ON THE DIRECTIONS DETERMINED BY CARTESIAN PRODUCTS AND THE CLIQUE NUMBER OF GENERALIZED PALEY GRAPHS

Chi Hoi Yip
Dept. of Mathematics, University of British Columbia, Vancouver, BC, Canada
kyleyip@math.ubc.ca

Received: 10/8/20, Accepted: 4/20/21, Published: 5/4/21

Abstract

It is known that the number of directions determined by a Cartesian product $A \times B \subset AG(2,p)$ is at least $|A||B| - \min\{|A|,|B|\} + 2$, provided p is prime and $|A||B| < p$. This implies the best known upper bound on the clique number of the Paley graph over $\mathbb{F}_p$. In this paper, we extend this result to $AG(2,q)$, where q is a prime power. We also give improved upper bounds on the clique number of generalized Paley graphs over $\mathbb{F}_q$. In particular, for a cubic Paley graph, we improve the trivial upper bound $\sqrt{q}$ to $0.769\sqrt{q}+1$. In general, as an application of our key result on the number of directions, for any positive function h such that $h(x) = o(x)$ as $x \to \infty$, we improve the trivial upper bound $\sqrt{q}$ to $\sqrt{q} - h(p)$ for almost all non-squares q.

1. Introduction

Let $q = p^s$ be a prime power and $\mathbb{F}_q$ the finite field with q elements. Throughout this work, all polynomials considered will be defined over $\mathbb{F}_q$.

In the first half of the paper, we will improve lower bounds on the number of directions determined by a Cartesian product in the affine Galois plane $AG(2,q)$, which extends the work of Di Benedetto, Solymosi, and White [7]. In the second part of the paper, we will improve upper bounds on the clique number of generalized Paley graphs over $\mathbb{F}_q$, which extends the work of Bachoc, Matolcsi, and Ruzsa [2]; Hanson and Petridis [11]; and Yip [22]. The connection between the number of directions and the clique number will be made precise in Section 1.4.

1.1. Directions Determined by a Point Set in an Affine Galois Plane

Let $AG(2,q)$ denote the *affine Galois plane* over the finite field $\mathbb{F}_q$. Let $U \subset AG(2,q)$, we use Cartesian coordinates in $AG(2,q)$ so that $U = \{(x_i, y_i) : 1 \leq$

$i \le |U|\}$. The set of *directions determined by* $U \subset AG(2,q)$ is

$$D := D(U) = \left\{ \frac{y_j - y_i}{x_j - x_i} : 1 \le i < j \le |U| \right\} \subset \mathbb{F}_q \cup \{\infty\}.$$

The possible values on $|D|$ have been studied by many authors. For a survey of such kind of results, readers can refer to [21]. We begin with some relevant results where the point set U is not necessarily a Cartesian product. The following theorem was proved by Rédei [16] in the case $|U| = p$, and later extended by Szőnyi [20, 21] to any $|U| \le p$.

Theorem 1.1 ([21, Theorem 5.2]). *Let p be a prime, and let $U \subset AG(2,p)$ with $1 < |U| \le p$. Then either U is contained in a line, or U determines at least $\frac{|U|+3}{2}$ directions.*

When the underlying field becomes $\mathbb{F}_q$, the problem becomes much more difficult. Szőnyi [21] proved the following interesting result, which is of a similar flavor as Theorem 1.1. However, when we are working in $\mathbb{F}_q$, there are cases where $|D|$ is small; see the remarks before Theorem 1.7.

Theorem 1.2 ([20, Theorem 4]). *Let $U \subset AG(2,q)$ with $|U| = q - k$, where $0 \le k \le \sqrt{q}/2$. Then either U determines at least $(q+1)/2$ directions, or it can be extended to a set V with $|V| = q$, which determines the same set of directions as U.*

Note that in Theorem 1.2, $|U|$ is assumed to be close to q. In general, $|U|$ could be much smaller compared to q, and the best-known result is the following theorem.

Theorem 1.3 ([8, Theorem 1.3]). *Let $q = p^s$ be a prime power, and let $U \subset AG(2,q)$ with $1 < |U| \le q$. Then either U is contained in a line or U determines at least $\frac{|U|}{\sqrt{q}}$ directions if s is even, and $\frac{|U|}{p^{\frac{s-1}{2}}+1}$ directions if s is odd.*

We point out that the Rédei polynomial with Szőnyi's extension is the main tool to prove the above theorems. Another key idea is to study the properties of lacunary polynomials, which are polynomials where there exists a substantial gap between the degree of two consecutive terms. In Section 2.1, we will describe these tools.

1.2. Directions Determined by a Cartesian Product

When the point set U is a Cartesian product $A \times B$, we expect that the lower bound on $|D|$ can be improved, as U is more structured. Let $A, B \subset \mathbb{F}_q$ be such that $|A| = m, |B| = n$. Denote $A = \{a_1, a_2, \ldots, a_m\}, B = \{b_1, b_2, \ldots, b_n\}$. The set of directions determined by $A \times B \subset AG(2,q)$ is

$$D = \frac{B-B}{A-A} = \left\{ \frac{y_2 - y_1}{x_2 - x_1} : x_1, x_2 \in A, y_1, y_2 \in B \right\} \subset \mathbb{F}_q \cup \{\infty\},$$

where for a set X, we denote $X - X = \{x_1 - x_2 : x_1, x_2 \in X\}$. Estimating the size of the set D determined by certain Cartesian products (in particular $A \times A$) turns out to be useful in sum-product estimates over finite fields; see [15, 17, 18] for more details and examples. In this paper, we focus on improving the lower bound on $|D|$.

Note that if $m = 1$ or $n = 1$, the direction set D is trivial. If $mn > q$, a simple pigeonhole argument shows that $D = \mathbb{F}_q \cup \{\infty\}$. Also note that the set of directions only depends on the set $A - A, B - B$. Without loss of generality, we always assume that $m, n \geq 2$, $k = q - mn > 0$, and $b_n = 0$.

When $U = A \times B$, it turned out Theorem 1.1 can be significantly improved. In [7], Di Benedetto, Solymosi, and White showed the following theorem.

Theorem 1.4 ([7, Theorem 1])**.** *Let $A, B \subset \mathbb{F}_p$ be sets each of size at least two such that $|A||B| < p$. Then the set of points $A \times B \subset AG(2, p)$ determines at least $|A||B| - \min\{|A|, |B|\} + 2$ directions.*

Observe that the key lemma used in their proof is the following lemma.

Lemma 1.5 ([7, Lemma 6])**.** *Let $R, S \in \mathbb{F}_p[x]$ be polynomials each with constant term 1. Suppose that R and R' are relatively prime and R does not divide S, where R' is the formal derivative of R. If $x^{deg(R)+deg(S)+1}$ divides $R^m(x)S(x) - 1$ for some m not divisible by p, then $R(x) = 1$.*

In general, it is possible that R divides S. To use this lemma, we need to first write $S = R^r T$, where r is the largest integer such that $R^r \mid S$. Then T does not divide S, and $R^m(x)S(x) - 1 = R^{m+r}(x)T(x) - 1$, so we can apply the lemma with R and T. If we are working in $AG(2, p)$ and we wish to apply this lemma to estimate $|D|$, then we could expect $m + r < p$ and conclude that $R(x) = 1$. Unfortunately, we fail to give effective bounds on $m + r$ when we are working in $AG(2, q)$.

To extend their method to $AG(2, q)$, we need to generalize Lemma 1.5. In Section 3, we first prove Lemma 3.1 and then apply that to prove Theorem 1.6. The symmetric polynomials $f_{m,t}(b_1, b_2, \ldots, b_{n-1}, 0)$ in the statement of Theorem 1.6 will be defined via recurrence relations in Section 2.1, and we will give an explicit formula for $f_{m,t}$ in Section 2.2. Theorem 1.6 is central in proving our main results, Theorem 1.7 and Theorem 1.9.

Theorem 1.6. *Let $q = p^s$ be a prime power. Let $m, n \geq 2$ be integers such that $k = q - mn > 0$. Let $A, B \subset \mathbb{F}_q$ with $|A| = m$ and $|B| = n$, and write $B = \{b_1, b_2, \ldots, b_{n-1}, 0\}$. Suppose l is the smallest non-negative integer such that $f_{m,k-l}(b_1, b_2, \ldots, b_{n-1}, 0) \neq 0$. Suppose one of the following conditions is satisfied:*

1. *Every integer between m and $m + \lfloor \frac{k-l}{n-1} \rfloor$ is not a multiple of p.*
2. *$p \nmid (m + l)$.*

Then the number of directions determined by the set $A \times B \subset AG(2, q)$ is at least $mn - n + l + 2$.

In Corollary 3.2, which is a corollary of Theorem 1.6, it will be made precise that Theorem 1.6 is indeed a generalization of Theorem 1.4. To apply Theorem 1.6, it is important to understand the polynomial $f_{m,k}(r_1, r_2, \ldots, r_{n-1}, 0)$, especially the distribution of roots of $f_{m,k}$, which we will discuss in Section 4. In view of Corollary 2.6, which gives the explicit formula for $f_{m,k}$, we also need to study how binomial coefficients behave modulo the prime p. A useful tool in determining this is Lucas's Theorem. It states that if p is a prime and if m, n are non-negative integers with base-p representation $m = m_r p^r + m_{r-1}p^{r-1} + \cdots + m_1 p + m_0 = (m_r, m_{r-1}, \ldots, m_0)_p$, $n = n_r p^r + n_{r-1}p^{r-1} + \cdots + n_1 p + n_0 = (n_r, n_{r-1}, \ldots, n_0)_p$, where $0 \le m_j, n_j \le p-1$ for each $0 \le j \le r$, then $\binom{m}{n} \equiv \prod_{j=0}^{r} \binom{m_j}{n_j} \pmod p$. Therefore, $\binom{m}{n} \not\equiv 0 \pmod p$ if and only if there is no carrying between the addition of n and $m-n$ in base-p representation. For an example of the application of Lucas's Theorem in estimating the number of directions determined by a point set in $AG(2, p^2)$, we refer to [10].

Furthermore, if we are working on $\mathbb{F}_q$, there must be some restriction on the sets A, B so that we can conclude something similar to Theorem 1.4. This is because if E is a proper subfield of $\mathbb{F}_q$, and $A - A, B - B \subset E$, then all the directions determined by $A \times B \subset AG(2, q)$ are in $E \cup \{\infty\}$, and thus $|D| \le |E| + 1$. Then the inequality $|A||B| - \min\{|A|, |B|\} + 2 \le |D| \le |E| + 1$ fails to hold when $|A|, |B| \ge \sqrt{|E|} + 1$.

We will show that for given A and $|B|$, it is very likely that the number of directions determined by $A \times B$ is close to $|A||B|$. The precise statement is given in the following theorem, which is our first main result, to be proved in Section 4.

Theorem 1.7. *Let $p \ge 3$ and $q = p^s$ be a prime power. Suppose $m \ge n \ge p$ and $k = q - mn > 0$. Then for any $A \subset \mathbb{F}_q$ with $|A| = m$, if we choose an n-element set B from $\mathbb{F}_q$ uniformly at random, we have*

$$\Pr\left[\#\{\textit{directions in } A\times B\} \ge \frac{p-2}{p-1}(m-1)n+2\right] \ge 1-\frac{(q+(p-2)k-n)(q-1)^{n-2}}{(p-1)(q-1)\cdots(q-n+1)}.$$

Note that when k is small compared to q, the lower bound of the above probability behaves like $\frac{p-2}{p-1}$. Compared to Theorem 1.3, we see that the lower bound on $|D|$ can be improved greatly when the point set is a Cartesian product. Recall that Theorem 1.2 states that for a point set $U \subset AG(2, q)$, such that $|U|$ is close to q (i.e., $k = q - |U|$ is small), there are two possibilities. The first one is the desired scenario, where we can conclude that the point set U determines many directions. However, Theorem 1.2 does not predict how likely the desired scenario will happen. Theorem 1.7 gives us further insights in the conclusion of Theorem 1.2. It implies that the desired scenario is very likely to occur, provided the point set U is a Cartesian product $A \times B$.

1.3. Clique Number of Paley Graphs and Generalized Paley Graphs

For an undirected graph G, the *clique number* of G, denoted by $\omega(G)$, is the size of a maximum clique of G. Finding a reasonably good upper bound of the clique

number of a Paley graph remains to be an open problem in additive combinatorics [6]. In the second half of the paper, we will discuss how to get improved upper bounds on the clique number of generalized Paley graphs over $\mathbb{F}_q$.

We first define the (standard) Paley graph. Suppose p a prime, such that $q = p^s \equiv 1 \pmod 4$. The *Paley graph* on $\mathbb{F}_q$, denoted by P_q, is the undirected graph whose vertices are elements in $\mathbb{F}_q$, such that two vertices are adjacent if and only if the difference of the two vertices is a square in $\mathbb{F}_q$. The trivial upper bound for $\omega(P_q)$ is $\sqrt{q}$. And when q is a square, the trivial upper bound is tight [4].

For the case $q = p$, the current best result is the clique number of P_p is at most $\sqrt{\frac{p}{2}} + 1$, which was proved by Hanson and Petridis [11] using Stepanov's method. For the case that q is an odd power of p, it is harder to improve the trivial upper bound. In [2], Bachoc, Ruzsa, and Matolcsi showed that $\omega(P_q) \leq \sqrt{q} - 1$ for some non-squares q. In [22], the author extended the idea from Hanson and Petridis and improved the upper bound on $\omega(P_q)$ to $\min\left(p^r\left\lfloor\sqrt{\frac{p}{2}}\right\rfloor, \sqrt{\frac{q}{2}} + \frac{p^r+1}{4} + \frac{\sqrt{2p}}{32}p^{r-1}\right)$ for $q = p^{2r+1}$. For other relevant results on the clique number and other properties of Paley graphs, we refer to the introduction section of [22] and the survey paper [9].

Similarly one can define generalized Paley graphs. They were first introduced by Cohen [5] in 1988, and reintroduced by Lim and Praeger [14] in 2009. Let $d > 1$ be a positive integer. The *d-Paley graph* on $\mathbb{F}_q$, denoted by $GP(q, d)$, is the undirected graph whose vertices are elements in $\mathbb{F}_q$, where two vertices are adjacent if and only if the difference of the two vertices is a d-th power of x for some $x \in \mathbb{F}_q$. Note that 2-Paley graphs are just the standard Paley graphs. 3-Paley graphs are also called *cubic Paley graphs* [1].

One significant difference between Paley graphs and generalized Paley graphs is that when $d \geq 3$, d-Paley graphs lose some nice graph-theoretical properties that Paley graphs have (see [9, Section 3.3]). For example, Paley graphs are self-complementary and connected, while when $d \geq 3$, d-Paley graphs are not necessarily self-complementary or connected. This potentially makes it much more difficult to estimate the clique number of generalized Paley graphs.

Similar to Paley graphs, the trivial upper bound for $\omega\big(GP(q, d)\big)$ is also $\sqrt{q}$; see Lemma 5.2. Since there are only a few results on the estimates of the clique number of generalized Paley graphs, we will list all of them, and give some new bounds in Section 5. In particular, for certain d-Paley graphs over $\mathbb{F}_q$, we show that the clique number can be improved to $\sqrt{\frac{q}{d}}(1 + o(1))$; see Theorem 5.10 for the precise statement.

Our second main result is an improved upper bound on the clique number of the cubic Paley graph over $\mathbb{F}_q$. We show that $\omega\big(GP(q, 3)\big)$ can be improved to $0.769\sqrt{q} + 1$, unless the clique number is $\sqrt{q}$ for obvious reasons (in which case the subfield $\mathbb{F}_{\sqrt{q}}$ is a maximum clique).

Theorem 1.8. *Let $q \equiv 1 \pmod 6$. If q is not a square, then $\omega\big(GP(q, 3)\big) <$*

$0.718\sqrt{q}+1$. *If q is a square, then $\omega\big(GP(q,3)\big) = \sqrt{q}$ if $3 \mid (\sqrt{q}+1)$ and $\omega\big(GP(q,3)\big) < 0.769\sqrt{q}+1$ otherwise.*

1.4. Connection Between the Two Problems

The connection between the clique number of generalized Paley graphs of prime order and the number of directions determined by a Cartesian product in $AG(2,p)$ was first studied in [7]. In fact, it is straightforward to use Theorem 1.4 to recover the Hanson-Petridis bound (Theorem 5.7) by the following observation: if C is a clique of $GP(p,d)$, then the direction set determined by $C \times C \subset AG(2,p)$ is

$$D = \frac{C-C}{C-C} \subset (\mathbb{F}_p^*)^d \cup \{0,\infty\}.$$

This implies that $|D| \leq \frac{p-1}{\gcd(d,p-1)} + 2$; combining this with the lower bound on $|D|$ given in Theorem 1.4, we can establish an upper bound on $|C|$.

It is clear that the same observation also works for $GP(q,d)$. Since we have obtained a similar result on $AG(2,q)$, we can also apply Theorem 1.6 to get an upper bound for generalized Paley graphs of prime power order. Unfortunately, for standard Paley graphs, the upper bound obtained in this way is much worse than the bound described in [22]. In Section 6, we will establish a slightly complicated idea, which leads to improved bounds on $\omega\big(GP(q,d)\big)$.

Let $\mathcal{P}$ be the set of primes. For positive integers r and d, we define $\mathcal{Q}_{r,d} = \{p \in \mathcal{P} : p^{2r+1} \equiv 1 \pmod{2d}\}$. In Section 6, utilizing an equidistribution result from analytic number theory, we obtain our third main result in this paper.

Theorem 1.9. *Let h be a positive function such that $h(x) = o(x)$ as $x \to \infty$. Let r, d be positive integers such that $d \geq 3$. Then $\omega\big(GP(p^{2r+1},d)\big) \leq p^{r+1/2} - h(p)$ for almost all $p \in \mathcal{Q}_{r,d}$.*

2. Rédei Polynomials With Szőnyi's Extension

We mentioned that Rédei polynomials are the main tools to estimate the size of the direction set in the introduction section. We begin by defining Rédei polynomials.

2.1. Rédei Polynomials

Let $A = \{a_1, a_2, \ldots, a_m\}$ and $B = \{b_1, b_2, \ldots, b_n\}$ be subsets of $\mathbb{F}_q$. The Rédei polynomial of $A \times B \subset AG(2,q)$ is defined as

$$H(x,y) = \prod_{i=1}^{m}\prod_{j=1}^{n}(x + a_i y - b_j).$$

For each $y \in \mathbb{F}_q$, define $A_y := A_y(B) = \{-a_i y + b_j : 1 \le i \le m, 1 \le j \le n\}$, as a multiset. Note that $x^q - x = \prod_{z \in \mathbb{F}_q}(x - z)$, so $H(x, y)$ divides $x^q - x$ if and only if the elements of A_y are all distinct, which is equivalent to $y \notin D$. We can write

$$H(x,y) = \sum_{t=0}^{mn} (-1)^{mn-t} \sigma_{mn-t}(A_y) x^t = x^{mn} - \sigma_1(A_y) x^{mn+1} + \cdots + (-1)^{mn} \sigma_{mn}(A_y),$$

where $\sigma_j(A_y)$, $j = 1, 2, \cdots, mn$, are elementary symmetric polynomials on the multiset A_y. When $y \notin D$, Szőnyi (see for example [21]) extended Rédei polynomial by introducing the polynomial $F(x, y) = (x^q - x)/H(x, y)$, where

$$F(x,y) = x^k - \sigma_1(\mathbb{F}_q \setminus A_y) x^{k-1} + \sigma_2(\mathbb{F}_q \setminus A_y) x^{k-2} + \cdots + (-1)^m \sigma_k(\mathbb{F}_q \setminus A_y). \quad (1)$$

Note that for each $0 \le t \le k$, $\sigma_t(A_y)$ is well-defined for a multiset A_y. However, it is not clear what is the meaning of $\sigma_t(\mathbb{F}_q \setminus A_y)$ for a multiset A_y. Next we follow the same idea in [21] to show that it can be defined using a recurrence relation.

Observe that, when $y \notin D$, for each $1 \le t \le k$, we have

$$\sum_{j=0}^{t} \sigma_j(A_y) \sigma_{t-j}(\mathbb{F}_q \setminus A_y) = 0.$$

Therefore, for $y \notin D$, we have the following recurrence relation for $\sigma_t(\mathbb{F}_q \setminus A_y)$:

$$\sigma_0(\mathbb{F}_q \setminus A_y) = 1,$$

$$\sigma_t(\mathbb{F}_q \setminus A_y) = -\sum_{j=1}^{t} \sigma_j(A_y) \sigma_{t-j}(\mathbb{F}_q \setminus A_y), \quad 1 \le t \le k.$$

In this way, we see that $\sigma_t(\mathbb{F}_q \setminus A_y)$ is a polynomial in y with degree at most t, and can be extended to be defined on all $y \in \mathbb{F}_q$. In this way, we can also extend $F(x, y)$ to be defined on all $y \in \mathbb{F}_q$ via the equation (1). Let

$$H(x,y)F(x,y) = x^q + h_1(y) x^{q-1} + h_2(y) x^{q-2} + \cdots + h_q(y), \quad (2)$$

and let $c_i = h_i(0)$ for each $1 \le i \le q$. then $\deg(h_i) \le i$. Next, we shall see how $H(x, y)$ and $F(x, y)$ can be used to obtain a lower bound on $|D|$. The proof of the following lemma is contained in Section 2 and Section 3 of [7]. Here we include the proof for the sake of completeness.

Lemma 2.1. *If $c_i \neq 0$ for some $1 \le i \le q$, then $|D| \ge q + 1 - i$.*

Proof. By the definition of the symmetric polynomials $\sigma_t(A_y)$ and $\sigma_t(\mathbb{F}_q \setminus A_y)$, we have $\deg(h_i) \le i$. By definition, when $y \notin D$, $H(x, y)F(x, y) = x^q - x$, so we have $h_i(y) = 0$ for all $y \notin D$. Since there are $q + 1$ directions in $AG(2, q)$, and $\infty \in D$,

there are $q+1-|D|$ directions not in D, and all such directions are in $\mathbb{F}_q$. This implies that $h_i \equiv 0$ for all $i < q+1-|D|$. Equivalently, if $h_i \not\equiv 0$ for some $1 \le i \le q$, then $|D| \ge q+1-i$. We proceed by setting $y=0$ in equation (2):

$$H(x,0)F(x,0) = F(x,0)\prod_{j=1}^{n}(x-b_j)^m = x^q + c_1x^{q-1} + c_2x^{q-2} + \cdots + c_q. \quad (3)$$

So if $c_i \neq 0$ for some $1 \le i \le q$, then $h_i \not\equiv 0$ and $|D| \ge q+1-i$. □

In [7], Lemma 1.5 and Lemma 2.1 are combined to prove Theorem 1.4. As we pointed out in the introduction, Lemma 1.5 is not strong enough for the application in $AG(2,q)$.

2.2. Explicit Formulas

For our purpose, we would like to find an explicit formula for the symmetric polynomial $\sigma_t(\mathbb{F}_q \setminus A_y)$. Recall that $A_0 = A_0(B)$ is the multiset $\{b_j : 1 \le i \le m, 1 \le j \le n\} = \cup_{j=1}^{n}\{b_j, b_j, \ldots, b_j\}$, where each b_j appears m times. Next we revisit the the recurrence relation defined above. For example, when $t = 1, 2$, we have

$$\begin{aligned}
\sigma_1\big(\mathbb{F}_q \setminus A_0(B)\big) &= -\sigma_1\big(A_0(B)\big) = -m\sum_{j=1}^{n} b_j = \binom{-m}{1}\sum_{j=1}^{n} b_j,\\
\sigma_2\big(\mathbb{F}_q \setminus A_0(B)\big) &= -\sigma_2\big(A_0(B)\big) - \sigma_1\big(A_0(B)\big)\sigma_1\big(\mathbb{F}_q \setminus A_0(B)\big)\\
&= -\sum_{1\le i<j\le n} m^2 b_ib_j - \binom{m}{2}\sum_{j=1}^{n} b_j^2 + m^2(\sum_{j=1}^{n} b_j)^2\\
&= m^2\sum_{1\le i<j\le n} b_ib_j + \frac{m(m+1)}{2}\sum_{j=1}^{n} b_j^2\\
&= \binom{-m}{1}\binom{-m}{1}\sum_{1\le i<j\le n} b_ib_j + \binom{-m}{2}\sum_{j=1}^{n} b_j^2.
\end{aligned}$$

A pattern on the binomial coefficient could be conjectured based on the above computation, and we verify that in the following two lemmas.

Lemma 2.2. *If $1 \le r \le n$, $b_1 = b_2 = \cdots = b_r = 1$ and $b_{r+1} = b_{r+2} = \cdots = b_n = 0$, then for each $1 \le t < q$, $\sigma_t(\mathbb{F}_q \setminus A_0) = \binom{-mr}{t}$.*

Proof. We prove the statement by induction on t. For $t = 1$,

$$\sigma_1(\mathbb{F}_q \setminus A_0) = -\sigma_1(A_0) = -\binom{mr}{1} = \binom{-mr}{1}.$$

Suppose that the statement is true for $t < l$, where $l \geq 2$; then by the recurrence relation, we have

$$\begin{aligned}\sigma_l(\mathbb{F}_q \setminus A_0) &= -\sigma_l(A_0) - \sum_{j=1}^{l-1} \sigma_j(A_0)\sigma_{l-j}(\mathbb{F}_q \setminus A_0) \\ &= -\binom{mr}{l} - \sum_{j=1}^{l-1} \binom{mr}{j}\binom{-mr}{l-j} \\ &= -\sum_{j=1}^{l} \binom{mr}{j}\binom{-mr}{l-j}.\end{aligned}$$

By the Chu–Vandermonde identity for binomial coefficients,

$$\sum_{j=0}^{l} \binom{mr}{j}\binom{-mr}{l-j} = \binom{mr+(-mr)}{l} = 0,$$

so it follows that

$$\begin{aligned}\sigma_l(\mathbb{F}_q \setminus A_0) &= 0 - \sum_{j=1}^{l} \binom{mr}{j}\binom{-mr}{l-j} \\ &= \sum_{j=0}^{l} \binom{mr}{j}\binom{-mr}{l-j} - \sum_{j=1}^{l} \binom{mr}{j}\binom{-mr}{l-j} \\ &= \binom{-mr}{l}.\end{aligned}$$

□

Lemma 2.3. *$\sigma_t\big(\mathbb{F}_q \setminus A_0(B)\big)$ is a homogeneous symmetric polynomial in b_j's with degree t.*

Proof. From the definition of $\sigma_t\big(A_0(B)\big)$, it is either the zero polynomial or a homogeneous symmetric polynomial in b_j's, with degree t. Then from the recurrence relation, inductively it is easy to show $\sigma_t\big(\mathbb{F}_q \setminus A_0(B)\big)$ is either the zero polynomial, or a homogeneous symmetric polynomial in b_j's with degree t. By Lemma 2.2, if $b_1 = b_2 = \cdots = b_n = 1$, then by Lucas's Theorem,

$$\sigma_t\big(\mathbb{F}_q \setminus A_0(B)\big) = \binom{-mn}{t} = (-1)^t\binom{mn+t-1}{t} = (-1)^t\binom{q-1}{t} \neq 0.$$

So $\sigma_t\big(\mathbb{F}_q \setminus A_0(B)\big)$ is not the zero polynomial, and the statement follows. □

Define

$$f_{m,t}(b_1, b_2, \ldots, b_n) = \sigma_t\big(\mathbb{F}_q \setminus A_0(B)\big).$$

Note that $f_{m,t}$ does not depend on A, and $f_{m,t}$ is a homogeneous symmetric polynomial with degree t. Recall that for our purpose, we assume $b_n = 0$. We would like to study the distribution of roots of $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0)$, so we first need to check if this is a zero polynomial or not. If $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0)$ is the zero polynomial, then all terms in $f_{m,t}$ without r_n have zero coefficients. Since $f_{m,t}$ is symmetric, this implies that all terms in $f_{m,t}$ have zero coefficients except those terms with factors $r_1 r_2 \cdots r_n$. In particular, this implies the following corollary.

Corollary 2.4. *If $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0)$ is the zero polynomial, then $t \geq n$.*

We will give an efficient algorithm to check whether $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0)$ is the zero polynomial in the beginning of Section 4.

Now we are ready to find an explicit formula for $\sigma_t\big(\mathbb{F}_q \setminus A_0(B)\big)$.

Theorem 2.5. *For each $1 \leq t < q$,*

$$\sigma_t\big(\mathbb{F}_q \setminus A_0(B)\big) = \sum_{\substack{r_1+r_2+\cdots+r_n=t \\ r_i \geq 0}} \prod_{i=1}^{n} \binom{-m}{r_i} b_i^{r_i}.$$

Proof. We prove the statement by induction on t. For each $t \geq 0$, by the definition of $\sigma_t(A_0)$, we have

$$\sigma_t\big(A_0(B)\big) = \sum_{\substack{\sum_{i=1}^{n} l_i = t \\ l_i \geq 0}} \prod_{i=1}^{n} \binom{m}{l_i} b_i^{l_i}.$$

For $t = 1$, the statement is true since

$$\sigma_1\big(\mathbb{F}_q \setminus A_0(B)\big) = -m\Big(\sum_{i=1}^{n} b_i\Big) = \sum_{i=1}^{n} \binom{-m}{1} b_i.$$

Suppose that the statement is true for $t < t_0$, where $t_0 \geq 2$; then for $t = t_0$, by the recurrence relation and inductive hypothesis, we have

$$\begin{aligned}
&\sum_{\substack{\sum_{i=1}^{n} r_i = t \\ r_i \geq 0}} \prod_{i=1}^{n} \binom{-m}{r_i} b_i^{r_i} - \sigma_t\big(\mathbb{F}_q \setminus A_0(B)\big) \\
&= \sum_{\substack{\sum_{i=1}^{n} r_i = t \\ r_i \geq 0}} \prod_{i=1}^{n} \binom{-m}{r_i} b_i^{r_i} + \sigma_t\big(A_0(B)\big) + \sum_{j=1}^{t-1} \sigma_j\big(A_0(B)\big)\sigma_{t-j}\big(\mathbb{F}_q \setminus A_0(B)\big) \\
&= \sum_{j=0}^{t} \sum_{\substack{\sum_{i=1}^{n} l_i = j \\ l_i \geq 0}} \prod_{i=1}^{n} \binom{m}{l_i} b_i^{l_i} \sum_{\substack{\sum_{i=1}^{n} r_i = t-j \\ r_i \geq 0}} \prod_{i=1}^{n} \binom{-m}{r_i} b_i^{r_i}
\end{aligned}$$

$$= \sum_{\substack{\sum_{i=1}^n (l_i+r_i)=t \\ l_i,r_i\geq 0}} \prod_{i=1}^n \binom{m}{l_i}\binom{-m}{r_i} b_i^{l_i+r_i}$$

$$= \sum_{\substack{\sum_{i=1}^n t_i=t \\ t_i\geq 0}} \sum_{0\leq l_i\leq t_i} \prod_{i=1}^n \binom{m}{l_i}\binom{-m}{t_i-l_i} b_i^{t_i}$$

$$= \sum_{\substack{\sum_{i=1}^n t_i=t \\ t_i\geq 0}} \prod_{i=1}^n b_i^{t_i}\Big(\sum_{l_i=0}^{t_i} \binom{m}{l_i}\binom{-m}{t_i-l_i}\Big).$$

By Chu–Vandermonde identity, for each $1 \leq i \leq n$ and each $t_i \geq 0$,

$$\sum_{l_i=0}^{t_i} \binom{m}{l_i}\binom{-m}{t_i-l_i} = \binom{m+(-m)}{t_i} = \binom{0}{t_i} = \begin{cases} 0 & t_i > 0 \\ 1 & t_i = 0 \end{cases}.$$

If $t_i \geq 0$ for each $1 \leq i \leq n$, and $\sum_{i=1}^n t_i = t \geq 2$, then there exists i_0 such that $t_{i_0} \geq 1$, so we have $\prod_{i=1}^n \binom{0}{t_i} = 0$. It follows that

$$\sum_{\substack{\sum_{i=1}^n r_i=t \\ r_i\geq 0}} \prod_{i=1}^n \binom{-m}{r_i} b_i^{r_i} - \sigma_t\big(\mathbb{F}_q \setminus A_0(B)\big) = \sum_{\substack{\sum_{i=1}^n t_i=t \\ t_i\geq 0}} \prod_{i=1}^n \binom{0}{t_i} b_i^{t_i} = 0. \qquad \square$$

Corollary 2.6. *For each $1 \leq t < q$,*

$$f_{m,t}(b_1, b_2, \ldots, b_{n-1}, 0) = (-1)^t \sum_{\substack{t_1+t_2+\cdots+t_{n-1}=t \\ t_i\geq 0}} \prod_{i=1}^{n-1} \binom{m+t_i-1}{m-1} b_i^{t_i}.$$

Proof. This follows immediately from Theorem 2.5 and

$$\binom{-m}{t_i} = (-1)^{t_i}\binom{m+t_i-1}{t_i} = (-1)^{t_i}\binom{m+t_i-1}{m-1}. \qquad \square$$

3. Directions Determined by a Cartesian Product in $AG(2, q)$

In this section, we will prove Theorem 1.6, and give some corollaries. We begin by giving a stronger version of Lemma 1.5.

Lemma 3.1. *Let $q = p^s$ be a prime power. Let $R, S \in \mathbb{F}_q[x]$ be non-constant polynomials each with constant term 1. Suppose that R and R' are relatively prime, where R' is the formal derivative of R. Assume that $m, n \geq 2$, $k = q - mn > 0$, $\deg R = n - 1$, and $\deg S = k - l$ for some integer $0 \leq l \leq k$. Assume that one of the following conditions is satisfied:*

1. *Every integer between m and $m + \lfloor \frac{k-l}{n-1} \rfloor$ is not a multiple of p.*
2. *$p \nmid (m + l)$.*

Then $x^{\deg R+\deg S+1}$ does not divide $R^m(x)S(x) - 1$.

Proof. We use proof by contradiction. Suppose there exists a polynomial $P(x) \in \mathbb{F}_q[x]$ such that

$$R^m(x)S(x) = 1 + x^{\deg R+\deg S+1}P(x). \tag{4}$$

Let r be the highest power of R dividing S; then $0 \le r \le \lfloor \frac{k-l}{n-1} \rfloor$. Let $T = \frac{S}{R^r}$; then R does not divide T, and we have

$$R^{m+r}(x)T(x) = 1 + x^{\deg R+\deg S+1}P(x) = 1 + x^{n+k-l}P(x). \tag{5}$$

By differentiating (5), we obtain

$$R^{m+r-1}(x)\big((m+r)R'(x)T(x)+R(x)T'(x)\big) = x^{n+k-l-1}\big((n+k-l)P(x)+xP'(x)\big).$$

Since the constant term in $R^{m+r-1}(x)$ is 1, we see that $x^{n+k-l-1}$ divides $(m + r)R'(x)T(x) + R(x)T'(x)$. But the degree of $(m + r)R'(x)T(x) + R(x)T'(x)$ is at most $n + k - l - 2$, so we must have

$$(m + r)R'(x)T(x) + R(x)T'(x) = (n + k - l)P(x) + xP'(x) = 0.$$

Since R and R' are relatively prime, then $R(x) \mid (m + r)T(x)$. Since R does not divide T, we must have $m + r = 0$ in $\mathbb{F}_q$, i.e., $p \mid (m + r)$. Note that $m \le m + r \le m + \lfloor \frac{k-l}{n-1} \rfloor$, so there is a integer between m and $m + \lfloor \frac{k-l}{n-1} \rfloor$ which is a multiple of p. Moreover, we must also have $R(x)T'(x) = 0$. Since $\mathbb{F}_q[x]$ is an integral domain, and $R(x)$ has constant term 1, then it follows that $T'(x) = 0$. Therefore $T(x) = g(x^p)$ for some polynomial $g \in \mathbb{F}_q[x]$, and in particular,

$$p \mid \deg T = \deg S - r \deg R = k - l - r(n - 1) = q - mn - l - r(n - 1).$$

Combining with $p \mid (m + r)$, we obtain that $p \mid (m + l)$. □

We remark that we actually proved a slightly stronger statement: if $p \nmid (m + r)$ or $p \nmid (m+l)$, where r is the highest power of R dividing S, then $x^{\deg R+\deg S+1}$ does not divide $R^m(x)S(x) - 1$. However, the exact value of r is difficult to compute without knowing the explicit factorizations of polynomials R and S, which is indeed the case in our application.

Lemma 2.1, Lemma 3.1 can be combined to prove Theorem 1.6.

Proof of Theorem 1.6. We will consider equation (1) and (3). Suppose that $c_1 = c_2 = \cdots = c_{k+n-l-1} = 0$. Set $R(y) = \prod_{j=1}^{n-1}(1 - b_j y)$, and $S(y) = y^k F(y^{-1}, 0)$. Then $R(y), S(y) \in \mathbb{F}_q[y]$, and $\deg R = n-1$. Note that $f_{m,0}(b_1, b_2, \ldots, b_{n-1}, 0) = 1$,

since l is the smallest non-negative integer such that $f_{m,k-l}(b_1, b_2, \ldots, b_{n-1}, 0) \neq 0$, then $l \leq k$, and $\deg S = k - l$. Substitute $x = y^{-1}$ and multiply by y^q in equation (3) to obtain

$$R^m(y)S(y) = 1 + c_1 y + c_2 y^2 + \cdots + c_q y^q = 1 + y^{k+n-l}U(y), \tag{6}$$

for some polynomial $U(y) \in \mathbb{F}_q[y]$. Since the elements of B are distinct, all roots of R have multiplicity 1, and R is relatively prime to R'. However, given one of the conditions in the statement, equation (6) is impossible to hold in view of Lemma 3.1. It follows that at least one of $c_1, \ldots, c_{k+n-l-1}$ is nonzero, and thus by Lemma 2.1, there are at least $q - (k+n-l-1) + 1 = mn - n + l + 2$ directions determined by $A \times B$. □

In particular, when $q = p$, we get a slightly stronger version of Theorem 1.4.

Corollary 3.2. *Let p be a prime. Let $m \geq n \geq 2$ be integers such that $k = p - mn > 0$. Let $A, B \subset \mathbb{F}_p$ with $|A| = m$ and $|B| = n$, and write $B = \{b_1, b_2, \ldots, b_{n-1}, 0\}$. Suppose l is the smallest non-negative integer such that $f_{m,k-l}(b_1, b_2, \ldots, b_{n-1}, 0) \neq 0$; then the number of directions determined by the set $A \times B \subset AG(2, p)$ is at least $mn - n + l + 2$.*

Proof. Note that $l \leq k$, so $0 < m + l \leq m + k < 2m + k \leq mn + k = p$. This implies that $p \nmid (m + l)$. So by Theorem 1.6, the number of directions determined by the set $A \times B$ is at least $mn - n + l + 2$. □

The following are some special cases where we can conclude the same lower bound on the number of directions without any additional assumptions.

Corollary 3.3. *Let p be a prime. Let m, n be integers such that $2 \leq m < p < n$ and $k = p^2 - mn > 0$. Let $A, B \subset \mathbb{F}_{p^2}$ with $|A| = m$ and $|B| = n$. Then the number of directions determined by the set $A \times B \subset AG(2, p^2)$ is at least $mn - n + 2$.*

Proof. We have

$$m + \left\lfloor \frac{k}{n-1} \right\rfloor \leq m + \left\lfloor \frac{p^2 - mn}{n-1} \right\rfloor = \left\lfloor \frac{p^2 - m}{n-1} \right\rfloor \leq \left\lfloor \frac{p^2 - 2}{p} \right\rfloor < p.$$

So by Theorem 1.6, the number of directions is at least $mn - n + 2$. □

Corollary 3.4. *Let $q = p^s$ be a prime power. Let $A, B \subset \mathbb{F}_q$ with $|A| = m, |B| = n$, where $m, n \geq 2$ are integers such that $p \nmid m$ and $0 < k = q - mn < n - 1$. Then the number of directions determined by the set $A \times B \subset AG(2, q)$ is at least $mn - n + 2$. In particular, if $p \nmid m$, $2 \leq m \leq \sqrt{q} - 1$, and $n = \lfloor \frac{q}{m} \rfloor$, then the number of directions determined by the set $A \times B \subset AG(2, q)$ is at least $mn - n + 2$.*

Proof. Let l be the smallest non-negative integer such that $f_{m,k-l}(b_1, b_2, \ldots, b_{n-1}, 0) \neq 0$. Since $\lfloor \frac{k-l}{n-1} \rfloor \leq \lfloor \frac{k}{n-1} \rfloor = 0$, and $p \nmid m$, then the condition (1) in Theorem 1.6 is satisfied, so the number of directions is at least $mn - n + 2$. In particular, if $p \nmid m$, and $m \geq 2$, then $m \nmid q$, and thus $0 < q - mn = k < m$. Since $m \leq \lfloor \sqrt{q} \rfloor - 1$, then $n \geq \lfloor \sqrt{q} \rfloor + 1 \geq m + 2$. Thus $k < n - 1$, and the conclusion follows. □

4. Number of Roots of $f_{m,k}(r_1, r_2, \ldots, r_{n-1}, 0)$

To apply Theorem 1.6, it is crucial to understand when is $f_{m,k}(b_1, b_2, \ldots, b_{n-1}, 0) = 0$. In particular, one needs to identify whether $f_{m,k}(r_1, r_2, \ldots, r_{n-1}, 0) \equiv 0$. Recall Corollary 2.4 says that $f_{m,k}(r_1, r_2, \ldots, r_{n-1}, 0) \equiv 0$ could happen only when $k \geq n$.

4.1. Polynomial Identity Testing

In general, we can use the Schwartz–Zippel Lemma as a tool to design a randomized algorithm to test whether a given multivariate polynomial is the zero polynomial (see for example [19]). However, since we have worked out the explicit formula in Corollary 2.6, we have the following deterministic and efficient algorithm, Algorithm 1, to check whether $f_{m,k}(r_1, r_2, \ldots, r_{n-1}, 0) \equiv 0$. We need the following simple lemma as a preparation.

Lemma 4.1. *Let $d \geq 2$ be a fixed positive integer. Suppose $k \geq 0$ and $a_0, a_1, \ldots, a_k \geq 0$ such that $A := a_0 + a_1 d + a_2 d + \ldots + a_k d^k > d^{k+1}$, then there exist $b_0, b_1, \ldots, b_k$ such that $0 \leq b_j \leq a_j$ for each $0 \leq j \leq k$, and $b_0 + b_1 d + b_2 d + \ldots + b_k d^k = A - d^{k+1}$.*

Proof. We prove by inducting on k. The case $k = 0$ is trivial. Suppose $k \geq 1$ and $a_0, a_1, \ldots, a_k \geq 0$ such that $A := a_0 + a_1 d + a_2 d + \ldots + a_k d^k > d^{k+1}$. If $a_k \geq d$, then we can set $b_j = a_j$ for $0 \leq j \leq k-1$ and $b_k = a_k - d$ so that $b_0 + b_1 d + b_2 d + \ldots + b_k d^k = A - d^{k+1}$. Next assume $a_k < d$, and let $l = d - a_k$, $b_k = 0$. Let $B = a_0 + a_1 d + a_2 d + \ldots + a_{k-1} d^{k-1}$, then $B > l d^k$. By inductive hypothesis, there exists $b_0, b_1, \ldots, b_{k-1}$ such that $0 \leq b_j \leq a_j$ for each $0 \leq j \leq k-1$, and $b_0 + b_1 d + b_2 d + \ldots + b_{k-1} d^{k-1} = B - l d^k$. Then it follows that $b_0 + b_1 d + b_2 d + \ldots + b_{k-1} d^{k-1} + b_d^k = B - l d^k = A - (a_k + l) d^k = A - d^{k+1}$. □

Proposition 4.2. *Suppose $1 \leq t < q$. Let $m - 1 = (m_{s-1}, m_{s-2}, \ldots, m_0)_p$, and $t = (h_{s-1}, h_{s-2}, \ldots, h_0)_p$ be the base-p representation of $m - 1$ and t, respectively. The following algorithm can detect whether $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0) \equiv 0$. Moreover, the running time is $O(\log q)$.*

Algorithm 1: Check whether $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0)$ is the zero polynomial.

```
S_0 ← 0
for j ← 0 to s − 1 do
    S_j ← S_j + (n − 1)(p − 1 − m_j)
    if S_j < h_j then
        return "zero polynomial"
    else
        S_{j+1} ← ⌊(S_j − h_j)/p⌋
return "nonzero polynomial"
```

Proof. It is clear that the running time of the above algorithm is $O(s) = O(\log q)$. By Corollary 2.6, $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0)$ is not the zero polynomial if and only if there exist $t_1, t_2, \ldots, t_{n-1} \geq 0$ such that

$$\sum_{i=1}^{n-1} t_i = t, \prod_{i=1}^{n-1} \binom{m-1+t_i}{m-1} \not\equiv 0 \pmod{p}. \tag{7}$$

Note that $t < q = p^s$. Fix $T_0, T_1, \ldots, T_{s-1} \geq 0$. Let $t_1, t_2, \ldots, t_{n-1}$ be such that $0 \leq t_i < q$, with base-p representations $t_i = (g_{s-1,i}, g_{s-2,i}, \ldots, g_{0,i})_p$ for each $1 \leq i \leq n-1$ satisfying $T_j = \sum_{i=0}^{n-1} g_{j,i}$ for each $0 \leq j \leq s-1$. By Lucas's Theorem, $\binom{m-1+t_i}{m-1} \not\equiv 0 \pmod{p}$ if and only if there is no carrying in the addition of $m-1$ and t_i in the base-p representation. Therefore, $\prod_{i=1}^{n-1} \binom{m-1+t_i}{m-1} \not\equiv 0 \pmod{p}$ if and only if $g_{j,i}$ takes value between 0 and $p-1-m_j$ for each $1 \leq i \leq n-1$ and $0 \leq j \leq s-1$. It follows that there exist $t_1, t_2, \ldots, t_{n-1}$ such that $0 \leq t_i < q$ and $\prod_{i=1}^{n-1} \binom{m-1+t_i}{m-1} \not\equiv 0 \pmod{p}$ if and only if $T_j \leq (n-1)(p-1-m_j)$ for each $0 \leq j \leq s-1$.

Let

$$T_0 + T_1 p + T_2 p^2 + \ldots + T_{s-1} p^{s-1} = R_0 + R_1 p + R_2 p^2 + \ldots + R_{s-1} p^{s-1} + R_s p^s,$$

where $0 \leq R_j < p$ for each $0 \leq j \leq s-1$, and $R_s \geq 0$. Note that

$$T_0 + T_1 p + T_2 p^2 + \ldots + T_{s-1} p^{s-1} = \sum_{i=1}^{n-1} t_i \equiv t \pmod{q}$$

is equivalent to

$$\sum_{i=1}^{n-1} t_i \equiv t \pmod{p}, \sum_{i=1}^{n-1} t_i \equiv t \pmod{p^2}, \ldots, \sum_{i=1}^{n-1} t_i \equiv t \pmod{p^s}.$$

Therefore, there exist $t_1, t_2, \ldots, t_{n-1}$ such that $0 \leq t_i < q$ and $\sum_{i=1}^{n-1} t_i \equiv t \pmod{q}$ if and only if $R_j = h_j$ for each $0 \leq j \leq s-1$.

It is clear that for each $0 \le j \le s-1$, the S_j computed in the above algorithm is exactly the maximum value of R_j provided $T_k \le (n-1)(p-1-m_k)$ for each $0 \le k \le j$ and $\sum_{i=1}^{n-1} t_i \equiv t \pmod{p^j}$, where $\lfloor \frac{S_j - h_j}{p} \rfloor$ is the maximum number of carries between the addition of $t_1, t_2, \ldots, t_{n-1}$ from p^j digit to the p^{j+1} digit. In particular, if equation (7) holds for $t_1, t_2, \ldots, t_{n-1}$, then $T_j \le (n-1)(p-1-m_j)$, and $S_j \ge R_j = h_j$ for each $0 \le j \le s-1$. Therefore, if $S_j < h_j$ for some $0 \le j \le s-1$, then $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0)$ is the zero polynomial, and Algorithm 1 correctly returns "zero polynomial".

Conversely, suppose Algorithm 1 returns "nonzero polynomial", then $S_j \ge h_j$ for each $0 \le j \le s-1$. Furthermore, there are $T_0, T_1, \ldots, T_{s-1}$ (which are maximized) such that $0 \le T_j \le (n-1)(p-1-m_j)$ for each j and

$$T_0 + T_1 p + T_2 p^2 + \ldots + T_{s-1} p^{s-1} = h_0 + h_1 p + h_2 p^2 + \ldots + h_{s-1} p^{s-1} + S_s p^s = t + S_s p^s$$

for $S_s = \lfloor \frac{S_{s-1} - h_{s-1}}{p} \rfloor \ge 0$ given in the Algorithm 1. Since $S_s \ge 0$, by Lemma 4.1, there exist $T_0', T_1', \ldots, T_{s-1}'$ such that $0 \le T_j' \le T_j$, and

$$T_0' + T_1' p + T_2' p^2 + \ldots + T_{s-1}' p^{s-1} = h_0 + h_1 p + h_2 p^2 + \ldots + h_{s-1} p^{s-1} = t.$$

It follows that there exist $t_1, t_2, \ldots, t_{n-1}$ such that $0 \le t_i < q$ and equation (7) holds. Therefore, $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0)$ is a nonzero polynomial, and Algorithm 1 returns the correct answer. □

Below we see a family of pairs (m, t) where Algorithm 1 returns "nonzero polynomial".

Corollary 4.3. *Let $m-1 = (m_{s-1}, m_{s-2}, \ldots, m_0)_p$, and $t = (h_{s-1}, h_{s-2}, \ldots, h_0)_p$ be the base-p representation of $m-1$ and t, respectively. If $m_j \ne p-1$ for each $0 \le j \le s-1$, and $n-1 \ge \max\{h_j : 0 \le j \le s-1\}$, then $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0)$ is a nonzero polynomial.*

Proof. For each $0 \le j \le s-1$, since $m_j \ne p-1$, we have $S_j \ge (n-1)(p-1-m_j) \ge n-1 \ge h_j$. Then by Proposition 4.2, $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0)$ is a nonzero polynomial. □

In particular, when $n \ge p$, we have $n-1 \ge \max\{h_j : 0 \le j \le s-1\}$. Thus, we obtain the following corollary.

Corollary 4.4. *If $n \ge p$ and the base-p representation of $m-1$ does not contain $p-1$, then $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0)$ is a nonzero polynomial.*

The conditions in the above corollary might not hold for all m, but m can be always reduced slightly to make that feasible.

Lemma 4.5. *If $p \geq 3$, then for any $2 \leq m < q$, there is $m' < m$ such that $(m'-1) \geq \frac{p-2}{p-1}(m-1)$, $p \nmid m'$ and the base-p representation of $m'-1$ does not contain $p-1$.*

Proof. Let $m-1 = (m_{s-1}, m_{s-2}, \ldots, m_0)_p$. Let j_0 be the largest integer such that $m_{j_0} = p-1$. Let $m' = 1 + (m_{s-1}, \ldots, m_{j_0+1}, p-2, \ldots, p-2)_p$. Then the base-$p$ representation of $m'-1$ does not contain $p-1$, $p \nmid m'$, and $m-1 \leq (m_{s-1}, \ldots, m_{j_0+1}, p-1, \ldots, p-1)_p$. So we have

$$\frac{m'-1}{m-1} \geq \frac{(m_{s-1}, \ldots, m_{j_0+1}, p-2, \ldots, p-2)_p}{(m_{s-1}, \ldots, m_{j_0+1}, p-1, \ldots, p-1)_p} \geq \frac{p-2}{p-1}. \qquad \square$$

We will use a combination of Corollary 4.4 and Lemma 4.5 to prove Theorem 4.10.

4.2. Upper Bounds on the Number of Roots

We aim to find a lower bound for the probability on $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0) \neq 0$. Schwartz–Zippel Lemma (see for example [19, Corollary 1]) is useful in bounding the number of roots of a nonzero multivariate polynomial.

Lemma 4.6 (Schwartz–Zippel Lemma)**.** *Let $g \in F[x_1, x_2, \ldots, x_n]$ be a non-zero polynomial with degree d over a field F. Let S be a finite subset of F and let $r_1, r_2, \ldots, r_n$ be selected at random independently and uniformly from S. Then*

$$\Pr[g(r_1, r_2, \ldots, r_n) = 0] \leq \frac{d}{|S|}.$$

Next, we use Schwartz–Zippel Lemma to bound the number of roots with distinct coordinates.

Proposition 4.7. *Let $1 \leq t < q$. Suppose $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0)$ is not the zero polynomial, if we choose a $(n-1)$-set $B' = \{b_1, b_2, \ldots, b_{n-1}\}$ from $\mathbb{F}_q^*$ uniformly at random, then*

$$\Pr[f_{m,t}(b_1, b_2, \ldots, b_{n-1}, 0) = 0] \leq \frac{t(q-1)^{n-2}}{(q-1)\cdots(q-n+1)}.$$

Proof. Since $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0)$ is not the zero polynomial, it is a symmetric polynomial with degree t. Let $S = \mathbb{F}_q^*$, then by Schwartz–Zippel Lemma, if we pick $r_1, r_2, \ldots, r_{n-1}$ from S independently and uniformly, we have

$$\Pr[f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0) = 0] \leq \frac{t}{q-1}.$$

So the number of $(n-1)$-tuples $(r_1, r_2, \ldots, r_{n-1}) \in S^{n-1}$ with $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0) = 0$ is at most $\frac{t}{q-1}(q-1)^{n-1} = t(q-1)^{n-2}$. If $f_{m,t}(b_1, b_2, \ldots, b_{n-1}, 0) = 0$, then

since $f_{m,t}$ is a symmetric polynomial, we also have $f_{m,t}(b_{\pi(1)}, b_{\pi(2)}, \ldots, b_{\pi(n-1)}, 0) = 0$ for any permutation $\pi \in \mathrm{Sym}(n-1)$. So the number of $(n-1)$-sets $B' = \{b_1, b_2, \ldots, b_{n-1}\}$ of $\mathbb{F}_q^*$ such that $f_{m,t}(b_1, b_2, \ldots, b_{n-1}, 0) = 0$ is at most $\frac{t(q-1)^{n-2}}{(n-1)!}$. Since the number of $(n-1)$-sets B' of $\mathbb{F}_q^*$ is $\binom{q-1}{n-1}$, if we choose a $(n-1)$-set B' from $\mathbb{F}_q^*$ uniformly at random, then

$$\Pr[f_{m,t}(b_1, b_2, \ldots, b_{n-1}, 0) = 0] \le \frac{t(q-1)^{n-2}}{(n-1)!\binom{q-1}{n-1}} = \frac{t(q-1)^{n-2}}{(q-1)\cdots(q-n+1)}. \quad \square$$

4.3. Proof of Theorem 1.7

In this subsection, we will prove Theorem 1.7. There are two different cases: $f_{m,k}(r_1, r_2, \ldots, r_{n-1}, 0) \equiv 0$ and $f_{m,k}(r_1, r_2, \ldots, r_{n-1}, 0) \not\equiv 0$.

If $f_{m,k}(r_1, r_2, \ldots, r_{n-1}, 0)$ is not the zero polynomial (which is the case when $k < n$, by Corollary 2.4), then by combining Theorem 1.6 and Proposition 4.7, we have the following estimate on the probability.

Theorem 4.8. *Let $q = p^s$ be a prime power. Let $m, n \ge 2$ be integers such that $k = q - mn > 0$. Suppose $p \nmid m$ and $f_{m,k}(r_1, r_2, \ldots, r_{n-1}, 0)$ is not the zero polynomial (in particular when $k < n$; in general, this can be checked efficiently by Algorithm 1 in $O(\log q)$ time). Then for any $A \subset \mathbb{F}_q$ with $|A| = m$, if we choose a n-set B from $\mathbb{F}_q$ uniformly at random, we have*

$$\Pr[\#\{\textit{directions in } A \times B\} \ge mn - n + 2] \ge 1 - \frac{k(q-1)^{n-2}}{(q-1)\cdots(q-n+1)}.$$

If $f_{m,k}(r_1, r_2, \ldots, r_{n-1}, 0)$ is indeed the zero polynomial, then in view of Theorem 1.6, we need to find the smallest positive integer l such that $f_{m,k-l}(r_1, r_2, \ldots, r_{n-1}, 0)$ is a nonzero polynomial. Recall that Corollary 2.4 states that $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0) \equiv 0$ could happen only when $t \ge n$, so such l exists. We can run Algorithm 1 to check that for each l using brute force, which takes at most $O(ks) = O(k \log q)$ time. In this way, by using Theorem 1.6 and Proposition 4.7 with $t = k - l$, we obtain the following theorem.

Theorem 4.9. *Let $q = p^s$ be a prime power. Let $m, n \ge 2$ be integers such that $k = q - mn > 0$. Suppose l is the smallest non-negative integer such that $f_{m,k-l}(r_1, r_2, \ldots, r_{n-1}, 0)$ is not the zero polynomial. If $p \nmid (m + l)$, then for any $A \subset \mathbb{F}_q$ with $|A| = m$, if we choose a n-set B from $\mathbb{F}_q$ uniformly at random, we have*

$$\Pr[\#\{\textit{directions in } A \times B\} \ge mn - n + 2] \ge 1 - \frac{(k-l)(q-1)^{n-2}}{(q-1)\cdots(q-n+1)}.$$

However, it is still possible that $p \mid (m + l)$. In which case our approach is to reduce the parameter m slightly to obtain a nonzero polynomial by the observation

in Corollary 4.4 and Lemma 4.5. Note that reducing m corresponds to discarding some elements from A, which only decreases the number of directions determined.

Theorem 4.10. *Let $p \geq 3$ and $q = p^s$ be a prime power. Let m, n be integers such that $m \geq n \geq p$ and $k = q - mn > 0$. Suppose l is the smallest non-negative integer such that $f_{m,k-l}(r_1, r_2, \ldots, r_{n-1}, 0)$ is not the zero polynomial. If $p \mid (m + l)$, then for any $A \subset \mathbb{F}_q$ with $|A| = m$, if we choose a n-set B from $\mathbb{F}_q$ uniformly at random, we have*

$$\Pr\left[\#\{\textit{directions in } A{\times}B\} \geq \frac{p-2}{p-1}(m{-}1)n{+}2\right] \geq 1{-}\frac{(q+(p-2)k-n)(q-1)^{n-2}}{(p-1)(q-1)\cdots(q-n+1)}.$$

Proof. By Lemma 4.5, there is $m' < m$ such that $(m'-1) \geq \frac{p-2}{p-1}(m-1)$, $p \nmid m'$ and the base-p representation of $m'-1$ does not contain $p-1$. Then $m' \geq 1 + \frac{p-2}{p-1} > 1$, so $m' \geq 2$. Let A' be any subset of A with $|A'| = m'$, then by Corollary 4.4, the polynomial $f_{m',k'}(r_1, r_2, \ldots, r_{n-1}, 0)$ associated to the set A' and $k' = q - m'n$, is a nonzero polynomial. Note that

$$k' = q{-}m'n \leq q{-}\frac{p-2}{p-1}(m{-}1)n{-}n = q{-}\frac{p-2}{p-1}\left(\frac{q-k}{n}{-}1\right)n{-}n = \frac{q+(p-2)k-n}{p-1}.$$

Since $p \nmid m'$, and $A' \subset A$, by Theorem 4.8, we have

$$\begin{aligned}
&\Pr\left[\#\{\text{directions in } A \times B\} \geq \frac{p-2}{p-1}(m-1)n + 2\right] \\
&\geq \Pr[\#\{\text{directions in } A' \times B\} \geq (m'-1)n + 2] \\
&\geq 1 - \frac{k'(q-1)^{n-2}}{(q-1)\cdots(q-n+1)}. \\
&\geq 1 - \frac{(q+(p-2)k-n)(q-1)^{n-2}}{(p-1)(q-1)\cdots(q-n+1)}.
\end{aligned}$$

□

In particular, if we do not bother with the exact value of l, then we can combine Theorem 4.9 and Theorem 4.10 to get a slightly weaker version, which is Theorem 1.7.

5. Clique Number of Generalized Paley Graphs

Let p be an odd prime and s a positive integer such that $q = p^s$. Recall that two vertices of $GP(q, d)$ are adjacent if and only if their difference is a d-th power. It is clear that if $\gcd(d, q-1) = \gcd(d', q-1)$, then $GP(q, d)$ and $GP(q, d')$ are isomorphic graphs since $\mathbb{F}_q^*$ is a cyclic group. So we can replace d by $\gcd(d, q-1)$, and assume $d \mid (q-1)$. Also note that in order for $GP(q, d)$ to be an undirected graph, we need -1 to be a d-th power in $\mathbb{F}_q^*$, i.e., $\frac{q-1}{d}$ to be an even number.

In the following discussion, we will always assume $d > 1$ and d is a divisor of $\frac{q-1}{2}$, or equivalently $q \equiv 1 \pmod{2d}$. Let $N = \omega\big(GP(q,d)\big)$ and let $C = \{v_1, v_2, \ldots, v_N\} \subset \mathbb{F}_q$ be a clique of maximum size in $GP(q,d)$. We are interested in finding a reasonably good lower and upper bound for the clique number.

5.1. Known Bounds

We begin by giving some trivial upper bounds for the clique number in the case $d \geq 3$.

Lemma 5.1. *If $q \equiv 1 \pmod{2d}$, then $\omega\big(GP(q,d)\big) \leq \frac{q-1}{d} + 1$.*

Proof. Note that $v_2 - v_1, v_3 - v_1, \ldots, v_N - v_1$ are distinct nonzero d-th powers in $\mathbb{F}_q^*$ and the number of d-th powers in $\mathbb{F}_q^*$ is $\frac{q-1}{d}$. So $\omega\big(GP(q,d)\big) \leq \frac{q-1}{d} + 1$. □

In the literature [2, 11, 22], the trivial upper bound on $\omega\big(GP(q,d)\big)$ is given by $\sqrt{q}$. Here we include a short proof for completeness.

Lemma 5.2. *If $q \equiv 1 \pmod{2d}$, then $\omega\big(GP(q,d)\big) \leq \sqrt{q}$.*

Proof. Let g be a be a primitive root of $\mathbb{F}_q^*$, and consider the set $W = \{v_i + gv_j : 1 \leq i, j \leq N\}$. Note that if $v_i + gv_j = v_i' + gv_j'$, then $v_i - v_i' = g(v_j' - v_j)$, which is impossible unless $i = i'$ and $j = j'$. So each element of W is different from the others. This means that $|W| = N^2 \leq q$, i.e., $N \leq \sqrt{q}$. □

In [5], Cohen proved the following theorem on the lower bound of clique number.

Theorem 5.3 ([5, Theorem 3])**.** *If $d \geq 3$ and $q \equiv 1 \pmod{2d}$, then $\omega\big(GP(q,d)\big) \geq \frac{p}{(p-1)\log d}(\frac{1}{2}\log q - 2\log\log q) - 1$.*

The lower bound Cohen obtained is of the order $\log q$, which is significantly smaller compared to the trivial upper bound. The following theorem shows that the lower bound can be greatly improved in certain cases.

Theorem 5.4 ([4, Theorem 1])**.** *Let $q \equiv 1 \pmod{2d}$, and let r be the largest integer such that $d \mid \frac{q-1}{p^r-1}$; then $\omega\big(GP(q,d)\big) \geq p^r$.*

Combining Theorem 5.4 and the trivial upper bound Lemma 5.2, we get the following.

Corollary 5.5. *If q is a square and $d \mid (\sqrt{q}+1)$, then $\omega\big(GP(q,d)\big) = \sqrt{q}$.*

This means that Lemma 5.2 gives the best trivial upper bound, in the sense that we cannot improve it without any additional assumption. Theorem 5.4 also implies that the lower bound $q^{1/d}$ can be obtained in the following cases.

Proposition 5.6. *If* $\gcd(d, \phi(d)) = 1$, $2d \mid (q-1)$ *and* $d \mid s$, *then* $\omega\big(GP(q,d)\big) \geq q^{1/d}$. *In particular, if* d *is a prime such that* $2d \mid (q-1)$ *and* $d \mid s$, *then* $\omega\big(GP(q,d)\big) \geq q^{1/d}$.

Proof. Let δ be the order of p modulo d. Then by Euler's Theorem, we have $d \mid (p^{\phi(d)} - 1)$, so $\delta \mid \phi(d)$ and $\gcd(\delta, d) = 1$ since $\gcd(d, \phi(d)) = 1$. On the other hand, since $d \mid (q-1)$, we have $\delta \mid s$. Now $d \mid s$ and $\gcd(\delta, d) = 1$ imply $\delta \mid \frac{s}{d}$, so $p^{s/d} \equiv 1 \pmod{d}$, and we have

$$\frac{q-1}{p^{s/d}-1} = \frac{p^s-1}{p^{s/d}-1} = 1 + p^{s/d} + p^{2s/d} + \cdots + p^{(d-1)s/d} \equiv d \equiv 0 \pmod{d}.$$

So by Theorem 5.4, we have $\omega\big(GP(q,d)\big) \geq p^{s/d} = q^{1/d}$. □

5.2. Stepanov's Method and Binomial Coefficients

In [11], Hanson and Petridis used Stepanov's method to improve the upper bound on $\omega\big(GP(p,d)\big)$. In [7], Di Benedetto, Solymosi, and White recovered the same bound.

Theorem 5.7 ([11, Corollary 1.5])**.** *Let* p *be a prime such that* $p \equiv 1 \pmod{2d}$, *then* $\omega^2\big(GP(p,d)\big) - \omega\big(GP(p,d)\big) \leq \frac{p-1}{d}$. *Equivalently,* $\omega\big(GP(p,d)\big) \leq \sqrt{\frac{p-1}{d} + \frac{1}{4}} + \frac{1}{2}$.

Note that both methods only work in prime fields. In [22], the author extended Hanson and Petridis' method to improve the trivial upper bound on the clique number of Paley graphs of prime power order, by carefully analyzing the binomial coefficients. Actually, in certain cases, a similar idea also leads to an improved upper bound for generalized Paley graphs. Similar to [22, Theorem 1.6], we have the following theorem for generalized Paley graphs.

Theorem 5.8. *If* $q \equiv 1 \pmod{2d}$, *and* $2 \leq n \leq N = \omega\big(GP(q,d)\big)$ *satisfies* $\binom{n-1+\frac{q-1}{d}}{\frac{q-1}{d}} \not\equiv 0 \pmod{p}$, *then* $(N-1)n \leq \frac{q-1}{d}$.

Proof. Let $C = \{v_1, v_2, \ldots, v_N\} \subset \mathbb{F}_q$ be a clique of maximum size in $GP(q,d)$. Consider the following polynomial

$$f(x) = \sum_{i=1}^{n} c_i (x - v_i)^{n-1+\frac{q-1}{d}} - 1 \in \mathbb{F}_q[x],$$

where $c_1, c_2, ..., c_n$ is the unique solution of the following system of equations:

$$\begin{cases} \sum_{i=1}^{n} c_i (-v_i)^j = 0, & 0 \leq j \leq n-2 \\ \sum_{i=1}^{n} c_i (-v_i)^{n-1} = 1. \end{cases}$$

Note the above system of equations has a unique solution since the coefficient matrix of the system is a Vandermonde matrix with parameters $v_1, v_2, \dots v_n$ all distinct. Similar to the proof of [22, Theorem 1.6], we can show that the degree of f is $\frac{q-1}{d}$, each of $v_1, v_2, \dots v_n$ is a root of f of multiplicity at least $n-1$, and each of $v_{n+1}, v_{n+2}, \dots v_N$ is a root of f of multiplicity at least n. Therefore

$$n(n-1) + (N-n)n = (N-1)n \leq \deg f = \frac{q-1}{d}. \qquad \square$$

The following corollary shows that Theorem 5.8 is a generalization of Theorem 5.7.

Corollary 5.9. *If $q \equiv 1 \pmod{2d}$, and $N = \omega\big(GP(q,d)\big)$ satisfies $\binom{N-1+\frac{q-1}{d}}{\frac{q-1}{d}} \not\equiv 0 \pmod{p}$, then $\omega\big(GP(q,d)\big) \leq \sqrt{\frac{q-1}{d} + \frac{1}{4}} + \frac{1}{2}$. In particular, if $p \equiv 1 \pmod{2d}$, then $\omega\big(GP(p,d)\big) \leq \sqrt{\frac{p-1}{d} + \frac{1}{4}} + \frac{1}{2}$.*

Proof. If $\binom{N-1+\frac{q-1}{d}}{\frac{q-1}{d}} \not\equiv 0 \pmod{p}$, then we can take $n = N$ in Theorem 5.8 to conclude that $(N-1)N \leq \frac{q-1}{d}$, i.e., $N \leq \sqrt{\frac{q-1}{d} + \frac{1}{4}} + \frac{1}{2}$. When q is a prime, note that by Lemma 5.1, $N = \omega\big(GP(p,d)\big) \leq \frac{p-1}{d} + 1$, then $N - 1 + \frac{p-1}{d} \leq \frac{2(p-1)}{d} \leq p - 1 < p$ and therefore $\binom{N-1+\frac{p-1}{d}}{\frac{p-1}{d}} \not\equiv 0 \pmod{p}$. $\square$

5.3. Improved Bounds on the Clique Number of Certain Generalized Paley Graphs

In this subsection, we will extend the idea in [22] to obtain improved bounds on $\omega\big(GP(q,d)\big)$. In particular, we will prove Theorem 1.8, which shows that for $\omega\big(GP(q,3)\big)$, the trivial bound $\sqrt{q}$ can be improved to $0.769\sqrt{q} + 1$.

We need to deal with the case when q is a prime power. We can assume $\sqrt{q} \geq N > \sqrt{\frac{q-1}{d} + \frac{1}{4}} + \frac{1}{2}$. In view of Theorem 5.8, we need to determine the largest $n \leq N$ such that $\binom{n-1+\frac{q-1}{d}}{\frac{q-1}{d}} \not\equiv 0 \pmod{p}$. Again, our main tool is Lucas's Theorem. For each given q and d, we shall have no difficulty finding the desired n by hand. However, in general, the analysis will be much more complicated than the case $d = 2$ (standard Paley graph). For example, it highly depends on the base-p representation of $\frac{q-1}{d}$ and the size of $\log_q d$, as we need to compare the number of digits of the the base-p representations of $\frac{q-1}{d}$, $\lfloor\sqrt{q}\rfloor$ and $\left\lceil \sqrt{\frac{q-1}{d} + \frac{1}{4}} + \frac{1}{2} \right\rceil$.

We first focus on the case $d \mid (p-1)$. In this case, the base-p representation of $\frac{q-1}{d}$ is simply

$$\frac{q-1}{d} = \left(\frac{p-1}{d}, \frac{p-1}{d}, \dots, \frac{p-1}{d}\right)_p.$$

We need to deal with the cases s is odd and s is even separately because $\sqrt{q}$ behaves very differently in the two cases. When s is odd, we can mimic the proof of [22, Theorem 3.5].

Theorem 5.10. *If $q = p^{2r+1} \equiv 1 \pmod{2d}$, $d \geq 3, r \geq 1$, and $d \mid (p-1)$, then*

$$\omega\big(GP(q,d)\big) < \sqrt{\frac{q}{d}}\left(1 + \frac{(d-1)^2}{8dp} + \frac{1}{2}\big(1 - \frac{1}{d}\big)\sqrt{\frac{d}{p}}\right) + 1.$$

Proof. Since $d \geq 3$, we have $p \geq 7$. In view of Lemma 5.2, we can assume that $\sqrt{p} \cdot p^r \geq N > \sqrt{\frac{p}{d}} \cdot p^r$. Let the base-$p$ representation of $N-1$ be $N-1 = (z_r, z_{r-1}, ..., z_0)_p$; then $\sqrt{\frac{p}{d}} \leq z_r \leq \sqrt{p}$. Note that $z_r + \frac{p-1}{d} \leq \sqrt{p} + \frac{p-1}{d} \leq \sqrt{p} + \frac{p-1}{3} < p$ since $p \geq 7$.

- If $z_{r-1} + \frac{p-1}{d} \leq p-1$, we can take $n-1 = z_r p^r + z_{r-1} p^{r-1}$. Then $N - p^{r-1} + 1 \leq n \leq N \leq n$ if $r \geq 2$, and $n = N$ if $r = 1$. And Lucas's Theorem implies that
$$\binom{n-1+\frac{q-1}{d}}{\frac{q-1}{d}} \equiv \binom{z_r + \frac{p-1}{d}}{\frac{p-1}{d}}\binom{z_{r-1} + \frac{p-1}{d}}{\frac{p-1}{d}} \not\equiv 0 \pmod{p}.$$
- If $z_{r-1} + \frac{p-1}{d} > p-1$, we can take $n - 1 = z_r p^r + p^r - 1 - \frac{p^r-1}{d}$. Then $N - p^r + \frac{p^r-1}{d} \leq n \leq N \leq n$ and
$$\binom{n-1+\frac{q-1}{d}}{\frac{q-1}{d}} \equiv \binom{z_r + \frac{p-1}{d}}{\frac{p-1}{d}}\binom{p-1}{\frac{p-1}{d}}^r \not\equiv 0 \pmod{p}.$$

To conclude, we can always find an n such that $N - p^r + \frac{p^r-1}{d} \leq n \leq N$, and $\binom{n-1+\frac{q-1}{d}}{\frac{q-1}{d}} \not\equiv 0 \pmod{p}$. Then by Theorem 5.8, we have $(N-1)(N - p^r + \frac{p^r-1}{d}) \leq (N-1)n \leq \frac{q-1}{d}$, so $N^2 - (p^r + 1 - \frac{p^r-1}{d})N \leq \frac{q+p^r-2}{d} - p^r$ and therefore

$$\begin{aligned}
N &\leq \sqrt{\frac{q+p^r-2}{d} - p^r + \frac{1}{4}\left(p^r + 1 - \frac{p^r-1}{d}\right)^2} + \frac{1}{2}\left(p^r + 1 - \frac{p^r-1}{d}\right) \\
&= \sqrt{\frac{q}{d} + \frac{1}{4}p^{2r}\left(1-\frac{1}{d}\right)^2 - p^r\left(1 - \frac{1}{d} + \frac{1}{2} - \frac{1}{2d^2}\right) + \frac{1}{4}\left(1+\frac{1}{d}\right)^2} + \frac{1}{2}\left(p^r + 1 - \frac{p^r-1}{d}\right) \\
&< \sqrt{\frac{q}{d}} + \left(1-\frac{1}{d}\right)^2 \frac{\sqrt{d}}{8} p^{r-1/2} + \frac{1}{2} + \frac{1}{2}\left(p^r + 1 - \frac{p^r}{d}\right) \\
&= \sqrt{\frac{q}{d}}\left(1 + \frac{(d-1)^2}{8dp} + \frac{1}{2}\big(1-\frac{1}{d}\big)\sqrt{\frac{d}{p}}\right) + 1.
\end{aligned}$$

□

In the case q is a square, $d \mid (p-1)$ would imply $q \equiv 1 \pmod{2d}$, so we do not need to assume that explicitly. Recall that for the (standard) Paley graph over $\mathbb{F}_q$, the clique number attains the trivial upper bound $\sqrt{q}$ if q is a square. Next, we show this is not the case for generalized Paley graphs. We will give a better bound in Theorem 5.12.

Lemma 5.11. *If q is a square, $d \geq 3$ and $d \mid (p-1)$, then $\omega\big(GP(q,d)\big) \leq \sqrt{q} - 1$.*

Proof. Let $q = p^{2r}$. In view of Lemma 5.2, it suffices to show that $N \neq p^r$. Suppose $N = p^r$; then we can take $n = p^r - \frac{p^r-1}{d} < N$ such that

$$n - 1 + \frac{q-1}{d} = \left(\frac{p-1}{d}, \ldots, \frac{p-1}{d}, p-1, \ldots, p-1\right)_p,$$

$$\binom{n-1+\frac{q-1}{d}}{\frac{q-1}{d}} \equiv \binom{\frac{p-1}{d}}{\frac{p-1}{d}}^r \binom{p-1}{\frac{p-1}{d}}^r \not\equiv 0 \pmod{p}.$$

Then by Theorem 5.8, we have $(N-1)n \leq \frac{q-1}{d}$, i.e., $(p^r-1)(p^r - \frac{p^r-1}{d}) \leq \frac{p^{2r}-1}{d}$. This implies $dp^r - (p^r - 1) \leq p^r + 1$, i.e., $d \leq 2$, a contradiction. □

Theorem 5.12. *If q is a square, $d \geq 3$ and $d \mid (p-1)$, then*

$$\omega\big(GP(q,d)\big) < \sqrt{\frac{q}{d}}\big(1 + \frac{1}{2\sqrt{d}} + \frac{1}{8d}\big) + 1.$$

Proof. Let $q = p^{2r}$. We can assume that $p^r - 1 \geq N > \sqrt{\frac{p^2}{d}} \cdot p^{r-1}$. Let the base-$p$ representation of $N-1$ be $N-1 = (z_{r-1}, z_{r-2}, ..., z_0)_p$; then $\sqrt{\frac{p^2}{d}} \leq z_{r-1} \leq p-1$.

- If $z_{r-1} + \frac{p-1}{d} < p$, then we can take $n-1 = z_{r-1}p^{r-1}$. We have $N - p^{r-1} + 1 \leq n \leq N$ and

$$\binom{n-1+\frac{q-1}{d}}{\frac{q-1}{d}} \equiv \binom{z_{r-1}+\frac{p-1}{d}}{\frac{p-1}{d}} \not\equiv 0 \pmod{p}.$$

- If $z_{r-1} + \frac{p-1}{d} \geq p$, then we can take $n - 1 = p^r - 1 - \frac{p^r-1}{d}$. We have $N - \frac{p^r-1}{d} \leq n \leq N$ and

$$\binom{n-1+\frac{q-1}{d}}{\frac{q-1}{d}} \equiv \binom{p^r-1}{\frac{p^r-1}{d}} \equiv \binom{p-1}{\frac{p-1}{d}}^r \not\equiv 0 \pmod{p}.$$

To conclude, we can always find $N - \frac{p^r-1}{d} \leq n \leq N$ such that $\binom{n-1+\frac{q-1}{d}}{\frac{q-1}{d}} \not\equiv 0 \pmod{p}$. Then by Theorem 5.8, we have $(N-1)(N - \frac{p^r-1}{d}) \leq (N-1)n \leq \frac{q-1}{d}$, so $N^2 - (\frac{p^r-1}{d} + 1)N \leq \frac{q+p^r-2}{d}$ and therefore

$$\begin{aligned} N &\leq \sqrt{\frac{q+p^r-2}{d} + \frac{1}{4}\left(\frac{p^r-1}{d}+1\right)^2} + \frac{1}{2}\left(\frac{p^r-1}{d}+1\right) \\ &= \sqrt{\frac{q}{d} + \frac{p^{2r}}{4d^2} + p^r\left(\frac{1}{d} + \frac{d-1}{2d^2}\right) + \frac{(d-1)^2}{4d^2} - \frac{2}{d}} + \frac{1}{2}\left(\frac{p^r-1}{d}+1\right) \end{aligned}$$

$$< \sqrt{\frac{q}{d} + \frac{p^{2r}}{4d^2} + \frac{3p^r}{2d} + \frac{1}{4}} + \frac{1}{2}\left(\frac{p^r - 1}{d} + 1\right)$$
$$< \sqrt{\frac{q}{d}} + \frac{p^r}{8d\sqrt{d}} + \frac{1}{2} + \frac{1}{2}\left(\frac{p^r - 1}{d} + 1\right)$$
$$< \sqrt{\frac{q}{d}}\left(1 + \frac{1}{2\sqrt{d}} + \frac{1}{8d}\right) + 1. \qquad \square$$

Note that when $d \geq 3$,

$$\frac{1}{\sqrt{d}} + \frac{1}{2d} + \frac{1}{8d\sqrt{d}} \leq \frac{1}{\sqrt{3}} + \frac{1}{6} + \frac{1}{24\sqrt{3}} < 0.769,$$

so this bound is always better than the trivial bound.

In general, given $d \geq 3$, to estimate $\omega\big(GP(q,d)\big)$ using Theorem 5.8, we need to determine all possible values of the order of p modulo d. If the order is $\delta \mid \phi(d)$, then $\frac{q-1}{d}$ will be periodic in base-p representation, with period δ, and we can try to apply Theorem 5.8 to obtain an upper bound on the clique number. It should be clear that the analysis will be very complicated when the number of divisors of $\phi(d)$ is large. We demonstrate this process for cubic Paley graphs and prove Theorem 1.8.

Proof of Theorem 1.8. Let $q = p^s$. Since $q \equiv 1 \pmod 6$, then either $p \equiv 1 \pmod 3$, or $p \equiv 2 \pmod 3$ and s is an even integer.

If $p \equiv 1 \pmod 3$, then $p \geq 7$. If s is odd, then by Theorem 5.10,

$$\omega\big(GP(q,3)\big) < \sqrt{\frac{q}{d}}\left(1 + \frac{1}{6p} + \frac{1}{3}\sqrt{\frac{3}{p}}\right) + 1 < 0.718\sqrt{q} + 1.$$

If s is even, then by Theorem 5.12, $\omega\big(GP(q,3)\big) < 0.769\sqrt{q} + 1$.

If $p \equiv 2 \pmod 3$, and s is even, then we can set $s = 2r$. Let $N = \omega\big(GP(q,3)\big)$. If r is odd, then $3 \mid (\sqrt{q} + 1)$ and thus by Corollary 5.5, $N = \sqrt{q}$. Next we assume r is even. We have

$$\frac{q-1}{3} = \left(\frac{p-2}{3}, \frac{2p-1}{3}, \frac{p-2}{3}, \frac{2p-1}{3}, \ldots, \frac{p-2}{3}, \frac{2p-1}{3}\right)_p.$$

We can assume that $p^r \geq N > \sqrt{\frac{p^2}{d}} \cdot p^{r-1}$. Let the base-$p$ representation of $N-1$ be $N-1 = (z_{r-1}, z_{r-2}, ..., z_0)_p$, then $\sqrt{\frac{p^2}{d}} \leq z_{r-1} \leq p-1$.

- If $z_{r-1} + \frac{p-2}{3} < p$, then we can take $n-1 = z_{r-1}p^{r-1}$. We have $N - p^{r-1} + 1 \leq n \leq N$ and

$$\binom{n-1+\frac{q-1}{3}}{\frac{q-1}{3}} \equiv \binom{z_{r-1}+\frac{p-2}{3}}{\frac{p-2}{3}} \not\equiv 0 \pmod p.$$

- If $z_{r-1}+\frac{p-2}{3} \geq p$, then we can take $n = p^r - \frac{p^r-1}{3}$. We have $N - \frac{p^r-1}{3} \leq n \leq N$ and

$$\binom{n-1+\frac{q-1}{3}}{\frac{q-1}{3}} \equiv \binom{p^r-1}{\frac{p^r-1}{3}} \equiv \binom{p-1}{\frac{p-2}{3}}^{r/2} \binom{p-1}{\frac{2p-1}{3}}^{r/2} \not\equiv 0 \pmod{p}.$$

  To conclude, we can always find n such that $N - \frac{p^r-1}{3} \leq n \leq N$ and $\binom{n-1+\frac{q-1}{3}}{\frac{q-1}{3}} \not\equiv 0 \pmod{p}$. Similar to the computation in the proof of Theorem 5.12, we have $N < \sqrt{\frac{q}{3}}\big(1 + \frac{1}{2\sqrt{3}} + \frac{1}{24}\big) + 1 < 0.769\sqrt{q} + 1$. □

Using Proposition 5.6, we see that the clique number of certain cubic Paley graphs is at least $q^{1/3}$. For such cubic Paley graphs, it is an open question to improve the range $[q^{1/3}, 0.769\sqrt{q}+1]$ on the clique number.

6. Proof of Theorem 1.9

In this section, we make use of Theorem 1.6 and an equidistribution result from analytic number theory to prove our third main result, Theorem 1.9.

6.1. Equidistribution Results Involving Prime Powers

A sequence $\{y_n : n \in \mathbb{N}\} \subset \mathbb{R}$ is called equidistributed modulo 1 if for any $\alpha \in [0,1]$, we have $\lim_{n\to\infty} \frac{Z(n,\alpha)}{n} = \alpha$, where $Z(n,\alpha) = \#\{y_j : 1 \leq j \leq n, \{y_j\} \leq \alpha\}$. Let $e(x) = \exp(2\pi i x)$. The characterization of equidistributed sequences is given by the following well-known Weyl's criterion.

Lemma 6.1 (Weyl's criterion)**.** *A sequence $\{y_n\}$ is equidistributed if and only if for any integer $t \neq 0$, $\sum_{n\leq x} e(ty_n) = o(x)$ as $x \to \infty$.*

Similar to the 1-dimensional case, we can also define the notion of equidistribution in a similar way for the multidimensional case, and we also have the multidimensional Weyl's criterion (see for example [13, Section 1.6]).

Recall we denote $\mathcal{P}$ to be the set of primes (with the natural order). Let g be a nice function, we would like to show the sequence $(g(p))_{p\in\mathcal{P}}$ is equdistributed modulo 1. By Weyl's criterion and partial summation, it suffices to show that for any non-zero integer t, we have

$$\sum_{n\leq x} e(tg(n))\Lambda(n) = o(x), \text{ as } x \to \infty. \tag{8}$$

To estimate the exponential sum of the above form, it is standard to use van der Corput's method and Vaughan's identity (see for example Chapter 8 and Chapter

13 in [12]). In particular, When $g(x) = \sqrt{x}$, for any $\alpha \neq 0$, we have (see [12, page 348])

$$\sum_{n \leq x} e(\alpha\sqrt{n})\Lambda(n) \ll_\alpha x^{\frac{5}{6}} (\log x)^4.$$

Therefore, $(\sqrt{p})_{p\in\mathcal{P}}$ is equidistributed modulo 1. In general, we have the following equidistribution result involving prime powers.

Theorem 6.2 ([3, Corollary 2.1])**.** *Let $\xi(x) = \sum_{j=1}^m \alpha_j x^{\theta_j}$, where $0 < \theta_1 < \theta_2 < \cdots < \theta_m$, α_j are nonzero real numbers. Assume that if all $\theta_j \in \mathbb{N}$, then at least one α_j is irrational. Then for any $h \in \mathbb{Z}$, the sequence $(\xi(p-h))_{p\in\mathcal{P}}$ is equdistributed modulo 1.*

For any two positive integers a and b, we define $\mathcal{P}_{a,b} = \mathcal{P} \cap (a\mathbb{Z} + b)$. In [3, Corollary 2.3], a stronger version of Theorem 6.2 is proved. It basically states that the sequence is still equdistributed when we restrict $\mathcal{P}$ to a certain residue class $\mathcal{P}_{a,b}$, where $(a, b) = 1$. It seems there are some typos in the original statement and proof of Corollary 2.2 and 2.3 in [3]. For the sake of completeness, we prove the following version of [3, Corollary 2.3].

Corollary 6.3. *Let $0 < \theta_1 < \theta_2 < \cdots < \theta_m$ and let $\gamma_1, \gamma_2, \ldots, \gamma_m$ be nonzero real numbers such that $\gamma_j \notin \mathbb{Q}$ if $\theta_j \in \mathbb{N}$. Then for any $h \in \mathbb{Z}$ and any coprime positive integers a, b, the sequence*

$$\Big(\big(\gamma_1(p-h)^{\theta_1}, \gamma_2(p-h)^{\theta_2}, \ldots, \gamma_m(p-h)^{\theta_m}\big)\Big)_{p\in\mathcal{P}_{a,b}}$$

is equdistributed modulo 1 in $\mathbb{T}^m$.

Proof. By the multidimensional Weyl's criterion (see for example [13, Section 1.6]), it suffices to show that for each $(\beta_1, \beta_2, \ldots, \beta_m) \in \mathbb{Z}^m \setminus \{(0, 0, \ldots, 0)\}$,

$$\sum_{\substack{p\leq x\\ p\equiv b \pmod a}} e\Big(\sum_{j=1}^m \beta_j\gamma_j(p-h)^{\theta_j}\Big) = o\Big(\frac{\pi(x)}{\phi(a)}\Big) = o\big(\pi(x)\big), \text{ as } x \to \infty. \tag{9}$$

By orthogonality relations,

$$\frac{1}{a}\sum_{i=1}^a e\Big(\frac{i(p-b)}{a}\Big) = \begin{cases} 1, & p \equiv b \pmod a \\ 0, & \text{otherwise.} \end{cases}$$

It follows that

$$\sum_{\substack{p\leq x\\ p\equiv b \pmod a}} e\Big(\sum_{j=1}^m \beta_j\gamma_j(p-h)^{\theta_j}\Big)$$

$$= \sum_{p\le x} e\Big(\sum_{j=1}^{m}\beta_j\gamma_j(p-h)^{\theta_j}\Big)\frac{1}{a}\sum_{i=1}^{a} e\Big(\frac{i(p-b)}{a}\Big)$$
$$= \frac{1}{a}\sum_{i=1}^{a} e\Big(\frac{i(h-b)}{a}\Big)\sum_{p\le x} e\Big(\sum_{j=1}^{m}\beta_j\gamma_j(p-h)^{\theta_j}+\frac{i(p-h)}{a}\Big).$$

Note that for each $1 \le i \le a$,

$$\xi_i(x) := \sum_{j=1}^{m}\beta_j\gamma_j x^{\theta_j} + \frac{i}{a}x = \sum_{\beta_j\neq 0}\beta_j\gamma_j x^{\theta_j} + \frac{i}{a}x$$

is of the required form in Theorem 6.2 since $\beta_j \neq 0$ and $\theta_j \in \mathbb{N}$ imply $\beta_j\gamma_j \notin \mathbb{Q}$. Therefore, $\big(\xi_i(p-h)\big)_{p\in\mathcal{P}}$ is equidistributed modulo 1. By Lemma 6.1 with $t = 1$, as $x \to \infty$,

$$\sum_{i=1}^{a} e\Big(\frac{i(h-b)}{a}\Big)\sum_{p\le x} e\Big(\sum_{j=1}^{m}\beta_j\gamma_j(p-h)^{\theta_j}+\frac{i(p-h)}{a}\Big) = o\big(\pi(x)\big). \qquad \square$$

In particular, for any positive integer r, and any coprime positive integers a, b, Corollary 6.3 implies that $(p^{r-1/2})_{p\in\mathcal{P}_{a,b}}$ is equidistributed modulo 1. Recall $\mathcal{Q}_{r,d} = \{p \in \mathcal{P} : p^{2r+1} \equiv 1 \pmod{2d}\}$. It is clear that $\mathcal{Q}_{r,d}$ is a union of primes in disjoint residue classes:

$$\mathcal{Q}_{r,d} = \bigcup_{\substack{1\le b<2d\\ b^{2r+1}\equiv 1 \pmod{2d}}} \mathcal{P}_{2d,b}.$$

Using Weyl's criterion, it is easy to show that the union of finitely many disjoint equidistributed sequences is also an equidistributed sequence. Therefore, we obtain the following corollary.

Corollary 6.4. *For any positive integers r and d, the sequence $(p^{r-1/2})_{p\in\mathcal{Q}_{r,d}}$ is equdistributed modulo 1.*

6.2. Proof of Theorem 1.9

In this subsection, we will prove Theorem 1.9. We will use the observation outlined in Section 1.4, which connects the clique number and the number of directions.

By Theorem 1.6, we can deduce the following information about the clique number.

Theorem 6.5. *Let $q = p^{2r+1} \equiv 1 \pmod{2d}$ such that $r \ge 1$ and $d \ge 3$. Then for any $0 < c < (p-1)/2$, the clique number $N = \omega\big(GP(q,d)\big)$ of the generalized Paley graph $GP(q,d)$ satisfies one of the following:*

1. *$N \le \sqrt{q} - c$.*

2. One of $N, N+1, \ldots, N+\lfloor 2c+\frac{c^2+2c}{\sqrt{q}-c-1}\rfloor$ is a multiple of p.

Proof. Lemma 5.2 gives the trivial upper bound $N \le \sqrt{q}$. Since q is not a square, we have $N < \sqrt{q}$. Suppose $N > \sqrt{q}-c$. Then $0 < k = q - N^2 < q - (\sqrt{q}-c)^2 = 2c\sqrt{q} - c^2$ and

$$\frac{k}{N-1} < \frac{2c\sqrt{q}-c^2}{\sqrt{q}-c-1} = 2c + \frac{c^2+2c}{\sqrt{q}-c-1}.$$

Let C be a clique in $GP(q,d)$ with $|C| = N$. If none of $N, N+1, \ldots, N+\lfloor 2c+\frac{c^2+2c}{\sqrt{q}-c-1}\rfloor$ is a multiple of p, then by Theorem 1.6, the number of directions determined by the Cartesian product $C \times C \subset AG(2,q)$ is at least $N^2 - N + 2$. However, each direction determined by $C \times C$ is a d-th power in $\mathbb{F}_q$ or ∞, so the number of directions is at most $\frac{q-1}{d}+2$ and we have $N^2 - N + 2 \le \frac{q-1}{d}+2$, i.e., $N(N-1) \le \frac{q-1}{d}$, or $N \le \sqrt{\frac{q-1}{d}+\frac{1}{4}}+\frac{1}{2}$. This implies

$$\sqrt{q} - \frac{p-1}{2} < \sqrt{q} - c < N \le \sqrt{\frac{q-1}{d}+\frac{1}{4}}+\frac{1}{2} < \sqrt{\frac{q}{d}}+1 \le \sqrt{\frac{q}{3}}+1,$$

that is, $\sqrt{q} - \sqrt{\frac{q}{3}} \le \frac{p+1}{2}$, which fails since $q \ge 27$. So one of $N, N+1, \ldots, N+\lfloor 2c+\frac{c^2+2c}{\sqrt{q}-c-1}\rfloor$ must be a multiple of p. □

Note that we assume $c < (p-1)/2$ so that the second condition does not hold automatically. We remark that a similar proof for Theorem 6.5 also holds for square q, but note that we will only be able to conclude that the clique number is at most $\sqrt{q}$, since $p \mid \sqrt{q}$.

Now we are ready to use Corollary 6.4 and Theorem 6.5 to prove Theorem 1.9.

Proof of Theorem 1.9. Since $h(x) = o(x)$ as $x \to \infty$, there is $M > 0$ such that $h(x) < \frac{x-1}{2}$ for any $x > M$. Let $X = \{p \in \mathcal{Q}_{r,d} : \omega\big(P(p^{2r+1}, d)\big) > p^{r+1/2} - h(p)\}$. If $X \cap (M, \infty) = \emptyset$, then the statement follows trivially.

Next we assume $X \cap (M,\infty) \neq \emptyset$. Let $p \in X \cap (M,\infty)$, $q = p^{2r+1}$, and $N = \omega\big(P(q,d)\big)$. Since $N > \sqrt{q} - h(p)$ and $h(p) < \frac{p-1}{2}$, by Theorem 6.5, one of $N, N+1, \cdots, N+\big\lfloor 2h(p)+\frac{h(p)^2+2h(p)}{\sqrt{q}-h(p)-1}\big\rfloor$ is a multiple of p. Since $\sqrt{q}-h(p) < N \le \sqrt{q}$, one of $\lceil\sqrt{q}-h(p)\rceil, \lceil\sqrt{q}-h(p)\rceil+1, \ldots, \big\lfloor\sqrt{q}+2h(p)+\frac{h(p)^2+2h(p)}{\sqrt{q}-h(p)-1}\big\rfloor$ must be a multiple of p. Therefore, $\lfloor\sqrt{q}\rfloor$ is congruent to one of

$$\left\lfloor -2h(p) - \frac{h(p)^2+2h(p)}{\sqrt{q}-h(p)-1}\right\rfloor, \left\lfloor -2h(p) - \frac{h(p)^2+2h(p)}{\sqrt{q}-h(p)-1}\right\rfloor + 1, \ldots, \lceil h(p)\rceil \pmod p.$$

Note that $\sqrt{q} = p^{r+1/2}$. If $0 \le m < p$, then $\lfloor\sqrt{q}\rfloor \equiv \lfloor p\{p^{r-1/2}\}\rfloor \equiv m \pmod p$ is equivalent to $\{p^{r-1/2}\} \in [\frac{m}{p}, \frac{m+1}{p})$. Therefore, $p \in X \cap (M,\infty)$ implies that

$$\{p^{r-1/2}\} \in \left[0, \frac{\lceil h(p)\rceil+1}{p}\right) \cup \left[1 - \frac{\big\lfloor -2h(p) - \frac{h(p)^2+2h(p)}{\sqrt{q}-h(p)-1}\big\rfloor}{p}, 1\right).$$

Since $h(x) = o(x)$ as $x \to \infty$,

$$2h(x) + \frac{h(x)^2 + 2h(x)}{x^{r+1/2} - h(x) - 1} = o(x) + o\big(x^{3/2-r}\big) = o(x) \quad \text{as } x \to \infty.$$

Then for any $\varepsilon > 0$, there exists $M_\varepsilon > M$ such that $\{p^{r-1/2}\} \in [0, \varepsilon) \cup [1-\varepsilon, 1)$ for any $p \in X \cap (M_\varepsilon, \infty)$. Therefore, for any $\varepsilon > 0$, by the equidistribution of $(p^{r-1/2})_{p \in \mathcal{Q}_{r,d}}$, the relative upper density of $X \subset \mathcal{Q}_{r,d}$ is at most 2ε. Letting $\varepsilon \to 0^+$, we conclude that the relative density of $X \subset \mathcal{Q}_{r,d}$ is zero. Therefore, $\omega\big(P(p^{2r+1}, d)\big) \le p^{r+1/2} - h(p)$ holds for almost all $p \in \mathcal{Q}_{r,d}$. □

Acknowledgements. The author would like to thank Greg Martin, József Solymosi, Ethan White, and Joshua Zahl for valuable suggestions. The author would like to thank Daniel Di Benedetto, Gabriel Currier, and Stephanie van Willigenburg for helpful discussions. The author would also like to thank the anonymous referee for a careful reading of the draft.

References

[1] W. Ananchuen, On the adjacency properties of generalized Paley graphs, *Australas. J. Combin.*, **6** (2001), 129-147.

[2] C. Bachoc, M. Matolcsi, and I. Z. Ruzsa, Squares and difference sets in finite fields, *Integers* **13** (2013), #A77.

[3] V. Bergelson, G. Kolesnik, M. Madritsch, Y. Son, and R. Tichy, Uniform distribution of prime powers and sets of recurrence and van der Corput sets in $\mathbb{Z}^k$, *Israel J. Math.* **201** (2014), no. 2, 729-760.

[4] I. Broere, D. Döman, and J. N. Ridley, The clique numbers and chromatic numbers of certain Paley graphs, *Quaestiones Math.* **11** (1988), 91-93.

[5] S. Cohen, Clique numbers of Paley graphs, *Quaestiones Math.* **11** (1988), 225-231.

[6] E. Croot, and V. Lev, Open problems in additive combinatorics, *Additive combinatorics*, 207–233, CRM Proc. Lecture Notes, 43, Amer. Math. Soc., Providence, RI, 2007.

[7] D. Di Benedetto, J. Solymosi, and E. P. White, On the directions determined by a Cartesian product in an affine Galois plane, arXiv:2001.06994 (2020). To appear in *Combinatorica*.

[8] D. Dona, Number of directions determined by a set in $\mathbb{F}_q^2$ and growth in $\mathrm{Aff}(\mathbb{F}_q)$, arXiv:1910.06752 (2019). To appear in *Discrete Comput. Geom.*

[9] A. N. Elsawy, Paley graphs and their generalizations, MSc thesis, Heinrich Heiner University, Germany, 2009. arXiv:1203.1818.

[10] A. Gács, L. Lovász, and T. Szőnyi, Directions in $AG(2, p^2)$, *Innov. Incidence Geom.* **6/7** (2007/08), 189–201.

[11] B. Hanson, and G. Petridis, Refined estimates concerning sumsets contained in the roots of unity, *Proc. Lond. Math. Soc. (3)* **122** (2021), no. 3, 353–358.

[12] H. Iwaniec, and E. Kowalski, *Analytic Number Theory*, American Mathematical Society, Providence, RI, 2004.

[13] L. Kuipers, and H. Niederreiter, *Uniform Distribution of Sequences*, Wiley-Interscience, New York, 1974.

[14] T. K. Lim, and C. E. Praeger, On generalized Paley graphs and their automorphism groups, *Michigan Math. J.* **58** (2009), no. 1, 293–308.

[15] B. Murphy, G. Petridis, O. Roche-Newton, M. Rudnev, and I. D. Shkredov, New results on sum-product type growth over fields, *Mathematika* **65** (2019), no. 3, 588–642.

[16] L. Rédei, *Lückenhafte Polynome über endlichen Körperrn*, Birkhäuser, Basel, 1970.

[17] M. Rudnev, and I. D. Shkredov, On growth rate in $SL_2(\mathbb{F}_p)$, the affine group and sum-product type implications, arXiv:1812.01671 (2019).

[18] T. Schoen, and I. D. Shkredov, Character sums estimates and an application to a problem of Balog, arXiv:2004.01885 (2020).

[19] J. Schwartz, Fast probabilistic algorithms for verification of polynomial identities, *J. Assoc. Comput. Mach.* **27** (1980), no. 4, 701–717.

[20] 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), no. 1, 141-146.

[21] T. Szőnyi, Around Rédei's theorem, *Discrete Math.* **208/209** (1999), 557-575.

[22] C. H. Yip, On the clique number of Paley Graphs of prime power order, arXiv:2004.01175 (2020).