On the clique number of Paley graphs and generalized Paley graphs

by

Chi Hoi Yip

B.Sc., The Hong Kong University of Science and Technology, 2019

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

in

The Faculty of Graduate and Postdoctoral Studies

(Mathematics)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

January 2021

The following individuals certify that they have read, and recommend to the Faculty of Graduate and Postdoctoral Studies for acceptance, the thesis entitled:

On the clique number of Paley graphs and generalized Paley graphs

submitted by **Chi Hoi Yip** in partial fulfillment of the requirements for the degree of **Master of Science** in **Mathematics**.

Examining Committee:
Greg Martin, Mathematics
Co-supervisor
József Solymosi, Mathematics
Co-supervisor
Joshua Zahl, Mathematics
Supervisory Committee Member

Abstract

Finding reasonably good upper and lower bounds for the clique number of Paley graphs and generalized Paley graphs is an old and open problem in additive combinatorics. In this thesis, we use polynomial methods, together with various tools from number theory, graph theory, and combinatorics, to study this problem. Specifically, we obtain improved upper bounds on the clique number of Paley graphs and generalized Paley graphs over a finite field. We also obtain new upper bounds on the number of distinct roots of lacunary polynomials and improve lower bounds on the number of directions determined by a Cartesian product in an affine Galois plane over a finite field.

Lay Summary

Graph theory is the study of graphs, which are abstract mathematical structures modeling pairwise relations between a set of objects. For example, we can define a relationship graph based on a group of people, where two vertices are connected if the corresponding two persons know each other. Graph theory is now a useful tool in mathematics, computer science, electrical engineering, economics, and many other areas.

Given a graph, we are interested in estimating its clique number, which is the largest number of vertices such that every pair of vertices are connected. Computing the clique number is extremely difficult, yet it is possible to give some estimates on the clique number if the given graph has some nice structures. In this thesis, we will study the clique number of certain graphs called "(generalized) Paley graphs" from many different perspectives. We will review the known bounds, and give some improved bounds.

Preface

Chapters 1 to 4 are mostly expository.

Chapter 5 is a joint work with József Solymosi and Ethan P. White. The starting point, Theorem 5.1.2, is due to József Solymosi. The remaining sections are the product of collaborative research.

Unless otherwise stated, the results in Chapters 6 to 8 of this thesis are original intellectual product of the author.

Table of Contents

List of Tables

List of Figures

Acknowledgements

I would never have completed this work without the help from many people. First of all, I would like to thank my supervisors, Dr. Greg Martin, Dr. József Solymosi, and Dr. Joshua Zahl for their guidance in the past two years. They provided me precious opportunities for experiencing research in number theory and combinatorics. They also answered my numerous questions and helped me to decide how to present everything coherently.

I would like to thank Daniel Di Benedetto, Gabriel Currier, Dr. Karen Gunderson, Dr. Karen Meagher, Dr. Joy Morris, Ethan White, Qidi Zhang, and Junjie Zhu for valuable suggestions and helpful discussions in writing this thesis. I am also grateful for the precious learning opportunities provided by UBC Department of Mathematics and Pacific Institute for the Mathematical Sciences (PIMS).

Last but not least, I thank my parents and my brother, for their continued support and encouragement.

Chapter 1

Introduction

Paley graphs are named after Raymond Edward Alan Christopher Paley (1907–1933), an English mathematician, whose main contributions include Paley construction for Hadamard matrices, the Paley–Wiener theorem, and Littlewood–Paley theory. Paley graphs are closely related to the Paley construction [94] in 1933 for constructing Hadamard matrices from quadratic residues. They were introduced as graphs independently by Sachs [101] in 1962 and by Erdős and Rényi [36] in 1963. We refer to [58, Sections 8-10] for an interesting discussion on the origin and the history of the Paley graphs. Surprisingly, the study of Paley graphs connects many branches of mathematics, such as combinatorics, number theory, discrete geometry, group theory, graph theory, design theory, matrix theory, and coding theory [58].

Throughout this thesis, we let $q = p^s$ be an odd prime power and $\mathbb{F}_q$ the finite field with q elements. Throughout the thesis, unless otherwise stated, all polynomials considered will be defined over $\mathbb{F}_q$.

In this chapter, we will first introduce the definition of Paley graphs and generalized Paley graphs, and then give an overview of the clique number problem.

1.1 Definition of Paley graphs

Definition 1.1.1. *The* Paley *graph on $\mathbb{F}_q$, denoted P_q, is the undirected graph whose vertices are the elements of $\mathbb{F}_q$, such that two vertices are adjacent if and only if the difference of the two vertices is a quadratic residue in $\mathbb{F}_q$.*

Note that $q \equiv 1 \pmod 4$ is needed to ensure that the graph is undirected.

Example 1.1.2. *The Paley graph over $\mathbb{F}_5$ is simply a cycle of length 5.*

Example 1.1.3. *The following is a figure ([32]) of the Paley graph with order 17. We can see that 1 is adjacent to 3 since 2 is a quadratic residue in $\mathbb{F}_{17}$, while 1 is not adjacent to 4 since 3 is a quadratic non-residue in $\mathbb{F}_{17}$.*

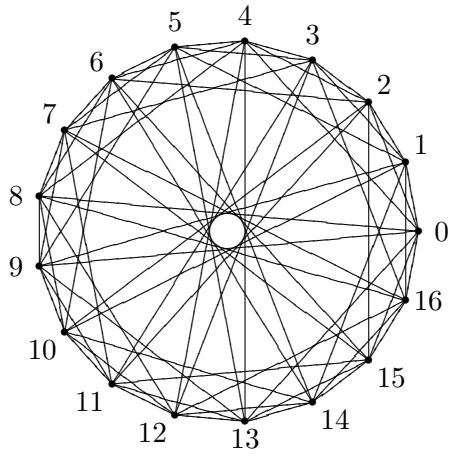

Figure 1.1: The Paley graph with order 17.

1.2 Generalized Paley graphs

It seems that generalized Paley graphs were first introduced by Cohen [24] in 1988, and reintroduced by Lim and Praeger [74] in 2009.

Definition 1.2.1. *Let $d > 1$ be a positive integer. The* d-Paley graph *on $\mathbb{F}_q$, denoted $P(q, d)$, is the undirected graph whose vertices are the elements of 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*, 4-Paley graphs are also called *quadruple Paley graphs* [5].

It is clear that if $\gcd(d, q-1) = \gcd(d', q-1)$, then $P(q, d)$ and $P(q, d')$ 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 $P(q, d)$ to be a 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, for a generalized Paley graph $P(q, d)$, we will always assume $d > 1$ and d is a divisor of $\frac{q-1}{2}$, or equivalently $q \equiv 1 \pmod{2d}$. The following are some examples of generalized Paley graphs [32].

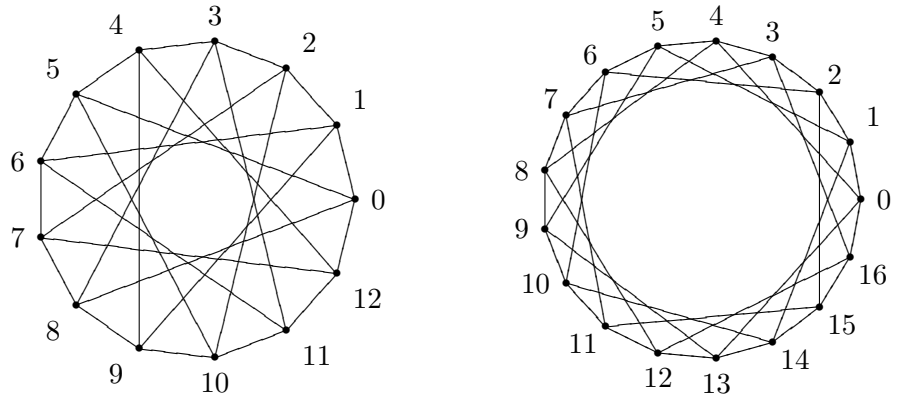

Figure 1.2: The cubic Paley graph with order 13 and the quadruple Paley graph with order 17.

1.3 Clique number

Definition 1.3.1. *A* clique *in a graph X is a subgraph of X that is a complete graph. A* maximum clique *is a clique with the maximum size, while a* maximal clique *is a clique where one cannot add another vertex to it and still have a clique. For an (undirected) graph X, the* clique number *of X, denoted $\omega(X)$, is the size of a maximum clique of X.*

Definition 1.3.2. *An* independent set *(or a* coclique*) is a set of vertices in which no two vertices are adjacent. For a graph X, the* independence number *of X, denoted $\alpha(X)$, is the size of a maximum independent set of X.*

The independent set problem and the clique problem are complementary: a clique in X is an independent set in the complement graph of X, and vice versa. Given a subset of vertices, we can use a polynomial-time algorithm to check whether it is a maximal clique (maximal independent set). However, it is believed that there is no efficient polynomial-time algorithm for finding the clique number and the independence number, in fact, they have been shown to be NP-complete [63].

The following table gives the clique numbers for Paley Graphs of order less than 340 [14, 37]. One can observe that $\omega(P_q)$ behaves like a polylogarithmic function in q, unless q is a square. We will see why $\omega(P_q) = \sqrt{q}$ when q is a square in Corollary 3.7.2.

In Chapter 2, we will show that Paley graphs have many nice graph-theoretical properties; for example, they are strongly regular, connected, self-complementary, and symmetric. 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 Section 3.3 in [32]). 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.

q	$\omega(P_q)$	q	$\omega(P_q)$	q	$\omega(P_q)$	q	$\omega(P_q)$	q	$\omega(P_q)$
5	2	9	3	13	3	17	3	25	5
29	4	37	4	41	5	49	7	53	5
61	5	73	5	81	9	89	5	97	6
101	5	109	6	113	7	121	11	125	7
137	7	149	7	157	7	169	13	173	8
181	7	193	7	197	8	229	9	233	7
241	7	257	7	269	8	277	8	281	7
289	17	293	8	313	8	317	9	337	9

Table 1.1: Clique Numbers for Paley Graphs of order less than 340.

Finding a reasonably good upper bound of the clique number of a Paley graph remains an open problem in additive combinatorics [27]. Let $q \equiv 1 \pmod{2d}$, and $N = \omega\big(P(q,d)\big)$, and let $C = \{v_1, v_2, \ldots, v_N\} \subset \mathbb{F}_q$ be a maximum clique in $P(q,d)$. The following is a trivial upper bound.

Lemma 1.3.3. *If $q \equiv 1 \pmod{2d}$, then $\omega\big(P(q,d)\big) \leq \frac{q-1}{d} + 1$.*

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

In the literature [8, 13, 24, 27, 53], the trivial upper bound on $\omega\big(P(q,d)\big)$ is given by $\sqrt{q}$.

Theorem 1.3.4. *If $q \equiv 1 \pmod{2d}$, then $\omega\big(P(q,d)\big) \leq \sqrt{q}$.*

We will give several proofs and some generalizations of Theorem 1.3.4 in Chapter 2 and Chapter 3 from different perspectives (in particular, see Sections 2.2, 2.3, and 3.4). Interestingly, some proofs use combinatorial tools, while others are purely number-theoretic.

1.4 Directions determined by a point set in an affine Galois plane

Let $AG(2,q)$ denote the affine Galois plane over the finite field $\mathbb{F}_q$. For $U \subset AG(2,q)$, we use Cartesian coordinates in $AG(2,q)$ so that $U = \{(x_i, y_i) : 1 \leq i \leq |U|\}$. The set of *directions* determined by $U \subset AG(2, \mathbb{F}_q)$ is

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

The possible values on $|D|$ have been studied by many authors. For a survey of such kind of results, readers can refer to [115]. We begin with some relevant results where the point set U is not necessarily a Cartesian product. The following theorem was proved by Rédei [98] in the case $|U| = p$, and later extended by Szőnyi [114, 115] to any $|U| \leq p$.

Theorem 1.4.1 (Theorem 5.2 in [115])**.** *Let p be a prime, and let $U \subset AG(2,p)$ with $1 < |U| \leq p$. Then either U is contained in a line, or U determines at least $\frac{|U|+3}{2}$ directions.*

When the underlying field becomes $\mathbb{F}_q$ for a proper prime power q, the problem becomes much more difficult. This is partially due to the fact that when we are working in $\mathbb{F}_q$, there are cases where $|D|$ is small; see the remarks after Theorem 1.6.3. Szőnyi [115] proved the following interesting result, which is of a similar flavor to Theorem 1.4.1.

Theorem 1.4.2 (Theorem 4 in [114]). *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 $|V| = q$ that determines the same set of directions as U.*

Note that in Theorem 1.4.2, $|U|$ 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 1.4.3 (Theorem 1.3 in [31]). *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.*

When $U = A \times B$, it turned out Theorem 1.4.1 can be significantly improved. In [9], Di Benedetto, Solymosi, and White showed the following theorem.

Theorem 1.4.4 (Theorem 1 of [9]). *Let $A, B \subset \mathbb{F}_p$ be sets each of size at least 2 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.*

We will give a generalization of Theorem 1.4.3 in Chapter 7.

1.5 Recent developments on the upper bound

Paley graphs are notoriously difficult to study, particularly finding bounds for their clique numbers [89]. We have seen many different proofs of the trivial upper bound, but it is difficult to improve the trivial upper bound for the clique number of Paley graphs and generalized Paley graphs. There was practically no improvement on the trivial upper bound until 2006 by Maistrelli and Penman [77]; see Theorem 1.5.2.

The current best upper bound for a Paley graph of prime order p and a generalized Paley graph of order p is $O(\sqrt{p})$, which is the same as the above trivial bound given in Theorem 1.3.4. Recently, Hanson and Petridis [53] used Stepanov's method to improve the upper bound on $\omega\big(P(p,d)\big)$. In [9], Di Benedetto, Solymosi, and White recovered the same bound using Theorem 1.4.4.

Theorem 1.5.1 (Corollary 1.5 in [53], Corollary 2 in [9]). *If p is a prime such that $p \equiv 1 \pmod{2d}$, then $\omega^2\big(P(p,d)\big) - \omega\big(P(p,d)\big) \le \frac{p-1}{d}$. Equivalently, $\omega\big(P(p,d)\big) \le \sqrt{\frac{p-1}{d} + \frac{1}{4}} + \frac{1}{2}$.*

Numerical data for primes $p < 10000$ by Exoo [37] suggests that $\omega(P_p)$ behaves like a polylogarithmic function. And the best known lower bounds on $\omega(P_p)$ are $O(\log p)$ and $\Omega(\log p \log\log p)$; see the discussion on Sections 2.5, 3.5, and 3.6. Therefore, there is still a huge gap between the

best known upper bound and the best known lower bound for $\omega(P_p)$. It remains an open problem to determine whether there exists $\epsilon > 0$ such that $\omega(P_p) \leq p^{1/2-\epsilon}$ infinitely often.

For the case that q is a prime power, we should focus on the case that q is a non-square for Paley graphs P_q, as the trivial upper bound $\sqrt{q}$ can be actually achieved in the case that q is a square (see Corollary 3.7.2). In 2006, Maistrelli and Penman [77] improved the trivial upper bound to $\sqrt{q-4}$.

Theorem 1.5.2 (Proposition 2.3 in [77]). *If $q \equiv 1 \pmod 4$, q is a non-square, and $q > 5$, then $\omega(P_q) \leq \sqrt{q-4}$.*

The best known result is due to Bachoc, Matolcsi, and Ruzsa [8].

Theorem 1.5.3 (Theorem 2.1 in [8]). *Assume $p \equiv 1 \pmod 4$ and q is a non-square. Let $N = \omega(P_q)$.*

- *If $[\sqrt{q}]$ is even then $N^2 + N - 1 \leq q$.*
- *If $[\sqrt{q}]$ is odd then $N^2 + 2N - 2 \leq q$.*

So roughly speaking, $\omega(P_q)$ is at most $\sqrt{q} - 1$ for about half of the non-squares q. Theorem 1.5.3 can be generalized to a larger family of graphs. The precise definition of conference graphs in the next theorem will be given in Definition 2.3.3.

Theorem 1.5.4 (Theorem 1 in [46]). *Let X be a conference graph with n vertices. Suppose that*

$$0 < \{\sqrt{n}/2\} < \frac{1}{4} - \big(\sqrt{n + 5/4} - \sqrt{n}\big)/2.$$

Then $\omega(X) \leq \lfloor \sqrt{n} - 1 \rfloor$.

Theorem 1.5.1 suggests that we could expect $\omega\big(P(q,d)\big)$ to be bounded above by $\sqrt{\frac{q}{d}}\big(1+o(1)\big)$. However, the current best known bound is $\sqrt{q} - 1$.

In Chapter 6 and Chapter 7 of this thesis, we will see that the approaches by Hanson and Petridis; and by Di Benedetto, Solymosi, and White only work in a prime field. The main motivation for this thesis is to extend their method and give improved upper bounds on the clique number of Paley graphs and generalized Paley graphs of prime power order.

1.6 Main results of the thesis

In this thesis, we will improve upper bounds on the clique number of Paley graphs and generalized Paley graphs over $\mathbb{F}_q$, which extends the work of Bachoc, Matolcsi, and Ruzsa [8]; and Hanson and Petridis [53]. Recall the trivial upper bound is $\sqrt{q}$.

Our first main result is an improved upper bound on the clique number of the Paley graph over $\mathbb{F}_q$, where q is a non-square.

Theorem 1.6.1. *Assume $p \equiv 1 \pmod 4$ and $q = p^{2s+1}$ for some nonneagtive integer s. Then*

$$\omega(P_q) \leq \min\left(p^s\left\lceil\sqrt{\frac{p}{2}}\right\rceil, \sqrt{\frac{q}{2}} + \frac{p^s+1}{4} + \frac{\sqrt{2p}}{32}p^{s-1}\right).$$

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 $\omega\big(P(q,3)\big)$ 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 1.6.2. *Let $q \equiv 1 \pmod 6$. If q is not a square, then $\omega\big(P(q,3)\big) < 0.718\sqrt{q}+1$. If q is a square, then $\omega\big(P(q,3)\big) = \sqrt{q}$ if $3 \mid (\sqrt{q}+1)$ and $\omega\big(P(q,3)\big) < 0.769\sqrt{q}+1$ otherwise.*

For a generalized Paley graph that is not a Paley graph or a cubic Paley graph, it will be difficult to improve the trivial upper bound. We will prove that for any positive function h such that $h(x) = o(x)$ as $x \to \infty$, the trivial upper bound on $P(q,d)$ can be improved to $\sqrt{q} - h(p)$ for almost all non-squares q.

Let $\mathcal{P}$ be the set of primes. For positive integers r and d, we define $\mathcal{Q}_{r,d} = \{p \in \mathcal{P} : p^{2r+1} \equiv 1 \pmod{2d}\}$. The precise statement of the improved bound is given in the following theorem.

Theorem 1.6.3. *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 $\omega\big(P(p^{2r+1}, d)\big) \leq p^{r+1/2} - h(p)$ for almost all $p \in \mathcal{Q}_{r,d}$.*

In the thesis, we will also improve lower bounds on the number of directions formed by a Cartesian product in the affine Galois plane $AG(2,q)$, which extends the work of Di Benedetto, Solymosi, and White [9]. The symmetric polynomials $f_{m,t}(b_1, b_2, \ldots, b_{n-1}, 0)$ in the statement of Theorem 1.6.4 will be defined via recurrence relations in Section 7.1, and we will give an explicit formula for $f_{m,t}$ in Section 7.2.

Theorem 1.6.4. *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 $mn - n + l + 2$.

Note that when 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 1.4.4. 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 $|D| \leq |E| + 1$. Then the inequality $|A||B| - \min\{|A|, |B|\} + 2 \leq |D| \leq |E| + 1$ fails to hold when $|A|, |B| \geq \sqrt{|E|} + 1$.

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.

Theorem 1.6.5. *Let $p \geq 3$ and $q = p^s$ be a prime power. Suppose $m \geq n \geq p$ 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*

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

Note that when k is small compared to q, the lower bound for the above probability behaves like $\frac{p-2}{p-1}$. Compared to Theorem 1.4.3, we see that the lower bound on $|D|$ can be improved greatly when the point set is a Cartesian product. Recall that Theorem 1.4.2 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 1.4.2 does not predict how likely the desired scenario will happen. Theorem 1.6.5 gives us further insights in the conclusion of Theorem 1.4.2. It implies that the desired scenario is very likely to occur, provided the point set U is a Cartesian product $A \times B$.

One key ingredient in the proof of above theorems is the polynomial method. In particular, we would like to understand various properties of polynomials over finite fields.

For a polynomial $f(x) \in \mathbb{F}_q[x]$ we will denote by f° the degree of f, and $Z^*(f)$ the set of roots of $f(x)$ in $\mathbb{F}_q^*$. A fundamental question is to improve the trivial degree bound on the number of distinct zeros of a polynomial, and in the case that f is sparse or lacunary, we expect to obtain some improvement on $|Z^*(f)|$. Our main focus will be on polynomials $f(x) \in \mathbb{F}_q[x]$ of the form

$$f(x) = x^{\frac{q-1}{d}-\ell} + g(x), \tag{1.1}$$

where $\ell \geq 0$ and d is a positive divisor of $q-1$, and $g^\circ < \frac{q-1}{d} - \ell$. Since we are interested in nonzero roots, we will always assume that the constant term of $f(x)$ is nonzero. The following theorem provides a new bound on the number of roots of a lacunary polynomial.

Theorem 1.6.6. *Let $f(x) \in \mathbb{F}_q[x]$ be as in equation (1.1), and assume that the constant term of f is nonzero. Then exactly one of the following holds.*

(1) *If $\ell > \frac{q-1}{d(d+1)}$ and $i \geq -1$ is the largest integer such that*

$$\ell + g^\circ < (q-1)\left(\frac{1+d^{-2i-1}}{d(d+1)}\right), \tag{1.2}$$

then

$$|Z^*(f)| \leq \frac{q-1}{d+1} - d^{2i+2}\left(\ell - \frac{q-1}{d(d+1)}\right).$$

(2) *If $\ell + g^\circ < \frac{q-1}{d(d+1)}$ and $i \geq -1$ is the largest integer such that*

$$\ell > (q-1)\left(\frac{1-d^{-2i-2}}{d(d+1)}\right), \tag{1.3}$$

then

$$|Z^*(f)| \leq \frac{q-1}{d+1} - d^{2i+3}\left(\frac{q-1}{d(d+1)} - (\ell + g^\circ)\right).$$

(3) *If* $\ell \leq \frac{q-1}{d(d+1)}$, $\ell + g^\circ \geq \frac{q-1}{d(d+1)}$, *and* $d(d+1)\ell + d^2 g^\circ < q-1$, *then* $|Z^*(f)| \leq d(\ell + g^\circ)$.

(4) *If* $\ell \leq \frac{q-1}{d(d+1)}$, $\ell + g^\circ \geq \frac{q-1}{d(d+1)}$, *and* $d(d+1)\ell + d^2 g^\circ \geq q-1$, *then* $|Z^*(f)| \leq f^\circ = \frac{q-1}{d} - \ell$.

1.7 Organization of the thesis

In Chapter 2, we will describe some nice properties of Paley graphs which lead to several proofs of the trivial upper bound on the clique number. We will also discuss the connection between the clique problem and Ramsey theory.

In Chapter 3, we will study the connection between character sums and the clique number of Paley graphs. We will see the clique problem is related to several important questions in number theory.

In Chapter 4, we will introduce some useful tools in polynomials over finite fields, which are preparations of the polynomial methods used in the thesis.

In Chapter 5, we will study a class of important polynomials, lacunary polynomials. We will obtain some new bounds on the number of roots of a lacunary polynomial over a finite field, and show that the trivial degree bound can often be improved. In particular, we will prove Theorem 1.6.6.

In Chapter 6, we will use Stepanov's method and binomial coefficients to obtain improved upper bounds on the clique number of Paley graphs and generalized Paley graphs. In particular, we will prove Theorem 1.6.1 and Theorem 1.6.2.

In Chapter 7, we will study the direction set determined by a Cartesian product in an affine Galois plane $AG(2, q)$. In particular, we will improve the lower bound on the size of the direction set, and prove Theorem 1.6.4 and Theorem 1.6.5.

In Chapter 8, we will see some classical estimates on exponential sums over primes, and prove an interesting equidistribution result involving prime powers. At the end of this chapter, we will discuss the connection between the clique number problem and the direction problem, and then we will give the proof for Theorem 1.6.3.

Chapter 2

Properties of Paley graphs and generalized Paley graphs

In this chapter, we will discuss graph-theoretical properties of Paley graphs and generalized Paley graphs. And we will see how can we make use of these nice properties to deduce bounds on the clique number.

2.1 Cayley graphs

Definition 2.1.1. *Let X be a graph. We write $x \sim_X y$ to denote that the vertices x, y are adjacent.*

Definition 2.1.2. *Two graphs X, Y are* isomorphic *if there is a bijective function $f : V(X) \to V(Y)$ such that for any two vertices $u, v \in V(X)$, $u \sim_X v$ iff $f(u) \sim_Y f(v)$.*

Definition 2.1.3. *An isomorphism from a graph X to itself is called an* automorphism *of X. The set of all automorphisms of X forms a group under the composition of functions, called the* automorphism group *of X, denoted by* $\mathrm{Aut}(X)$.

Definition 2.1.4. *Suppose a group G acts on a set Ω. We say the group action is* transitive *if for any $x, y \in \Omega$, there is $g \in G$ such that $g(x) = y$.*

Definition 2.1.5. *A graph is* vertex-transitive *if its automorphism group acts transitively on the set of vertices.*

Definition 2.1.6. *For any group G and connection set $S \subset G$, the* Cayley (di)graph $\mathrm{Cay}(G; S)$ *is the (di)graph whose vertices are elements of G, and $g \sim sg$ if and only if $s \in S$. If this is a graph, then $S = S^{-1}$. If G is an abelian group, we will use additive notation.*

A particularly nice form of transitive action is the regular action.

Definition 2.1.7. *A permutation group G acting on a set Ω is* regular *if its action is sharply transitive; i.e., if for every $v, w \in \Omega$, there is a unique $g \in G$ such that $g(v) = w$.*

Note that every group has a regular action, since any group G can act by right-multiplication on the elements of the set G. This action is called the *right regular action* of the group G on itself.

Let $X = \mathrm{Cay}(G; S)$. Right-multiplying all of the vertices of X by some element $g \in G$, gives an automorphism of X, since $h \sim sh$ if and only if $hg \sim shg$. This automorphism is denoted g_R. The

collection of all such automorphisms forms a regular subgroup isomorphic to G in $\mathrm{Aut}(X)$, called the right regular representation of G, and denoted G_R. Therefore, we have proved the following lemma.

Lemma 2.1.8. *Cayley graphs are vertex-transitive.*

Let $\mathbb{F}_q^+$ denote the additive group of $\mathbb{F}_q$. According to the definition, Paley graphs and generalized Paley graphs are special classes of Cayley graphs. Note that $P_q = \mathrm{Cay}(\mathbb{F}_q^+; (\mathbb{F}_q^*)^2)$, $P(q,d) = \mathrm{Cay}(\mathbb{F}_q^+; (\mathbb{F}_q^*)^d)$, where $(\mathbb{F}_q^*)^d$ is the set of d-th powers in $\mathbb{F}_q^*$.

In algebraic graph theory, a class of problems is related to the automorphism group of graphs. For a given Cayley graph, it is interesting to understand its automorphism group. The following is Alspach's characterization of the automorphism groups of Cayley graphs on p vertices.

Theorem 2.1.9 ([4])**.** *Let p be prime. If $S = \emptyset$ or $S = \mathbb{Z}_p^*$, then* $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p; S)) = \mathrm{Sym}(p)$. *Otherwise,* $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p; S)) = \{T_{a,b} : a \in E(S), b \in \mathbb{Z}_p\}$, *where $E(S)$ is the largest even-order subgroup of $\mathbb{Z}_p^*$ such that S is a union of cosets of $E(S)$, and $T_{a,b}(x) = ax + b$.*

In practice, we have the following efficient Algorithm [87] to determine the automorphism group for a Cayley graph of prime order.

- Find A, the set of all $a \in \mathbb{Z}_p^*$ such that $aS = S$.
- If $A = \mathbb{Z}_p^*$, then $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p; S)) = \mathrm{Sym}(p)$.
- Otherwise, $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p; S)) = \{T_{a,b} : a \in A, b \in \mathbb{Z}_p\}$.

Using this algorithm, for a generalized Paley graph of prime order, it is easy to describe its automorphism group.

Corollary 2.1.10. *If $p \equiv 1 \pmod{2d}$, then* $\mathrm{Aut}(P(p,d)) = \{T_{a,b} : a \in (\mathbb{F}_p^*)^d, b \in \mathbb{F}_p\}$.

For a Paley graph of prime power order, its automorphism group is given by the following theorem.

Theorem 2.1.11 ([20])**.** *The group of automorphism of the Paley graph P_q consists of the maps $x \to ax^\sigma + b$ where $a \in (\mathbb{F}_q^*)^2, b \in \mathbb{F}_q$, and $\sigma = p^j$ with $0 \le j < s$.*

For a generalized Paley graph of prime power order, it is much more difficult to determine its automorphism group. In [74], Lim and Praeger used association scheme to study the automorphism groups of generalized Paley graphs.

In 2001, Alon [2] purposed the following conjecture about the clique number of a Cayley graph on an abelian group.

Conjecture 2.1.12 ([2])**.** *There exists a fixed constant c such that every abelian group G has a subset $S \subseteq G$ with $-S = S$ for which the Cayley graph* $\mathrm{Cay}(G; S)$ *has no clique or independent set of size $> c \log |G|$.*

This conjecture was confirmed in the case that G is a cyclic group by Green and Morris [49, 50].

Theorem 2.1.13 ([49, 50])**.** *For all sufficiently large integers N there exists a set $A \subseteq \mathbb{Z}_N$ for which the Cayley graph $\mathrm{Cay}(\mathbb{Z}_N; A)$ has no cliques or independent sets of size $160 \log_2 N$. For any $\epsilon > 0$ and for all sufficiently large primes N there exists a set $A \subseteq \mathbb{Z}_N$ for which the Cayley graph $\mathrm{Cay}(\mathbb{Z}_N; A)$ has no cliques or independent sets of size $(2+\epsilon)\log_2 N$.*

In fact, they showed a stronger statement that almost all Cayley graphs on $\mathbb{F}_p^+ \cong \mathbb{Z}_p$ has clique number $(2+\epsilon)\log_2 p$. In Sections 2.5, 3.5, and 3.6, we will explore the lower bounds on the clique number of Paley graphs, and we will see in Corollary 3.5.5 that Paley graphs are "exceptional" Cayley graphs in terms of the clique number.

2.2 Self-complementary symmetric graphs

Definition 2.2.1. *A graph X is* self-complementary *if it is isomorphic to its complement.*

Lemma 2.2.2. *If X is self-complementary, then $\omega(X) = \alpha(X)$.*

Proof. Since X is self-complementary, there is a one-to-one correspondence between the cliques in X and the independent sets (with the same size) in X. In particular, $\omega(X) = \alpha(X)$. □

Lemma 2.2.3. *Paley graphs are self-complementary.*

Proof. Let $X = P_q$, and let r be a quadratic non-residue in $\mathbb{F}_q$. Consider the bijective map $f : \mathbb{F}_q \to \mathbb{F}_q$ defined by $f(x) = rx$ for each $x \in \mathbb{F}_q$. Then for any $x, y \in \mathbb{F}_q$ with $x \neq y$, $x \sim_X y$ iff $y - x$ is a quadratic residue; $f(x) \sim_{X^c} f(y)$ iff $r(y-x)$ is a quadratic non-residue. Since r is a quadratic non-residue, f defines a graph isomphism from X to X^c. □

There are many nice results on self-complementary graphs; we refer to [38].

Definition 2.2.4. *A graph is* symmetric *if its automorphism group acts transitively on the vertices and edges.*

Lemma 2.2.5. *Paley graphs are symmetric.*

Proof. Paley graphs are special classes of Cayley graphs, so they are vertex-transitive. To show Paley graphs are symmetric, it suffices to prove they are edge-transitive.

Given the Paley graph P_q, we consider two adjacent pair of vertices $x_1 \sim y_1$, $x_2 \sim y_2$. Let $a = \frac{y_2 - x_2}{y_1 - x_1}$, and let $b = x_2 - a x_1$. Then the linear transformation $T_{a,b}$ maps x_1 to x_2, and maps y_1 to y_2. Moreover, by Theorem 2.1.11, $T_{a,b} \in \mathrm{Aut}(P_q)$. Therefore, Paley graphs are edge-transitive. □

We see Paley graphs are self-complementary and symmetric. Zhang [130] gave the following algebraic characterization on self-complementary symmetric graphs.

Theorem 2.2.6 ([130]). *A graph is self-complementary and symmetric if and only if it is isomorphic to a Cayley graph $X = \mathrm{Cay}(V; O_H)$, where V is the additive group of the vector space of dimension r over the finite field with p elements, $p^r \equiv 1 \pmod 4$, and O_H is an orbit of a group H, where H is contained in another group G, such that $[G : H] = 2, G, H \subset GL(V)$, G is transitive on $V \setminus \{0\}$, and H is not transitive on $V \setminus \{0\}$.*

From this characterization, it does not follow whether such graphs, other than the well-known Paley graphs, exist. In [96], Peisert discovered a new infinite family of self-complementary symmetric graphs, called P^*-graphs (Peisert graphs). Similar to Paley graphs, Peisert graphs are defined on finite fields.

Definition 2.2.7. *The* Peisert graph *of order $q = p^r$, where $p \equiv 3 \pmod 4$ and r is even, denoted P_q^*, is defined to be the graph with vertices in $\mathbb{F}_q$. Two elements are adjacent if their difference belongs to the set $M = \{g^j : j \equiv 0, 1 \pmod 4\}$, where g is a primitive root of the field. Equivalently, $P_q^* = \mathrm{Cay}(V_q^+; M)$.*

Let $p \equiv 3 \pmod 4$ and let r be even. Let g be a primitive roots of the field $\mathbb{F}_{p^r}$, then the set $M = \{g^j : j \equiv 0, 1 \pmod 4\}$ satisfies $M = -M$ since $p^r \equiv 1 \pmod 8$ implies $g^{4k} = -1$ for some integer k. Therefore, $P^*(p^r)$ is an undirected graph. It is easy to see that the definition does not depend on the choice of the primitive root. In Section 6 of [96], by considering the automorphism groups, Peisert showed that P_q and P_q^* are not ismorphic except when $q = 9$.

Theorem 2.2.8 (Theorem 3.1 in [96]). *Let $q = p^r$, where $p \equiv 3 \pmod 4$ and r is even. The Peisert graph P_q^* is self-complementary and symmetric.*

Proof. Let g be a primitive roots of the field $\mathbb{F}_q$. Since $M \cap g^2M = \emptyset$ and $M \cup g^2M = \mathbb{F}_q^*$, it follows that the map $x \mapsto g^2x$ defines a graph isomorphism from P_q^* to its complement. So P_q^* is self-complementary.

Every Cayley graph is vertex-transitive, and so is $X = P_q^*$. It remains to show X is edge-transitive. First, the permutation $\beta : x \mapsto g^4x$ is clearly an automorphism of X. It has two orbits on the set of edges incident with 0, namely

$$O_1 = \{xy | x - y = g^{4k} \text{ for some integer } k\}, \text{ and } O_2 = \{xy | x - y = g^{4k+1} \text{ for some integer } k\}.$$

Note that $\mathrm{Aut}(X)$ acts transitively on the orbits O_1 and O_2.

Let $\phi : x \mapsto x^p$ be the Frobenius automorphism of the field $\mathbb{F}_q$. Now, consider another permutation γ of $\mathbb{F}_q$, which maps each x to $g\phi(x)$. Let xy be an edge in X, then we have the following two cases:

- If $x - y = g^{4k}$ for some integer k, then $\gamma(x) - \gamma(y) = g\phi(x - y) = g^{4kp+1}$.
- If $x - y = g^{4k+1}$ for some integer k, then $\gamma(x) - \gamma(y) = g\phi(x - y) = g^{(4k+1)p+1} = g^{4s}$ for some integer s, since $p \equiv 3 \pmod 4$.

Therefore, γ is a graph automorphism of X, and it exchanges the orbits O_1 and O_2 of β. Therefore, $\mathrm{Aut}(X)$ acts transitively on the set of edges incident with 0. Since X is vertex-transitive, it follows that X is edge-transitive. □

In [95], Peisert proved that the Paley graphs of prime order are the only self-complementary symmetric graphs of prime order; furthermore, in [96], he proved that the following theorem.

Theorem 2.2.9 ([96])**.** *A graph G is self-complementary and symmetric if and only if $|G| = p^r \equiv 1 \pmod 4$ for some prime p, and G is isomorphic to the Paley graph P_q, or the Peisert graph $PG^*(q)$, or the exceptional graph $G(23^2)$ with 23^2 vertices.*

The definition of the exceptional graph $G(23^2)$ is complicated and can be found in Section 3 in [96].

Motivated by the similarity shared by Paley graphs and Peisert graphs, and the introduction of generalized Paley graphs, Natalie Mullin introduced generalized Peisert graphs in Section 5.3 of [91]. (It seems the original definition is not quite correct; we need $q \equiv 1 \pmod{2d}$ to make $P^*(q,d)$ undirected.)

Definition 2.2.10. *Let d be a positive even integer, and let q be a prime power such that $q \equiv 1 \pmod{2d}$. The* d-th power Peisert graph *of order q, denoted $P^*(q,d)$, is the graph with vertex set $\mathbb{F}_q$, where two vertices x and y are adjacent if and only if $x - y \in M_d$, where*

$$M_d = \left\{ g^{dk+i} : 0 \le i \le \frac{d}{2} - 1, k \in \mathbb{Z} \right\},$$

and g is a primitive root of $\mathbb{F}_q^*$.

Note that $P^*(q,2)$ is precisely the Paley graph P_q, and $P^*(q,4)$ is precisely the Peisert graph P_q^* if $p \equiv 3 \pmod 4$. It is straightforward to show generalized Peisert graphs are also self-complementary (see Lemma 5.3.5 in [91]).

(Generalized) Paley graphs and Peisert graphs have many nice properties, and they have many applications in coding theory and design theory; see for example [58], [122], [75], [68].

Finally, we make use of the self-complementary property to upper bound the clique number of generalized Paley graphs and generalized Peisert graphs.

Theorem 2.2.11. *If $q \equiv 1 \pmod{2d}$, then $\omega\big(P(q,d)\big) \le \sqrt{q}$, and $\omega\big(P^*(q,d)\big) \le \sqrt{q}$. In particular, if $q \equiv 1 \pmod 4$, then $\omega(P_q) \le \sqrt{q}$; if $q = p^r$, where $p \equiv 3 \pmod 4$ and r is even, then $\omega(P_q^*) \le \sqrt{q}$.*

Proof. Let $N = \omega\big(P(q,d)\big)$ and let $C = \{v_1, v_2, \ldots, v_N\} \subset \mathbb{F}_q$ be a clique of the maximum size in $P(q,d)$. Let g be a be a primitive root of $\mathbb{F}_q^*$, and consider the set $W = \{v_i + gv_j : 1 \le i, j \le N\}$. 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 $|W| = N^2 \le q$, i.e. $N \le \sqrt{q}$.

For a generalized Peisert graph $P^*(q,d)$, we can proceed in a similar way. Let g be a primitive root of $\mathbb{F}_q^*$, we consider the set $W = \{v_i + g^{d/2}v_j : 1 \le i, j \le N\}$. □

In general, for a vertex-transitive graph, we have the following clique-coclique bound.

Theorem 2.2.12 (Clique-coclique bound, Theorem 3.9 in [30])**.** *If X is vertex-transitive, then $\omega(X)\alpha(X) \leq |V(X)|$.*

We have shown that Cayley graphs are vertex-transitive, so we have the following corollary.

Corollary 2.2.13. *If X is a self-complementary Cayley graph, then $\omega(X) \leq \sqrt{|V(X)|}$. In particular, if $q \equiv 1 \pmod 4$, then $\omega(P_q) \leq \sqrt{q}$; if $q = p^r$, where $p \equiv 3 \pmod 4$ and r is even, then $\omega(P_q^*) \leq \sqrt{q}$.*

Proof. Since X is a Cayley graph, it is vertex-transitive. Since X is self-complementary, we have $\omega(X) = \alpha(X)$. So by clique-coclique bound, we have $\omega^2(X) = \omega(X)\alpha(X) \leq |V(X)|$. Since Paley graphs and Peisert graphs are self-complementary Cayley graphs, the upper bounds on their clique numbers follow. □

2.3 Strongly regular graphs

In this section, we will prove that Paley graphs are strongly regular. We start with the basic terminology.

Definition 2.3.1. *A graph X is* d-regular *if all of the vertices have the same degree d.*

Definition 2.3.2. *A graph X is a* strongly regular graph *with parameters (n, d, λ, μ), denoted* $\mathrm{srg}(n, d, \lambda, \mu)$*, if X is a d-regular graph with n vertices, such that any two adjacent vertices have λ common neighbors, and any two non-adjacent vertices have μ common neighbors.*

Definition 2.3.3. *A strongly regular graph $\mathrm{srg}(n, d, \lambda, \mu)$ whose parameters satisfy $d = (n-1)/2, \lambda = (n-5)/4$, and $\mu = (n-1)/4$ are called conference graphs.*

Definition 2.3.4. *Let X be a graph, we say x is an eigenvalue of X if x is an eigenvalue of the adjacency matrix of X.*

The following lemma shows that for a regular graph X, the spectrum of $\overline{X}$ can be deduced from the spectrum of X.

Lemma 2.3.5. *Let X be a k-regular graph on n vertices. Then k is an eigenvalue of X. Moreover, if X has eigenvalues $k, \lambda_1, \lambda_2, \ldots, \lambda_{n-1}$, then the eigenvalues of the complement $\overline{X}$ are $n-1-k, -1-\lambda_1, -1-\lambda_2, \ldots, -1-\lambda_{n-1}$.*

Proof. Let $A(X)$ and $A(\overline{X})$ be the adjacency matrix of X and $\overline{X}$, respectively. Let w be the all-1 vector. Since X is k-regular, then $A(X)w = kw$. Also, $\overline{X}$ is $(n-1-k)$-regular and $A(\overline{X})w = (n-1-k)w$. So k is an eigenvalue of $A(X)$ and $n-1-k$ is an eigenvalue of $A(\overline{X})$.

Let λ be an eigenvalue of $A(X)$ with eigenvector v, such that v is orthogonal to the all ones vectors. Let $v = (v_1, \ldots, v_n)$, then $\sum_{i=1}^{n} v_i = 0$. Let I be the identity matrix, and let J be the all-1 matrix. Then $Jv = 0$ and $A(X) + A(\overline{X}) = J - I$. Therefore,

$$\big(A(X) + A(\overline{X})\big)v = -v,$$

and thus

$$A(\overline{X})v = -v - A(X)v = (-1 - \lambda)v,$$

i.e. v is an eigenvector for $A(\overline{X})$ with eigenvalue $-1 - \lambda$.

Note that $A(X)$ and $A(\overline{X})$ are real symmetric matrices, so both matrices has an eigenbasis. The above argument shows that they actually share the same eigenbasis, but corresponding to different eigenvalues. If $A(X)$ has eigenvalues $k, \lambda_1, \lambda_2, \ldots, \lambda_{n-1}$, then the eigenvalues of $A(\overline{X})$ are $n - 1 - k, -1 - \lambda_1, -1 - \lambda_2, \ldots, -1 - \lambda_{n-1}$. □

Theorem 2.3.6. *If $q \equiv 1 \pmod 4$, then P_q is a connected strongly regular $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$ graph. Moreover, the eigenvalues of P_q are $\frac{q-1}{2}$ (with multiplicity 1), $\frac{1}{2}(-1 \pm \sqrt{q})$ (each with multiplicity $\frac{q-1}{2}$).*

Proof. Let A be the adjacency matrix of P_q, then A is symmetric. It is clear that P_q is $\frac{q-1}{2}$ regular, so the (u, u)-entry of A^2 is $\frac{q-1}{2}$ for each $u \in \mathbb{F}_q$. Let χ be the standard quadratic character, then for each $u \neq v$,

$$\sum_{x \in \mathbb{F}_q} \chi(x-u)\chi(x-v) = \sum_{x \in \mathbb{F}_q} \chi(x)\chi(x+u-v) = \sum_{x \in \mathbb{F}_q^*} \chi(x^2)\chi\left(\frac{x+u-v}{x}\right) = \sum_{x \in \mathbb{F}_q^*} \chi\left(1 + \frac{u-v}{x}\right),$$

note that as x runs over $\mathbb{F}_q^*$, $\frac{u-v}{x}$ also runs over $\mathbb{F}_q^*$, so

$$\sum_{x \in \mathbb{F}_q} \chi(x-u)\chi(x-v) = \sum_{x \in \mathbb{F}_q^*} \chi(1+x) = \sum_{x \in \mathbb{F}_q} \chi(x) - \chi(1) = -1.$$

Then for each $u \neq v$, the (u, v) entry of A^2 is

$$\frac{1}{4} \sum_{x \in \mathbb{F}_q} \big(\chi(x-u) + 1\big)\big(\chi(x-v) + 1\big) - \frac{1}{2}\big(\chi(u-v) + 1\big) = \frac{q-1}{4} - \frac{1}{2}\big(\chi(u-v) + 1\big).$$

So the (u, v) entry of A^2 is $\frac{q-5}{4}$ when u, v are adjacent, and the (u, v) entry of A^2 is $\frac{q-1}{4}$ when u, v are not adjacent. Therefore, P_q is a strongly regular $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$ graph.

To see P_q is connected, notice that if u, v are non-adjacent vertices of P_q, then they have $\frac{q-1}{4} \geq 1$ common neighbors, and thus there is a path of length 2 from u to v.

Let $R = A^2 + A$. The (u, u)-entry of R is $\frac{q-1}{2}$ for each $u \in \mathbb{F}_q$. If $u \neq v$, then the (u, v) entry of R is $\frac{q-5}{4} + 1 = \frac{q-1}{4}$ when u, v are adjacent, and the (u, v) entry of R is $\frac{q-1}{4} + 0 = \frac{q-1}{4}$ when u, v are not adjacent. Therefore, $R = \frac{q-1}{4}(I + J)$, where I is the identity matrix, and J is the all-1 matrix.

Note that $Jw = qw$, where w is the all-1 vector, so q is an eigenvalue of J. Since $\operatorname{rank} J = 1$, we conclude that q is an eigenvalue of J with multiplicity 1, and 0 is eigenvalue of J with multiplicity $q-1$. Therefore, $\frac{q-1}{4}(1+q) = \frac{q^2-1}{4}$ is an eigenvalue of R with multiplicity 1, and $\frac{q-1}{4}$ is eigenvalue of R with multiplicity $q-1$.

If z is an eigenvalue of A, then z^2+z is an eigenvalue of R. Note that the eigenvalue $\frac{q-1}{2}$ of A corresponds to the eigenvalue $\frac{q^2-1}{4}$ of R (both with multiplicity 1). So every eigenvalue $z \neq \frac{q-1}{2}$ of A satisfies $z^2+z = \frac{q-1}{4}$, i.e. $z \in \{\frac{1}{2}(-1-\sqrt{q}), \frac{1}{2}(-1+\sqrt{q})\}$. Since P_q is self-complementary, by Lemma 2.3.5, it follows that the multiplicity of both $\frac{1}{2}(-1-\sqrt{q})$ and $\frac{1}{2}(-1+\sqrt{q})$ is $\frac{q-1}{2}$. □

Definition 2.3.7. *A* pseudo-Paley graph *is a strongly regular graph with the same parameters n, d, λ, μ as a Paley graph.*

Similar to the proof in Theorem 2.3.6, one can prove the following.

Proposition 2.3.8 ([122])**.** *Peisert graphs are pseudo-Paley graphs.*

Together with Theorem 2.2.9, we have the following corollary.

Corollary 2.3.9. *Apart from the exceptional graph $G(23^2)$ with 23^2 vertices, the graphs P_q and P_q^* are the only pseudo-Paley graphs that are self-complementary and symmetric.*

Recently, Klin, Kriger, and Woldar [70] used association schemes based on affine planes to construct pseudo-Paley graphs of order p^2. Most of these are neither self-complementary nor symmetric for sufficiently large primes p.

Delsarte, in his Ph.D. thesis [30], generalized the MacWilliams transform of coding theory to the theory of association schemes and gave some powerful applications. In particular, for a strongly regular graph, we have the following Delsarte bound (also known as the ratio bound) on the clique number.

Theorem 2.3.10 (Delsarte bound)**.** *For a d-regular strongly regular graph X with smallest eigenvalue $r < 0$, $\omega(X) \leq \lfloor 1 - d/r \rfloor$.*

Therefore, since one can write s in terms of the parameters of X, one can determine the Delsarte bound knowing only the parameters (n, d, λ, μ) of X.

Corollary 2.3.11. *If $q \equiv 1 \pmod 4$, then $\omega(P_q) \leq \sqrt{q}$; if $q = p^r$, where $p \equiv 3 \pmod 4$ and r is even, then $\omega(P_q^*) \leq \sqrt{q}$.*

Proof. Let $q \equiv 1 \pmod 4$. We have shown that P_q is $\frac{q-1}{2}$-regular, and the smallest eigenvalue of P_q is $-\frac{\sqrt{q}+1}{2}$. So by Delsarte bound,

$$\omega(P_q) \leq \left\lfloor 1 + \frac{q-1}{\sqrt{q}+1} \right\rfloor \leq 1 + \sqrt{q} - 1 = \sqrt{q}.$$

The proof for the upper bound on the clique number of Peisert graphs is similar. □

2.4 Clique number of random induced subgraphs

In this section, we show that we can expect that the clique number of a random induced subgraph of P_q is much smaller than $\sqrt{q}$.

Definition 2.4.1 ((n, d, λ)-expander graph)**.** *If X is a n-vertex d-regular graph with the second largest eigenvalue (in absolute values) of its adjacency matrix upper bounded by λ, then we say X is an (n, d, λ)-expander graph.*

We have shown P_q is a strongly regular graph and we have determined its eigenvalues. It follows that P_q is a $(q, \frac{q-1}{2}, \frac{\sqrt{q}+1}{2})$-expander graph.

Lemma 2.4.2 (Lemma 2.2 in [3])**.** *Let $X = (V, E)$ be an an (n, d, λ)-expander graph, and let $B \subset V$ be a subset of bn vertices of G. Let*

$$C = \left\{ v \in V : |N(v) \cap B| \leq \frac{d|B|}{2n} = \frac{db}{2} \right\},$$

then $|B \cap C| < \frac{2\lambda}{d} n$.

Proof. Let A denote the adjacency matrix of X, and define a vector $x = (x_v : v \in V)$ by $x_v = -b$ if $v \notin B$ and $x_v = 1 - b$ if $v \in B$. As the sum of coordinates of x is zero, it is orthogonal to the all-1 vector, which is the eigenvector of the largest eigenvalue of A. Then

$$||Ax||^2 = x^T A^T A x \leq \lambda^2 x^T x = \lambda^2 b(1-b)n.$$

On the other hand,

$$||Ax||^2 = \sum_{v \in V} \big(|N(v) \cap B|(1-b) - (d - |(N(v) \cap B|)b\big)^2 = \sum_{v \in V} \big(|N(v) \cap B| - db\big)^2.$$

Therefore,

$$\sum_{v \in V} \big(|N(v) \cap B| - db\big)^2 \leq \lambda^2 b(1-b)n.$$

Note that each $v \in C$ contributes to the left-hand side more than $d^2 b^2/4$, so

$$|C| d^2 b^2/4 < \lambda^2 b(1-b)n < \lambda^2 bn.$$

It follows that $|B||C| < \frac{4\lambda^2}{d^2} n^2$, and therefore $|B \cap C| \leq \min\{|B|, |C|\} < \frac{2\lambda}{d} n$. □

Theorem 2.4.3 (Theorem 2.1 in [3])**.** *Let $X = (V, E)$ be an (n, d, λ)-expander graph. Then for any $m \geq s = \frac{2n}{d} \log n$, the number of independent sets of size m in X is at most*

$$\frac{1}{m!} \binom{m}{s} n^s \left(\frac{2\lambda}{d} n \right)^{m-s}$$

Proof. Consider the number of m-triples $(v_1, v_2, \ldots, v_m)$ of m vertices in X that form an independent set. Let $B_0 = V$, and let B_i denote the set of vertices that are not adjacent to any vertex among $v_1, v_2, \ldots, v_i$. Then $v_j \in B_i$ if $j > i$. For each $0 \le i \le m$, define

$$C_i = \left\{ u \in V : |N(u) \cap B_i| \le \frac{d|B_i|}{2n} \right\},$$

then by Lemma 2.4.2, $|B_i \cap C_i| < \frac{2\lambda}{d} n$.

Note that $(1 - 1/x)^x < 1/e$ for any $x > 0$, so $n(1 - \frac{d}{2n})^s < 1$. Also note that if the $v_{i+1} \notin C_i$, then $|B_{i+1}| < (1 - \frac{d}{2n})|B_i|$. It follows that with at most s possible exceptions, v_{i+1} has to lie in $B_i \cap C_i$. So the number of m-triples $(v_1, v_2, \ldots, v_m)$ is at most

$$\binom{m}{s} n^s \left(\frac{2\lambda}{d} n \right)^{m-s}. \qquad \square$$

Corollary 2.4.4 (Theorem 6 in [90]). *Let X be an (n, d, λ)-expander graph with $d \ge 1$, $\lambda \ge 1/2$, and let $m \ge 2n \log^2 n/d$ be an integer. Then the number of independent sets of size m in X is at most $(\frac{2e^2\lambda}{\log^2 n})^m$.*

Proof. By Theorem 2.4.3, the number of independent sets of size m in X is at most

$$\frac{1}{m!} \binom{m}{s} n^s \left(\frac{2\lambda}{d} n \right)^{m-s} \le \left(\frac{e}{m} \right)^m 2^m n^s \left(\frac{2\lambda}{d} n \right)^{m-s} = \left(\frac{2e}{m} \right)^m \left(\frac{2\lambda}{d} n \right)^m \left(\frac{d}{2\lambda} \right)^s,$$

where $s = \frac{2n}{d} \log n$. Since $\lambda \ge 1/2$, we have $\frac{d}{2\lambda} \le d \le n$, and thus

$$\left(\frac{d}{2\lambda} \right)^s \le n^s \le n^{m/\log n} = e^m.$$

Therefore, the number of independent sets of size m in X is at most

$$\left(\frac{2e}{m} \right)^m \left(\frac{2\lambda}{d} n \right)^m \left(\frac{d}{2\lambda} \right)^s \le \left(\frac{4e\lambda n}{dm} \right)^m e^m \le \left(\frac{2e^2\lambda}{\log^2 n} \right)^m. \qquad \square$$

Finally we present the proof of a claim made by Dhruv Mubayi and Jacques Verstraete in the concluding remarks of [90]. Roughly speaking, it states that the upper bound of the clique number of a random subgraph of P_q can be greatly improved.

Proposition 2.4.5 ([90]). *Let U be a random set of vertices of P_q where each vertex is chosen independently with probability*

$$x = \frac{\log^2 q}{2e^2(\sqrt{q} + 1)},$$

then almost surely the induced subgraph $P_q[U]$ has clique number at most $\lceil 4q \log^2 q/(q-1) \rceil$.

Proof. Let $Z(U)$ be the number of independent sets of size $m = \lceil 4q \log^2 q/(q-1) \rceil$ in the induced subgraph $P_q[U]$. Note that the probability that all vertices of an independent sets of size m in P_q

are contained in U is x^m. Then by Corollary 2.4.4 and the choice of x,

$$\mathbb{E}[Z(U)] \le x^m \Big(\frac{e^2(\sqrt{q}+1)}{\log^2 q}\Big)^m = 2^{-m}.$$

Therefore $\Pr[Z(U) \ge 1] \le 2^{-m}$ and $\Pr[Z(U) = 0] \ge 1 - 2^{-m}$, i.e. the probability that the induced graph $P_q[U]$ has no independent sets of size m is at least $1 - 2^{-m}$. Since P_q is self-complementary, this also implies that the probability that the induced graph $P_q[U]$ has no clique of size m is at least $1 - 2^{-m}$. Note that as $q \to \infty$, $m \to \infty$, so we have $1 - 2^{-m} \to 1$. Therefore, almost surely we have $\omega\big(P_q[U]\big) \le \lceil 4q \log^2 q/(q-1) \rceil$. □

The concluding remarks in [90] also mentioned that Alon had already observed a better statement (in 1991, unpublished): there exists $\alpha \in (0,1)$ such that one can randomly take q^α vertices from P_q, such that the resulting induced subgraph almost surely has clique number $O(\log q)$. We will discuss the polylogarithmic bounds on the clique number in Sections 3.5 and 3.6. We will see that the $O(\log^2 q)$ bound obtained in Proposition [90] is not surprising, while the unpublished result by Alon, the $O(\log q)$ bound, is very impressive.

2.5 Clique numbers and diagonal Ramsey numbers

The *Ramsey number* $R(k,\ell)$, introduced by Ramsey [97], is defined to be smallest positive integer n such that every graph on n vertices contains a complete subgraph on k or the empty graph on ℓ vertices. In other words, if X is a graph with at least $R(k,\ell)$ vertices, then either $\omega(X) \ge k$ or $\alpha(X) \ge \ell$. In 1935, Erdős and Szekeres [33] gave the classic upper bound

$$R(k+1, \ell+1) \le \binom{k+\ell}{k}. \tag{2.1}$$

When $k = \ell$, we call $R(k,k)$ the *diagonal Ramsey number*. Note if X is a self-complementary graph with at least $R(k,k)$ vertices, then $\omega(X) = \alpha(X) \ge k$.

The best known upper bound on Ramsey numbers is due to Ashwin Sah (2020).

Theorem 2.5.1 ([103])**.** *There is an absolute constant $c > 0$, such that when $k \ge 3$,*

$$R(k+1, k+1) \le \exp\big(-c(\log k)^2\big)\binom{2k}{k}.$$

Corollary 2.5.2. *Let c be the absolute constant as in Theorem 2.5.1. If X is a self-complementary graph with m vertices, then $\omega(X) \ge \log_4 m + \frac{c(\log\log m)^2}{2\log 2} + O(\log\log m)$.*

Proof. If $n \ge R(k,k) \ge \exp(-c(\log(k-1))^2)\binom{2k-2}{k-1}$, then any self-complementary graph with n vertices has a clique of size k. By Stirling's formula,

$$\binom{2k-2}{k-1} = \frac{(2k-2)!}{(k-1)!(k-1)!} \sim \frac{\sqrt{2\pi(2k-2)}(\frac{2k-2}{e})^{2k-2}}{2\pi(k-1)(\frac{k-1}{e})^{2k-2}} = \frac{2^{2k-2}}{\sqrt{\pi(k-1)}}.$$

Let $m = \exp\big(-c(\log(k-1))^2\big)\binom{2k-2}{k-1}$, then

$$\log m = -c(\log k)^2 + (2k-2)\log 2 - \frac{1}{2}\log \pi(k-1) + O(1).$$

So we have $k = \Theta(\log m)$ and $\log k = \log\log m + O(1)$. Therefore,

$$\log m = -c(\log\log m + O(1))^2 + 2k\log 2 + O(\log k) = -c(\log\log m)^2 + 2k\log 2 + O(\log\log m),$$

$$k = \frac{\log m + c(\log\log m)^2 + O(\log\log m)}{2\log 2} = \log_4 m + \frac{c(\log\log m)^2}{2\log 2} + O(\log\log m).$$

Since X is a self-complementary graph with m vertices, it follows that

$$\omega(X) \geq \log_4 m + \frac{c(\log\log m)^2}{2\log 2} + O(\log\log m). \qquad \square$$

Since Paley graphs and Peisert graphs are self-complementary, we have the following lower bound on their clique numbers.

Corollary 2.5.3. *Let c be the absolute constant as in Theorem 2.5.1. If $q \equiv 1 \pmod 4$, then $\omega(P(q)) \geq \log_4 q + \frac{c(\log\log q)^2}{2\log 2} + O(\log\log q)$. If $q = p^r$, where $p \equiv 3 \pmod 4$ and r is even, then $\omega(P_q^*) \geq \log_4 q + \frac{c(\log\log q)^2}{2\log 2} + O(\log\log q)$.*

We have seen that upper bounds on diagonal Ramsey numbers $R(k,k)$ implies lower bounds on clique number $\omega(P_q)$. Conversely, it turned out Paley graphs are sometimes the extremal colorings for determining the lower bound for diagonal Ramsey numbers. From Table 1.1, we have $\omega(P_{17}) = 3$, $\omega(P_{37}) = 4$, $\omega(P_{101}) = 5$, $\omega(P_{109}) = 6$, $\omega(P_{281}) = 7$. It follows that $R(4,4) \geq 18, R(5,5) \geq 38, R(6,6) \geq 102, R(7,7) \geq 110, R(8,8) \geq 282$ [18]. In fact, Greenwood and Gleason [47] showed that $R(4,4) = 18$. By considering nice self-complementary graph that are similar to Paley graphs or Peisert graphs, there are many improved lower bounds on Ramsey numbers. For example, Clapham [21] established $R(7,7) > 113$ (by considering generalized Peisert graphs); Guldan and Tomasta [51] showed that $R(10,10) > 457$ and $R(11,11) > 541$. Based on a new observation on the automorphism group of Paley graphs, Xu, Wu, Liang and Su [126] designed an efficient algorithm on computing clique numbers of Paley graphs and obtained new bounds on 2 diagonal Ramsey numbers: $R(20,20) > 18877, R(21,21) > 25949$.

We can interpret Ramsey number $R(k,\ell)$ as the smallest number, such that any 2-coloring of the edges in a complete graph of order at least $R(k,\ell)$, using red and blue, admits either a monochromatic red complete subgraph of order k, or a monochromatic blue complete subgraph of order ℓ. It is natural to generalize this definition to *multicolor Ramsey numbers*. $R(n_1, n_2, \ldots, n_k)$ is defined to be the smallest number, such that any k-coloring of the edges in a complete graph of order at least $R(n_1, n_2, \ldots, n_k)$, using colors $c_1, c_2, \ldots, c_k$, admits a complete subgraph of order n_i in color c_i for some $1 \leq i \leq k$. Similar to the estimate (2.1), the multicolor Ramsey numbers can be upper bounded by multinomial coefficients [47]

$$R(n_1+1, n_2+1, \ldots, n_k+1) \leq \frac{(n_1+n_2+\cdots+n_k)!}{n_1!n_2!\cdots n_k!}. \tag{2.2}$$

If $n_1 = n_2 = \cdots = n_k = n$, then we denote $R_k(n) := R(n_1, n_2, \ldots, n_k)$ and we call it a *multicolor diagonal Ramsey number*.

Dawsey and McCarthy [28] studied the relationship between the generalized Paley graphs and multicolor Ramsey numbers. They gave lower bounds for the multicolor diagonal Ramsey numbers $R_3(4) \geq 128, R_4(4) \geq 458, R_5(4) \geq 942, R_6(4) \geq 3458$, although these lower bound are not the best known ones. The relationship can be roughly summarized by the following observation.

Proposition 2.5.4. *If $q \equiv 1 \pmod{2d}$, and $\omega\big(P(q,d)\big) = m$, then $R_d(m+1) \geq q+1$.*

Sketch of the proof. Let $G_0 = P(q,d) = \mathrm{Cay}(\mathbb{F}_q^+; (\mathbb{F}_q^*)^d)$ and let g be a primitive root in $\mathbb{F}_q^*$. For each $1 \leq i < d$, we define G_i to be the Cayley graph $\mathrm{Cay}(\mathbb{F}_q^+; g^i(\mathbb{F}_q^*)^d)$. Then the map $x \mapsto g^i x$ clearly defines a graph isomorphism from G_0 to G_i. Therefore, all graphs $G_0, G_1, \cdots, G_{d-1}$ are isomorphic, and in particular, they share the same clique number. Note that the edge sets of $G_0, G_1, \cdots, G_{d-1}$ are disjoint, and the union of them forms the edge set of a complete graph on $\mathbb{F}_q^+$. Now consider the complete graph K on $\mathbb{F}_q^+$, and color the edge ab with color i if ab is an edge in G_i. Then the color i subgraph of K is G_i, and a monochromatic complete subgraph of K is a clique in some G_i. Therefore, if $\omega(G_0) = \omega\big(P(q,d)\big) = m$, then the maximum monochromatic complete subgraph of K has size m, so we must have $R_d(m+1) \geq q+1$. □

Chapter 3

Character sums and Paley graphs

In this chapter, we introduce some basic material on character sums, together with its connection with the clique number of Paley graphs. Readers can refer to [62], a nice survey paper on character sums and their applications.

3.1 Discrete Fourier transform

Let m be a positive integer. Let e_m be the function on $\mathbb{R}$ such that $e_m(x) = \exp(2\pi ix/m)$. We have the following orthogonality relations, which follows trivially from the formula for summing a geometric sequence.

Lemma 3.1.1 (Orthogonality Relations)**.** *For an integer n, we have*

$$\frac{1}{m}\sum_{j=0}^{m-1} e_m(nj) = \begin{cases} 1, & m \mid n \\ 0, & \textit{otherwise.} \end{cases}$$

The following is the definition of the discrete Fourier transform over $\mathbb{Z}/m\mathbb{Z}$, which plays an important role in discrete Fourier analysis.

Definition 3.1.2. *If $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$, for each $n \in \mathbb{Z}/m\mathbb{Z}$, we define*

$$\hat{f}(n) := \frac{1}{m}\sum_{j=0}^{m-1} e_m(-jn)f(j).$$

Similar to the standard Fourier transform defined on $\mathbb{R}$, we could expect a similar inversion formula and Plancherel's identity.

Lemma 3.1.3 (Inversion formula)**.** *If $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$, then for each $n \in \mathbb{Z}/m\mathbb{Z}$,*

$$f(n) = \sum_{j=0}^{m-1} e_m(jn)\hat{f}(j).$$

Proof. By Lemma 3.1.1,

$$\begin{aligned}\sum_{j=0}^{m-1} e_m(jn)\hat{f}(j) &= \frac{1}{m}\sum_{j=0}^{m-1} e_m(jn)\Big(\sum_{k=0}^{m-1} e_m(-kj)f(k)\Big)\\ &= \frac{1}{m}\sum_{j,k=0}^{m-1} e_m\big(j(n-k)\big)f(k)\\ &= \frac{1}{m}\sum_{k=0}^{m-1} f(k)\Big(\sum_{j=0}^{m-1} e_m\big(j(n-k)\big)\Big) = f(n).\end{aligned}$$

□

Lemma 3.1.4 (Plancherel's identity)**.** *If $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$, then*

$$\sum_{j=0}^{m-1} |\hat{f}(j)|^2 = \frac{1}{m}\sum_{j=0}^{m-1} |f(j)|^2.$$

Proof. By Lemma 3.1.1,

$$\begin{aligned}\sum_{j=0}^{m-1} |\hat{f}(j)|^2 &= \frac{1}{m^2}\sum_{j=0}^{m-1}\sum_{k,l=0}^{m-1} e_m\big(-j(k-l)\big)f(k)\overline{f(l)}\\ &= \frac{1}{m^2}\sum_{k,l=0}^{m-1} f(k)\overline{f(l)}\Big(\sum_{j=0}^{m-1} e_m\big(-j(k-l)\big)\Big) = \frac{1}{m}\sum_{j=0}^{m-1} |f(j)|^2.\end{aligned}$$

□

3.2 Characters

Definition 3.2.1. *Let G be a finite abelian group. A* character χ *of G is a homomorphism from G into the multiplicative group U of complex numbers of modulus* 1.

In this chapter, we are interested in the cases that G is the integer ring $\mathbb{Z}/m\mathbb{Z}$ or G is the finite field $\mathbb{F}_q$. When $G = \mathbb{Z}/m\mathbb{Z}$, a Dirichlet character χ modulo m is essentially a character of the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^*$.

Definition 3.2.2. *A* Dirichlet character χ *modulo m is a function $\chi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ that satisfies $|\chi(x)| = 1$ for all $x \in (\mathbb{Z}/m\mathbb{Z})^*$, $\chi(x) = 0$ for all $x \in \mathbb{Z}/m\mathbb{Z} \setminus (\mathbb{Z}/m\mathbb{Z})^*$, and $\chi(xy) = \chi(x)\chi(y)$ for each $x, y \in \mathbb{Z}/m\mathbb{Z}$. We say χ is a* non-principal character *if there is $a \in (\mathbb{Z}/m\mathbb{Z})^*$ such that $\chi(a) \neq 1$.*

Lemma 3.2.3. *For a non-principal Dirichlet character $\chi \pmod m$, we have $\sum_{j=0}^{m-1} \chi(j) = 0$.*

Proof. Pick $a \in (\mathbb{Z}/m\mathbb{Z})^*$ such that $\chi(a) \neq 1$. Note that when j runs over $\mathbb{Z}/m\mathbb{Z}$, aj also runs over $\mathbb{Z}/m\mathbb{Z}$, so

$$\sum_{j=0}^{m-1} \chi(j) = \sum_{j=0}^{m-1} \chi(aj) = \chi(a)\sum_{j=0}^{m-1} \chi(j).$$

Since $\chi(a) \neq 1$, it follows that $\sum_{j=0}^{m-1} \chi(j) = 0$. □

Definition 3.2.4. *Let χ be a Dirichlet character mod m, and let $d \mid m$. The number d is called an* induced modulus *for χ if we have $\chi(a) = 1$ whenever $(a, m) = 1$ and $a \equiv 1 \pmod{d}$.*

The following lemma provides a more detailed characterization of an induced modulus. The proof is simple, and can be found in for example Theorem 8.15 in [7].

Lemma 3.2.5. *Let χ be a Dirichlet character mod m, and let $d \mid m$. Then d is an induced modulus for χ if and only if $\chi(a) = \chi(b)$ whenever $(a, m) = (b, m) = 1$ and $a \equiv b \pmod{d}$.*

Definition 3.2.6. *Let χ be a Dirichlet character mod m. χ is said to be* primitive *if there is no $d \mid m$, $d < m$, such that d is an induced modulus for χ.*

Lemma 3.2.7. *If χ is a primitive Dirichlet character mod m, $d \mid m$ and $1 \leq d < m$, then for any integer k,*

$$\sum_{\substack{0 \leq j \leq m-1 \\ j \equiv k \pmod{d}}} \chi(j) = 0.$$

Proof. Since χ is primitive and $d < m$, d is not an induced modulus for χ. By Lemma 3.2.5, we can find a, b such that $a \equiv b \pmod{d}$, $(a, m) = (b, m) = 1$, and $\chi(a) \neq \chi(b)$. Then there exists an integer c such that $ac \equiv b \pmod{m}$. Then we have $\chi(a)\chi(c)\chi(ac) = \chi(b)$, so $\chi(c) \neq 1$. Note that $c \equiv 1 \pmod{d}$ and $(c, m) = 1$, and so

$$S := \sum_{\substack{0 \leq j \leq m-1 \\ j \equiv k \pmod{d}}} \chi(j) = \sum_{\substack{0 \leq j \leq m-1 \\ j \equiv k \pmod{d}}} \chi(cj) = \chi(c) \sum_{\substack{0 \leq j \leq m-1 \\ j \equiv k \pmod{d}}} \chi(j).$$

Since $\chi(c) \neq 1$, $S = 0$. □

Next we consider the characters of the finite field $\mathbb{F}_q$. Let $q = p^s$. For the finite field $\mathbb{F}_q$ (with characteristic p), there are two finite abelian groups that are of significance, namely, the additive group and the multiplicative group of the field. A character χ of the multiplicative group $\mathbb{F}_q^*$ of $\mathbb{F}_q$ is called a *multiplicative character* of $\mathbb{F}_q$. It is a custom to define $\chi(0) = 0$.

A character of the additive group of $\mathbb{F}_q$ is often said to be an *additive character* of $\mathbb{F}_q$. Let $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ be the absolute trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$:

$$\mathrm{Tr}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{s-1}}.$$

Note that for $c_1, c_2 \in \mathbb{F}_q$, by the binomial theorem, we have $(c_1 + c_2)^{p^k} = c_1^{p^k} + c_2^{p^k}$ for any $k \in \mathbb{N}$, so $\mathrm{Tr}(c_1) + \mathrm{Tr}(c_2) = \mathrm{Tr}(c_1 + c_2)$. Let $\psi_1(c) = e_p\big(\mathrm{Tr}(c)\big)$ for all $c \in \mathbb{F}_q$, so that $\psi_1(c_1 + c_2) = \psi_1(c_1) + \psi_1(c_2)$ for any $c_1, c_2 \in \mathbb{F}_q$. Therefore, ψ_1 is an additive character of $\mathbb{F}_q$, called the *canonical additive character* of $\mathbb{F}_q$, in the sense that all additive characters can be generated by ψ_1.

Lemma 3.2.8 (Theorem 5.7 in [73])**.** *For $b \in \mathbb{F}_q$, the function ψ_b with $\psi_b(c) = \psi_1(bc)$ for all $c \in \mathbb{F}_q$ is an additive character of $\mathbb{F}_q$, and every additive character of $\mathbb{F}_q$ is obtained in this way.*

The following lemma is a generalization of Lemma 3.1.1.

Lemma 3.2.9. *For any $a \in \mathbb{F}_q^*$, we have $S := \sum_{c\in\mathbb{F}_q} e_p\big(\operatorname{Tr}(ac)\big) = 0$.*

Proof. Since $a \in \mathbb{F}_q^*$, as c runs over $\mathbb{F}_q$, ac also runs over $\mathbb{F}_q$, so

$$S = \sum_{c\in\mathbb{F}_q} e_p\big(\operatorname{Tr}(ca)\big) = \sum_{c\in\mathbb{F}_q} e_p\big(\operatorname{Tr}(c)\big).$$

Note that $\operatorname{Tr}(x) = 0$ has at most p^{r-1} solutions, so there exists $y \in \mathbb{F}_q$ such that $\operatorname{Tr}(y) \neq 0$, i.e. $e_p\big(\operatorname{Tr}(c)\big) \neq 1$. Observe that as c runs over $\mathbb{F}_q$, $c + y$ also runs over $\mathbb{F}_q$, so we have

$$S = \sum_{c\in\mathbb{F}_q} e_p\big(\operatorname{Tr}(c)\big) = \sum_{c\in\mathbb{F}_q} e_p\big(\operatorname{Tr}(c+y)\big) = e_p\big(\operatorname{Tr}(y)\big) \sum_{c\in\mathbb{F}_q} e_p\big(\operatorname{Tr}(c)\big) = e_p\big(\operatorname{Tr}(y)\big)S.$$

Therefore, $S = 0$. □

Gauss sums are fundamental in studying various character sums. We first define Gauss sums for a Dirichlet character.

Definition 3.2.10. *For a Dirichlet character χ mod m, we define the* Gauss sum *to be $G(\chi; a) = \sum_{j=0}^{m-1} e_m(aj)\chi(j)$. We denote $G(\chi) := G(\chi; 1) = \sum_{j=0}^{m-1} e_m(j)\chi(j)$.*

Using the triangle inequality, we have the trivial bound $|G(\chi)| \leq m$. In fact, we have the following celebrated result on Gauss sums.

Theorem 3.2.11. *If χ is a primitive Dirichlet character mod m, then $|G(\chi)| = \sqrt{m}$.*

Proof. By Plancherel's identity,

$$\sum_{j=0}^{m-1} |\hat{\chi}(j)|^2 = \frac{1}{m} \sum_{j=0}^{m-1} |\chi(j)|^2 = \frac{\phi(m)}{m}.$$

By Lemma 3.2.3,

$$\hat{\chi}(0) = \frac{1}{p} \sum_{j=0}^{p-1} \chi(j) = 0. \tag{3.1}$$

If $(a, m) = d > 1$, then by Lemma 3.2.7, we have

$$\hat{\chi}(a) = \frac{1}{m} \sum_{j=0}^{m-1} e_m(-aj)\chi(j) = \frac{1}{m} \sum_{k=0}^{m/d-1} e_m(-dk) \bigg(\sum_{j=0}^{d-1} \chi(jd + k) \bigg) = 0. \tag{3.2}$$

For each $a \in (\mathbb{Z}/m\mathbb{Z})^*$, when j runs over $\mathbb{Z}/m\mathbb{Z}$, aj also runs over $\mathbb{Z}/m\mathbb{Z}$, so we have

$$\hat{\chi}(a) = \frac{1}{m} \sum_{j=0}^{m-1} e_m(-aj)\chi(j) = \chi(a^{-1}) \frac{1}{m} \sum_{j=0}^{m-1} e_m(-aj)\chi(aj) = \chi(a^{-1})\hat{\chi}(1). \tag{3.3}$$

It follows that $|\hat{\chi}(1)| = |\hat{\chi}(a)|$ for each $a \in (\mathbb{Z}/m\mathbb{Z})^*$, so we have $|\hat{\chi}(1)| = \frac{1}{\sqrt{m}}$ and $|G(\chi)| = m|\hat{\chi}(1)| = \sqrt{m}$. □

The following corollary is useful in many applications.

Corollary 3.2.12. *If χ is a primitive Dirichlet character mod m, then for each $a \in Z/mZ$,*

$$\overline{\chi(a)} = \frac{1}{G(\chi)} \sum_{j=0}^{m-1} e_m(-aj)\chi(j).$$

Proof. If $a \in (Z/mZ)^*$, then by equation (3.3), we have $\hat{\chi}(a) = \chi(a^{-1})\hat{\chi}(1) = \overline{\chi(a)}\hat{\chi}(1)$. If $a \notin (Z/mZ)^*$, then by equations (3.1) and (3.2), we have $\hat{\chi}(a) = \chi(a) = 0$. Therefore, for each $a \in Z/mZ$, we have

$$\overline{\chi(a)} = \frac{\hat{\chi}(a)}{\hat{\chi}(1)} = \frac{1}{m\hat{\chi}(1)} \sum_{j=0}^{m-1} e_m(-aj)\chi(j) = \frac{1}{G(\chi)} \sum_{j=0}^{m-1} e_m(-aj)\chi(j). \qquad \square$$

The Gauss sums can be also defined in the finite field $\mathbb{F}_q$. Let χ be a multiplicative and ψ an additive character of $\mathbb{F}_q$; then the *Gauss sum* is defined to be $G(\chi, \psi) = \sum_{c \in \mathbb{F}_q} \chi(c)\psi(c)$. We denote $G(\chi) := G(\chi, \psi_1)$, where ψ_1 is the canonical additive character of $\mathbb{F}_q$. Similar to Theorem 3.2.11 and Corollary 3.2.12, we have the following analogous versions of results for characters in $\mathbb{F}_q$.

Theorem 3.2.13 (Theorem 5.11 in [73])**.** *Let χ be a multiplicative and ψ an additive character of $\mathbb{F}_q$. If χ, ψ are non-trivial, then $|G(\chi, \psi)| = \sqrt{q}$.*

Theorem 3.2.14 (Theorem 5.12 in [73])**.** *Let χ be a multiplicative character of $\mathbb{F}_q$. Then for any $a \in \mathbb{F}_q$,*

$$\overline{\chi(a)} = \frac{G(\chi, \psi_a)}{G(\chi, \psi_1)} = \frac{1}{G(\chi)} \sum_{c \in \mathbb{F}_q} \chi(c)\psi_a(c) = \frac{1}{G(\chi)} \sum_{c \in \mathbb{F}_q} \chi(c) e_p\big(\operatorname{Tr}(ac)\big).$$

3.3 The Pólya-Vinogradov inequality

The following is the well-known Pólya-Vinogradov inequality. We follow the proof by Schur [107].

Theorem 3.3.1 (Pólya-Vinogradov inequality)**.** *Let $m \geq 2$, and let χ be a primitive Dirichlet character modulo m. Then for any integers $M \leq N$,*

$$\left| \sum_{M \leq n \leq N} \chi(n) \right| < \sqrt{m} \log m.$$

Proof. By Theorem 3.2.11 and Corollary 3.2.12,

$$\begin{aligned}\left|\sum_{M\le n\le N}\chi(n)\right| &= \frac{1}{\sqrt{m}}\left|\sum_{M\le n\le N}\sum_{j=1}^{m-1}\overline{\chi(j)}e_m(nj)\right| \\ &= \frac{1}{\sqrt{m}}\left|\sum_{j=1}^{m-1}\overline{\chi(j)}\Big(\sum_{M\le n\le N}e_m(nj)\Big)\right| \\ &= \frac{1}{\sqrt{m}}\left|\sum_{j=1}^{m-1}\overline{\chi(j)}e_m(Mj)\frac{1-\exp\big(2\pi i(N-M+1)/m\big)}{1-\exp(2\pi ij/m)}\right| \\ &\le \frac{1}{\sqrt{m}}\sum_{j=1}^{m-1}\frac{1}{\sin(\frac{\pi j}{m})} = \sqrt{m}\sum_{j=1}^{m-1}\frac{1}{m\sin(\frac{\pi j}{m})}.\end{aligned}$$

Note that the function $\frac{1}{\sin(\pi x)}$ is convex in the interval $(0,1)$, so by Jensen's inequality,

$$\left|\sum_{M\le n\le N}\chi(n)\right| \le \sqrt{m}\sum_{j=1}^{m-1}\frac{1}{m\sin(\frac{\pi j}{m})} \le \sqrt{m}\int_{\frac{1}{2m}}^{1-\frac{1}{2m}}\frac{1}{\sin(\pi x)}\,dx = 2\sqrt{m}\int_{\frac{1}{2m}}^{\frac{1}{2}}\frac{1}{\sin(\pi x)}\,dx.$$

Finally, since $\sin(\pi x) > 2x$ in $(0,\frac{1}{2})$,

$$\left|\sum_{M\le n\le N}\chi(n)\right| < 2\sqrt{m}\int_{\frac{1}{2m}}^{\frac{1}{2}}\frac{1}{2x}\,dx = \sqrt{q}\left(\log\frac{1}{2}-\log\frac{1}{2m}\right) = \sqrt{m}\log m. \qquad \square$$

Theorem 3.3.2. *Let χ be a non-principal Dirichlet character modulo m. Then for any integers $M \le N$, we have*

$$\left|\sum_{M\le n\le N}\chi(n)\right| < 2\sqrt{m}\log m.$$

Proof. If χ is primitive, the inequality follows from the Pólya-Vinogradov inequality. Next assume that χ is not primitive. Then χ is induced by a primitive character χ_1 modulo m', with $m = m'r$. Then $\chi_1(n) = \chi(n)$ whenever $(n,r) = 1$ and $\chi_1(n) = 0$ otherwise. Therefore

$$\left|\sum_{M\le n\le N}\chi(n)\right| = \left|\sum_{\substack{M\le n\le N\\(n,r)=1}}\chi_1(n)\right| = \left|\sum_{M\le n\le N}\Big(\sum_{d|(n,r)}\mu(d)\Big)\chi_1(n)\right| = \left|\sum_{d|r}\mu(d)\sum_{\frac{M}{d}\le k\le\frac{N}{d}}\chi_1(dk)\right|.$$

Since r has at most $2\sqrt{r}$ positive divisors, we can apply the Pólya-Vinogradov inequality to the primitive character χ_1 to get

$$\left|\sum_{M\le n\le N}\chi(n)\right| < \sum_{d|r}\sqrt{m'}\log m' < 2\sqrt{r}\sqrt{m'}\log m' < 2\sqrt{m}\log m. \qquad \square$$

Assuming GRH, Montgomery and Vaughan [83] improved the upper bounds on the Pólya-Vinogradov inequality.

Theorem 3.3.3 ([83])**.** *Suppose that GRH is true. Then for any non-principal Dirichlet character χ modulo m and any integers $M \leq N$,*

$$\left| \sum_{M \leq n \leq N} \chi(n) \right| \ll \sqrt{m} \log \log m.$$

On the other hand, Paley [93] showed that the lower bound of the above character sum is also of the order $\sqrt{m} \log \log m$.

By taking χ to be the quadratic character modulo p, we can use the upper bounds on the character sums to give an upper bound on the least quadratic non-residue $n(p)$ modulo p.

Corollary 3.3.4. *$n(p) = O(\sqrt{p} \log p)$. Assuming GRH, $n(p) = O(\sqrt{p} \log \log p)$.*

In fact, we can get an improved upper bound on $n(p)$ with a refined argument. The key observation is that any positive integer which is $\big(n(p) - 1\big)$-friable, i.e. with all prime divisors smaller than $n(p)$, is a quadratic residue. We need the following well-known estimate on sums of reciprocals of primes. The proof can be found in Theorem 2.7 in [85].

Theorem 3.3.5 (Mertens' theorem)**.** *For $x \geq 2$,*

$$\sum_{p \leq x} \frac{1}{p} = \log \log x + b + O(1/\log x),$$

where b is a constant.

Corollary 3.3.6. *For any $\epsilon > 0$, $n(p) \ll_\epsilon p^{1/2\sqrt{e}+\epsilon}$.*

Proof. Fix $\epsilon > 0$. Let $P(n)$ denote the largest prime dividing n and let $\psi(x, y)$ denote the number of integers between 1 and x that are y-friable. Suppose that $\chi(n) = 1$ for $n \leq y$. Then for any y-friable positive integer m, $\chi(m) = 1$. If $y \leq x < y^2$, then

$$\sum_{n \leq x} \chi(n) = \psi(x, y) + \sum_{\substack{y < q \leq x \\ q \text{ prime}}} \chi(q) \#\{n \leq x : P(n) = q\} = \psi(x, y) + \sum_{\substack{y < q \leq x \\ q \text{ prime}}} \chi(q) \left\lfloor \frac{x}{q} \right\rfloor.$$

Therefore

$$\left| \sum_{n \leq x} \chi(n) \right| \geq \psi(x, y) - \sum_{\substack{y < q \leq x \\ q \text{ prime}}} \left\lfloor \frac{x}{q} \right\rfloor = \lfloor x \rfloor - 2 \sum_{\substack{y < q \leq x \\ q \text{ prime}}} \left\lfloor \frac{x}{q} \right\rfloor = x - 2x \sum_{\substack{y < q \leq x \\ q \text{ prime}}} \frac{1}{q} + O\big(\pi(x)\big).$$

Using Mertens' theorem,

$$\begin{aligned} x - 2x \sum_{y<q\le x} \frac{1}{q} + O(\pi(x)) &= x - 2x \left(\sum_{q\le x} \frac{1}{q} - \sum_{q\le y} \frac{1}{q} \right) + O\big(\pi(x)\big) \\ &= x - 2x \left(\log\log x - \log\log y + O\left(\frac{1}{\log(x)} \right) \right) + O\left(\frac{x}{\log x} \right) \\ &= x \left(1 - 2\log \frac{\log x}{\log y} \right) + O\left(\frac{x}{\log x} \right). \end{aligned}$$

Setting $x = \sqrt{p}(\log p)^2$, the Pólya-Vinogradov inequality and the above estimate give the following inequality when $y \le x < y^2$:

$$\sqrt{p}\log p > \left| \sum_{n\le x} \chi(n) \right| \ge x \left(1 - 2\log \frac{\log x}{\log y} \right) + O\left(\frac{x}{\log x} \right).$$

If $x > y > x^{1/\sqrt{e}+\varepsilon}$, then $y \le x < y^2$, and the sum on the left is $o(x)$, while the sum on the right is $\gg \varepsilon x$, which is impossible when when p is large. Therefore, $n(p) \ll p^{1/2\sqrt{e}+\epsilon}$. □

This is not the best known upper bound on $n(p)$. We will discuss bounds on the least quadratic non-residue and their connections to Paley graphs in Section 3.6.

3.4 Paley Graph Conjecture

Let A, B be arbitrary subsets of the field $\mathbb{F}_p$, and χ be a non-principal Dirichlet character modulo p. Many authors have studied the following double character sum (see for example [22, 23, 34, 60–62, 120])

$$\sum_{a\in A,\, b\in B} \chi(a+b), \tag{3.4}$$

and their goal is to obtain good upper bounds on its absolute value. The following classical estimate is due to Erdős and Shapiro [34].

Theorem 3.4.1 ([34]). *If χ is a non-principal Dirichlet character modulo p, then for any $A, B \subset \mathbb{F}_p$,*

$$\left| \sum_{a\in A,\, b\in B} \chi(a+b) \right| \le \sqrt{p|A||B|}.$$

In [23, Theorem 2.1], Chung improved the upper bound in Theorem 3.4.1 by a multiplicative factor $\big(1 - \frac{|A|}{p}\big)^{1/2}\big(1 - \frac{|B|}{p}\big)^{1/2}$. In fact, her method can be easily generalized to work in all finite fields.

Theorem 3.4.2. *If χ is a non-trivial multiplicative character of $\mathbb{F}_q$, then for any $A, B \subset \mathbb{F}_q$,*

$$\Big|\sum_{a\in A,\, b\in B}\chi(a+b)\Big| \le \sqrt{q|A||B|}\Big(1-\frac{|A|}{q}\Big)^{1/2}\Big(1-\frac{|B|}{q}\Big)^{1/2}.$$

Proof. By Theorem 3.2.14,

$$\sum_{a\in A,\, b\in B}\overline{\chi(a+b)} = \frac{1}{G(\chi)}\sum_{a\in A,\, b\in B, c\in\mathbb{F}_q}\chi(c)e_p\big(\operatorname{Tr}((a+b)c)\big) = \frac{1}{G(\chi)}\sum_{c\in\mathbb{F}_q}\chi(c)\sum_{a\in A,\, b\in B}e_p\big(\operatorname{Tr}((a+b)c)\big).$$

Since χ is nontrivial, by Theorem 3.2.13, $|G(\chi)| = \sqrt{q}$. Recall that $|\chi(c)| = 1$ for each $c \in \mathbb{F}_q^*$, so that

$$\begin{aligned}\Big|\sum_{a\in A,\, b\in B}\chi(a+b)\Big| &\le \frac{1}{\sqrt{q}}\sum_{c\in\mathbb{F}_q^*}\Big|\sum_{a\in A,\, b\in B}e_p\big(\operatorname{Tr}((a+b)c)\big)\Big| \\ &= \frac{1}{\sqrt{q}}\sum_{c\in\mathbb{F}_q^*}\Big|\sum_{a\in A}e_p\big(\operatorname{Tr}(ac)\big)\Big|\Big|\sum_{b\in B}e_p\big(\operatorname{Tr}(bc)\big)\Big| \\ &\le \frac{1}{\sqrt{q}}\Big(\sum_{c\in\mathbb{F}_q^*}\Big|\sum_{a\in A}e_p\big(\operatorname{Tr}(ac)\big)\Big|^2\Big)^{1/2}\Big(\sum_{c\in\mathbb{F}_q^*}\Big|\sum_{b\in B}e_p\big(\operatorname{Tr}(bc)\big)\Big|^2\Big)^{1/2},\end{aligned}$$

where we used the Cauchy-Schwarz inequality in the last step. By Lemma 3.2.9,

$$\begin{aligned}\sum_{c\in\mathbb{F}_q^*}\Big|\sum_{a\in A}e_p\big(\operatorname{Tr}(ac)\big)\Big|^2 &= \sum_{c\in\mathbb{F}_q}\Big|\sum_{a\in A}e_p\big(\operatorname{Tr}(ac)\big)\Big|^2 - |A|^2 = \sum_{c\in\mathbb{F}_q}\sum_{a_1,a_2\in A}e_p\big(\operatorname{Tr}(c(a_1-a_2))\big) - |A|^2 \\ &= q|A| + \sum_{\substack{a_1,a_2\in A\\ a_1\neq a_2}}\Big(\sum_{c\in\mathbb{F}_q}e_p\big(\operatorname{Tr}(c(a_1-a_2))\big)\Big) - |A|^2 = q|A| - |A|^2.\end{aligned}$$

Similarly, we have

$$\sum_{c\in\mathbb{F}_q^*}\Big|\sum_{b\in B}e_p\big(\operatorname{Tr}(bc)\big)\Big|^2 = q|B| - |B|^2.$$

It follows that

$$\Big|\sum_{a\in A,\, b\in B}\chi(a+b)\Big| \le \frac{1}{\sqrt{q}}\big(q|A|-|A|^2\big)^{1/2}\big(q|B|-|B|^2\big)^{1/2}. \qquad \square$$

Next we establish the connection between the character sum estimate of equation (3.4) and the clique number of a generalized Paley graph.

Corollary 3.4.3. *If $q \equiv 1 \pmod{2d}$, then $\omega\big(P(q,d)\big) \le \sqrt{q}$.*

Proof. Let χ be a multiplicative character of $\mathbb{F}_q$, with order d. Let A be a maximum clique in $P(q,d)$ with $|A| = N$, and let $B = -A$. Then for any $a \in A, b \in B$, either $a+b = 0$ or $a+b$ is a d-th power in $\mathbb{F}_q^*$. Therefore, $\sum_{a\in A,\, b\in B}\chi(a+b) = N^2 - N$. Combining Theorem 3.4.2, we get $N^2 - N \le \sqrt{q}N(1-\frac{N}{q})$, which implies $N \le \sqrt{q}$. $\square$

The Paley Graph Conjecture is a well-known hypothesis on sums of the form (3.4); see for example Conjecture 2.2 of [23], Conjecture D of [109], Problem 4.3 in [22], and [120]. It turns out that the Paley Graph Conjecture is closely related to many unsolved problems in combinatorics and number theory. See [52] for an example of its connection to the Diophantine tuples problem, and [105] for an example of its connection with compressed sensing.

Conjecture 3.4.4 (Paley Graph Conjecture)**.** *Let $\delta > 0$, and let $A, B \subset \mathbb{F}_p$ be arbitrary sets with $|A| > p^\delta$ and $|B| > p^\delta$. Then there exist $c(\delta), \tau(\delta) > 0$ such that for any sufficiently large prime number p and any non-principal Dirichlet character χ modulo p,*

$$\left| \sum_{a \in A,\, b \in B} \chi(a+b) \right| \leq c(\delta) p^{-\tau} |A||B|\,. \tag{3.5}$$

Unfortunately, at the moment, we do not understand Conjecture 3.4.4 very well; even the case $|A| \sim |B| \sim p^{\frac{1}{2}}$ inequality (3.5) is unknown (see [62]). However, using tools from classical character estimates (as we did in this section) together with ideas from additive combinatorics (in particular a particular form of additive energy), nontrivial bounds for the sum (3.4) can be obtained for certain structured sets A and B. An affirmative answer to Conjecture 3.4.4 was obtained in the case $|A| > p^{\frac{1}{2}+\delta}$, $|B| > p^\delta$, see [60]—[62]. Volostnov [120] proved the following estimate.

Theorem 3.4.5 ([120])**.** *Let $A, B \subset \mathbb{F}_p$ be sets and $K, L, \delta > 0$ be numbers with $|A|, |B| > p^{\frac{1}{3}+\delta}, |A+A| < K|A|, |B+B| < L|B|$. Then there exists $\tau = \tau(\delta, K) = \delta^2 (\log 2K)^{-3+o(1)}$ such that the inequality*

$$\left| \sum_{a \in A,\, b \in B} \chi(a+b) \right| < p^{-\tau} |A||B|$$

holds for all primes $p > p(\delta, K, L)$, where χ is a non-principal multiplicative character modulo p.

In particular, when $A = B$, we have the following (folklore) conjecture, which refines the bound in the inequality (3.5). The case that $\delta < 1/2$ remains open. Note that the case $\delta > 1/2$ has been confirmed in Theorem 3.4.2.

Conjecture 3.4.6 (Paley Graph Conjecture, refined version)**.** *Let $\delta > 0$, and let $A \subset \mathbb{F}_p$ be an arbitrary set with $|A| > p^\delta$. Then there exists $\tau(\delta) > 0$ such that*

$$\left| \sum_{a,b \in A} \chi(a-b) \right| < |A|^{2-\tau} \tag{3.6}$$

for any sufficiently large prime number p and any non-principal Dirichlet character χ modulo p.

Similar to the proof of Corollary 3.4.3, by taking χ to be the quadratic character, it is easy to see that this refined conjecture would imply $\omega(P_p) \ll_\delta p^\delta$ for any positive δ.

Chung [23] pointed out that the analogous version of Conjecture 3.4.6 for characters in $\mathbb{F}_q$ instead of in $\mathbb{F}_p$ is not true in general. One obstruction is that Conjecture 3.4.6 is false when A, B lie in a certain subfield of $\mathbb{F}_q$; we refer the reader to the discussion in Section 3.8.

3.5 Least quadratic non-residue

For each prime p, let $n(p)$ be the the least positive integer that is a quadratic non-residue modulo p. Readers can refer to the survey papers [15], [79] for more information.

Note that for each prime $p \equiv 1 \pmod 4$, the set $C = \{0, 1, \cdots, n(p)-1\}$ has the property that for any two distinct $x, y \in C$, $|x-y| < n(p)$; in particular, $x-y$ is a quadratic residue. So C forms a Paley clique and we have $\omega(P_p) \geq n(p)$. Therefore, one way to study the clique number of Paley graphs is to estimate the size of $n(p)$.

Recall that in Corollary 3.3.6, we used the Pólya-Vinogradov inequality to deduce an upper bound for $n(p)$. Note that the Pólya-Vinogradov inequality is independent of the length of the interval, so one way to refine the bound (and then get improved bounds on $n(p)$) is to fix the length of the interval. Estimates for character sums over an interval in terms of the length of the interval were considered by Burgess [16, 17] and by Wang [121]. The best known upper bound on $n(p)$ is due to Burgess [17].

Theorem 3.5.1 (Burgess's bound, [17]). *For any $\epsilon > 0$, $n(p) \ll_\epsilon p^{1/4\sqrt{e}+\epsilon}$.*

The key in the proof of Theorem 3.5.1, as discussed above, is the following refined estimate on character sums. The idea of the proof of Theorem 3.5.1 is similar to the proof of Corollary 3.3.6.

Theorem 3.5.2 ([17]). *For any prime p and any non-principal Dirichlet character χ mod p, and any $N, r \in \mathbb{N}$, $M \in \mathbb{Z}$,*

$$\left| \sum_{n=M+1}^{M+r} \chi(n) \right| \ll N^{1-\frac{1}{r+1}} p^{\frac{1}{4r}} \log p.$$

For any prime p, let $y(p)$ denote the smallest integer y such that every reduced residue class (mod p) is represented by the product of some subset of $\{1, 2, \cdots, y\}$. Recently, Martin and Parvardi [78] showed that for any $\epsilon > 0$, $y(p) \ll_\epsilon p^{1/4\sqrt{e}+\epsilon}$. Note that we must have $y(p) \geq n(p)$, for otherwise any subproduct of the set $\{1, 2, \cdots, y(p)\}$ is a quadratic residue. Therefore, this result strengthens Burgess's classical result.

Conjecture 3.5.3 (Vinogradov's Conjecture). *For any $\epsilon > 0$, $n(p) \ll_\epsilon p^\epsilon$.*

Linnik [76] verified that Vinogradov's Conjecture holds for almost all primes.

Theorem 3.5.4 ([76]). *For any $\epsilon > 0$, $\#\{p \leq N : n(p) > p^\epsilon\} = O(N^\epsilon)$.*

Assuming GRH, the upper bound on $n(p)$ can be improved significantly. In 1952, Ankeny [6] proved that $n(p) = O\big((\log p)^2\big)$ under GRH. And the best known result is due to Lamzouri, Li and Soundararajan [72], where they proved under GRH, $n(p) \leq (\log p)^2$ for $p \geq 5$.

As for the lower bound, in 1949, Fridlender [40] and Salle [104] independently showed that $n(p) = \Omega(\log p)$. In 1971, Montgomery [82] proved $n(p) = \Omega(\log p \log\log p)$ assuming GRH. In 1990, Graham and Ringrose [44] proved $n(p) = \Omega(\log p \log\log\log p)$ unconditionaly. In the end of the paper [44], Graham and Ringrose mentioned that the proof can be modified slightly to show that there are infinitely many primes $p \equiv 1 \pmod 4$ such that $n_p \gg \log p \log\log\log p$.

Corollary 3.5.5. $\omega(P_p) = \Omega(\log p \log\log\log p)$. *And if GRH is true, then* $\omega(P_p) = \Omega(\log p \log\log p)$.

Finally, we discuss the heuristic of the distribution on $n(p)$ (see for example [79]), and the conjectured bound $n(p) = O(\log p \log\log p)$, on probabilistic grounds. Note that $n(p)$ must be a prime. Let p_k be the k-th prime. Using quadratic reciprocity, the Chinese remainder theorem, and Dirichlet's theorem, it is straightforward to show that

$$\lim_{x\to\infty} \frac{\#\{p \le x : n(p) = p_k\}}{\pi(x)} = \frac{1}{2^k}.$$

Now if $\pi(x) \approx 2^k$, then we expect $n(p_{\pi(x)}) \le p_k$. Therefore, by the prime number theorem, we expect $n(p) = n(p_{\pi(p)}) = O(p_{\log \pi(p)}) = O(\log \pi(p) \log\log \pi(p)) = O(\log p \log\log p)$. Using the large sieve of Linnik, Erdős [35] refined the above observation and showed the following result about the average size of $n(p)$.

Theorem 3.5.6 ([35])**.** *As* $x \to \infty$, *we have* $\frac{1}{\pi(x)} \sum_{p\le x} n(p) = \big(1+o(1)\big)C_0$, *where* $C_0 = \sum_{k=1}^{\infty} \frac{p_k}{2^k} \approx 3.67464$.

Intuitively, one might expect that $C = \{0, 1, \cdots, n(p)-1\}$ is the clique of the maximum size in the Paley graph P_p. So some authors believe that the following conjecture is true; see for example Kalai [59]. Perhaps they observed a similar heuristic for the distribution on $n(p)$.

Conjecture 3.5.7. $\omega(P_p) = O(\log p \log\log p)$.

Note that this upper bound is the same as the best known lower bound assuming GRH.

3.6 Lower bounds on the clique number

The following heuristic argument by Cohen [24] shows $\log_2 q + 3/2$ as the expected value for $\omega(P_q)$. Let y be a square in $\mathbb{F}_q^*$ with order n. If $y^i - 1$ is a square in $\mathbb{F}_q^*$ for each $i = 1, 2, \ldots, n-1$, then $\{0, y, y^2, \ldots, y^{n-1}, y^n = 1\}$ forms a Paley clique since $y^j - y^i = y^i(y^{j-i}-1)$ is a square for any $0 \le i < j \le n$. If we assume squares behave randomly, then the probability that $\{0, z, z^2, \ldots, z^{n-1}, z^n = 1\}$ forms a Paley clique is $\frac{1}{2^n}$. If n is much smaller compared to q, then with probability $1/2$, we are able to extend this clique by at least 1. Cohen used cyclotomic polynomials and Weil bound to prove the following lower bound on clique number of Paley graphs and generalized Paley graphs.

Theorem 3.6.1 ([24])**.** *If* $q \equiv 1 \pmod 4$, *then* $\omega(P_q) \ge \frac{p}{p-1}\left(\frac{\frac{1}{2}\log q - 2\log\log q}{\log 2} + 1\right)$.

Theorem 3.6.2 ([24])**.** *If* $d \ge 3$ *and* $q \equiv 1 \pmod{2d}$, *then*

$$\omega\big(P(q,d)\big) \ge \frac{p}{(p-1)\log d}\left(\frac{1}{2}\log q - 2\log\log q\right) - 1.$$

Roughly speaking, the lower bound Cohen obtained for $\omega(P_q)$ is $\log_4 q$, which is the same as Corollary 2.5.3 using diagonal Ramsey numbers. The following is the well-known Weil bound on character sums.

Theorem 3.6.3 (Weil's bound, Theorem 5.41 in [73]). *Let χ be a multiplicative character of $\mathbb{F}_q$ of order $m > 1$, and let $f \in \mathbb{F}_q[x]$ be a monic polynomial of positive degree that is not an m-th power of a polynomial. Let d be the number of distinct roots of f in its splitting field over $\mathbb{F}_q$. Then for any $a \in \mathbb{F}_q$,*

$$\left| \sum_{x \in \mathbb{F}_q} \chi\big(af(x)\big) \right| \leq (d-1)\sqrt{q}\,.$$

Recently, Solymosi [111] improved the $\log_4 q$ lower bound to about $\log_3 q$. The key observation is the following lemma, which tells us how much can we extend a Paley clique of size $\log_4 q - 2\log_2 \log q$ (obtained from Theorem 3.6.1, for example) into a larger one. The proof of the lemma is very similar to the proof of Theorem 3.6.1 as well as the main theorem in [45], where Graham and Spencer discussed the size of Paley tournament defined by a directed Paley graph of order p, where $p \equiv 3 \pmod 4$. This is a nice example of the application of Weil's bound.

Lemma 3.6.4 ([111]). *Let χ be the quadratic character in $\mathbb{F}_q$. For any Paley clique $A = \{a_1, a_2, \ldots, a_k\}$ of P_q, if $k \leq \log_4 q - 2\log_2 \log q$ then there are at least $\sqrt{q}(\log q)(\log q - 1)$ elements $e \in \mathbb{F}_q$, such that $\chi(a_i - e) = 1$ for every $1 \leq i \leq k$.*

Proof. Let us consider the product $\prod_{i=1}^{k} \big(\chi(x - a_i) + 1\big)$. If $x - a_i$ is a quadratic non-residue for some i, then the product is zero. If each $x - a_i$ is a quadratic residue, then the product is 2^k. If $x = a_i$ for some i, then the product is 2^{k-1} since A is a Paley clique.

We can break the product into sums of sub-products as follows:

$$\prod_{i=1}^{k} (\chi(x - a_i) + 1) = 1 + \sum_{\emptyset \neq I \subset \{1,\ldots,k\}} \prod_{i \in I} \chi(x - a_i) = 1 + \sum_{\emptyset \neq I \subset \{1,\ldots,k\}} \chi\big(g_I(x)\big)\,,$$

where $g_I(x) = \prod_{i \in I}(x - a_i)$ is a fully reducible polynomial of degree $|I|$. By Weil's bound,

$$\begin{aligned}\sum_{x \in \mathbb{F}_q} \left(1 + \sum_{\emptyset \neq I \subset \{1,\ldots,k\}} \chi\big(g_I(x)\big)\right) &= q + \sum_{\emptyset \neq I \subset \{1,\ldots,k\}} \sum_{x \in \mathbb{F}_q} \chi\big(g_I(x)\big) \\ &\geq q - \sum_{r=1}^{k} \binom{k}{r} (r-1)\sqrt{q} \geq q - \big((k-2)2^{k-1} + 1\big)\sqrt{q}.\end{aligned}$$

So the number of elements $e \in \mathbb{F}_q$ such that $\chi(a_i - e) = 1$ for every $1 \leq i \leq k$ equals

$$2^{-k} \sum_{x \in \mathbb{F}_q} \left(1 + \sum_{\emptyset \neq I \subset \{1,\ldots,k\}} \chi\big(g_I(x)\big)\right) - 2^{-k} k 2^{k-1} \geq \frac{q}{2^k} - \frac{k-2}{2}\sqrt{q} - \frac{\sqrt{q}}{2^k} - \frac{k}{2}.$$

Since $k \leq \log_4 q - 2\log_2 \log q$, we have $2^k \leq \frac{\sqrt{q}}{(\log q)^2}$ and

$$\frac{q}{2^k} - \frac{k-2}{2}\sqrt{q} - \frac{\sqrt{q}}{2^k} - \frac{k}{2} \geq \sqrt{q}(\log q)(\log q - 1). \qquad \square$$

Note that if A is a maximal clique in P_q with $|A| = k$, then it is impossible to extend this clique. So we must have $q - \big((k-2)2^{k-1}+1\big)\sqrt{q} \le 0$, and we obtain the following corollary.

Corollary 3.6.5. *If A is a maximal clique in P_q with $|A| = k$, then $(k-2)2^{k-1}+1 \ge \sqrt{q}$; in particular, $k \ge \log_4 q - 2\log_2\log q$.*

Using Lemma 3.6.4, we can improve the lower bounds on the clique number.

Theorem 3.6.6 ([111])**.** *If $q \equiv 1 \pmod 4$, then $\omega(P_q) \ge \log_{3.009} q$.*

Sketch of the proof. By Theorem 3.6.1, there is a complete subgraph of size $k = \lfloor \log_4 q - 2\log_2\log q \rfloor$ in P_q, denoted by K_k. By Lemma 3.6.4, there are at least $m = \sqrt{q}(\log q)(\log q - 1)$ vertices $v_1, \dots, v_m$, outside of K_k such that $K_k \subset \bigcap_{i=1}^m N(v_i)$. For any $c > 0$ and $\ell \in \mathbb{N}$, if $m \ge \binom{(\frac{1}{2}+c)\ell + c\ell}{c\ell} = \binom{(\frac{1}{2}+2c)\ell}{c\ell}$, then V contains an empty $\lfloor (1/2+c)\ell \rfloor$ or a complete $\lfloor c\ell \rfloor$ subgraph by the classical Ramsey estimate of Erdős and Szekeres (2.1). We set $c = 0.1294037$ and $\ell = \log_2 q$. Since P_q is self-complementary, we can conclude that the $\omega(P_q) \ge \big(1/2 + c - o(1)\big)\log_2 q$. A more involved numerical computation would show $\omega(P_q) \ge \log_{3.009} q$. □

The above proof can be modified to get an improved lower bound for the clique number of generalized Paley graphs $P(q,d)$, although the computation will be much more complicated.

For multi-dimensional character sum of the form $\sum_{\gamma \in \mathbb{F}_q^m} \chi\big(f(\gamma)\big)$, Deligne's revolutionary work [29] in algebraic geometry has the following consequence (see for example Chapter 5 of [65]): if f is a polynomial of degree d not divisible by the characteristic p of $\mathbb{F}_q$ and if the homogeneous part of f of degree d is nonsingular in a certain sense, then

$$\left| \sum_{\gamma \in \mathbb{F}_q^m} \chi\big(f(\gamma)\big) \right| \le (d-1)^m q^{m/2}. \tag{3.7}$$

Thomason [117] mentioned the possibility of obtaining $\omega(P_q) > \log_2 q$ by replacing Weil's estimates by those of Deligne, but said that "this would be a formidable undertaking". In [80], Meir discussed the extension of Weil bound to multi-dimensional character sum, and he conjectured the following, which is a stronger version of (3.7) for certain polynomials. See Chapter 3 of Meir's thesis [80] for more discussion on this conjecture.

Conjecture 3.6.7 ([80])**.** *Let χ be a multiplicative character of $\mathbb{F}_q$ of order $k > 1$, and let f be a non-degenerate polynomial in m variables that is the product d distinct linear forms with multiplicities $r_1, r_2, \dots, r_d$ over $\overline{\mathbb{F}_q}$, such that $0 < r_i < k$. Then*

$$\left| \sum_{\gamma \in \mathbb{F}_q^m} \chi\big(f(\gamma)\big) \right| \le (d/m)^m q^{m/2}.$$

Meir remarked that Conjecture 3.6.7 is "hopefully a consequence, albeit not an easy one, of Deligne's great work". Assuming Conjecture 3.6.7, Meir showed that Thomason's observation could be made realistic with delicate computation and analysis.

Theorem 3.6.8 (Section 9 in [80]). *Assuming Conjecture 3.6.7, we have $\omega(P_q) > \log_2 q$ for any $q \equiv 1 \pmod 4$.*

3.7 Subfield constructions for the lower bounds

We have seen that the best known lower bound is $\omega(P_p) = \Omega(\log p \log\log p)$, by assuming GRH. The following theorem shows that the lower bound can be greatly improved in certain cases, by considering some subfields of $\mathbb{F}_q$.

Theorem 3.7.1 (Theorem 1 in [13]). *Let $q \equiv 1 \pmod{2d}$, and let r be the largest integer such that $d \mid \frac{q-1}{p^r-1}$, then $\omega\big(P(q,d)\big) \geq p^r$.*

Proof. Note that $(p^r - 1) \mid (q-1)$ implies $r \mid s$, so $\mathbb{F}_{p^r}$ is a subfield of $\mathbb{F}_q$. We claim that $\mathbb{F}_{p^r}$ is a d-Paley clique in $P(q,d)$. To prove that, it suffices to show that each $x \in \mathbb{F}_{p^r}$ is a d-th power. Let g be a primitive root of $\mathbb{F}_q^*$; then g has order $q-1$, and the nonzero elements of $\mathbb{F}_{p^r}$ are exactly the roots of $x^{p^r-1} = 1$. If $x = g^l \in \mathbb{F}_{p^r}^*$, then $x^{p^r-1} = 1$, which is equivalent to $(q-1) \mid l(p^r-1)$, and so $d \mid l$, that is, x is a d-th power. □

Combining Theorem 3.7.1 and the trivial upper bound Lemma 1.3.4, we obtain the following.

Corollary 3.7.2. *When q is a square and $d \mid (\sqrt{q}+1)$, $\omega\big(P(q,d)\big) = \sqrt{q}$. In particular, when q is a square, $\omega(P_q) = \sqrt{q}$.*

This means that Lemma 1.3.4 gives the best trivial upper bound, in the sense that we cannot improve it without any additional assumption. The maximum clique of a Paley graph with a square order has been shown to have a rigid structure.

Theorem 3.7.3 ([11]). *If q is an odd prime power, then the only q-subset of $\mathbb{F}_{q^2}$ with the property that the difference of any two elements is always a square, are the lines of $\mathbb{F}_{q^2}$ when considered as the affine plane $AG(2,q)$.*

In particular, when q is a square, if $0, 1 \in C$, the above theorem implies that $C = \mathbb{F}_{\sqrt{q}}$. In general, when q is a square, C must be obtained from an affine transformation of $\mathbb{F}_{\sqrt{q}}$. Theorem 3.7.1 also implies that the lower bound $q^{1/d}$ can be attained in the following cases.

Proposition 3.7.4. *If $\gcd(d, \phi(d)) = 1$, $2d \mid (q-1)$ and $d \mid s$, then $\omega\big(P(q,d)\big) \geq q^{1/d}$. In particular, if d is a prime such that $2d \mid (q-1)$ and $d \mid s$, then $\omega\big(P(q,d)\big) \geq q^{1/d}$.*

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 3.7.1, we have $\omega\big(P(q,d)\big) \geq p^{s/d} = q^{1/d}$. □

Similarly, by considering an appropriate subfield of $\mathbb{F}_q$, we can obtain a lower bound on the clique number of the Peisert graph over $\mathbb{F}_q$.

Theorem 3.7.5 (Theorem 5.1 in [69]). *Let $q = p^s$, where $p \equiv 3 \pmod 4$ and $s = 2k$. If k is odd, then $\omega(P_q^*) = \sqrt{q}$; if k is even, then $\omega(P_q^*) \geq q^{1/4}$.*

Chapter 4

Polynomials over finite fields

In this chapter, we discuss some useful tools from finite fields and polynomials over finite fields. They will be used in later chapters, when we apply polynomial methods.

4.1 Hyper-derivatives

Using Talyor expansion centered at a root, we have the following well-known relation between the multiplicity of roots and the derivatives.

Lemma 4.1.1. *Let $0 \neq f \in F[x]$, where F is a field with characteristic zero. Suppose c is a root of $f^{(n)}(x)$ for $n = 0, 1, \ldots, m-1$, then c is a root of multiplicity at least m.*

However, the same result fails to hold for fields with nonzero characteristic. This is because if $\operatorname{char} K = p > 0$, then for any polynomial $f \in K[x]$, we have $f^{(p)}(x) \equiv 0$. This means we need to modify the definition of derivative in order to overcome the nonzero characteristic, and a good idea is to introduce the binomial coefficients into the derivatives. The following is the definition of hyper-derivatives [73], also known as Hasse derivatives.

Definition 4.1.2. *Let K be a field and let $b_0, b_1, \ldots b_d \in K$. If n is a non-negative integer, then the n-th order* hyper-derivative *of $f(x) = \sum_{j=0}^{d} b_j x^j$ is*

$$E^{(n)}(f) = \sum_{j=0}^{d} \binom{j}{n} b_j x^{j-n}.$$

Recall that when $j < n$, $\binom{j}{n} = 0$, so the summation above actually only sums over $n \leq j \leq d$, and thus x^{j-n} makes sense.

Note that $E^{(1)}$ matches with the usual first order derivative. And if $\operatorname{char} K = 0$, or $\operatorname{char} K > n!$ then $E^{(n)}(f) = \frac{1}{n!} f^{(n)}$. We present some simple properties of hyper-derivatives with proof, and one can refer to Chapter 6.4 of [73] for more applications of hyper-derivatives and Stepanov's method.

The following is analogous to Leibniz rule for standard derivatives.

Lemma 4.1.3 (Leibniz rule for hyper-derivatives)**.** *If $f_1, \ldots, f_t \in K[x]$, then*

$$E^{(n)}(f_1 \ldots f_t) = \sum_{\substack{n_1, \ldots n_t \geq 0, \\ n_1 + \ldots + n_t = n}} E^{(n_1)}(f_1) \ldots E^{(n_t)}(f_t)$$

Proof. Note that hyper-derivatives are linear. So it suffices to consider the case for monomials. Assume $f_j(x) = x^{k_j}$ for $1 \leq j \leq t$ and $k = \sum_{j=1}^{t} k_j$. Then

$$E^{(n)}(f_1 \dots f_t) = E^{(n)}(x^k) = \binom{k}{n} x^{k-n},$$

$$\sum_{\substack{n_1,\dots n_t \geq 0,\\ n_1+\dots+n_t=n}} E^{(n_1)}(f_1) \dots E^{(n_t)}(f_t) = \sum_{\substack{n_1,\dots n_t \geq 0,\\ n_1+\dots+n_t=n}} \left(\prod_{j=1}^{t} \binom{k_j}{n_j} \right) x^{k-n}.$$

Consider the coefficient of x^n of the two sides of the identity $(1+x)^k = \prod_{j=1}^{t} (1+x)^{k_j}$, we get

$$\binom{k}{n} = \sum_{\substack{n_1,\dots n_t \geq 0,\\ n_1+\dots+n_t=n}} \prod_{j=1}^{t} \binom{k_j}{n_j},$$

which proves the proposition. □

Corollary 4.1.4. $E^{(n)}\big((x-c)^t\big) = \binom{t}{n}(x-c)^{t-n}$.

Proof. For $1 \leq i \leq t$, let $f_i(x) = x - c$, then $E^{(1)}(f_i) = 1$, and $E^{(k)}(f_i) = 0$ for $k \geq 2$. So by Leibniz rule,

$$E^{(n)}\big((x-c)^t\big) = \sum_{\substack{n_1,\dots n_t \in \{0,1\},\\ n_1+\dots+n_t=n}} (x-c)^{t-n} = \binom{t}{n}(x-c)^{t-n}.$$ □

Now we are able to establish a relation between the multiplicity of roots and the hyper-derivatives parallel to Lemma 4.1.1:

Lemma 4.1.5. *Let $0 \neq f \in K[x]$. Suppose c is a root of $E^{(n)}(f)$ for $n = 0, 1, \dots, m-1$, then c is a root of multiplicity at least m.*

Proof. Let $f(x) = b_0 + b_1(x-c) + \dots + b_d(x-c)^d$, where $b_d \neq 0$, then

$$E^{(n)}(f)(x) = b_n + \binom{n+1}{n} b_{n+1}(x-c) + \dots + \binom{d}{n} b_d (x-c)^{d-n}.$$

Since c is a root of $E^{(n)}(f)$ for $n = 0, 1, \dots, m-1$, then $b_n = 0$ for $n = 0, 1, \dots, m-1$. So c is a root of multiplicity at least m. □

4.2 Combinatorial Nullstellensatz and Schwartz–Zippel Lemma

In this section, we introduced Combinatorial Nullstellensatz and Schwartz–Zippel Lemma. They are fundamental results on the roots of a polynomial (over any field), and they have many interesting applications in number theory and combinatorics (see for example [1], [81], [118]).

Combinatorial Nullstellensatz, [1, 2] which gives us conditions under which we are assured a point within a defined sub-cube for which our polynomial doesn't vanish. We follow the short proof given in [81].

Theorem 4.2.1 (Combinatorial Nullstellensatz, Theorem 1.2 in [1]). *Let F be a field. Let $g \in F[x_1, x_2, \ldots, x_n]$ with $\deg g = \sum_{i=1}^{n} k_i$, where each $k_i \geq 0$ and the coefficient of $x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$ of g is non-zero. Then for any collection of subsets $S_1, S_2, \ldots, Sn \subset F$ such that $|S_i| > k_i$ for each i, g does not vanish on $S_1 \times S_2 \times \ldots \times S_n$.*

Proof. We proceed by induction on $d = \deg g$. The base case $d = 1$ is trivial. Suppose the statement holds for all polynomials with degree at most $d-1$, where $d \geq 2$. For contradiction's sake, assume that $g \in F[x_1, x_2, \ldots, x_n]$ has degree d and it vanishes on $S_1 \times S_2 \times \ldots \times S_n$. Without loss of generality, assume $k_n > 0$. Now fix a $s \in S_n$, then the division algorithm gives

$$g(x_1, x_2, \ldots, x_n) = (x_n - s)h(x_1, x_2, \ldots, x_n) + m(x_1, \ldots, x_{n-1}),$$

where $m(x_1, \ldots, x_{n-1}) = g(x_1, x_2, \ldots, x_{n-1}, s)$. Since g vanishes on $S_1 \times S_2 \times \ldots \times S_n$ and $s \in S_n$, then m vanishes on $S_1 \times S_2 \times \ldots \times S_{n-1}$. Therefore, $\deg h = \deg g - 1$ and h vanishes $S_1 \times S_2 \times \ldots \times S_{n-1} \times (S_n \setminus \{s\})$, contradicting the inductive hypothesis. □

The following lemma is useful in bounding the number of roots of a nonzero multivariate polynomial.

Lemma 4.2.2 (Schwartz–Zippel Lemma, Corollary 1 in [108]). *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*

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

Proof. We proceed by induction on n. The case $n = 1$ gives a univariate polynomial, so the statement follows. Suppose the statement holds for $n-1$, where $n \geq 2$. For a given non-zero polynomial $g \in F[x_1, x_2, \ldots, x_n]$, without loss of generality, we assume x_1 occurs in a monomial of g. We can then write

$$g(x_1, x_2, \ldots, x_n) = \sum_{i=0}^{d} x_1^i h_{d-i}(x_2, x_3, \ldots, x_n),$$

where $\deg h_{d-i} \leq d - i$. Let k be the largest positive integer such that $h_{d-k}(x_2, x_3, \ldots, x_n) \not\equiv 0$. Let $r_2, r_3, \ldots, r_n$ be selected at random independently and uniformly from S, then by the inductive hypothesis,

$$\Pr[h_{d-k}(r_2, r_3, \ldots, r_n) = 0] \leq \frac{d-k}{|S|}.$$

If $h_{d-k}(r_2, r_3, \ldots, r_n) \neq 0$, then $g(x_1, r_2, r_3, \ldots, r_n)$ is a univariate polynomial in x_1, with degree k.

Therefore,

$$\begin{aligned}\Pr[g(r_1, r_2, \ldots, r_n) \neq 0] &\geq \Pr[g(r_1, r_2, \ldots, r_n) \neq 0, h_{d-k}(r_2, r_3, \ldots, r_n) \neq 0] \\ &= \Pr[g(r_1, r_2, \ldots, r_n) \neq 0 | h_{d-k}(r_2, r_3, \ldots, r_n) \neq 0] \Pr[h_{d-k}(r_2, r_3, \ldots, r_n) \neq 0] \\ &\geq \left(1 - \frac{k}{|S|}\right)\left(1 - \frac{d-k}{|S|}\right) \\ &\geq 1 - \frac{d}{|S|},\end{aligned}$$

and the statement follows. □

More generally, Schwartz–Zippel Lemma is an important tool in polynomial identity testing (PIT). We can use Schwartz–Zippel Lemma to design a randomized algorithm to test whether two multivariate polynomials are identical (see for example [108]). In particular, given a multivariate polynomial, we can test whether this polynomial is the zero polynomial.

4.3 Lucas's Theorem

Lucas's Theorem is a powerful tool in studying how binomial coefficients behave modulo the prime p.

Theorem 4.3.1 (Lucas's Theorem)**.** *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 $0 \leq m_j, n_j \leq p-1$ for each $0 \leq j \leq r$, then

$$\binom{m}{n} \equiv \prod_{j=0}^{r} \binom{m_j}{n_j} \pmod{p}.$$

Sketch of the proof. Consider the coefficient of x^n on both sides of the following identity

$$(1+x)^m = \prod_{j=0}^{r} (1+x)^{m_j p^j} = \prod_{j=0}^{r} \left(1 + x^{p^j}\right)^{m_j} \in \mathbb{F}_p[x].$$ □

Corollary 4.3.2. *If m, n are non-negative integers such that $m \geq n$, then $\binom{m}{n} \not\equiv 0 \pmod{p}$ if and only if there is no carrying between the addition of n and $m-n$ in base-p representation.*

Proof. Let the base-p representations of $m, n, m-n$ be

$$m = (m_r, m_{r-1}, \ldots, m_0)_p, n = (n_r, n_{r-1}, \ldots, n_0)_p, m-n = (a_r, a_{r-1}, \ldots, a_0)_p.$$

If there is no carrying between the addition of n and $m-n$, then for each $0 \leq j \leq r$, we have $n_j + a_j = m_j$, in particular, $0 \leq n_j \leq m_j \leq p-1$. Then for for each $0 \leq j \leq r$, $\binom{m_j}{n_j} \not\equiv 0 \pmod{p}$, so by Lucas's theorem, $\binom{m}{n} \not\equiv 0 \pmod{p}$.

Conversely, suppose there exists a carrying between the addition of n and $m-n$. Then there is $k < r$, such that $n_k + a_k \geq p$, while for each $0 \leq j < k$, we have $n_j + a_j = m_j$. Note that $p \leq n_k + a_k < 2p$, so we must have $m_k = n_k + a_k - p < n_k$. It follows that $\binom{m_k}{n_k} \equiv 0 \pmod{p}$, so by Lucas's theorem, $\binom{m}{n} \equiv 0 \pmod{p}$. □

4.4 Lacunary polynomials and sparse polynomials

A polynomial is *lacunary* if there is a substantial gap between the degree of two consecutive terms. Most often, the gap between the highest and second highest terms is considered. What entails a substantial and useful gap depends on the context.

A class of polynomials related to lacunary polynomials are sparse polynomials. A *t-sparse polynomial* is a polynomial with t terms in its monomial expansion. Sparse polynomials are referred to as lacunary by some authors. Note lacunary polynomials are not necessarily sparse, and vice versa. Recall that Descartes' rule of signs gives an upper bound on the number of positive roots of a polynomial $f \in \mathbb{R}[x]$ based on the number of sign changes.

Theorem 4.4.1 (Descartes' rule of signs)**.** *Let $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$ be a polynomial with real coefficients. Let s be the number of sign changes in the sequence $c_n, c_{n-1}, \ldots, c_0$. Let r be the number of positive roots of $f(x)$ (counted with multiplicity). Then $s - r$ is a nonnegative even number. In particular, $r \leq s$.*

Let t be the number of nonzero coefficients of f, then it is clear that the number of sign changes $s \leq t-1$. Thus, if f is a t-sparse polynomial in $\mathbb{R}[x]$, then the number of positive roots is bounded by $t-1$. The number of negative roots is bounded by the number of sign changes of the coefficients in $f(-x)$, which is also bounded by $t-1$. Therefore, we get the following improved bound on the number of nonzero roots.

Corollary 4.4.2. *For a t-sparse polynomial $f \in \mathbb{R}[x]$, f has at most $2(t-1)$ roots.*

We are working on t-sparse polynomials $f \in \mathbb{F}_q[x]$, and we expect the trivial degree bound on $|Z^*(f)|$ can be also greatly improved. For a t-sparse polynomial $f(x) = \sum_{i=1}^{t} c_i x^{a_i} \in \mathbb{F}_q[x]$, define

$$\delta(f) = \min_i \max_{j \neq i} \gcd(a_i - a_j, q-1).$$

Let $C(f)$ denote the size of the largest coset in $\mathbb{F}_q^*$ on which f vanishes completely.

An upper bound on the number of roots of sparse polynomials has been investigated by several authors. A simple strategy for obtaining sparsity-dependent bounds on $|Z^*(f)|$ is doing affine transformations on the exponents in the monomial expansion of f. Note if $\gcd(e, q-1) = 1$, then the map $x \mapsto x^e$ simply permutes the elements of $\mathbb{F}_q^*$, thus we have $|Z^*(f(x))| = |Z^*(f(x^e))|$.

Furthermore, $f(x^e)$ is equivalent (as a mapping on $\mathbb{F}_q^*$) to any $g(x) = c_1 x^{b_1} + \cdots + c_t x^{b_t}$ with $b_i \equiv ea_i \bmod (q-1)$. Thus the basic idea is to find some e so that the remainders of $ea_i \bmod (q-1)$ are all relatively small, yielding a g of small degree, and thus $|Z^*(f)| = |Z^*(g)| \leq \deg g$.

For a t-sparse polynomial f, Karpinski and Shparlinski [64] showed that $|Z^*(f)| \leq \frac{t-1}{t}(q-1)$, and gave an efficient approximation algorithm for $|Z^*(f)|$. Canetti et al. [19] proved a finite field analogue of Descartes' rule of signs using pigeonholing based on geometry of numbers and the above strategy.

Theorem 4.4.3 (Lemma 7 in [19]). *For a t-sparse polynomial $f(x) \in \mathbb{F}_q[x]$, we have*

$$|Z^*(f)| \leq 2(q-1)^{1-1/(t-1)}\delta(f)^{1/(t-1)} + O\left((q-1)^{1-2/(t-1)}\delta(f)^{2/(t-1)}\right).$$

Kelley [66] refined their method and showed that $C(f) \leq \delta(f)$. Thus the following theorem improves Theorem 4.4.3.

Theorem 4.4.4 (Theorem 2.3 in [66]). *For a t-sparse polynomial $f(x) \in \mathbb{F}_q[x]$, we have*

$$|Z^*(f)| \leq 2(q-1)^{1-1/(t-1)}C(f)^{1/(t-1)}. \tag{4.1}$$

In the case $t = 3$, Kelley and Owen [67] improved the above bound on $|Z^*(f)|$ for trinomials f to the following.

Theorem 4.4.5 ([67]). *For a trinomial $f(x) = x^n + ax^s + b \in \mathbb{F}_q[x]$, where $a, b \neq 0$, we have*

$$|Z^*(f)| \leq D(f)\left\lfloor \frac{1}{2} + \sqrt{\frac{q-1}{D(f)}} \right\rfloor, \quad \text{where } D(f) = \gcd(n, s, q-1). \tag{4.2}$$

Furthermore, if q is a square, and $D(f) = 1$, then this bound is tight.

Based on numerical evidence, they conjectured the upper bound can be improved significantly.

Conjecture 4.4.6 ([67]). *For a trinomial $f(x) = x^n + ax^s + b \in \mathbb{F}_p[x]$, where $a, b \neq 0$, we have $|Z^*(f)| = O(D(f)\log p)$, where $D(f) = \gcd(n, s, p-1)$.*

4.5 Singularity of generalized Vandermonde matrices over a finite field

Lemma 4.5.1. *Let K be a field. If $a_1, a_2, \ldots, a_n \in K$, then the* Vandermonde matrix

$$V_n(a_1, a_2, \ldots a_n) = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ a_1 & a_2 & \cdots & a_{n-1} & a_n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_1^{n-2} & a_2^{n-2} & \cdots & a_{n-1}^{n-2} & a_n^{n-2} \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_{n-1}^{n-1} & a_n^{n-1} \end{pmatrix}$$

is invertible if and only of $a_1, a_2, \ldots, a_n$ are all distinct.

Proof. It is a classical result that the determinant of $V_n(a_1, a_2, \ldots a_n)$ is

$$\prod_{1 \le i < j \le n} (a_i - a_j). \qquad \square$$

Definition 4.5.2. *Let K be a field. A* generalized Vandermonde matrix *is of the form*

$$V_n(a_1, a_2, \ldots a_n; b_1, b_2, \ldots b_n) = \begin{pmatrix} a_1^{b_1} & a_2^{b_1} & \cdots & a_{n-1}^{b_1} & a_n^{b_1} \\ a_1^{b_2} & a_2^{b_2} & \cdots & a_{n-1}^{b_2} & a_n^{b_2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_1^{b_{n-1}} & a_2^{b_{n-1}} & \cdots & a_{n-1}^{b_{n-1}} & a_n^{b_{n-1}} \\ a_1^{b_n} & a_2^{b_n} & \cdots & a_{n-1}^{b_n} & a_n^{b_n} \end{pmatrix},$$

where $a_1, a_2, \ldots, a_n \in K$, and $b_1, b_2, \ldots, b_n$ are nonnegative integers.

We are interested in studying the invertibility of a generalized Vandermonde matrix. There are explicit formulas in computing some special types of generalized Vandermonde determinants, see for example [56] and [39]. In general, if $b_1 > b_2 > \ldots > b_n$, we have the bialternant formula [102] that

$$\begin{aligned} &\det V_n(a_1, a_2, \ldots a_n; b_1, b_2, \ldots b_n) \\ &= \det V_n(a_1, a_2, \ldots, a_n; n-1, n-2, \ldots, 0) s_\lambda(a_1, a_2, \ldots, a_n) \\ &= s_\lambda(a_1, a_2, \ldots, a_n) \prod_{1 \le i < j \le n} (a_i - a_j), \end{aligned}$$

where $\lambda = (b_1 - (n-1), b_2 - (n-2), \ldots, b_n)$ and s is the Schur polynomial. However, it is not an easy task to determine the zeros of a Schur polynomial. See [41] for a further discussion on the relation between generalized Vandermonde matrices and Schur polynomials. When the underlying field is $\mathbb{R}$, we have the following classical result.

Theorem 4.5.3. *Let $a_1 < a_2 < \ldots < a_n$ be positive real numbers, and let $b_1 < b_2 < \ldots < b_n$ be positive integers, then*

$$\det V_n(a_1, a_2, \ldots a_n; b_1, b_2, \ldots b_n) > 0.$$

Sketch of the proof. Note that we can treat the determinant as a continuous function of $b_1, b_2, \ldots, b_n$. When $b_j = j$ for each $1 \le j \le n$, the determinant is the standard Vandermonde determinant, which is positive. Therefore, it suffices to show that the determinant is always nonzero. To prove that, it is equivalent to show for any $c_1, c_2, \ldots, c_n \in \mathbb{R}$, not all 0, the equation

$$f(x) = \sum_{j=1}^{n} c_j x^{b_j}$$

has at most $n-1$ positive roots. If all b_j's are integers, this follows from Descartes' rule of signs. $\square$

When the underlying field is a cyclotomic field, the following theorem says all generalized Vandermonde matrices are non-singular. This result was first proved by by Chebotarëv [113] in 1926, and Tao gave a simple proof in [116].

Theorem 4.5.4 (Lemma 1.3 in [116]). *Let p be a prime and $1 \leq n \leq p$. Let $x_1, \ldots, x_n$ be distinct elements of $\mathbb{Z}/p\mathbb{Z}$, and let $b_1, \ldots, b_n$ also be distinct elements of $\mathbb{Z}/p\mathbb{Z}$. Set $a_j = \exp(2\pi i x_j/p)$, then*

$$\det V_n(a_1, a_2, \ldots a_n; b_1, b_2, \ldots b_n) \neq 0.$$

We expect that a similar result will hold when the underlying field is $\mathbb{F}_q$. Using Theorem 4.4.3, Shparlinski [110] showed that, for a fixed n, almost all $n \times n$ generalized Vandermonde matrices over $\mathbb{F}_q$ are invertible. To be precise, let $a_1, a_2, \ldots, a_n \in \mathbb{F}_q^*$, we denote $T(a_1, a_2, \ldots, a_n)$ be the number of n-tuples $(b_1, b_2, \ldots, b_m)$ such that

$$\det V_n(a_1, a_2, \ldots a_n; b_1, b_2, \ldots b_n) = 0.$$

Let W_n be the average, i.e.

$$W_n = \frac{1}{(q-1)^n} \sum_{a_1, a_2, \ldots, a_n \in \mathbb{F}_q^*} T(a_1, a_2, \ldots, a_n).$$

Theorem 4.5.5 (Theorem 4 in [110]). *For any $n \geq 2$ and any $\varepsilon > 0$, we have*

$$W_n = O(q^{n-1/(n-1)+\varepsilon}).$$

This is the best known bound, but we expect this bound can be greatly improved.

Chapter 5

On the number of distinct roots of a lacunary polynomial over finite fields

This chapter is based on [112].

The theory of lacunary polynomials has nice applications to computing theory, character sums, and discrete geometry. László Rédei's monograph [98] is one of the most significant and important works on lacunary polynomials. or a polynomial $f(x) \in \mathbb{F}_q[x]$, we will denote by f° and $f^{\circ\circ}$ the degree of $f(x)$, and the degree of the second highest term of $f(x)$, respectively. One of Rédei's seminal results on lacunary polynomials is the following.

Theorem 5.0.1 (Theorem 5 in [98])**.** *Let q be a prime power and $d > 1$ be a divisor of $q-1$. Let $f(x) \in \mathbb{F}_q[x]$ be a monic polynomial such that*

$$f(x)|(x^{q-1}-1), \quad f^\circ = \frac{q-1}{d}, \quad \textit{and} \quad f^{\circ\circ} \leq \frac{q-1}{d^2}.$$

Then $f(x)$ is an Euler binomial

$$x^{\frac{q-1}{d}} - \alpha, \quad \textit{for some} \quad \alpha \in (\mathbb{F}_q^*)^{\frac{q-1}{d}},$$

or if $p \neq 2$, $4|(q-1)$, and $d = 2$, then possibly takes the form

$$\left(x^{\frac{q-1}{4}} - \beta\right)\left(x^{\frac{q-1}{4}} - \gamma\right), \ \textit{where} \quad \beta^2 = 1, \gamma^2 = -1.$$

The above theorem shows that within a certain class of polynomials, a polynomial $f(x)$ cannot be simultaneously lacunary and possess f° distinct roots. In this chapter, we will extended this property to a larger class of polynomials and show that the number of distinct roots of many lacunary polynomials is often less than its degree. Recall that Our main focus will be on polynomials $f(x) \in \mathbb{F}_q[x]$ of the form $f(x) = x^{\frac{q-1}{d}-\ell} + g(x)$, where $\ell \geq 0$, d is a positive divisor of $q-1$, and $\deg g < \frac{q-1}{d} - \ell$. Since we are interested in nonzero roots, we will always assume that the constant term of $f(x)$ is nonzero.

5.1 Improving the degree bound

Our first two theorems are motivated by the following well-known result in the case $d = 1$.

Lemma 5.1.1. *Suppose $f(x) \in \mathbb{F}_q[x]$ has the form $x^m + g(x)$, for some $g(x) \in \mathbb{F}_q[x]$ such that $1 \leq g^\circ < m \leq q-1$. Let $\delta = m - g^\circ$ be the gap between the exponents of the two highest terms. Then $|Z^*(f)| \leq q - 1 - \delta$.*

Proof. Note that for any $a \in \mathbb{F}_q^*$, $a^{q-1} = 1$. Consequently, for any $a \in \mathbb{F}_q^*$ we have $a^{q-1-m} f(a) = a^{q-1-m} g(a) + 1$. This gives

$$|Z^*(f)| = |Z^*(x^{q-1-m} g(x) + 1)| \leq q - 1 - m + g^\circ = q - 1 - \delta. \qquad \square$$

If the degree of the polynomial f is bounded by $\frac{q-1}{d}$, then we have the following improved upper bound of $|Z^*(f)|$.

Theorem 5.1.2. *Let $\ell \geq 0$ be a nonnegative integer. Suppose $f(x) \in \mathbb{F}_q[x]$ has the form $x^{\frac{q-1}{d}-\ell} + g(x)$, for some $g(x) \in \mathbb{F}_q[x]$ such that $1 \leq g^\circ < \frac{q-1}{d} - \ell$. Let $\delta = \frac{q-1}{d} - \ell - g^\circ$, be the gap between the exponents of the two highest terms. Then $|Z^*(f)| \leq d(\ell + g^\circ) = q - 1 - d\delta$.*

Proof. Since $Z^*(f) = Z^*(x^\ell f)$, we consider the roots of $x^{\frac{q-1}{d}} + x^\ell g(x)$. A root of $x^\ell f(x)$ is a root of

$$\xi + x^\ell g(x), \tag{5.1}$$

for some $\xi \in (\mathbb{F}_q^*)^{\frac{q-1}{d}}$. Since $g^\circ \geq 1$, (5.1) has at most $\ell + g^\circ$ roots. Combining this with $|(\mathbb{F}_q^*)^{\frac{q-1}{d}}| = d$ gives the required bound. $\square$

For a polynomial $f(x)$ satisfying the hypotheses of Theorem 5.0.1 that is not a binomial, note that Theorem 5.1.2 implies that $f^{\circ\circ} = \frac{q-1}{d^2}$. Below is an example when Theorem 5.1.2 is tight.

Example 5.1.3. *Let p be a prime $p \equiv 7 \pmod{20}, p > 7, d = 2, \ell = 1$ and $g^\circ = 2$. By the law of quadratic reciprocity, we have*

$$\left(\frac{5}{p}\right)\left(\frac{p}{5}\right) = (-1)^{2 \cdot \frac{p-1}{2}} = 1.$$

Since $(\frac{p}{5}) = (\frac{2}{5}) = -1$, we have $(\frac{5}{p}) = -1$, and so 5 is a quadratic non-residue in $\mathbb{F}_p$. Then -5 is a quadratic residue in $\mathbb{F}_p$ since $p \equiv 3 \pmod 4$. Let $a \in \mathbb{F}_p$ be such that $-5a = 1$, thus a is a quadratic residue in $\mathbb{F}_p$. Let $S = \{1, 4, 4a\}$. Then S is a subset of quadratic residues and $-S$ is a subset of quadratic non-residues. Define the polynomial

$$f(x) = x^{\frac{p-1}{2}-1} - 16ax^2 - (4a+5) \in \mathbb{F}_p[x].$$

It is easy to check that $S^{-1} \cup (-S^{-1}) \subseteq Z^*(f)$. By Theorem 5.1.2, $|Z^*(f)| \leq 6$, and so $Z^*(f) = S^{-1} \cup (-S^{-1})$ and Theorem 5.1.2 is tight in this case. In particular, when $p = 47$, we can take $S = \{1, 4, 18\}$ and $f(x) = x^{22} + 22x^2 + 24$.

We can combine Theorem 5.1.2 and the trivial degree bound on $|Z^*(f)|$ to obtain the following bound, which is independent of the divisor d.

Corollary 5.1.4. *Let $\ell \geq 0$ be a nonnegative integer. Suppose $f(x) \in \mathbb{F}_q[x]$ has the form $x^{\frac{q-1}{d}-\ell} + g(x)$, for some $g(x) \in \mathbb{F}_q[x]$ such that $1 \leq g^\circ < \frac{q-1}{d} - \ell$. Then $|Z^*(f)| \leq \sqrt{(q-1)(\ell + g^\circ)}$.*

Proof. Note that we have the trivial degree bound $|Z^*(f)| \leq f^\circ \leq \frac{q-1}{d}$, and by Theorem 5.1.2, $|Z^*(f)| \leq d(\ell + g^\circ)$. Therefore, $|Z^*(f)| \leq \sqrt{\frac{q-1}{d} d(\ell + g^\circ)} = \sqrt{(q-1)(\ell + g^\circ)}$. □

In the above discussion, we restricted ℓ to be a nonnegative integer. When $\ell < 0$, a similar trick leads to the following theorem.

Theorem 5.1.5. *Let $m \geq 0$ be a nonnegative integer. Suppose $f(x) \in \mathbb{F}_q[x]$ has the form $x^{\frac{q-1}{d}+m} + g(x)$, for some $g(x) \in \mathbb{F}_q[x]$ such that $1 \leq g^\circ < \frac{q-1}{d} + m$. Then $|Z^*(f)| \leq d \max\{m, g^\circ\}$.*

Proof. If $x \neq 0$, then

$$f(x) = \xi x^m + g(x), \tag{5.2}$$

for some $\xi \in (\mathbb{F}_q^*)^{\frac{q-1}{d}}$. Since $g^\circ \geq 1$, and the constant term of g is nonzero, then $\xi x^m + g(x)$ is a nonzero polynomial with degree at most $\max\{m, g^\circ\}$, so (5.2) has at most $\max\{m, g^\circ\}$ roots. There are d such $\xi \in (\mathbb{F}_q^*)^{\frac{q-1}{d}}$ and so the required bound follows. □

Below is an example when Theorem 5.1.5 is tight.

Example 5.1.6. *Let p be a prime $p \equiv 3 \pmod 4, p > 3, d = 2, m = 1$ and $g^\circ = 2$. Let $r_1, r_2 \in \mathbb{F}_p^*$ be any two quadratic residues. Note that $r_1 + r_2 \neq 0$ since $p \equiv 3 \pmod 4$. Let $a \in \mathbb{F}_p$ be such that $a(r_1 + r_2) = -1$. Define the polynomial*

$$f(x) = x^{\frac{p-1}{2}+1} + ax^2 + ar_1r_2 \in \mathbb{F}_p[x].$$

It is easy to check that $Z^*(f) = \{r_1, r_2, -r_1, -r_2\}$.

We remark that in general the best known bounds on the number of zeros of a trinomial are due to Kelley and Owen [67] and recorded in Equation (4.2). Their bounds are on the order of $\sqrt{q}$ in magnitude. For trinomials satisfying the hypotheses of Theorem 5.1.2 or Theorem 5.1.5, the respective theorems offer a significantly better bound on $|Z^*(f)|$. Examples for which Theorem 5.1.2 or Theorem 5.1.5 is tight seem harder to construct for larger g°. The example below gives a class of examples for primes p for which -29 is a square in $\mathbb{F}_p$.

Example 5.1.7. *Let p be a prime $p \equiv 31 \pmod{116}, d = 2, m = 1$ and $g^\circ = 4$. Let $S = \{4, 9, 16, -29\}$, using a similar argument as in Example 5.1.3, we can show S is a subset of quadratic residues and $-S$ is a subset of quadratic non-residues. Define the polynomial*

$$f(x) = 6500x^{\frac{p-1}{2}+1} + (x-4)(x-9)(x-16)(x+29) - 6500x \in \mathbb{F}_p[x].$$

It is easy to check that $Z^*(f) = S \cup (-S)$.

In the above example, $f(x)$ is a 4-sparse polynomial with 8 distinct roots. Kelley's bound in Equation (4.1) gives a bound on $|Z^*(f)|$ on the order $p^{2/3}$. Once again this demonstrates that a sparsity-only bound on $|Z^*(f)|$ such as (4.1) can be significantly improved if f is also lacunary.

We will see that the above two theorems can be combined and iterated to yield a stronger statement on the size of $|Z^*(f)|$. The coloured regions in Figure 5.1 indicate when the degree bound on $|Z^*(f)|$ can be improved in terms of ℓ and g°. We will prove the content of Figure 5.1 in Theorem 5.1.8. The numbers on the coloured regions of Figure 5.1 correspond to the cases described in Theorem 5.1.8.

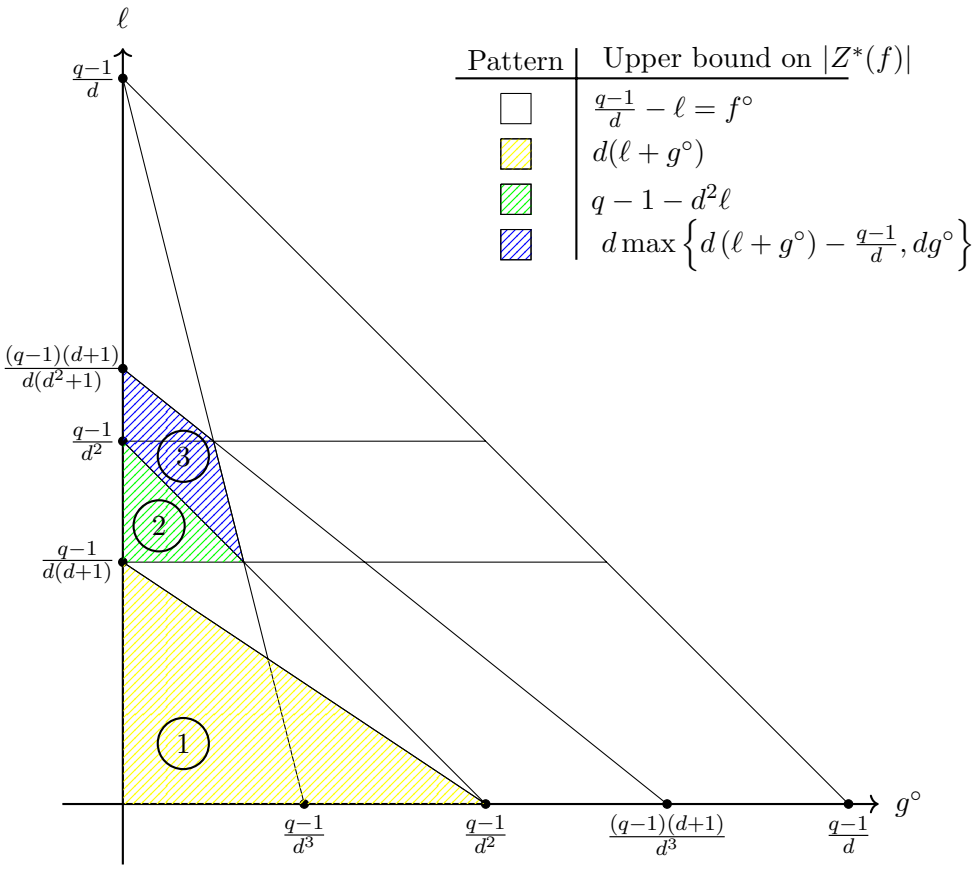

Figure 5.1: Bounding $|Z^*(f)|$ for $f(x) = x^{\frac{q-1}{d}-\ell} + g(x)$.

Theorem 5.1.8. *Let $\ell \geq 0$ be a nonnegative integer. Suppose $f(x) \in \mathbb{F}_q[x]$ has the form $x^{\frac{q-1}{d}-\ell} + g(x)$, for some $g(x) \in \mathbb{F}_q[x]$ such that $1 \leq g^\circ < \frac{q-1}{d} - \ell$. If one of the following holds, then $|Z^*(f)| < f^\circ$.*

(1) *$d(d+1)\ell + d^2 g^\circ < q-1$;*

(2) *$d^2(\ell + g^\circ) \leq q-1$ and $d(d+1)\ell > q-1$;*

(3) *$d^2(\ell + g^\circ) > q-1$, $d\ell + d^3 g^\circ < q-1$, and $d(d^2+1)\ell + d^3 g^\circ < (q-1)(d+1)$.*

Proof. By Theorem 5.1.2, we have $|Z^*(f)| \le d(\ell+g^\circ)$, which is an improved bound when $d(\ell+g^\circ) < \frac{q-1}{d} - \ell$, i.e. $d(d+1)\ell + d^2 g^\circ < q-1$.
If $\ell = 0$, then obviously (2) and (3) do not hold. In the following discussion, we assume $\ell > 0$. Note the proof of Theorem 5.1.2 shows that all nonzero roots of $f(x)$ are roots of

$$\prod_{\xi \in (\mathbb{F}_q^*)^{\frac{q-1}{d}}} \left(x^\ell g(x) + \xi\right) = x^{d\ell} g^d(x) - 1, \tag{5.3}$$

and the constant term of $x^{d\ell} g^d(x) - 1$ is -1 since $\ell > 0$. By using the substitution $x = y^{-1}$ and multiplying by $-y^{d(\ell+g^\circ)}$ in (5.3), we see the number of roots of (5.3) is the same as the number of nonzero roots of the following monic polynomial

$$h(y) = y^{d(\ell+g^\circ)} - y^{dg^\circ} g^d(y^{-1}). \tag{5.4}$$

Note that the degree of h is $d(\ell+g^\circ)$, and the degree of $y^{dg^\circ} g^d(y^{-1})$ is dg°. Let $\ell' = \frac{q-1}{d} - d(\ell+g^\circ)$. We consider two cases.

- If $\ell' \ge 0$, then we can apply Theorem 5.1.2 to conclude that

  $$|Z^*(f)| \le |Z^*(h)| \le d(\ell' + dg^\circ) = q - 1 - d^2\ell,$$

  which is an improved bound provided $\frac{q-1}{d} - d(\ell + g^\circ) \ge 0$ and $q - 1 - d^2\ell < \frac{q-1}{d} - \ell$, i.e. $d^2(\ell + g^\circ) \le q-1$ and $d(d+1)\ell > q-1$.

- If $\ell' < 0$, then we can apply Theorem 5.1.5 to show that

  $$|Z^*(f)| \le |Z^*(h)| \le d \max\left\{-\ell', dg^\circ\right\} = d \max\left\{d\left(\ell + g^\circ\right) - \frac{q-1}{d}, dg^\circ\right\},$$

  which is an improved bound provided $\frac{q-1}{d} - d(\ell + g^\circ) < 0$ and
  $d \max\left\{d\left(\ell + g^\circ\right) - \frac{q-1}{d}, dg^\circ\right\} < \frac{q-1}{d} - \ell$, i.e.
  $d^2(\ell + g^\circ) > q-1$, $d^2(\ell + g^\circ) - (q-1) < \frac{q-1}{d} - \ell$ and $d^2 g^\circ < \frac{q-1}{d} - \ell$. □

Below we give examples of polynomials where $|Z^*(f)| = f^\circ$, showing limitations of extending Theorem 5.1.8 for a larger range of g°, ℓ.

Example 5.1.9. *Let $D, n \ge 1$ be positive integers such that $D(n+1)|(q-1)$. Then $x^{D(n+1)} - 1 = 0$ has $D(n+1)$ distinct nonzero solutions. Moreover,*

$$f(x) = x^{Dn} + x^{D(n-1)} + \cdots + x^D + 1 = \frac{x^{D(n+1)} - 1}{x^D - 1}, \tag{5.5}$$

has Dn distinct nonzero solutions, i.e. we have a class of lacunary polynomials $f(x)$ with $|Z^*(f)| =$

f°. We will compare these examples to Theorem 5.1.8 in the case $n = d = 2$. Let

$$x^{2D} + x^D + 1 = x^{\frac{q-1}{2}-\ell} + g(x),$$

and so $\ell = (q-1)/2 - 2D$ and $g^\circ = D$. Therefore such examples lie on a line in the ℓ, g°-axis system used above. In Figure 5.2 we illustrate the relation between this line of examples and the regions of improvement.

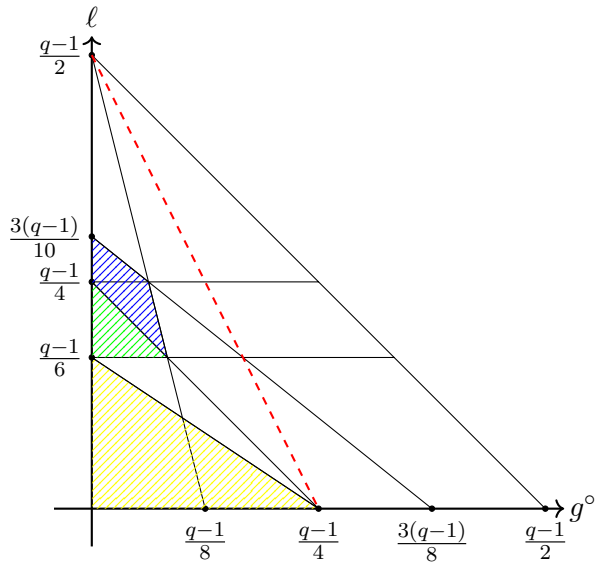

Figure 5.2: Limitations to improving the degree bound.

It seems plausible that Theorem 5.1.8 could be improved to include more regions that appear left of the red dashed line in Figure 5.2. We leave this as an open problem. We conclude this section with several generalizations of the above results. In the next result we show that the polynomials of interest in Theorem 5.1.2 and Theorem 5.1.5 belong to a much larger class of polynomials for which strong bounds on the number of distinct roots exist. In particular, the factor of $x^{-\ell}$ or x^m appearing in the leading term can be extended to any rational function satisfying a linear independence condition.

Theorem 5.1.10. *Let $s(x), t(x), g(x) \in \mathbb{F}_q[x]$ be polynomials such that the rational function defined by $r(x) = s(x)/t(x)$ and $g(x)$ are linearly independent. Also let $h(x) \in \mathbb{F}_q[x]$ be a non-constant polynomial with no zeros in $\mathbb{F}_q^*$. Define the rational function $f(x) = (h(x))^{\frac{q-1}{d}} r(x) + g(x)$. Then the number of distinct nonzero roots of $f(x)$ is at most $d \max\{s^\circ, g^\circ + t^\circ\}$.*

The ideas behind Theorem 5.1.2 and Theorem 5.1.5 can be reused to prove Theorem 5.1.10. Note that the linearly independent assumption is necessary since we need to ensure $\xi s(x) + t(x)g(x)$ is a nonzero polynomial for $\xi \in (\mathbb{F}_q^*)^{\frac{q-1}{d}}$. Theorem 5.1.10 is noteworthy since the polynomials $f(x)$ to which it applies may be neither lacunary nor sparse.

The following is a result for t-sparse polynomials. It extends Theorem 5.1.2 and Theorem 5.1.5. The proof employs a similar argument to those seen above. Note that Theorem 5.1.11 does not require a polynomial with degree close to $\frac{q-1}{d}$.

Theorem 5.1.11. *Let*

$$h(x) = \sum_{i=1}^{t} c_i x^{e_i} \in \mathbb{F}_q[x],$$

be a t-sparse polynomial. Suppose that there exist integers a_i, b_i, $i = 1, 2, \ldots, t$ such that

$$e_i = a_i \frac{q-1}{d} + b_i, \text{ where } -\frac{q-1}{d} < b_i < \frac{q-1}{d}.$$

Let A, B be integers such that $\{b_i : 1 \le i \le t\}$ are contained in the interval $[A, B]$. If $h(x)$ does not vanish on any coset of $(\mathbb{F}_q^*)^d$ in $\mathbb{F}_q^*$, then $|Z^*(h)| \le d(B - A)$.

Proof. Let $\{\xi_1, \ldots, \xi_d\} = (\mathbb{F}_q^*)^{\frac{q-1}{d}}$ and define $S_i = \{a \in \mathbb{F}_q^* \colon a^{\frac{q-1}{d}} = \xi_i\}$. Note that $S_1, \ldots, S_d$ are the cosets of $\mathbb{F}_q^*$ of size $\frac{q-1}{d}$. Fix an i in $[1, t]$. For $y \in S_i$ we have

$$y^{-A} h(y) = y^{-A} \sum_{i=1}^{t} c_i y^{e_i} = \sum_{i=1}^{t} c_i \xi_i^{a_i} y^{b_i - A}. \tag{5.6}$$

Observe that above expression is a polynomial in y. Moreover, since h does not vanish on any coset of $\mathbb{F}_q^*$ of size $\frac{q-1}{d}$, (5.6) is a nonzero polynomial with degree at most $B - A$. Therefore, for each i, h has at most $B - A$ zeros in S_i. It follows that $|Z^*(h)| \le d(B - A)$. □

We remark that the assumption that $h(x)$ does not vanish on any coset of $(\mathbb{F}_q^*)^d$ in $\mathbb{F}_q^*$ is often guaranteed. This is the case for the polynomials we will discuss in the remaining of the section. Below we see an example of Theorem 5.1.11 in practice.

Example 5.1.12. *Let $h(x) = \sum_{j=1}^{m} c_j x^{\frac{q-1}{d_j}} + ax + b$, where $d_j \mid (q-1)$ and $d_j < q - 1$. Take $d = \operatorname{lcm}\{d_1, d_2, \ldots, d_m\}$, then it follows that the interval we obtained is $[A, B] = [0, 1]$ since $\frac{q-1}{d}$ divides all the exponents expect the linear term and the constant term. So $|Z^*(h)| \le d = \operatorname{lcm}\{d_1, d_2, \ldots, d_m\}$.*

Theorem 5.1.2 and Theorem 5.1.5 can be obtained from Theorem 5.1.11 in the following way. For Theorem 5.1.2, we can take the interval $[A, B]$ to be $[-\ell, g^\circ]$. For Theorem 5.1.5, we can take the interval $[A, B]$ to be $[0, \max\{m, g^\circ\}]$. Theorem 5.1.11 is strongest when the remainders of the exponents dividing $\frac{q-1}{d}$ are concentrated in a short interval.

The following is a corollary of Theorem 5.1.11. It generalizes Theorem 5.1.2. The point is that if a large gap appears between any consecutive exponents, then an improved bound on the number of distinct roots may be possible.

Corollary 5.1.13. *Let $h(x) = \sum_{i=1}^{t} c_i x^{e_i} \in \mathbb{F}_q[x]$ be a t-sparse polynomial, where $\frac{q-1}{d} \ge e_1 > e_2 > \cdots > e_t$. Define the gap δ of $h(x)$ to be the largest difference between consecutive exponents, i.e. $\delta = \max\{e_{i-1} - e_i : 2 \le i \le t\}$, then $|Z^*(h)| \le q - 1 - d\delta$.*

Proof. Suppose $\delta = e_{j-1} - e_j$, then the exponents modulo $\frac{q-1}{d}$ are all contained in the interval $[-(\frac{q-1}{d} - e_{j-1}), e_j]$. By Theorem 5.1.11, $|Z^*(h)| \leq d(e_j + \frac{q-1}{d} - e_{j-1}) = q - 1 - d\delta$. □

We remark that Karpinski and Shparlinski's bound $|Z^*(h)| \leq \frac{t-1}{t}(q-1)$ given in [64] can be recovered from the above corollary by taking $d = 1$.

5.2 Iterating to obtain stronger bounds on $|Z^*(f)|$

In this section we build on the ideas presented in the proof of Theorem 5.1.8. In particular we iterate the argument of Theorem 5.1.8 as many times as possible, to yield a stronger bound on $|Z^*(f)|$. Throughout this section, $d, \ell \geq 1$ will be positive integers such that $d|(q-1)$ and $\frac{q-1}{d} - \ell > 1$, $g(x) \in \mathbb{F}_q[x]$ will be such that $1 \leq g^\circ < \frac{q-1}{d} - \ell$, $x \nmid g(x)$, and $f(x) \in \mathbb{F}_q[x]$ will be given by

$$f(x) = x^{\frac{q-1}{d} - \ell} + g(x).$$

Put $\ell_0 = \ell$, and $g_0(x) = g(x)$. For $i \geq 0$, define

$$g_{i+1}(x) = -x^{dg_i^\circ} g_i^d(x^{-1}), \quad \text{and} \quad \ell_{i+1} = \frac{q-1}{d} - d(\ell_i + g_i^\circ). \tag{5.7}$$

Lemma 5.2.1. *Let the sequences $\{g_i\}_{i\geq 0}$, $\{\ell_i\}_{i\geq 0}$ be as in (5.7). Suppose that for an integer $k \geq -1$ we have*

$$d(\ell_i + g_i^\circ) < \frac{q-1}{d}, \quad \text{for} \quad 0 \leq i \leq k.$$

Then

$$|Z^*(f)| \leq \min_{0 \leq i \leq k+1} d(\ell_i + g_i^\circ).$$

Proof. The case $k = -1$ is Theorem 5.1.2. Suppose the hypothesis of the theorem holds for $k \geq 0$. Put

$$f_i(x) = x^{\frac{q-1}{d} - \ell_i} + g_i(x).$$

Note that $f_0 = f$. Fix any i, $0 \leq i \leq k+1$. If $i = 0$, then $\ell_i > 0$ by definition. For $i \geq 1$, since $d(\ell_{i-1} + g_{i-1}^\circ) < \frac{q-1}{d}$, we again have $\ell_i > 0$. A nonzero root of $f_i(x)$ is a root of $x^{\ell_i} f_i(x)$, and therefore is also a root of

$$\prod_{\xi \in (\mathbb{F}_q^*)^{\frac{q-1}{d}}} \left(x^{\ell_i} g_i(x) + \xi\right) = x^{d\ell_i} g_i^d(x) - 1.$$

Substituting $x = y^{-1}$ and multiplying by $-y^{d(\ell_i + g_i^\circ)}$ in the above gives the polynomial

$$y^{d(\ell_i + g_i^\circ)} - y^{dg_i^\circ} g_i^d(y^{-1}) = f_{i+1}(y).$$

Therefore $|Z^*(f_{i+1})| \geq |Z^*(f_i)|$. Since $|Z^*(f_{i+1})| \leq f_{i+1}^\circ$, we have the desired result. □

Lemma 5.2.1 potentially provides many upper bounds on $|Z^*(f)|$. To aid with determining the best bound, we use explicit formulae for the sequences $\{g_i^\circ\}, \{\ell_i + g_i^\circ\}$.

Lemma 5.2.2. *The sequences $\{g_i^\circ\}$ and $\{\ell_i + g_i^\circ\}$ are given by*

$$g_i^\circ = d^i g^\circ,$$

and

$$\ell_i + g_i^\circ = \begin{cases} d^i(\ell + g^\circ) - \frac{q-1}{d(d+1)}(d^i - 1) & \text{if } i \text{ is even;} \\ -d^i\ell + \frac{q-1}{d(d+1)}(d^i + 1) & \text{if } i \text{ is odd.} \end{cases}$$

Proof. From the assumption that $g(x)$ has a nonzero constant term and the recurrence relation $g_{i+1}(x) = -x^{dg^\circ} g_i^d(x^{-1})$, the first statement immediately follows. For the second statement, note that $\ell_{i+1} = \frac{q-1}{d} - d(\ell_i + g_i^\circ)$ implies that

$$\ell_{i+1} + g_{i+1}^\circ = \frac{q-1}{d} - d\ell_i = \frac{q-1}{d} - d(\ell_i + g_i^\circ) + d^{i+1}g^\circ.$$

Dividing d^{i+1} on both sides yields

$$\frac{\ell_{i+1} + g_{i+1}^\circ}{d^{i+1}} = \frac{q-1}{d^{i+2}} - \frac{\ell_i + g_i^\circ}{d^i} + g^\circ.$$

Now if we set $a_i = \frac{\ell_i + g_i^\circ}{d^i}$ for $i \geq 0$, then we get $a_0 = \ell + g^\circ$, and $a_{i+1} + a_i = \frac{q-1}{d^{i+2}} + g^\circ$ for $i \geq 0$. If i is odd, then

$$\begin{aligned} a_i &= (a_i + a_{i-1}) - (a_{i-1} + a_{i-2}) + \cdots + (a_1 + a_0) - a_0 \\ &= -\ell + \frac{(q-1)(1-d)(1+d^{-i})}{d(1-d^2)} = -\ell + \frac{(q-1)(1+d^{-i})}{d(d+1)}. \end{aligned}$$

If i is even, then

$$\begin{aligned} a_i &= (a_i + a_{i-1}) - (a_{i-1} + a_{i-2}) + \cdots + (a_2 + a_1) - (a_1 + a_0) + a_0 \\ &= \ell + g^\circ + \frac{(q-1)(1-d)(1-d^{-i})}{d(1-d^2)} = \ell + g^\circ + \frac{(q-1)(1-d^{-i})}{d(d+1)}. \end{aligned}$$

Now applying the relation $\ell_i + g_i^\circ = d^i a_i$ gives the required result. □

From now on, we will use Lemma 5.2.2 without explicitly saying so. If $d = 1$, then the sequence $\{\ell_i + g_i^\circ\}$ oscillates between the values $\ell + g^\circ$ and $q - 1 - \ell$, and so nothing is gained by considering later terms in $\{d(\ell_i + g_i^\circ)\}$. We will only consider $d \geq 2$. Now better estimates of $|Z^*(f)|$ may appear later in the sequence $\{d(\ell_i + g_i^\circ)\}$. For example, the first five terms of $\{d(\ell_i + g_i^\circ)\}$ are

$$d(\ell + g^\circ),\ q - 1 - d^2\ell,\ d^3(\ell + g^\circ) - (q-1)(d-1),$$

$$(q-1)(d^2-d+1)-d^4\ell,\ d^5(\ell+g^\circ)-(q-1)(d^3-d^2+d-1). \tag{5.8}$$

In Figure 5.3 we illustrate which bound in Equation (5.8) is best when it is applicable.

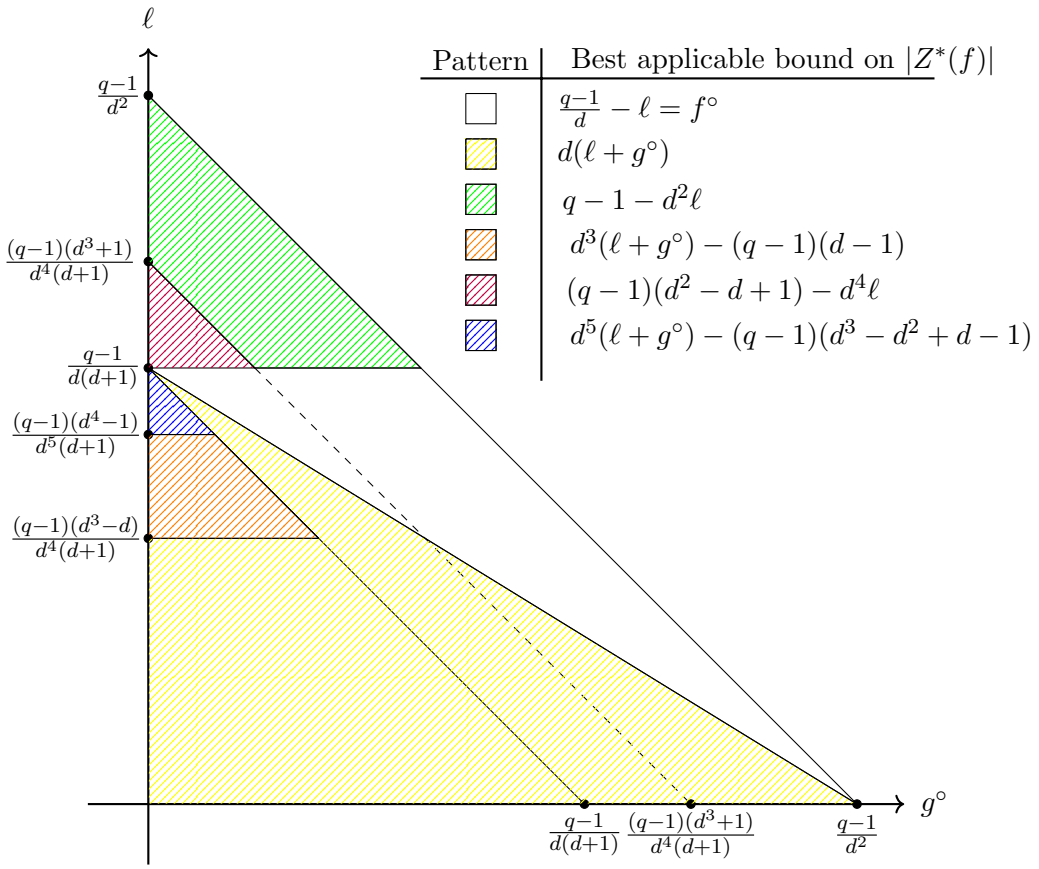

Figure 5.3: Comparing the six bounds in (5.8) for $|Z^*(f)|$

The formulae in Lemma 5.2.2 can be used to determine the minimum $d(\ell_i+g_i^\circ)$.

Lemma 5.2.3. ***(1)*** *If $\ell > \frac{q-1}{d(d+1)}$, then for all $i>j\geq 0$ and $t\geq 0$,*

$$\ell_{2i+1}+g_{2i+1}^\circ < \ell_{2j+1}+g_{2j+1}^\circ < \frac{q-1}{d}-\ell, \quad \textit{and} \quad \ell_{2i+1}+g_{2i+1}^\circ < \ell_{2t}+g_{2t}^\circ.$$

(2) *If $\ell+g^\circ < \frac{q-1}{d(d+1)}$, then for all $i>j\geq 0$ and $t\geq 0$,*

$$\ell_{2i}+g_{2i}^\circ < \ell_{2j}+g_{2j}^\circ < \frac{q-1}{d}-\ell, \quad \textit{and} \quad \ell_{2i}+g_{2i}^\circ < \ell_{2t+1}+g_{2t+1}^\circ.$$

(3) *If $\ell \leq \frac{q-1}{d(d+1)}$, and $\ell+g^\circ \geq \frac{q-1}{d(d+1)}$, then for all $i>j\geq 0$,*

$$\ell_{2i}+g_{2i}^\circ \geq \ell_{2j}+g_{2j}^\circ, \quad \textit{and} \quad \ell_{2i+1}+g_{2i+1}^\circ \geq \ell_{2j+1}+g_{2j+1}^\circ.$$

Proof. By Lemma 5.2.2, for each $i \geq 0$, we have

$$\ell_{2i} + g^{\circ}_{2i} = \frac{q-1}{d(d+1)} + d^{2i}\left(\ell + g^{\circ} - \frac{q-1}{d(d+1)}\right), \quad \ell_{2i+1} + g^{\circ}_{2i+1} = \frac{q-1}{d(d+1)} + d^{2i+1}\left(\frac{q-1}{d(d+1)} - \ell\right).$$

To determine the monotonicity of the two sequences, it suffices to compare the size of $\ell + g^{\circ}, \ell$ and $\frac{q-1}{d(d+1)}$. Therefore, there are the following three cases:

(1) If $\ell > \frac{q-1}{d(d+1)}$, then the sequence $\{\ell_{2i} + g^{\circ}_{2i}\}$ is strictly increasing, the sequence $\{\ell_{2i+1} + g^{\circ}_{2i+1}\}$ is strictly decreasing, and $\ell_1 + g^{\circ}_1 < \ell_0 + g^{\circ}_0$.

(2) If $\ell + g^{\circ} < \frac{q-1}{d(d+1)}$, then the sequence $\{\ell_{2i} + g^{\circ}_{2i}\}$ is strictly decreasing, the sequence $\{\ell_{2i+1} + g^{\circ}_{2i+1}\}$ is strictly increasing, and $\ell_1 + g^{\circ}_1 > \ell_0 + g^{\circ}_0$.

(3) If $\ell \leq \frac{q-1}{d(d+1)}$, and $\ell + g^{\circ} \geq \frac{q-1}{d(d+1)}$, then both sequences $\{\ell_{2i} + g^{\circ}_{2i}\}$ and $\{\ell_{2i+1} + g^{\circ}_{2i+1}\}$ are increasing. □

It remains to analyse the inequalities $d(\ell_i + g^{\circ}_i) \leq \frac{q-1}{d}$. Using the formulae in Lemma 5.2.2, we see that for $i \geq 0$, $d(\ell_{2i} + g^{\circ}_{2i}) \leq \frac{q-1}{d}$ is equivalent to

$$\ell + g^{\circ} \leq (q-1)\left(\frac{1 + d^{-2i-1}}{d(d+1)}\right).$$

And for $i \geq 0$, $d(\ell_{2i+1} + g^{\circ}_{2i+1}) \leq \frac{q-1}{d}$ is equivalent to

$$\ell \geq (q-1)\left(\frac{1 - d^{-2i-2}}{d(d+1)}\right).$$

Now we are ready to prove Theorem 1.6.6. We use Lemma 5.2.3 to determine what bound from Lemma 5.2.1 is best.

Theorem 1.6.6. *Let $f(x) \in \mathbb{F}_q[x]$ be as in (1.1) and assume that the constant term of f is nonzero. Then exactly one of the following holds.*

(1) *If $\ell > \frac{q-1}{d(d+1)}$ and $i \geq -1$ is the largest integer such that*

$$\ell + g^{\circ} < (q-1)\left(\frac{1 + d^{-2i-1}}{d(d+1)}\right), \tag{5.9}$$

then

$$|Z^*(f)| \leq \frac{q-1}{d+1} - d^{2i+2}\left(\ell - \frac{q-1}{d(d+1)}\right).$$

(2) *If $\ell + g^{\circ} < \frac{q-1}{d(d+1)}$ and $i \geq -1$ is the largest integer such that*

$$\ell > (q-1)\left(\frac{1 - d^{-2i-2}}{d(d+1)}\right), \tag{5.10}$$

then

$$|Z^*(f)| \leq \frac{q-1}{d+1} - d^{2i+3}\left(\frac{q-1}{d(d+1)} - (\ell + g^\circ)\right).$$

(3) *If* $\ell \leq \frac{q-1}{d(d+1)}$, $\ell + g^\circ \geq \frac{q-1}{d(d+1)}$, *and* $d(d+1)\ell + d^2 g^\circ < q-1$, *then*

$$|Z^*(f)| \leq d(\ell + g^\circ).$$

(4) *If* $\ell \leq \frac{q-1}{d(d+1)}$, $\ell + g^\circ \geq \frac{q-1}{d(d+1)}$, *and* $d(d+1)\ell + d^2 g^\circ \geq q-1$, *then*

$$|Z^*(f)| \leq f^\circ = \frac{q-1}{d} - \ell.$$

Proof. ***(1)*** The condition $\ell > \frac{q-1}{d(d+1)}$ gives that $d(\ell_j + g_j^\circ) < \frac{q-1}{d}$ for all odd $j \geq 1$. Equation (5.9) implies that $d(\ell_j + g_j^\circ) < \frac{q-1}{d}$ for all even $0 \leq j \leq 2i$. By Lemma 5.2.1, $|Z^*(f)| \leq d(\ell_j + g_j^\circ)$ for $0 \leq j \leq 2i+1$. By Lemma 5.2.3, the lowest upper bound of this set is

$$d(\ell_{2i+1} + g_{2i+1}^\circ) = \frac{q-1}{d+1}\left(d^{2i+1}+1\right) - d^{2i+2}\ell.$$

(2) The condition $\ell + g^\circ < \frac{q-1}{d(d+1)}$ gives that $d(\ell_j + g_j^\circ) < \frac{q-1}{d}$ for all even $j \geq 0$. Equation (5.10) implies that $d(\ell_j + g_j^\circ) < \frac{q-1}{d}$ for all odd $1 \leq j \leq 2i+1$. By Lemma 5.2.1, $|Z^*(f)| \leq d(\ell_j + g_j^\circ)$ for $0 \leq j \leq 2i+2$. By Lemma 5.2.3, the lowest upper bound of this set is

$$d(\ell_{2i+2} + g_{2i+2}^\circ) = d^{2i+3}(\ell + g^\circ) - \frac{q-1}{d+1}\left(d^{2i+2}-1\right).$$

(3&4) If $\ell \leq \frac{q-1}{d(d+1)}$ and $\ell + g^\circ \geq \frac{q-1}{d(d+1)}$, then by Lemma 5.2.3, $\{d(\ell_{2i} + g_{2i}^\circ)\}_{i\geq 0}$ is increasing. Similarly, $\{d(\ell_{2i+1} + g_{2i+1}^\circ)\}_{i\geq 0}$ is increasing and $f^\circ < d(\ell_1 + g_1^\circ)$. Therefore either f° or $d(\ell + g^\circ)$ is the lowest upper bound on $|Z^*(f)|$, and the remaining two cases follow immediately. □

To illustrate how the bound improves over the iteration employed in Theorem 1.6.6, consider the difference between the bound on $|Z^*(f)|$ given in part (2) of Theorem 1.6.6 and the degree bound.

$$\begin{aligned}&\frac{q-1}{d} - \ell - \left(\frac{q-1}{d+1} - d^{2i+3}\left(\frac{q-1}{d(d+1)} - (\ell + g^\circ)\right)\right)\\ &= \left(1 + d^{2i+3}\right)\left(\frac{q-1}{d(d+1)} - (\ell + g^\circ)\right) + g^\circ.\end{aligned}$$

In other words, the difference in the degree bound and the iterative bound grows exponentially in the number of iterations.

In Example 5.1.3 and in Example 5.1.9, we saw that the bound in cases (3) and (4) of Theorem 1.6.6 can be tight. The following is an example where the bound in case (1) of Theorem 1.6.6 is tight.

Example 5.2.4. *Let* $p = 379$, $d = 2$, $\ell = \frac{p-7}{4} = 93, g^\circ = 1$, *and* $f(x) = x^{96} + x + 317 \in \mathbb{F}_p[x]$.

Below we give $f_i(x) = x^{\frac{q-1}{d}-\ell_i} + g_i(x)$ *for* $i = 1, 2$*. These are the polynomials formed in the iteration technique introduced in Lemma 5.2.1 and have the property* $|Z^*(f)| \leq |Z^*(f_i)|$*.*

$$f_1(x) = x^{188} - 54x^2 - 255x - 1, \quad f_2(x) = x^6 + 378x^4 + 248x^3 + 55x^2 + 127x + 116.$$

Therefore $|Z^*(f)| \leq |Z^*(f_1)| \leq |Z^*(f_2)| \leq 6$*. Note that we can also bound* $|Z^*(f)|$ *by applying Theorem 1.6.6 which gives* $|Z^*(f)| \leq p - 1 - d^2\ell = 6$*. Indeed, we can verify that* $Z^*(f) = \{21, 37, 89, 303, 322, 365\}$*, so the iterative technique gives a tight bound in this case.*

Chapter 6

Stepanov's method and binomial coefficients

This chapter is based on [127] and Section 5 of [128]. We will improve the trivial upper bound on the clique number for Paley graphs and generalized Paley graphs of prime power order.

Recall we are interested in finding an upper bound for the size of a maximum clique $C = \{a_1, a_2, \ldots, a_N\}$ of the generalized Paley graph $P(q, d)$.

We roughly describe how that *Stepanov's method* works in finding an upper bound on N in the following. We would like to construct a nonzero polynomial f with degree $\deg f = d$, such that each $a_i (i = 1, 2, \cdots, N)$ is a root of multiplicity at least k. Then $Nk \leq d$, so $N \leq d/k$. To get a good upper bound on N, it is preferable that the degree of f is relatively low, and in the meanwhile, each root a_i vanishes with a high multiplicity.

6.1 Extending the idea of Hanson and Petridis

Next we extend the idea of Hanson and Petridis in [53] and give an improvement on the upper bound of $\omega(P(q, d)))$. Theorem 6.1.1 can be regarded as a generalization of Theorem 1.5.1. Note that the original proof of Theorem 1.5.1 by Hanson and Petridis implicitly uses the fact that when p is a prime, the binomial coefficient

$$\binom{\omega\big(P(p,d)\big) - 1 + \frac{p-1}{d}}{\frac{p-1}{d}} \not\equiv 0 \pmod{p}.$$

This condition is crucial to ensure the polynomial we constructed is nonzero. However, this condition no longer holds if we are working on a finite field $\mathbb{F}_q$, and we shall see the main difficulty in extending their method to $\mathbb{F}_q$ is to optimize an upper bound while ensuring the polynomial we are interested in is not identically zero.

Theorem 6.1.1. *If* $q \equiv 1 \pmod{2d}$, *and* $2 \leq n \leq N = \omega\big(P(q,d)\big)$ *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. Consider the following polynomial

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

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

$$\begin{cases} \sum_{i=1}^{n} c_i(-a_i)^j = 0, \quad 0 \le j \le n-2 \\ \\ \sum_{i=1}^{n} c_i(-a_i)^{n-1} = 1 \end{cases} \tag{F}$$

Note the above system of equations has a unique solution since the coefficient matrix of the system is a Vandermonde matrix with parameters $a_1, a_2, \dots a_n$ all distinct. For each $0 \le k \le n-1+\frac{q-1}{d}$, the coefficient of $x^{n-1+\frac{q-1}{d}-k}$ is

$$\sum_{i=1}^{n} \binom{n-1+\frac{q-1}{2}}{k} c_i(-a_i)^k = \binom{n-1+\frac{q-1}{2}}{k} \sum_{i=1}^{n} c_i(-a_i)^k.$$

Now by our construction, the coefficient of $x^{n-1+\frac{q-1}{d}-k}$ is 0 for $k = 0, 1, \dots, n-2$, and the coefficient of $x^{\frac{q-1}{d}}$ is $\binom{n-1+\frac{q-1}{d}}{n-1} = \binom{n-1+\frac{q-1}{d}}{\frac{q-1}{d}} \not\equiv 0 \pmod{p}$, so the degree of f is $\frac{q-1}{d}$.

Note that for each $1 \le j \le N$, we have

$$\begin{aligned} E^{(0)}f(a_j) &= f(a_j) \\ &= \sum_{i=1}^{n} c_i(a_j - a_i)^{n-1+\frac{q-1}{d}} - 1 \\ &= \sum_{i=1}^{n} c_i(a_j - a_i)^{n-1} - 1 \\ &= \sum_{l=0}^{n-1} \binom{n-1}{l} \Big(\sum_{i=1}^{n} c_i(-a_i)^l \Big) a_j^{n-1-l} - 1 \\ &= \sum_{i=1}^{n} c_i(-a_i)^{n-1} - 1 \\ &= 0. \end{aligned}$$

For each $1 \le j \le N$ and $1 \le k \le n-2$, we have

$$\begin{aligned} E^{(k)}f(a_j) &= \binom{n-1+\frac{q-1}{d}}{k} \sum_{i=1}^{n} c_i(a_j - a_i)^{n-1+\frac{q-1}{d}-k} \\ &= \binom{n-1+\frac{q-1}{d}}{k} \sum_{i=1}^{n} c_i(a_j - a_i)^{n-1-k} \\ &= \binom{n-1+\frac{q-1}{d}}{k} \sum_{l=0}^{n-1-k} \binom{n-1-k}{l} \Big(\sum_{i=1}^{n} c_i(-a_i)^l \Big) a_j^{n-1-k-l} \\ &= 0. \end{aligned}$$

For each $n+1 \le j \le N$, we additionally have

$$E^{(n-1)}f(a_j) = \binom{n-1+\frac{q-1}{d}}{n-1}\sum_{i=1}^{n} c_i(a_j-a_i)^{\frac{q-1}{d}} = \binom{n-1+\frac{q-1}{d}}{n-1}\sum_{i=1}^{n} c_i = 0.$$

Now by Lemma 4.1.5, each of $a_1, a_2, \dots a_n$ is a root of f of multiplicity at least $n-1$, and each of $a_{n+1}, a_{n+2}, \dots a_N$ is a root of f of multiplicity at least n. Therefore

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

The following Corollary shows that Theorem 6.4.2 is a generalization of Theorem 1.5.1.

Corollary 6.1.2. *If $q \equiv 1 \pmod{2d}$, and $N = \omega\big(P(q,d)\big)$ satisfies $\binom{N-1+\frac{q-1}{d}}{\frac{q-1}{d}} \not\equiv 0 \pmod{p}$, then $\omega\big(P(q,d)\big) \le \sqrt{\frac{q-1}{d}+\frac{1}{4}}+\frac{1}{2}$. In particular, if $p \equiv 1 \pmod{2d}$, then $\omega\big(P(p,d)\big) \le \sqrt{\frac{p-1}{d}+\frac{1}{4}}+\frac{1}{2}$.*

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 6.4.2 to conclude that $(N-1)N \le \frac{q-1}{d}$, i.e. $N \le \sqrt{\frac{q-1}{d}+\frac{1}{4}}+\frac{1}{2}$. When q is a prime, note that by Lemma 1.3.3, $N = \omega\big(P(p,d)\big) \le \frac{p-1}{d}+1$, then $N-1+\frac{p-1}{d} \le \frac{2(p-1)}{d} \le p-1 < p$ and therefore $\binom{N-1+\frac{p-1}{d}}{\frac{p-1}{d}} \not\equiv 0 \pmod{p}$. $\square$

6.2 Improved upper bounds on $\omega(P_q)$

Corollary 6.2.1. *If $p \equiv 1 \pmod{4}$, then $\omega(P_p) \le \left\lceil \sqrt{\frac{p}{2}} \right\rceil$.*

Proof. Assume $p = 2r^2 + t$, where $1 \le t \le 4r+1$, then $2r^2 < p < 2(r+1)^2$, $\left\lceil \sqrt{\frac{p}{2}} \right\rceil = r+1$. Note

$$2p-1 = 4r^2 + (2t-1) \le 4r^2 + 8r + 1 < (2r+2)^2,$$

so $\sqrt{2p-1} < 2r+2$. Then by Theorem 1.5.1, $\omega(P_p) \le \frac{1}{2}(\sqrt{2p-1}+1) \le r+1+\frac{1}{2}$. Since $\omega(P_p)$ is an integer, we have $\omega(P_p) \le r+1 = \left\lceil \sqrt{\frac{p}{2}} \right\rceil$. $\square$

Theorem 6.2.2. *If $p \equiv 1 \pmod{4}$, then for $q = p^3$, $N = \omega(P_q)$ satisfies $(N-1)(N-\frac{p-1}{2}) \le \frac{q-1}{2}$.*

Proof. Without loss of generality, we may assume $\frac{1}{2}(\sqrt{2q-1}+1) < N < \sqrt{q}$. Suppose the base-$p$ representation of $N-1$ is $N-1 = (A,B)_p$, then $\lfloor\sqrt{\frac{p-1}{2}}\rfloor \le A \le \lfloor\sqrt{p}\rfloor$. Let $n-1 = (A,b)_p$, where $b = \min(\frac{p-1}{2}, B)$, then $n \le N \le n+\frac{p-1}{2}$. Then

$$n-1+\frac{q-1}{2} = (\frac{p-1}{2}, A+\frac{p-1}{2}, b+\frac{p-1}{2})_p,$$

and by Lucas's Theorem,

$$\binom{n-1+\frac{q-1}{2}}{\frac{q-1}{2}} = \binom{\frac{p-1}{2}}{\frac{p-1}{2}}\binom{A+\frac{p-1}{2}}{\frac{p-1}{2}}\binom{b+\frac{p-1}{2}}{\frac{p-1}{2}} \not\equiv 0 \pmod{p}.$$

So by Theorem 6.1.1, $(N-1)(N-\frac{p-1}{2}) \leq (N-1)n \leq \frac{q-1}{2}$. □

Theorem 6.2.3. *If $q = p^{2s+1}, p \equiv 1 \pmod 4$, and $s \geq 2$, then $N = \omega(P_q)$ satisfies $(N-1)(N-\frac{p^s-1}{2}) \leq \frac{q-1}{2}$.*

Proof. Without loss of generality, we may assume $\frac{1}{2}(\sqrt{2q-1}+1) < N < \sqrt{q}$. Suppose the base-$p$ representation of $N-1$ is

$$N-1 = (z_s, z_{s-1}, ..., z_0)_p,$$

then since $p \geq 5$, we have $1 \leq \lfloor\sqrt{\frac{p-1}{2}}\rfloor \leq z_s \leq \lfloor\sqrt{p}\rfloor \leq \frac{p-1}{2}$.

- If $z_{s-1} \leq \frac{p-1}{2}$, let

  $$n-1 = (z_s, z_{s-1}, z'_{s-2}, \cdots, z'_0)_p,$$

  to be the largest number no greater than N such that $z'_j \leq \frac{p-1}{2}$ for each $0 \leq j \leq s-2$. Then $n \leq N \leq n + \frac{1}{2}(p^{s-1}-1)$ and by Lucas's Theorem,

  $$\binom{n-1+\frac{q-1}{2}}{\frac{q-1}{2}} \equiv \binom{z_s+\frac{p-1}{2}}{\frac{p-1}{2}}\binom{z_{s-1}+\frac{p-1}{2}}{\frac{p-1}{2}}\prod_{j=0}^{s-2}\binom{\frac{p-1}{2}+z'_j}{\frac{p-1}{2}} \not\equiv 0 \pmod{p}.$$

- If $z_{s-1} > \frac{p-1}{2}$, let

  $$n-1 = (z_s, \frac{p-1}{2}, \ldots, \frac{p-1}{2})_p,$$

  Then

  $$n \leq N \leq n + p^s - 1 - \frac{p^s-1}{2} = n + \frac{p^s-1}{2},$$

  and by Lucas's Theorem,

  $$\binom{n-1+\frac{q-1}{2}}{\frac{q-1}{2}} \equiv \binom{z_s+\frac{p-1}{2}}{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}}^s \not\equiv 0 \pmod{p}.$$

In both cases, we have $n \leq N \leq n + \frac{p^s-1}{2}$, and $\binom{n-1+\frac{q-1}{2}}{\frac{q-1}{2}} \not\equiv 0 \pmod p$. So by Theorem 6.1.1, we have $(N-1)(N-\frac{p^s-1}{2}) \leq (N-1)n \leq \frac{q-1}{2}$. □

Theorem 6.2.4. *If $q = p^{2s+1}, p \equiv 1 \pmod 4$, and s is a nonnegative integer, then*

$$\omega(P_q) < \sqrt{\frac{q}{2}} + \frac{p^s+1}{4} + \frac{\sqrt{2p}}{32}p^{s-1}.$$

Proof. When $s = 0$, by Theorem 1.5.1, we have

$$\omega(P_p) \leq \frac{\sqrt{2p-1}+1}{2} < \frac{\sqrt{2p}+1}{2} = \sqrt{\frac{p}{2}} + \frac{1}{2} < \sqrt{\frac{p}{2}} + \frac{p^0+1}{4} + \frac{\sqrt{2p}}{32}p^{-1}.$$

When $s \geq 1$, by Theorem 6.2.2 and Theorem 6.2.3, we have

$$\omega(P_q)^2 - \frac{p^s+1}{2}\omega(P_q) \leq \frac{q-p^s}{2},$$

and therefore

$$\begin{aligned}
\omega(P_q) &\leq \frac{p^s+1}{4} + \sqrt{\frac{q-p^s}{2} + (\frac{p^s+1}{4})^2} \\
&= \frac{p^s+1}{4} + \sqrt{\frac{q}{2} + \frac{p^{2s}-6p^s+1}{16}} \\
&< \frac{p^s+1}{4} + \sqrt{\frac{q}{2} + \frac{p^{2s}}{16}} \\
&< \frac{p^s+1}{4} + \sqrt{\frac{q}{2}} + \frac{\sqrt{2p}}{32}p^{s-1}.
\end{aligned}$$

□

Corollary 6.2.5. *If $q = p^{2s+1}, p \equiv 1 \pmod 4$, and $s \geq 1$, then $\omega(P_q) \leq \lceil\sqrt{\frac{p}{2}}\rceil p^s$.*

Proof. Suppose $\omega(P_q) > \lceil\sqrt{\frac{p}{2}}\rceil p^s$. Then by Theorem 6.2.4,

$$\left\lceil\sqrt{\frac{p}{2}}\right\rceil p^s + 1 \leq \omega(P_q) < \sqrt{\frac{q}{2}} + \frac{p^s+1}{4} + \frac{\sqrt{2p}}{32}p^{s-1}.$$

Then if $q = p^3$, we must have $p > 5$, i.e. $p \geq 13$, since for $p = 5$, we have $\omega(P_{125}) = 7 < 2 \cdot 5$. And when $p \geq 13$, we have

$$1 \leq \omega(P_q) - \left\lceil\sqrt{\frac{p}{2}}\right\rceil p \leq 1 + \frac{p+1}{4} + \frac{\sqrt{2p}}{32} < \frac{p-1}{2}.$$

Then as in the proof of Theorem 6.2.2, we have $\omega(P_q)(\omega(P_q)-1) \leq \frac{q-1}{2}$, and hence

$$\omega(P_q) \leq \frac{\sqrt{2q-1}+1}{2} < \sqrt{\frac{q}{2}} + \frac{1}{2} < \left\lceil\sqrt{\frac{p}{2}}\right\rceil p^s + 1,$$

a contradiction.
If $q = p^{2s+1}$ for some $s \geq 2$, then

$$1 \leq \omega(P_q) - \left\lceil\sqrt{\frac{p}{2}}\right\rceil p^s \leq 1 + \frac{p^s+1}{4} + \frac{\sqrt{2p}}{32}p^{s-1} < \frac{p^s-1}{2}.$$

Then as in the proof of Theorem 6.2.3, we have $\omega(P_q)(\omega(P_q)-1) \leq \frac{q-1}{2}$, and hence $\omega(P_q) <$

$\lceil\sqrt{\frac{p}{2}}\rceil p^s + 1$, a contradiction. □

Now we are ready to prove Theorem 1.6.1.

Theorem 1.6.1. *Assume $p \equiv 1 \pmod 4$ and $q = p^{2s+1}$ for some nonneagtive integer s. Then*

$$\omega(P_q) \le \min\left(p^s\left\lceil\sqrt{\frac{p}{2}}\right\rceil, \sqrt{\frac{q}{2}} + \frac{p^s+1}{4} + \frac{\sqrt{2p}}{32}p^{s-1}\right).$$

Proof. By Theorem 1.5.1, 6.2.4, we have

$$\omega(P_q) \le p^s\left\lceil\sqrt{\frac{p}{2}}\right\rceil.$$

And by Corollary 6.2.1, 6.2.5, we have

$$\omega(P_q) \le \sqrt{\frac{q}{2}} + \frac{p^s+1}{4} + \frac{\sqrt{2p}}{32}p^{s-1}.$$ □

6.3 Improved upper bounds on clique number of generalized Paley graphs

In this section, we discuss how to get improved upper bounds on the clique number of generalized Paley graphs over $\mathbb{F}_q$. Recall the trivial upper bound for $\omega\big(P(q,d)\big)$ is $\sqrt{q}$.

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 6.3.1 for the precise statement.

Recall $N = \omega\big(P(q,d)\big)$ and we need to deal with the case when q is a prime power. We can assume $\sqrt{q} \ge N > \sqrt{\frac{q-1}{d} + \frac{1}{4}} + \frac{1}{2}$. In view of Theorem 6.4.2, we need to determine the largest $n \le N$ 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

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

We need to deal with the cases s is odd and s is even separately because $\sqrt{q}$ behaves very differently in both cases. When s is odd, we can mimic the proof of Theorem 3.5 in [127].

Theorem 6.3.1. *If $q = p^{2r+1} \equiv 1 \pmod{2d}$, $d \geq 3, r \geq 1$, and $d \mid (p-1)$, then*

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

Proof. Since $d \geq 3$, we have $p \geq 7$. In view of Lemma 1.3.4, 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 $z_{r-1} + \frac{p-1}{d} > p-1$, let $n-1 = z_r p^r + p^r - 1 - \frac{p^r-1}{d}$, 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 $N - p^r + \frac{p^r-1}{d} \leq n \leq N$ such that $\binom{n-1+\frac{q-1}{d}}{\frac{q-1}{d}} \not\equiv 0 \pmod{p}$. Then by Theorem 6.4.2, 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 6.3.3.

Lemma 6.3.2. *If q is a square, $d \geq 3$ and $d \mid (p-1)$, then $\omega\big(P(q,d)\big) \leq \sqrt{q} - 1$.*

Proof. Let $q = p^{2r}$. In view of Lemma 1.3.4, 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 6.4.2, 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 6.3.3. *If q is a square, $d \geq 3$ and $d \mid (p-1)$, then $\omega\big(P(q,d)\big) < \sqrt{\frac{q}{d}}\big(1 + \frac{1}{2\sqrt{d}} + \frac{1}{8d}\big) + 1$.*

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 6.4.2, 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

$$\begin{aligned}
N &\leq \sqrt{\frac{q+p^r-2}{d} + \frac{1}{4}\left(\frac{p^r-1}{d}+1\right)^2} + \frac{1}{2}\left(\frac{p^r-1}{d}+1\right) \\
&= \sqrt{\frac{q}{d} + \frac{p^{2r}}{4d^2} + p^r\left(\frac{1}{d} + \frac{d-1}{2d^2}\right) + \frac{(d-1)^2}{4d^2} - \frac{2}{d}} + \frac{1}{2}\left(\frac{p^r-1}{d}+1\right) \\
&< \sqrt{\frac{q}{d} + \frac{p^{2r}}{4d^2} + \frac{3p^r}{2d} + \frac{1}{4}} + \frac{1}{2}\left(\frac{p^r-1}{d}+1\right) \\
&< \sqrt{\frac{q}{d}} + \frac{p^r}{8d\sqrt{d}} + \frac{1}{2} + \frac{1}{2}\left(\frac{p^r-1}{d}+1\right) \\
&< \sqrt{\frac{q}{d}}\left(1 + \frac{1}{2\sqrt{d}} + \frac{1}{8d}\right) + 1.
\end{aligned}$$

□

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 $\omega\big(P(q,d)\big)$ using Theorem 6.4.2, 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 6.4.2 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.

Theorem 1.6.2. *Let $q \equiv 1 \pmod 6$. If q is not a square, then $\omega\big(P(q,3)\big) < 0.718\sqrt{q}+1$. If q is a square, then $\omega\big(P(q,3)\big) = \sqrt{q}$ if $3 \mid (\sqrt{q}+1)$ and $\omega\big(P(q,3)\big) < 0.769\sqrt{q}+1$ otherwise.*

Proof. 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 6.3.1, $\omega\big(P(q,3)\big) < \sqrt{\frac{q}{d}}\left(1 + \frac{1}{6p} + \frac{1}{3}\sqrt{\frac{3}{p}}\right) + 1 < 0.718\sqrt{q}+1$. If s is even, then by Theorem 6.3.3, $\omega\big(P(q,3)\big) < 0.769\sqrt{q}+1$.

If $p \equiv 2 \pmod 3$, and s is even, then we can set $s = 2r$. Let $N = \omega\big(P(q,3)\big)$. If r is odd, then $3 \mid (\sqrt{q}+1)$ and thus by Corollary 3.7.2, $N = \sqrt{q}$. 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 $N - \frac{p^r-1}{3} \leq n \leq N$ such that $\binom{n-1+\frac{q-1}{3}}{\frac{q-1}{3}} \not\equiv 0 \pmod p$. Similar to the computation in the proof of Theorem 6.3.3, 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 3.7.4, we see that the clique number of certain cubic Paley graphs is at least $q^{1/3}$. For such generalized Paley graphs, it is an open question to improve the range $[q^{1/3}, 0.769\sqrt{q}+1]$ on the clique number.

6.4 A variant of Theorem 6.1.1

We expect we could use a similar method to get an improved bound on the clique number of a Paley graph P_q.

Conjecture 6.4.1. *There is some constant $c > 0$, such that if $p \equiv 1 \pmod 4$, and $q = p^{2s+1}$ for some positive integer s, then $\omega(P_q) \leq \sqrt{\frac{q}{2}} + cp^{s-1}$.*

Observe that in the proof of Theorem 6.1.1, not every equation of the system (F) is really needed. In fact, some of them will be unnecessary due to the vanishing binomial coefficients (recall we are working on a field with characteristic p). For $n \in \mathbb{N}$, let $L(n)$ denote the set of the integers l such that $0 \leq l \leq n-1$ and there exists a k such that $0 \leq k \leq n-1$, and

$$\binom{n-1+\frac{q-1}{2}}{k}\binom{n-1-k}{l} \not\equiv 0 \pmod p.$$

It turns out that only the rows with indices in the set $L(n)$ are needed, and we are able to generalize Theorem 6.1.1 by introducing a new parameter m in the following:

Theorem 6.4.2. *Suppose $q = p^{2s+1}, p \equiv 1 \pmod 4$, $n \leq N = \omega(P_q)$, $\frac{q-1}{2} \geq m > n$ and $\binom{n-1+\frac{q-1}{2}}{m} \not\equiv 0 \pmod p$. If $D = \{d_1, d_2, \ldots, d_n\}$ is a n-subset of C such that the following system of equations*

$$\begin{cases} \sum_{i=1}^{n} c_i(-d_i)^l = 0, \quad \forall l \in L(n) \\ \\ \sum_{i=1}^{n} c_i(-d_i)^m = 1 \end{cases} \tag{$E_{n,m,D}$}$$

has a solution $c_1, c_2, ..., c_n$, then $n(N-2) \leq \frac{q-3}{2}$.

Proof. Consider the polynomial

$$f(x) = \sum_{i=1}^{n} c_i(x-d_i)^{n-1+\frac{q-1}{2}}.$$

Note that f is a nonzero polynomial since the coefficient of $x^{n-1+\frac{q-1}{2}-m}$ is

$$\binom{n-1+\frac{q-1}{2}}{m}\sum_{i=1}^{n} c_i(-d_i)^m = \binom{n-1+\frac{q-1}{2}}{m} \not\equiv 0 \pmod p,$$

and we have $\deg f \leq n-1+\frac{q-1}{2}$.

For each $0 \le k \le n-2$ and $1 \le j \le N$, we have

$$\begin{aligned} E^{(k)} f(a_j) &= \binom{n-1+\frac{q-1}{2}}{k} \sum_{i=1}^{n} c_i (a_j - d_i)^{n-1+\frac{q-1}{2}-k} \\ &= \binom{n-1+\frac{q-1}{2}}{k} \sum_{i=1}^{n} c_i (a_j - d_i)^{n-1-k} \\ &= \binom{n-1+\frac{q-1}{2}}{k} \sum_{l=0}^{n-1-k} \binom{n-1-k}{l} \Big(\sum_{i=1}^{n} c_i (-d_i)^l \Big) a_j^{n-1-k-l}. \end{aligned}$$

If $\binom{n-1+\frac{q-1}{2}}{k} \not\equiv 0 \pmod{p}$, then for each $0 \le l \le n-1-k \le n-1$ such that $\binom{n-1-k}{l} \not\equiv 0 \pmod{p}$, we have $l \in L(n)$ and $\sum_{i=1}^{n} c_i (-d_i)^l = 0$. So we have $E^{(k)} f(a_j) = 0$.

Note that $0 \in L(n)$, so for each $a_j \notin D$, we additionally have

$$E^{(n-1)} f(a_j) = \binom{n-1+\frac{q-1}{2}}{n-1} \sum_{i=1}^{n} c_i (a_j - d_i)^{\frac{q-1}{2}} = \binom{n-1+\frac{q-1}{2}}{n-1} \sum_{i=1}^{n} d_i = 0.$$

Now by Lemma 4.1.5, each $a_j \in D$ is a root of f of multiplicity at least $n-1$, and each $a_j \notin D$ is a root of f of multiplicity at least n. Therefore

$$(n-1)n + n(N-n) = nN - n \le n - 1 + \frac{q-1}{2},$$

i.e. $n(N-2) \le \frac{q-3}{2}$. □

Remark 6.4.3. *We do need the assumption that $m \le \frac{q-1}{2}$, otherwise it is possible that $0 < m' = m - \frac{q-1}{2} \in L(n)$, then $\sum_{i=1}^{n} c_i (-d_i)^{m'} = 0$ will imply that $\sum_{i=1}^{n} c_i (-d_i)^m = 0$ as each d_i is a quadratic residue.*

Consider the $(|L(n)|+1) \times N$ matrix

$$A_{m,n} := \big((-a_i)^l \big)_{1 \le i \le N, l \in L(n) \cup \{m\}}.$$

Note that the coefficient matrix of the system $(E_{n,m,D})$ is a submatrix of $A_{m,n}$.

Lemma 6.4.4. *If $n \le N$ and $n - 1 \equiv \frac{p+1}{2} \pmod{p}$, then $|L(n)| < n$.*

Proof. Since $n-1 \equiv \frac{p+1}{2} \pmod{p}$, we have $p \mid n-1+\frac{q-1}{2}$. If $l \in L(n)$, then there exists k such that $0 \le k \le n-1$ and $\binom{n-1+\frac{q-1}{2}}{k}\binom{n-1-k}{l} \not\equiv 0 \pmod{p}$. Now by Lucas's Theorem, we must have $p \mid k$ and $n-1-k \equiv \frac{p+1}{2} \pmod{p}$. Since $\binom{n-1-k}{l} \not\equiv 0 \pmod{p}$, by Lucas's Theorem, $l \equiv 0, 1, \ldots \frac{p+1}{2} \pmod{p}$. Then in particular, $\frac{p+3}{2} \notin L(n)$, and $|L(n)| < n$. □

Lemma 6.4.5. *Suppose $n \le N = \omega(P_q)$ be such that $n - 1 \equiv \frac{p+1}{2} \pmod{p}$, and $\frac{q-1}{2} \ge m \ge n$ be such that $\binom{n-1+\frac{q-1}{2}}{m} \not\equiv 0 \pmod{p}$. Suppose further that for any n-subset D of C, the above system*

of equations $(E_{n,m,D})$ has no solution. Then the last row of $A_{m,n}$ is a linear combination of the first $|L(n)|$ rows.

Proof. Note that by Lemma 6.4.4, $|L(n)|+1 \le n \le N$. If $A = A_{m,n}$ has full rank, which equals to $|L(n)|+1$, then A has an invertible $(|L(n)|+1)\times(|L(n)|+1)$ sub-matrix, which columns correspond to a $(|L(n)|+1)$-subset F of C. Then for any n-subset D of C containing F, the coefficient matrix of $(E_{n,m,D})$ in Theorem 6.4.2 has full rank, and thus the system has a solution. So by our assumption, A does not have full rank, which means the rows of A are linearly dependent. Note that the first $|L(n)|$ rows of A (i.e. those rows with $l \in L(n)$) form a sub-matrix of the Vandermonde matrix $\left((-a_i)^j\right)_{1\le i\le N, 0\le j\le N-1}$, so the first $|L(n)|$ rows are linearly independent. Therefore, the last row of A is a linear combination of the first $|L(n)|$ rows. □

We focus on the case $s \ge 2$. In view of the proof of Theorem 6.2.3, we see if $z_{s-1} < \frac{p-1}{2}$, we can get $N \le \frac{1}{2}(\sqrt{2q-1}+1) + p^{s-1}$, which is a good upper bound. In the case $z_{s-1} = \frac{p-1}{2}$, we could instead let

$$n-1 = (z_s, z_{s-1}-1, \frac{p-1}{2}, \ldots, \frac{p-1}{2})_p,$$

to get the improved upper bound $N \le \frac{1}{2}(\sqrt{2q-1}+1) + 2p^{s-1}$. Therefore, we see that the case $z_{s-1} \le \frac{p-1}{2}$ is consistent with Conjecture 6.4.1. In the following discussion, we will focus on the case $z_{s-1} > \frac{p+1}{2}$. We assume

$$n-1 = (z_s, z_{s-1}, \frac{p-1}{2}, \ldots, \frac{p-1}{2}, \frac{p+1}{2})_p,$$

is the largest number of this form no greater than $N-1$, then

$$n-1+\frac{q-1}{2} = (\frac{p-1}{2}, \ldots, \frac{p-1}{2}, z'_s, z'_{s-1}, 0, \ldots, 0)_p,$$

where $z'_s = z_s + \frac{p+1}{2}, z'_{s-1} = z_{s-1} - \frac{p-1}{2}$, and we have $n \le N < n + p^{s-1}$.

Let M denote the set of all possible integers m such that

$$\binom{n-1+\frac{q-1}{2}}{m} \not\equiv 0 \pmod p, \text{ and } n \le m \le \frac{q-1}{2}.$$

Using Lucas's Theorem, it is easy to verify that

$$M = \{m = (c_{2s}, \ldots, c_s, c_{s-1}, \ldots, 0)_p \ge n : c_j \le \frac{p-1}{2} \text{ for } s \le j \le 2s, \text{ and } c_{s-1} \le z'_{s-1}\}.$$

We can also determine the structure of the set $L(n)$:

Lemma 6.4.6. *If $l = (l_s, l_{s-1}, \ldots, l_0)_p \in L(n)$, then $0 \le l_0 \le \frac{p+1}{2}$ and $0 \le l_j \le \frac{p-1}{2}$ for each $1 \le j \le s-2$.*

Proof. If $l = (l_s, l_{s-1}, \ldots, l_0)_p \in L(n)$, then there exists $0 \le k \le n-1$ such that $\binom{n-1+\frac{q-1}{2}}{k} \not\equiv 0 \pmod p$ and $\binom{n-1-k}{l} \not\equiv 0 \pmod p$. Note that $p^{s-1} \mid n-1+\frac{q-1}{2}$, then by Lucas's Theorem, we

must have $p^{s-1} \mid k$. So

$$n-1-k \equiv n-1 \equiv \left(\frac{p-1}{2}, \ldots, \frac{p-1}{2}, \frac{p+1}{2}\right)_p \pmod{p^{s-1}}.$$

Since $\binom{n-1-k}{l} \not\equiv 0 \pmod{p}$, then we need

$$\binom{(\frac{p-1}{2}, \ldots, \frac{p-1}{2}, \frac{p+1}{2})_p}{(l_{s-2}, \ldots, l_0)_p} = \binom{\frac{p+1}{2}}{l_0} \prod_{j=1}^{s-2} \binom{\frac{p-1}{2}}{l_j} \not\equiv 0 \pmod{p}.$$

Therefore, $0 \le l_0 \le \frac{p+1}{2}$ and $0 \le l_j \le \frac{p-1}{2}$ for each $1 \le j \le s-2$. □

Conjecture 6.4.1 could be proved if we showed the existence of an $m \in M$ with the following properties:

Conjecture 6.4.7. *There is an integer $m \in M$ such that and the last row is linearly independent with the first $|L(n)|$ rows in the matrix $A_{m,n}$.*

Theorem 6.4.8. *Conjecture 6.4.7 implies Conjecture 6.4.1.*

Proof. Let $m \in M$ be such that the last row is linearly independent with the first $|L(n)|$ rows in the matrix $A_{m,n}$. Then in view of the proof of Lemma 6.4.5, there exists a n-subset D of C such that the system $(E_{n,m,D})$ has a solution. Since $n \le m \le \frac{q-1}{2}, \binom{n-1+\frac{q-1}{2}}{m} \not\equiv 0 \pmod{p}$, by Theorem 6.4.2, we have $n(N-2) \le \frac{q-3}{2}$. By the construction of n, we have $n \le N < n + p^{s-1}$. Then we get $(N - p^{s-1})(N-2) \le \frac{q-3}{2}$, and therefore

$$\begin{aligned} N &\le \frac{p^{s-1}+2}{2} + \sqrt{\frac{q-3}{2} - 2p^{s-1} + \left(\frac{p^{s-1}+2}{2}\right)^2} \\ &\le \frac{p^{s-1}+2}{2} + \sqrt{\frac{q-1}{2} + \frac{p^{2s-2}}{4}} \\ &\le \frac{p^{s-1}+2}{2} + \sqrt{\frac{q}{2}} + \frac{p^{2s-2}}{8\sqrt{\frac{q}{2}}} \\ &< \sqrt{\frac{q}{2}} + \frac{12+\sqrt{2}}{8} p^{s-1}. \end{aligned}$$

□

We remark that Conjecture 6.4.7 is closely related to the singularity of generalized Vandermonde matrices, which we have discussed in Section 4.5. However, the result described in Section 4.5 is not strong enough to prove Conjecture 6.4.7.

Chapter 7

Directions determined by a Cartesian product in an affine Galois plane

This chapter is rewritten from Sections 2 to 4 in [128].

In Section 1.5, we discussed the direction set D determined by a point set U in an affine Galois plane. 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

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

Estimating the size of the set of D determined by certain Cartesian products (in particular $A \times A$) turns out to be useful in sum-product estimates over finite fields; see [92, 100, 106] for more details and examples. In this chapter, we focus on improving the lower bound on $|D|$.

Note that if $m = 1$ or $n = 1$, the direction set D is trivial. And 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 $b_n = 0$.

We restate the main result in [9] for readers' convenience.

Theorem 1.4.4. *Let $A, B \subset \mathbb{F}_p$ be sets each of size at least 2 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.*

We point out that Rédei polynomial with Szőnyi's extension is the main tool to prove the above theorem, as well as the theorems listed in Section 1.5. Another key idea is to study the properties of lacunary polynomials. In Section 6.1, we will describe these tools.

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

Lemma 7.0.1 (Lemma 6 of [9])**.** *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. 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 7.0.1. In Section 7.3, we first prove Lemma 7.3.1 and then apply that to prove theorem 1.6.4. The symmetric polynomials $f_{m,t}(b_1, b_2, \ldots, b_{n-1}, 0)$ in the statement of Theorem 1.6.4 will be defined via recurrence relations in Section 7.1, and we will give an explicit formula for $f_{m,t}$ in Section 7.2. Theorem 1.6.4 is central in proving our main results, Theorem 1.6.5 and Theorem 1.6.3.

In Corollary 7.3.2, which is a corollary of Theorem 1.6.4, it will be made precise that Theorem 1.6.4 is indeed a generalization of Theorem 1.4.4. To apply Theorem 1.6.4, 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 7.4. In view of Corollary 7.2.5, which gives the explicit formula for $f_{m,k}$, we will apply Lucas's Theorem. 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 [43].

7.1 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.

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 [115]) extended Rédei polynomial by introducing the polynomial $F(x,y) = (x^q - x)/H(x,y)$, where

$$F(x,y) = x^k - \sigma_1(\mathbb{F}_q \setminus A_y) x^{k-1} + \sigma_2(\mathbb{F}_q \setminus A_y) x^{k-2} + \cdots + (-1)^m \sigma_k(\mathbb{F}_q \setminus A_y). \tag{7.1}$$

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 [115] 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 $\sigma_t(\mathbb{F}_q \setminus A_y)$:

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

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

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 (7.1). Let

$$H(x, y)F(x, y) = x^q + h_1(y)x^{q-1} + h_2(y)x^{q-2} + \cdots + h_q(y), \tag{7.2}$$

and let $c_i = h_i(0)$ for each $1 \leq i \leq q$. then $\deg(h_i) \leq i$. 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 [9]. Here we include the proof for the sake of completeness.

Lemma 7.1.1. *If $c_i \neq 0$ for some $1 \leq i \leq q$, then $|D| \geq q + 1 - i$.*

Proof. By the definition of the symmetric polynomials $\sigma_t(A_y)$ and $\sigma_t(\mathbb{F}_q \setminus A_y)$, we have $\deg(h_i) \leq i$. 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 $1 \leq i \leq q$, then $|D| \geq q + 1 - i$. We proceed by setting $y = 0$ in equation (7.2):

$$H(x, 0)F(x, 0) = F(x, 0)\prod_{j=1}^{n}(x - b_j)^m = x^q + c_1x^{q-1} + c_2x^{q-2} + \cdots + c_q. \tag{7.3}$$

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

In [9], Lemma 7.0.1 and Lemma 7.1.1 are combined to prove Theorem 1.4.4. As we pointed out in the introduction section, Lemma 7.0.1 is not strong enough for the application in $AG(2, q)$.

7.2 Explicit formulas of polynomials $\sigma_t(\mathbb{F}_q \setminus A_y)$

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 $\{b_j : 1 \leq i \leq m, 1 \leq j \leq n\} = \cup_{j=1}^{n}\{b_j, b_j, \ldots, b_j\}$, where each b_j appears m times. Next we revisit the the recurrence relation defined above. For

example, when $t = 1, 2$, we have

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

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

Lemma 7.2.1. *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 the statement is true for $t < l$, where $l \ge 2$, 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 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 7.2.2. *$\sigma_t\big(\mathbb{F}_q \setminus A_0(B)\big)$ 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. And by Lemma 7.2.1, 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. And 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 7.2.3. *If $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0)$ is the zero polynomial, then $t \geq n$, and*

$$f_{m,t}(r_1, r_2, \cdots, r_{n-1}, r_n) = r_1 r_2 \cdots r_n g(r_1, r_2, \ldots, r_{n-1}, r_n),$$

where g is a homogeneous symmetric polynomial with degree $t - n$.

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 $\sigma_t\big(\mathbb{F}_q \setminus A_0(B)\big)$, or $f_{m,t}(b_1, b_2, \ldots, b_{n-1}, b_n)$.

Theorem 7.2.4. *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

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

And for $t = 1$, the statement is true since

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

Suppose 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

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

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

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

Proof. This follows immediately from Theorem 7.2.4 and

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

Next, we use Schwartz–Zippel Lemma to bound the number of roots (with distinct coordinates) of $f_{m,t}(r_1,r_2,\ldots,r_{n-1},0)$.

Proposition 7.2.6. *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 Lemma 4.2.2, 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 $(r_1,r_2,\ldots,r_{n-1})\in S^{n-1}$ such that $f_{m,t}(r_1,r_2,\ldots,r_{n-1},0)=0$ 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

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

7.3 Proof of Theorem 1.6.4

In this section, we will prove Theorem 1.6.4, and give some corollaries. We begin by giving a stronger version of Lemma 7.0.1.

Lemma 7.3.1. *Let $q = p^s$ to 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, $m, n \geq 2$, $k = q - mn > 0$, $\deg R = n - 1$, and $\deg S = k - l$ for some integer $0 \leq l \leq k$. If 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

$$R^m(x)S(x) = 1 + x^{\deg R + \deg S + 1}P(x). \tag{7.4}$$

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

$$R^{m+r}(x)T(x) = 1 + x^{\deg R + \deg S + 1}P(x) = 1 + x^{n+k-l}P(x). \tag{7.5}$$

By differentiating (7.5), 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 $R(x) \mid (m + r)T(x)$. And since R does not divide T, we must have $m + r = 0$ in $\mathbb{F}_q$, i.e. $p \mid (m + r)$. Note that $m \leq m + r \leq m + \lfloor \frac{k-l}{n-1} \rfloor$, 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 or r is difficult to compute without knowing the explicit factorizations of polynomials R and S, which is indeed the case in our application.

Lemma 7.1.1, Lemma 7.3.1 can be combined to prove Theorem 1.6.4.

Theorem 1.6.4. *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 $mn - n + l + 2$.

Proof. We will consider equation (7.1) and (7.3). 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 $f_{m,0}(b_1, b_2, \ldots, b_{n-1}, 0) = 1$, and 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 $x = y^{-1}$ in and multiply by y^q in (7.3) to obtain

$$R^m(y)S(y) = 1 + c_1 y + c_2 y^2 + \cdots + c_q y^q = 1 + y^{k+n-l} U(y), \tag{7.6}$$

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 (7.6) is impossible to hold in view of Lemma 7.3.1. It follows that at least one of $c_1, \ldots, c_{k+n-l-1}$ is nonzero, and thus by Lemma 7.1.1, 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 1.4.4.

Corollary 7.3.2. *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 1.6.4, 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 7.3.3. *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 1.6.4, the number of directions is at least $mn - n + 2$. □

Corollary 7.3.4. *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. Suppose l is the smallest non-negative integer such that $f_{m,k-l}(b_1, b_2, \ldots, b_{n-1}, 0) \neq 0$. 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 1.6.4 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. □

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

To apply Theorem 1.6.4, it is crucial to understand when is $f_{m,k}(b_1, b_2, \ldots, b_{n-1}, 0) = 0$. In particular, one need to identify whether $f_{m,k}(r_1, r_2, \ldots, r_{n-1}, 0) \equiv 0$. Recall Corollary 7.2.3 says that $f_{m,k}(r_1, r_2, \ldots, r_{n-1}, 0) \equiv 0$ could happen only when $k \geq n$.

In general, we can use 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 [108]). However, since we have worked out the explicit formula in Corollary 7.2.5, 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 7.4.1. *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 exists $b_0, b_1, \ldots, b_k$ 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 7.4.2. *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 7.2.5, $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0)$ is not the zero polynomial if and only if there exist $t_1, t_2, \ldots, t_{n-1} \geq 0$ such that

$$\sum_{i=1}^{n-1} t_i = t, \prod_{i=1}^{n-1} \binom{m-1+t_i}{m-1} \not\equiv 0 \pmod{p}. \tag{7.7}$$

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 $0 \leq j \leq s-1$, the S_j computed in the above algorithm is exactly the maximum value of R_j provided $T_k \leq (n-1)(p-1-m_k)$ for each $0 \leq k \leq j$ 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 (7.7) holds for $t_1, t_2, \ldots, t_{n-1}$, then $T_j \leq (n-1)(p-1-m_j)$, and $S_j \geq R_j = h_j$ for each $0 \leq j \leq s-1$. Therefore, if $S_j < h_j$ for some $0 \leq j \leq s-1$, 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 $S_j \geq h_j$ for each $0 \leq j \leq s-1$. Furthermore, there are $T_0, T_1, \ldots, T_{s-1}$ (which are maximized) such that $0 \leq T_j \leq (n-1)(p-1-m_j)$ 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 $S_s = \lfloor \frac{S_{s-1} - h_{s-1}}{p} \rfloor \geq 0$ given in the Algorithm 1. Since $S_s \geq 0$, by Lemma 7.4.1, there exist $T'_0, T'_1, \ldots, T'_{s-1}$ such that $0 \leq T'_j \leq T_j$, 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 $0 \leq t_i < q$ and (7.7) 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 7.4.3. *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 $m_j \neq p-1$ for each $0 \leq j \leq s-1$, and $n-1 \geq \max\{h_j : 0 \leq j \leq s-1\}$, then $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0)$ is a nonzero polynomial.*

Proof. For each $0 \leq j \leq s-1$, since $m_j \neq p-1$, we have $S_j \geq (n-1)(p-1-m_j) \geq n-1 \geq h_j$. Then by Proposition 7.4.2, $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0)$ is a nonzero polynomial. □

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

Corollary 7.4.4. *If $n \geq p$ 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 7.4.5. *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

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

□

We will use a combination of Corollary 7.4.4 and Lemma 7.4.5 to prove Theorem 7.5.3.

7.5 Proof of Theorem 1.6.5

In this section, we will prove Theorem 1.6.5. 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 7.2.3), then by combining Theorem 1.6.4 and Proposition 7.2.6, we have the following estimate on the probability.

Theorem 7.5.1. *Let $q = p^s$ be a prime power. Let $m, n \geq 2$ 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*

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

If $f_{m,k}(r_1, r_2, \ldots, r_{n-1}, 0)$ is indeed the zero polynomial, then in view of Theorem 1.6.4, 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 7.2.3 states that $f_{m,t}(r_1, r_2, \ldots, r_{n-1}, 0) \equiv 0$ could happen only when $t \geq n$, 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 1.6.4 and Proposition 7.2.6 with $t = k - l$, we obtain the following theorem.

Theorem 7.5.2. *Let $q = p^s$ be a prime power. Let $m, n \geq 2$ 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*

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

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 7.4.4 and Lemma 7.4.5. Note that reducing m corresponds to discarding some elements from A, which only decreases the number of directions determined.

Theorem 7.5.3. *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 7.4.5, 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 7.4.4, 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 7.5.1, 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 the exact value of l, then we can combine Theorem 7.5.2 and Theorem 7.5.3 to get the following slightly weaker version.

Theorem 1.6.5. *Let $p \geq 3$ and $q = p^s$ be a prime power. Suppose $m \geq n \geq p$ 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*

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

Chapter 8

Equidistribution and exponential sum over primes

In this chapter, we will discuss some classical estimates on exponential sum over primes using tools from analytic number theory. Our goal will be outlining the proof of Theorem 8.6.4, an equidistribution result involving prime powers. Readers can refer to [71], [57] and [84] for further discussion on this topic. At the end of this chapter, we will use this equidistribution result to prove an improved upper bound on the clique number for almost all generalized Paley graphs with non-square order.

The following notation will be used throughout this chapter.

1. Let $\mathcal{P}$ be the set of primes (with the natural order).
2. $e(x) = \exp(2\pi i x)$.
3. $X \asymp Y$ means $C_1 X \leq Y \leq C_2 X$ for some positive constants C_1 and C_2.
4. $X \ll Y$ means $|X| \leq CY$ for some positive constant C.
5. $f(x) \lll A$ means that for any $\epsilon > 0$, there is a positive constant $C(\epsilon)$ such that $|f(x)| \leq C(\epsilon) A x^{\epsilon}$ holds for all sufficiently large x.
6. We denote the circle group $\mathbb{T} = \mathbb{R}/\mathbb{Z}$.
7. For $\alpha \in \mathbb{R}$, $\|\alpha\|$ denotes the distance from α to the nearest integer.
8. For each function f and each integer h, we denote $f_h(x) = f(x+h) - f(x)$ to be the difference function of f with step h.
9. The interval $I = (a, b]$ for some integers $a < b$. For any integer h, we denote
$$I_h = (\max\{a, a-h\}, \min\{b, b-h\}).$$
10. μ is the Möbius function.
11. Λ is the von Mangoldt function, defined as
$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some prime } p \text{ and integer } k \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

12. $\mathbb{1}_{\mathcal{P}}$ denotes the characteristic function on the set of primes $\mathcal{P}$.

13. $\psi(x) = \sum_{n \le x} \Lambda(n)$, and $\theta(x) = \sum_{p \le x} \log p = \sum_{n \le x} \mathbb{1}_{\mathcal{P}}(n) \log n$.

14. For $s \in \mathbb{N}$, the s-fold divisor function is defined as

$$d_s(n) = \sum_{\substack{n_1 \cdots n_s = n \\ n_1, n_2, \ldots, n_s \in \mathbb{N}}} 1.$$

8.1 Weyl's criterion

Equidistribution theory started with Weyl's seminal paper [123].

Definition 8.1.1. *A sequence $\{x_n : n \in \mathbb{N}\} \subset \mathbb{R}$ 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 $Z(n,\alpha) = \#\{x_j : 1 \le j \le n, x_j - \lfloor x_j \rfloor \le \alpha\}$.*

The following lemma is straightforward to prove using the definition. It roughly says that the equidistributed property is translation-invariant in the limiting sense.

Lemma 8.1.2 (Theorem 1.1.2 in [71])**.** *If the sequence $\{y_n : n \in \mathbb{N}\}$ is equidistributed, and $\lim_{n\to\infty}(x_n - y_n)$ exists, then the sequence $\{x_n : n \in \mathbb{N}\}$ is equidistributed.*

The characterization of equidistributed sequences is given by the following well-known criterion.

Lemma 8.1.3 (Weyl's criterion)**.** *A sequence $\{y_n\}$ is equidistributed if and only if for any integer $t \neq 0$, $\sum_{n \le x} e(ty_n) = o(x)$ as $x \to \infty$.*

Given a nice smooth function $f : \mathbb{R}^+ \to \mathbb{C}$, we can check whether $\{f(n) : n \in \mathbb{N}\}$ is equidistributed by estimating $\sum_{n \le x} e\big(kf(n)\big)$. The functions f we are most interested in are polynomial-like functions (which are not polynomials over $\mathbb{Q}$), which means the derivatives $f^{(k)}(x)$ behave like $f(x)x^{-k}$.

For example, if $f(x) = \alpha x$, where α is an irrational number, then then it is easy to directly verify that $\{\alpha n : n \in \mathbb{N}\}$ is equidistributed. We can also use Weyl's criertion as $\sum_{n \le x} e(ka_n)$ is just a geometric series.

Another example is $f(x) = \sqrt{x}$. Again we can verify that $\{\sqrt{n} : n \in \mathbb{N}\}$ is equidistributed directly. We can also apply the following theorem, which is a consequence of Weyl's criterion.

Theorem 8.1.4 (Fejér's Theorem, Theorem 1.2.5 in [71])**.** *If $\Delta f(n) = f(n+1) - f(n)$ is monotone as n increases, $\lim_{n\to\infty} \Delta f(n) = 0$ and $\lim_{n\to\infty} n|\Delta f(n)| = \infty$, then $\{f(n) : n \in \mathbb{N}\}$ is equidistributed. In particular, for any $\beta \in (0,1)$ and $\gamma \in \mathbb{R}$, $\{n^\beta (\log n)^\gamma : n \in \mathbb{N}\}$ is equidistributed.*

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 Section 1.6 of [71]).

8.2 Exponential sum over primes

An interesting question is whether the same result holds if we restrict the indices to be prime. For example, we can ask the question for the sequences $\{\alpha n\}$ and $\{\sqrt{n}\}$. More precisely, for an irrational number α, is $\{\alpha p : p \in \mathcal{P}\}$ equidistributed? And is $\{\sqrt{p} : p \in \mathcal{P}\}$ equidistributed? It turns out the answers to both questions are positive.

By Weyl's criterion and the prime number theorem, , our goal is to show

$$\sum_{p\le x} e\big(kf(p)\big) = o\big(\pi(x)\big) = o(x/\log x), \text{ as } x\to\infty. \tag{8.1}$$

Instead of showing this directly, it is standard to establish the following estimate:

$$\sum_{n\le x} e\big(kf(n)\big)\Lambda(n) = o(x), \text{ as } x\to\infty. \tag{8.2}$$

Lemma 8.2.1. *Equation* (8.2) *implies equation* (8.1).

Proof. We first show that the contribution of prime powers in equation (8.2) is small. By equation (8.1) and the fact $\psi(x) = \theta(x) + O(\sqrt{x})$,

$$\begin{aligned}\Big|\sum_{p\le x} e\big(kf(p)\big)\log p\Big| &= \Big|\sum_{n\le x} e\big(kf(n)\big)\mathbb{1}_{\mathcal{P}}(n)\log n\Big| \\ &\le \Big|\sum_{n\le x} e\big(kf(n)\big)\Lambda(n)\Big| + \sum_{n\le x}\Big|e\big(kf(n)\big)\Big|\big(\Lambda(n) - \mathbb{1}_{\mathcal{P}}(n)\log n\big) \\ &= o(x) + \big(\psi(x) - \theta(x)\big) = o(x) + O(\sqrt{x}) = o(x).\end{aligned}$$

Let $A(x) = \sum_{p\le x} e\big(kf(p)\big)\log p$. Next we apply partial summation to get

$$\sum_{p\le x} e\big(kf(p)\big) = \int_{2^-}^{x} \frac{1}{\log u} dA(u) = \frac{A(u)}{\log u}\Big|_{2^-}^{x} + \int_2^x \frac{A(u)}{u\log^2 u} du = o\Big(\frac{x}{\log x}\Big) + o\Big(\int_2^x \frac{1}{\log^2 u} du\Big).$$

Note that

$$\int_2^x \frac{1}{\log^2 u} du \ll \sqrt{x} + \int_{\sqrt{x}}^x \frac{1}{\log^2 u} du \ll \sqrt{x} + \frac{x}{\log^2 x} \ll \frac{x}{\log^2 x}.$$

Hence $\sum_{p\le x} e\big(kf(p)\big) = o\big(\pi(x)\big) = o(x/\log x)$ as $x\to\infty$, and so equation (8.1) holds. □

Corollary 8.2.2. *If equation* (8.2) *holds for a function* $f(x)$*, then the sequence* $\{f(p) : p \in \mathcal{P}\}$ *is equdistributed.*

To estimate the exponential sum of the above form, it is standard to use Weyl's method, Vinogradov's method, van der Corput's method, and Vaughan's identity (see for example [42], Chapters 8 and 13 in [57], and Chapters 2 to 4 in [84]). We first discuss Vaughan's identity, which is a useful decomposition of the von Mangoldt function Λ.

Lemma 8.2.3 (Vaughan's identity)**.** *For any $y, z \geq 1$,*

$$\Lambda(n) = \sum_{\substack{b|n \\ b\leq y}} \mu(b)\log\frac{n}{b} - \sum_{\substack{bc|n \\ b\leq y, c\leq z}} \mu(b)\Lambda(c) + \sum_{\substack{bc|n \\ b>y, c>z}} \mu(b)\Lambda(c) + R(n),$$

where $R(n) = 0$ when $n > z$, and $R(n) = \Lambda(n)$ when $n \leq z$.

Proof. Since $\log = 1 * \Lambda$, $\Lambda = \mu * \log$ follows from the Möbius inversion formula. Therefore,

$$\begin{aligned}
\Lambda(n) &= \sum_{b|n} \mu(b)\log\frac{n}{b} \\
&= \sum_{\substack{b|n \\ b\leq y}} \mu(b)\log\frac{n}{b} + \sum_{\substack{b|n \\ b>y}} \mu(b)\Big(\sum_{bc|n}\Lambda(c)\Big) \\
&= \sum_{\substack{b|n \\ b\leq y}} \mu(b)\log\frac{n}{b} + \sum_{\substack{bc|n \\ b>y, c>z}} \mu(b)\Lambda(c) + \sum_{\substack{bc|n \\ b>y, c\leq z}} \mu(b)\Lambda(c) \\
&= \sum_{\substack{b|n \\ b\leq y}} \mu(b)\log\frac{n}{b} + \sum_{\substack{bc|n \\ b>y, c>z}} \mu(b)\Lambda(c) + \sum_{\substack{c|n \\ c\leq z}} \Lambda(c)\Big(\sum_{bc|n}\mu(b) - \sum_{\substack{bc|n \\ b<y}}\mu(b)\Big) \\
&= \sum_{\substack{b|n \\ b\leq y}} \mu(b)\log\frac{n}{b} - \sum_{\substack{bc|n \\ b\leq y, c\leq z}} \mu(b)\Lambda(c) + \sum_{\substack{bc|n \\ b>y, c>z}} \mu(b)\Lambda(c) + \sum_{\substack{c|n \\ c\leq z}} \Lambda(c)J(n/c),
\end{aligned}$$

where $J(1) = 0$ and $J(x) = 0$ otherwise. When $n > z$, $\sum_{c|n, c\leq z}\Lambda(c)J(n/c) = 0$; while when $n \leq z$, $\sum_{c|n, c\leq z}\Lambda(c)J(n/c) = \Lambda(n)$. □

8.3 Equidistribution of polynomial sequences

In [123], Weyl proved the following equidistribution result for polynomials.

Theorem 8.3.1 (Weyl equidistribution theorem for polynomials)**.** *Let P be a nonconstant polynomial. The sequence $\{P(n) : n \in \mathbb{N}\}$ is equidistributed if and only if at least one of the coefficients of P, other than the constant term, is irrational.*

One direction should be clear: if all coefficients (other than the constant term) of P are rational, then $P(n)$ is an integer for a positive proportion of n , so the sequence $\{P(n) : n \in \mathbb{N}\}$ is not equidistributed. For the other direction, the idea is to estimate the exponential sum and apply Weyl's criterion. We will estimate sums of the form $S = \sum_{n=1}^{N} e\big(P(n)\big)$, where P is a polynomial with real coefficients. Such a sum is called a Weyl sum. We begin with the simplest case that P is linear.

Lemma 8.3.2. *Let $\alpha, \beta \in \mathbb{R}$. Then for all $N \in \mathbb{N}$,*

$$\left|\sum_{n=1}^{N} e(\alpha n + \beta)\right| \le \min\left\{N, \frac{1}{2\|\alpha\|}\right\}.$$

Proof. If $a \in \mathbb{Z}$, then the sum is N. If $\alpha \notin \mathbb{Z}$, then

$$\left|\sum_{n=1}^{N} e(\alpha n + \beta)\right| = \left|\sum_{n=1}^{N} e(\alpha n)\right| \le \frac{|1 - e(\alpha N)|}{|1 - e(\alpha)|} \le \frac{|\sin \pi\alpha N|}{|\sin \pi\alpha|} \le \frac{1}{2\|\alpha\|}. \qquad \square$$

Weyl's criterion and Lemma 8.3.2 immediately imply the following result.

Corollary 8.3.3. *If α is an irrational number, and $\beta \in \mathbb{R}$, then the sequence $\{\alpha n + \beta : n \in \mathbb{N}\}$ is equdistributed.*

Weyl [123] observed that by squaring the sum $S = \left|\sum_{n=1}^{N} e\big(P(n)\big)\right|$, we have the following estimate:

$$\begin{aligned}
|S|^2 &= \sum_{n=1}^{N}\sum_{m=1}^{N} e\big(P(m) - P(n)\big) \\
&= \sum_{n=1}^{N}\sum_{h=1-n}^{N-n} e\big(P(n+h) - P(n)\big) \\
&= N + \sum_{h=1}^{N-1}\sum_{n=1}^{N-h} e\big(P(n+h) - P(n)\big) + \sum_{h=1-N}^{-1}\sum_{n=1-h}^{N} e\big(P(n+h) - P(n)\big) \\
&= N + 2\,\mathrm{Re}\sum_{h=1}^{N-1}\sum_{n=1}^{N-h} e\big(P(n+h) - P(n)\big) \\
&\le N + 2\sum_{h=1}^{N-1}\left|\sum_{n=1}^{N-h} e\big(P(n+h) - P(n)\big)\right|.
\end{aligned}$$

In this way, one can estimate S in terms of other exponential sums involving the difference $P(n+h)-P(n)$, which is a polynomial of degree $\deg P - 1$. This process is called Weyl differencing.

Lemma 8.3.4 (Weyl differencing)**.** *If $P(x)$ is a polynomial, and $S = \left|\sum_{n=1}^{N} e\big(P(n)\big)\right|$, then*

$$|S|^2 \le N + 2\sum_{h=1}^{N-1}\left|\sum_{n=1}^{N-h} e\big(P(n+h) - P(n)\big)\right|.$$

If one continues the differencing process, then the polynomial finally becomes linear after $(\deg P - 1)$ steps, and we can then use Lemma 8.3.2. To illustrate this method, next we consider a quadratic polynomial.

Theorem 8.3.5 (Weyl's inequality for quadratic polynomials)**.** *Let $a \in \mathbb{Z}$ and $m \in \mathbb{N}$ with $(a, m) =$*

1 *and* $N \in \mathbb{N}$ *with* $N \geq 2$. *If* $\alpha, \beta, \gamma \in \mathbb{R}$ *with* $|\alpha - a/m| \leq m^{-2}$, *then*

$$\left|\sum_{n=1}^{N} e(\alpha n^2 + \beta n + \gamma)\right| \ll \frac{N}{\sqrt{m}} + \sqrt{N \log m} + \sqrt{m \log m}.$$

Proof. Let $P(x) = \alpha x^2 + \beta x + \gamma$ so that $P(x+h) - P(x) = 2\alpha hx + \alpha h^2 + \beta h$. Let $S = \sum_{n=1}^{N} e\big(P(n)\big)$. Then by Lemma 8.3.2 and Lemma 8.3.4,

$$|S|^2 \leq N + 2\sum_{h=1}^{N-1}\left|\sum_{n=1}^{N-h} e(2\alpha hn)\right| \leq N + 2\sum_{h=1}^{N-1} \min\left\{N - h, \frac{1}{\|2\alpha h\|}\right\} \ll N + \sum_{h=1}^{2N} \min\left\{N, \frac{1}{\|\alpha h\|}\right\}.$$

Let $\alpha = a/m + \delta$ so that $|\delta| \leq m^{-2}$. Note that if $0 < |h_2 - h_1| \leq m/2$, then $(a, m) = 1$ implies that

$$\|\alpha h_2 - \alpha h_1\| \geq \|(h_2 - h_1)\, a/m\| - \|(h_2 - h_1)\, \delta\| \geq 1/m - 1/2m = 1/2m.$$

Therefore, by dividing the interval into blocks of length at most m, we have

$$\begin{aligned}
\sum_{h=1}^{2N} \min\left\{N, \frac{1}{\|\alpha h\|}\right\} &\leq \sum_{k=0}^{\lfloor 4N/m \rfloor} \sum_{h=k\lfloor m/2 \rfloor + 1}^{(k+1)\lfloor m/2 \rfloor} \min\left\{N, \frac{1}{\|\alpha h\|}\right\} \\
&\ll \left(\frac{N}{m} + 1\right) \sum_{j=0}^{m} \min\left\{N, \frac{m}{j}\right\} \\
&\ll \left(\frac{N}{m} + 1\right) N + \left(\frac{N}{m} + 1\right) \sum_{1 \leq j \leq m} \frac{m}{j} \\
&\ll N^2/m + N + N \log m + m \log m.
\end{aligned}$$

It follows that $|S| \leq \frac{N}{\sqrt{m}} + \sqrt{N \log m} + \sqrt{m \log m}$. □

In general, for a polynomial with an arbitrary degree, we can apply Weyl differencing multiple times until the difference polynomial becomes linear. By induction, we have the following estimate on exponential sums.

Theorem 8.3.6 (Theorem 3.2 in [84])**.** *Let* $\epsilon > 0$ *be fixed. Let* $a \in \mathbb{Z}$ *and* $m \in \mathbb{N}$ *with* $(a, m) = 1$. *Let* $\alpha \in \mathbb{R}$ *with* $|\alpha - a/m| \leq m^{-2}$. *Then for any monic polynomial* P *with degree* $k \geq 2$, *we have*

$$\left|\sum_{n \leq N} e\big(\alpha P(n)\big)\right| \ll_k N^{1+\varepsilon}\left(\frac{1}{m} + \frac{1}{N} + \frac{m}{N^k}\right)^{2^{1-k}} \tag{8.3}$$

The following lemma concerning with the rational approximation of irrational numbers, together with Theorem 8.3.6 and Weyl's criterion, can be used to prove Theorem 8.3.1. The proof of Dirichlet's theorem uses a standard pigeonholing argument.

Lemma 8.3.7 (Dirichlet's theorem)**.** *If* α *is irrational, there exists* $a \in \mathbb{Z}$ *and* $m \in \mathbb{N}$ *such that*

$|\alpha - \frac{a}{m}| \leq \frac{1}{m^2}$.

Next, we briefly discuss Vinogradov's method for estimating Weyl sums. Vinogradov's method leads to improved estimates on Weyl sums $S = \sum_{n=1}^{N} e\big(P(n)\big)$ provided $\deg P$ is sufficiently large (say $\deg P > 10$) [84]. Roughly speaking, Vinogradov's method reduces the problem of estimating Weyl sums to the problem of counting the number of solutions to certain diophantine equations.

For each integers $s \geq 1$ and $n, N \geq 2$, we denote $J_{s,n}(N)$ the number of integral solutions for the following system (called a *Vinogradov system*):

$$X_1^i + \ldots + X_s^i = X_{s+1}^i + \ldots + X_{2s}^i, \;\; 1 \leq i \leq n,$$

with $1 \leq X_1, \ldots, X_{2s} \leq N$. One can show the number $J_{s,n}(N)$ has the following well-known analytic representation using the Fourier transform (see for example the introduction section of [129]):

$$J_{s,n}(N) = \int_{\mathbb{T}^n} \left| \sum_{j=1}^{N} e(\alpha_1 j + \alpha_2 j^2 + \ldots + \alpha_n j^n) \right|^{2s} d\alpha_1 \ldots d\alpha_n.$$

It is realtively easy to show $J_{s,n}(N) \gg N^s + N^{2s - \frac{n(n+1)}{2}}$ (see for example Theorem 2.3 in [129]). The main conjecture in Vinogradov's mean value theorem asserts that this lower bound is close to tight.

Conjecture 8.3.8 (Vinogradov's mean value conjecture)**.** *For each $s \geq 1$ and $n, N \geq 2$, we have the upper bound*

$$J_{s,n}(N) \ll_\epsilon N^{s+\epsilon} + N^{2s - \frac{n(n+1)}{2} + \epsilon}, \quad \forall \epsilon > 0.$$

By Hölder's inequality, one can show that it suffices to prove the conjecture for the case $s = \frac{n(n+1)}{2}$, the critical exponent; see for example Theorem 2.4 in [129]. The case $n = 1$ is easy, and the case $n = 2$ can be solved using algebraic manipulation and basic analytic number theory; see Section 3 in [129]. The case $n = 3$ was solved by Wooley in [124] using the so-called efficient congruencing method; see Section 4 in [129] for a rough idea. Recently, Conjecture 8.3.8 was confirmed by Bourgain, Demeter and Guth [12] using decoupling and later by Wooley [125] using an adapted efficient congruencing method.

The following theorem serves as an example of how can one relates $J_{s,n}(N)$ to the Weyl sums.

Theorem 8.3.9 (Theorem 4.4 in [84])**.** *Suppose that $P(x)$ is a polynomial of degree k with real coefficients whose leading coefficient α is irrational and satisfies the inequality $|\alpha - a/m| \leq m^{-2}$ with $(a, m) = 1$. Then*

$$\sum_{n=1}^{N} e\big(P(n)\big) \ll \Big(b^k k\Big)^{\frac{1}{2b}} N \left(\frac{J_{2b,k-1}(3N)}{N^{2b-k(k-1)/2}} \right)^{\frac{1}{2b}} \left(\frac{1}{m} + \frac{\log m}{N} + \frac{m \log m}{N^k} \right)^{\frac{1}{2b}}.$$

Since Conjecture 8.3.8 has been confirmed, by taking $b = k(k-1)/2$, we get the following estimate, which improves on Weyl's estimate for $k \geq 6$.

Corollary 8.3.10. *Let $P(x)$ be as in Theorem 8.3.9. Then*

$$\sum_{n=1}^{N} e\big(P(n)\big) \ll_k N^{1+\epsilon}\left(\frac{1}{m}+\frac{\log m}{N}+\frac{m\log m}{N^k}\right)^{\frac{1}{k(k-1)}}.$$

Next we consider the equidistribution of polynomial sequence restricted to prime terms. In 1937, Vinogradov [119] showed that if α is an irrational number, then $\{\alpha p : p \in \mathcal{P}\}$ is equidistributed, by establishing

$$\sum_{n\le x}\Lambda(n)e(n\alpha) \ll \left(\frac{x}{\sqrt{m}}+\sqrt{mx}+x^{4/5}\right)\log^3 x, \tag{8.4}$$

provided $|\alpha - a/m| \le m^{-2}$ and $(a,m)=1$. One can use Vaughan's identity, Lemma 8.3.2, and the estimate on bilinear forms to prove (8.4); see for example Chapter 13 in [57]. We will demonstarate a similar process in Section 8.5.

Theorem 8.3.1 gives the full characterization for polynomial sequences being equidistributed. Using Vinogradov's method, Rhin [99] showed the following theorem, which says the same characterization also holds when we restrict the indices to be prime numbers $\mathcal{P}$.

Theorem 8.3.11 ([99])**.** *Let f be a nonconstant polynomial. The sequence $\{f(p) : p \in \mathcal{P}\}$ is equidistributed if and only if at least one of the coefficients of f, other than the constant term, is irrational.*

8.4 Van der Corput method: process A

In 1922, Van der Corput [25] modified and improved Weyl differencing. We begin the following simple yet useful inequality.

Lemma 8.4.1 (Van der Corput's inequality)**.** *Suppose $\xi(n)$ is a complex-valued function such that $\xi(n)=0$ if $n \notin I=(a,b]$, where $a,b\in\mathbb{Z}$. If H is a positive integer, then*

$$\left|\sum_n \xi(n)\right|^2 \le \frac{|I|+H}{H}\sum_{|h|<H}\left(1-\frac{|h|}{H}\right)\sum_n \xi(n)\overline{\xi(n-h)}.$$

Proof. Since ξ is supported on I, we have

$$H\sum_n \xi(n) = \sum_{k=1}^{H}\sum_n \xi(n+k) = \sum_n\sum_{k=1}^{H}\xi(n+k) = \sum_{a-H<n\le b-1}\sum_{k=1}^{H}\xi(n+k).$$

By the Cauchy-Schwarz inequality,

$$\begin{aligned} H^2\left|\sum_n \xi(n)\right|^2 &\le (|I|+H)\sum_n\left|\sum_{k=1}^{H}\xi(n+k)\right|^2 \\ &= (|I|+H)\sum_{k=1}^{H}\sum_{l=1}^{H}\sum_n \overline{\xi(n+k)}\xi(n+l) \\ &= (|I|+H)\sum_{k=1}^{H}\sum_{l=1}^{H}\sum_n \xi(n)\overline{\xi(n+k-l)} \\ &= (|I|+H)\sum_{|h|<H}(H-|h|)\sum_n \xi(n)\overline{\xi(n-h)}, \end{aligned}$$

where we substitute $h = l - k$ in the last step. □

Using Van der Corput's inequality, we can establish the following equidistribution test.

Theorem 8.4.2 (Van der Corput's difference theorem, [26])**.** *Let $(x_n)_{n\in\mathbb{N}}$ be a sequence of real numbers. If the sequences $(x_{n+h}-x_n)_{n\in\mathbb{N}}$ are equidistributed for all positive integers h, then $(x_n)_{n\in\mathbb{N}}$ is also equidistributed.*

Proof. Fix a nonzero integer k and positive integer H. For each $M \in \mathbb{N}$, by van der Corput's inequality with $\xi(n) = e(kx_n)$ for $n \in I = (0, M]$, we have

$$\left|\sum_{n\le M} e(kx_n)\right|^2 \le \frac{M+H}{H}\left(M + \sum_{h=1}^{H}\sum_{|h|\le n\le M} e\big(k(x_n - x_{n-h})\big) + \sum_{h=1}^{H}\sum_{0\le n\le M-|h|} e\big(k(x_n - x_{n-h})\big)\right).$$

Since $(x_{n+h} - x_n)_{n\in\mathbb{N}}$ is equidistributed for every positive integer h, when M is sufficiently large we can guarantee that each inner exponential sum is bounded by M/H^2. So for each sufficiently large M,

$$\left|\sum_{n\le M} e(kx_n)\right|^2 \le \frac{M(M+H)}{H} + \frac{2(M+H)}{H}\sum_{h=1}^{H}\frac{M}{H^2} \le \frac{M(M+H)}{H} + \frac{2M(M+H)}{H^2} \le \frac{3M(M+H)}{H}.$$

Letting $H \to \infty$, we obtain $\sum_{n\le M} e(kx_n) = o(M)$ as $M \to \infty$. Therefore, by Weyl's criterion, $(x_n)_{n\in\mathbb{N}}$ is also equidistributed. □

Using van der Corput's difference theorem, we have the following simplified proof of Theorem 8.3.1.

Proof of Theorem 8.3.1. Let $d = \deg P$. We will prove the theorem by inducting on d. The case $d = 1$ has been proved in Corollary 8.3.3. Suppose $d \ge 2$, and the claim holds for all polynomials with degree at most $d - 1$.

- If the leading coefficient of P is irrational, then for each h, $P(n+h)-P(n)$ is a polynomial is of degree $d-1$, with leading coefficient irrational, so by the inductive hypothesis, $\{P(n+h)-P(n) : n \in \mathbb{N}\}$ is equidistributed. Then by Theorem 8.4.2, $\{P(n) : n \in \mathbb{N}\}$ is equidistributed.

- If the leading coefficient of P is rational, then $P(x) = \frac{a}{b}x^d + Q(x)$ for some rational number $\frac{a}{b} \neq 0$ and a polynomial Q of degree less than d that has an irrational coefficient other than the constant term. Then for any nonzero integer k,

$$\begin{aligned}\sum_{n\leq x} e\big(kP(n)\big) &= \sum_{m=0}^{b-1} \sum_{\substack{n\leq x \\ n\equiv m \pmod b}} e\bigg(kQ(n) + \frac{ak}{b}n^d\bigg) \\ &= \sum_{m=0}^{b-1} \sum_{n\leq \frac{x-m}{b}} e\bigg(kQ(bn+m) + \frac{ak}{b}(bn+m)^d\bigg) \\ &= \sum_{m=0}^{b-1} \sum_{n\leq \frac{x-m}{b}} e\bigg(kQ(bn+m) + \frac{ak}{b}m^d\bigg) \ll \sum_{m=0}^{b-1} \sum_{n\leq \frac{x-m}{b}} e\bigg(kQ(bn+m)\bigg).\end{aligned}$$

  By using the inductive hypothesis and Weyl's criterion on the polynomial $Q(bn+m)$, we conclude that $\sum_{n\leq x} e\big(kP(n)\big) = o(x)$ for any nonzero integer k. So by Weyl's criterion, $\{P(n) : n \in \mathbb{N}\}$ is equidistributed. □

Another important consequence of van der Corput's inequality is the following theorem, usually called "process A" of van der Corput's method. For the proof, we just need to take $\xi(n) = e\big(f(n)\big)$ if $n \in I$, and $\xi(n) = 0$ if $n \notin I$.

Theorem 8.4.3 (Process A)**.** *Let $f : I = [a, b) \to \mathbb{R}$ be a function and $H \leqslant |I|$ an integer. Then*

$$\left|\sum_{n\in I} e\big(f(n)\big)\right|^2 \leqslant \frac{2|I|^2}{H} + \frac{2|I|}{H} \cdot \sum_{1\leqslant|h|\leqslant H} \left|\sum_{n\in I_h} e\big(f_h(n)\big)\right|.$$

Next, we give several estimates on exponential sums based on the size of the derivatives. The first estimate is due to Kusmin and Landau [86]. We need the following computation as a preparation.

Lemma 8.4.4. *If $x \in \mathbb{R}$, and $e(x) \neq 1$, then*

$$\frac{1}{1-e(x)} = \frac{1}{2}(1 + i\cot \pi x).$$

Proof. We have

$$\begin{aligned}\frac{1}{1-e(x)} &= \frac{1}{1-\cos(2\pi x) - i\sin(2\pi x)} = \frac{1}{2\sin^2(\pi x) - 2i\sin(\pi x)\cos(\pi x)} \\ &= \frac{1}{2\sin(\pi x)} \frac{\sin(\pi x) + i\cos(\pi x)}{\sin^2(\pi x) - i^2\cos^2(\pi x)} = \frac{1}{2}(1 + i\cot \pi x).\end{aligned}$$

□

Theorem 8.4.5 (First derivative test)**.** *Let $f : I \to \mathbb{R}$ be continuously differentiable. If f' is monotonic, and $\|f'(x)\| \geq \lambda > 0$ on I, then*

$$\sum_{n\in I} e\big(f(n)\big) \ll \lambda^{-1},$$

where the implicit constant is absolute.

Proof. Without loss of generality, we may assume f' is increasing. The condition $\|f'\| \geq \lambda > 0$ means that there is an integer k such that $k + \lambda \leq f'(n) \leq k + 1 - \lambda$ for all $n \in I$. Note that

$$\sum_{n\in I} e\big(f(n)\big) = \sum_{n\in I} e(f(n) - kn),$$

so we may assume that $\lambda \leq f'(n) \leq 1 - \lambda$. Define $g(n) = f(n + 1) - f(n)$. By the mean value theorem, there is some $x_n \in (n, n+1)$ such that $g(n) = f'(x_n)$. Consequently, $\{g(n)\}$ is increasing and $\lambda \leq g(n) \leq 1 - \lambda$. Then by Lemma 8.4.4, we have

$$e\big(f(n)\big) = \frac{e\big(f(n)\big) - e\big(f(n+1)\big)}{1 - e(g(n))} = \Big(e\big(f(n)\big) - e\big(f(n+1)\big)\Big)C_n,$$

where $C_n = \frac{1}{2}(1 + i\cot \pi g(n))$. Therefore

$$\begin{aligned}\sum_{n\in I} e\big(f(n)\big) &= \sum_{n=a+1}^{b-1} \Big(e\big(f(n)\big) - e\big(f(n+1)\big)\Big)C_n + e\big(f(b)\big).\\ &= \sum_{n=a+2}^{b-1} e\big(f(n)\big)\left(C_n - C_{n-1}\right) + e\big(f(a+1)\big)C_{a+1} + e\big(f(b)\big)\left(1 - C_{b-1}\right),\end{aligned}$$

and thus

$$\left|\sum_{n\in I} e\big(f(n)\big)\right| \leq \frac{1}{2}\sum_{n=a+2}^{b-1} \left|\cot\big(\pi g(n-1)\big) - \cot\big(\pi g(n)\big)\right| + |C_{a+1}| + |1 - C_{b-1}|.$$

Since $\{\cot\big(\pi g(n)\big)\}$ is a decreasing sequence, we can remove the absolute value sign in the summation on the right-hand side and obtain

$$\left|\sum_{n\in I} e\big(f(n)\big)\right| \leq \frac{1}{2}\Big(\cot\big(\pi g(a+1)\big) - \cot\big(\pi g(b-1)\big)\Big) + |C_{a+1}| + |1 - C_{b-1}|.$$

The theorem follows by the bound $|\cot \pi x| \leq \frac{1}{|sin(\pi x)|} \leq \frac{1}{2\|x\|}$ for $x \in (0, 1)$. □

Similar to the first derivative test, we also have the following second derivative test and third derivative test. Both tests are due to van der Corput [25].

Theorem 8.4.6 (Second derivative test)**.** *Let $f : I \to \mathbb{R}$ be twice continuously differentiable. If there is some $\lambda > 0$ and some $\alpha \geq 1$ such that $\lambda \leq |f''(x)| \leq \alpha\lambda$ on I, then*

$$\sum_{n\in I} e\big(f(n)\big) \ll \alpha|I|\lambda^{1/2} + \lambda^{-1/2},$$

where the implicit constant is absolute.

Sketch of the proof. If $\lambda > 1/4$, the result follows from the trivial estimate. Next we assume $\lambda \leq 1/4$. Note that f' is monotone. Let $\delta < 1/2$ be a parameter to be determined. By the mean value theorem, we have $|f'(b) - f'(a)| \leq \alpha\lambda|I|$, so I can be split into $\leq \alpha\lambda|I| + 2$ intervals on which $\|f'\| \geq \delta$, and $\leq \alpha\lambda|I| + 1$ other intervals, each of length $\leq 2\delta/\lambda$. We apply Theorem 8.4.5 to the former set of intervals, and the trivial estimate to the latter, to get

$$\sum_{n\in I} e\big(f(n)\big) \ll (\alpha\lambda|I| + 2)(1/\delta + \delta/\lambda + 1).$$

Since $\lambda \leq 1/4$, we can choose $\delta = \lambda^{1/2} \leq 1/2$ to minimize $1/\delta + \delta/\lambda$, and obtain the estimate

$$\sum_{n\in I} e\big(f(n)\big) \ll (\alpha\lambda|I| + 2)(\lambda^{-1/2} + 1) \ll \alpha\lambda|I|^{1/2} + \lambda^{-1/2}. \qquad \square$$

Theorem 8.4.7 (Third derivative test)**.** *Let $f : I \to \mathbb{R}$ be three times continuously differentiable. If there is some $\lambda > 0$ and some $\alpha \geq 1$ such that $\alpha^2\lambda \geqslant |I|^{-3}$ and $\lambda \leqslant |f'''(x)| \leqslant \alpha\lambda$ for all $x \in I$, then*

$$\sum_{n\in I} e\big(f(n)\big) \ll \alpha^{1/3}|I|\lambda^{1/6} + \alpha^{1/6}|I|^{1/2}\lambda^{-1/6},$$

where the implicit constant is absolute.

Proof. By the mean value theorem, $|h|\lambda \leqslant |(f_h)''(x)| = |f''(x+h) - f''(x)| \leqslant |h|\alpha\lambda$ for all $x \in I_h$ and for all nonzero integers h. Therefore, by Theorem 8.4.6, we get

$$\sum_{n\in I_h} e\big(f_h(n)\big) \ll \alpha|I|(\lambda|h|)^{1/2} + (\lambda|h|)^{-1/2}.$$

If $H \leqslant |I|$ is an integer, then Theorem 8.4.3 implies that

$$\begin{aligned}\left|\sum_{n\in I} e\big(f(n)\big)\right|^2 &\leq \frac{2|I|^2}{H} + \frac{2|I|}{H}\cdot\sum_{1\leqslant|h|\leqslant H}\left|\sum_{n\in I_h} e\big(f_h(n)\big)\right| \\ &\ll \frac{|I|^2}{H} + \frac{|I|}{H}\cdot\Big(\alpha|I|\lambda^{1/2}H^{3/2} + \lambda^{-1/2}H^{1/2}\Big) \\ &\ll \alpha|I|^2\lambda^{1/2}H^{1/2} + |I|\lambda^{-1/2}H^{-1/2} + |I|^2H^{-1}.\end{aligned}$$

Since $\alpha^2\lambda \geqslant |I|^{-3}$, we can set $H := \lfloor\alpha^{-2/3}\lambda^{-1/3}\rfloor \leq |I|$ to minimize $\alpha|I|^2\lambda^{1/2}H^{1/2} + |I|^2H^{-1}$. Thus

we get

$$\left|\sum_{n\in I} e\big(f(n)\big)\right|^2 \ll \alpha^{2/3}|I|^2\lambda^{1/3} + \alpha^{1/3}|I|\lambda^{-1/3}. \qquad \square$$

The proof presented above is nice, and can be generalized to prove the higher-order derivative tests. Next we illustrate how higher-order derivative tests work by iterating process A. We begin with applying process A twice. Let $S = \sum_{n\in I} e\big(f(n)\big)$. Theorem 8.4.3 states that for any positive integer $H_1 \le |I|$,

$$|S|^2 \leqslant \frac{2|I|^2}{H_1} + \frac{2|I|}{H_1}\cdot \sum_{1\leqslant|h|\leqslant H_1}\left|\sum_{n\in I_h} e\big(f_h(n)\big)\right|.$$

Let $S_1(h) = \sum_{n\in I_h} e\big(f_h(n)\big)$. Note that

$$f_h(n) = f(n+h) - f(n) = \int_0^1 \frac{\partial}{\partial t} f(n+ht)\,dt.$$

Using the inequality $(a+b)^2 \le 2(a^2+b^2)$ and the Cauchy-Schwarz inequality, we get

$$|S|^4 \leqslant \frac{8|I|^4}{H_1^2} + \frac{16|I|^2}{H_1}\cdot \sum_{1\leqslant|h_1|\leqslant H_1}|S_1(h_1)|^2.$$

Now we apply process A to each $|S_1(h_1)|^2$. For any positive integers $H_1, H_2 \le |I|$,

$$|S|^4 \leqslant \frac{8|I|^4}{H_1^2} + \frac{64|I|^4}{H_2} + \frac{32|I|^3}{H_1H_2}\cdot \sum_{1\leqslant|h_1|\leqslant H_1}\sum_{1\leqslant|h_2|\leqslant H_2}|S_2(h_1,h_2)|,$$

where

$$S_2(h_1,h_2) = \sum_{n\in I(h_1,h_2)} e(f_{h_1,h_2}(n)),$$

$$f_{h_1,h_2}(n) = f_{h_1}(n+h_2) - f_{h_1}(n) = \int_0^1 \frac{\partial}{\partial t_2} f_{h_1}(n+h_2t_2)\,dt_2 = \int_0^1\int_0^1 \frac{\partial^2}{\partial t_1\partial t_2} f(n+h_1t_1+h_2t_2)\,dt_1\,dt_2,$$

and

$$I(h_1,h_2) = \{n\in I : n+h_1, n+h_2, n+h_1+h_2 \in I\}.$$

If $H_2 = H_1^2 \le |I|$, then we get

$$|S|^4 \leqslant 8^3\left\{\frac{|I|^4}{H_2} + \frac{|I|^3}{H_1H_2}\cdot \sum_{1\leqslant|h_1|\leqslant H_1}\sum_{1\leqslant|h_2|\leqslant H_2}|S_2(h_1,h_2)|\right\}.$$

By iterating process A, we can establish the following theorem.

Theorem 8.4.8 (Lemma 2.7 in [42]). *Let m be a positive integer, and let $M = 2^m$. If $H \le$*

$|I|, H_m = H$, $H_{m-1} = H^{1/2}, H_{m-2} = H^{1/4}, \ldots,$ *and* $H_1 = H^{2/M}$, *then*

$$|S|^M \leq 8^{M-1} \left\{ \frac{|I|^M}{H} + \frac{|I|^{M-1}}{H_1 \ldots H_m} \sum_{1 \leq h_1 \leq H_1} \cdots \sum_{1 \leq h_m \leq H_m} |S_m(\mathbf{h})| \right\},$$

where

$$\mathbf{h} = (h_1, h_2, \ldots h_m), S_m(\mathbf{h}) = \sum_{n \in I(\mathbf{h})} e\left(f_m(n; \mathbf{h})\right),$$

$$f_m(n; \mathbf{h}) = \int_0^1 \ldots \int_0^1 \frac{\partial^m}{\partial t_1 \partial t_2 \ldots \partial t_m} f(n + \mathbf{h} \cdot \mathbf{t}) dt_1 \ldots dt_m = h_1 h_2 \cdots h_m \int_0^1 \ldots \int_0^1 f^{(m)}(n + \mathbf{h} \cdot \mathbf{t}) dt_1 \ldots dt_m,$$

$$\mathbf{t} = (t_1, \ldots, t_m), \text{ and } I(\mathbf{h}) = (a, b - h_1 - h_2 - \ldots - h_m].$$

Combining Theorem 8.4.8 and the second derivative test, together with some nice inequalities (see Lemma 2.4 in [42]), we can prove the following theorem, the $(m+2)$-nd order derivative test.

Theorem 8.4.9 (Theorem 2.8 in [42])**.** *Let m be a positive integer and let $M = 2^m$. Suppose that f is a real-valued function with $m+2$ continuous derivatives on I. Suppose also that for some $\lambda > 0$ and for some $\alpha \geq 1$, $\lambda \leq \left|f^{(m+2)}(x)\right| \leq \alpha\lambda$ on I. Then*

$$S \ll |I| \left(\alpha^2 \lambda\right)^{1/(4M-2)} + |I|^{1-1/2M} \alpha^{1/2M} + |I|^{1-2/M+1/M^2} \lambda^{-1/2M},$$

where the implicit constant is absolute.

8.5 $\{\sqrt{p} : p \in \mathcal{P}\}$ is equidistributed

Recall our first goal in this chapter is to show polynomial-like functions are equidistributed over $\mathcal{P}$. In this section, we will demonstrate the general process by proving the following estimate, which implies $\{\sqrt{p} : p \in \mathcal{P}\}$ is equidistributed by Corollary 8.2.2.

Theorem 8.5.1. *For any real number $\alpha \neq 0$,*

$$\sum_{n \leq x} e(\alpha\sqrt{n}) \Lambda(n) \ll_\alpha x^{27/28} \log x.$$

We remark that the constant 27/28 stated in the exponent of Theorem 8.5.1 could be improved. The estimate on the exponential sums over primes usually relies on the decomposition of the von Mangoldt function Λ. In the proof of Theorem 8.5.1, we apply Vaughan's identity. One could instead use Heath-Brown's generalization of Vaughan's identity [54] to improve the exponent.

One would expect that the best possible upper bound for $\sum_{n \leq x} e(\alpha\sqrt{n})\Lambda(n)$ is $(x \log x)^{1/2}$ by the following computation on its lower bound.

$$\int_0^T \Big|\sum_{n\le x} e(\alpha\sqrt{n})\Lambda(n)\Big|^2 d\alpha = \int_0^T \Big(\sum_{m\le x}\sum_{n\le x} e\big(\alpha(\sqrt{m}-\sqrt{n})\big)\Lambda(m)\Lambda(n)\Big)d\alpha$$
$$= T\sum_{m\le x}\Lambda(m)^2 + \frac{1}{2\pi i}\sum_{m\le x}\sum_{\substack{n\le x\\ n\neq m}} \frac{\Lambda(m)\Lambda(n)}{\sqrt{m}-\sqrt{n}}\big(e\big(T(\sqrt{m}-\sqrt{n})\big)-1\big)$$
$$= T\big(x\log x + O(x)\big) + R(x,T).$$

Using the trivial bound $\big|e(T(\sqrt{m}-\sqrt{n}))-1\big|\le 2$, we see that the error term $R(x,T)$ is bounded as a function of x uniformly in T. When T is sufficiently large, this implies that there exists some $\alpha\in(0,T)$ such that $\Big|\sum_{n\le x} e(\alpha\sqrt{n})\Lambda(n)\Big|^2 \gg x\log x$.

We begin by estimating the exponential sum over integers. Note that when t is large and comparable to x, the first estimate in the following estimate is trivial. So we need the second estimate on the exponential sum when t is large. The first estimate outperforms when $t\le x^{1/2}$.

Lemma 8.5.2. *For any real number $t>0$,*

$$\sum_{n\le x} e(t\sqrt{n}) \ll \min\{x^{\frac{1}{2}}t^{-1}+t, t^{1/2}x^{1/4}+t^{-1/2}x^{3/4}\},$$

where the implicit constant does not depend on t.

Proof. Let $g(y)=t\sqrt{y}$ so that $g'(y)=\frac{1}{2}ty^{-1/2}$ is decreasing on $(0,\infty)$, and $g''(y)=-\frac{1}{4}ty^{-3/2}$.

We first prove the first estimate. Note that the trivial upper bound is x, so the above estimate is trivial when $x\le 2$ or $x\le t$. Next we assume $x>2$ and $x>t$. If $t\le 1$, then $\frac{1}{2}tx^{-1/2}\le g'(n)\le \frac{1}{2}t<\frac{1}{2}$ for each $1<y\le x$, so $\|f'(y)\|\ge \frac{1}{2}tx^{-1/2}>0$ on $I=(1,\lfloor x\rfloor]$. By Theorem 8.4.5 (the first derivative test), we have

$$\sum_{n\le x} e(t\sqrt{n}) \ll 1+\Big|\sum_{n\in I} e\big(g(n)\big)\Big| \ll 1+x^{1/2}t^{-1} \ll x^{1/2}t^{-1}.$$

If $t>1$, then

$$\sum_{n\le x} e(t\sqrt{n}) \ll t^{2/3}+1+\Big|\sum_{t^{2/3}<n\le x} e\big(g(n)\big)\Big| \ll t+\Big|\sum_{t^{2/3}<n\le x} e\big(g(n)\big)\Big|.$$

Note that when $y>t^{2/3}$, $0<g'(y)<\frac{1}{2}t^{2/3}$. Let $s=\lfloor\frac{1}{2}t^{2/3}\rfloor$. For each integer $k\in[1,\frac{1}{2}t^{2/3}]$, we set $\lambda_k=\frac{(k+1)^{3/2}}{2t}$ so that $\lambda_k<\frac{1}{2}$. Note that

$$\{g'(n): t^{2/3}<n\le x\}\subset\Big(\frac{1}{2}tx^{-1/2},\frac{1}{2t}\Big)\bigcup\Big(\bigcup_{k=1}^{s+1}(k-\lambda_{k-1},k+\lambda_k)\Big)\bigcup\Big(\bigcup_{k=0}^{s}[k+\lambda_k,k+1-\lambda_k]\Big).$$

By Theorem 8.4.5 (the first derivative test), there is a constant $C>0$ such that for each integer

$0 \le k \le s$,

$$\sum_{\substack{t^{2/3}<n\le x\\ g'(n)\in[k+\lambda_k,k+1-\lambda_k]}} e\big(g(n)\big) \le C\lambda_k^{-1},$$

and also

$$\sum_{\substack{t^{2/3}<n\le x\\ g'(n)\in(\frac{1}{2}tx^{-1/2},\frac{1}{2t})}} e\big(g(n)\big) \le 2Cx^{1/2}t^{-1}.$$

For an integer $1 \le k \le s+1$, note that the number of integers n such that $g'(n) \in (k-\lambda_{k-1}, k+\lambda_k)$ is at most

$$1 + \frac{t^2}{4(k-\lambda_{k-1})^2} - \frac{t^2}{4(k+\lambda_k)^2} \le 1 + \frac{t^2(k\lambda_k+\lambda_k^2-\lambda_{k-1}^2)}{2(k-\lambda_{k-1})^2(k+\lambda_k)^2} \le 1 + \frac{t^2(k+2)\lambda_k}{2(k-\lambda_{k-1})^2k^2}.$$

Therefore

$$\Big|\sum_{t^{2/3}<n\le x} e\big(g(n)\big)\Big| \le 2Cx^{1/2}t^{-1} + s + 1 + \sum_{k=0}^{s} C\lambda_k^{-1} + \sum_{k=1}^{s+1} \frac{t^2(k+2)\lambda_k}{2(k-\lambda_{k-1})^2k^2} \ll x^{1/2}t^{-1} + t.$$

For the second estimate, we use Theorem 8.4.6 (the second derivative test). Recall $g''(y) = -\frac{1}{4}ty^{-3/2}$. When $y \in (N, 2N]$, we have $\lambda \le |g''(y)| \le 2^{3/2}\lambda$, where $\lambda = \frac{1}{4}t(2N)^{-3/2}$. Therefore, for any integer N,

$$\sum_{n\in(N,2N]} e\big(g(n)\big) \ll N\lambda^{1/2} + \lambda^{-1/2} \ll t^{1/2}N^{1/4} + t^{-1/2}N^{3/4},$$

where the implicit constant is absolute. Therefore,

$$\sum_{n\le x} e\big(g(n)\big) \ll 1 + \sum_{k=1}^{\log_2 x} \sum_{n\in(x/2^k,2x/2^k]} e\big(g(n)\big) \ll t^{1/2}x^{1/4} + t^{-1/2}x^{3/4}.$$

To conclude,

$$\sum_{n\le x} e(t\sqrt{n}) \ll \min\{x^{\frac{1}{2}}t^{-1} + t, t^{1/2}x^{1/4} + t^{-1/2}x^{3/4}\}. \qquad \square$$

In fact, without too much work, one can write

$$\sum_{n\le x} e(t\sqrt{n}) \ll \begin{cases} x^{\frac{1}{2}}t^{-1}, & \text{if } 0 < t \le x^{1/4},\\ t, & \text{if } x^{1/4} < t \le x^{1/2},\\ t^{1/2}x^{1/4}, & \text{if } x^{1/2} < t \le x^{3/2},\\ x, & \text{if } x^{3/2} < t. \end{cases}$$

Note that the term $t^{-1/2}x^{3/4}$ never dominates, and the last bound is the trivial bound.

Next we will use Lemma 8.5.2 to prove a series of estimates on exponential sums, and we will

sometimes only use the first estimate since that will be sufficient for our purpose.

Corollary 8.5.3. *For any positive real numbers α, x, y such that $y \le x$,*

$$\sum_{n \le x/y} e(\alpha\sqrt{ny}) \ll x^{1/2}y^{-1}\alpha^{-1} + \alpha y^{1/2}.$$

Proof. By the first estimate $x^{\frac{1}{2}}t^{-1} + t$ in Lemma 8.5.2,

$$\sum_{n \le x/y} e(\alpha\sqrt{ny}) = \sum_{n \le x/y} e\big((\alpha\sqrt{y})\sqrt{n}\big) \ll (x/y)^{1/2}\alpha^{-1}y^{-1/2} + \alpha y^{1/2}. \qquad \square$$

Lemma 8.5.4. *For any positive real numbers α, x, y such that $y \le x$,*

$$\sum_{m \le y} \left| \sum_{mn \le x} e(\alpha\sqrt{mn}) \log n \right| \ll x^{1/2}\alpha^{-1} \log x \log y + y^{3/2}\alpha \log x.$$

Proof. Fix $m \le y$ first and set $A(u) = \sum_{n \le u} e(\alpha\sqrt{mn})$. Then by Corollary 8.5.3,

$$A(u) \ll (um)^{1/2}m^{-1}\alpha^{-1} + \alpha m^{1/2} \ll u^{1/2}m^{-1/2}\alpha^{-1} + \alpha m^{1/2}.$$

By partial summation, we get

$$\begin{aligned}
\sum_{mn \le x} e(\alpha\sqrt{mn}) \log n &= \int_{1^-}^{x/m} \log u \, dA(u) \\
&= A(u) \log u \Big|_{1^-}^{x/m} - \int_1^{x/m} \frac{A(u)}{u} \, du \\
&\ll (x/m)^{1/2}m^{-1/2}\alpha^{-1} \log x + \alpha m^{1/2} \log x + (x/m)^{1/2}m^{-1/2}\alpha^{-1} + \alpha m^{1/2} \log x \\
&\ll x^{1/2}m^{-1}\alpha^{-1} \log x + \alpha m^{1/2} \log x.
\end{aligned}$$

Therefore,

$$\begin{aligned}
\sum_{m \le y} \left| \sum_{mn \le x} e(\alpha\sqrt{mn}) \log n \right| &\ll \sum_{m \le y} \big(x^{1/2}m^{-1}\alpha^{-1} \log x + \alpha m^{1/2} \log x\big) \\
&\ll x^{1/2}\alpha^{-1} \log x \log y + y^{3/2}\alpha \log x. \qquad \square
\end{aligned}$$

Next we start to estimate the bilinear forms. For any positive real numbers M, N, α, and sequences of complex numbers $\{\beta_m\}$ and $\{\gamma_n\}$, we define

$$A(M, N) := A(M, N, \alpha, \beta, \gamma) = \sum_{M < m \le 2M} \sum_{N < n \le 2N} \beta_m \gamma_n e(\alpha\sqrt{mn}).$$

Lemma 8.5.5. *For any positive real numbers M, N, α, and complex numbers β_m, γ_n with $|\beta_m| \le 1$*

and $|\gamma_n| \le 1$,

$$A(M,N) \ll MN^{1/2} + M^{1/4}N^{3/4}\alpha^{-1/2}(\log N)^{1/2} + N^{5/4}\alpha^{1/2}.$$

Proof. By the Cauchy-Schwarz inequality,

$$\begin{aligned}
A^2(M,N) &\ll \Big(\sum_{M<m\le 2M}|\beta_m|^2\Big)\Big(\sum_{M<m\le 2M}\Big|\sum_{N<n\le 2N}\gamma_n e(\alpha\sqrt{mn})\Big|^2\Big)\\
&\ll M\sum_{M<m\le 2M}\sum_{N<n_1,n_2\le 2N}\overline{\gamma_{n_1}}\gamma_{n_2}e\big(\alpha(\sqrt{n_2}-\sqrt{n_1})\sqrt{m}\big)\\
&\ll M\sum_{N<n_1,n_2\le 2N}\Big|\sum_{M<m\le 2M}e\big(\alpha(\sqrt{n_2}-\sqrt{n_1})\sqrt{m}\big)\Big|\\
&\ll M^2N + \sum_{N<n_1<n_2\le 2N}\Big|\sum_{m\le 2M}e(\alpha(\sqrt{n_2}-\sqrt{n_1})\sqrt{m})\Big|\\
&\qquad + \sum_{N<n_1<n_2\le 2N}\Big|\sum_{m\le M}e(\alpha(\sqrt{n_2}-\sqrt{n_1})\sqrt{m})\Big|,
\end{aligned}$$

as the contribution of the diagonal terms is $\ll M^2N$. Therefore, by Lemma 8.5.2, we have

$$\begin{aligned}
A^2(M,N) &\ll M^2N + \sum_{N<n_1<n_2\le 2N}(2M)^{1/2}\alpha^{-1}\frac{\sqrt{n_2}+\sqrt{n_1}}{n_2-n_1}\\
&\qquad + \sum_{N<n_1<n_2\le 2N}M^{1/2}\alpha^{-1}\frac{\sqrt{n_2}+\sqrt{n_1}}{n_2-n_1} + \sum_{N<n_1<n_2\le 2N}\alpha(\sqrt{n_2}-\sqrt{n_1})\\
&\ll M^2N + \sum_{N<n_1<n_2\le 2N}M^{1/2}\alpha^{-1}\frac{\sqrt{n_2}}{n_2-n_1} + N^{5/2}\alpha\\
&\ll M^2N + M^{1/2}\alpha^{-1}\sum_{N<n_2\le 2N}\sqrt{n_2}\log N + N^{5/2}\alpha\\
&\ll M^2N + M^{1/2}N^{3/2}\alpha^{-1}\log N + N^{5/2}\alpha.
\end{aligned}$$

□

Next we estimate a different bilinear form. For any positive real numbers N, x, α, and a sequence of complex numbers $\{\beta_m\}$, we define

$$B(x;N) := B(x,N,\alpha,\beta) = \sum_{N<n\le 2N}\Big|\sum_{mn\le x}\beta_m e(\alpha\sqrt{mn})\Big|.$$

Lemma 8.5.6. *For any real numbers* $\alpha > 0$, $N \le x$ *and complex numbers* β_m *with* $|\beta_m| \le 1$,

$$B(x;N) \ll N^{1/2}x^{1/2} + \alpha^{-1/2}x^{3/4}(\log x)^{1/2} + (\alpha^{1/2}+\alpha^{-1/4})xN^{-1/4} + \alpha^{1/4}x^{9/8}N^{-1/2}.$$

Proof. By the Cauchy-Schwarz inequality,

$$\begin{aligned}
B^2(x;N) &\ll N \sum_{N<n\le 2N} \sum_{m_1 n\le x, m_2 n\le x} \overline{\beta_{m_1}}\beta_{m_2} e\big(\alpha(\sqrt{m_2}-\sqrt{m_1})\sqrt{n}\big) \\
&\ll N \sum_{m_1\le m_2\le \frac{x}{N}} \Big| \overline{\beta_{m_1}}\beta_{m_2} \sum_{\substack{N<n\le 2N \\ m_2 n\le x}} e\big(\alpha(\sqrt{m_2}-\sqrt{m_1})\sqrt{n}\big)\Big| \\
&\ll N \sum_{m_1\le m_2\le \frac{x}{N}} \Big| \sum_{\substack{N<n\le 2N \\ m_2 n\le x}} e\big(\alpha(\sqrt{m_2}-\sqrt{m_1})\sqrt{n}\big)\Big| \\
&\ll Nx + N \sum_{m_1<m_2\le \frac{x}{N}} \Big| \sum_{\substack{n\le 2N \\ m_2 n\le x}} e\big(\alpha(\sqrt{m_2}-\sqrt{m_1})\sqrt{n}\big)\Big| \\
&\qquad + N \sum_{m_1<m_2\le \frac{x}{N}} \Big| \sum_{\substack{n\le N \\ m_2 n\le x}} e\big(\alpha(\sqrt{m_2}-\sqrt{m_1})\sqrt{n}\big)\Big|,
\end{aligned}$$

as the the contribution of the diagonal terms is $\ll N\frac{x}{N}(2N-N) = Nx$. When $\sqrt{m_2}-\sqrt{m_1}\le\sqrt{N}$, we apply the first estimate in Lemma 8.5.2 to get

$$\begin{aligned}
\Big| \sum_{\substack{n\le N \\ m_2 n\le x}} e\big(\alpha(\sqrt{m_2}-\sqrt{m_1})\sqrt{n}\big)\Big| &\ll N^{1/2}\alpha^{-1}(\sqrt{m_2}-\sqrt{m_1})^{-1} + \alpha(\sqrt{m_2}-\sqrt{m_1}) \\
&\ll N^{1/2}\alpha^{-1}\frac{\sqrt{m_2}}{m_2-m_1} + \alpha N^{1/2}.
\end{aligned}$$

When $\sqrt{m_2}-\sqrt{m_1}>\sqrt{N}$, we apply the second estimate in Lemma 8.5.2 to get

$$\begin{aligned}
\Big| \sum_{\substack{n\le N \\ m_2 n\le x}} e\big(\alpha(\sqrt{m_2}-\sqrt{m_1})\sqrt{n}\big)\Big| &\ll N^{1/4}\alpha^{1/2}(\sqrt{m_2}-\sqrt{m_1})^{1/2} + N^{3/4}\alpha^{-1/2}(\sqrt{m_2}-\sqrt{m_1})^{-1/2} \\
&\ll N^{1/4}\alpha^{1/2}m_2^{1/4} + N^{1/2}\alpha^{-1/2}.
\end{aligned}$$

Therefore,

$$\begin{aligned}
B^2(x;N) &\ll Nx + N \sum_{m_1<m_2\le \frac{x}{N}} \left(N^{1/2}\alpha^{-1}\frac{\sqrt{m_2}}{m_2-m_1} + \alpha N^{1/2} + N^{1/4}\alpha^{1/2}m_2^{1/4} + N^{1/2}\alpha^{-1/2}\right) \\
&\ll Nx + N^{3/2}\alpha^{-1} \sum_{m_2\le\frac{x}{N}} \sum_{k=1}^{m_2} \frac{\sqrt{m_2}}{k} + N^{3/2}\alpha(x/N)^2 + N^{5/4}\alpha^{1/2} \sum_{m_2\le\frac{x}{N}} m_2^{5/4} + N^{3/2}\alpha^{-1/2}(x/N)^2 \\
&\ll Nx + N^{3/2}\alpha^{-1} \sum_{m_2\le\frac{x}{N}} \sqrt{m_2}\log m_2 + \alpha x^2 N^{-1/2} + N^{5/4}\alpha^{1/2}(x/N)^{9/4} + \alpha^{-1/2}x^2N^{-1/2} \\
&\ll Nx + N^{3/2}\alpha^{-1}(x/N)^{3/2}\log x + (\alpha+\alpha^{-1/2})x^2N^{-1/2} + \alpha^{1/2}x^{9/4}N^{-1} \\
&\ll Nx + \alpha^{-1}x^{3/2}\log x + (\alpha+\alpha^{-1/2})x^2N^{-1/2} + \alpha^{1/2}x^{9/4}N^{-1}.
\end{aligned}$$

To conclude,

$$B(x;N) \ll N^{1/2}x^{1/2} + \alpha^{-1/2}x^{3/4}(\log x)^{1/2} + (\alpha^{1/2}+\alpha^{-1/4})xN^{-1/4} + \alpha^{1/4}x^{9/8}N^{-1/2}. \qquad \square$$

Lemma 8.5.7. *For any real numbers $\alpha > 0$, $M, N < \sqrt{x}$ and complex numbers β_m, γ_n with $|\beta_m| \le 1, |\gamma_n| \le 1$,*

$$\sum_{\substack{mn\le x\\ m>M, n>N}} \beta_m\gamma_n e(\alpha\sqrt{mn}) \ll x^{3/4} + \alpha^{-1/2}x^{3/4}(\log x)^{3/2} + (\alpha^{1/2}+\alpha^{-1/4})x(M^{-1/4}+N^{-1/4}) + \alpha^{1/4}x^{9/8}(M^{-1/2}+N^{-1/2}) + MN + \alpha^{1/2}x^{5/8}\log x.$$

Proof. We have

$$\sum_{\substack{mn\le x\\ m>M, n>N}} \beta_m\gamma_n e(\alpha\sqrt{mn}) = \sum_{N<n\le\sqrt{x}} \gamma_n \sum_{mn\le x} \beta_m e(\alpha\sqrt{mn}) + \sum_{M<m\le\sqrt{x}} \beta_m \sum_{mn\le x} \gamma_n e(\alpha\sqrt{mn}) + \sum_{m\le M, n\le N} \beta_m\gamma_n e(\alpha\sqrt{mn}) - \sum_{m\le\sqrt{x}, n\le\sqrt{x}} \beta_m\gamma_n e(\alpha\sqrt{mn}).$$

If $\frac{\sqrt{x}}{N}$ is an integer power of 2, then for the first sum, by Lemma 8.5.6,

$$\begin{aligned}
&\sum_{N<n\le\sqrt{x}} \gamma_n \sum_{mn\le x} \beta_m e(\alpha\sqrt{mn})\\
&\ll \sum_{N<n<\sqrt{x}} \left| \sum_{mn\le x} \beta_m e(\alpha\sqrt{mn}) \right|\\
&\ll \sum_{k=1}^{\log_2\frac{\sqrt{x}}{N}} \sum_{2^{k-1}N<n\le 2^kN} \left| \sum_{mn\le x} \beta_m e(\alpha\sqrt{mn}) \right|\\
&\ll \sum_{k=1}^{\log_2\frac{\sqrt{x}}{N}} \left((2^kN)^{1/2}x^{1/2} + \alpha^{-1/2}x^{3/4}(\log x)^{1/2} + (\alpha^{1/2}+\alpha^{-1/4})x(2^kN)^{-1/4} + \alpha^{1/4}x^{9/8}(2^kN)^{-1/2} \right)\\
&\ll x^{3/4} + \alpha^{-1/2}x^{3/4}(\log x)^{1/2}\log\sqrt{x} + (\alpha^{1/2}+\alpha^{-1/4})xN^{-1/4} + \alpha^{1/4}x^{9/8}N^{-1/2}\\
&\ll x^{3/4} + \alpha^{-1/2}x^{3/4}(\log x)^{3/2} + (\alpha^{1/2}+\alpha^{-1/4})xN^{-1/4} + \alpha^{1/4}x^{9/8}N^{-1/2}.
\end{aligned}$$

If $\frac{\sqrt{x}}{N}$ is not an integer power of 2, then we can slightly decrease the size of N such that $\frac{\sqrt{x}}{N}$ is an integer power of 2, and the bound we get will only be increased by multiplying an absolute constant. So we always have

$$\sum_{N<n\le\sqrt{x}} \gamma_n \sum_{mn\le x} \beta_m e(\alpha\sqrt{mn}) \ll x^{3/4} + \alpha^{-1/2}x^{3/4}(\log x)^{3/2} + (\alpha^{1/2}+\alpha^{-1/4})xN^{-1/4} + \alpha^{1/4}x^{9/8}N^{-1/2}.$$

Similarly, for the second sum, we have

$$\sum_{M<m\le\sqrt{x}}\beta_m\sum_{mn\le x}\gamma_n e(\alpha\sqrt{mn})\ll x^{3/4}+\alpha^{-1/2}x^{3/4}(\log x)^{3/2}+(\alpha^{1/2}+\alpha^{-1/4})xM^{-1/4}+\alpha^{1/4}x^{9/8}M^{-1/2}$$

For the third sum, the trivial estimate gives

$$\sum_{m\le M,n\le N}\beta_m\gamma_n e(\alpha\sqrt{mn})\ll MN.$$

For the last sum, using Lemma 8.5.5 and a similar argument as above (depending on whether $\lceil\sqrt{x}\rceil$ is a power of 2),

$$\begin{aligned}\sum_{m\le\sqrt{x},n\le\sqrt{x}}\beta_m\gamma_n e(\alpha\sqrt{mn})&\ll\sum_{2^k\le\sqrt{x},2^l\le\sqrt{x}}\Big|\sum_{2^{k-1}<m\le 2^k}\sum_{2^{l-1}<n\le 2^l}\beta_m\gamma_n e(\alpha\sqrt{mn})\Big|\\&\ll\sum_{2^k\le\sqrt{x},2^l\le\sqrt{x}}\big(2^{k+l/2}+2^{k/4+3l/4}\alpha^{-1/2}(\log\sqrt{x})^{1/2}+2^{5l/4}\alpha^{1/2}\big)\\&\ll x^{3/4}+\alpha^{-1/2}x^{1/2}(\log x)^{1/2}+\alpha^{1/2}x^{5/8}\log x.\end{aligned}$$

Therefore,

$$\begin{aligned}\sum_{\substack{mn\le x\\ m>M,n>N}}\beta_m\gamma_n e(\alpha\sqrt{mn})&\ll x^{3/4}+\alpha^{-1/2}x^{3/4}(\log x)^{3/2}+(\alpha^{1/2}+\alpha^{-1/4})x(M^{-1/4}+N^{-1/4})\\&\quad+\alpha^{1/4}x^{9/8}(M^{-1/2}+N^{-1/2})+MN+\alpha^{1/2}x^{5/8}\log x.\end{aligned}$$

□

Now we are ready to prove the main estimate in this section.

Proof of Theorem 8.5.1. Without loss of generality, we can assume $\alpha>0$. Let y,z be positive real numbers less than $\sqrt{x}$, to be determined. By Vaughan's identity,

$$\begin{aligned}\sum_{n\le x}e(\alpha\sqrt{n})\Lambda(n)&=\sum_{\substack{n\le x\\ b|n\\ b\le y}}\mu(b)e(\alpha\sqrt{n})\log\frac{n}{b}-\sum_{\substack{n\le x\\ bc|n\\ b\le y,c\le z}}\mu(b)\Lambda(c)e(\alpha\sqrt{n})\\&\quad+\sum_{\substack{n\le x\\ bc|n\\ b>y,c>z}}\mu(b)\Lambda(c)e(\alpha\sqrt{n})+O\Big(\sum_{n\le z}\Lambda(n)\Big).\end{aligned}$$

The last sum is $\sum_{n\le z}\Lambda(n)\ll z\ll\sqrt{x}$. For the first sum, by setting $l=\frac{n}{b}$, we obtain

$$\sum_{\substack{n\le x\\ b|n\\ b\le y}}\mu(b)e(\alpha\sqrt{n})\log\frac{n}{b}=\sum_{\substack{bl\le x\\ b\le y}}\mu(b)e(\alpha\sqrt{bl})\log l$$
$$\ll\sum_{b\le y}\Big|\sum_{l\le x/b}e(\alpha\sqrt{bl})\log l\Big|\ll_\alpha x^{1/2}\log x\log y+y^{3/2}\log x,$$

where we used Lemma 8.5.4 in the last step. For the second sum, by setting $l=\frac{n}{bc}$, we obtain

$$\sum_{\substack{n\le x\\ bc|n\\ b\le y,c\le z}}\mu(b)\Lambda(c)e(\alpha\sqrt{n})=\sum_{\substack{bcl\le x\\ b\le y,c\le z}}\mu(b)\Lambda(c)e(\alpha\sqrt{bcl})$$
$$\ll\sum_{b\le y,c\le z}|\mu(b)\Lambda(c)|\Big|\sum_{l\le x/bc}e(\alpha\sqrt{bcl})\Big|$$
$$\ll\sum_{b\le y,c\le z}\Big|\sum_{l\le x/bc}e(\alpha\sqrt{bcl})\Big|\Lambda(c)\ll\sum_{b\le y,c\le z}\Lambda(c)\big(x^{1/2}(bc)^{-1}+(bc)^{1/2}\big),$$

where we used Corollary 8.5.3 in the last step. Finally, by partial summation,

$$\sum_{\substack{n\le x\\ bc|n\\ b\le y,c\le z}}\mu(b)\Lambda(c)e(\alpha\sqrt{n})\ll_\alpha x^{1/2}\log y\log z+(yz)^{3/2}.$$

For the third sum, by setting $l=\frac{n}{bc}$ and $k=cl$, we get

$$\sum_{\substack{n\le x\\ bc|n\\ b>y,c>z}}\mu(b)\Lambda(c)e(\alpha\sqrt{n})=\sum_{\substack{bcl\le x\\ b>y,c>z}}\mu(b)\Lambda(c)e(\alpha\sqrt{bcl})=\sum_{\substack{bk\le x\\ b>y,k>z}}\mu(b)e(\alpha\sqrt{bk})\Big(\sum_{\substack{c|k\\ c>z}}\Lambda(c)\Big).$$

Note that

$$\sum_{\substack{c|k\\ c>z}}\Lambda(c)\le\sum_{c|k}\Lambda(c)=(\Lambda*1)(k)=\log k\le\log x,$$

and so

$$\sum_{\substack{n\le x\\ bc|n\\ b>y,c>z}}\mu(b)\Lambda(c)e(\alpha\sqrt{n})=\log x\sum_{\substack{bk\le x\\ b>y,k>z}}\mu(b)\gamma_k e(\alpha\sqrt{bk}),$$

where $\gamma_k = \frac{1}{\log x}\sum_{\substack{c|k\\ c>z}} \Lambda(c)$. Since $|\mu(b)| \le 1, |\gamma_k| \le 1$, Lemma 8.5.7 implies

$$\sum_{\substack{n\le x\\ bc|n\\ b>y,c>z}} \mu(b)\Lambda(c)e(\alpha\sqrt{n}) \ll_\alpha x^{3/4}(\log x)^{5/2} + x(y^{-1/4}+z^{-1/4})\log x + x^{9/8}(y^{-1/2}+z^{-1/2})\log x + yz\log x.$$

combining the three bounds we obtained above and setting $y, z = x^{1/3-\epsilon}$, where $\epsilon \in (0, 1/3)$, we conclude that

$$\begin{aligned}\sum_{n\le x} e(\alpha\sqrt{n})\Lambda(n) &\ll_\alpha x^{1/2}\log x\log y + y^{3/2}\log x + x^{1/2}\log y\log z + (yz)^{3/2} + x^{3/4}(\log x)^{5/2}\\ &\quad + x(y^{-1/4}+z^{-1/4})\log x + x^{9/8}(y^{-1/2}+z^{-1/2})\log x + yz\log x\\ &\ll_\alpha x^{1-3\epsilon} + x^{3/4}(\log x)^{5/2} + x^{11/12+\epsilon/4}\log x + x^{23/24+\epsilon/2}\log x\\ &\ll_\alpha x^{1-3\epsilon} + x^{23/24+\epsilon/2}\log x.\end{aligned}$$

If we let $\epsilon = 1/84$, then the sum is $\ll_\alpha x^{27/28}\log x$. □

8.6 Equdistribution of polynomial-like sequences on $\mathcal{P}$

The following technical theorem is a generalization of what did in the last section. The basic idea is to use Vaughan's identity, but the proof is mainly based on a very delicate argument in Heath-Brown's paper [55].

Theorem 8.6.1 (Lemma 2.3 in [10]). *Assume $F(x)$ to be any function defined on the real line, supported on $[N/2, N]$ and bounded in absolute value by F_0. Let further U, V, Z be any parameters satisfying $3 \le U < V < Z < N$, $Z \ge 4U^2$, $N \ge 64Z^2U$, $V^3 \ge 32N$ and $Z - \frac{1}{2} \in \mathbb{N}$. Then*

$$\left|\sum_n \Lambda(n)F(n)\right| \ll K\log N + F_0 + L(\log N)^8,$$

where the summation over n is restricted to the interval $[N/2, N]$, and K and L are defined by

$$K = \max_M \sum_{m=1}^{\infty} d_3(m)\left|\sum_{Z<n\le M} F(mn)\right|,$$
$$L = \sup \sum_{m=1}^{\infty} d_4(m)\left|\sum_{U<n<V} b(n)F(mn)\right|,$$

where the supremum is taken over all arithmetic functions $b(n)$ satisfying $|b(n)| \le d_3(n)$.

The following theorem provides a useful estimate for exponential sums on polynomial-like functions. The proof is based on Theorem 8.4.9 and induction.

Theorem 8.6.2 (Theorem 2.9 in [42]). *Let $m \geq 0$ be an integer and $X \in \mathbb{N}$. Suppose that $f(x)$ has $(m+2)$ continuous derivatives on an interval $I \subset (X, 2X]$. Assume also that there is some constant G such that*

$$|f^{(r)}(x)| \asymp GX^{-r} \tag{8.5}$$

on I for $r = 1, \ldots, m+2$. Then

$$\left|\sum_{x \in I} e(f(x))\right| \ll G^{\frac{1}{4M-2}} X^{1-\frac{m+2}{4M-2}} + \frac{X}{G},$$

where $M = 2^m$ and the implicit constant in $\ll$ depends only on m and on the implicit constants in $\asymp$ of equation (8.5).

Using Theorem 8.6.1 and Theorem 8.6.2, together with a few technical estimates, Bergelson et al. [10] established the following equidistribution result on polynomial-like sequences on $\mathcal{P}$.

Theorem 8.6.3 (Proposition 2.1 in [10]). *Let $P(x)$ be a polynomial of degree k, and let $f(x) = \sum_{j=1}^{r} d_j x^{\theta_j}$ with $r \geq 1$, $d_r \neq 0$, d_j real, $0 < \theta_1 < \theta_2 < \cdots < \theta_r$ and $\theta_j \notin \mathbb{Z}^+$. Assume that $l < \theta_r < l+1$ for some l. Let $1 \leq |m| \leq N^{1/10}$. Then*

$$\left|\sum_{p \leq N} e(mf(p) + mP(p))\right| \lll N^{1-\frac{1}{3K}} + \frac{N}{(mN^{\theta_r})^{1/K}} + N^{1-\frac{1}{64KL^5-4K}} + N^{1-1/10},$$

where $K = 2^k$ and $L = 2^l$.

Theorem 8.6.4 (Theorem 2.1 in [10]). *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 the sequence $\big(\xi(p)\big)_{p \in \mathcal{P}}$ is equdistributed.*

Proof. If all $\theta_j \in \mathbb{N}$, then $\xi(x)$ is a polynomial and at least one coefficient α_j is irrational. Then by Theorem 8.3.11, $\big(\xi(p)\big)_{p \in \mathcal{P}}$ is equdistributed modulo 1.

If at least one $\theta_j \notin \mathbb{N}$. Then the function $\xi(x)$ can be rewritten as $f(x) + P(x)$ as in Theorem 8.6.3, namely, $P(x)$ is a polynomial and $f(x) = \sum_{j=1}^{r} d_j x^{\theta_j}$ with $r \geq 1$, $d_r \neq 0$, d_j real, $0 < \theta_1 < \cdots < \theta_r$ and $\theta_j \notin \mathbb{N}$, so $\big(\xi(p)\big)_{p \in \mathcal{P}}$ is equdistributed. □

Corollary 8.6.5 (Corollary 2.1 in [10]). *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 $\big(\xi(p-h)\big)_{p \in \mathcal{P}}$ is equdistributed modulo 1.*

Proof. Fix $h \in \mathbb{Z}$. Note that if $k < \theta < k+1$, where k is a non-negative integer, then by Lagrange's theorem, there are $a_1, a_2, \cdots, a_k$ and $g(x)$ such that

$$(x-h)^\theta = x^\theta + a_1 x^{\theta-1} + \cdots + a_k x^{\theta-k} + g(x) \quad \text{where } \lim_{x \to \infty} g(x) = 0.$$

Therefore, $\xi(x-h)=\sum_{j=1}^{m}\alpha_j(x-h)^{\theta_j}$ can be written as the sum of $\tilde{\xi}(x)+G(x)$, where $\tilde{\xi}(x)$ is of the required form as in Theorem 8.6.4 and $\lim_{x\to\infty}G(x)=0$. Then the result follows from Theorem 8.6.4 and Lemma 8.1.2. □

For any two positive integers a and b, we define $\mathcal{P}_{a,b}=\mathcal{P}\cap(a\mathbb{Z}+b)$. In [10, Corollary 2.3], a stronger version of Theorem 8.6.5 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 [10]. For the sake of completeness, we prove the following version of Corollary 2.3 in [10].

Corollary 8.6.6. *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 Section 1.6 of [71]), it suffices to show that for each $(\beta_1,\beta_2,\ldots,\beta_m)\in\mathbb{Z}^m\setminus\{(0,0,\ldots,0)\}$,

$$\sum_{\substack{p\le x\\ p\equiv b \pmod a}} e\Big(\sum_{j=1}^{m}\beta_j\gamma_j(p-h)^{\theta_j}\Big)=o\Big(\frac{\pi(x)}{\phi(a)}\Big)=o\big(\pi(x)\big),\ \text{as } x\to\infty. \tag{8.6}$$

By orthogonality relations (Lemma 3.1.1),

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

It follows that

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

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

$$\xi_i(x):=\sum_{j=1}^{m}\beta_j\gamma_j x^{\theta_j}+\frac{i}{a}x=\sum_{\beta_j\neq0}\beta_j\gamma_j x^{\theta_j}+\frac{i}{a}x$$

is of the required form in Corollary 8.6.5 since $\beta_j\neq0$ 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 8.1.3 with $t=1$, as $x\to\infty$,

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

In particular, for any positive integer r, and any coprime positive integers a, b, Corollary 8.6.6 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 8.6.7. *For any positive integers r and d, the sequence $(p^{r-1/2})_{p\in\mathcal{Q}_{r,d}}$ is equdistributed modulo 1.*

8.7 Connection between the number of directions and the clique number

This section is based on Section 1 and Section 6 in [128].

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 [9]. In fact, it is straightforward to use Theorem 1.4.4 to recover the Hanson-Petridis bound (Theorem 1.5.1) by the following observation: if C is a clique of $P(p,d)$, 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 $|D|\le\frac{p-1}{\gcd(d,p-1)}+2$; combining this with the lower bound on $|D|$ given in Theorem 1.4.4, we can establish an upper bound on $|C|$.

It is clear that the same observation also works for $P(q,d)$. Since we have obtained a similar result on $AG(2,q)$, we can also apply Theorem 1.6.4 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 Theorem 1.6.1. In this section, we will employ a slightly complicated idea, together with the equidistribution result developed in the previous sections, to obtain improved bounds on $\omega\big(P(q,d)\big)$.

By Theorem 1.6.4, we can deduce the following information about the clique number.

Theorem 8.7.1. *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 $N=\omega\big(P(q,d)\big)$ of the generalized Paley graph $P(q,d)$ 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 1.3.4 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 $P(q,d)$ 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 1.6.4, 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 formed 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 8.7.1 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 8.6.7 and Theorem 8.7.1 to prove Theorem 1.6.3.

Theorem 1.6.3. *Let h be a positive function such that $h(x) = o(x)$ as $x \to \infty$. Let r, d be positive integers such that $d \ge 3$. Then $\omega\big(P(p^{2r+1}, d)\big) \le p^{r+1/2} - h(p)$ for almost all $p \in \mathcal{Q}_{r,d}$.*

Proof. 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 8.7.1, 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

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

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 $p \in \mathcal{Q}_{r,d}$. $\square$

Bibliography

[1] N. Alon. *Combinatorial Nullstellensatz*. Comb. Probab. Comput. **8** (1999), 7-29.

[2] N. Alon. *Ramsey properties of Cayley graphs*. `http://garden.irmacs.sfu.ca/op/ramsey_properties_of_cayley_graphs`

[3] N. Alon, V. Rödl. *Sharp bounds for some multicolor Ramsey numbers*. Combinatorica **25** (2005), no. 2, 125–141.

[4] B. Alspach, *Point-symmetric graphs and digraphs of prime order and transitive permutation groups of prime degree*. J. Combinatorial Theory Ser. B **15** (1973), 12–17.

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

[6] N.C. Ankeny. *The least quadratic non residue*. Ann. of Math. (2) **55** (1952), 65–72.

[7] T. M. Apostol. *Introduction to analytic number theory*. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976. xii+338 pp.

[8] C. Bachoc, M. Matolcsi, I. Z. Ruzsa. *Squares and difference sets in finite fields*. Integers **13** (2013), Paper No. A77, 5 pp.

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

[10] V. Bergelson, G. Kolesnik, M. Madritsch, Y. Son, 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.

[11] A. Blokhuis. *On subsets of* $GF(q^2)$ *with square differences*. Nederl. Akad. Wetensch. Indag. Math. **46** (1984), no. 4, 369–372.

[12] J. Bourgain, C. Demeter, L. Guth. *Proof of the main conjecture in Vinogradov's Mean Value Theorem for degrees higher than three.* Ann. of Math. (2) **184** (2016), no. 2, 633–682.

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

[14] A. E. Brouwer. *Paley graphs*. `https://www.win.tue.nl/~aeb/drg/graphs/Paley.html`.

[15] C. A. Bruni. *Least Quadratic Non-residue and least primitive root*. Manuscript, 2011. `https://www.math.ubc.ca/~gerg/teaching/613-Winter2011/LeastQuadraticNonResidue.pdf`

[16] D. A. Burgess. *The distribution of quadratic residues and non-residues*. Mathematika **4** (1957), 106–112.

[17] D.A. Burgess. *On character sums and primitive roots*. Proc. London Math. Soc. **12** (1962), 179-192.

[18] J. P. Burling, S. W. Reyner. *Some lower bounds of the Ramsey numbers* $n(k,k)$. J. Combin. Theory Ser. B **13** (1972), 168–169.

[19] R. Canetti, J. Friedlander, S. Konyagin, M. Larsen, D. Lieman, I. Shparlinski. *On the statistical properties of Diffie-Hellman distributions*. Israel J. Math. **120** (2000), part A, 23–46.

[20] L. Carlitz. *A theorem on permutations in a finite field*. Proc. Amer. Math. Soc. **11** (1960) 456–459.

[21] C. R. J. Clapham. *A class of self-complementary graphs and lower bounds of some Ramsey numbers*. J. Graph Theory **3** (1979), no. 3, 287–289.

[22] M. C. Chang. *On a question of Davenport and Lewis and new character sum bounds in finite fields,* Duke Math. J. **145**:3 (2008), 409–442.

[23] F. R. K. Chung. *Several generalizations of Weil sums*. J. Number Theory **49** (1994), no. 1, 95–106.

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

[25] J. G. van der Corput. *Verschärfung der Abschätzung beim Teilerproblem* (German). Math. Ann. **87** (1922), no. 1-2, 39–65.

[26] J. G. van der Corput. *Diophantische Ungleichungen. I. Zur Gleichverteilung Modulo Eins*. (German) Acta Math. **56** (1931), 373–456.

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

[28] M. L. Dawsey, D. McCarthy. *Generalized Paley graphs and their complete subgraphs of orders three and four*. arXiv:2006.14716(2020).

[29] P. Deligne. *La conjecture de Weil. I.* (French) Inst. Hautes Études Sci. Publ. Math. No. 43 (1974), 273–307.

[30] P. Delsarte. *An algebraic approach to the association schemes of coding theory*. Philips Res. Rep. Suppl. 1973, no. 10, vi+97 pp.

[31] 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).

[32] A. N. Elsawy. *Paley Graphs and Their Generalizations*. Master's thesis, Heinrich Heiner University (2009). arXiv:1203.1818.

[33] P. Erdős, G. Szekeres. *A combinatorial problem in geometry*. Compositio Math. **2** (1935),463-470.

[34] P. Erdős, H. N. Shapiro. *On the least primitive root of a prime*. Pacific J. Math. **7** (1957), 861–865.

[35] P. Erdős. *Remarks on number theory. I.* (Hungarian) Mat. Lapok **12** (1961), 10–17.

[36] P. Erdős, A. Rényi. *Asymmetric graphs*. Acta Math. Acad. Sci. Hungar. **14** (1963), 295–315.

[37] G. Exoo. *Clique Numbers for Small Paley Graphs*. `http://cs.indstate.edu/ge/Paley/cliques.html`.

[38] A. Farrugia. *Self-complementary graphs and generalisations: a comprehensive reference manual*. Master's thesis, University of Malta (1999).

[39] R. P. Flowe, G . A. Harris. *A note on generalized Vandermonde determinants*. SIAM J. Matrix Anal. Appl. **14** (1993), no. 4, 1146–1151.

[40] V. R. Fridlender. *On the least nth-power non-residue*. (Russian) Doklady Akad. Nauk SSSR (N.S.) **66**, (1949). 351–352.

[41] R. Fröberg, B. Shapiro. *Vandermonde varieties and relations among Schur polynomials*. arXiv:1302.1298 (2013).

[42] S. W. Graham, G. Kolesnik. *van der Corput's method of exponential sums*. London Mathematical Society Lecture Note Series, 126. Cambridge University Press, Cambridge, 1991.

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

[44] S. Graham, C. Ringrose. *Lower bounds for least quadratic non-residues*. Analytic Number Theory: Proceedings of a Conference in Honor of Paul T. Bateman, 269-309 (1990).

[45] R. L. Graham, J. H. Spencer. *A constructive solution to a tournament problem*. Canad. Math. Bull. **14** (1971), 45–48.

[46] G. Greaves, L. H. Soicher. *On the clique number of a strongly regular graph*. Electron. J. Combin. **25** (2018), no. 4, Paper No. 4.15, 15 pp.

[47] R. E. Greenwood, A. M. Gleason. *Combinatorial relations and chromatic graphs.* Canad. J. Math. **7** (1955), 1–7.

[48] C. Godsil, G. Royle. *Algebraic graph theory.* Graduate Texts in Mathematics, 207. Springer-Verlag, New York, 2001. xx+439 pp.

[49] B. Green. *Counting sets with small sumset, and the clique number of random Cayley graphs.* Combinatorica **25** (2005), no. 3, 307–326.

[50] B. Green, R. Morris. *Counting sets with small sumset and applications.* Combinatorica **36** (2016), no. 2, 129–159.

[51] F. Guldan, P. Tomasta. *New lower bounds of some diagonal Ramsey numbers.* J. Graph Theory **7** (1983), 149–151.

[52] A. M. Güloğlu, M. R. Murty. *The Paley graph conjecture and Diophantine m-tuples.* J. Combin. Theory Ser. A **170** (2020), 105155, 9 pp.

[53] B. Hanson, G. Petridis. *Refined estimates concerning sumsets contained in the roots of unity.* arXiv:1905.09134 (2019). To appear on Proc. London Math. Soc.

[54] D. R. Heath-Brown. *Prime numbers in short intervals and a generalized Vaughan identity.* Canadian J. Math. **34** (1982), no. 6, 1365–1377.

[55] D. R. Heath-Brown. *The Pjateckiĭ-Šapiro prime number theorem.* J. Number Theory **16** (1983), no. 2, 242-266.

[56] E. R. Heineman. *Generalized Vandermonde determinants.* Trans. Amer. Math. Soc. **31** (1929), no. 3, 464–476.

[57] H. Iwaniec, E. Kowalski. *Analytic Number Theory.* American Mathematical Society Colloquium Publications, 53. American Mathematical Society, Providence, RI, 2004. xii+615 pp.

[58] G. Jones. *Paley and the Paley graphs.* Isomorphisms, Symmetry and Computations in Algebraic Graph Theory, Springer Proceedings in Mathematics & Statistics, vol 305, Springer, Cham, 155-183.

[59] G. Kalai. *The largest clique in the Paley Graph: unexpected significant progress and surprising connections.* Manuscript, 2020. `https://gilkalai.wordpress.com/2020/02/08/the-largest-clique-in-the-paley-graph-unexpected-significant-progress-and-surprising-conne`

[60] A. A. Karatsuba. *The distribution of values of Dirichlet characters on additive sequences,* Soviet Math. Dokl., **44**:1 (1992), 145–148.

[61] A. A. Karatsuba. *Distribution of power residues and non-residues in additive sequences,* Soviet Math. Dokl., **11** (1970), 235–236.

[62] A. A. Karatsuba. *Arithmetic problems in the theory of Dirichlet characters,* Russian Math. Surveys **63** (2008), no. 4, 641–690.

[63] R. Karp. *Reducibility among combinatorial problems.* Complexity of computer computations (Proc. Sympos., IBM Thomas J. Watson Res. Center, Yorktown Heights, N.Y., 1972), pp. 85–103. Plenum, New York, 1972.

[64] M. Karpinski, I. Shparlinski. *On some approximation problems concerning sparse polynomials over finite fields.* Theoret. Comput. Sci. **157** (1996), 259-266.

[65] N. M. Katz. *Sommes exponentielles.* (French) Course taught at the University of Paris, Orsay, Fall 1979. With a preface by Luc Illusie. Notes written by Gérard Laumon. With an English summary. Astérisque, 79. Société Mathématique de France, Paris, 1980. 209 pp.

[66] Z. Kelley. *Roots of Sparse Polynomials over a Finite Field.* LMS J. Comput. Math. **19** (2016), 196-204.

[67] Z. Kelley, S. Owen. *Estimating the Number Of Roots of Trinomials over Finite Fields.* J. Symbolic Comput. **79** (2017), 108-118.

[68] J. D. Key, B. G. Rodrigues. *Special LCD codes from Peisert and generalized Peisert graphs.* Graphs Combin. **35** (2019), no. 3, 633–652.

[69] A. Kisielewicz, W. Peisert. *Pseudo-random properties of self-complementary symmetric graphs.* J. Graph Theory **47** (2004), no. 4, 310–316.

[70] M. Klin, N. Kriger, A. Woldar. *On the existence of self-complementary and nonself-complementary strongly regular graphs with Paley parameters.* J. Geom. **107** (2016), 329–356.

[71] L. Kuipers, H. Niederreiter. *Uniform Distribution of Sequences.* Pure and Applied Mathematics. Wiley-Interscience [John Wiley & Sons], New York-London-Sydney, 1974. xiv+390 pp.

[72] Y. Lamzouri, X. Li, K. Soundararajan. *Conditional bounds for the least quadratic non-residue and related problems.* Math. Comp. **84** (2015), no. 295, 2391–2412.

[73] R. Lidl, H. Niederreiter. *Finite Fields*, second edition. Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1997. xiv+755 pp.

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

[75] J. Limbupasiriporn. *Binary codes from Paley graphs of prime-power-square order.* Discrete Math. **342** (2019), no. 12, 111588, 12 pp.

[76] U. V. Linnik. *A remark on the least quadratic non-residue.* C. R. (Doklady) Acad. Sci. URSS (N.S.) **36** (1942), 119–120.

[77] E. Maistrelli, D. B. Penman. *Some colouring problems for Paley graphs*. Discrete Math. **306** (2006), no. 1, 99–106.

[78] G. Martin, A. Parvardi. *Subproducts of small residue classes*. arXiv:2008.10198 (2020).

[79] K. McGown, E. Treviño. The least quadratic non-residue. Manuscript, 2019. `http://campus.lakeforest.edu/trevino/SurveyLeastNonResidue.pdf`

[80] I. D. Meir. *Simultaneous solutions to diagonal equations over the p-adic numbers and finite fields, and some connections with combinatorics*. Ph.D. thesis, University of Sheffield (1997).

[81] M. Michałek. *A short proof of combinatorial Nullstellensatz*. Amer. Math. Monthly **117** (2010), no. 9, 821–823.

[82] H. L. Montgomery. *Topics in multiplicative number theory*. Lecture Notes in Mathematics, Vol. 227. Springer-Verlag, Berlin-New York, 1971. ix+178 pp.

[83] H. L. Montgomery, R. C. Vaughn. *Exponential sums with multiplicative coefficients*. Invent. Math **43** (1977), 69-82.

[84] H. L. Montgomery. *Ten lectures on the interface between analytic number theory and harmonic analysis*. CBMS Regional Conference Series in Mathematics, 84. American Mathematical Society, Providence, RI, 1994. xiv+220 pp.

[85] H. L. Montgomery, R. C. Vaughn. *Multiplicative number theory. I. Classical theory*. Cambridge Studies in Advanced Mathematics, 97. Cambridge University Press, Cambridge, 2007. xviii+552 pp.

[86] L.J. Mordell. *On the Kusmin-Landau inequality for exponential sums*. Acta Arith. **4** (1958), 3–9.

[87] J. Morris. *Automorphism groups of circulant graphs—a survey*. Graph theory in Paris, 311–325, Trends Math., Birkhäuser, Basel, 2007.

[88] J. Morris. *Lecture notes on Cayley graphs and digraphs*. Manuscript, 2020.

[89] R. Mrazović. *A random model for the Paley graph*. Q. J. Math. **68** (2017), no. 1, 193–206.

[90] D. Mubayi, J. Verstraete. *A note on pseudorandom Ramsey graphs*. arXiv:1909.01461 (2019).

[91] N. Mullin. *Self-complementary arc-transitive graphs and their imposters*. Master's thesis, University of Waterloo (2009).

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

[93] R. E. A. C. Paley. *A theorem on characters*. J. London Math. Soc. **7** (1932), 28-32.

[94] R. E. A. C. Paley. *On orthogonal matrices*. J. Math. and Phys. **12** (1933), 311–320.

[95] W. Peisert. *Direct product and uniqueness of automorphism groups of graphs*. Discrete Math. **270** (1999), no. 1-3, 189–197.

[96] W. Peisert, *All Self-Complementary Symmetric Graphs*. J. Algebra **240** (2001), no. 1, 209–229.

[97] F. P. Ramsey. *On a Problem of Formal Logic*. Proc. London Math. Soc. (2) **30** (1929), 264-286.

[98] L. Rédei. *Lacunary polynomials over finite fields*. Translated from the German by I. Földes. North-Holland Publishing Co., Amsterdam-London; American Elsevier Publishing Co., Inc., New York, 1973. x+257 pp.

[99] G. Rhin. *Sur la répartition modulo* 1 *des suites* $f(p)$. (French) Acta Arith. **23** (1973), 217–248.

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

[101] H. Sachs. *Über selbstkomplementäre Graphen*. (German) Publ. Math. Debrecen **9** (1962), 270–288.

[102] B. Sagan. *The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions*. Graduate texts in mathematics, 203. Springer-Verlag New York, 2001.

[103] A. Sah. *Diagonal Ramsey via effective quasirandomness*. arXiv:2005.09251 (2020).

[104] H. Salie. *Über den kleinsten positiven quadratischen Nichtrest nach einer Primzahl*. (German) Math. Nachr. **3** (1949), 7–8.

[105] S. Satake. *On the restricted isometry property of the Paley matrix*. arXiv:2011.02907 (2020).

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

[107] I. Schur. *Einige Bemerkungen zu der vorstehenden Arbeit des Herrn G. Polya: Über die Verteilung der quadratischen Reste und Nichtreste*. (German) Goettingen Nachr (1918), 30-36.

[108] J. Schwartz. *Fast Probabilistic Algorithms for Verification of Polynomial Identities*. J. Assoc. Comput. Mach. **27** (1980), no. 4, 701–717.

[109] I. D. Shkredov. *Sumsets in quadratic residues*. Acta Arith. **164** (2014), no. 3, 221–243.

[110] I. Shparlinski. *On the singularity of generalised Vandermonde matrices over finite fields*. Finite Fields Appl. **11** (2005), no. 2, 193–199.

[111] J. Solymosi. *Clique number of Paley graphs*. Manuscript, 2020.

[112] J. Solymosi, E. P. White, C. H. Yip. *On the number of distinct roots of a lacunary polynomial over finite fields*. arXiv:2008.09962 (2020).

[113] P. Stevenhagen, H.W. Lenstra Jr. *Chebotarëv and his density theorem*. Math. Intelligencer **18** (1996), no. 2, 26–37.

[114] T. Szőnyi. *On the Number of Directions Determined by a Set of Points in an Affine Galois Place*. J. Combin. Theory, Ser. A **74** (1996), no. 1, 141-146.

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

[116] T. Tao. *An uncertainty principle for cyclic groups of prime order*. Math. Res. Lett. **12** (2005), no. 1, 121–127.

[117] A. Thomason. *Random graphs, strongly regular graphs and pseudorandom graphs*. Surveys in combinatorics 1987, 173–195, London Math. Soc. Lecture Note Ser., 123, Cambridge Univ. Press, Cambridge, 1987.

[118] W. T. Tutte. *The factorization of linear graphs*. J. London Math. Soc. **22** (1947), 107–111.

[119] I. M. Vinogradov. *Representation of an odd number as the sum of three primes*. Dokl. Akad. Nauk SSSR **15** (1937), 291–294.

[120] A. S. Volostnov. On double sums with multiplicative characters. Math. Notes **104** (2018), no. 1-2, 197–203.

[121] Y. Wang. *A note on the least primitive root of a prime*. Sci. Record (N.S.) **3** (1959), 174-179.

[122] G. Weng, W. Qiu, Z. Wang, Q. Xiang. *Pseudo-Paley graphs and skew Hadamard difference sets from presemifields*. Des. Codes Cryptogr. **44** (2007), no. 1-3, 49–62.

[123] H. Weyl. *Über die Gleichverteilung von Zahlen mod. Eins.*(German) Math. Ann. **77** (1916), 313–352.

[124] T. D. Wooley. *The cubic case of the main conjecture in Vinogradov's mean value theorem*. Adv. Math. **294** (2016), 532–561.

[125] T. D. Wooley. *Nested efficient congruencing and relatives of Vinogradov's mean value theorem*. Proc. Lond. Math. Soc. (3) **118** (2019), no. 4, 942–1016.

[126] C. Z. Xu, K. Wu, W. Z. Liang, H. Chen, W. L. Su. *New method for computing lower bounds for diagonal Ramsey numbers with Paley graphs*. (Chinese) J. Math. (Wuhan) **32** (2012), no. 3, 547–555.

[127] C. H. Yip. *On the Clique Number of Paley Graphs of Prime Power Order*. arXiv:2004.01175 (2020).

[128] C. H. Yip. *On the directions determined by Cartesian products and the clique number of generalized Paley graphs*. arXiv:2010.01784 (2020).

[129] C. H. Yip. *Vinogradov's Mean Value Conjecture*. Manuscript, 2020. `https://drive.google.com/file/d/15WtAhVM0WUUXKRhvfnC0HhCWtfzOP_cL/view`

[130] H. Zhang. *Self-complementary symmetric graphs*. J. Graph Theory **16**, no.1 (1992), 1–5.