l-1}.$$

Hence

$$\begin{aligned}\frac{p^e-1}{p^i+p^j} - \frac{p^e-1}{k} &= (p^e-1)\Big[\frac{1}{p^i+p^j} - \frac{1}{k_0p^0+\cdots+k_ip^i+p^j}\Big]\\ &< (p^e-1)\left[\frac{1}{p^i+p^j} - \frac{1}{\frac{p^l}{p^l-1}p^i+p^j}\right]\\ &= \frac{p^e-1}{p^l-1}\frac{p^i}{(p^i+p^j)\big(\frac{p^l}{p^l-1}p^i+p^j\big)}\\ &< \frac{p^{e+i}}{p(p^i+p^j)\big(\frac{p^l}{p^l-1}p^i+p^j\big)}\\ &< \frac{p^{e+i}}{p^{2j+1}} = p^{e+e-1-2l-2(e-1-l)-1} = 1.\end{aligned}$$

Therefore by (6.2),

$$a = p^{e-j}\big[1 - p^{i-j} + \cdots + (-1)^u p^{u(i-j)}\big] = p^{l+1}(1-p^{-l}) \equiv_p 0,$$

which is a contradiction. □

Many odd primes p satisfy the condition $\alpha(p) > (p-1)/2$. Among the first 1000 odd primes p, the equation $\alpha(p) = p-1$ holds with 211 exceptions. The first few exceptions are $\alpha(29) = 10$, $\alpha(31) = 8$, $\alpha(47) = 18, \ldots$. In fact, for any odd prime p, either $\alpha(p) = p-1$ or $\alpha(p) \leq (p-1)/2$; this follows from a symmetry described below.

Note that for integer $m \geq 0$,

$$2^{-2m}\binom{2m}{m} = \frac{(2m)!}{(2^m\cdot m!)^2} = \frac{(2m-1)!!}{(2m)!!}.$$

(Recall that for any integer $i \geq 0$, $i!! = \prod_{0\leq j<i/2}(i-2j)$.) Thus $\alpha(p)$ is the smallest positive even integer $2m$ ($\leq p-1$) such that

$$\frac{(2m-1)!!}{(2m)!!} \equiv_p (-1)^m. \tag{6.4}$$

Let $0 \leq m \leq (p-1)/2$. Since

$$\begin{aligned}&2^{-2m}\binom{2m}{m}\Big[2^{-(p-1-2m)}\binom{p-1-2m}{\frac{p-1}{2}-m}\Big]^{-1}\\ &= \frac{(2m-1)!!}{(2m)!!}\cdot\frac{(p-1-2m)!!}{(p-2-2m)!!} \equiv_p \frac{(p-2)!!}{(p-1)!!} = \prod_{\substack{2\leq i\leq p-1\\ i \text{ even}}}\frac{p-i}{i} \equiv_p (-1)^{\frac{p-1}{2}},\end{aligned}$$

condition (6.4) is unchanged when m is replaced by $(p-1)/2 - m$.

For integers $i \le j$, denote $i(i+1)\cdots j$ by $[i,j]$. Then we have

$$\binom{2m}{m} = \frac{[m+1,2m]}{[1,m]},$$
$$\binom{p-1-2m}{\frac{p-1}{2}-m} = \frac{[\frac{p+1}{2}-m, p-1-2m]}{[1,\frac{p-1}{2}-m]} \equiv_p \frac{[2m+1,\frac{p-1}{2}+m]}{[\frac{p+1}{2}+m, p-1]}.$$

Hence

$$\binom{2m}{m}\binom{p-1-2m}{\frac{p-1}{2}-m} \equiv_p \frac{[m+1,m+\frac{p-1}{2}]}{[1,m][m+\frac{p+1}{2},p-1]} = \frac{[m+1,m+\frac{p-1}{2}]^2}{[1,p-1]}$$
$$\equiv_p -\Big[m+1,m+\frac{p-1}{2}\Big]^2.$$

Therefore, if (6.4) is satisfied, one has

$$\prod_{i=1}^{\frac{p-1}{2}} (m+i)^2 \equiv_p (-1)^{\frac{p+1}{2}}.$$

7. Proof of Conjecture 1.1

We continue to use the notation introduced at the beginning of Section 4. For $1 \le k \le q-1$ with $\gcd(k,q-1)=1$, the parameters k', b and c are defined in (4.2) and (4.3).

Assume to the contrary that Conjecture 1.1 is false. Then for some $k \in \{1,\dots,q-1\}$ which is not a power of p, both A_k and B_k are PPs of $\mathbb{F}_q$. We will see that the same argument as in the proof of Theorem 6.2 gives that $c := \lfloor (q-1)/k' \rfloor \equiv_p 0$. The purpose of the following lemma is to establish an equation that cannot be satisfied when $c \equiv_p 0$.

Lemma 7.1. *Assume that q is odd, $1 < k \le q-1$, and both A_k and B_k are PPs of $\mathbb{F}_q$. Then c is even and*

$$2^{-2ck'} = \binom{2(q-1)-2ck'}{q-1-ck'} + (-1)^{\frac{q-1}{2}+\frac{c}{2}+1}\binom{2(q-1)-2ck'}{\frac{1}{2}(q-1)-(\frac{c}{2}-1)k'}\binom{2c}{c+2}. \tag{7.1}$$

Proof. By Lemma 4.7, c is even. Let $s = (2cb)^*$. Since $2cb \not\equiv 0 \pmod{q-1}$, we have $1 \le s \le q-2$. Clearly, $2ck' > q-1$. (Otherwise, $2c \le (q-1)/k'$, which implies that $2c \le c$, a contradiction.) It follows that

$$s = 2(q-1) - 2ck'.$$

Note that $c < (q-1)/2$. (Otherwise, since $\gcd(k',q-1)=1$, we have $k' < (q-1)/2 \le 2$, which implies that $k'=1$, i.e., $k=1$, which is a contradiction.) Thus

$$(ks)^* = q-1-2c.$$

By (3.5),

$$\sum_i (-1)^i \binom{s}{i}\binom{(2ki)^*}{q-1-2c} \equiv_p (-2)^s. \tag{7.2}$$

For each $0 \le l \le c$, let $i \in \{0,\dots,q-1\}$ be such that $(2ki)^* = q-1-2l$. Then

$$i = \frac{3}{2}(q-1) - lk' \quad \text{or} \quad q-1-lk' \quad \text{or} \quad \frac{1}{2}(q-1)-lk'.$$

In each of these cases, we determine the necessary conditions on l such that i satisfies $0 \le i \le s$.

Case 1. Assume that $i = \frac{3}{2}(q-1) - lk'$. In this case,

$$\begin{aligned} i &\ge \frac{3}{2}(q-1) - ck' > 2(q-1) - 2ck' \qquad (\text{since } 2ck' > q-1) \\ &= s. \end{aligned}$$

Case 2. Assume that $i = q - 1 - lk'$. In this case we always have $i \ge 0$. Moreover,

$$\begin{aligned} i \le s &\Leftrightarrow q - 1 - lk' \le 2(q-1) - 2ck' \\ &\Leftrightarrow l \ge 2c - \frac{q-1}{k'} \\ &\Leftrightarrow l \ge c. \end{aligned}$$

Case 3. Assume that $i = \frac{1}{2}(q-1) - lk'$. In this case, $i \ge 0$ if and only if $l \le c/2$. Moreover,

$$\begin{aligned} i \le s &\Leftrightarrow \frac{1}{2}(q-1) - lk' \le 2(q-1) - 2ck' \\ &\Leftrightarrow l \ge 2c - \frac{3}{2} \cdot \frac{q-1}{k'} \\ &\Rightarrow l > 2c - \frac{3}{2}(c+1) \\ &\Rightarrow l \ge \frac{c}{2} - 1. \end{aligned}$$

Combining the above three cases, we see that (7.2) becomes

$$\begin{aligned} 2^{-2ck'} \equiv_p & \binom{2(q-1)-2ck'}{q-1-ck'} \\ & + (-1)^{\frac{q-1}{2}+\frac{c}{2}+1} \binom{2(q-1)-2ck'}{\frac{1}{2}(q-1)-(\frac{c}{2}-1)k'} \binom{q-1-2(\frac{c}{2}-1)}{q-1-2c} \\ & + (-1)^{\frac{q-1}{2}+\frac{c}{2}} \binom{2(q-1)-2ck'}{\frac{1}{2}(q-1)-\frac{c}{2}k'} \binom{q-1-c}{q-1-2c}. \end{aligned} \tag{7.3}$$

In the above,

$$\binom{q-1-2(\frac{c}{2}-1)}{q-1-2c} \equiv_p \binom{-c+1}{2+c} = \binom{2c}{c+2},$$

and, by (4.7),

$$\binom{q-1-c}{q-1-2c} \equiv_p \binom{-1-c}{c} = \binom{2c}{c} \equiv_p 0.$$

Hence (7.1) follows from (7.3). □

Theorem 7.2. *Conjecture 1.1 is true.*

Proof. Assume to the contrary that Conjecture 1.1 is false. Then there exists $1 \le k \le q-1$, which is not a power of p, such that both A_k and B_k are PPs of $\mathbb{F}_q$.

By Lemma 4.5, all the base p digits of k' are ≤ 1. By exactly the same argument as in the proof of Theorem 6.2, with k and a replaced by k' and c, respectively, we

conclude that we may assume that $c \equiv_p 0$. Then obviously,

$$\binom{2c}{c+2} \equiv_p 0. \tag{7.4}$$

Since $q-1-ck' \equiv_p p-1$, the sum $(q-1-ck')+(q-1-ck')$ has a carry in base p at p^0, implying that

$$\binom{2(q-1)-2ck'}{q-1-ck'} \equiv_p 0. \tag{7.5}$$

Combining (7.1), (7.4) and (7.5), we have a contradiction. □

As a concluding remark, we reiterate that Conjectures A and B are still open and we hope that they will stimulate further research.

Acknowledgments

The authors are thankful to Qing Xiang who facilitated their collaboration. The authors would also like to thank the referees whose comments helped to improve the paper.

References

[1] B. Bollobás, *Modern Graph Theory*, Springer-Verlag, New York, 1998.
[2] J. A. Bondy and M. Simonovits, *Cycles of even length in graphs*, J. Combin. Theory, Ser. B **16** (1974), 97 – 105.
[3] J. A. Bondy, *Extremal problems of Paul Erdös on circuits in graphs*, Paul Erdös and His Mathematics. II, Bolyai Society, Mathematical Studies, 11, Budapest, 2002, 135 – 156.
[4] V. Dmytrenko, F. Lazebnik, J. Williford, *On monomial graphs of girth eight*, Finite Fields Appl. **13** (2007), 828 – 842.
[5] G. Exoo and R. Jajcay, *Dynamic cage survey*, Electron. J. Combin. (2013), #DS16, 1 – 55.
[6] Z. Füredi and M. Simonovits, *The history of degenerate (bipartite) extremal graph problems*, Erdős centennial, 169 – 264, Bolyai Soc. Math. Stud., 25, János Bolyai Math. Soc., Budapest, 2013.
[7] X. Hou, *Permutation polynomials over finite fields — a survey of recent advances*, Finite Fields Appl. **32** (2015), 82 – 119.
[8] B. G. Kronenthal, *Monomial graphs and generalized quadrangles*, Finite Fields Appl. **18** (2012), 674 – 684.
[9] F. Lazebnik and V. A. Ustimenko, *New examples of graphs without small cycles and of large size*, European J. Combin. **14** (1993), 445 – 460.
[10] F. Lazebnik, V.A. Ustimenko and A.J. Woldar, *A new series of dense graphs of high girth*, Bull. Amer. Math. Soc. (N.S.) **32** (1995), 73 – 79.
[11] F. Lazebnik and A. J. Woldar, *General properties of some families of graphs defined by systems of equations*, J. Graph Theory **38** (2001), 65 – 86.
[12] F. Lazebnik and D. Mubayi, *New lower bounds for Ramsey numbers of graphs and hypergraphs*, Adv. in Appl. Math. **28** (2002), 544 – 559.
[13] F. Lazebnik and J. Verstraëte, *On hypergraphs of girth five*, Electron. J. Combin. **10** (2003), R25, 1 – 15.
[14] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications 20, Cambridge University Press, Cambridge, 1997.
[15] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. **1** (1878), 197 – 240.
[16] M. Miller and J. Širáň, *Moore graphs and beyond: A survey of the degree/diameter problem*, Electron. J. Combin. (2013), **20** (2), #DS14v2, 1 – 92.

Department of Mathematics and Statistics, University of South Florida, Tampa, FL 33620
E-mail address: xhou@usf.edu

Department of Mathematics and Statistics, University of South Florida, Tampa, FL 33620
E-mail address: slappano@mail.usf.edu

Department of Mathematical Sciences, University of Delaware, Newark, DE 19716
E-mail address: fellaz@udel.edu