PALEY AND PEISERT GRAPHS OVER FINITE FIELDS, AND THEIR GENERALIZATIONS

ANWITA BHOWMIK

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI
GUWAHATI - 781039, INDIA

DECEMBER 2023

Paley and Peisert graphs over finite fields, and their generalizations

by

Anwita Bhowmik

Roll No. 186123003

Department of Mathematics

submitted in fulfillment of the requirements of the degree of Doctor of Philosophy

to the

Indian Institute of Technology Guwahati
Guwahati - 781039, India

December 2023

This work is dedicated

to

my family

Certificate

This is to certify that the thesis entitled **"Paley and Peisert graphs over finite fields, and their generalizations"** submitted by **Ms. Anwita Bhowmik** to the **Indian Institute of Technology Guwahati**, for the award of the Degree of **Doctor of Philosophy**, is a record of the original bona fide research work carried out by her under my guidance and supervision. The thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted in part or full to any other university or institute for the award of any degree or diploma.

Date: 13th December, 2023
Guwahati, India

Prof. Rupam Barman
Professor
Department of Mathematics
Indian Institute of Technology Guwahati

Acknowledgements

First and foremost, I express my deepest gratitude to my supervisor, *Prof. Rupam Barman,* for his invaluable guidance, unflinching support and constant encouragement throughout my journey. I must admit that I was not the easiest student to deal with, and I am grateful to him for being patient with me, motivating me and pushing me to be better. His strong work ethic and professionalism have inspired me to develop as a person and a researcher.

I am sincerely thankful to the members of my doctoral committee, *Prof. Anupam Saikia*, *Prof. K. V. Krishna* and *Prof. Sukanta Pati,* for reviewing my research work periodically and giving valuable suggestions. I have received many constructive comments from my doctoral committee, which have helped my research.

I want to take the pleasure of thanking *Prof. Ken Ono* for introducing me to the world of Paley graphs, which worked as a starting point for this thesis. I am also grateful to him for providing some insightful comments about my work. I express my sincere gratitude to *Prof. Ronald Evans* and *Prof. M. R. Pournaki* for their helpful suggestions.

I am grateful to the Indian Institute of Guwahati (IITG) for providing me with various facilities to conduct my research. I take this opportunity to thank all the faculty members of the Department of Mathematics, IITG. I feel delighted to have learnt from various academic courses and to have been a part of multiple teaching

opportunities, seminars, conferences and workshops. I am also thankful to the MHRD for providing me with the financial assistance for my work.

I thank all my friends and colleagues that I got to know during my stay at the IITG. I am happy to thank my dear seniors and colleagues at the IITG, Dr. Neelam, Dr. Chiranjit, Dr. Nilanjan, Dr. Mohit, Dr. Shamik, Dr. Jaitra, Dr. Ajit, Deepa, Laxmi, Sulakashna and Gurinder for their support. My special thanks go to Rohit, Susmoy, Subhajit, Subho, Balasubramannyan, Pronay *da*, Sourav *da*, Anil *bhaiyya* and Aritra for being such awesome friends and for always being there for me.

Finally, I wholeheartedly thank my family: my parents and my brother. I am grateful to my late paternal aunt *Boro Pishi*, maternal aunt *Tatapata*, maternal grandmother *Didibhai*, late paternal grandmother *Thakuma* and cousin *Guddu*. No words are enough to describe the unconditional love and support I have received from all of them, and I am indebted to them for always having my back.

Date: 13th December, 2023

Guwahati, India Anwita Bhowmik

Abstract

This thesis is mainly devoted to the computation of the number of cliques of certain Cayley graphs, namely the *Paley-type graphs, Peisert graphs* and *Peisert-like graphs*. Barring the case of the Peisert graphs, the focus is on the number of cliques of orders three (triangles) and four. Let q be a prime power such that $q \equiv 1 \pmod 4$. The Paley graph of order q is the graph with vertex set as the finite field $\mathbb{F}_q$ and edges defined as, ab is an edge if and only if $a-b$ is a non-zero square in $\mathbb{F}_q$. The first part of this thesis involves defining a generalization of the Paley graph, called the Paley-type graph on the commutative ring $\mathbb{Z}_n$ for certain values of n, precisely $n = 2^s p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $s = 0$ or 1, $\alpha_i \geq 1$, where the distinct primes p_i satisfy $p_i \equiv 1 \pmod 4$ for all $i = 1, \ldots, k$. For such n, we define the graph with vertex set $\mathbb{Z}_n$ and edges defined as, ab is an edge if and only if $a-b$ is a square in the set of units of $\mathbb{Z}_n$. We look at some properties of this graph. For primes $p \equiv 1 \pmod 4$, Evans, Pulham and Sheehan computed the number of complete subgraphs of order four in the Paley graph. Recently, Dawsey and McCarthy found the number of triangles and complete subgraphs of order four in the generalized Paley graph of prime power order. We find the number of triangles and complete subgraphs of order four in the Paley-type graph successively for $n = p^\alpha$ ($p \equiv 1 \pmod 4$ being a prime and $\alpha \geq 1$) and for general n, using character sums and combinatorial methods.

A graph is called symmetric if its automorphism group acts transitively both on

the vertices and edges. Another kind of symmetry occurs if a graph is isomorphic to its complement, in which case the graph is called self-complementary. It turns out that the Paley graphs are both self-complementary and symmetric (SCS). Peisert gave a full description of SCS graphs as well as their automorphism groups. He derived that there is another infinite family of SCS graphs apart from the Paley graphs, and in addition, one more graph not belonging to any of the two former families. The graphs in the infinite family that he discovered are now known as Peisert graphs. The second part of the thesis is devoted to the computation of the number of cliques in the Peisert graph. We find the number of triangles and cliques of order four and express them using finite field hypergeometric functions as developed by Greene, McCarthy and Ono, which are assembled with the well known Gauss and Jacobi sums. Then, we provide an asymptotic result on the number of cliques of order $m \geq 1$ in the graph.

The final part of the thesis involves defining a Peisert-like graph analogous to the Peisert graph and exploring some of its properties. We follow in the footsteps of Greene and define hypergeometric functions corresponding to Dirichlet characters. Then, using these functions, we find the number of triangles and cliques of order four in the Peisert-like graph.

Contents

Introduction

Graph theory is the study of graphs, which are abstract mathematical structures modeling pairwise relations among a set of objects. It is a useful tool in mathematics, computer science, electrical engineering, economics and other areas galore. A (simple) graph is a pair $G = (V, E)$, where V is a set whose elements are called vertices, and E is a set of pairs of distinct vertices whose elements are called edges. Cayley graphs are a well known family of graphs, see for example [28]. These graphs are defined on groups and are a central tool in combinatorial and geometric group theory.

Graphs exhibiting some form of symmetry spike the interest to delve into them. To this end, the Paley graphs have, since their inception, piqued the interest of many. Paley graphs are a special class of Cayley graphs that enjoy a variety of properties. As Jones [36] puts it, "Anyone who seriously studies algebraic graph theory or finite permutation groups will, sooner or later, come across the Paley graphs and their automorphism groups". Named after Raymond E. A. C. Paley, they were introduced as graphs independently by Sachs [51] in 1962, and Erdős and Rényi [25] in 1963. While Sachs studied the self-complementarity properties of the Paley graphs, Erdős and Rényi were interested in their symmetries. Paley graphs are defined in the following way. Let q be a prime power such that $q \equiv 1 \pmod 4$ and let $\mathbb{F}_q$ denote the finite field with q elements. The Paley graph of order q is the graph

with vertex set $\mathbb{F}_q$, where ab is an edge if $a-b$ is a non-zero square in $\mathbb{F}_q$. They are closely related to the Paley construction for constructing Hadamard matrices from quadratic residues, as stated in Paley's paper [47] in 1933. Remarkably, the study of this family of graphs connects many branches of mathematics such as combinatorics, number theory, group theory, graph theory, design theory, matrix theory and coding theory. One can refer to [36] for a presentation on the origin of Paley graphs and a survey on them.

A complete graph is one in which every pair of distinct vertices are adjacent. In combinatorial mathematics, Ramsey's theorem, in one of its graph-theoretic forms, states that, given c number of colors and positive integers $n_1, \ldots, n_c$, there is a number $R(n_1, \ldots, n_c)$ such that if the edges of a complete graph on $R(n_1, \ldots, n_c)$ vertices are colored with c different colors, then for some i, $1 \leq i \leq c$, it must contain a complete subgraph (clique) of order n_i whose edges are all colored i. For $c = 2$, the only values of m for which the diagonal Ramsey number $R(m, m)$ are known are $m \leq 4$. Now, let $G^{(n)}$ denote a graph on n vertices and let $\overline{G^{(n)}}$ be the complement of $G^{(n)}$. For a graph G, let $\mathcal{K}_m(G)$ denote the number of cliques of order m contained in G. Then, let $T_m(n) := \min\left(\mathcal{K}_m(G^{(n)}) + \mathcal{K}_m(\overline{G^{(n)}})\right)$, where the minimum is taken over all graphs $G^{(n)}$. Here we note that the study of $T_m(n)$ can be linked to Ramsey theory. This is because $R(m, m)$ is the smallest positive integer n such that $T_m(n)$ is positive. Erdős [24] proved that

$$T_m(n) \leq \frac{\binom{n}{m}}{2^{\binom{m}{2}-1}}$$

and conjectured that $\lim_{n\to\infty} T_m(n)/\binom{n}{m} = 2^{1-\binom{m}{2}}$. Subsequent attempts by Goodman [29] and Thomason [55] generated the interest to calculate $T_m(n)$ for different $m \in \mathbb{N}$.

Computing $T_m(n)$ in turn, put the focus on Paley graphs. Indeed, for the function $\mathcal{K}_m(G^{(n)}) + \mathcal{K}_m(\overline{G^{(n)}})$ on graphs with $n = p$ vertices, p being a prime, it turns out that Paley graphs are minimal in certain ways. For example, in order to show that

$R(4,4)$ is at least 18, the Paley graph with 17 vertices acts as the only graph (upto isomorphism) such that $\mathcal{K}_4(G^{(17)}) + \mathcal{K}_4(\overline{G^{(17)}}) = 0$. It is also seen that, although the conjecture given by Erdős is false in general, it holds true for Paley graphs. As a result, there has been an acute interest in computing the number of cliques in Paley graphs and some generalizations of these graphs. Character sums have been extensively used to study cliques in these graphs, for instance see [26, 57]. In view of such work, the first part of the thesis involves defining a generalization called the *Paley-type graph* on the commutative ring $\mathbb{Z}_n$ for some particular values of n, investigating some of its properties and finding the number of cliques of orders three (triangles) and four therein, using two different methods: a Dirichlet character sum approach and a combinatorial one.

It is natural to study the extent to which a graph exhibits symmetry. A graph is called symmetric if its automorphism group acts transitively both on the vertices and edges. Another kind of symmetry occurs if a graph is isomorphic to its complement, in which case the graph is called self-complementary. It turns out that the Paley graphs are both self-complementary and symmetric (SCS), see for example [23]. Thus arose a quest for the classification of all SCS graphs. In 2001, Peisert gave a full description of SCS graphs as well as their automorphism groups in [49]. Using elaborate algebraic techniques, he derived that there is another infinite family of SCS graphs apart from the Paley graphs, and in addition, one more graph not belonging to any of the two former families. The graphs in the infinite family that he discovered are now known as Peisert graphs. A similarity in the definitions of the Paley graphs and Peisert graphs has led to numerous studies of the latter in the same flavour as that of the former, for example in [1, 39, 53, 58]. The second part of the thesis is mainly devoted to the computation of the number of triangles and cliques of order four in the Peisert graph and expressing them using finite field hypergeometric functions as developed by Greene, McCarthy, and Ono [32, 33, 42, 46], which are assembled with the well known Gauss and Jacobi sums.

The final part of the thesis involves defining a *Peisert-like graph* analogous to the Peisert graph and exploring some of its properties. We follow in the footsteps of Greene [32, 33] and define hypergeometric functions corresponding to Dirichlet characters. Then, using these functions, we find the number of triangles and cliques of order four in the Peisert-like graph.

There have been a number of studies on cliques of maximum (and maximal) size in the Paley, Peisert, generalized Paley and generalized Peisert graphs, some of which are [7, 44, 58, 59, 60]. The generalizations of Paley and Peisert graphs in the existing literature are cyclotomic graphs, that is, Cayley graphs with the connection set being the union of cyclotomic classes (a reference for cyclotomic graphs is [15]). Cyclotomic graphs are of special interest in both algebraic graph theory and number theory; in particular, character sums and Gauss sums have been used extensively to study these graphs. With respect to clique(s) in a graph, one can study the size of a largest clique; alternatively, one can find the number of cliques of a particular order. In this thesis, we focus on computing the number of cliques of a particular order in the Paley-type, Peisert and Peisert-like graphs, following the likes of [11, 16, 21, 26, 30] etc.

Organization of the Thesis

We present the entire work of the thesis in eight chapters as described below.

- Chapter 1: Preliminaries
- Chapter 2: On a Paley-type graph on $\mathbb{Z}_n$
- Chapter 3: Triangles in the Paley-type graph
- Chapter 4: Cliques of order four in the Paley-type graph on $\mathbb{Z}_{p^\alpha}$
- Chapter 5: Cliques of order four in the Paley-type graph on $\mathbb{Z}_n$ for general n

- Chapter 6: The number of cliques in Peisert graphs
- Chapter 7: Hypergeometric functions for Dirichlet characters
- Chapter 8: On a Peisert-like graph on $\mathbb{Z}_n$

In Chapter 1, we will recall some preliminary definitions and results on the group of units of the commutative ring $\mathbb{Z}_n$; finite fields; characters on finite abelian groups and some character sums associated with finite fields, namely Jacobi sums and hypergeometric functions; and graphs.

In Chapter 2, we define a generalization of the Paley graph on $\mathbb{Z}_n$, namely the *Paley-type graph* G_n. We study some properties of the graph and also associate some character sums with it.

In Chapter 3, we compute the number of triangles in G_n. First, we consider the case $n = p^\alpha$ for a prime $p \equiv 1 \pmod 4$ and a positive integer α. Then, we find the number of triangles in G_n for general n.

In Chapter 4, we evaluate the number of cliques of order four in G_{p^α} for a prime $p \equiv 1 \pmod 4$ and a positive integer α. We express the result in terms of Jacobi sums on Dirichlet characters modulo p^α.

In Chapter 5, we obtain an expression for the number of cliques of order four in G_n without involving Jacobi sums. Hence, combining this expression and the one we obtained in Chapter 4, we find values of certain character sums modulo p^α which were earlier known for prime modulus only.

In Chapter 6, we find the number of cliques in the Peisert graph using character sums. First, we provide a new proof for computing the number of triangles. Next, we express the number of cliques of order four in the graph using finite field hypergeometric functions. This involves some tedious computations on character sums. To overcome the difficulty in this method, we provide an asymptotic result on the number of cliques of order $m \geq 1$, in the graph.

In Chapter 7, we define hypergeometric functions corresponding to Dirichlet

characters modulo p^α for an odd prime p and a positive integer α. The following is the motivation behind doing so. In Chapter 8, we introduce a Peisert-like graph. To find the number of cliques of order four in the Peisert-like graph, we need to evaluate certain character sums involving Dirichlet characters. Our goal is to find $\mathbb{Z}_{p^\alpha}$-analogues of transformations satisfied by Greene's finite field hypergeometric functions as given in [32, 33]. Then, these transformations will be used to study Peisert-like graphs.

In Chapter 8, we define a generalization of the Peisert graph on $\mathbb{Z}_n$ and name it the *Peisert-like graph* $G(n)$. After studying some basic properties of the graph, we provide results on the number of triangles and cliques of order four in this graph, while making use of the hypergeometric functions defined in Chapter 7.

1 Preliminaries

In this chapter, we recall some necessary definitions and results from the literature. First, we provide some algebraic background on the group of units of the commutative ring $\mathbb{Z}_n$ as well as finite fields. Then, we state some results about characters and some of their known sums. Finally, we provide some basics on graph theory.

Before we proceed, we adopt the following notation for this thesis.

(i) n denotes a positive integer, p denotes a prime, q denotes a power of a prime.

(ii) For a set S, the number of elements in S is denoted by $|S|$.

(iii) Let z be a complex number. Then $\bar{z}, |z|, \mathrm{Re}(z), \mathrm{Im}(z)$ denote the complex

conjugate, modulus, real part and imaginary part of z, respectively.

(iv) ϕ denotes the Euler's totient function, so $\phi(n)$ counts the number of positive integers less than or equal to n that are relatively prime to n. If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the prime factorization of $n > 1$, then $\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$. This result can be found in any classical text on number theory, for example in [35, Prop. 2.2.5.].

(v) For non-negative integers a and b, $\binom{a}{b}$ denotes the classical binomial coefficient.

(vi) $\mathcal{G}$ denotes a group. Let $g \in \mathcal{G}$. Then,

- The order of g is denoted by $o(g)$,
- $\langle g \rangle := \{g^k : k \in \mathbb{Z}\}$, and
- $\mathcal{G}^n := \{x^n : x \in \mathcal{G}\}$. Note that if $\mathcal{G}$ is abelian then $\mathcal{G}^n$ becomes a subgroup of $\mathcal{G}$.

(vii) The set of units in a ring R with unity is denoted by R^*. Note that R^* forms a group under multiplication.

1.1 Some algebraic background

In this section, we provide some results on the structure of $\mathbb{Z}_n^*$, solutions of congruences modulo n and the Chinese remainder theorem. Then, we give a classification of finite fields. The results we state can be found in [22, 35].

1.1.1 Structure of $\mathbb{Z}_n^*$ and the Chinese remainder theorem

We begin by observing the cyclicity of $\mathbb{Z}_n^*$ as a group. The following famous result is due to Gauss. We shall recall this result in the thesis multiple times.

Proposition 1.1. [35, Proposition 4.1.3] *Let n be a positive integer and let $\mathbb{Z}_n^*$ denote the multiplicative group of units of $\mathbb{Z}_n$. Then, $\mathbb{Z}_n^*$ is cyclic if and only if $n = 2, 4, p^\alpha$ or $2p^\alpha$, where p is an odd prime and α is a positive integer.*

The following result sheds light on the structure of $\mathbb{Z}_n^*$ when n is a power of 2 and $n \neq 2, 4$.

Theorem 1.2. [35, Theorem 2′] *Let $n \geq 3$, and let $\mathbb{Z}_{2^n}^*$ denote the multiplicative group of units of $\mathbb{Z}_{2^n}$. Then,*

$$\mathbb{Z}_{2^n}^* = \{(-1)^x 5^y : x = 0, 1 \text{ and } 0 \leq y < 2^{n-2}\}.$$

It follows that $\mathbb{Z}_{2^n}^*$ is the direct product of two cyclic groups, one of order 2, the other of order 2^{n-2}.

Next, we observe the existence of solutions of congruences modulo 2^e for an integer $e \geq 3$.

Proposition 1.3. [35, Proposition 4.2.2] *Suppose that n is a positive integer, a is an odd integer and $e \geq 3$, and consider the congruence $x^n \equiv a \pmod{2^e}$. If n is odd, a solution always exists and is unique. If n is even, a solution exists if and only if $a \equiv 1 \pmod 4$, $a^{\frac{2^{e-2}}{d}} \equiv 1 \pmod{2^e}$, where $d = \gcd(n, 2^{e-2})$; when a solution exists, there are exactly $2d$ solutions.*

Finally, we shall state the Chinese remainder theorem for rings, and consequently have some corollaries. First, we present some terminology in ring theory.

Notation 1.4. *Let R_1 and R_2 be rings such that they are isomorphic. Then we write $R_1 \cong R_2$.*

Notation 1.5. *Let R be a commutative ring with identity $1 \neq 0$. The product AB, of the ideals A and B of R, is the ideal consisting of all finite sums of elements of the form xy, where $x \in A$ and $y \in B$.*

Definition 1.6 (Comaximal ideals)**.** *Let R be a commutative ring with identity $1 \neq 0$. The ideals A and B of R are said to be comaximal if $A + B = R$.*

The following theorem is known as the Chinese remainder theorem for rings.

Theorem 1.7. [22, Chapter 7, Theorem 17] *Let $A_1, A_2, \ldots, A_k$ be ideals of a commuative ring R with identity $1 \neq 0$. The map*

$$R \to R/A_1 \times R/A_2 \times \cdots \times R/A_k \text{ defined by } r \mapsto (r + A_1, r + A_2, \ldots, r + A_k)$$

is a ring homomorphism with kernel $A_1 \cap A_2 \cap \cdots \cap A_k$. If for each $i, j \in \{1, 2, \ldots, k\}$ with $i \neq j$ the ideals A_i and A_j are comaximal, then this map is onto and $A_1 \cap A_2 \cap \cdots \cap A_k = A_1 A_2 \cdots A_k$, so

$$R/(A_1 A_2 \cdots A_k) = R/(A_1 \cap A_2 \cap \cdots \cap A_k) \cong R/A_1 \times R/A_2 \times \cdots \times R/A_k.$$

We have the following corollary to the above theorem, which provides the structure of $\mathbb{Z}_n^*$ as a group.

Corollary 1.7.1. [22, Chapter 7, Corollary 18] *Let n be a positive integer and let $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be its factorization into powers of distinct primes. Then $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}$ as rings, so in particular we have the following isomorphism of multiplicative groups:*

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{\alpha_1}}^* \times \mathbb{Z}_{p_2^{\alpha_2}}^* \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}^*.$$

As a corollary, we have the following result which is immediate from the statement of the theorem.

Corollary 1.7.2. [22, Chapter 7, Exercise 5(a)] *Let $n_1, \ldots, n_k$ be integers which are pairwise coprime, that is, $\gcd(n_i, n_j) = 1$ if $i \neq j$. Then, for $a_1, \ldots, a_k \in \mathbb{Z}$ there is a solution $x \in \mathbb{Z}$ to the system of congruences*

$$x \equiv a_1 \pmod{n_1}, \cdots, x \equiv a_k \pmod{n_k}.$$

Moreover, the solution is unique modulo $n_1 \cdots n_k$.

We also obtain the well known result that ϕ is a multiplicative function.

Corollary 1.7.3. [22, p. 267] *Let* n *be a positive integer and let* $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *be its factorization into powers of distinct primes. Then* $\phi(n) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \cdots \phi(p_k^{\alpha_k})$.

1.1.2 Structure of finite fields

The following result provides a classification of all finite fields.

Theorem 1.8. [22, p. 549, Example: (Existence and Uniqueness of Finite Fields)] *Any finite field has order* p^n*, where* p *is a prime and* n *is a positive integer. Moreover, for any prime* p *and positive integer* n*, finite fields of order* p^n *exist and are unique upto isomorphism.*

Notation 1.9. *For a prime power* q*,* $\mathbb{F}_q$ *denotes the finite field with* q *elements.*

Proposition 1.10. [22, Chapter 9, Proposition 18] *A finite subgroup of the multiplicative group of a field is cyclic. In particular, if* $\mathbb{F}_q$ *is a finite field whose order is a prime power* q*, then the multiplicative group* $\mathbb{F}_q^*$ *of non-zero elements of* $\mathbb{F}_q$ *is a cyclic group.*

$\mathbb{F}_q^*$ is cyclic, so let g be a generator of $\mathbb{F}_q^*$, that is $\mathbb{F}_q^* = \langle g \rangle$. Then g is called a *primitive element* of $\mathbb{F}_q$. Using the above proposition, we also obtain the following.

Corollary 1.10.1. *Let* q *be a prime power and let* $\mathbb{F}_q$ *denote the finite field with* q *elements. Then,* $a \in \{x^2 : x \in \mathbb{F}_q^*\}$ *if and only if* $a^{\frac{q-1}{2}} = 1$.

Definition 1.11 (k-th power residue)**.** *Let* q *be a prime power. For the finite field* $\mathbb{F}_q$ *and a positive integer* k*, an element of* $(\mathbb{F}_q^*)^k$ *is called a* k*-th power residue.*

For $k = 2, 3, 4$, an element of $(\mathbb{F}_q^*)^k$ is called a quadratic residue, a cubic residue and a quartic residue, respectively.

1.2 Multiplicative characters and some associated character sums

In this section, we introduce characters, Jacobi sums and hypergeometric functions over finite fields. We state some related results. The definitions of characters and Jacobi sums can be found in classical texts related to number theory, for example in [6, 35]. The definition of hypergeometric functions that we provide is due to Greene [32, 33].

1.2.1 Characters

Characters serve as an integral tool in number theory.

Definition 1.12 (Multiplicative Character)**.** *A multiplicative character (or character) on a finite abelian group $\mathcal{G}$ is a group homomorphism from $\mathcal{G}$ to the multiplicative group of non-zero complex numbers.*

Definition 1.13 (Character group/Group of characters)**.** *Let $\mathcal{G}$ be a finite abelian group. The set of characters on $\mathcal{G}$ becomes a group under multiplication defined as $(\psi\chi)(a) := \psi(a)\chi(a)$ for $a \in \mathcal{G}$, where ψ and χ are two characters on $\mathcal{G}$. This group is known as the character group of $\mathcal{G}$.*

Notation 1.14. *The character group of $\mathcal{G}$ is denoted by $\widehat{\mathcal{G}}$. The identity of $\widehat{\mathcal{G}}$ (which takes all elements of $\mathcal{G}$ to 1) is denoted by ε. For a character ψ, its inverse is denoted by $\overline{\psi}$; for $a \in \mathcal{G}$, $\overline{\psi}(a) = \overline{\psi(a)}$.*

Definition 1.15 (Order of a character)**.** *Let $\mathcal{G}$ be a finite abelian group with its group of characters $\widehat{\mathcal{G}}$. Then the order of a character is its order as an element in $\widehat{\mathcal{G}}$.*

A character of order 2 is called a *quadratic character*. On the finite field $\mathbb{Z}_p$, the Legendre symbol, denoted by $\left(\frac{\cdot}{p}\right)$, is the unique quadratic character. The following theorem characterizes $\widehat{\mathcal{G}}$ in terms of $\mathcal{G}$.

Theorem 1.16. [19, Theorem 3.13] *If $\mathcal{G}$ is a finite abelian group, then its character group $\widehat{\mathcal{G}}$ is isomorphic to $\mathcal{G}$. In particular, if $\mathcal{G}$ is finite and cyclic, then so is $\widehat{\mathcal{G}}$.*

As a corollary to Proposition 1.1 and Theorem 1.16, we have the following result which we shall use extensively in our work.

Proposition 1.17. *Let p be an odd prime and let α be a positive integer. For $n = p^\alpha$ and $n = 2p^\alpha$, $\widehat{\mathbb{Z}_n^*}$ contains a unique character of order 2. Moreover, if $p \equiv 1 \pmod 4$ then there exist exactly two distinct characters of order 4.*

Theorem 1.18. [19, Theorem 3.15 (b)] *Let $\mathcal{G}$ be a finite abelian group and let $g \in \mathcal{G}$. Let $m \in \mathbb{Z}$. Then, g is an m-th power in $\mathcal{G}$ if and only if $\psi(g) = 1$ for every $\psi \in \widehat{\mathcal{G}}$ satisfying $\psi^m = \varepsilon$.*

Following are two useful identities, famously known as orthogonal identities.

Theorem 1.19. [6, Theorem 6.10] *Let $\mathcal{G}$ be a finite abelian group with character group $\widehat{\mathcal{G}}$. Let $\psi \in \widehat{\mathcal{G}}$. Then,*

$$\sum_{x \in \mathcal{G}} \psi(x) = \begin{cases} |\mathcal{G}|, & \text{if } \psi = \varepsilon; \\ 0, & \text{if } \psi \neq \varepsilon. \end{cases}$$

Theorem 1.20. [6, Theorem 6.13] *Let $\mathcal{G}$ be a finite abelian group with identity $e_{\mathcal{G}}$, and character group $\widehat{\mathcal{G}}$. Let $x \in \mathcal{G}$. Then,*

$$\sum_{\psi \in \widehat{\mathcal{G}}} \psi(x) = \begin{cases} |\mathcal{G}|, & \text{if } x = e_{\mathcal{G}}; \\ 0, & \text{if } x \neq e_{\mathcal{G}}. \end{cases}$$

Remark 1.21. *If $\mathcal{G} = \mathbb{F}_q^*$ then one extends every $\psi \in \widehat{\mathbb{F}_q^*}$ to $\mathbb{F}_q$ by setting $\psi(0) := 0$.*

The following lemma is stated in [13] in the paragraph preceding Theorem 3.3.1. It will be used in the proof of one of the main results in Chapter 6.

Lemma 1.22. [13] *Let $p \equiv 1 \pmod 8$ and let ψ be a character modulo p of order 8. Then, $\psi(-4) = \pm 1$.*

On the way to proving the famous theorem on primes in arithmetic progressions, Dirichlet introduced what we now call Dirichlet characters.

Definition 1.23 (Dirichlet character)**.** *Let n be a positive integer. A function ψ from $\mathbb{Z}$ to $\mathbb{C}$ is called a Dirichlet character modulo n if it has the following properties:*

- $\psi(1) = 1$,
- $\psi(ab) = \psi(a)\psi(b) \quad \forall a, b \in \mathbb{Z}$,
- $\psi(a) = \psi(b)$ *if* $a \equiv b \pmod n$,
- $\psi(a) = 0$ *if* $\gcd(a, n) > 1$.

A Dirichlet character modulo n is essentially a character on the group $\mathcal{G} = \mathbb{Z}_n^*$. Weil gave a strong bound on the magnitude of a character sum; see [52]. We shall use the following deep result in our work to give an asymptotic result on the number of cliques in the Peisert graph.

Theorem 1.24 (Weil's estimate)**.** *Let $\mathbb{F}_q$ be the finite field of order q, and let ψ be a character of $\mathbb{F}_q$ of order $s > 1$. Let $f(x)$ be a polynomial of degree d over $\mathbb{F}_q$ such that $f(x)$ cannot be written in the form $c \cdot h(x)^s$, where $c \in \mathbb{F}_q$. Then*

$$\left| \sum_{x \in \mathbb{F}_q} \psi(f(x)) \right| \leq (d-1)\sqrt{q}.$$

1.2.2 Jacobi sums

Next, we define a type of character sum called the Jacobi sum. Defined generally in the case of finite fields, it is an analogue of the beta function. Such sums were introduced by Jacobi in connection with the theory of cyclotomy. The arithmetic properties of Jacobi sums have a very long history in number theory, with applications in Diophantine equations and the theory of L-functions.

Definition 1.25 (Jacobi sum)**.** *Let p be a prime, and let $\mathbb{F}_q$ be the finite field with q elements, where $q = p^r, r \geq 1$, and let ψ, χ be two multiplicative characters of $\mathbb{F}_q$. Then the Jacobi sum for ψ, χ is given by*

$$J(\psi, \chi) := \sum_{x \in \mathbb{F}_q} \psi(x)\chi(1-x).$$

The following result gives the magnitude of a Jacobi sum.

Theorem 1.26. [13, Theorem 2.1.3 (b)] *Let q be a prime power, and let χ and ψ be characters of $\mathbb{F}_q$ such that $\chi\psi$ is non-trivial. Then,*

$$|J(\chi, \psi)| = \sqrt{q}.$$

It is easy to see that any function $f : \mathbb{F}_q \to \mathbb{C}$ has a unique representation

$$f(x) = f(0) \cdot \delta(x) + \sum_{\psi \in \widehat{\mathbb{F}_q^*}} f_\psi \cdot \psi(x), \tag{1.1}$$

where

$$f_\psi = \frac{1}{q-1} \sum_{x \in \mathbb{F}_q} f(x) \cdot \overline{\psi}(x) \quad \text{and} \quad \delta(x) = \begin{cases} 1, & \text{if } x = 0; \\ 0, & \text{otherwise.} \end{cases}$$

A character sum analogue for the classical binomial theorem follows easily from (1.1) with $f(x) = A(1+x)$, where A is a multiplicative character on $\mathbb{F}_q$.

Theorem 1.27. [33, Theorem 2.3] *Let p be a prime, and let $\mathbb{F}_q$ denote the finite field with q elements, where $q = p^r, r \geq 1$. For any multiplicative character A of $\mathbb{F}_q$ and $x \in \mathbb{F}_q$, we have*

$$A(1+x) = \delta(x) + \frac{1}{q-1} \sum_{\psi \in \widehat{\mathbb{F}_q^*}} J(A, \overline{\psi})\psi(-x).$$

Thus, it is inferred from Theorem 1.27 that the Jacobi sum can be considered as the finite field analogue of the binomial coefficient.

Definition 1.28 (Binomial coefficient)**.** *Let p be a prime, and let $\mathbb{F}_q$ denote the finite field with q elements, where $q = p^r, r \geq 1$. For multiplicative characters A and B of $\mathbb{F}_q$, the binomial coefficient $\binom{A}{B}$ is defined by*

$$\binom{A}{B} := \frac{B(-1)}{q} J(A, \overline{B}).$$

Later on, in Chapter 7 we shall formally define the Jacobi sum and the binomial coefficient corresponding to Dirichlet characters too. Following are some useful relations among binomial coefficients, which are analogues of (2.6), (2.7) and (2.8) in [33].

Proposition 1.29. *Let p be a prime, and let $\mathbb{F}_q$ denote the finite field with q elements, where $q = p^r, r \geq 1$. For multiplicative characters A and B of $\mathbb{F}_q$, let $\binom{A}{B}$ denote the binomial coefficient. Then,*

$$\begin{aligned}
\binom{A}{B} &= \binom{A}{A\overline{B}}; \\
\binom{A}{B} &= \binom{\overline{A}B}{B} B(-1); \\
\binom{A}{B} &= \binom{\overline{B}}{\overline{A}} AB(-1).
\end{aligned}$$

Now, we state some results on Jacobi sums.

Theorem 1.30. [13, Theorem 2.1.4] *Let p be an odd prime, and let q be a positive power of p. If ψ is a non-trivial character of $\mathbb{F}_q$ and ϕ is the quadratic character of $\mathbb{F}_q$, then*

$$J(\psi, \phi) = \psi(4) J(\psi, \psi).$$

Theorem 1.31. [13, Theorem 2.1.5] *Let q be a prime power. If χ and ψ are characters of $\mathbb{F}_q$ with χ, ψ and $\chi\psi$ non-trivial, then*

$$J(\chi, \psi) = \psi(-1)J(\overline{\chi\psi}, \psi) = \chi(-1)J(\overline{\chi\psi}, \chi).$$

Theorem 1.32. [13, Theorem 2.1.6] *Let p be an odd prime and let q be a positive power of p. Let ϕ be the quadratic character of $\mathbb{F}_q$. Let ψ be a non-trivial character of $\mathbb{F}_q$ with $\psi \neq \phi$. Then,*

$$\phi(-1)J(\overline{\psi}\phi, \phi) = J(\psi, \phi) = \psi(-1)J(\psi, \overline{\psi}\phi).$$

In particular, if ψ has order $2j$, where $j > 1$, then

$$\phi(-1)J(\psi^{j-1}, \phi) = J(\psi, \phi) = \psi(-1)J(\psi, \psi^{j-1}).$$

The following theorem evaluates a character sum (commonly known as a *Jacobsthal sum*) in terms of Jacobi sums. We state its proof (as given in [12]) as well, since the method of proof shall be used to prove a result in Chapter 4.

Theorem 1.33. [12, Theorem 2.7] *Let n be a positive integer and let p be a prime such that $p \equiv 1 \pmod{2n}$. Let $\left(\frac{\cdot}{p}\right)$ be the Legendre symbol modulo p, and let ψ be a character modulo p of order $2n$. Let $a \in \mathbb{F}_p^*$. Then,*

$$\sum_{x \in \mathbb{Z}_p} \left(\frac{x}{p}\right)\left(\frac{x^n + a}{p}\right) = \psi(-1)\sum_{j=0}^{n-1} \psi^{n+2j+1}(a)J(\psi^{2j+1}, \psi^n).$$

Proof. ψ is of order $2n$, which implies that $\psi^n = \left(\frac{\cdot}{p}\right)$. We have

$$\sum_{x \in \mathbb{Z}_p} \left(\frac{x}{p}\right)\left(\frac{x^n + a}{p}\right) = \sum_{x \in \mathbb{Z}_p} \psi^n(x)\psi^n(x^n + a)$$

$$= \sum_{x\in\mathbb{Z}_p} \psi(x^n)\psi^n(x^n+a)$$
$$= \sum_{x\in\mathbb{Z}_p} \psi(x)\psi^n(x+a)\sum_{j=0}^{n-1}\psi^{2j}(x). \tag{1.2}$$

Using the substitution $x \mapsto -ax$, (1.2) yields

$$\sum_{x\in\mathbb{Z}_p}\left(\frac{x}{p}\right)\left(\frac{x^n+a}{p}\right) = \psi(-1)\psi^{n+1}(a)\sum_{x\in\mathbb{Z}_p}\psi(x)\psi^n(1-x)\sum_{j=0}^{n-1}\psi^{2j}(ax)$$
$$= \psi(-1)\psi^{n+1}(a)\sum_{j=0}^{n-1}\psi^{2j}(a)J(\psi^{2j+1},\psi^n).$$

This completes the proof. ■

The following results provide values of Jacobi sums in certain cases.

Theorem 1.34. [13, Theorem 2.1.8] *Let $q \equiv 1 \pmod 4$ be a prime power. Let ϕ be the quadratic character of $\mathbb{F}_q$ and let ψ be a character of $\mathbb{F}_q$ of order 4. Then,*

$$\frac{J(\psi,\phi)+q}{2(1-i)} \in \mathbb{Z}[i].$$

We state the next result along with its proof, since the method of proof will be used in proving a result later on, in Chapter 6.

Theorem 1.35. [12, Theorem 3.9; 13, Theorem 3.2.1] *Let $p \equiv 1 \pmod 4$ be a prime. Let ϕ be the quadratic character of $\mathbb{F}_p$ and let ψ be a character of $\mathbb{F}_p$ of order 4. Then,*

$$J(\psi,\phi) = a_4 + ib_4,$$

where a_4, b_4 are integers such that $a_4^2 + b_4^2 = p$ and $a_4 \equiv -(\frac{p+1}{2}) \pmod 4$.

Proof. Since $\psi(x) \in \mathbb{Z}[i]$ for each $x \in \mathbb{F}_p$, it follows that $J(\psi,\phi) = a_4 + ib_4$ for integers a_4 and b_4. Moreover, by Theorem 1.26, $a_4^2 + b_4^2 = p$. Further, by Theorem 1.34,

$\frac{a_4+ib_4+p}{2(1-i)} \in \mathbb{Z}[i]$ and so, 8 divides $|(a_4+p)+ib_4|^2 = a_4^2+b_4^2+p^2+2a_4p = p(p+1+2a_4)$, which implies $a_4 \equiv -(\frac{p+1}{2}) \pmod 4$. This completes the proof. ■

Proposition 1.36. [37, Proposition 1] *Let $p \equiv 3 \pmod 4$ and let $q \equiv 1 \pmod 4$ be a power of p. Let ψ be a character of $\mathbb{F}_q$ of order 4. Then the system of diophantine equations $q = s^2 + t^2$, $s \equiv 1 \pmod 4$ has a unique solution viz. $s = (-p)^{\frac{n}{2}}$, $t = 0$. For this solution, the Jacobi sum*

$$J(\psi, \psi) = -s + it.$$

Theorem 1.37. [13, Theorem 3.3.3] *Let $p \equiv 1 \pmod 8$ and let g be a primitive element of $\mathbb{F}_p$. Suppose that ϕ is the quadratic character on $\mathbb{F}_p$ and ψ is a character on $\mathbb{F}_p$ such that $\psi(g) = e^{\frac{2\pi i}{8}}$, a primitive 8-th root of unity. Then the Jacobi sum*

$$J(\psi, \psi^2) = \psi(-4)(a_4 + ib_4),$$

where a_4 and b_4 are integers such that $p = a_4^2 + b_4^2$ and $a_4 \equiv -\phi(2) \pmod 4$.

Remark 1.38. *It is noted in the proof of Lemma 3.6 (3) in [21] that Theorem 1.37 also holds if we replace a prime $p \equiv 1 \pmod 8$ by a prime power $q \equiv 1 \pmod 8$ and take any character ψ of $\mathbb{F}_q$ of order 8.*

Lemma 1.39. [21, Lemma 3.6 (2)] *Let $q \equiv 1 \pmod 8$ be a prime power and let ψ be a character of $\mathbb{F}_q$ of order 8. Write $q = u^2 + 2v^2$ for integers u and v, such that $u \equiv 3 \pmod 4$ and $p \nmid u$ when $p \equiv 1, 3 \pmod 8$. Then,*

$$Re(J(\psi, \psi)) = \psi(4)u.$$

1.2.3 Hypergeometric functions

Classical hypergeometric series have been studied for ages. There have been multiple works to establish relations between classical hypergeometric series and

different mathematical objects. In 1987, Greene [32, 33] introduced a finite field character sum analogue of classical hypergeometric series that satisfies summation and transformation formulae similar to the classical one. Here we recall these finite field hypergeometric functions.

Definition 1.40 (Hypergeometric function)**.** *Let p be a prime, and let $\mathbb{F}_q$ denote the finite field with q elements, where $q = p^r, r \geq 1$. For a positive integer n, and $A_0, \ldots, A_n, B_1, \ldots, B_n \in \widehat{\mathbb{F}_q^*}$, the ${}_{n+1}F_n$ finite field hypergeometric function over $\mathbb{F}_q$ is defined as*

$$ {}_{n+1}F_n\left(\begin{matrix} A_0, & A_1, & \ldots, & A_n \\ & B_1, & \ldots, & B_n \end{matrix}\Big| x\right) := \frac{q}{q-1}\sum_{\psi\in\widehat{\mathbb{F}_q^*}} \binom{A_0\psi}{\psi}\binom{A_1\psi}{B_1\psi}\cdots\binom{A_n\psi}{B_n\psi}\psi(x). $$

For $n = 2$, we recall the following result from [33, Corollary 3.14]:

$$ q^2\cdot {}_3F_2\left(\begin{matrix} A, & B, & C \\ & D, & E \end{matrix}\Big| 1\right) = \sum_{x,y\in\mathbb{F}_q} A\overline{E}(x)\overline{C}E(1-x)B(y)\overline{B}D(1-y)\overline{A}(x-y). $$

Lemma 1.41. [33, Theorem 3.13] *Let q be a power of a prime. For characters A_0, A_1, …, A_n, and $B_1, \ldots, B_n$ of $\mathbb{F}_q$ and $x \in \mathbb{F}_q$, we have*

$$ \begin{aligned} &{}_{n+1}F_n\left(\begin{matrix} A_0, & A_1, & \ldots, & A_n \\ & B_1, & \ldots, & B_n \end{matrix}\Big| x\right) \\ &= \frac{A_nB_n(-1)}{q}\sum_{y\in\mathbb{F}_q} {}_nF_{n-1}\left(\begin{matrix} A_0, & A_1, & \ldots, & A_{n-1} \\ & B_1, & \ldots, & B_{n-1} \end{matrix}\Big| xy\right) A_n(y)\overline{A_n}B_n(1-y). \end{aligned} $$

Theorem 1.42. [33, Theorem 4.37] *Let q be a power of a prime. Let ϕ be the quadratic character of $\mathbb{F}_q$. Let δ be the function defined on the group of characters of $\mathbb{F}_q$ as*

$$ \delta(A) = \begin{cases} 1, & \text{if } A \text{ is the trivial character;} \\ 0, & \text{otherwise.} \end{cases} $$

Then, for characters A, B and C of $\mathbb{F}_q$, we have

$$
\begin{aligned}
{}_3F_2\left(\begin{matrix} A, & B, & C \\ & \overline{A}C, & \overline{B}C \end{matrix}\Big|1\right) &= \frac{q-1}{q^2}BC(-1)\delta(A) \\
&\quad - \frac{q-1}{q^2}AC(-1)\delta(B) - \frac{q-1}{q^2}A(-1)\delta(\overline{AB}C) \\
&\quad + AB(-1)\begin{cases} 0, & \text{if } C \text{ is not a square}; \\ \binom{D}{A}\binom{B\overline{D}}{AB\overline{D}} + \binom{\phi D}{A}\binom{\phi B\overline{D}}{\phi AB\overline{D}}, & \text{if } C = D^2. \end{cases}
\end{aligned}
$$

Greene [32, 33] gave some transformation formulae which we state here as follows.

Theorem 1.43. [32, Theorems 5.14, 5.18 & 5.20],[33, Theorem 4.2 (i),(ii) and Equations (4.23)-(4.26)] *Let q be a power of a prime, and let A, B, C, D, E be characters of $\mathbb{F}_q$. Then, we have*

$$
{}_3F_2\left(\begin{matrix} A, & B, & C \\ & D, & E \end{matrix}\Big|1\right) = {}_3F_2\left(\begin{matrix} B\overline{D}, & A\overline{D}, & C\overline{D} \\ & \overline{D}, & E\overline{D} \end{matrix}\Big|1\right), \tag{1.3}
$$

$$
{}_3F_2\left(\begin{matrix} A, & B, & C \\ & D, & E \end{matrix}\Big|1\right) = ABCDE(-1)\cdot {}_3F_2\left(\begin{matrix} A, & A\overline{D}, & A\overline{E} \\ & A\overline{B}, & A\overline{C} \end{matrix}\Big|1\right), \tag{1.4}
$$

$$
{}_3F_2\left(\begin{matrix} A, & B, & C \\ & D, & E \end{matrix}\Big|1\right) = ABCDE(-1)\cdot {}_3F_2\left(\begin{matrix} B\overline{D}, & B, & B\overline{E} \\ & B\overline{A}, & B\overline{C} \end{matrix}\Big|1\right), \tag{1.5}
$$

$$
{}_3F_2\left(\begin{matrix} A, & B, & C \\ & D, & E \end{matrix}\Big|1\right) = AE(-1)\cdot {}_3F_2\left(\begin{matrix} A, & B, & E\overline{C} \\ & AB\overline{D}, & E \end{matrix}\Big|1\right), \tag{1.6}
$$

$$
{}_3F_2\left(\begin{matrix} A, & B, & C \\ & D, & E \end{matrix}\Big|1\right) = AD(-1)\cdot {}_3F_2\left(\begin{matrix} A, & D\overline{B}, & C \\ & D, & AC\overline{E} \end{matrix}\Big|1\right), \tag{1.7}
$$

$$
{}_3F_2\left(\begin{matrix} A, & B, & C \\ & D, & E \end{matrix}\Big|1\right) = B(-1)\cdot {}_3F_2\left(\begin{matrix} \overline{A}D, & B, & C \\ & D, & BC\overline{E} \end{matrix}\Big|1\right), \tag{1.8}
$$

$$
{}_3F_2\left(\begin{matrix} A, & B, & C \\ & D, & E \end{matrix}\Big|1\right) = AB(-1)\cdot {}_3F_2\left(\begin{matrix} \overline{A}D, & \overline{B}D, & C \\ & D, & DE\overline{AB} \end{matrix}\Big|1\right). \tag{1.9}
$$

1.3 Terminology in graph theory

This section deals with some basic definitions on finite graphs, and can be found in any standard text on graph theory, for example in [28, 34].

Definition 1.44 (Graph). *A (simple) graph is a pair $G = (V, E)$, where V is a finite set whose elements are called vertices, and E is a finite set of unordered pairs of distinct vertices whose elements are called edges.*

A graph is often represented pictorially by drawing a dot for each vertex, and joining two dots by a line if the corresponding vertices are adjacent.

Definition 1.45 (Adjacent vertices). *Let $G = (V, E)$ be a graph. For $u, v \in V$ if $(u, v) \in E$, then u and v are said to be adjacent in G, or uv forms an edge in G.*

Definition 1.46 (Degree of a vertex). *Let $G = (V, E)$ be a graph and $v \in V$. Then the degree of v, denoted by $deg(v)$, is the number of vertices adjacent to v.*

Definition 1.47 (Order of a graph). *Let $G = (V, E)$ be a graph. The number of elements in V is called the order of G.*

Definition 1.48 (Path in a graph). *A path in a graph is a sequence of distinct vertices such that two vertices are adjacent if they are consecutive in the sequence.*

If P is a path with the sequence $v_0, \ldots, v_n$ of vertices, we say that v_0 and v_n are connected by a path.

We define some particular cases of graphs.

Definition 1.49 (Complete graph). *A graph in which every pair of distinct vertices are adjacent is called a complete graph.*

Notation 1.50. *A complete graph on n vertices is denoted by K_n.*

Definition 1.51 (Complement of a graph). *The complement of a graph $G = (V, E)$ is the graph $\overline{G} = (V, \overline{E})$, where $(u, v) \in \overline{E}$ if and only if $(u, v) \notin E$.*

Definition 1.52 (Subgraph). *A graph $G_1 = (V_1, E_1)$ is called a subgraph of the graph $G = (V, E)$ if $V_1 \subseteq V$ and $E_1 \subseteq E$.*

We define some particular kinds of subgraphs.

Definition 1.53 (Induced subgraph). *A subgraph $G_1 = (V_1, E_1)$ of the graph $G = (V, E)$ is called an induced subgraph, if $(u, v) \in E$ with $u, v \in V_1$, then $(u, v) \in E_1$.*

Notation 1.54. *For a graph $G = (V, E)$ if $H \subseteq V$ then $\langle H \rangle$ denotes the subgraph of G induced by H.*

Definition 1.55 (Spanning subgraph). *A subgraph $G_1 = (V_1, E_1)$ of the graph $G = (V, E)$ is called a spanning subgraph if $V_1 = V$.*

Definition 1.56 (Complete subgraph/Clique). *A subgraph $G_1 = (V_1, E_1)$ of the graph $G = (V, E)$ is called a complete subgraph or a clique if every pair of distinct vertices in G_1 are adjacent.*

Notation 1.57. *For a graph G, we will denote the number of cliques of order ℓ in G by $\mathcal{K}_\ell(G)$. For a vertex u of G, we will denote the number of cliques of order ℓ in G containing u by $\mathcal{K}_\ell(G, u)$.*

Definition 1.58 (Clique number of a graph). *The order of a clique of maximum size contained in a graph is known as the clique number of the graph.*

We recall the following notation as given in [10, p. 2855].

Notation 1.59. *Let $G = (V, E)$ be a graph. If $\{G_i\}_{i \in I}$ is a family of edge-disjoint subgraphs of a graph G such that $E(G) = \cup_{i \in I} E(G_i)$, we write $G = \bigoplus_{i \in I} G_i$. In this case if $G_i \cong H$ for every $i \in I$, then we write $G = \bigoplus_{i \in I} H$.*

Definition 1.60 (Graph isomorphism; Graph automorphism). *Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be two graphs. A graph isomorphism between G_1 and G_2 is a bijection $f : V_1 \to V_2$ such that two vertices u and v of G_1 are adjacent in G_1 if and only if $f(u)$ and $f(v)$ are adjacent in G_2.*

A graph isomorphism from a graph onto itself is called a graph automorphism.

If two graphs are isomorphic, then they share the same graph properties and only differ by the labels of their vertices and edges. Thus, from a graph-theoretic point of view, two isomorphic graphs are essentially the same. The set of automorphisms on a graph G forms a group under the operation of composition of functions, and is denoted by $Aut(G)$.

1.3.1 Types of graphs

Now, we define some more properties of graphs, which may be satisfied by the graphs we will study.

Definition 1.61 (Connected graph)**.** *A graph is called connected if every two distinct vertices in the graph are connected by a path.*

Definition 1.62 (Regular graph)**.** *A graph is said to be regular if each vertex of the graph has the same degree.*

Definition 1.63 (Cycle/Cycle graph)**.** *A cycle is a connected graph in which each vertex has exactly two distinct vertices adjacent to it.*

Definition 1.64 (Self-complementary graph)**.** *A graph is said to be self-complementary if there exists a graph automorphism from the graph to its complement.*

Definition 1.65 (Vertex-transitive graph)**.** *A graph is called vertex-transitive if given any two vertices in the graph, there is a graph automorphism mapping one of the vertices to the other.*

Definition 1.66 (Edge-transitive graph)**.** *A graph is called edge-transitive if given any two edges in the graph, there exists a graph automorphism sending one edge to the other.*

Definition 1.67 (Symmetric graph)**.** *A graph which is both vertex-transitive and edge-transitive is known as a symmetric graph.*

The following definition of a graph given by Cayley [17] connects graphs and groups.

Definition 1.68 (Cayley graph)**.** *Let $\mathcal{G}$ be a group and let C be a subset of $\mathcal{G}$ that is closed under taking inverses and does not contain the identity. Then the Cayley graph associated with $\mathcal{G}$ and connection set C is the graph with vertex set $\mathcal{G}$, where gh forms an edge if $hg^{-1} \in C$.*

Finally, for the sake of completeness, we define the Paley graph.

Definition 1.69 (Paley graph)**.** *Let $q = p^r \equiv 1 \pmod 4$ be a prime power. Then the Paley graph $P(q)$ of order q is the graph with vertex set $\mathbb{F}_q$, where ab is an edge if $a - b \in (\mathbb{F}_q^*)^2$.*

It is thus the Cayley graph for the additive group of $\mathbb{F}_q$, with $(\mathbb{F}_q^*)^2$ as the connection set.

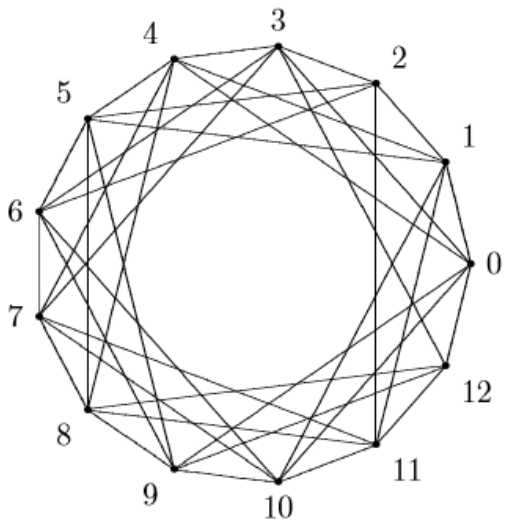

Figure 1.1: The Paley graph of order 13

2

On a Paley-type graph on $\mathbb{Z}_n$

2.1 Introduction

Paley graphs are well studied, and enjoy many properties. Researchers have attempted to attack problems on these graphs using various tools; implementing character sums is one of them which is widely used in the literature.

In the spirit of the Paley graph, some of its generalizations have been defined too. Ananchuen and Caccetta [3, 4, 5] studied some adjacency properties of the cubic and quadruple graphs. Let q be a power of an odd prime. Let $S_3 = \{x^3 : x \in \mathbb{F}_q^*\}$ and $S_4 = \{x^4 : x \in \mathbb{F}_q^*\}$. For $q \equiv 1 \pmod 3$, the graph with vertex set $\mathbb{F}_q$ and

[1]The contents of this chapter have been published in *Graphs Combin.* (2022).

edges ab, where $a - b \in S_3$ is called the cubic Paley graph. For $q \equiv 1 \pmod 8$, the graph with vertex set $\mathbb{F}_q$ and edges ab, where $a - b \in S_4$ is called the quadruple Paley graph. In 2006, Lim and Praeger [41] generalized further: let $k(\in \mathbb{N}) \geq 2$ and q be a prime power such that $q \equiv 1 \pmod k$ if q is even, or $q \equiv 1 \pmod{2k}$ if q is odd; then the generalized Paley graph $G_k(q)$ is the graph with vertex set $\mathbb{F}_q$, where ab is an edge if $a - b$ is a k-th power residue. In a recent paper, Dawsey and McCarthy [21] have computed the number of complete subgraphs of order four in Lim and Praeger's graph using finite field hypergeometric functions, which in turn, generalizes the results of Evans et al. [26] for $G_k(q)$. Yip's thesis [57] and very recent paper [60] offer an insight into the order and structure of maximum cliques in $G_k(q)$, while Elsawy studied some properties of this graph for odd k. Wage [56] constructed three other generalizations with vertex set $\mathbb{F}_p$. Some other generalizations can be found in [16, 43, 50, 54].

2.2 Defining a Paley-type graph on $\mathbb{Z}_n$

A natural question that arises is what the analogue of a Paley graph can be if the vertex set has n vertices, in general, where n is a natural number. In this chapter, we attempt to define an analogue of the Paley graph with vertex set as the commutative ring $\mathbb{Z}_n$. We look at some properties of this graph, especially those whose deductions involve similar approaches as done for the Paley graphs.

The property $q \equiv 1 \pmod 4$ for a Paley graph of order q ensures that -1 is a quadratic residue in $\mathbb{F}_q^*$, so an edge is well-defined. For our purpose, we draw an analogy between $\mathbb{F}_q^*$ and $\mathbb{Z}_n^*$. We first find out the values of n for which the graph G_n is well-defined.

Proposition 2.1. *Let $n > 2$ be an integer. There exists $x \in \mathbb{Z}_n^*$ such that $x^2 \equiv -1 \pmod n$ if and only if $n = 2^s p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where the distinct primes $p_i \equiv 1 \pmod 4$ for all $i = 1, \ldots, k$ and $s = 0$ or 1.*

Proof. Let $n = 2^s p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $p_i \equiv 1 \pmod 4$ for all $i = 1, \ldots, k$ and $s = 0$ or 1. Then by Corollary 1.7.1, $\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{\alpha_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}^*$ and by Proposition 1.1, each $\mathbb{Z}_{p_i^{\alpha_i}}^*$ is cyclic of order $p_i^{\alpha_i - 1}(p_i - 1)$. Let $a_i \pmod{p_i^{\alpha_i}}$ be an element of order 4 in $\mathbb{Z}_{p_i^{\alpha_i}}^*$. Then

$$(a_1 \pmod{p_1^{\alpha_1}}, \ldots, a_k \pmod{p_k^{\alpha_k}})^2 = (-1 \pmod{p_1^{\alpha_1}}, \ldots, -1 \pmod{p_k^{\alpha_k}})$$

in $\mathbb{Z}_{p_1^{\alpha_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}^*$. This gives an element x in $\mathbb{Z}_n^*$ with the required property due to the isomorphism.

Conversely, let there exist some $x \in \mathbb{Z}_n^*$ such that $x^2 \equiv -1 \pmod n$. If 2^2 divides n, then $x^2 \equiv -1 \pmod 4$ which is not possible. Therefore, $n = 2^s p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $s = 0$ or 1, $k \geq 1$ and p_i's are distinct primes other than 2. Again, $x^2 \equiv -1 \pmod{p_i}$ implies that $p_i \equiv 1 \pmod 4$ for $i = 1, 2, \ldots, k$. ■

Now, we define a Paley-type graph on $\mathbb{Z}_n$, which we will denote by G_n. We exclude the cases $n = 1$ and $n = 2$ since the graphs turn out to be empty and trivial, respectively.

Definition 2.2 (Paley-type graph G_n)**.** *Let $n = 2^s p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where the distinct primes $p_i \equiv 1 \pmod 4$ for all $i = 1, \ldots, k$ and $s = 0$ or 1. Then, G_n is defined as the graph with vertex set $\mathbb{Z}_n$, where ab is an edge if and only if $a - b \equiv x^2 \pmod n$ for some $x \in \mathbb{Z}_n^*$.*

The Paley-type graphs of orders $25 = 5^2$ and $26 = 2 \times 13$ are shown in Figures 2.1 and 2.2 respectively. In G_{25}, the vertex 0 is adjacent to the vertices $1, 4, 6, 9, 11, 14, 16, 19, 21$ and 24; in G_{26}, the vertex 0 is adjacent to the vertices $1, 3, 9, 17, 23$ and 25.

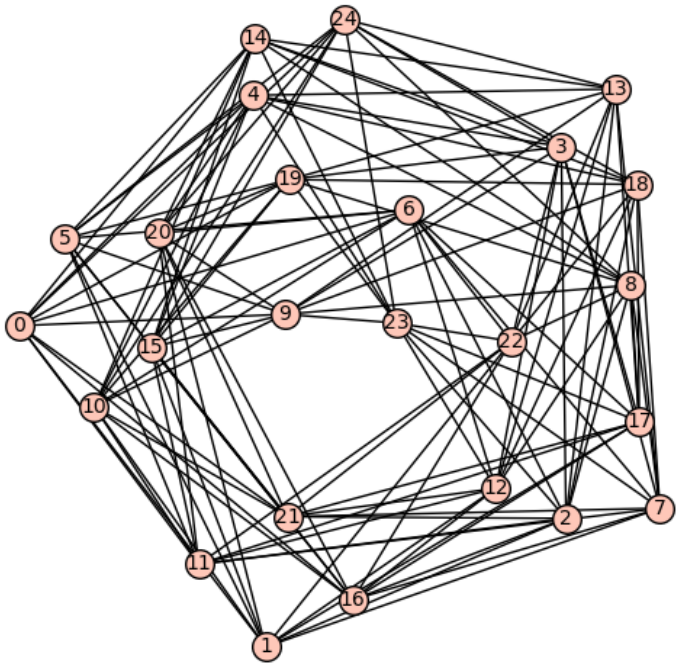

Figure 2.1: The Paley-type graph of order 25

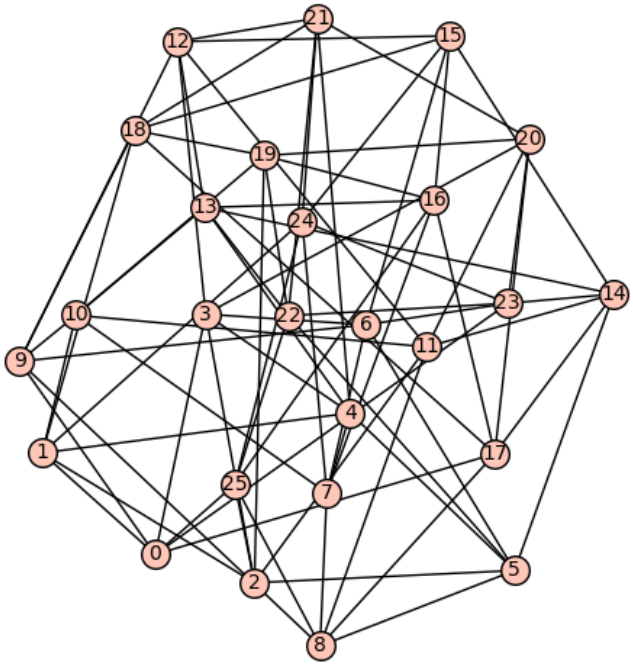

Figure 2.2: The Paley-type graph of order 26

2.3 Fixing an appropriate quadratic Dirichlet character mod n

There have been multiple instances where character sums were implemented to find out about properties of the Paley graph and its generalizations, for example in [11, 14, 21, 26, 56]. In case of the Paley graph of prime order, character sums involving the Legendre symbol modulo p were evaluated. Here we do the same using Dirichlet characters modulo n.

We are interested in calculating the number of complete subgraphs in G_n using a character sum approach. So, we try to define an appropriate quadratic Dirichlet character analogous to the unique quadratic character on $\mathbb{F}_p^*$ (p being a prime). We are looking for a character ψ such that

$$\psi(x) = 1 \text{ if and only if } x \equiv a^2 \pmod{n} \text{ for some } a \in \mathbb{Z}_n^*. \tag{2.1}$$

We define three possible candidates for such a character. Let $a \in \mathbb{Z}_n^*$.

- $\chi_1(a) := \left(\frac{a}{n}\right)$. This is the Jacobi symbol which is a Dirichlet character modulo n.
- For suitable n when $a^{\frac{\phi(n)}{2}} \equiv \pm 1 \pmod{n}$, we may define

$$\chi_2(a) := a^{\frac{\phi(n)}{2}} \pmod{n}.$$

- $\chi_3(a) := \begin{cases} 1, & \text{if } x^2 \equiv a \pmod{n} \text{ has a solution;} \\ -1, & \text{otherwise.} \end{cases}$

Proposition 2.3. *Let $k \geq 2$ be an integer. Let $n = 2^s p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where p_i's are distinct primes satisfying $p_i \equiv 1 \pmod{4}$ for all $i = 1, \ldots, k$ and $s = 0$ or 1. Then, χ_1 does not satisfy the condition (2.1).*

Proof. Here, $n = 2^s p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $k \geq 2$, $p_i \equiv 1 \pmod 4$ for all $i = 1, 2, \ldots, k$ and $s = 0$ or 1. Then for $a \in \mathbb{Z}_n^*$, $\chi_1(a) = \left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}$. Let R_p and N_p denote the set of quadratic residues modulo p and the set of quadratic non-residues modulo p, respectively. For $1 \leq i \leq k$, let $\alpha_i = 2\beta_i + \gamma_i$, where $0 \leq \gamma_i \leq 1$. It is enough to find $a \in \mathbb{Z}_n^*$ such that $\left(\frac{a}{p_i}\right) = -1$ for some $i \in \{1, 2, \ldots, k\}$ but $\left(\frac{a}{p_1}\right)^{\gamma_1} \left(\frac{a}{p_2}\right)^{\gamma_2} \cdots \left(\frac{a}{p_k}\right)^{\gamma_k} = 1$. If some α_i is even then we choose $b \in N_{p_i}$; then the system of equations

$$x \equiv b \pmod{p_i} \text{ and } x \equiv 1 \pmod{p_j}\ \forall j = 1, \ldots, k, j \neq i$$

has a solution which gives the desired $a \in \mathbb{Z}_n^*$. So let us assume that all α_i's are odd. Then

$$\chi_1(a) = \left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_k}\right).$$

We choose $b \in N_{p_1}$ and $c \in N_{p_2}$, then the system of equations

$$x \equiv b \pmod{p_1},\ x \equiv c \pmod{p_2} \text{ and } x \equiv 1 \pmod{p_j}\ \forall j \neq 1, 2$$

has a solution which gives the desired $a \in \mathbb{Z}_n^*$. ■

Proposition 2.4. *Let n be a positive integer. Then, $\chi_2 = \varepsilon$ whenever $\mathbb{Z}_n^*$ is not cyclic and consequently does not satisfy the condition (2.1).*

Proof. First, we note that χ_2 is a character on $\mathbb{Z}_n^*$. This is because $\left(a^{\frac{\phi(n)}{2}}\right)^2 = 1$ for all $a \in \mathbb{Z}_n^*$, so $a^{\frac{\phi(n)}{2}}$ can be one of the t elements modulo n whose square is 1, say $h_1, h_2, \ldots, h_t$. Let $\chi_2(a) = h_i, \chi_2(b) = h_j$. Then $\chi_2(ab) = h_i h_j$, so χ_2 is a character on $\mathbb{Z}_n^*$.

If $\mathbb{Z}_n^*$ is not cyclic, then by Proposition 1.1, n can be one of the following forms:

1. $n = 2^\alpha (\alpha \geq 3)$: In this case, $\mathbb{Z}_{2^\alpha}^*$ has order $2^{\alpha-1}$. But it is not cyclic, so any element raised to the power $2^{\alpha-2}$ is 1. Hence, $\chi_2 = \varepsilon$.

2. $n = 2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}(\alpha \geq 2, k \geq 1, \alpha_i \geq 1 \forall i, p_i$'s are distinct odd primes): We first consider that $\alpha = 2$. We know that $\mathbb{Z}_{2^2}^*$ is cyclic of order 2. Let $x, a_1, a_2, \ldots, a_k$ be generators of $\mathbb{Z}_{2^2}^*, \mathbb{Z}_{p_1^{\alpha_1}}^*, \mathbb{Z}_{p_2^{\alpha_2}}^*, \ldots, \mathbb{Z}_{p_k^{\alpha_k}}^*$, respectively. Then, the order of the element $(x, a_1, \ldots, a_k)$ is equal to

$$\begin{aligned}&\operatorname{lcm}\left\{2, p_1^{\alpha_1-1}(p_1-1), \ldots, p_k^{\alpha_k-1}(p_k-1)\right\}\\ &\leq p_1^{\alpha_1-1}(p_1-1)\cdots p_k^{\alpha_k-1}(p_k-1) = \frac{\phi(n)}{2}.\end{aligned}$$

So $a^{\frac{\phi(n)}{2}} = 1$ for all $a \in \mathbb{Z}_n^*$. Hence, $\chi_2 = \varepsilon$. If $\alpha \geq 3$, then $\mathbb{Z}_{2^\alpha}^*$ is not cyclic, and hence $\frac{2^{\alpha-1}}{2}$ is the maximum order of an element. Therefore, the order of an element in $\mathbb{Z}_{2^\alpha}^* \times \mathbb{Z}_{p_1^{\alpha_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}^*$ is atmost $2^{\alpha-2}p_1^{\alpha_1-1}(p_1-1)\cdots p_k^{\alpha_k-1}(p_k-1)$ which is equal to $\frac{\phi(n)}{2}$. This gives $\chi_2 = \varepsilon$.

3. $n = 2p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}(k \geq 2, \alpha_i \geq 1 \forall i, p_i$'s are distinct odd primes): Following similarly as shown in the previous cases, we find that $\chi_2 = \varepsilon$.

4. $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}(k \geq 2, \alpha_i \geq 1 \forall i, p_i$'s are distinct odd primes): In this case also, it follows that $\chi_2 = \varepsilon$, and the proof goes along similar lines.

This completes the proof of the proposition. ■

Proposition 2.5. *If $\mathbb{Z}_n^*$ is not cyclic, then there exist $a, b \in \mathbb{Z}_n^*$ such that a, b, ab are all non-squares.*

Proof. Since $\mathbb{Z}_n^*$ is not cyclic, so by Proposition 1.1, n can be one of the following forms:

1. n is a power of a prime: In this case, we have $n = 2^\alpha$, where $\alpha \geq 3$. Let $a = 3$ and $b = 5$. From Proposition 1.3 we find that a and ab are non-squares in $\mathbb{Z}_{2^\alpha}^*$. Again, Theorem 1.2 implies that 5 cannot be a square in $\mathbb{Z}_{2^\alpha}^*$. Consequently, $a = 3$, $b = 5$ and $ab = 15$ are all non-squares in $\mathbb{Z}_{2^\alpha}^*$.

2. n is divided by atleast two distinct primes: Let R_n and N_n be the subsets of $\mathbb{Z}_n^*$ of squares and non-squares, respectively. Let $x \in N_n$. It is enough to show that $\exists\ y \in N_n$ such that $xy \in N_n$. Suppose that there does not exist any such y. Then, $\{xy : y \in N_n\} \subseteq R_n$ which yields $\phi(n) \leq 2|R_n|$. In each of the cases below, we prove that $\phi(n) \nleq 2|R_n|$.

   - 2 is a factor of n: We have the following two cases.

     (i) $n = 2^\alpha p_1^{\alpha_1} \cdots p_k^{\alpha_k}, k \geq 1, \alpha \geq 2$, p_i's are distinct odd primes: In this case,
     $$|R_n| = \frac{\phi(n)}{2 \times h \times 2^k},$$
     where $h = 1$ or 2. Hence, $\phi(n) \nleq 2|R_n|$.

     (ii) $n = 2p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, k \geq 2$, p_i's are distinct odd primes: In this case $|R_n| = \frac{\phi(n)}{2^k}$, and hence $\phi(n) \nleq 2|R_n|$.

   - 2 is not a factor of n: In this case, we have $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where $k \geq 2$ and p_i's are distinct odd primes. We find that $|R_n| = \frac{\phi(n)}{2^k}$, and hence $\phi(n) \nleq 2|R_n|$.

This completes the proof of the proposition. ■

Corollary 2.5.1. *From Proposition 2.5, it follows that χ_3 cannot be a character unless $\mathbb{Z}_n^*$ is cyclic.*

The above propositions suggest to take χ_3 as the desired quadratic character and consequently take n such that $\mathbb{Z}_n^*$ is cyclic, in order that χ_3 be defined. Then by Proposition 1.1, $n = 2, 4, p^\alpha$ or $2p^\alpha$, where p is an odd prime and α is a positive integer. Note that by Proposition 1.17, $\chi_2 = \chi_3$ is the unique quadratic character when $\mathbb{Z}_n^*$ is cyclic. In this case, using Theorem 1.18 we observe that for $x \in \mathbb{Z}_n^*$,

$$\frac{1 + \chi_3(x)}{2} = \begin{cases} 1, & \text{if } x \text{ is a square in } \mathbb{Z}_n^*; \\ 0, & \text{otherwise.} \end{cases} \tag{2.2}$$

Before stating the next lemma, we define the p-adic valuation of a non-zero integer and recall Legendre's formula, which finds out the p-adic valuation of $n!$ for a positive integer n.

Definition 2.6 (p-adic valuation)**.** *The p-adic valuation of a non-zero integer n (denoted by $v_p(n)$) is the exponent of the highest power of the prime p that divides n.*

Lemma 2.7. [40, Theorem 3.9] *Let n be a positive integer, and let p be a prime. Then,*

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

(note that the terms become zero when $p^j > n$, so this is a finite sum).

Lemma 2.8. *Let $p \equiv 1 \pmod 4$ be a prime and let $\alpha \geq 1$ be an integer. We have $\binom{\phi(n)/2}{i} p^i \equiv 0 \pmod{p^\alpha}$, where $n = p^\alpha, 1 \leq i \leq \alpha - 1$.*

Proof. Enough to show that $p^{\alpha-i} \mid \binom{p^{\alpha-1}(\frac{p-1}{2})}{i}$ for $1 \leq i \leq \alpha - 1$. We have

$$\begin{aligned}\binom{p^{\alpha-1}(\frac{p-1}{2})}{i} &= \frac{p^{\alpha-1}(\frac{p-1}{2})(p^{\alpha-1}(\frac{p-1}{2}) - 1)\cdots(p^{\alpha-1}(\frac{p-1}{2}) - i + 1)}{i!} \\ &= \frac{p^{\alpha-i}p^{i-1}(\frac{p-1}{2})(p^{\alpha-1}(\frac{p-1}{2}) - 1)\cdots(p^{\alpha-1}(\frac{p-1}{2}) - i + 1)}{i!}.\end{aligned}$$

For an integer $x \neq 0$, let $\sigma_p(x)$ be the sum of digits of the base-p representation of x. By Lemma 2.7, $v_p(i!) = \sum_{k=1}^{\infty} \left\lfloor \frac{i}{p^k} \right\rfloor$, from which it follows that $v_p(i!) = \dfrac{i - \sigma_p(i)}{p-1}$. If possible, let $p^i \mid i!$. Then, $v_p(i!) \geq i$, that is $\dfrac{i - \sigma_p(i)}{p-1} \geq i$, which is not possible. This completes the proof of the lemma. ∎

The following lemma, a consequence of Lemma 2.8, will be useful in evaluating character sums later on.

Lemma 2.9. *Let $n = p^\alpha$, where $\alpha \geq 1$ and $p \equiv 1 \pmod 4$, and let χ be the unique character mod n of order 2. Let $x \in \mathbb{Z}_n$. Then we have $\chi(x) = \chi(x + pk)$ for any integer k.*

Proof. Let $x \in \mathbb{Z}_n$ and let k be any integer. If $x \notin \mathbb{Z}_n^*$ then we have $\chi(x) = \chi(x + pk) = 0$, and hence we obtain the required result. So, let $x \in \mathbb{Z}_n^*$. Then the result follows from the binomial expansion of $(x + p)^{\frac{\phi(n)}{2}}$ and Lemma 2.8. ■

2.4 Some basic properties of G_n

In this section we look at some properties of the graph G_n. We have seen that the graph is well-defined for $n = 2^s p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where the distinct primes $p_i \equiv 1 \pmod 4$ for all $i = 1, \ldots, k$ and $s = 0$ or 1. So, we consider these forms of n. Like the Paley graph, we see that G_n is also regular.

Proposition 2.10. *Let $n = 2^s p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, where the distinct primes $p_i \equiv 1 \pmod 4$ for all $i = 1, \ldots, k$ and $s = 0$ or 1. Then G_n is regular of degree equal to $\dfrac{\phi(n)}{2^k}$.*

Proof. Let R_n be the subset of $\mathbb{Z}_n^*$ of squares. Clearly, G_n is regular of degree equal to $|R_n|$. Let $a_1, \ldots, a_t$ be the distinct elements in $\mathbb{Z}_n^*$ whose squares are equal to 1. Then $|R_n| = \dfrac{\phi(n)}{t}$. Now, we find the number of solutions of $x^2 \equiv 1 \pmod n$. This is equivalent to finding the solutions of

$$x^2 \equiv 1 \pmod{2^s}, \quad x^2 \equiv 1 \pmod{p_1^{\alpha_1}}, \quad \ldots, \quad x^2 \equiv 1 \pmod{p_k^{\alpha_k}}.$$

If $s = 1$ then $x^2 \equiv 1 \pmod{2^s}$ has 1 solution, and $x^2 \equiv 1 \pmod{p_1^{\alpha_1}}, \ldots, x^2 \equiv 1 \pmod{p_k^{\alpha_k}}$ have two solutions each. So t must be equal to 2^k. Therefore, $|R_n| = \dfrac{\phi(n)}{2^k}$. This completes the proof of the result. ■

Let $p \equiv 1 \pmod 4$ be a prime and let α be a positive integer. Proposition 1.1 and Theorem 1.16 imply that there exists a unique Dirichlet character modulo p^α;

let us call it χ. It is known from Proposition 2.10 that G_{p^α} is regular; we see that the same can be deduced using the character sum given in (2.2). Let $a \in \mathbb{Z}_{p^\alpha}^*$, then

$$\deg(a) = \sum_{\substack{b=0 \\ a-b\in\mathbb{Z}_{p^\alpha}^*}}^{n-1} \frac{1+\chi(a-b)}{2},$$

where $\deg(a)$ denotes the degree of the vertex a in G_{p^α}. It is easy to calculate this sum and see that $\deg(a) = \dfrac{\phi(p^\alpha)}{2}$ which agrees with the proposition.

In the following, we prove that G_n is not self-complementary unless n is a prime.

Proposition 2.11. *Let $n = 2^s p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where the distinct primes $p_i \equiv 1 \pmod 4$ for all $i = 1, \ldots, k$ and $s = 0$ or 1. Then G_n is not self-complementary unless n is a prime. If n is a prime, G_n, being the Paley graph of order n, is self complementary.*

Proof. The graph G_n has $\dfrac{n\frac{\phi(n)}{2^k}}{2}$ number of edges. But we know that a self-complementary graph must have $\dfrac{n(n-1)}{4}$ number of edges. So, if G_n is self-complementary, we must have $\dfrac{n\frac{\phi(n)}{2^k}}{2} = \dfrac{n(n-1)}{4}$ which gives $\phi(n) = (n-1)2^{k-1}$, which is not possible except for the case $k = 1, s = 0, \alpha_1 = 1$. This completes the proof of the proposition. ■

Proposition 2.12. *Let $n = 2^s p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where the distinct primes $p_i \equiv 1 \pmod 4$ for all $i = 1, \ldots, k$ and $s = 0$ or 1. Then G_n is not a complete graph.*

Proof. A necessary condition that G_n is a complete graph is $x - y$ is a square in $\mathbb{Z}_n^*$ for all distinct $x, y \in \mathbb{Z}_n$. This implies that $\{x - y : x, y \in \mathbb{Z}_n, x \neq y\} \subseteq R_n$, where R_n is the subset of $\mathbb{Z}_n^*$ of squares. Hence, $n - 1 \leq \dfrac{\phi(n)}{2^k}$, which is not possible. Thus G_n is not complete. ■

Paley graphs are connected, and we find that the Paley-type graphs are connected as well.

Proposition 2.13. *Let $n = 2^s p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where the distinct primes $p_i \equiv 1 \pmod 4$ for all $i = 1, \ldots, k$ and $s = 0$ or 1. Then the graph G_n is connected.*

Proof. Let $x < y$ be two distinct vertices of the graph. Let (i, j) denote the edge between two vertices i and j. Then the edges $(x, x+1), (x+1, x+2), \ldots, (y-1, y)$ form a path between x and y. Hence, G_n is connected. ■

Since 1 is always a quadratic residue modulo n, G_n always contains a spanning cycle. In the following proposition we check when the graph is a cycle graph.

Proposition 2.14. *Let $n = 2^s p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where the distinct primes $p_i \equiv 1 \pmod 4$ for all $i = 1, \ldots, k$ and $s = 0$ or 1. Then G_n is a cycle if and only if $n = 5$ or 10.*

Proof. We observe that G_n is a cycle if and only if 1 and -1 are the only squares modulo n. Let the graph be a cycle. If $n \neq 5, 10$, then $n > 10$ and $3 \in \mathbb{Z}_n^*$, which means that 9 is a square in $\mathbb{Z}_n^*$ which is neither 1 nor -1. This completes the proof of the proposition. ■

Proposition 2.15. *Let $n = 2^s p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where the distinct primes $p_i \equiv 1 \pmod 4$ for all $i = 1, \ldots, k$ and $s = 0$ or 1. Then G_n is a vertex-transitive graph.*

Proof. Let $a, b \in \mathbb{Z}_n^*$ and a is a square modulo n. Then for $x \in \mathbb{Z}_n^*$, $x \mapsto ax + b$ is a graph isomorphism on G_n. Using this isomorphism and taking appropriate values of a and b we see that G_n becomes vertex-transitive. ■

Thus, both the Paley and Paley-type graphs are vertex-transitive. In fact, one can proceed along similar lines as in the proof of [23, Prop. 2.2.1] to show that the Paley-type graphs are also edge-transitive. However, we do not use edge-transitivity of Paley-type graphs in the proofs of our results. The following result provides a formula for counting cliques in the Paley-type graph. Recall that for a graph G, we denote the number of cliques of order ℓ in G by $\mathcal{K}_\ell(G)$, and for a vertex u of G, we denote the number of cliques of order ℓ in G containing u by $\mathcal{K}_\ell(G, u)$.

Proposition 2.16. *Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $\alpha_i \geq 1$ and the distinct primes p_i satisfy $p_i \equiv 1 \pmod 4$ for all $i = 1, \ldots, k$. Let R_n denote the set of squares in $\mathbb{Z}_n^*$ and let H_n denote the subgraph of G_n induced by R_n. Then for $\ell \geq 3$,*

$$\mathcal{K}_\ell(G_n) = \frac{n\phi(n)}{2^k \ell(\ell-1)} \times \mathcal{K}_{\ell-1}(H_n, 1).$$

Proof. As observed in Proposition 2.15, G_n is vertex-transitive. So, we find that

$$\mathcal{K}_\ell(G_n) = \frac{n}{\ell} \times \mathcal{K}_\ell(G_n, 0) = \frac{n}{\ell} \times \mathcal{K}_{\ell-1}(H_n). \tag{2.3}$$

Let $r \in R_n$ be fixed. Then, the map $x \mapsto rx$ on R_n gives a graph isomorphism on H_n. This proves that H_n is also vertex-transitive. So, we have

$$\mathcal{K}_{\ell-1}(H_n) = \frac{|R_n|}{\ell-1} \times \mathcal{K}_{\ell-1}(H_n, 1). \tag{2.4}$$

Combining (2.3) and (2.4), we obtain the required result. ∎

In the forthcoming chapters we will study the number of cliques in G_n for the case $n = p^\alpha$, where $p \equiv 1 \pmod 4$ is a prime and $\alpha \geq 1$. So, we prove a result about the structure of the graph G_{p^α}. We follow Notation 1.59.

Proposition 2.17. *Let α be a positive integer. Let $n = p^\alpha$, where p is a prime satisfying $p \equiv 1 \pmod 4$. Let χ be the quadratic character mod n. Let $P(p)$ be the Paley graph of order p. Then a copy of $P(p)$ exists in the graph G_n. In fact, we can write*

$$G_n = \bigoplus_{i=1}^{p^{\alpha-1}} P(p) \bigoplus \left(\bigoplus_{j=1}^{\frac{p^{\alpha-1}(p^{\alpha-1}-1)}{2}} \left(\bigoplus_{m=1}^{p} K_{1,\frac{p-1}{2}} \right) \right),$$

where $K_{1,\frac{p-1}{2}}$ is a complete bipartite graph.

Proof. Let k be an integer such that $0 \leq k \leq p^{\alpha-1} - 1$. We define a map from $P(p)$ to the subgraph of G_n induced by the vertices $\{kp, kp+1, \ldots, kp+p-1\}$. For

$i \in \mathbb{F}_p = \{0, 1, \ldots, p-1\}$, let $i \mapsto kp + i$. We show that this is an isomorphism. Let i and j be elements of $\mathbb{F}_p$ such that $i - j$ is a quadratic residue in $\mathbb{F}_p^*$. Then $(i-j)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ by Corollary 1.10.1, and so $(i-j)^{\frac{p-1}{2}} = 1 + p\ell$ for some $\ell \in \mathbb{Z}$. Therefore, $(i-j)^{\frac{p-1}{2} \times p^{\alpha-1}} = (1+p\ell)^{p^{\alpha-1}} \equiv 1 \pmod{p^\alpha}$ by using binomial theorem and proceeding in the same way as in Lemma 2.8 after replacing $\frac{\phi(n)}{2}$ by $p^{\alpha-1}$ in the statement of the lemma. So, $\chi((kp+i)-(kp+j)) = \chi(i-j) = 1$ and hence $(kp+i)-(kp+j)$ is a square modulo p^α and thus there is an edge between the vertices $kp+i$ and $kp+j$ in the induced subgraph of G_n. For the converse, let $kp+i$ and $kp+j$ be two vertices in the induced subgraph of G_n connected by an edge, where $0 \le i, j \le p-1$. Then $i - j \equiv x^2 \pmod{p^\alpha}$ for some $1 \le x \le p-1$. This implies that $i - j \equiv x^2 \pmod{p}$, and hence there is an edge between the vertices i and j in $P(p)$.

So each induced subgraph of G_n comprising of the vertices $\{kp, kp+1, \ldots, kp+p-1\}$, where $0 \le k \le p^{\alpha-1} - 1$, is a copy of $P(p)$. Each such induced subgraph has $\dfrac{p(p-1)}{4}$ edges, and there are $p^{\alpha-1}$ such induced subgraphs. The total number of edges of G_n exhausted this way is $p^{\alpha-1}\dfrac{p(p-1)}{4}$. The number of edges remaining in G_n is

$$\frac{n\phi(n)}{4} - p^{\alpha-1}\frac{p(p-1)}{4} = p^\alpha \left(\frac{p-1}{4}\right)(p^{\alpha-1} - 1).$$

We see how these edges are exhausted as follows. Let $r_1, r_2, \ldots, r_{\frac{p-1}{2}}$ be the quadratic residues in the range 1 to $p-1$. Then for $1 \le k \le p^{\alpha-1} - 1$,

$$\chi(r_1 + kp) = 1,\ \chi(r_2 + kp) = 1, \ldots, \chi(r_{\frac{p-1}{2}} + kp) = 1.$$

So, $r_1 + kp, r_2 + kp, \ldots, r_{\frac{p-1}{2}} + kp$ are quadratic residues too. In fact, these are the quadratic residues in the range kp to $kp + p - 1$. So, from the induced subgraph of $\{0, 1, \ldots, p-1\}$ we have the following edges:

0 has edges with the vertices $r_1 + kp, r_2 + kp, \ldots, r_{\frac{p-1}{2}} + kp$;

1 has edges with the $r_1 + kp + 1, r_2 + kp + 1, \ldots, r_{\frac{p-1}{2}} + kp + 1$;

$\vdots$

$p-1$ has edges with the vertices $r_1 + kp + p - 1, r_2 + kp + p - 1, \ldots$

$\ldots, r_{\frac{p-1}{2}} + kp + p - 1.$

Since each edge is counted twice, the total number of edges among these $p^{\alpha-1}$ induced subgraphs is $\frac{\frac{p(p-1)}{2}(p^{\alpha-1}-1)p^{\alpha-1}}{2}$. This completes the proof. ■

3

Triangles in the Paley-type graph

3.1 Introduction

For a prime $p \equiv 1 \pmod 4$, let $G^{(p)}$ denote a graph on p vertices and let $\overline{G^{(p)}}$ be the complement of $G^{(p)}$. In 1981, Evans, Pulham and Sheehan [26] gave a simple closed formula to calculate the number of cliques of order 4 in $P(p)$, $P(p)$ being the Paley graph of order p. The purpose was to give an upper bound for $T_4(p) = \min\left(\mathcal{K}_4(G^{(p)}) + \mathcal{K}_4(\overline{G^{(p)}})\right)$, where the minimum is taken over all graphs $G^{(p)}$. They computed character sums involving the Legendre symbol. This work was extended by Atanasov et al. [11] for a prime power $q = p^n \equiv 1 \pmod 4$ when

[1]The contents of this chapter have partially been published in *Graphs Comb.* (2022).

$p \equiv 1 \pmod 4$. In a recent paper, Dawsey and McCarthy [21] have computed the number of triangles and complete subgraphs of order four in the graph $G_k(q)$ introduced by Lim and Praeger in [41], using finite field character sums and hypergeometric functions, which in turn, generalizes the results of Evans et al. The general formula they provided for the number of triangles in $G_k(q)$ gives lower bounds for the multicolor diagonal Ramsey numbers $R_k(3) = R(3, 3, \ldots, 3)$. Wage [56] constructed three other generalizations with vertex set $\mathbb{F}_p$ for a prime p, and gave asymptotic answers to the number of cliques for those generalized graphs, besides Paley graphs.

3.2 The number of triangles in G_n

In this chapter, we put our focus on computing the number of triangles in the Paley-type graph. Let p be a prime such that $p \equiv 1 \pmod 4$ and let $\alpha \geq 1$ be an integer. First, we use a character sum approach to compute the number of triangles in the graph G_{p^α}. Then, using this result and some basic combinatorics, we find the number of triangles in the graph G_n for all n for which the graph is defined. We exclude the case when n is even, since there cannot exist cliques of order more than 2 in that case, and we see why. Let $n = 2p^\alpha$, and if possible let x, y and z be vertices in G_n which form a clique. Then $x - y, y - z$ and $x - z$ are necessarily elements in $\mathbb{Z}_n^*$, and therefore, are odd integers, which contradicts that $x - z = x - y + y - z$. Thus, we consider only the case $n = p^\alpha$. In the following theorem, for primes $p \equiv 1 \pmod 4$ and any positive integer α, we find the number of triangles contained in the graph G_{p^α}.

Theorem 3.1. *Let p be a prime such that $p \equiv 1 \pmod 4$. For any positive integer α, we have*

$$\mathcal{K}_3(G_{p^\alpha}) = \frac{p^{3\alpha-2}(p-1)(p-5)}{2^4 \times 3}.$$

It is easy to see that the expression for $\mathcal{K}_3(G_{p^\alpha})$ is an integer. We write $\mathcal{K}_3(G_{p^\alpha}) = \dfrac{p^{3\alpha-2}\left(\frac{p-1}{4}\right)\left(\frac{p-1}{4}-1\right)}{3}$, and observe that $3 \nmid \frac{p-1}{4} + 1$, so $3 \mid \left(\frac{p-1}{4}\right)\left(\frac{p-1}{4}-1\right)$.

In [20], Das introduced Paley-type graphs Γ_N modulo N, where $N = pq$, p and q being distinct primes satisfying $p \equiv q \equiv 1 \pmod 4$. The graph Γ_N is a special case of the Paley-type graphs G_n, and it turns out to be G_{pq}. He gave a formula for $\mathcal{K}_3(G_{pq})$, where p and q are distinct primes satisfying $p \equiv q \equiv 1 \pmod 4$, and G_{pq} is the Paley-type graph of order pq. In the following theorem we find the number of triangles in G_n for all odd n for which the graph is defined.

Theorem 3.2. *Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $\alpha_i \geq 1$ and the distinct primes p_i satisfy $p_i \equiv 1 \pmod 4$ for all $i = 1, \ldots, k$. Then, the number of triangles in G_n is given by*

$$\mathcal{K}_3(G_n) = \frac{1}{3 \times 2^{3k+1}} \prod_{i=1}^{k} \left[p_i^{3\alpha_i - 2}(p_i - 1)(p_i - 5) \right].$$

To show that the expression for $\mathcal{K}_3(G_n)$ is an integer, we write $\mathcal{K}_3(G_n) = \frac{1}{3\times 2} \prod_{i=1}^{k} p_i^{3\alpha_i - 2} \left(\frac{p_i - 1}{4}\right) \left(\frac{p_i - 1}{2} - 2\right)$. Let $p_1 = 4s_1 + 1$. Then, it is enough to show that $3 \mid \left(\frac{p_1 - 1}{4}\right) \left(\frac{p_1 - 1}{2} - 2\right)$, that is, $3 \mid 2s_1(s_1 - 1)$, which holds since $p \nmid s_1 + 1$.

We find the values of $\mathcal{K}_3(G_n)$ for some particular values of n by using `Python` which are listed in Table 3.1.

n	$\mathcal{K}_3(G_n)$	n	$\mathcal{K}_3(G_n)$
13^2	57122	13×17	10608
17^2	334084	$13^2 \times 17$	23305776
29^2	9901934	29×37	2163168
37^2	44979864	29×41	2996280

Table 3.1: Values of $\mathcal{K}_3(G_n)$

We obtain the same values of $\mathcal{K}_3(G_n)$ from Theorem 3.2 as well.

Remark 3.3. *If we take $k = 2$, $\alpha_1 = \alpha_2 = 1$ and $p_1 = 5$ in Theorem 3.2, then we obtain Theorem 7 in [20]. Also, if we take $k = 2$, $\alpha_1 = \alpha_2 = 1$ in Theorem 3.2, then we obtain Theorem 12 in [20].*

3.2.1 Proof of Theorem 3.1

In this section we present the proof of Theorem 3.1.

Proof of Theorem 3.1. Since $\mathbb{Z}_{p^\alpha}^*$ is cyclic by Proposition 1.1, we infer from Proposition 1.17 that there exists a unique character modulo p^α of order 2; let us call it χ. Let H_{p^α} denote the subgraph of G_{p^α} induced by the set of squares in $\mathbb{Z}_{p^\alpha}^*$. Using Proposition 2.16 and (2.2), we readily obtain that

$$\begin{aligned}\mathcal{K}_3(G_{p^\alpha}) &= \frac{p^\alpha\phi(p^\alpha)}{12} \times \text{ number of edges in } H_{p^\alpha} \text{ containing } 1\\ &= \frac{p^\alpha\phi(p^\alpha)}{12} \times \sum_{\substack{x\in\mathbb{Z}_{p^\alpha}\\ x,x-1\in\mathbb{Z}_{p^\alpha}^*}} \left(\frac{1+\chi(x)}{2}\right)\left(\frac{1+\chi(1-x)}{2}\right). \end{aligned} \tag{3.1}$$

We will evoke Lemma 2.9 as required. We have

$$\sum_{\substack{x\in\mathbb{Z}_{p^\alpha}\\ x,x-1\in\mathbb{Z}_{p^\alpha}^*}} 1 = p^{\alpha-1}(p-2) \tag{3.2}$$

and evoking Theorem 1.19, we have

$$\begin{aligned}\sum_{\substack{x\in\mathbb{Z}_{p^\alpha}\\ x,x-1\in\mathbb{Z}_{p^\alpha}^*}} \chi(x) &= \sum_{x\in\mathbb{Z}_{p^\alpha}^*} \chi(x) - \sum_{\substack{x\in\mathbb{Z}_{p^\alpha}^*\\ p\mid x-1}} \chi(x)\\ &= -\left[\chi(1)+\chi(p+1)+\chi(2p+1)+\cdots+\chi((p^{\alpha-1}-1)p+1)\right]\\ &= -p^{\alpha-1}. \end{aligned} \tag{3.3}$$

Similarly, we have

$$\sum_{\substack{x\in\mathbb{Z}_{p^\alpha}\\ x,x-1\in\mathbb{Z}_{p^\alpha}^*}} \chi(1-x) = -p^{\alpha-1} \tag{3.4}$$

and

$$\begin{aligned}\sum_{\substack{x\in\mathbb{Z}_{p^\alpha}\\ x,x-1\in\mathbb{Z}^*_{p^\alpha}}}\chi(x(x-1)) &= \sum_{p\nmid x}\chi(x(x-1))\chi(x^{-2})\\ &= \sum_{p\nmid x}\chi(1-x^{-1})\\ &= \sum_{p\nmid x}\chi(1-x)\\ &= -p^{\alpha-1}. \end{aligned} \tag{3.5}$$

Combining (3.2), (3.3), (3.4) and (3.5), (3.1) yields

$$\mathcal{K}_3(G_{p^\alpha}) = \frac{p^\alpha p^{\alpha-1}(p-1)}{12} \times \frac{1}{4}(p-5)p^{\alpha-1},$$

completing the proof of the theorem. ■

3.2.2 Proof of Theorem 3.2

By the statement of the theorem, $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$, where $\alpha_i \geq 1$ and the distinct primes p_i satisfy $p_i \equiv 1 \pmod 4$ for all $i = 1,\ldots,k$. The following lemma states a relation between the squares in $\mathbb{Z}_n^*$ and the squares in $\mathbb{Z}^*_{p_i^{\alpha_i}}$, for $i \in \{1,\ldots,k\}$.

Lemma 3.4. *Let $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$, where $\alpha_i \geq 1$ and the distinct primes p_i satisfy $p_i \equiv 1 \pmod 4$ for all $i = 1,\ldots,k$. Let $\mathbb{Z}_n^*$ denote the group of units in $\mathbb{Z}_n$, and let R_n and $R_{p_i^{\alpha_i}}$ $(1 \leq i \leq k)$ denote the group of squares in $\mathbb{Z}_n^*$ and $\mathbb{Z}^*_{p_i^{\alpha_i}}$, respectively. Then, for $x \in \mathbb{Z}_n$ we find that*

$$x \in R_n \text{ if and only if } x \in \bigcap_{i=1}^{k} R_{p_i^{\alpha_i}}.$$

Proof. Let $x \in \mathbb{Z}_n$ be such that $x \in R_n$. Then $x \equiv a^2 \pmod n$ for some $a \in \mathbb{Z}_n^*$, which yields $x \equiv a^2 \pmod{p_i^{\alpha_i}}$ for each $i \in \{1,\ldots,k\}$. Conversely, let $x \equiv a_1^2$

$(\text{mod } p_1^{\alpha_1}), \ldots, x \equiv a_k^2 \pmod{p_k^{\alpha_k}}$ for $a_i \in \mathbb{Z}^*_{p_i^{\alpha_i}}$. Let z be an integer satisfying the system of congruences

$$z \equiv a_1 \pmod{p_1^{\alpha_1}}, \ldots, z \equiv a_k \pmod{p_k^{\alpha_k}}.$$

Then by Corollary 1.7.2 we find that $x \equiv z^2 \pmod{n}$ and so, $x \in R_n$. This completes the proof of the lemma. ■

Now, using the above lemma, we prove Theorem 3.2.

Proof of Theorem 3.2. Let H_n denote the subgraph of G_n induced by the group of squares in $\mathbb{Z}^*_n$.

Employing Proposition 2.16 and using Notation 1.57, we find that the number of triangles in G_n is given by

$$\mathcal{K}_3(G_n) = \frac{n\phi(n)}{3 \times 2^{k+1}} \times \mathcal{K}_2(H_n, 1). \tag{3.6}$$

Let E denote the set of edges in H_n containing the vertex 1, and for $i \in \{1, \ldots, k\}$ let E_i denote the set of edges in $H_{p_i^{\alpha_i}}$ containing the vertex 1. Let $(1, x)$ denote the edge connecting the vertices 1 and x. We define a function $f : E \to E_1 \times \cdots \times E_k$ as follows.

$$(1, x) \mapsto ((1 \pmod{p_1^{\alpha_1}}, x \pmod{p_1^{\alpha_1}}), \ldots, (1 \pmod{p_k^{\alpha_k}}, x \pmod{p_k^{\alpha_k}})).$$

f is well defined, and evoking Corollary 1.7.2 and Lemma 3.4 we find that f is one-one and onto as well. Thus, f is a bijection which implies $|E| = \prod_{i=1}^{k} |E_i|$. So, (3.6) yields

$$\mathcal{K}_3(G_n) = \frac{n\phi(n)}{3 \times 2^{k+1}} \times \prod_{i=1}^{k} \mathcal{K}_2(H_{p_i^{\alpha_i}}, 1). \tag{3.7}$$

Now, let $i \in \{1, \ldots, k\}$ and let χ_i be the unique quadratic character modulo $p_i^{\alpha_i}$. Using (2.2), we have

$$\begin{aligned} \mathcal{K}_2(H_{p_i^{\alpha_i}}, 1) &= \text{ number of edges in } H_{p_i^{\alpha_i}} \text{ containing } 1 \\ &= \sum_{\substack{x \in \mathbb{Z}_{p_i^{\alpha_i}} \\ x, x-1 \in \mathbb{Z}^*_{p_i^{\alpha_i}}}} \left(\frac{1+\chi_i(x)}{2}\right)\left(\frac{1+\chi_i(1-x)}{2}\right), \end{aligned} \tag{3.8}$$

as expressed in (3.1). So, using (3.2),(3.3),(3.4) and (3.5), where we replace p and α by p_i and α_i, respectively, (3.8) yields

$$\mathcal{K}_2(H_{p_i^{\alpha_i}}, 1) = \frac{1}{4}[p_i^{\alpha_i - 1}(p_i - 2) - 3p_i^{\alpha_i - 1}] = \frac{p_i^{\alpha_i - 1}(p_i - 5)}{4}.$$

Hence, substituting this expression in (3.7) yields the required result. ■

4

Cliques of order four in the Paley-type graph on $\mathbb{Z}_{p^\alpha}$

4.1 Introduction

In this chapter, we find the number of cliques of order 4 in the Paley-type graph G_n, for some particular values of n. Let $p \equiv 1 \pmod 4$ be a prime; we recall that $P(p)$ denotes the Paley graph of order p. Evans et al. in [26] provided the number of cliques of order 4 in $P(p)$ by the following formula. Write $p = a^2 + b^2$, where

[1]The contents of this chapter have been published in *Graphs Comb.* (2022)

$a, b \in \mathbb{Z}$, and a is even. Then,

$$\mathcal{K}_4(P(p)) = \frac{p(p-1)((p-9)^2 - 4a^2)}{2^9 \times 3}.$$

They proved the above result using character sums involving the Legendre symbol modulo p. Now, let q be a power of an odd prime. For the generalized Paley graph $G_k(q)$ defined in [41], Dawsey and McCarthy have provided a general formula for $\mathcal{K}_4(G_k(q))$ using character sums and finite field hypergeometric functions (as developed by Greene [33]). Then the authors proceed to show that the formula gives lower bounds for the multicolor diagonal Ramsey numbers $R_k(4) = R(4, 4, \ldots, 4)$.

4.2 The number of cliques of order four in G_{p^α}

Inspired by the above mentioned works, we find $\mathcal{K}_4(G_n)$ for some particular values of n. In this chapter, we consider the case $n = p^\alpha$, where $p \equiv 1 \pmod 4$ is a prime and α is a positive integer, because we intend to use a character sum approach, and thus use the quadratic character that we fixed in the discussion in Chapter 2 satisfying the condition given in (2.1). In the following theorem, we find the number of complete subgraphs of order 4 contained in the graph G_{p^α} for primes $p \equiv 1 \pmod 4$.

Theorem 4.1. *Let p be a prime such that $p \equiv 1 \pmod 4$, and let α be a positive integer. Let χ denote the unique quadratic Dirichlet character mod p^α and let ψ be a Dirichlet character mod p^α of order 4. Let $J(\psi, \chi) = \sum_{x \in \mathbb{Z}_{p^\alpha}} \psi(x)\chi(1-x)$ be the Jacobi sum of ψ and χ. Then,*

$$\mathcal{K}_4(G_{p^\alpha}) = \frac{p^{2\alpha-1}(p-1)[p^{2\alpha-2}\{(p-9)^2 - 2p\} + J(\psi,\chi)^2 + \overline{J(\psi,\chi)}^2]}{2^9 \times 3}.$$

Remark 4.2. *If we take $\alpha = 1$, then we can further simplify the Jacobi sum appearing in Theorem 4.1 and obtain the result of Evans et al. proved in [26].*

4.2.1 Some lemmas involving character sums

Here, we evaluate some character sums which shall be required to prove the results on the number of cliques of order four in G_{p^α}. By the statement of the theorem, χ denotes the unique character mod p^α of order 2. It is easy to see that $\chi(-1) = 1$.

Lemma 4.3. *Let $n = p^\alpha$, where $\alpha \geq 1$ and $p \equiv 1 \pmod 4$. Let χ be the unique character mod n of order 2. Then, for $a \in \mathbb{Z}_n^*$, we have*

$$\sum_{x \in \mathbb{Z}_n^*} \chi(x^2 - a) = -(1 + \chi(a))p^{\alpha-1}.$$

Proof. For $x \in \mathbb{Z}_n^*$, let x^{-1} denote the multiplicative inverse of x in $\mathbb{Z}_n^*$. We employ (2.2), and find that

$$\begin{aligned}\sum_{x \in \mathbb{Z}_n^*} \chi(x^2 - a) &= 2 \sum_{\substack{x \in \mathbb{Z}_n^* \\ x \text{ is a square}}} \chi(x - a) \\ &= \sum_{x \in \mathbb{Z}_n^*} \chi(x - a)(1 + \chi(x)) \\ &= \sum_{x \in \mathbb{Z}_n^*} \chi(x - a) + \sum_{x \in \mathbb{Z}_n^*} \chi(x(x - a)). \end{aligned} \tag{4.1}$$

Now, using Theorem 1.19 and Lemma 2.9, we have

$$\begin{aligned}\sum_{x \in \mathbb{Z}_n^*} \chi(x - a) &= \sum_{\substack{x \in \mathbb{Z}_n^* \\ x - a \in \mathbb{Z}_n^*}} \chi(x - a) \\ &= \sum_{x - a \in \mathbb{Z}_n^*} \chi(x - a) - \sum_{\substack{x - a \in \mathbb{Z}_n^* \\ x \notin \mathbb{Z}_n^*}} \chi(x - a)\end{aligned}$$

$$= -\sum_{\substack{x-a\in\mathbb{Z}_n^* \\ p|x}} \chi(x-a)$$
$$= -\chi(a)p^{\alpha-1}, \tag{4.2}$$

and

$$\begin{aligned}\sum_{x\in\mathbb{Z}_n^*}\chi(x(x-a)) &= \sum_{x\in\mathbb{Z}_n^*}\chi(x(x-a)x^{-2}) \\ &= \sum_{x\in\mathbb{Z}_n^*}\chi(1-ax^{-1}) \\ &= \sum_{x\in\mathbb{Z}_n^*}\chi(1-ax) \\ &= \chi(a)\sum_{x\in\mathbb{Z}_n^*}\chi(a^{-1}-x) \\ &= \chi(a)\left[\sum_{x\in\mathbb{Z}_n}\chi(a^{-1}-x) - \sum_{\substack{x\in\mathbb{Z}_n \\ p|x}}\chi(a^{-1}-x)\right] \\ &= -p^{\alpha-1}. \end{aligned} \tag{4.3}$$

Combining (4.1), (4.2) and (4.3) we obtain the required result. ■

Lemma 4.4. *Let $n = p^\alpha$, where $\alpha \geq 1$ and $p \equiv 1 \pmod 4$. Let χ be the unique character mod n of order 2. We have*

$$|\{x \in \mathbb{Z}_n : p \nmid x, 1-x^2; \chi(1-x^2) = 1\}| = \frac{p^{\alpha-1}(p-5)}{2}.$$

Proof. We evoke (2.2) and find that

$$|\{x \in \mathbb{Z}_{p^\alpha} : p \nmid x, 1-x^2; \chi(1-x^2) = 1\}| = \sum_{\substack{x\in\mathbb{Z}_{p^\alpha} \\ p\nmid x, 1-x^2}} \frac{1+\chi(1-x^2)}{2}$$

$$= \frac{1}{2} \sum_{\substack{x \in \mathbb{Z}_{p^\alpha} \\ p \nmid x, 1-x^2}} 1 + \frac{1}{2} \sum_{\substack{x \in \mathbb{Z}_{p^\alpha} \\ p \nmid x, 1-x^2}} \chi(1-x^2). \quad (4.4)$$

Since $p \nmid x$, let $x = pm + k$, where $0 < k < p$ and $m \in \mathbb{Z}$. If p divides $x^2 - 1$, then p divides $k^2 - 1 = (k-1)(k+1)$ which yields $k = 1$ or $p-1$. Hence the number of $x \in \mathbb{Z}_{p^\alpha}$ such that $p \nmid x$ but $p \mid x^2 - 1$ is equal to $2p^{\alpha-1}$. Now,

$$\begin{aligned} \sum_{\substack{x \in \mathbb{Z}_{p^\alpha} \\ p \nmid x, 1-x^2}} 1 &= |\{x \in \mathbb{Z}_{p^\alpha} : p \nmid x\}| - |\{x \in \mathbb{Z}_{p^\alpha} : p \nmid x, p \mid (1-x^2)\}| \\ &= \phi(p^\alpha) - 2p^{\alpha-1} \\ &= p^{\alpha-1}(p-3). \end{aligned}$$

Using this and employing Lemma 4.3 with $a = 1$, (4.4) yields the required result. ■

Lemma 4.5. *Let $n = p^\alpha$, where $\alpha \geq 1$ and $p \equiv 1 \pmod 4$. Let χ be the unique character mod n of order 2. For $a, b \in \mathbb{Z}_n$, we have*

$$\sum_{x \in \mathbb{Z}_n} \chi((x-a)(x-b)) = \begin{cases} p^{\alpha-1}(p-1), & \text{if } p \mid a, p \mid b; \\ -p^{\alpha-1}, & \text{if } p \mid a, p \nmid b; \\ -p^{\alpha-1}, & \text{if } p \nmid a, p \nmid b, p \nmid 1 - ba^{-1}; \\ p^{\alpha-1}(p-1), & \text{if } p \nmid a, p \nmid b, p \mid 1 - ba^{-1}. \end{cases}$$

Proof. We consider each of the four cases as given in the statement of the lemma. Let R_n and N_n be the subsets of $\mathbb{Z}_n^*$ of squares and non-squares, respectively. We make use of Theorem 1.19 as needed.

Case 1: Let $p \mid a$ and $p \mid b$. Then, using Lemma 2.9 we readily obtain that

$$\sum_{x \in \mathbb{Z}_n} \chi((x-a)(x-b)) = \sum_{x \in R_n} 1 + \sum_{x \in N_n} 1 = \phi(n) = p^{\alpha-1}(p-1).$$

Case 2: Let $p \mid a$ and $p \nmid b$. Again using Lemma 2.9, we have

$$\begin{aligned}\sum_{x\in\mathbb{Z}_n}\chi((x-a)(x-b)) &= \sum_{x\in R_n}\chi(x-b) - \sum_{x\in N_n}\chi(x-b)\\ &= 2\sum_{x\in R_n}\chi(x-b) - \sum_{x\in\mathbb{Z}_n^*}\chi(x-b). \qquad (4.5)\end{aligned}$$

We find that

$$2\sum_{x\in R_n}\chi(x-b) = \sum_{x\in\mathbb{Z}_n^*}\chi(x^2-b) = -(1+\chi(b))p^{\alpha-1} \qquad (4.6)$$

and

$$\sum_{x\in\mathbb{Z}_n^*}\chi(x-b) = -\sum_{p|x}\chi(x-b) = -\chi(b)p^{\alpha-1}. \qquad (4.7)$$

Combining (4.5), (4.6) and (4.7) we obtain the result.

Case 3: Let $p \nmid a$ and $p \nmid b$. Then

$$\begin{aligned}\sum_{x\in\mathbb{Z}_n}\chi((x-a)(x-b)) &= \sum_{x\in\mathbb{Z}_n}\chi((ax-a)(ax-b))\\ &= \sum_{x\in\mathbb{Z}_n}\chi((x-1)(x-ba^{-1}))\\ &= \sum_{y\in\mathbb{Z}_n^*}\chi(y)\chi(y+1-ba^{-1}). \qquad (4.8)\end{aligned}$$

The last equality is obtained by using the substitution $x-1=y$. If $p \mid 1-ba^{-1}$ then (4.8) becomes

$$\sum_{y\in\mathbb{Z}_n^*}\chi(y)\chi(y+1-ba^{-1}) = \sum_{y\in\mathbb{Z}_n^*}1 = \phi(n) = p^{\alpha-1}(p-1), \qquad (4.9)$$

and if $p \nmid 1 - ba^{-1}$ then using the substitution $c = 1 - ba^{-1}$ we have in (4.8),

$$\begin{aligned}\sum_{y\in\mathbb{Z}_n^*} \chi(y)\chi(y+1-ba^{-1}) &= \sum_{y\in\mathbb{Z}_n^*} \chi(1+cy^{-1}) \\ &= \sum_{y\in\mathbb{Z}_n^*} \chi(1+cy) \\ &= \chi(c)\sum_{y\in\mathbb{Z}_n^*} \chi(c^{-1}+y) \\ &= \chi(c)\left[-\sum_{p|y} \chi(c^{-1}+y)\right] \\ &= -p^{\alpha-1}.\end{aligned}$$

This completes the proof of the lemma. ■

4.2.2 Proof of Theorem 4.1

We prove Theorem 4.1 in the following manner. First, we prove two lemmas which will be required to prove the theorem. These lemmas essentially deal with the most intricate character sum that we encounter in the proof of the theorem. Using these lemmas, we provide the entire proof, where we recall these lemmas appropriately.

Lemma 4.6. *For a positive integer α, let $n = p^\alpha$, where p is a prime satisfying $p \equiv 1 \pmod 4$. Let χ be the quadratic character mod n. Let*

$$S = \sum_{x\in\mathbb{Z}_n}\sum_{y\in\mathbb{Z}_n} \chi((1-x^2)(1-y^2)(x^2-y^2))$$

and

$$S_0 = \sum_{(x,y)\in X}\sum \chi((1-x^2)(1-y^2)(x^2-y^2)),$$

where $X = \{(x,y) \in \mathbb{Z}_n \times \mathbb{Z}_n : p \nmid x, y, 1-x^2, 1-y^2, x^2-y^2\}$. Then, $S_0 = S + 4p^{2\alpha-2}$.

Proof. Breaking the double sum $\sum_{x\in\mathbb{Z}_n}\sum_{y\in\mathbb{Z}_n}$ in S as

$$\sum_{(x,y)\in X}\sum + \sum_{p|x}\sum_{y} + \sum_{\substack{p\nmid x\\ p|1-x^2}}\sum_{y} + \sum_{\substack{p\nmid x\\ p\nmid 1-x^2}}\sum_{p|y} + \sum_{\substack{p\nmid x\\ p\nmid 1-x^2}}\sum_{\substack{p\nmid y\\ p|1-y^2}} + \sum_{\substack{p\nmid x\\ p\nmid 1-x^2\\ p|x^2-y^2}}\sum_{\substack{p\nmid y\\ p\nmid 1-y^2}},$$

we write

$$S = S_0 + T_1 + T_2 + T_3 + T_4 + T_5. \tag{4.10}$$

We evoke Lemma 2.9 and employ Lemma 4.3 with $a = 1$ to evaluate the T_i's. We have

$$\begin{aligned}
T_1 &= \sum_{p|x}\sum_{y}\chi(1-x^2)\chi((1-y^2)(x^2-y^2))\\
&= \sum_{t=1}^{p^{\alpha-1}}\sum_{y}\chi((1-y^2)(p^2t^2-y^2))\\
&= \sum_{t=1}^{p^{\alpha-1}}\sum_{p|y}\chi(1-y^2)\chi(p^2t^2-y^2) \;+\; \sum_{t=1}^{p^{\alpha-1}}\sum_{p\nmid y}\chi(1-y^2)\chi(p^2t^2-y^2)\\
&= \sum_{t=1}^{p^{\alpha-1}}\sum_{p\nmid y}\chi(1-y^2)\\
&= -2p^{2\alpha-2}.
\end{aligned} \tag{4.11}$$

We also find that

$$\begin{aligned}
T_3 &= \sum_{\substack{p\nmid x\\ p\nmid 1-x^2}}\sum_{p|y}\chi(1-x^2)\chi(1-y^2)\chi(x^2-y^2)\\
&= \sum_{\substack{p\nmid x\\ p\nmid 1-x^2}}\sum_{t=1}^{p^{\alpha-1}}\chi(1-x^2)\chi(x^2-p^2t^2)
\end{aligned}$$

$$= \sum_{\substack{p\nmid x \\ p\nmid 1-x^2}} \sum_{t=1}^{p^{\alpha-1}} \chi(1-x^2)$$

$$= -2p^{2\alpha-2}. \tag{4.12}$$

It is easy to see that

$$T_2 = T_4 = T_5 = 0. \tag{4.13}$$

Using (4.11), (4.12) and (4.13), (4.10) yields the required result. ■

Lemma 4.7. *For a positive integer α, let $n = p^\alpha$, where p is a prime satisfying $p \equiv 1 \pmod 4$. Let χ be the quadratic character mod n and let ψ be a character mod n of order 4; let $J(\psi,\chi) = \sum_{x\in\mathbb{Z}_n} \psi(x)\chi(1-x)$ be the Jacobi sum of ψ and χ. If*

$$K = \sum_{x\in\mathbb{Z}_n^*} \sum_{y\in\mathbb{Z}_n^*} \chi((1-x)(1-y)(y-x)xy),$$

then $K = J(\psi,\chi)^2 + \overline{J(\psi,\chi)}^2$.

Proof. The proof goes along similar lines as adopted in [26]. For $x \in \mathbb{Z}_n^*$, we use the notation $\frac{1}{x}$ or x^{-1} to refer to the multiplicative inverse of x in $\mathbb{Z}_n^*$. We have

$$K = \sum_{\substack{p\nmid x,1-x \\ p\nmid x-y}} \sum_{p\nmid y,1-y} \chi((1-x)(1-y)(y-x)xyx^{-2}y^{-2})$$

$$= \sum_{\substack{p\nmid x,x-1 \\ p\nmid x-y}} \sum_{p\nmid y,y-1} \chi\left(\left((x-1)y^{-1}\right)\left((y-1)x^{-1}\right)(y-x)\right).$$

We break the sum into two parts. One part deals with the case when $p \mid x+y-1$ and the other part deals with the case when $p \nmid x+y-1$. First, we evaluate the part when $p \mid x+y-1$. Let $x+y-1 = tp$ for some $k \in \mathbb{Z}, 1 \le t \le p^{\alpha-1}$. Then by Lemma 2.9,

$$\chi((x-1)y^{-1}) = \chi(-1+tpy^{-1}) = \chi(-1) = 1.$$

Similarly,

$$\chi((y-1)x^{-1}) = 1 \text{ and } \chi(y-x) = \chi(2x-1).$$

Using these and Theorem 1.19, we get

$$\begin{aligned}
&\sum_{\substack{p\nmid x,x-1\\ p\nmid x-y\\ p\nmid x+y-1}} \sum_{p\nmid y,y-1} \chi((x-1)y^{-1})\chi((y-1)x^{-1})\chi(y-x)\\
&= \sum_{p\nmid x,x-1,2x-1} \sum_{t=1}^{p^{\alpha-1}} \chi(2x-1)\\
&= p^{\alpha-1} \sum_{p\nmid x,x-1,2x-1} \chi(2x-1)\\
&= p^{\alpha-1}\left[0 - \sum_{p\mid x} \chi(2x-1) - \sum_{\substack{p\nmid x\\ p\mid x-1}} \chi(2x-1)\right]\\
&= -2p^{2\alpha-2},
\end{aligned}$$

where we have used Lemma 2.9 as required. So K is reduced to the following expression.

$$K = -2p^{2\alpha-2} + \sum_{\substack{p\nmid x,x-1\\ p\nmid x-y\\ p\nmid x+y-1}} \sum_{p\nmid y,y-1} \chi\left(\frac{x-1}{y}\right)\chi\left(\frac{y-1}{x}\right)\chi(y-x). \tag{4.14}$$

Now, we use the substitution $t = \frac{x-1}{y}$ and $u = \frac{y-1}{x}$ in the above sum. Let

$$U = \sum_{\substack{p\nmid x,x-1\\ p\nmid x-y\\ p\nmid x+y-1}} \sum_{p\nmid y,y-1} \chi\left(\frac{x-1}{y}\right)\chi\left(\frac{y-1}{x}\right)\chi(y-x)$$

and

$$V = \sum_{\substack{p\nmid t,t+1\\ p\nmid u-t\\ p\nmid ut-1}} \sum_{p\nmid u,u+1} \chi(tu(u-t)(ut-1)).$$

Then we show that $U = V$ in what follows, which will imply that the substitution $t = \frac{x-1}{y}$ and $u = \frac{y-1}{x}$ is possible. It is easy to see that

$$\left\{\left(\frac{x-1}{y}, \frac{y-1}{x}\right) : (x,y) \in \mathbb{Z}_n \times \mathbb{Z}_n \text{ and } p \nmid x, x-1, y, y-1, x-y, x+y-1\right\}$$
$$=\{(t,u) : (t,u) \in \mathbb{Z}_n \times \mathbb{Z}_n \text{ and } p \nmid t, t+1, u, u+1, u-t, ut-1\}.$$

Let

$$U_1 = \{(x,y) \in \mathbb{Z}_n \times \mathbb{Z}_n \mid p \nmid x, x-1, y, y-1, x-y, x+y-1\};$$
$$V_1 = \{(t,u) \in \mathbb{Z}_n \times \mathbb{Z}_n \mid p \nmid t, t+1, u, u+1, u-t, ut-1\}.$$

Then

$$U = \sum_{(x,y)\in U_1} \sum \chi\left(\frac{x-1}{y}\right)\chi\left(\frac{y-1}{x}\right)\chi(y-x) \quad \text{and} \quad V = \sum_{(t,u)\in V_1} \sum \chi(tu(u-t)(ut-1)).$$

We note that $|U_1| = |V_1| = (p-3)^2 p^{2\alpha-2}$. Let us define an equivalence relation on U_1 as

$$(x,y) \sim (x',y') \quad \text{if and only if} \quad x \equiv x' \pmod{p} \quad \text{and} \quad y \equiv y' \pmod{p}$$

and similarly we define an equivalence relation on V_1 as

$$(t,u) \sim_1 (t',u') \quad \text{if and only if} \quad t \equiv t' \pmod{p} \quad \text{and} \quad u \equiv u' \pmod{p}.$$

Then

$$U = \sum_{(x,y)\in U_1}\sum (p^{\alpha-1})^2 \ \chi\left(\frac{x-1}{y}\right)\chi\left(\frac{y-1}{x}\right)\chi(y-x), \tag{4.15}$$

where the summation is over distinct equivalence class representatives corresponding to the equivalence relation $\sim$, because each equivalence class contains $(p^{\alpha-1})^2$ elements and for (x,y) and (x',y') in the same equivalence class,

$$\chi\left(\frac{x-1}{y}\right)\chi\left(\frac{y-1}{x}\right)\chi(y-x) = \chi\left(\frac{x'-1}{y'}\right)\chi\left(\frac{y'-1}{x'}\right)\chi(y'-x').$$

Again, let $(t,u) \in V_1$. Then for any $(t',u') \in V_1$ which belongs to the equivalence class of (t,u) corresponding to the equivalence relation $\sim_1$, $\chi(tu(u-t)(ut-1)) = \chi(t'u'(u'-t')(u't'-1))$. So

$$V = \sum_{(t,u)\in V_1}\sum (p^{\alpha-1})^2 \ \chi(tu(u-t)(ut-1)), \tag{4.16}$$

where the summation is over distinct equivalence class representatives corresponding to the equivalence relation $\sim_1$, similar to (4.15).

Now, for a class representative $(x,y) \in U_1$ corresponding to the equivalence relation $\sim$, $\chi\left(\frac{x-1}{y}\right)\chi\left(\frac{y-1}{x}\right)\chi(y-x) = \chi(tu(u-t)(ut-1))$ for some $(t,u) \in V_1$. So

$$(p^{\alpha-1})^2 \ \chi\left(\frac{x-1}{y}\right)\chi\left(\frac{y-1}{x}\right)\chi(y-x) = (p^{\alpha-1})^2\chi(tu(u-t)(ut-1)). \tag{4.17}$$

What remains to be seen is that if (x,y) and $(x_1,y_1) \in U_1$ are in different equivalence classes of the equivalence relation $\sim$, (t,u) and $(t_1,u_1) \in V_1$ are in different equivalence classes of the equivalence relation $\sim_1$ as well, where $t = \frac{x-1}{y}, u = \frac{y-1}{x}, t_1 = \frac{x_1-1}{y_1}, u_1 = \frac{y_1-1}{x_1}$. But this is immediate since $(x,y) \not\sim (x_1,y_1)$ implies that $(t,u) \not\sim_1 (t_1,u_1)$. Thus combining (4.15), (4.16) and (4.17) we have proved that

$U = V$. Therefore, (4.14) yields

$$\begin{aligned} K &= -2p^{2\alpha-2} + \sum_{p\nmid t,t+1} \sum_{\substack{p\nmid u,u+1 \\ p\nmid u-t \\ p\nmid ut-1}} \chi(tu(u-t)(ut-1)) \\ &= \sum_{p\nmid t} \sum_{\substack{p\nmid u \\ p\nmid u-t \\ p\nmid ut-1}} \chi(tu(u-t)(ut-1)) \\ &= \sum_{p\nmid t,t-1} \chi(t(t-1)) \sum_{p\nmid u,u^2-t} \chi(u(u^2-t)), \end{aligned} \tag{4.18}$$

where the last summation is obtained by the substitution $t \mapsto \frac{t}{u}$. The sum in (4.18) indexed by u remains to be reduced, and following a similar approach as given in [26], we proceed as in the proof of Theorem 1.33 to simplify this sum. Then for each t in the sum indexed by t in (4.18), we have

$$\begin{aligned} \sum_{p\nmid u,u^2-t} \chi(u(u^2-t)) &= \sum_{p\nmid u,u^2-t} \psi^2(u)\psi^2(u^2-t) \\ &= \sum_{u\in\mathbb{Z}_n^*} \psi(u^2)\psi^2(u^2-t) \\ &= \sum_{u\in\mathbb{Z}_n^*} \psi(u)\psi^2(u-t)(1+\chi(u)) \\ &= \sum_{u\in\mathbb{Z}_n^*} \psi(u)\psi^2(u-t) + \sum_{u\in\mathbb{Z}_n^*} \psi\chi(u)\psi^2(u-t). \end{aligned} \tag{4.19}$$

The first sum in (4.19) is

$$\begin{aligned} \sum_{u\in\mathbb{Z}_n^*} \psi(u)\psi^2(u-t) &= \sum_{u\in\mathbb{Z}_n^*} \psi(ut)\psi^2(ut-t) \\ &= \overline{\psi}(t) \sum_{u\in\mathbb{Z}_n^*} \psi(u)\psi^2(u-1) \\ &= \overline{\psi}(t) J(\psi,\psi^2) \\ &= \overline{\psi}(t) J(\psi,\chi). \end{aligned} \tag{4.20}$$

Similarly we simplify the second sum in (4.19) and obtain

$$\sum_{u\in\mathbb{Z}_n^*}\psi\chi(u)\psi^2(u-t)=\psi(t)J(\overline{\psi},\chi). \tag{4.21}$$

Combining (4.19), (4.20), (4.21), and (4.18), we have

$$K=\sum_{p\nmid t,t-1}\chi(t(t-1))[\bar{\psi}(t)J(\psi,\chi)+\psi(t)J(\overline{\psi},\chi)]$$

and hence $K=J(\psi,\chi)^2+\overline{J(\psi,\chi)}^2$. This completes the proof of the lemma. ■

Having all the required lemmas proved, we are now ready to prove Theorem 4.1. We shall proceed in a similar fashion as in [26].

Proof of Theorem 4.1. Let H_{p^α} denote the subgraph of G_{p^α} induced by the set of squares in $\mathbb{Z}_{p^\alpha}^*$, and let $f(p^\alpha)$ denote the number of triangles in H_{p^α} containing 1. Then, Proposition 2.16 yields

$$\mathcal{K}_4(G_{p^\alpha})=\frac{p^{2\alpha-1}(p-1)f(p^\alpha)}{24}, \tag{4.22}$$

so we are left to evaluate $f(p^\alpha)$. Let

$$X=\{(x,y)\in\mathbb{Z}_{p^\alpha}\times\mathbb{Z}_{p^\alpha}:p\nmid x,y,1-x^2,1-y^2,x^2-y^2\}.$$

Then,

$$f(p^\alpha)=\frac{1}{8}\times|\{(x,y)\in X:\chi(1-x^2)=\chi(1-y^2)=\chi(x^2-y^2)=1\}|.$$

Let $X=A_1\cup A_2\cup\cdots\cup A_8$, where $A_1,A_2,\ldots,A_8$ are as given in Table 4.1. For example, A_2 is the subset of X such that for any $(x,y)\in A_2$, we have $\chi(1-x^2)=1,\chi(1-y^2)=1$ and $\chi(x^2-y^2)=-1$. Let $\beta_i=|A_i|$ for $i=1,2,\ldots,8$. Our objective is to find β_1 since we have $f(p^\alpha)=\frac{1}{8}\beta_1$. To find β_1, we employ some relations

Subset of X	$\chi(1-x^2)$	$\chi(1-y^2)$	$\chi(x^2-y^2)$
A_1	1	1	1
A_2	1	1	-1
A_3	1	-1	1
A_4	1	-1	-1
A_5	-1	1	1
A_6	-1	1	-1
A_7	-1	-1	1
A_8	-1	-1	-1

Table 4.1: The sets $A_1, \ldots, A_8$

between the β_i's which we proceed to find out, similar to what is done in [26]. Now,

$A_1 \cup A_2$

$= \{(x,y) \in \mathbb{Z}_{p^\alpha} \times \mathbb{Z}_{p^\alpha} : p \nmid x, 1-x^2, y, 1-y^2, x^2-y^2; \chi(1-x^2)=1; \chi(1-y^2)=1\}.$

Using Lemma 4.4, we find that

$$A := |A_1 \cup A_2| = p^{2\alpha-2}\left(\frac{p-5}{2}\right)\left(\frac{p-9}{2}\right). \tag{4.23}$$

Again, we have

$A_3 \cup A_4$

$= \{(x,y) \in \mathbb{Z}_{p^\alpha} \times \mathbb{Z}_{p^\alpha} : p \nmid x, 1-x^2, y, 1-y^2, x^2-y^2; \chi(1-x^2)=1; \chi(1-y^2)=-1\}.$

We calculate the cardinality of $A_3 \cup A_4$ in the following manner. The total number of $y \in \mathbb{Z}_{p^\alpha}^*$ such that $\chi(1-y^2) = \pm 1$ is the number of $y \in \mathbb{Z}_{p^\alpha}^*$ such that $p \nmid y^2-1$, which is $p^\alpha - 2p^{\alpha-1} = p^{\alpha-1}(p-2)$. Out of them, the number of $y \in \mathbb{Z}_{p^\alpha}^*$ such that $\chi(1-y^2)=1$ is $\frac{p^{\alpha-1}(p-5)}{2}$ by Lemma 4.4. So the remaining number of $y \in \mathbb{Z}_{p^\alpha}^*$ is $p^{\alpha-1}(p-2) - \frac{p^{\alpha-1}(p-5)}{2} - \gamma$, where γ is the number of y such that $\chi(1-y^2)=1$ and

$p \mid y$. Clearly, $\gamma = p^{\alpha-1}$. Hence

$$B := |A_3 \cup A_4| = p^{2\alpha-2}\left(\frac{p-5}{2}\right)\left(\frac{p-1}{2}\right). \tag{4.24}$$

Recalling (4.23) and (4.24) we get

$$\beta_1 + \beta_2 = A$$

$$\beta_3 + \beta_4 = B.$$

We define a bijection from $A_1 \cup A_3$ to $A_1 \cup A_2$ as

$$(x, y) \mapsto (x, xy^{-1}).$$

Then $\beta_1 + \beta_3 = \beta_1 + \beta_2$. In a similar fashion we get other relations among the β_i's in terms of A and B (as named in (4.23) and (4.24)). In particular, we have

$$\begin{aligned}
\beta_1 + \beta_2 &= A;\\
\beta_1 + \beta_3 &= A;\\
\beta_3 + \beta_4 &= B;\\
\beta_1 + \beta_5 &= A;\\
\beta_2 + \beta_6 &= B;\\
\beta_5 + \beta_7 &= B;\\
\beta_7 + \beta_8 &= B.
\end{aligned} \tag{4.25}$$

Let

$$S = \sum_{x \in \mathbb{Z}_{p^\alpha}} \sum_{y \in \mathbb{Z}_{p^\alpha}} \chi((1-x^2)(1-y^2)(x^2-y^2))$$

and

$$S_0 = \sum_{(x,y)\in X}\sum \chi((1-x^2)(1-y^2)(x^2-y^2)).$$

Using (4.25) we have

$$\begin{aligned} S_0 &= \sum_{(x,y)\in A_1}\sum \chi((1-x^2)(1-y^2)(x^2-y^2)) + \cdots + \sum_{(x,y)\in A_8}\sum \chi((1-x^2)(1-y^2)(x^2-y^2)) \\ &= \beta_1 - \beta_2 - \beta_3 + \beta_4 - \beta_5 + \beta_6 + \beta_7 - \beta_8 \\ &= \beta_1 - (A-\beta_1) - (A-\beta_1) + (B-\beta_3) - (A-\beta_1) + (B-\beta_2) + (B-\beta_5) - (B-\beta_7) \\ &= 64f(p^\alpha) + p^{2\alpha-2}(p-5)(15-p). \end{aligned} \tag{4.26}$$

Employing Lemma 4.6 and (4.26) we have

$$f(p^\alpha) = \frac{S + p^{2\alpha-2}(p^2-20p+79)}{64}. \tag{4.27}$$

Now,

$$S = \sum_{p|x}\sum_{y} \chi((1-x^2)(1-y^2)(x^2-y^2)) + \sum_{p\nmid x}\sum_{y} \chi((1-x^2)(1-y^2)(x^2-y^2)). \tag{4.28}$$

The first term in (4.28) is

$$\begin{aligned} \sum_{p|x}\sum_{y} \chi(1-x^2)\chi((1-y^2)(x^2-y^2)) &= \sum_{p|x}\sum_{p|y} \chi(1-y^2)\chi(x^2-y^2) \\ &\quad + \sum_{p|x}\sum_{p\nmid y} \chi(1-y^2)\chi(x^2-y^2) \\ &= \sum_{p|x}\sum_{p\nmid y} \chi(1-y^2)\chi(x^2-y^2) \\ &= \sum_{p|x}\sum_{p\nmid y} \chi(1-y^2) \end{aligned}$$

$$= -2p^{2\alpha-2}.$$

So, (4.28) yields

$$\begin{aligned} S &= -2p^{2\alpha-2} + \sum_{p\nmid x}\sum_{y} \chi((1-x^2)(1-y^2)(x^2-y^2)) \\ &= -2p^{2\alpha-2} + \sum_{p\nmid x}\sum_{p\mid y} \chi((1-x^2)(1-y^2)(x^2-y^2)) \\ &+ \sum_{p\nmid x}\sum_{p\nmid y} \chi((1-x^2)(1-y^2)(x^2-y^2)). \end{aligned} \tag{4.29}$$

We have

$$\sum_{p\nmid x}\sum_{p\mid y} \chi(1-x^2)\chi(1-y^2)\chi(x^2-y^2) = \sum_{p\nmid x}\sum_{p\mid y} \chi(1-x^2) = -2p^{2\alpha-2},$$

so (4.29) yields

$$\begin{aligned} S &= -4p^{2\alpha-2} + \sum_{p\nmid x}\sum_{p\nmid y} \chi((1-x^2)(1-y^2)(x^2-y^2)) \\ &= -4p^{2\alpha-2} + \sum_{p\nmid x} \chi(1-x^2) \sum_{p\nmid y} \chi((1-y)(x^2-y)) \{1+\chi(y)\} \\ &= -4p^{2\alpha-2} + \sum_{p\nmid y} \chi(1-y) \{1+\chi(y)\} \sum_{p\nmid x} \chi((1-x^2)(y-x^2)) \\ &= -4p^{2\alpha-2} + \sum_{p\nmid y} \chi(1-y) \{1+\chi(y)\} \sum_{p\nmid x} \chi((1-x)(y-x)) \{1+\chi(x)\} \\ &= -4p^{2\alpha-2} + \sum_{p\nmid x}\sum_{p\nmid y} \chi((1-x)(1-y)(y-x)) \{1+\chi(x)\} \{1+\chi(y)\}. \end{aligned}$$

Now, we break the sum S into three parts as in [26]. Let

$$S = -4p^{2\alpha-2} + I + 2J + K, \tag{4.30}$$

where

$$I = \sum_{p\nmid x}\sum_{p\nmid y}\chi((1-x)(1-y)(y-x)),$$

$$J = \sum_{p\nmid x}\sum_{p\nmid y}\chi((1-x)(1-y)(y-x)x),$$

and

$$K = \sum_{p\nmid x}\sum_{p\nmid y}\chi((1-x)(1-y)(y-x)xy).$$

We evaluate I using Lemma 4.5.

$$\begin{aligned}
I &= \sum_{p\nmid x}\sum_{p\nmid y}\chi((1-x)(1-y)(y-x)) \\
&= \sum_{p\nmid x}\chi(1-x)\sum_{p\nmid y}\chi((1-y)(x-y)) \\
&= \sum_{p\nmid x}\chi(1-x)\left[\sum_{y}\chi((1-y)(x-y)) - \sum_{p\mid y}\chi((1-y)(x-y))\right] \\
&= \sum_{\substack{p\nmid x\\ p\nmid 1-x}}\chi(1-x)\left[-p^{\alpha-1} - p^{\alpha-1}\chi(x)\right] \\
&= 2p^{2\alpha-2}.
\end{aligned} \tag{4.31}$$

We further evaluate J and evoke Lemma 4.5 for the same.

$$\begin{aligned}
J &= \sum_{p\nmid x}\sum_{p\nmid y}\chi((1-x)(1-y)(y-x)x) \\
&= \sum_{p\nmid x,x-1}\chi(x(1-x))\sum_{p\nmid y}\chi((1-y)(y-x)) \\
&= \sum_{p\nmid x,x-1}\chi(x(1-x))\left[-p^{\alpha-1} - p^{\alpha-1}\chi(x)\right] \\
&= 2p^{2\alpha-2}.
\end{aligned} \tag{4.32}$$

Using (4.31), (4.32) and Lemma 4.7, (4.30) yields

$$S = -4p^{2\alpha-2} + I + 2J + K = 2p^{2\alpha-2} + J(\psi,\chi)^2 + \overline{J(\psi,\chi)}^2. \tag{4.33}$$

Combining (4.27) and (4.33), we obtain

$$f(p^\alpha) = \frac{p^{2\alpha-2}(p^2 - 20p + 81) + J(\psi,\chi)^2 + \overline{J(\psi,\chi)}^2}{64}.$$

Finally, putting the value of $f(p^\alpha)$ in (4.22), we complete the proof. ■

5

Cliques of order four in the Paley-type graph on $\mathbb{Z}_n$ for general n

5.1 Introduction

The Paley-type graph G_n we defined in Chapter 2 resembles the classical Paley graph in a number of ways, and adds to the list of generalizations of the Paley graph. In Chapter 4, we found the number of cliques of order four in G_n, that is $\mathcal{K}_4(G_n)$, for $n = p^\alpha$ using a character sum approach. However, the same approach is not applicable for general n. In this chapter, we follow a combinatorial approach and

[1]The contents of this chapter are under review.

find $\mathcal{K}_4(G_n)$ for all n for which the graph G_n is defined. We omit the case when n is even since there cannot exist cliques of order more than two in G_n in that case. We note that the expression for $\mathcal{K}_4(G_n)$ proved in this chapter does not contain any Jacobi sums. Hence, combining this expression for $n = p^\alpha$ with the one given in Theorem 4.1, we find values of certain character sums modulo p^α which were earlier known for prime modulus only.

5.2 The number of cliques of order four in G_n

In the following theorem, we provide a closed formula for the number of cliques of order four in G_n for odd n. Note that if $p \equiv 1 \pmod 4$ is a prime, then there exist integers a and b such that $p = a^2 + b^2$, where a is even; a^2 and b^2 are unique.

Theorem 5.1. *Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $\alpha_i \geq 1$ and the distinct primes p_i satisfy $p_i \equiv 1 \pmod 4$ for all $i = 1, \ldots, k$. For $i \in \{1, \ldots, k\}$, let $p_i = a_i^2 + b_i^2$, where a_i, b_i are integers and a_i is even. Then, the number of cliques of order four in G_n is given by*

$$\mathcal{K}_4(G_n) = \frac{1}{3 \times 8^{2k+1}} \prod_{i=1}^{k} \left[p_i^{4\alpha_i - 3}(p_i - 1)\{(p_i - 9)^2 - 4a_i^2\} \right].$$

To show that the expression for $\mathcal{K}_4(G_n)$ is an integer, we begin by showing that for $i \in \{1, 2, \ldots, k\}$, $64 \mid (p_i - 9)^2 - 4a_i^2$. Let $p_i = 4s_i + 1$. We have, $(p_i - 9)^2 - 4a_i^2 = 16\left[\left(\frac{p_i - 1}{4} - 2\right)^2 - (\frac{a_i}{2})^2\right] = 16\left[(s_i - 2)^2 - (\frac{a_i}{2})^2\right]$, so it is enough to show that $4 \mid s_i^2 - (\frac{a_i}{2})^2$. The relation $4s_i + 1 = p_i = a_i^2 + b_i^2$ yields $s_i = (\frac{a_i}{2})^2 + (\frac{b_i^2 - 1}{4})$, and since $\frac{b_i^2 - 1}{4}$ is even, s_i and $\frac{a_i}{2}$ have the same parity. So, we obtain that $4 \mid s_i^2 - (\frac{a_i}{2})^2$. Now, to show that the expression for $\mathcal{K}_4(G_n)$ is an integer, we write $\mathcal{K}_4(G_n) = \frac{1}{3 \times 8} \prod_{i=1}^{k} \left[p_i^{4\alpha_i - 3}(p_i - 1) \left\{ \frac{(p_i - 9)^2 - 4a_i^2}{64} \right\} \right]$, so it is enough to show that $3 \times 8 \mid (p_1 - 1) \left\{ \frac{(p_1 - 9)^2 - 4a_1^2}{64} \right\}$, that is, $3 \times 8 \mid s_1 \left\{ (s_1 - 2)^2 - (\frac{a_1}{2})^2 \right\}$. We find that $8 \mid s_1 \left\{ (s_1 - 2)^2 - (\frac{a_1}{2})^2 \right\}$ follows from the fact that s_1 and $\frac{a_1}{2}$ have the same parity.

Finally, we obtain that $3 \mid s_1\left\{(s_1-2)^2-(\frac{a_1}{2})^2\right\}$ by considering the cases $s_1 \equiv 0,1,2 \pmod 3$ and using the relation $4s_1+1 = 4(\frac{a_1}{2})^2 + b_1^2$ after reduction modulo 3.

We find the values of $\mathcal{K}_4(G_n)$ for some specific values of n by using `Python` which are listed in Table 5.1.

n	$\mathcal{K}_4(G_n)$	n	$\mathcal{K}_4(G_n)$
13^2	0	13×17	0
17^2	0	$13^2 \times 17$	0
29^2	143578043	29×37	2703960
37^2	1040159355	29×41	4993800

Table 5.1: Values of $\mathcal{K}_4(G_n)$

For the primes $p = 13, 17, 29, 37, 41$, we have $p = a^2+b^2$, where $a^2 = 4, 16, 4, 36, 16$, respectively. By putting these values in Theorem 5.1, we obtain the same values of $\mathcal{K}_4(G_n)$ as listed in Table 5.1.

5.2.1 Some corollaries of Theorem 5.1

As a consequence of Theorem 5.1, we readily obtain the following formula for $\mathcal{K}_4(G_{p^\alpha})$ by taking $k = 1$ which does not involve any Jacobi sums, unlike Theorem 4.1 in the previous chapter.

Corollary 5.1.1. *Let $p \equiv 1 \pmod 4$ be a prime and let α be a positive integer. Let $p = a^2 + b^2$, where a and b are integers such that a is even. Then, the number of cliques of order four in G_{p^α} is given by*

$$\mathcal{K}_4(G_{p^\alpha}) = \frac{p^{4\alpha-3}(p-1)\{(p-9)^2-4a^2\}}{2^9 \times 3}.$$

Let $p \equiv 1 \pmod 4$ be a prime such that $p = a^2 + b^2$ with a even. Let χ and ψ be characters modulo p of orders 2 and 4, respectively. Then it follows from Theorem 1.35 that for suitably chosen signs of a and b, the Jacobi sum $J(\psi, \chi) =$

$b+ai$. Combining Theorem 4.1 and Corollary 5.1.1, we readily obtain the following corollary which extends Theorem 1.35 to characters modulo prime powers.

Corollary 5.1.2. *Let $p \equiv 1 \pmod 4$ be a prime such that $p = a^2 + b^2$ with a even. Let α be a positive integer. Let χ denote the unique quadratic Dirichlet character mod p^α and let ψ be a Dirichlet character mod p^α of order 4. Let $J := J(\psi, \chi) = x + iy$ be the Jacobi sum. Then,*

$$J^2 + \bar{J}^2 = 2(x^2 - y^2) = 2p^{2\alpha-2}(p - 2a^2). \tag{5.1}$$

Note that by Proposition 1.17 there are two Dirichlet characters modulo p^α of order 4, namely ψ and $\overline{\psi}$, and $J(\overline{\psi}, \chi) = \overline{J(\psi, \chi)} = x - iy$. So, (5.1) is independent of the choice of a character of order 4. The identity (5.1) follows from Theorem 1.35 when $\alpha = 1$. We do not know if the identity (5.1) already exists in the literature when $\alpha > 1$. In Table 5.2, we calculate x and y by using `Python` and verify (5.1) for some particular values of p and α.

$p, a^2, p-2a^2$	α	x	y	x^2-y^2	$p^{2\alpha-2}$
$p=5=2^2+1^2$,	2	5	10	$5^2\times(-3)$	5^2
$a^2=4, p-2a^2=-3$	3	25	50	$5^4\times(-3)$	5^4
$p=13=2^2+3^2$,	2	-39	26	$13^2\times 5$	13^2
$a^2=4, p-2a^2=5$	3	-507	338	$13^4\times 5$	13^4
$p=17=4^2+1^2$,	2	-17	68	$17^2\times(-15)$	17^2
$a^2=16, p-2a^2=-15$	3	-289	1156	$17^4\times(-15)$	17^4
$p=29=2^2+5^2$,	1	5	2	21	1
$a^2=4, p-2a^2=21$	2	145	58	$29^2\times 21$	29^2
$p=37=6^2+1^2$,	1	1	-6	-35	1
$a^2=36, p-2a^2=-35$	2	37	-222	$37^2\times(-35)$	37^2
$p=41=4^2+5^2$,	1	-5	4	9	1
$a^2=16, p-2a^2=9$	2	-205	164	$41^2\times 9$	41^2

Table 5.2: Numerical data for (5.1)

We also prove the following corollary which follows from Theorem 5.1.

Corollary 5.1.3. *Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $\alpha_i \geq 1$ and the distinct primes p_i satisfy $p_i \equiv 1 \pmod 4$ for all $i = 1, \ldots, k$. Then, $\mathcal{K}_4(G_n) = 0$ if and only if $p_i \in \{5, 13, 17\}$ for some $i \in \{1, \ldots, k\}$.*

Proof. From Theorem 5.1 we find that $\mathcal{K}_4(G_n) = 0$ if and only if $(p_i-9)^2-4a_i^2 = 0$ for some $i \in \{1, \ldots, k\}$, where $p_i = a_i^2+b_i^2$ for integers a_i and b_i such that a_i is even. So, we have $(p_i-9)^2-4a_i^2 = 0$ if and only if $(p_i-9)^2-4(p_i-b_i^2) = 0$. Solving this equation as a quadratic equation in p_i, we have $p_i^2 - 22p_i + (81 + 4b_i^2) = 0$, and readily obtain $p_i = 11 \pm 2\sqrt{10 - b_i^2}$. Then we have the inequality $p_i \leq 11 + 2\sqrt{10} \approx 17.3245\ldots$ and so, $p_i \leq 17$. The only primes $p \equiv 1 \pmod 4$ satisfying $p \leq 17$ are $5, 13$ and 17. Finally, we finish the proof by observing that for $p \in \{5, 13, 17\}$, if $p = a^2 + b^2$ for integers a and b such that a is even, then $(p - 9)^2 - 4a^2 = 0$. ■

As a consequence of Theorem 3.2 and Corollary 5.1.3, we readily obtain the following. Recall that the clique number of a graph is the order of a clique of maximum size contained in the graph.

Corollary 5.1.4. *Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $\alpha_i \geq 1$ and the distinct primes p_i satisfy $p_i \equiv 1 \pmod 4$ for all $i = 1, \ldots, k$. We have:*

1. *if $p_i = 5$ for some $i \in \{1, \ldots, k\}$ then the clique number of G_n is 2; and*
2. *if $p_i \in \{13, 17\}$ for some $i \in \{1, \ldots, k\}$ and $5 \nmid n$ then the clique number of G_n is 3.*

5.2.2 Proof of Theorem 5.1

For primes $p \equiv 1 \pmod 4$ and positive integers α, the following lemma lists the squares in $\mathbb{Z}_{p^\alpha}^*$ in terms of the squares in $\mathbb{Z}_p^*$.

Lemma 5.2. *Let p be a prime satisfying $p \equiv 1 \pmod 4$, and let α be a positive integer. Let R_p denote the set of non-zero squares in $\mathbb{Z}_p$, say $R_p := (\mathbb{Z}_p^*)^2 =$*

$\{r_1, \ldots, r_{\frac{p-1}{2}}\}$. *Then the set of squares in* $\mathbb{Z}^*_{p^\alpha}$ *is given by*

$$R_{p^\alpha} = \bigcup_{i=1}^{\frac{p-1}{2}} \{r_i + tp : t \text{ is an integer satisfying } 0 \leq t \leq p^{\alpha-1} - 1\}.$$

Proof. Consider $r_i \in R_p$ for some $i \in \{1, \ldots, \frac{p-1}{2}\}$, and $0 \leq t \leq p^{\alpha-1} - 1$. We show that $(r_i + tp)^{\frac{\phi(p^\alpha)}{2}} \equiv 1 \pmod{p^\alpha}$. By the binomial theorem, we find that

$$(r_i + tp)^{\frac{\phi(p^\alpha)}{2}} = \sum_{m=0}^{\frac{\phi(p^\alpha)}{2}} \binom{\frac{\phi(p^\alpha)}{2}}{m} r_i^{\frac{\phi(p^\alpha)}{2} - m} (tp)^m.$$

Then, using Lemma 2.8 we have $(r_i + tp)^{\frac{\phi(p^\alpha)}{2}} \equiv r_i^{\frac{\phi(p^\alpha)}{2}} \pmod{p^\alpha}$. So, we proceed to show that $r_i^{\frac{\phi(p^\alpha)}{2}} \equiv 1 \pmod{p^\alpha}$. Now, $r_i \in R_p$ implies $r_i^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ by Corollary 1.10.1, so we have $r_i^{\frac{p-1}{2}} = 1 + pX$ for some integer X. Again applying the binomial theorem, we find that

$$(r_i^{\frac{p-1}{2}})^{p^{\alpha-1}} = (1 + pX)^{p^{\alpha-1}} = \sum_{l=0}^{p^{\alpha-1}} \binom{p^{\alpha-1}}{l} p^l X^l.$$

So, it suffices to show that if $1 \leq l \leq \alpha - 1$ then $p^{\alpha-l} \mid \binom{p^{\alpha-1}}{l}$. We proceed along similar lines as in the proof of Lemma 2.8. Let $\sigma_p(y)$ denote the sum of the digits of the base-p representation of y. We have

$$\begin{aligned} \binom{p^{\alpha-1}}{l} &= \frac{p^{\alpha-1}(p^{\alpha-1} - 1) \cdots (p^{\alpha-1} - l + 1)}{l!} \\ &= \frac{p^{\alpha-l} p^{l-1} (p^{\alpha-1} - 1) \cdots (p^{\alpha-1} - l + 1)}{l!}. \end{aligned}$$

If possible, let $p^l \mid l!$. Recalling Definition 2.6, we have $v_p(l!) \geq l$, which implies $\frac{l - \sigma_p(l)}{p-1} \geq l$, which is not possible. So, $p^{\alpha-l} \mid \binom{p^{\alpha-1}}{l}$ and hence $r_i^{\frac{\phi(p^\alpha)}{2}} \equiv 1 \pmod{p^\alpha}$. Thus, we have proved that $(r_i + tp)^{\frac{\phi(p^\alpha)}{2}} \equiv 1 \pmod{p^\alpha}$. Since $\mathbb{Z}^*_{p^\alpha}$ is cyclic of order $\phi(p^\alpha)$, this implies $r_i + tp \in R_{p^\alpha}$. Conversely, let $z \in R_{p^\alpha}$. Then $z \equiv x^2 \pmod{p^\alpha}$

for some unit $x \in \mathbb{Z}_{p^\alpha}$, which implies $z \equiv x^2 \pmod{p}$. Thus, $z \equiv r_i \pmod{p}$ for some $i \in \{1, \ldots, \frac{p-1}{2}\}$ and our proof is complete. ■

Remark 5.3. *Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $\alpha_i \geq 1$ and the distinct primes p_i satisfy $p_i \equiv 1 \pmod{4}$ for all $i = 1, \ldots, k$. Let $x \in \mathbb{Z}_n$. Then by Lemmas 3.4 and 5.2, we have*

$$x \in R_n \text{ if and only if } x \pmod{p_i} \in R_{p_i} \text{ for } i = 1, \ldots, k.$$

This yields

$$|R_n| = \prod_{i=1}^{k} \left(p_i^{\alpha_i - 1} \times \frac{p_i - 1}{2} \right) = \frac{\phi(n)}{2^k}.$$

Now, we prove a lemma which will be used to prove Theorem 5.1. Before stating the lemma, we recall a proposition from [26] which will be used in the proof of the lemma.

Proposition 5.4. [26, Proposition 4] *Suppose that $p \equiv 1 \pmod{4}$ is a prime, and $p = a^2 + b^2$ with a even. Let $P(p)$ be the Paley graph of order p, let H_p be the subgraph of $P(p)$ induced by the set of non-zero squares in $\mathbb{Z}_p$ and let $f(p)$ be the number of triangles in H_p containing the vertex 1. Then,*

$$f(p) = \frac{(p-9)^2 - 4a^2}{64}.$$

The following lemma counts the number of triangles of a particular kind in the graph G_{p^α} in terms of the number of triangles in G_p. We use Notation 1.57.

Lemma 5.5. *Let $p \equiv 1 \pmod{4}$ be a prime and let α be a positive integer. Let G_{p^α} denote the Paley-type graph of order p^α and let H_{p^α} denote its subgraph induced by the set of squares in $\mathbb{Z}_{p^\alpha}^*$. Let $P(p)$ denote the Paley graph of order p and let H_p denote its subgraph induced by the non-zero squares in $\mathbb{Z}_p$. Let $p = a^2 + b^2$, where a and b are integers such that a is even. Then, the number of triangles in H_{p^α}*

containing the vertex 1 *is given by*

$$\mathcal{K}_3(H_{p^\alpha}, 1) = p^{2\alpha-2} \times \mathcal{K}_3(H_p, 1) = p^{2\alpha-2} \times \left(\frac{(p-9)^2 - 4a^2}{64}\right).$$

Proof. Let R_{p^α} and R_p denote the set of squares in $\mathbb{Z}_{p^\alpha}^*$ and $\mathbb{Z}_p^*$, respectively. Let $(1, x, y)$ denote a triangle in H_{p^α} containing the vertex 1, where $x, y \in \mathbb{Z}_{p^\alpha}$. Then, $x, y, x-1, y-1, x-y \in R_{p^\alpha}$ and so, $(1 \pmod p), x \pmod p), y \pmod p))$ yields a triangle in H_p containing the vertex 1. Conversely, let $(1, c, d)$ denote a triangle in H_p containing the vertex 1, whereby $c, d, c-1, d-1, c-d \in R_p$. Employing Lemma 5.2, we find that $(1, c+tp, d+t'p)$ yields a triangle in H_{p^α} containing the vertex 1, where t, t' are integers satisfying $0 \leq t, t' \leq p^{\alpha-1} - 1$. Each such triangle constructed in H_{p^α} is unique: if $(1, c+tp, d+t'p)$ and $(1, d+t''p, c+t'''p)$ yield the same triangle $(0 \leq t, t', t'', t''' \leq p^{\alpha-1} - 1)$, this implies $c \equiv d \pmod p$ which is a contradiction. Thus, the triangle $(1, c, d)$ in H_p produces $(p^{\alpha-1})^2$ distinct triangles in H_{p^α} containing the vertex 1. We have proved the first equality in the statement of the lemma. The second equality follows from Proposition 5.4. This completes the proof of the lemma. ■

Having all the required lemmas proved, we are now ready to prove Theorem 5.1.

Proof of Theorem 5.1. Let H_n denote the subgraph of G_n induced by the set of squares in $\mathbb{Z}_n^*$. Employing Proposition 2.16 and using Notation 1.57, we have

$$\mathcal{K}_4(G_n) = \frac{n\phi(n)}{3 \times 2^{k+2}} \times \mathcal{K}_3(H_n, 1). \tag{5.2}$$

Let F denote the set of triangles in H_n containing the vertex 1, and for $i \in \{1, \ldots, k\}$ let F_i denote the set of triangles in $H_{p_i^{\alpha_i}}$ containing the vertex 1. Let us set the notation $(1, x, y)$ to denote the triangle with the vertices $1, x$ and y. We define the

following map:

$$\begin{aligned} g : F &\to F_1 \times \cdots \times F_k \\ (1, x, y) &\mapsto ((1 \pmod{p_1^{\alpha_1}}, x \pmod{p_1^{\alpha_1}}, y \pmod{p_1^{\alpha_1}}), \ldots, \\ &\qquad (1 \pmod{p_k^{\alpha_k}}, x \pmod{p_k^{\alpha_k}}, y \pmod{p_k^{\alpha_k}})). \end{aligned}$$

g is a well defined function. Next, to show that g is onto we seek for a pre-image of an element in $F_1 \times \cdots \times F_k$, say $j := ((1, c_1, d_1), \ldots, (1, c_k, d_k))$. We find $x, y \in \mathbb{Z}_n$ such that $(1, x, y) \in F$. We have a solution for x and y if they satisfy the following system of congruences:

$$\begin{aligned} x &\equiv c_1 \pmod{p_1^{\alpha_1}}, \ldots, x \equiv c_k \pmod{p_k^{\alpha_k}}, \\ y &\equiv d_1 \pmod{p_1^{\alpha_1}}, \ldots, y \equiv d_k \pmod{p_k^{\alpha_k}}. \end{aligned} \tag{5.3}$$

Let us denote this system as $\begin{pmatrix} c_1 & \ldots & c_k \\ d_1 & \ldots & d_k \end{pmatrix}$. Note that interchanging the elements in any column of $\begin{pmatrix} c_1 & \ldots & c_k \\ d_1 & \ldots & d_k \end{pmatrix}$ and finding the solution to the corresponding system of congruences also gives another pre-image of j in F. However, $(1, c_i, d_i)$ and $(1, d_i, c_i)$ denote the same triangle, so the system $\begin{pmatrix} d_1 & \ldots & d_k \\ c_1 & \ldots & c_k \end{pmatrix}$ gives the same triangle in H_{p^α} as (5.3) does. Hence, each element in $F_1 \times \cdots \times F_k$ has $\frac{2^k}{2} = 2^{k-1}$ pre-images in F, and therefore, (5.2) yields

$$\mathcal{K}_4(G_n) = \frac{n\phi(n)}{3 \times 2^{k+2}} \times 2^{k-1} \times \prod_{i=1}^{k} \mathcal{K}_3(H_{p_i^{\alpha_i}}, 1). \tag{5.4}$$

Finally, employing Lemma 5.5 to substitute $\mathcal{K}_3(H_{p_i^{\alpha_i}}, 1)$ for $i \in \{1, \ldots, k\}$ in (5.4) completes the proof of the theorem. ■

6

Number of cliques in Peisert graphs

6.1 Introduction

It is a natural question to ask for the classification of all self-complementary and symmetric (SCS) graphs (see Definitions 1.64 and 1.67). In this direction, Peisert [48] observed that Chao's classification in [18] sheds light on the fact that the only such possible graphs of prime order are the Paley graphs. Zhang in [61], gave an algebraic characterization of SCS graphs using the classification of finite simple groups, although it did not follow whether one could find such graphs other than the Paley graphs. In 2001, Peisert gave a full description of SCS graphs as well as

[1]The contents of this chapter are under review.

their automorphism groups in [49]. He derived that there is another infinite family of SCS graphs apart from the Paley graphs, and, in addition, one more graph not belonging to any of the two former families. He constructed the P^*-graphs (which are now known as *Peisert graphs*) as follows.

Definition 6.1 (Peisert graph)**.** *Let $p \equiv 3 \pmod 4$ be a prime, and for a positive integer t, let $q = p^{2t}$. Let g be a primitive element of the finite field $\mathbb{F}_q$, that is, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\} = \langle g \rangle$. Then the Peisert graph $P^*(q)$ is defined as the graph with vertex set $\mathbb{F}_q$, where ab is an edge if and only if $a - b \in \langle g^4 \rangle \cup g\langle g^4 \rangle$.*

It is shown in [49] that the definition is independent of the choice of g. It turns out that an edge is well defined, since $q \equiv 1 \pmod 8$ implies that $-1 \in \langle g^4 \rangle$.

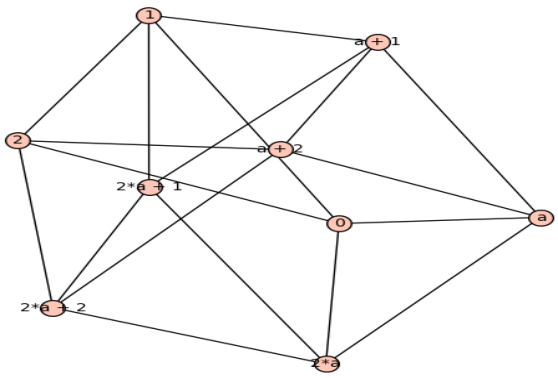

FIGURE 6.1: The Peisert graph of order 9

Various properties of Peisert graphs have been studied, for example, their automorphism groups by Peisert himself in [49], pseudo-random properties in [39], structure of maximal and maximum cliques in [58] and [8], critical groups of the graphs in [53], etc. Peisert graphs have been used to produce binary and ternary codes from their adjacency matrices in [38]. In [1], certain designs have been produced from Peisert graphs as well.

The Peisert graphs lie in the class of SCS graphs along with Paley graphs, so it would serve as a good analogy to study the number of cliques in the former class too. In [2], Alexander found the number of triangles using the properties that the Peisert

graphs are edge-transitive and that any pair of vertices connected by an edge have the same number of common neighbors. There was also an attempt to compute the number of cliques of order 4, but it was mentioned that the associated character sums "are notoriously difficult to simplify in any meaningful way". In this chapter, we follow a character sum approach to compute the number of cliques in Peisert graphs.

6.2 The number of triangles and cliques of order four in the Peisert graph

Cliques in Paley graphs have been extensively studied by implementing character sums. The Peisert graphs go hand in hand with Paley graphs; they are often mentioned in discussions related to Paley graphs, for example in [23, 36]. Moreover, the definition of a Peisert graph is quite similar to that of a Paley graph: both graphs involve a finite field as the vertex sets and have the edge sets depending on cosets of subgroups of the multiplicative group of the finite field. Thus, we are tempted to apply character sums in computing cliques in Peisert graphs. In the following theorem, we find the number of triangles in Peisert graphs by evaluating certain character sums.

Theorem 6.2. *Let $q = p^{2t}$, where $p \equiv 3 \pmod 4$ is a prime and t is a positive integer. Then, the number of triangles in the Peisert graph $P^*(q)$ is given by*

$$\mathcal{K}_3(P^*(q)) = \frac{q(q-1)(q-5)}{2^4 \times 3}.$$

It is easy to see that the expression for $\mathcal{K}_3(P^*(q))$ is an integer. We write $\mathcal{K}_3(P^*(q)) = \frac{q(\frac{q-1}{4})(\frac{q-1}{4}-1)}{3}$. Then, $3 \nmid \frac{q-1}{4}+1$ unless q is an even power of 3 (in which case $\mathcal{K}_3(P^*(q))$ is evidently an integer), so $3 \mid (\frac{q-1}{4})(\frac{q-1}{4}-1)$.

We note that the number of triangles in the Peisert graph of order q equals the

number of triangles in the Paley graph of the same order.

There is no known formula for the number of cliques of order 4 in the Peisert graph $P^*(q)$. The main purpose of this chapter is to provide a general formula for $\mathcal{K}_4(P^*(q))$. In this case, the character sums are difficult to evaluate. We use finite field hypergeometric functions to evaluate some of the character sums. In the following theorem, we express the number of cliques of order 4 in Peisert graphs in terms of finite field hypergeometric functions as given in Definition 1.40.

Theorem 6.3. *Let p be a prime such that $p \equiv 3 \pmod 4$. For a positive integer t, let $q = p^{2t}$. Let $q = u^2 + 2v^2$ for integers u and v such that $u \equiv 3 \pmod 4$ and $p \nmid u$ when $p \equiv 3 \pmod 8$. If χ_4 is a character of $\mathbb{F}_q$ of order 4, then the number of cliques of order 4 in the Peisert graph $P^*(q)$ is given by*

$$\mathcal{K}_4(P^*(q)) = \frac{q(q-1)}{2^{10}\times 3}\left[2(q^2-20q+81)+2u(-p)^t+3q^2\cdot {}_3F_2\left(\begin{matrix}\chi_4, & \chi_4, & \chi_4^3\\ \varepsilon, & \varepsilon & \end{matrix}\middle| 1\right)\right].$$

Using `SageMath`, we numerically verify Theorem 6.3 for certain values of q. We list some of the values in Table 6.1. We denote by ${}_3F_2(\cdot)$ the hypergeometric function appearing in Theorem 6.3.

p	q	$\mathcal{K}_4(P^*(q))$ (by `SageMath`)	u	$q^2\cdot {}_3F_2(\cdot)$ (by `SageMath`)	$\mathcal{K}_4(P^*(q))$ (by Theorem 6.3)	${}_3F_2(\cdot)$
3	9	0	-1	10	0	$0.1234\ldots$
7	49	2156	7	-30	2156	$-0.0123\ldots$
3	81	21060	7	-62	21060	$-0.0094\ldots$
11	121	116160	7	42	116160	$0.0028\ldots$
19	361	10515930	-17	522	10515930	$0.0040\ldots$
23	529	49135636	23	930	49135636	$0.0033\ldots$

Table 6.1: Numerical data for Theorem 6.3

6.2.1 Some preliminaries and lemmas

To count the number of cliques in Peisert graphs, we note that since the graph is vertex-transitive, any two vertices in the graph are contained in the same number of cliques of a particular order. Before we proceed to prove the main results, we begin by fixing some notation. For a prime $p \equiv 3 \pmod 4$ and positive integer t, let $q = p^{2t}$. Let g be a primitive element of the finite field $\mathbb{F}_q$, that is, $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\} = \langle g \rangle$. Now, we fix a multiplicative character χ_4 on $\mathbb{F}_q$ of order 4 (which exists since $q \equiv 1 \pmod 4$). Let φ be the unique quadratic character on $\mathbb{F}_q$. Then, we have $\chi_4^2 = \varphi$. Let $H = \langle g^4 \rangle \cup g\langle g^4 \rangle$. Since H is the union of two cosets of $\langle g^4 \rangle$ in $\langle g \rangle$, we see that $|H| = 2 \times \frac{q-1}{4} = \frac{q-1}{2}$. Peisert graphs being symmetric, are vertex-transitive. Also, the subgraphs induced by $\langle g^4 \rangle$ and $g\langle g^4 \rangle$ are both vertex-transitive: if s, t are two elements of $\langle g^4 \rangle$ (or $g\langle g^4 \rangle$) then the map on the vertex set of $\langle g^4 \rangle$ (or $g\langle g^4 \rangle$) given by $x \mapsto \frac{t}{s}x$ is an isomorphism sending s to t.

Throughout the chapter, we fix $h = 1 - \chi_4(g)$. For $x \in \mathbb{F}_q^*$, we have the following:

$$\frac{2 + h\chi_4(x) + \overline{h}\overline{\chi_4}(x)}{4} = \begin{cases} 1, & \text{if } \chi_4(x) \in \{1, \chi_4(g)\}; \\ 0, & \text{otherwise.} \end{cases} \tag{6.1}$$

We note here that for $x \neq 0$, $x \in H$ if and only if $\chi_4(x) = 1$ or $\chi_4(x) = \chi_4(g)$. Now, we state some preliminary lemmas which we make use of, to prove Theorems 6.2 and 6.3. We have the following lemma which will be used in proving the main results.

Lemma 6.4. *Let $q = p^{2t}$, where $p \equiv 3 \pmod 4$ is a prime and t is a positive integer. Let χ_4 be a multiplicative character of order 4 on $\mathbb{F}_q$, and let φ be the unique quadratic character. Then, we have $J(\chi_4, \chi_4) = J(\chi_4, \varphi) = -(-p)^t$.*

Proof. By Proposition 1.36, we have $J(\chi_4, \chi_4) = -(-p)^t$. By Theorem 1.35, where the result remains the same if we replace a field of prime order by a field with prime power order, and by Theorem 1.30, we see that $J(\chi_4, \varphi) = \chi_4(4)J(\chi_4, \chi_4) =$

$a_4 + ib_4$, where $a_4^2 + b_4^2 = q$ and $a_4 \equiv -(\frac{q+1}{2}) \pmod 4$. Hence, $a_4 \equiv 1 \pmod 4$ and $a_4 = -(-p)^t, b_4 = 0$. Thus, we obtain $J(\chi_4, \varphi) = J(\chi_4, \chi_4) = -(-p)^t$. ■

Next, we evaluate certain character sums in the following lemmas.

Lemma 6.5. *Let $q \equiv 1 \pmod 4$ be a prime power and let χ_4 be a character on $\mathbb{F}_q$ of order 4 such that $\chi_4(-1) = 1$, and let φ be the unique quadratic character. Let $a \in \mathbb{F}_q$ be such that $a \neq 0, 1$. Then,*

$$\sum_{y \in \mathbb{F}_q} \chi_4((y-1)(y-a)) = \varphi(a-1)J(\chi_4, \chi_4).$$

Proof. We have

$$\begin{aligned}
\sum_{y \in \mathbb{F}_q} \chi_4((y-1)(y-a)) &= \sum_{y' \in \mathbb{F}_q} \chi_4(y'(y'+1-a)) \\
&= \sum_{y'' \in \mathbb{F}_q} \chi_4((1-a)y'')\chi_4((1-a)(y''+1)) \\
&= \varphi(1-a) \sum_{y'' \in \mathbb{F}_q} \chi_4(y''(y''+1)) \\
&= \varphi(1-a) \sum_{y'' \in \mathbb{F}_q} \chi_4(-y''(-y''+1)) \\
&= \varphi(1-a)J(\chi_4, \chi_4),
\end{aligned}$$

where we used the substitutions $y - 1 = y'$, $y'' = y'(1-a)^{-1}$, and replaced y'' by $-y''$. ■

Lemma 6.6. *Let $q \equiv 1 \pmod 4$ be a prime power and let χ_4 be a character on $\mathbb{F}_q$ of order 4 such that $\chi_4(-1) = 1$. Let $a \in \mathbb{F}_q$ be such that $a \neq 0, 1$. Then,*

$$\sum_{y \in \mathbb{F}_q} \chi_4(y)\overline{\chi_4}(a-y) = -1.$$

Proof. We have

$$\begin{aligned}\sum_{y\in\mathbb{F}_q}\chi_4(y)\overline{\chi_4}(a-y) &= \sum_{y'\in\mathbb{F}_q}\chi_4(ay')\overline{\chi_4}(a-ay')\\ &= \sum_{y'\in\mathbb{F}_q}\chi_4(y')\overline{\chi_4}(1-y')\\ &= \sum_{y'\in\mathbb{F}_q}\chi_4\left(y'(1-y')^{-1}\right)\\ &= \sum_{y''\in\mathbb{F}_q, y''\neq -1}\chi_4(y'')\\ &= -1,\end{aligned}$$

where we used the substitutions $y' = ya^{-1}$ and $y'' = y'(1-y')^{-1}$, respectively. ■

Now, we prove Theorems 6.2 and 6.3. Note that we use Theorem 1.19 as and when required.

6.2.2 Proof of Theorem 6.2

In this section we present the proof of Theorem 6.2.

Proof of Theorem 6.2. Recall that $H = \langle g^4\rangle \cup g\langle g^4\rangle$ and $\langle H\rangle$ denotes the subgraph of $P^*(q)$ induced by H. We also use Notation 1.57. Using the vertex-transitivity of $P^*(q)$, we find that

$$\begin{aligned}\mathcal{K}_3(P^*(q)) &= \frac{1}{3}\times q\times \mathcal{K}_3(P^*(q),0)\\ &= \frac{q}{3}\times \text{number of edges in } \langle H\rangle. \end{aligned} \tag{6.2}$$

Now,

$$\text{the number of edges in } \langle H\rangle = \frac{1}{2}\times \sum_{\chi_4(x-y)\in\{1,\chi_4(g)\}}\sum 1, \tag{6.3}$$

where the first sum is taken over all x such that $\chi_4(x) \in \{1, \chi_4(g)\}$ and the second sum is taken over all $y \neq x$ such that $\chi_4(y) \in \{1, \chi_4(g)\}$. Hence, using (6.1) in (6.3), we find that

$$\begin{aligned}&\text{the number of edges in } \langle H \rangle \\ &= \frac{1}{2 \times 4^3} \sum_{x \neq 0} (2 + h\chi_4(x) + \overline{h}\overline{\chi_4}(x)) \\ &\qquad \times \sum_{y \neq 0, x} [(2 + h\chi_4(y) + \overline{h}\overline{\chi_4}(y))(2 + h\chi_4(x-y) + \overline{h}\overline{\chi_4}(x-y))]. \end{aligned} \tag{6.4}$$

We expand the inner summation in (6.4) to obtain

$$\sum_{y \neq 0, x} [(2 + h\chi_4(y) + \overline{h}\overline{\chi_4}(y))(2 + h\chi_4(x-y) + \overline{h}\overline{\chi_4}(x-y))] \tag{6.5}$$

$$\begin{aligned}&= \sum_{y \neq 0, x} [4 + 2h\chi_4(y) + 2\overline{h}\overline{\chi_4}(y) + 2h\chi_4(x-y) + 2\overline{h}\overline{\chi_4}(x-y) + 2\chi_4(y)\overline{\chi_4}(x-y) \\ &+ 2\overline{\chi_4}(y)\chi_4(x-y) - 2\chi_4(g)\chi_4(y(x-y)) + 2\chi_4(g)\overline{\chi_4}(y(x-y))]. \end{aligned} \tag{6.6}$$

We have

$$\sum_{y \neq 0, x} \chi_4(y(x-y)) = \sum_{y \neq 0, 1} \chi_4(xy)\chi_4(x - xy) = \varphi(x) J(\chi_4, \chi_4). \tag{6.7}$$

Using Lemma 6.6 and (6.7), (6.5) yields

$$\begin{aligned}&\sum_{y \neq 0, x} [(2 + h\chi_4(y) + \overline{h}\overline{\chi_4}(y))(2 + h\chi_4(x-y) + \overline{h}\overline{\chi_4}(x-y))] \\ &= 4(q-3) - 4h\chi_4(x) - 4\overline{h}\overline{\chi_4}(x) - 2\chi_4(g)\varphi(x)J(\chi_4, \chi_4) + 2\chi_4(g)\varphi(x)\overline{J(\chi_4, \chi_4)}. \end{aligned} \tag{6.8}$$

Now, putting (6.8) into (6.4), and then using Lemma 6.4, we find that

$$\text{the number of edges in } \langle H \rangle$$

$$
\begin{aligned}
&= \frac{1}{2 \times 4^3} \sum_{x \neq 0} [(2 + h\chi_4(x) + \overline{h}\overline{\chi_4}(x))(4(q-3) - 4h\chi_4(x) - 4\overline{h}\overline{\chi_4}(x))] \\
&= \frac{1}{2 \times 4^3} \sum_{x \neq 0} [8(q-5) + (4h(q-3) - 8h)\chi_4(x) + (4\overline{h}(q-3) - 8\overline{h})\overline{\chi_4}(x)] \\
&= \frac{(q-1)(q-5)}{16}.
\end{aligned}
$$

Substituting this value in (6.2) gives us the required result. ■

6.2.3 Proof of Theorem 6.3

The proof of Theorem 6.3 requires more machinery. We begin with some lemmas which will simplify some of the terms in the character sums that we come across in the proof of the theorem.

Lemma 6.7. *Let $q = p^{2t}$, where $p \equiv 3 \pmod 4$ is a prime and t is a positive integer. Let χ_4 be a character on $\mathbb{F}_q$ of order 4 and let φ be the unique quadratic character. Let $J(\chi_4, \chi_4) = J(\chi_4, \varphi) = \rho$, where $\rho = -(-p)^t$. Then,*

$$\sum_{x,y \in \mathbb{F}_q, x \neq 1} \overline{\chi_4}(x)\chi_4(y)\chi_4(1-y)\chi_4(x-y) = -2\rho \tag{6.9}$$

and

$$\sum_{x,y \in \mathbb{F}_q, x \neq 1} \overline{\chi_4}(x)\chi_4(y)\chi_4(1-y)\overline{\chi_4}(x-y) = 1 - \rho. \tag{6.10}$$

Proof. By Lemma 6.6, we have

$$
\begin{aligned}
\sum_{y \neq 0,1} \chi_4(y)\chi_4(1-y) \sum_{x \neq 0,1,y} \overline{\chi_4}(x)\chi_4(x-y) &= \sum_{y \neq 0,1} \chi_4(y)\chi_4(1-y)\left[-1 - \chi_4(y-1)\right] \\
&= -\rho - \sum_{y} \chi_4(y)\varphi(1-y) = -2\rho,
\end{aligned}
$$

which proves (6.9). Next, using the substitution $x' = xy^{-1}$, we have

$$\sum_{x} \overline{\chi_4}(x)\overline{\chi_4}(x-y) = \sum_{x'} \overline{\chi_4}(x'y)\overline{\chi_4}(x'y-y) = \varphi(y)\rho. \tag{6.11}$$

So, using (6.11), we find that

$$\begin{aligned}\sum_{y\neq 0,1} \chi_4(y)\chi_4(1-y) \sum_{x\neq 0,1,y} \overline{\chi_4}(x)\overline{\chi_4}(x-y) &= \sum_{y\neq 0,1} \chi_4(y)\chi_4(1-y)\left[\varphi(y)\rho - \overline{\chi_4}(y-1)\right] \\ &= \rho \sum_{y} \overline{\chi_4}(y)\chi_4(1-y) - \sum_{y\neq 1} \chi_4(y) \\ &= -\rho + 1.\end{aligned}$$

This completes the proof of the lemma. ■

We need to evaluate several analogous character sums as in Lemma 6.7. To this end, we have the following two lemmas whose proofs merely involve Lemmas 6.5 and 6.6 (as in Lemma 6.7).

Lemma 6.8. *Let $q = p^{2t}$, where $p \equiv 3 \pmod 4$ is a prime and t is a positive integer. Let χ_4 be a character on $\mathbb{F}_q$ of order 4 and let φ be the unique quadratic character. Let $J(\chi_4, \chi_4) = J(\chi_4, \varphi) = \rho$, where $\rho = -(-p)^t$. Then, we have*

$$\sum_{x,y\in\mathbb{F}_q, x\neq 0,1} \chi_4^{i_1}(y)\chi_4^{i_2}(1-y)\chi_4^{i_3}(x-y)$$
$$= \begin{cases} -2\rho, & \text{if } (i_1,i_2,i_3) \in \{(1,1,1),(-1,-1,-1)\}; \\ 2, & \text{if } (i_1,i_2,i_3) \in \{(1,1,-1),(-1,-1,1)\}; \\ 1-\rho, & \text{if } (i_1,i_2,i_3) \in \{(1,-1,1),(1,-1,-1),(-1,1,1),(-1,1,-1)\}. \end{cases}$$

Proof. The proofs are similar, and we provide one such instance. For $(i_1, i_2, i_3) =$

$(1,1,1)$, we have

$$\begin{aligned}\sum_{y\neq 0,1}\sum_{x\neq 0,1}\chi_4(y)\chi_4(1-y)\chi_4(x-y) &= \sum_{y\neq 0,1}\chi_4(y)\chi_4(1-y)\sum_{x\neq 0,1}\chi_4(x-y)\\ &= \sum_{y\neq 0,1}\chi_4(y)\chi_4(1-y)(-\chi_4(y)-\chi_4(1-y))\\ &= -\sum_{y\neq 0,1}\phi(y)\chi_4(1-y)-\sum_{y\neq 0,1}\chi_4(y)\phi(1-y)\\ &= -2\rho.\end{aligned}$$

■

Lemma 6.9. *Let $q=p^{2t}$, where $p\equiv 3 \pmod 4$ is a prime and t is a positive integer. Let χ_4 be a character on $\mathbb{F}_q$ of order 4 and let φ be the unique quadratic character. Let $J(\chi_4,\chi_4)=J(\chi_4,\varphi)=\rho$, where $\rho=-(-p)^t$. Then, for $i_1,i_2,i_3\in\{\pm 1\}$, we have the following tabulation of the values of the expression given below:*

$$\sum_{x,y\in\mathbb{F}_q, x\neq 0,1} A_x\cdot\chi_4^{i_1}(y)\chi_4^{i_2}(1-y)\chi_4^{i_3}(x-y). \tag{6.12}$$

For $w\in\{1,2,\ldots,8\}$ and $z\in\{1,2,\ldots,7\}$, the (w,z)-th entry in the table corresponds to (6.12), where A_x is either $\chi_4(x),\overline{\chi_4}(x),\chi_4(1-x)$ or $\overline{\chi_4}(1-x)$ and the

tuple (i_1, i_2, i_3) *depends on* w.

			A_x			
i_1	i_2	i_3	$\chi_4(x)$	$\overline{\chi_4}(x)$	$\chi_4(1-x)$	$\overline{\chi_4}(1-x)$
1	1	1	-2ρ	-2ρ	-2ρ	-2ρ
1	1	-1	$1-\rho$	$1-\rho$	$1-\rho$	$1-\rho$
1	-1	1	ρ^2+1	2	$\rho^2-\rho$	$1-\rho$
1	-1	-1	$1-\rho$	$\rho^2-\rho$	2	ρ^2+1
-1	1	1	$\rho^2-\rho$	$1-\rho$	ρ^2+1	2
-1	1	-1	2	ρ^2+1	$1-\rho$	$\rho^2-\rho$
-1	-1	1	$1-\rho$	$1-\rho$	$1-\rho$	$1-\rho$
-1	-1	-1	-2ρ	-2ρ	-2ρ	-2ρ

For example, the $(3,6)$*-th position contains the value* $\rho^2-\rho$. *Here* $w=3$ *corresponds to* $i_1=1, i_2=-1, i_3=1$; $z=6$ *corresponds to the column* $A_x=\chi_4(1-x)$. *So,*

$$\sum_{x,y\in\mathbb{F}_q, x\neq 0,1} \chi_4(1-x)\chi_4(y)\overline{\chi_4}(1-y)\chi_4(x-y) = \rho^2-\rho.$$

Proof. The calculations follow along the lines of Lemma 6.5 and Lemma 6.6. For example, in Lemma 6.7, one can take $\chi_4(x)$, $\chi_4(x-1)$ or $\overline{\chi_4}(x-1)$ in place of $\overline{\chi_4}(x)$ in (6.9) and (6.10) (which we denote by A_x), and easily evaluate the corresponding character sum. ■

Lemma 6.10. *Let* $q=p^{2t}$, *where* $p\equiv 3 \pmod 4$ *is a prime and* t *is a positive integer. Let* χ_4 *be a character of order* 4. *Let* φ *and* ε *be the quadratic and the trivial characters, respectively. Let* $q=u^2+2v^2$ *for integers* u *and* v *such that* $u\equiv 3 \pmod 4$ *and* $p\nmid u$ *when* $p\equiv 3 \pmod 8$. *Then,*

$${}_3F_2\left(\begin{matrix}\chi_4, & \chi_4, & \chi_4\\ & \varepsilon, & \varepsilon\end{matrix}\,\middle|\,1\right) = {}_3F_2\left(\begin{matrix}\overline{\chi_4}, & \overline{\chi_4}, & \overline{\chi_4}\\ & \varepsilon, & \varepsilon\end{matrix}\,\middle|\,1\right)$$

$$= {}_3F_2\left(\begin{matrix}\chi_4, & \overline{\chi_4}, & \overline{\chi_4}\\ & \varphi, & \varepsilon\end{matrix}\Big|1\right)$$
$$= {}_3F_2\left(\begin{matrix}\overline{\chi_4}, & \chi_4, & \chi_4\\ & \varphi, & \varepsilon\end{matrix}\Big|1\right)$$
$$= \frac{1}{q^2}[-2u(-p)^t].$$

Proof. Let χ_8 be a character of order 8 such that $\chi_8^2 = \chi_4$. Now, Proposition 1.36 tells us that $J(\chi_4, \chi_4) = -(-p)^t$ and hence it is real. Again, by Lemma 1.22 and Remark 1.38, $J(\chi_8, \chi_8^2) = \chi_8(-4)J(\chi_4, \chi_4)$, where $\chi_8(4) = \pm 1$ and thus, is also real. By Theorem 1.42, we have

$$\begin{aligned}{}_3F_2\left(\begin{matrix}\chi_4, & \chi_4, & \chi_4\\ & \varepsilon, & \varepsilon\end{matrix}\Big|1\right) &= \binom{\chi_8}{\chi_8^2}\binom{\chi_8}{\chi_8^3} + \binom{\chi_8^5}{\chi_8^2}\binom{\chi_8^5}{\overline{\chi_8}}\\ &= \frac{\chi_8(-1)}{q^2}[J(\chi_8, \chi_8^6)J(\chi_8, \chi_8^5) + J(\chi_8^5, \chi_8^6)J(\chi_8^5, \chi_8)].\end{aligned} \tag{6.13}$$

Using Theorems 1.31 and 1.32, we obtain

$$\begin{aligned}J(\chi_8, \chi_8^6) &= \chi_8(-1)J(\chi_8, \chi_8),\\ J(\chi_8, \chi_8^5) &= \chi_8(-1)J(\chi_8, \chi_8^2),\\ J(\chi_8^5, \chi_8^6) &= \chi_8(-1)\overline{J(\chi_8, \chi_8)}.\end{aligned}$$

Substituting these values in (6.13), and using Lemma 1.39 and Remark 1.38, we find that

$$\begin{aligned}{}_3F_2\left(\begin{matrix}\chi_4, & \chi_4, & \chi_4\\ & \varepsilon, & \varepsilon\end{matrix}\Big|1\right) &= \frac{\chi_8(-1)}{q^2}[J(\chi_8, \chi_8)J(\chi_8, \chi_8^2) + \overline{J(\chi_8, \chi_8)}J(\chi_8, \chi_8^2)]\\ &= \frac{1}{q^2}J(\chi_8, \chi_8^2) \times 2\,\mathrm{Re}(J(\chi_8, \chi_8)) \times \chi_8(-1)\end{aligned}$$

$$= \frac{1}{q^2}[-2u(-p)^t]. \tag{6.14}$$

Since ${}_3F_2\left(\begin{matrix}\overline{\chi_4}, & \overline{\chi_4}, & \overline{\chi_4}\\ & \varepsilon, & \varepsilon\end{matrix}\Big|1\right)$ is the conjugate of ${}_3F_2\left(\begin{matrix}\chi_4, & \chi_4, & \chi_4\\ & \varepsilon, & \varepsilon\end{matrix}\Big|1\right)$, so both are equal as the value given in (6.14) is a real number. Evoking Theorem 1.42 again, we have

$$\begin{aligned}{}_3F_2\left(\begin{matrix}\chi_4, & \overline{\chi_4}, & \overline{\chi_4}\\ & \varphi, & \varepsilon\end{matrix}\Big|1\right) &= \binom{\overline{\chi_8}}{\chi_8^2}\binom{\overline{\chi_8}}{\chi_8} + \binom{\chi_8^3}{\chi_8^2}\binom{\chi_8^3}{\overline{\chi_8}^3}\\ &= \frac{\chi_8(-1)}{q^2}[J(\overline{\chi_8},\overline{\chi_8}^2)J(\overline{\chi_8},\overline{\chi_8}) + J(\chi_8^3,\overline{\chi_8}^2)J(\chi_8^3,\chi_8^3)].\end{aligned} \tag{6.15}$$

Recalling Theorem 1.32 gives $J(\chi_8,\chi_8) = J(\chi_8^3,\chi_8^3)$. Also, Theorem 1.31 gives $J(\chi_8^3,\overline{\chi_8}^2) = \overline{J(\chi_8^5,\chi_8^2)} = \overline{J(\chi_8,\chi_8^2)} = J(\chi_8,\chi_8^2)$. Hence, (6.15) yields

$$\begin{aligned}{}_3F_2\left(\begin{matrix}\chi_4, & \overline{\chi_4}, & \overline{\chi_4}\\ & \varphi, & \varepsilon\end{matrix}\Big|1\right) &= \frac{1}{q^2}J(\chi_8,\chi_8^2)\times 2\,\mathrm{Re}(J(\chi_8,\chi_8))\times\chi_8(-1)\\ &= \frac{1}{q^2}[-2u(-p)^t],\end{aligned}$$

which is the same real number we found in (6.14). Hence, its complex conjugate, namely ${}_3F_2\left(\begin{matrix}\overline{\chi_4}, & \chi_4, & \chi_4\\ & \varphi, & \varepsilon\end{matrix}\Big|1\right)$ is also real and has the same value. This completes the proof of the lemma. ■

Next, we note the following observations given in the beginning of the sixth section in [21]. We state it as a lemma since we shall use it in proving Theorem 6.3. Let $X = \{(t_1,t_2,t_3,t_4,t_5)\in\mathbb{Z}_4^5 : t_1,t_2,t_3\neq 0, t_4,t_5;\ t_1+t_2+t_3\neq t_4,t_5\}$. To each of the transformations in (1.3)-(1.9), Dawsey and McCarthy in [21] associated a map

on X; for example, the transformation in (1.3) gives that

$$ {}_3F_2\left(\begin{matrix}\chi_4^{t_1}, & \chi_4^{t_2}, & \chi_4^{t_3} \\ & \chi_4^{t_4}, & \chi_4^{t_5}\end{matrix}\middle|1\right) = {}_3F_2\left(\begin{matrix}\chi_4^{t_2-t_4}, & \chi_4^{t_1-t_4}, & \chi_4^{t_3-t_4} \\ & \chi_4^{-t_4}, & \chi_4^{t_5-t_4}\end{matrix}\middle|1\right), $$

so it induces a map $f_1 : X \to X$ given by

$$ f_1(t_1, t_2, t_3, t_4, t_5) = (t_2 - t_4, t_1 - t_4, t_3 - t_4, -t_4, t_5 - t_4). $$

Similarly, the other transformations in (1.4)-(1.9) led to the construction of the maps f_2 to f_7.

Lemma 6.11. [21] *Let* $X = \{(t_1, t_2, t_3, t_4, t_5) \in \mathbb{Z}_4^5 : t_1, t_2, t_3 \neq 0, t_4, t_5;\ t_1 + t_2 + t_3 \neq t_4, t_5\}$. *Define the functions* $f_i : X \to X,\ i \in \{1, 2, \ldots, 7\}$ *in the following manner:*

$$ \begin{aligned} f_1(t_1, t_2, t_3, t_4, t_5) &= (t_2 - t_4, t_1 - t_4, t_3 - t_4, -t_4, t_5 - t_4), \\ f_2\left(t_1, t_2, t_3, t_4, t_5\right) &= \left(t_1, t_1 - t_4, t_1 - t_5, t_1 - t_2, t_1 - t_3\right), \\ f_3\left(t_1, t_2, t_3, t_4, t_5\right) &= \left(t_2 - t_4, t_2, t_2 - t_5, t_2 - t_1, t_2 - t_3\right), \\ f_4\left(t_1, t_2, t_3, t_4, t_5\right) &= \left(t_1, t_2, t_5 - t_3, t_1 + t_2 - t_4, t_5\right), \\ f_5\left(t_1, t_2, t_3, t_4, t_5\right) &= \left(t_1, t_4 - t_2, t_3, t_4, t_1 + t_3 - t_5\right), \\ f_6\left(t_1, t_2, t_3, t_4, t_5\right) &= \left(t_4 - t_1, t_2, t_3, t_4, t_2 + t_3 - t_5\right), \\ f_7\left(t_1, t_2, t_3, t_4, t_5\right) &= \left(t_4 - t_1, t_4 - t_2, t_3, t_4, t_4 + t_5 - t_1 - t_2\right). \end{aligned} $$

Then the group generated by $f_1, \ldots, f_7$, *with operation composition of functions, is the set*

$$ \mathcal{F} = \{f_0, f_i, f_j \circ f_l, f_4 \circ f_1, f_6 \circ f_2, f_5 \circ f_3, f_1 \circ f_4 \circ f_1 : 1 \leq i \leq 7,\ 1 \leq j \leq 3,\ 4 \leq l \leq 7\}, $$

where f_0 *is the identity map.*

Moreover, the group $\mathcal{F}$ acts on the set X, and X contains eleven orbits with representatives $(1,1,1,0,0)$, $(3,3,3,0,0)$, $(1,3,3,2,0)$, $(3,1,1,2,0)$, $(2,1,3,0,0)$, $(1,3,2,0,0)$, $(2,3,1,0,0)$, $(1,2,2,0,0)$, $(2,2,1,0,0)$, $(1,1,3,0,0)$ *and* $(2,2,2,0,0)$. *If we associate the* 5*-tuple* $(t_1,t_2,\ldots,t_5)\in X$ *to the hypergeometric function* ${}_3F_2\left(\begin{matrix}\chi_4^{t_1}, & \chi_4^{t_2}, & \chi_4^{t_3}\\ & \chi_4^{t_4}, & \chi_4^{t_5}\end{matrix}\Big|1\right)$, *then each orbit of the group action consists of a number of* 5*-tuples* $(t_1,t_2,\ldots,t_5)$, *and the corresponding* ${}_3F_2$ *terms have the same value.*

Proof. For a proof, see Section 6 of [21]. ■

Now, we prove Theorem 6.3. We will use the following notation. Let $J(\chi_4,\chi_4)=J(\chi_4,\varphi)=\rho$, where the value of ρ is given by Lemma 6.4. Let χ_8 be a character of order 8 such that $\chi_8^2=\chi_4$. Note that in the proof we shall use the fact that $\chi_4(-1)=1$ multiple times.

Proof of Theorem 6.3. Noting again that $P^*(q)$ is vertex-transitive, we find that

$$\begin{aligned}\mathcal{K}_4(P^*(q)) &= \frac{q}{4}\times \text{ number of cliques of order 4 in } P^*(q) \text{ containing } 0\\ &= \frac{q}{4}\times \mathcal{K}_3(\langle H\rangle).\end{aligned}\tag{6.16}$$

Here, $H=\langle g^4\rangle\cup g\langle g^4\rangle$ and $\langle H\rangle$ denotes the subgraph of $P^*(q)$ induced by H. We use Notation 1.57. Let $a,b\in H$ be such that $\chi_4(ab^{-1})=1$. We note that

$$\mathcal{K}_3(\langle H\rangle,a)=\frac{1}{2}\times\sum\sum_{\chi_4(x-y)\in\{1,\chi_4(g)\}}1,\tag{6.17}$$

where the 1st sum is taken over all x such that $\chi_4(x),\chi_4(a-x)\in\{1,\chi_4(g)\}$ and the 2nd sum is taken over all $y\neq x$ such that $\chi_4(y),\chi_4(a-y)\in\{1,\chi_4(g)\}$. Hence, using (6.1) in (6.17), we find that

$$\mathcal{K}_3(\langle H\rangle,a)$$

$$= \frac{1}{2\times 4^5}\sum_{x\neq 0,a}\sum_{y\neq 0,a,x}[(2+h\chi_4(a-x)+\overline{h}\overline{\chi_4}(a-x))$$
$$\times(2+h\chi_4(a-y)+\overline{h}\overline{\chi_4}(a-y))(2+h\chi_4(x-y)+\overline{h}\overline{\chi_4}(x-y))$$
$$\times(2+h\chi_4(x)+\overline{h}\overline{\chi_4}(x))(2+h\chi_4(y)+\overline{h}\overline{\chi_4}(y))].$$

Using the substitution $Y = ba^{-1}y$, the sum indexed by y in the above yields

$$\mathcal{K}_3(\langle H\rangle, a)$$
$$= \frac{1}{2\times 4^5}\sum_{x\neq 0,a}\sum_{Y\neq 0,b,ba^{-1}x}[(2+h\chi_4(a-x)+\overline{h}\overline{\chi_4}(a-x))$$
$$\times(2+h\chi_4(Y-b)+\overline{h}\overline{\chi_4}(Y-b))(2+h\chi_4(Y-ba^{-1}x)+\overline{h}\overline{\chi_4}(Y-ba^{-1}x))$$
$$\times(2+h\chi_4(x)+\overline{h}\overline{\chi_4}(x))(2+h\chi_4(Y)+\overline{h}\overline{\chi_4}(Y))]$$
$$= \frac{1}{2\times 4^5}\sum_{Y\neq 0,b}\sum_{x\neq 0,a,ab^{-1}Y}[(2+h\chi_4(a-x)+\overline{h}\overline{\chi_4}(a-x))$$
$$\times(2+h\chi_4(Y-b)+\overline{h}\overline{\chi_4}(Y-b))(2+h\chi_4(Y-ba^{-1}x)+\overline{h}\overline{\chi_4}(Y-ba^{-1}x))$$
$$\times(2+h\chi_4(x)+\overline{h}\overline{\chi_4}(x))(2+h\chi_4(Y)+\overline{h}\overline{\chi_4}(Y))].$$

Again, using the substitution $X = ba^{-1}x$ yields

$$\mathcal{K}_3(\langle H\rangle, a)$$
$$= \frac{1}{2\times 4^5}\sum_{Y\neq 0,b}\sum_{X\neq 0,b,Y}[(2+h\chi_4(b-X)+\overline{h}\overline{\chi_4}(b-X))$$
$$\times(2+h\chi_4(b-Y)+\overline{h}\overline{\chi_4}(b-Y))(2+h\chi_4(X-Y)+\overline{h}\overline{\chi_4}(X-Y))$$
$$\times(2+h\chi_4(X)+\overline{h}\overline{\chi_4}(X))(2+h\chi_4(Y)+\overline{h}\overline{\chi_4}(Y))]$$
$$= \mathcal{K}_3(\langle H\rangle, b).$$

Thus, if $a, b \in H$ are such that $\chi_4(ab^{-1}) = 1$, then

$$\mathcal{K}_3(\langle H\rangle, a) = \mathcal{K}_3(\langle H\rangle, b). \tag{6.18}$$

Let $\langle g^4\rangle = \{x_1, \ldots, x_{\frac{q-1}{4}}\}$ with $x_1 = 1$ and $g\langle g^4\rangle = \{y_1, \ldots, y_{\frac{q-1}{4}}\}$ with $y_1 = g$. Then,

$$\sum_{i=1}^{\frac{q-1}{4}} \mathcal{K}_3(\langle H\rangle, x_i) + \sum_{i=1}^{\frac{q-1}{4}} \mathcal{K}_3(\langle H\rangle, y_i) = 3 \times \mathcal{K}_3(\langle H\rangle). \tag{6.19}$$

By (6.18), we have

$$\mathcal{K}_3(\langle H\rangle, x_1) = \mathcal{K}_3(\langle H\rangle, x_2) = \cdots = \mathcal{K}_3(\langle H\rangle, x_{\frac{q-1}{4}})$$

and

$$\mathcal{K}_3(\langle H\rangle, y_1) = \mathcal{K}_3(\langle H\rangle, y_2) = \cdots = \mathcal{K}_3(\langle H\rangle, y_{\frac{q-1}{4}}).$$

Hence, (6.19) yields

$$\mathcal{K}_3(\langle H\rangle) = \frac{q-1}{12}[\mathcal{K}_3(\langle H\rangle, 1) + \mathcal{K}_3(\langle H\rangle, g)]. \tag{6.20}$$

Thus, we need to find only $\mathcal{K}_3(\langle H\rangle, 1)$ and $\mathcal{K}_3(\langle H\rangle, g)$. We first find $\mathcal{K}_3(\langle H\rangle, 1)$.

We have

$$\begin{aligned}
&\mathcal{K}_3(\langle H\rangle, 1)\\
&= \frac{1}{2\times 4^5} \sum_{x\neq 0,1} [(2 + h\chi_4(1-x) + \overline{h}\overline{\chi_4}(1-x))(2 + h\chi_4(x) + \overline{h}\overline{\chi_4}(x))]\\
&\qquad \sum_{y\neq 0,1,x} [(2 + h\chi_4(1-y) + \overline{h}\overline{\chi_4}(1-y))(2 + h\chi_4(x-y) + \overline{h}\overline{\chi_4}(x-y))\\
&\qquad\qquad \times (2 + h\chi_4(y) + \overline{h}\overline{\chi_4}(y))].
\end{aligned} \tag{6.21}$$

Let $i_1, i_2, i_3 \in \{\pm 1\}$ and let F_{i_1,i_2,i_3} denote the term $\chi_4^{i_1}(y)\chi_4^{i_2}(1-y)\chi_4^{i_3}(x-y)$. Using this notation, we expand and evaluate the inner summation in (6.21). We have

$$\sum_{y\neq 0,1,x} [2 + h\chi_4(y) + \overline{h}\overline{\chi_4}(y)][2 + h\chi_4(1-y) + \overline{h}\overline{\chi_4}(1-y)][2 + h\chi_4(x-y) + \overline{h}\overline{\chi_4}(x-y)]$$

$$
\begin{aligned}
&= \sum_{y\neq 0,1,x} [8 + 4h\chi_4(y) + 4\overline{h}\overline{\chi_4}(y) + 4h\chi_4(1-y) + 4\overline{h}\overline{\chi_4}(1-y) + 4h\chi_4(x-y) \\
&+ 4\overline{h}\overline{\chi_4}(x-y) + 4\chi_4(y)\overline{\chi_4}(1-y) + 4\overline{\chi_4}(y)\chi_4(1-y) + 4\chi_4(y)\overline{\chi_4}(x-y) \\
&+ 4\overline{\chi_4}(y)\chi_4(x-y) + 4\chi_4(1-y)\overline{\chi_4}(x-y) + 4\overline{\chi_4}(1-y)\chi_4(x-y) \\
&+ 2h^2\chi_4(y)\chi_4(1-y) + 2\overline{h}^2\overline{\chi_4}(y)\overline{\chi_4}(1-y) + 2h^2\chi_4(y)\chi_4(x-y) \\
&+ 2\overline{h}^2\overline{\chi_4}(y)\overline{\chi_4}(x-y) + 2h^2\chi_4(1-y)\chi_4(x-y) + 2\overline{h}^2\overline{\chi_4}(1-y)\overline{\chi_4}(x-y)] \\
&+ \sum_{y\neq 0,1,x} [h^3F_{1,1,1} + 2hF_{1,1,-1} + 2hF_{1,-1,1} + 2\overline{h}F_{1,-1,-1} + 2hF_{-1,1,1} + 2\overline{h}F_{-1,1,-1} \\
&+ 2\overline{h}F_{-1,-1,1} + \overline{h}^3F_{-1,-1,-1}]. \qquad (6.22)
\end{aligned}
$$

Now, referring to Lemmas 6.5 and 6.6, we can easily check that any term of the form $\sum_y \chi_4(\cdot)\overline{\chi_4}(\cdot)$ gives -1, $\sum_y \chi_4((y-1)(y-x))$ gives $\varphi(x-1)\rho$ and $\sum_y \chi_4(y(y-x))$ gives $\varphi(x)\rho$. Hence, (6.22) yields

$$
\begin{aligned}
&\sum_{y\neq 0,1,x} [2 + h\chi_4(y) + \overline{h}\overline{\chi_4}(y)][2 + h\chi_4(1-y) + \overline{h}\overline{\chi_4}(1-y)][2 + h\chi_4(x-y) + \overline{h}\overline{\chi_4}(x-y)] \\
&= A + B\chi_4(x) + \overline{B}\overline{\chi_4}(x) + B\chi_4(x-1) + \overline{B}\overline{\chi_4}(x-1) - 4\chi_4(x)\overline{\chi_4}(x-1) \\
&- 4\overline{\chi_4}(x)\chi_4(x-1) - 2h^2\chi_4(x)\chi_4(x-1) - 2\overline{h}^2\overline{\chi_4}(x)\overline{\chi_4}(x-1) \\
&+ \sum_{y\neq 0,1,x} [h^3F_{1,1,1} + 2hF_{1,1,-1} + 2hF_{1,-1,1} + 2\overline{h}F_{1,-1,-1} + 2hF_{-1,1,1} + 2\overline{h}F_{-1,1,-1} \\
&+ 2\overline{h}F_{-1,-1,1} + \overline{h}^3F_{-1,-1,-1}] \\
&=: \mathcal{I}, \qquad (6.23)
\end{aligned}
$$

where $A = 8(q-8)$ and $B = -12h$.

Next, we introduce some notation. Let

$$
\begin{aligned}
B_1 &= 16h(q-15), \\
E_1 &= 8h^2(q-15), \\
F_1 &= 16(q-15).
\end{aligned}
$$

For $i \in \{1,2,3,4\}$ and $j \in \{1,2,\ldots,8\}$, we define the following character sums.

$$T_j := \sum_{x\neq 0,1} \sum_{y} \chi_4^{i_1}(y)\chi_4^{i_2}(1-y)\chi_4^{i_3}(x-y),$$

$$U_{ij} := \sum_{x\neq 0,1} \chi_4^{l}(m) \sum_{y} \chi_4^{i_1}(y)\chi_4^{i_2}(1-y)\chi_4^{i_3}(x-y),$$

$$V_{ij} := \sum_{x} \chi_4^{l_1}(x)\chi_4^{l_2}(1-x) \sum_{y} \chi_4^{i_1}(y)\chi_4^{i_2}(1-y)\chi_4^{i_3}(x-y),$$

where

$$l = \begin{cases} 1, & \text{if } i \text{ is odd,} \\ -1, & \text{otherwise;} \end{cases}$$

$$m = \begin{cases} x, & \text{if } i \in \{1,2\}, \\ 1-x, & \text{otherwise;} \end{cases}$$

and

$$(l_1, l_2) = \begin{cases} (1,1), & \text{if } i = 1, \\ (1,-1), & \text{if } i = 2, \\ (-1,1), & \text{if } i = 3, \\ (-1,-1), & \text{if } i = 4. \end{cases}$$

Also, corresponding to each j, let (i_1, i_2, i_3) take the value according to the following:

$$(i_1,i_2,i_3)=\begin{cases}(1,1,1), & \text{if } j=1,\\ (1,1,-1), & \text{if } j=2,\\ (1,-1,1), & \text{if } j=3,\\ (1,-1,-1), & \text{if } j=4,\\ (-1,1,1), & \text{if } j=5,\\ (-1,1,-1), & \text{if } j=6,\\ (-1,-1,1), & \text{if } j=7,\\ (-1,-1,-1), & \text{if } j=8.\end{cases}$$

Then, using (6.23) and the notation we just described, (6.21) yields

$$\begin{aligned}
\mathcal{K}_3(\langle H\rangle,1) &= \frac{1}{2^{11}}\sum_{x\neq 0,1}[2+h\chi_4(x)+\overline{h}\overline{\chi_4}(x)][2+h\chi_4(1-x)+\overline{h}\overline{\chi_4}(1-x)]\times\mathcal{I}\\
=&\frac{1}{2^{11}}\sum_{x\neq 0,1}\Big[32(q-15)+B_1\chi_4(x)+\overline{B_1}\overline{\chi_4}(x)+B_1\chi_4(x-1)+\overline{B_1}\overline{\chi_4}(x-1)\\
&+E_1\chi_4(x)\chi_4(x-1)+\overline{E_1}\overline{\chi_4}(x)\overline{\chi_4}(x-1)+F_1\chi_4(x)\overline{\chi_4}(1-x)+\overline{F_1}\overline{\chi_4}(x)\chi_4(x-1)\Big]\\
&+\frac{1}{2^{11}}\Big[4h^3T_1+8hT_2+8hT_3+8\overline{h}T_4+8hT_5+8\overline{h}T_6+8\overline{h}T_7+4\overline{h}^3T_8\\
&+2h^4U_{11}+4h^2U_{12}+4h^2U_{13}+8U_{14}+4h^2U_{15}+8U_{16}+8U_{17}+4\overline{h}^2U_{18}\\
&+4h^2U_{21}+8U_{22}+8U_{23}+4\overline{h}^2U_{24}+8U_{25}+4\overline{h}^2U_{26}+4\overline{h}^2U_{27}+2\overline{h}^4U_{28}\\
&+2h^4U_{31}+4h^2U_{32}+4h^2U_{33}+8U_{34}+4h^2U_{35}+8U_{36}+8U_{37}+4\overline{h}^2U_{38}\\
&+4h^2U_{41}+8U_{42}+8U_{43}+4\overline{h}^2U_{44}+8U_{45}+4\overline{h}^2U_{46}+4\overline{h}^2U_{47}+2\overline{h}^4U_{48}\\
&+h^5V_{11}+2h^3V_{12}+2h^3V_{13}+4hV_{14}+2h^3V_{15}+4hV_{16}+4hV_{17}+4\overline{h}V_{18}\\
&+2h^3V_{21}+4hV_{22}+4hV_{23}+4\overline{h}V_{24}+4hV_{25}+4\overline{h}V_{26}+4\overline{h}V_{27}+2\overline{h}^3V_{28}\\
&+2h^3V_{31}+4hV_{32}+4hV_{33}+4\overline{h}V_{34}+4hV_{35}+4\overline{h}V_{36}+4\overline{h}V_{37}+2\overline{h}^3V_{38}\\
&+4hV_{41}+4\overline{h}V_{42}+4\overline{h}V_{43}+2\overline{h}^3V_{44}+4\overline{h}V_{45}+2\overline{h}^3V_{46}+2\overline{h}^3V_{47}+\overline{h}^5V_{48}\Big].
\end{aligned}$$

Using Lemmas 6.7, 6.8 and 6.9, we find that

$$\begin{aligned}\mathcal{K}_3(\langle H\rangle,1) = \frac{1}{2^{11}}\big[&32(q^2-20q+81)\\ &+h^5V_{11}+2h^3V_{12}+2h^3V_{13}+4hV_{14}+2h^3V_{15}+4hV_{16}+4hV_{17}+4\overline{h}V_{18}\\ &+2h^3V_{21}+4hV_{22}+4hV_{23}+4\overline{h}V_{24}+4hV_{25}+4\overline{h}V_{26}+4\overline{h}V_{27}+2\overline{h}^3V_{28}\\ &+2h^3V_{31}+4hV_{32}+4hV_{33}+4\overline{h}V_{34}+4hV_{35}+4\overline{h}V_{36}+4\overline{h}V_{37}+2\overline{h}^3V_{38}\\ &+4hV_{41}+4\overline{h}V_{42}+4\overline{h}V_{43}+2\overline{h}^3V_{44}+4\overline{h}V_{45}+2\overline{h}^3V_{46}+2\overline{h}^3V_{47}+\overline{h}^5V_{48}\big]. \end{aligned} \tag{6.24}$$

Now, we convert each term of the form V_{ij} $[i \in \{1,2,3,4\}, j \in \{1,2,\ldots,8\}]$ into its equivalent $q^2 \cdot {}_3F_2$ form. We use the notation $(t_1,t_2,\ldots,t_5) \in \mathbb{Z}_4^5$ for the term $q^2 \cdot {}_3F_2\left(\begin{matrix}\chi_4^{t_1}, & \chi_4^{t_2}, & \chi_4^{t_3}\\ & \chi_4^{t_4}, & \chi_4^{t_5}\end{matrix}\middle|1\right)$. Then, (6.24) yields

$$\begin{aligned}\mathcal{K}_3(\langle H\rangle,1) = \frac{1}{2^{11}}\big[&32(q^2-20q+81)\\ &+h^5(3,1,1,2,2)+2h^3(1,1,3,2,0)+2h^3(3,1,1,0,2)+4h(1,1,3,0,0)\\ &+2h^3(3,3,1,0,2)+4h(1,3,3,0,0)+4h(3,3,1,2,2)+4\overline{h}(1,3,3,2,0)\\ &+2h^3(3,1,3,2,2)+4h(1,1,1,2,0)+4h(3,1,3,0,2)+4\overline{h}(1,1,1,0,0)\\ &+4h(3,3,3,0,2)+4\overline{h}(1,3,1,0,0)+4\overline{h}(3,3,3,2,2)+2\overline{h}^3(1,3,1,2,0)\\ &+2h^3(3,1,3,2,0)+4h(1,1,1,2,2)+4h(3,1,3,0,0)+4\overline{h}(1,1,1,0,2)\\ &+4h(3,3,3,0,0)+4\overline{h}(1,3,1,0,2)+4\overline{h}(3,3,3,2,0)+2\overline{h}^3(1,3,1,2,2)\\ &+4h(3,1,1,2,0)+4\overline{h}(1,1,3,2,2)+4\overline{h}(3,1,1,0,0)+2\overline{h}^3(1,1,3,0,2)\\ &+4\overline{h}(3,3,1,0,0)+2\overline{h}^3(1,3,3,0,2)+2\overline{h}^3(3,3,1,2,0)+\overline{h}^5(1,3,3,2,2)\big]. \end{aligned} \tag{6.25}$$

Next, we use Lemma 6.11 along with the notation therein. We list the tuples $(t_1,t_2,\ldots,t_5)$ in each orbit of the group action of $\mathcal{F}$ on X, and then group the corresponding terms in (6.25) together. The orbit representatives $(1,1,1,0,0)$, $(3,3,3,0,0)$, $(1,3,3,2,0)$, $(3,1,1,2,0)$ and $(1,1,3,0,0)$ mentioned in Lemma 6.11

are the ones whose orbits exhaust the hypergeometric terms in (6.25). We denote the $q^2 \cdot {}_3F_2$ terms corresponding to these orbit representatives as $M_1, M_2, \ldots, M_5$, respectively. Then, (6.25) yields

$$\begin{aligned}\mathcal{K}_3(\langle H\rangle, 1) = \frac{1}{2^{11}}\big[&32(q^2-20q+81)\\ &+h^5M_4+2h^3M_1+2h^3M_1+4hM_5+2h^3M_1+4hM_5+4hM_1+4\overline{h}M_3\\ &+2h^3M_4+4hM_5+4hM_2+4\overline{h}M_1+4hM_5+4\overline{h}M_5+4\overline{h}M_5+2\overline{h}^3M_3\\ &+2h^3M_4+4hM_5+4hM_5+4\overline{h}M_5+4hM_2+4\overline{h}M_1+4\overline{h}M_5+2\overline{h}^3M_3\\ &+4hM_4+4\overline{h}M_2+4\overline{h}M_5+2\overline{h}^3M_2+4\overline{h}M_5+2\overline{h}^3M_2+2\overline{h}^3M_2+\overline{h}^5M_3\big].\end{aligned} \tag{6.26}$$

Using Lemma 6.10 (note that we could not reduce M_5), (6.26) yields

$$\mathcal{K}_3(\langle H\rangle, 1) = \frac{1}{2^7}\left[2(q^2-20q+81)+2u(-p)^t+3q^2\cdot{}_3F_2\left(\begin{matrix}\chi_4, & \chi_4, & \overline{\chi_4}\\ & \varepsilon, & \varepsilon\end{matrix}\Big|1\right)\right]. \tag{6.27}$$

Returning back to (6.20), we are now left to calculate $\mathcal{K}_3(\langle H\rangle, g)$. Again, we have

$$\begin{aligned}&\mathcal{K}_3(\langle H\rangle, g)\\ &=\frac{1}{2^{11}}\sum_{x\neq 0,g}\sum_{y\neq 0,g,x}\big[(2+h\chi_4(g-x)+\overline{h}\overline{\chi_4}(g-x))(2+h\chi_4(g-y)+\overline{h}\overline{\chi_4}(g-y))\\ &\times(2+h\chi_4(x-y)+\overline{h}\overline{\chi_4}(x-y))(2+h\chi_4(x)+\overline{h}\overline{\chi_4}(x))(2+h\chi_4(y)+\overline{h}\overline{\chi_4}(y))\big].\end{aligned} \tag{6.28}$$

Using the substitutions $Y = yg^{-1}$ and $X = xg^{-1}$, and then using the fact that $h\chi_4(g) = \overline{h}$, (6.28) yields

$$\mathcal{K}_3(\langle H\rangle, g)$$

$$= \frac{1}{2^{11}} \sum_{x\neq 0,1} \sum_{y\neq 0,1,x} \big[(2+\overline{h}\chi_4(1-x)+h\overline{\chi_4}(1-x))(2+\overline{h}\chi_4(1-y)+h\overline{\chi_4}(1-y))$$
$$\times\ (2+\overline{h}\chi_4(x-y)+h\overline{\chi_4}(x-y))(2+\overline{h}\chi_4(x)+h\overline{\chi_4}(x))(2+\overline{h}\chi_4(y)+h\overline{\chi_4}(y))\big]\,.$$

Comparing this with (6.21) we see that the expansion of the expression inside this summation will consist of the same summation terms as in (6.21), except that the coefficient corresponding to each summation will become the complex conjugate of the corresponding coefficient of the same summation. This means that, to calculate the coefficient of each summation after expanding the expression in (6.28), we need to replace each corresponding coefficient in (6.26) by its complex conjugate. Now, (6.27) is the final expression from (6.26), and we see that (6.27) contains three summands, two of them being real numbers and the other being a ${}_3F_2$ term whose coefficient is also a real number. Then by the foregoing argument, (6.28) yields the same value as given in (6.27). Thus, (6.20) gives that

$$\mathcal{K}_3(\langle H\rangle) = \frac{q-1}{2^8\times 3}\left[2(q^2-20q+81)+2u(-p)^t+3q^2\cdot {}_3F_2\left(\begin{matrix}\chi_4, & \chi_4, & \overline{\chi_4}\\ & \varepsilon, & \varepsilon\end{matrix}\,\Big|1\right)\right].$$

Substituting the above value in (6.16), we complete the proof of the theorem. ■

6.3 An asymptotic result on the number of cliques

The computations for the number of cliques of order 4 are quite tedious, so we further give an asymptotic result in the following theorem, for the number of cliques of order m in Peisert graphs, $m \geq 1$ being an integer.

Theorem 6.12. *Let p be a prime such that $p \equiv 3 \pmod 4$. For a positive integer t, let $q = p^{2t}$. For $m \geq 1$, let $\mathcal{K}_m(P^*(q))$ denote the number of cliques of order m in*

the Peisert graph $P^*(q)$. Then,

$$\lim_{q\to\infty}\frac{\mathcal{K}_m(P^*(q))}{q^m}=\frac{1}{2^{\binom{m}{2}}m!}.$$

Taking $m=3$ in Theorem 6.12, we find that

$$\lim_{q\to\infty}\frac{\mathcal{K}_3(P^*(q))}{q^3}=\frac{1}{2^4\times 3}.$$

We obtain the same limiting value from Theorem 6.2 as well.

Taking $m=4$ in Theorem 6.3 and Theorem 6.12, we obtain the following corollary which is also evident from Table 6.1.

Corollary 6.12.1. *We have*

$$\lim_{q\to\infty}{}_3F_2\left(\begin{matrix}\chi_4, & \chi_4, & \chi_4^3\\ & \varepsilon, & \varepsilon\end{matrix}\,\middle|\,1\right)=0.$$

Proof. Putting $m=4$ in Theorem 6.12, we have

$$\lim_{q\to\infty}\frac{\mathcal{K}_4(P^*(q))}{q^4}=\frac{1}{2^9\times 3}. \tag{6.29}$$

Putting $m=4$ in Theorem 6.3, we have

$$\lim_{q\to\infty}\frac{\mathcal{K}_4(P^*(q))}{q^4}=\frac{1}{2^9\times 3}+3\times\lim_{q\to\infty}{}_3F_2\left(\begin{matrix}\chi_4, & \chi_4, & \chi_4^3\\ & \varepsilon, & \varepsilon\end{matrix}\,\middle|\,1\right). \tag{6.30}$$

Combining (6.29) and (6.30), we complete the proof. ■

Now, we prove Theorem 6.12. The method follows along the lines of [56] and so we prove by the method of induction.

Proof of Theorem 6.12. We fix an enumeration of the elements of $\mathbb{F}_q$: let $\mathbb{F}_q=\{b_1,b_2,\ldots,b_q\}$. For $u,v\in\{1,2,\ldots,q\}$, we shall use the notation '$a_u<a_v$' to mean

that $a_u, a_v \in \mathbb{F}_q$ and a_u comes before a_v in the enumeration. Now, let $\mathbb{F}_q^* = \langle g \rangle$. Let χ_4 be a fixed character on $\mathbb{F}_q$ of order 4 and let $h = 1 - \chi_4(g)$. First, we note that the result holds for $m = 1, 2$ and so let $m \geq 3$. Let the induction hypothesis hold for $m - 1$. We shall use the notation '$a_m \neq a_i$' to mean that $a_m \in \mathbb{F}_q$ and $a_m \neq a_1, \ldots, a_{m-1}$. Recalling (6.1), we find that

$$\mathcal{K}_m(P^*(q)) = \sum_{\substack{a_1 \in \mathbb{F}_q \\ a_1 < \cdots < a_m}} \cdots \sum_{a_m \in \mathbb{F}_q} \prod_{1 \leq i < j \leq m} \frac{2 + h\chi_4(a_i - a_j) + \overline{h}\chi_4^3(a_i - a_j)}{4}. \tag{6.31}$$

Our goal is to use induction as used in the proofs in [56], so we isolate the sum indexed by a_m along with the associated terms involving a_m. We replace the condition $a_{m-1} < a_m$ by $a_m \neq a_i$, and note that this counts each set of m vertices m times, once for each possible final term, and so we must divide by m. Then, (6.31) yields

$$\begin{aligned}\mathcal{K}_m(P^*(q)) = \frac{1}{m} \sum_{\substack{a_1 \in \mathbb{F}_q \\ a_1 < \cdots < a_{m-1}}} \cdots \sum_{a_m \in \mathbb{F}_q} \Bigg[\prod_{1 \leq i < j \leq m-1} \frac{2 + h\chi_4(a_i - a_j) + \overline{h}\chi_4^3(a_i - a_j)}{4} \\ \frac{1}{4^{m-1}} \sum_{a_m \neq a_i} \prod_{i=1}^{m-1} \{2 + h\chi_4(a_m - a_i) + \overline{h}\chi_4^3(a_m - a_i)\} \Bigg]\end{aligned} \tag{6.32}$$

In order to use the induction hypothesis, we try to bound the expression

$$\mathcal{J} := \sum_{a_m \neq a_i} \prod_{i=1}^{m-1} \{2 + h\chi_4(a_m - a_i) + \overline{h}\chi_4^3(a_m - a_i)\}$$

in terms of q and m. We find that

$$\begin{aligned}\mathcal{J} &:= \sum_{a_m \neq a_i} \prod_{i=1}^{m-1} \{2 + h\chi_4(a_m - a_i) + \overline{h}\chi_4^3(a_m - a_i)\} \\ &= 2^{m-1}(q - m + 1) \\ &+ \sum_{a_m \neq a_i} [(3^{m-1} - 1) \text{ number of terms containing expressions in } \chi_4].\end{aligned} \tag{6.33}$$

Each term in (6.33) containing χ_4 is of the form

$$2^f h^{i'} \overline{h}^{j'} \chi_4((a_m - a_{i_1})^{j_1} \cdots (a_m - a_{i_s})^{j_s}),$$

where

$$\left.\begin{aligned} &0 \leq f \leq m-2, \\ &0 \leq i', j' \leq m-1, \\ &i_1, \ldots, i_s \in \{1, 2, \ldots, m-1\}, \\ &j_1, \ldots, j_s \in \{1, 3\}, \text{ and} \\ &1 \leq s \leq m-1. \end{aligned}\right\} \tag{6.34}$$

Let us consider such an instance of a term containing χ_4. Excluding the constant factor $2^f h^{i'} \overline{h}^{j'}$, we obtain a polynomial in the variable a_m. Let

$$g(a_m) = (a_m - a_{i_1})^{j_1} \cdots (a_m - a_{i_s})^{j_s} \in \mathbb{F}_q[a_m].$$

Using Weil's estimate (Theorem 1.24), we find that

$$|\sum_{a_m \in \mathbb{F}_q} \chi_4(g(a_m))| \leq (j_1 + \cdots + j_s - 1)\sqrt{q}. \tag{6.35}$$

Then, using (6.35) we have

$$\begin{aligned} |2^f h^{i'} \overline{h}^{j'} \sum_{a_m \in \mathbb{F}_q} \chi_4(g(a_m))| &\leq 2^{f+i'+j'}(j_1 + \cdots + j_s - 1)\sqrt{q} \\ &\leq 2^{3m-4}(3m-4)\sqrt{q} \\ &\leq 2^{3m} \cdot 3m\sqrt{q}. \end{aligned} \tag{6.36}$$

Noting that the values of χ_4 are roots of unity, using (6.36), and using the conditions

in (6.34), we obtain

$$|2^f h^{i'} \overline{h}^{j'} \sum_{a_m \neq a_i} \chi_4(g(a_m))| = |2^f h^{i'} \overline{h}^{j'} \left\{ \sum_{a_m} \chi_4(g(a_m)) - \chi_4(g(a_1)) - \cdots - \chi_4(g(a_{m-1})) \right\}|$$
$$\leq 2^{3m} \cdot 3m\sqrt{q} + 2^{2m-3}$$
$$\leq 2^{2m}(1 + 2^m \cdot 3m\sqrt{q}),$$

that is,

$$-2^{2m}(1 + 2^m \cdot 3m\sqrt{q}) \leq 2^f h^{i'} \overline{h}^{j'} \sum_{a_m \neq a_i} \chi_4(g(a_m)) \leq 2^{2m}(1 + 2^m \cdot 3m\sqrt{q}).$$

Then, (6.33) yields

$$2^{m-1}(q - m + 1) - 2^{2m}(1 + 2^m \cdot 3m\sqrt{q})(3^{m-1} - 1)$$
$$\leq \mathcal{J}$$
$$\leq 2^{m-1}(q - m + 1) + 2^{2m}(1 + 2^m \cdot 3m\sqrt{q})(3^{m-1} - 1),$$

and thus, (6.32) yields

$$[2^{m-1}(q - m + 1) - 2^{2m}(1 + 2^m \cdot 3m\sqrt{q})(3^{m-1} - 1)] \times \frac{1}{m \times 4^{m-1}} \mathcal{K}_{m-1}(P^*(q))$$
$$\leq \mathcal{K}_m(P^*(q))$$
$$\leq [2^{m-1}(q - m + 1) + 2^{2m}(1 + 2^m \cdot 3m\sqrt{q})(3^{m-1} - 1)] \times \frac{1}{m \times 4^{m-1}} \mathcal{K}_{m-1}(P^*(q)). \tag{6.37}$$

Dividing by q^m throughout in (6.37) and taking $q \to \infty$, we have

$$\lim_{q\to\infty} \frac{2^{m-1}(q - m + 1) - 2^{2m}(1 + 2^m \cdot 3m\sqrt{q})(3^{m-1} - 1)}{m \times 4^{m-1} \times q} \lim_{q\to\infty} \frac{\mathcal{K}_{m-1}(P^*(q))}{q^{m-1}}$$
$$\leq \lim_{q\to\infty} \frac{\mathcal{K}_m(P^*(q))}{q^m}$$

$$\leq \lim_{q\to\infty} \frac{2^{m-1}(q-m+1)+2^{2m}(1+2^m\cdot 3m\sqrt{q})(3^{m-1}-1)}{m\times 4^{m-1}\times q} \lim_{q\to\infty} \frac{\mathcal{K}_{m-1}(P^*(q))}{q^{m-1}}. \tag{6.38}$$

Now, using the induction hypothesis and noting that

$$\begin{aligned}
&\lim_{q\to\infty} \frac{2^{m-1}(q-m+1)\pm 2^{2m}(1+2^m\cdot 3m\sqrt{q})(3^{m-1}-1)}{m\times 4^{m-1}q} \\
&= \frac{2^{m-1}}{m\times 4^{m-1}} \\
&= \frac{1}{m\times 2^{m-1}},
\end{aligned}$$

we find that both the limits on the left hand side and the right hand side of (6.38) are equal. This completes the proof of the result. ■

7

Hypergeometric functions for Dirichlet characters

7.1 Introduction

Number theorists have introduced finite field hypergeometric functions as generalizations of classical hypergeometric functions by using Gauss and Jacobi sums, see for example [27, 32, 33, 42]. Some of the biggest motivations for studying finite field hypergeometric functions have been their connections with Fourier coefficients

[1]Contents of this chapter have been published in *La Matematica* (2023).

and eigenvalues of modular forms and with counting points on certain kinds of algebraic varieties. For example, Ono [45] gave formulae for the number of $\mathbb{F}_p$-points on elliptic curves in terms of special values of Greene's finite field hypergeometric functions. In [46], Ono wrote a beautiful chapter on finite field hypergeometric functions and mentioned several open problems on hypergeometric functions and their relations to modular forms and algebraic varieties. In recent times, many authors have studied and found solutions to some of the problems posed by Ono. Finite field hypergeometric functions have recently led to applications in graph theory as well, for example in the study of Paley and Peisert graphs [11, 21, 56].

In Chapter 8, we introduce a Peisert-like graph. To find the number of cliques of order four in the Peisert-like graph, we need to evaluate certain character sums involving Dirichlet characters. In this chapter, we introduce hypergeometric functions having Dirichlet characters modulo p^α as arguments, where p is an odd prime and α is a positive integer. Our goal is to find $\mathbb{Z}_{p^\alpha}$- analogues of transformations satisfied by Greene's finite field hypergeometric functions as given in [33]. Then, these transformations will be used to study Peisert-like graphs in Chapter 8.

7.2 Paving the way and the subsequent definition

Let $s, t \in \mathbb{Z}_{p^\alpha}$. We define the function $\delta_s(t)$ as

$$\delta_s(t) = \begin{cases} 1, & \text{if } s = t; \\ 0, & \text{otherwise.} \end{cases}$$

Firstly, we study some character sums involving Dirichlet characters. For Dirichlet characters A and B modulo n, the Jacobi sum is defined as

$$J(A, B) := \sum_{x \in \mathbb{Z}_n} A(x)B(1-x),$$

similar to Definition 1.25. The following lemma is an analogue of Theorem 1.27.

Lemma 7.1. *Let $q = p^\alpha$, where p is an odd prime and $\alpha \geq 1$ is an integer. Let A be a Dirichlet character mod q. For $x \in \mathbb{Z}_q$, we have*

$$A(1+x) = \sum_{t=0}^{p^{\alpha-1}-1} A(1+tp)\delta_{tp}(x) + \frac{1}{\phi(q)} \sum_{\chi \in \widehat{\mathbb{Z}_q^*}} J(A, \overline{\chi})\chi(-x). \tag{7.1}$$

Proof. For $a \in \mathbb{Z}_q^*$, we have

$$\frac{1}{\phi(q)} \sum_{\chi \in \widehat{\mathbb{Z}_q^*}} \chi(x)\overline{\chi}(a) = \begin{cases} 1, & \text{if } x = a; \\ 0, & \text{otherwise.} \end{cases}$$

Hence, we have

$$\begin{aligned} A(1+x) &= \sum_{t=0}^{p^{\alpha-1}-1} A(1+tp)\delta_{tp}(x) + \sum_{a \in \mathbb{Z}_q^*} A(1+a)\delta_a(x) \\ &= \sum_{t=0}^{p^{\alpha-1}-1} A(1+tp)\delta_{tp}(x) + \frac{1}{\phi(q)} \sum_{\chi \in \widehat{\mathbb{Z}_q^*}} \chi(x) \sum_{a \in \mathbb{Z}_q^*} A(1+a)\overline{\chi}(a). \end{aligned}$$

It is easy to see that

$$\sum_{a \in \mathbb{Z}_q} A(1+a)\overline{\chi}(a) = \sum_{a \in \mathbb{Z}_q} A(1-a)\overline{\chi}(-a) = \chi(-1)J(A, \overline{\chi}),$$

which completes the proof of the lemma. ∎

We have already observed in Theorem 1.27 that the finite field analogue of the binomial coefficient is the Jacobi sum. Following Greene, we define binomial coefficient for Dirichlet characters.

Definition 7.2. *Let $q = p^\alpha$, where p is an odd prime and $\alpha \geq 1$ is an integer. For Dirichlet characters A and B mod q, we define $\binom{A}{B} := \frac{B(-1)}{q} J(A, \overline{B})$.*

We can rewrite (7.1) in terms of binomial coefficients as follows.

$$A(1+x) = \sum_{t=0}^{p^{\alpha-1}-1} A(1+tp)\delta_{tp}(x) + \frac{q}{\phi(q)} \sum_{\chi \in \widehat{\mathbb{Z}_q^*}} \binom{A}{\chi} \chi(x). \tag{7.2}$$

In the following lemma, we state some properties of the binomial coefficients. This is an analogue of Proposition 1.29.

Lemma 7.3. *Let $q = p^\alpha$, where p is an odd prime and $\alpha \geq 1$ is an integer. For Dirichlet characters A and B mod q, we have*

$$\binom{A}{B} = \binom{A}{A\overline{B}}; \tag{7.3}$$

$$\binom{A}{B} = \binom{\overline{A}B}{B} B(-1); \tag{7.4}$$

$$\binom{A}{B} = \binom{\overline{B}}{\overline{A}} AB(-1). \tag{7.5}$$

Proof. We prove (7.3). By definition,

$$\begin{aligned} \binom{A}{A\overline{B}} &= \frac{AB(-1)}{q} J(A, \overline{A}B) \\ &= \frac{AB(-1)}{q} \sum_{p \nmid x, 1-x} A(x)\overline{A}B(1-x) \\ &= \frac{AB(-1)}{q} \sum_{p \nmid x, 1-x} A(x(1-x)^{-1})B(1-x). \end{aligned} \tag{7.6}$$

The following map

$$\begin{aligned} \{x \in \mathbb{Z}_q : p \nmid x, 1-x\} &\to \{y \in \mathbb{Z}_q : p \nmid y, y+1\} \\ x &\mapsto x(1-x)^{-1} \end{aligned}$$

is a bijection, so (7.6) yields

$$\begin{aligned}\binom{A}{A\overline{B}} &= \frac{AB(-1)}{q}\sum_{p\nmid y,y+1} A(y)\overline{B}(1+y)\\ &= \frac{AB(-1)}{q}\sum_{p\nmid y,y+1} A(-y)\overline{B}(1-y)\\ &= \frac{AB(-1)}{q}A(-1)J(A,\overline{B}),\end{aligned}$$

which equals $\binom{A}{B}$. This proves (7.3). The proofs of (7.4) and (7.5) follow in a similar fashion, using the definition of binomial coefficient and the bijection used in the proof of (7.3).

■

The following definition can be considered as a $\mathbb{Z}_{p^\alpha}$- analogue for the integral representation of the classical hypergeometric series.

Definition 7.4. *Let $q = p^\alpha$, where p is an odd prime and $\alpha \geq 1$ is an integer. Let A, B and C be Dirichlet characters mod q and let ε be the trivial character mod q. Then, for $x \in \mathbb{Z}_q$, we define*

$${}_2F_1\left(\begin{matrix}A, & B\\ & C\end{matrix}\,\middle|\, x\right) := \frac{\varepsilon(x)BC(-1)}{q}\sum_{y\in\mathbb{Z}_q} B(y)\overline{B}C(1-y)\overline{A}(1-xy).$$

In the following lemma we express the hypergeometric function in terms of the binomial coefficients, much like [33, Theorem 3.6].

Lemma 7.5. *Let $q = p^\alpha$, where p is an odd prime and $\alpha \geq 1$ is an integer. For Dirichlet characters A, B and C mod q,*

$${}_2F_1\left(\begin{matrix}A, & B\\ & C\end{matrix}\,\middle|\, x\right) = \frac{q}{\phi(q)}\sum_{\chi\in\widehat{\mathbb{Z}_q^*}}\binom{A\chi}{\chi}\binom{B\chi}{C\chi}\chi(x).$$

Proof. Let $y \in \mathbb{Z}_q$. By (7.2), we have

$$\overline{A}(1-xy) = \sum_{t=0}^{p^{\alpha-1}-1} \overline{A}(1+tp)\delta_{tp}(-xy) + \frac{q}{\phi(q)} \sum_{\chi \in \widehat{\mathbb{Z}_q^*}} \binom{\overline{A}}{\chi} \chi(-xy). \tag{7.7}$$

Using (7.4), (7.7) yields

$$\overline{A}(1-xy) = \sum_{t=0}^{p^{\alpha-1}-1} \overline{A}(1+tp)\delta_{tp}(-xy) + \frac{q}{\phi(q)} \sum_{\chi \in \widehat{\mathbb{Z}_q^*}} \binom{A\chi}{\chi} \chi(xy). \tag{7.8}$$

Substituting (7.8) in Definition 7.4 and noting that $\varepsilon(x)B(y)\delta_{tp}(-xy) = 0$ for all x and y yields

$$\begin{aligned}
{}_2F_1\left(\begin{matrix} A, & B \\ & C \end{matrix} \middle| x \right) &= \frac{BC(-1)}{\phi(q)} \sum_{y \in \mathbb{Z}_q} \sum_{\chi \in \widehat{\mathbb{Z}_q^*}} \binom{A\chi}{\chi} \chi(x) B\chi(y) \overline{B}C(1-y) \\
&= \frac{BC(-1)}{\phi(q)} \sum_{\chi \in \widehat{\mathbb{Z}_q^*}} \binom{A\chi}{\chi} J(B\chi, \overline{B}C)\chi(x) \\
&= \frac{q}{\phi(q)} \sum_{\chi \in \widehat{\mathbb{Z}_q^*}} \binom{A\chi}{\chi} \binom{B\chi}{B\overline{C}} \chi(x),
\end{aligned}$$

and we complete the proof by using (7.3). ∎

We now define hypergeometric functions containing Dirichlet characters for any $n \geq 1$.

Definition 7.6. *Let $q = p^\alpha$, where p is an odd prime and $\alpha \geq 1$ is an integer. For Dirichlet characters A_0, A_1, …, A_n, and $B_1, \ldots, B_n$ mod q and $x \in \mathbb{Z}_q$, the hypergeometric function ${}_{n+1}F_n$ is defined by*

$${}_{n+1}F_n\left(\begin{matrix} A_0, & A_1, & \ldots, & A_n \\ & B_1, & \ldots, & B_n \end{matrix} \middle| x \right) := \frac{q}{\phi(q)} \sum_{\chi \in \widehat{\mathbb{Z}_q^*}} \binom{A_0\chi}{\chi} \binom{A_1\chi}{B_1\chi} \cdots \binom{A_n\chi}{B_n\chi} \chi(x).$$

We have the following recursive formula, an analogue of Theorem 1.41.

Lemma 7.7. *Let $q = p^\alpha$, where p is an odd prime and $\alpha \geq 1$ is an integer. For Dirichlet characters A_0, A_1, ..., A_n, and $B_1, \ldots, B_n$ mod q and $x \in \mathbb{Z}_q$, we have*

$$
\begin{aligned}
&{}_{n+1}F_n\left(\begin{matrix} A_0, & A_1, & \ldots, & A_n \\ & B_1, & \ldots, & B_n \end{matrix}\,\middle|\, x\right) \\
&= \frac{A_nB_n(-1)}{q}\sum_y {}_nF_{n-1}\left(\begin{matrix} A_0, & A_1, & \ldots, & A_{n-1} \\ & B_1, & \ldots, & B_{n-1} \end{matrix}\,\middle|\, xy\right) A_n(y)\overline{A_n}B_n(1-y).
\end{aligned}
$$

Proof. Let $\chi \in \widehat{\mathbb{Z}_q^*}$. Using (7.3), we find that

$$
\begin{aligned}
\binom{A_n\chi}{B_n\chi} &= \binom{A_n\chi}{A_n\overline{B_n}} \\
&= \frac{A_nB_n(-1)}{q} J(A_n\chi, \overline{A_n}B_n) \\
&= \frac{A_nB_n(-1)}{q}\sum_{y\in\mathbb{Z}_q} A_n\chi(y)\overline{A_n}B_n(1-y). \qquad (7.9)
\end{aligned}
$$

Then, using (7.9) in Definition 7.6, we have

$$
\begin{aligned}
&{}_{n+1}F_n\left(\begin{matrix} A_0, & A_1, & \ldots, & A_n \\ & B_1, & \ldots, & B_n \end{matrix}\,\middle|\, x\right) \\
&= \frac{q}{\phi(q)}\sum_{\chi\in\widehat{\mathbb{Z}_q^*}}\left[\binom{A_0\chi}{\chi}\binom{A_1\chi}{B_1\chi}\cdots\binom{A_{n-1}\chi}{B_{n-1}\chi}\chi(x)\left(\frac{A_nB_n(-1)}{q}\sum_{y\in\mathbb{Z}_q} A_n\chi(y)\overline{A_n}B_n(1-y)\right)\right] \\
&= \frac{A_nB_n(-1)}{q}\sum_{y\in\mathbb{Z}_q}\left(\frac{q}{\phi(q)}\sum_{\chi\in\widehat{\mathbb{Z}_q^*}}\binom{A_0\chi}{\chi}\binom{A_1\chi}{B_1\chi}\cdots\binom{A_{n-1}\chi}{B_{n-1}\chi}\chi(xy)\right)A_n(y)\overline{A_n}B_n(1-y),
\end{aligned}
$$

and we complete the proof by noting Definition 7.6 again.

■

We have the following corollary which is an analogue of Corollary 3.14 in [33].

Corollary 7.7.1. *Let $q = p^\alpha$, where p is an odd prime and $\alpha \geq 1$ is an integer. Let A, B, C, D and E be Dirichlet characters mod q and let ε be the trivial character mod q. Then,*

$$ {}_3F_2\left(\begin{matrix} A, & B, & C \\ & D, & E \end{matrix}\Big| x\right) = \frac{\varepsilon(x)BCDE(-1)}{q^2} \times \sum_{y,z} C(y)\overline{C}E(1-y)B(z)\overline{B}D(1-z)\overline{A}(1-xyz), \quad (7.10) $$

$$ {}_3F_2\left(\begin{matrix} A, & B, & C \\ & D, & E \end{matrix}\Big| x\right) = \frac{\varepsilon(x)BD(-1)}{q^2} \times \sum_{y,z} A\overline{E}(y)\overline{C}E(1-y)B(z)\overline{B}D(1-z)\overline{A}(y-xz). \quad (7.11) $$

Proof. The proof of (7.10) follows from Lemma 7.7 and Definition 7.4. To prove (7.11), we note that

$$ \{x \in \mathbb{Z}_q : p \nmid y, 1-y\} \to \{y' \in \mathbb{Z}_q : p \nmid y', 1-y'\} $$
$$ y \mapsto y^{-1} $$

is a bijection. So, we use the substitution $y' = y^{-1}$ in the sum indexed by y in (7.10) and readily obtain (7.11).

■

7.3 Certain transformations of hypergeometric functions

Now, we list some transformation formulae satisfied by the aforementioned hypergeometric functions, along similar lines as in [33]. To be specific, we shall observe that (1.3)-(1.9) also hold if we replace multiplicative characters on a finite field by

Dirichlet characters modulo p^α. These transformations will be used to derive a formula for the number of cliques of order four in the Peisert-like graphs in the next chapter, hence we state them as lemmas. Recalling Definition 7.6, we have

$$ {}_3F_2\left(\begin{matrix} A, & B, & C \\ & D, & E \end{matrix}\Big|1\right) = \frac{p^\alpha}{\phi(p^\alpha)} \sum_{\chi \in \widehat{\mathbb{Z}^*_{p^\alpha}}} \binom{A\chi}{\chi}\binom{B\chi}{D\chi}\binom{C\chi}{E\chi}\chi(1). \tag{7.12} $$

Below are three lemmas whose proofs involve change of variable in the sum in (7.12). The following lemma is a $\mathbb{Z}_{p^\alpha}$- analogue of (1.3).

Lemma 7.8. *Let p be an odd prime and let $\alpha \geq 1$ be an integer. Let A, B, C, D, E be Dirichlet characters mod p^α. Then,*

$$ {}_3F_2\left(\begin{matrix} A, & B, & C \\ & D, & E \end{matrix}\Big|1\right) = {}_3F_2\left(\begin{matrix} B\overline{D}, & A\overline{D}, & C\overline{D} \\ & \overline{D}, & E\overline{D} \end{matrix}\Big|1\right). $$

Proof. Employing the transformation $\chi \mapsto \overline{D}\chi$ in (7.12) yields the required result. ∎

The following lemma is a $\mathbb{Z}_{p^\alpha}$- analogue of (1.4).

Lemma 7.9. *Let p be an odd prime and let $\alpha \geq 1$ be an integer. Let A, B, C, D, E be Dirichlet characters mod p^α. Then,*

$$ {}_3F_2\left(\begin{matrix} A, & B, & C \\ & D, & E \end{matrix}\Big|1\right) = ABCDE(-1){}_3F_2\left(\begin{matrix} A, & A\overline{D}, & A\overline{E} \\ & A\overline{B}, & A\overline{C} \end{matrix}\Big|1\right). $$

Proof. We employ the transformation $\chi \mapsto \overline{A\chi}$ in (7.12), and then use (7.5) to complete the proof. ∎

The following lemma is a $\mathbb{Z}_{p^\alpha}$- analogue of (1.5).

Lemma 7.10. *Let p be an odd prime and let $\alpha \geq 1$ be an integer. Let A, B, C, D, E be Dirichlet characters mod p^α. Then,*

$$ {}_3F_2\left(\begin{matrix} A, & B, & C \\ & D, & E \end{matrix}\Big|1\right) = ABCDE(-1){}_3F_2\left(\begin{matrix} B\overline{D}, & B, & B\overline{E} \\ & B\overline{A}, & B\overline{C} \end{matrix}\Big|1\right). $$

Proof. Employing the transformation $\chi \mapsto \overline{B\chi}$ in (7.12), and then using (7.5) we complete the proof. ∎

We further prove $\mathbb{Z}_{p^\alpha}$- analogues of certain transformations satisfied by the Greene's finite field hypergeometric functions. We shall evoke Definition 7.4 and Lemma 7.7 multiple times. Note that in the proofs, we denote the multiplicative inverse of $x \in \mathbb{Z}_{p^\alpha}^*$ by x^{-1}. Following is an $\mathbb{Z}_{p^\alpha}$- analogue of (1.6).

Lemma 7.11. *Let p be an odd prime and let $\alpha \geq 1$ be an integer. Let A, B, C, D, E be Dirichlet characters mod p^α. Then,*

$$ {}_3F_2\left(\begin{matrix} A, & B, & C \\ & D, & E \end{matrix}\Big|1\right) = AE(-1){}_3F_2\left(\begin{matrix} A, & B, & \overline{C}E \\ & AB\overline{D}, & E \end{matrix}\Big|1\right). $$

Proof. We first show that for $x \in \mathbb{Z}_{p^\alpha}^*$, if $p \nmid 1-x$, then

$$ {}_2F_1\left(\begin{matrix} A, & B \\ & D \end{matrix}\Big|x\right) = A(-1){}_2F_1\left(\begin{matrix} A, & B \\ & AB\overline{D} \end{matrix}\Big|1-x\right). \tag{7.13} $$

To prove (7.13), let $x \in \mathbb{Z}_{p^\alpha}^*$ be such that $p \nmid 1-x$. By Definition 7.4, we have

$$ {}_2F_1\left(\begin{matrix} A, & B \\ & D \end{matrix}\Big|x\right) = \frac{1 \times BD(-1)}{p^\alpha} \sum_{p\nmid y, 1-y, 1-xy} B(y)\overline{B}D(1-y)\overline{A}(1-xy). \tag{7.14} $$

We find that

$$\{y \in \mathbb{Z}_{p^\alpha} : p \nmid y, 1-y, 1-xy\} \to \{z \in \mathbb{Z}_{p^\alpha} : p \nmid z, 1-z, 1-(1-x)z\}$$
$$y \mapsto y(y-1)^{-1}$$

is a bijection. Hence, (7.14) yields

$$\begin{aligned}
{}_2F_1\left(\begin{matrix} A, & B \\ & D \end{matrix}\Big| x\right) &= \frac{BD(-1)}{p^\alpha} \sum_{\substack{p\nmid z,1-z,\\ 1-(1-x)z}} [B(z(z-1)^{-1})\overline{B}D(-(z-1)^{-1}) \\
&\qquad \times \overline{A}((z-1-xz)(z-1)^{-1})] \\
&= \frac{D(-1)}{p^\alpha} \sum_{\substack{p\nmid z,1-z,\\ 1-(1-x)z}} B(z)A\overline{D}(1-z)\overline{A}(1-(1-x)z). \qquad (7.15)
\end{aligned}$$

Thus, by Definition 7.4 and (7.15), and noting that $\varepsilon(1-x) = 1$, we conclude (7.13). Now, Lemma 7.7 and (7.13) give

$$\begin{aligned}
{}_3F_2\left(\begin{matrix} A, & B, & C \\ & D, & E \end{matrix}\Big| 1\right) &= \frac{CE(-1)}{p^\alpha} \sum_{p\nmid x,1-x} {}_2F_1\left(\begin{matrix} A, & B \\ & D \end{matrix}\Big| x\right) C(x)\overline{C}E(1-x) \\
&= \frac{ACE(-1)}{p^\alpha} \sum_{p\nmid x,1-x} {}_2F_1\left(\begin{matrix} A, & B \\ & AB\overline{D} \end{matrix}\Big| 1-x\right) C(x)\overline{C}E(1-x) \\
&= \frac{ACE(-1)}{p^\alpha} \sum_{p\nmid x,1-x} {}_2F_1\left(\begin{matrix} A, & B \\ & AB\overline{D} \end{matrix}\Big| x\right) C(1-x)\overline{C}E(x) \\
&= AE(-1){}_3F_2\left(\begin{matrix} A, & B, & \overline{C}E \\ & AB\overline{D}, & E \end{matrix}\Big| 1\right),
\end{aligned}$$

where we have used the substitution $x \mapsto 1-x$ in the penultimate line. This completes the proof of the lemma. ■

The following lemma gives a $\mathbb{Z}_{p^\alpha}$- analogue of (1.7).

Lemma 7.12. *Let p be an odd prime and let $\alpha \geq 1$ be an integer. Let A, B, C, D, E be Dirichlet characters mod p^α. Then,*

$$ {}_3F_2\left(\begin{matrix} A, & B, & C \\ & D, & E \end{matrix}\Big| 1\right) = AD(-1)\,{}_3F_2\left(\begin{matrix} A, & \overline{B}D, & C \\ & D, & AC\overline{E} \end{matrix}\Big| 1\right). $$

Proof. Putting $x = 1$ in (7.11) and using the substitutions $y' = 1 - y$ and $z' = 1 - z$ in the double summation therein yield the required result. ∎

The following lemma gives a $\mathbb{Z}_{p^\alpha}$- analogue of (1.8).

Lemma 7.13. *Let p be an odd prime and $\alpha \geq 1$ be an integer. Let A, B, C, D, E be Dirichlet characters mod p^α. Then,*

$$ {}_3F_2\left(\begin{matrix} A, & B, & C \\ & D, & E \end{matrix}\Big| 1\right) = B(-1)\,{}_3F_2\left(\begin{matrix} \overline{A}D, & B, & C \\ & D, & BC\overline{E} \end{matrix}\Big| 1\right). $$

Proof. At first, we show that if $x \in \mathbb{Z}_{p^\alpha}$ such that $p \nmid 1 - x$, then

$$ {}_2F_1\left(\begin{matrix} A, & B \\ & D \end{matrix}\Big| x\right) = \overline{B}(1-x)\,{}_2F_1\left(\begin{matrix} \overline{A}D, & B \\ & D \end{matrix}\Big| x(x-1)^{-1}\right). \tag{7.16} $$

To prove this, let $x \in \mathbb{Z}_{p^\alpha}$ be such that $p \nmid 1 - x$. We begin by employing Definition 7.4 to obtain

$$ {}_2F_1\left(\begin{matrix} A, & B \\ & D \end{matrix}\Big| x\right) = \frac{\varepsilon(x)BD(-1)}{p^\alpha} \sum_{p\nmid y, 1-y, 1-xy} B(y)\overline{B}D(1-y)\overline{A}(1-xy). \tag{7.17} $$

The following map

$$ \{y \in \mathbb{Z}_{p^\alpha} : p \nmid y, 1-y, 1-xy\} \to \{z \in \mathbb{Z}_{p^\alpha} : p \nmid z, 1-z, 1-x+xz\} $$
$$ y \mapsto y(1-x)(1-xy)^{-1} $$

is a bijection. Hence, using the substitution $y \mapsto y(1-x)(1-xy)^{-1}$ in the sum in (7.17) yields

$$\begin{aligned}
&{}_2F_1\left(\begin{matrix}A, & B\\ & D\end{matrix}\Big|x\right)\\
&= \frac{\varepsilon(x)BD(-1)}{p^\alpha}\sum_{\substack{p\nmid z,1-z,\\ 1-x+xz}}[B(z(1-x+xz)^{-1})\overline{B}D((1-x)(1-z)(1-x+xz)^{-1})\\
&\qquad\qquad \times \overline{A}((1-x)(1-x+xz)^{-1})]\\
&= \frac{\overline{AB}D(1-x)\varepsilon(x)BD(-1)}{p^\alpha}\sum_{\substack{p\nmid z,1-z,\\ 1-x+xz}} B(z)\overline{B}D(1-z)A\overline{D}(1-x+xz).\\
&= \frac{\overline{B}(1-x)\varepsilon(x)BD(-1)}{p^\alpha}\sum_{\substack{p\nmid z,1-z,\\ 1-x+xz}} B(z)\overline{B}D(1-z)A\overline{D}(1-xz(x-1)^{-1}). \qquad (7.18)
\end{aligned}$$

Note that we have assumed $p \nmid x-1$, so $p \mid x$ if and only if $p \mid x(x-1)^{-1}$. Therefore, we have $\varepsilon(x) = \varepsilon\left(x(x-1)^{-1}\right)$. Thus, replacing $\varepsilon(x)$ by $\varepsilon(x(x-1)^{-1})$ in (7.18) and then using Definition 7.4 in the same, we conclude (7.16).

Now, using Lemma 7.7 and (7.16) we find that

$$\begin{aligned}
{}_3F_2\left(\begin{matrix}A, & B, & C\\ & D, & E\end{matrix}\Big|1\right) &= \frac{CE(-1)}{p^\alpha}\sum_{p\nmid y,1-y}{}_2F_1\left(\begin{matrix}A, & B\\ & D\end{matrix}\Big|y\right)C(y)\overline{C}E(1-y)\\
&= \frac{CE(-1)}{p^\alpha}\sum_{p\nmid y,1-y}\left[{}_2F_1\left(\begin{matrix}\overline{A}D, & B\\ & D\end{matrix}\Big|y(y-1)^{-1}\right)\right.\\
&\qquad\qquad \left.\times C(y)\overline{BC}E(1-y)\right]. \qquad (7.19)
\end{aligned}$$

It is easy to see that

$$\begin{aligned}
\{y \in \mathbb{Z}_{p^\alpha} : p \nmid y, 1-y\} &\to \{z \in \mathbb{Z}_{p^\alpha} : p \nmid z, 1-z\}\\
y &\mapsto y(y-1)^{-1}
\end{aligned}$$

is a bijection, and hence, (7.19) together with Lemma 7.7 yields

$$
\begin{aligned}
{}_3F_2\left(\begin{matrix} A, & B, & C \\ & D, & E \end{matrix}\Big|1\right) &= \frac{CE(-1)}{p^\alpha}\sum_{p\nmid z,1-z}\left[{}_2F_1\left(\begin{matrix} \overline{A}D, & B \\ & D \end{matrix}\Big|z\right)\right. \\
&\qquad\left.\times\, C\left(z(z-1)^{-1}\right)\overline{BC}E\left(-(z-1)^{-1}\right)\right] \\
&= \frac{E(-1)}{p^\alpha}\sum_{p\nmid z,1-z} C(z)B\overline{E}(1-z){}_2F_1\left(\begin{matrix} \overline{A}D, & B \\ & D \end{matrix}\Big|z\right) \\
&= B(-1){}_3F_2\left(\begin{matrix} \overline{A}D, & B, & C \\ & D, & BC\overline{E} \end{matrix}\Big|1\right),
\end{aligned}
$$

concluding the proof of the lemma. ■

The following lemma is the $\mathbb{Z}_{p^\alpha}$- analogue of (1.9).

Lemma 7.14. *Let p be an odd prime and let $\alpha \geq 1$ be an integer. Let A, B, C, D, E be Dirichlet characters mod p^α. Then,*

$$
{}_3F_2\left(\begin{matrix} A, & B, & C \\ & D, & E \end{matrix}\Big|1\right) = AB(-1){}_3F_2\left(\begin{matrix} \overline{A}D, & \overline{B}D, & C \\ & D, & \overline{AB}DE \end{matrix}\Big|1\right).
$$

Proof. Firstly, we show that if $x \in \mathbb{Z}_{p^\alpha}$ is such that $p \nmid 1-x$, then

$$
{}_2F_1\left(\begin{matrix} A, & B \\ & D \end{matrix}\Big|x\right) = D(-1)\overline{AB}D(1-x){}_2F_1\left(\begin{matrix} \overline{A}D, & \overline{B}D \\ & D \end{matrix}\Big|x\right). \tag{7.20}
$$

To prove this, we assume that $x \in \mathbb{Z}_{p^\alpha}$ satisfying $p \nmid 1-x$. It is easy to see that the following map is a bijection.

$$
\begin{aligned}
\{y \in \mathbb{Z}_{p^\alpha} : p \nmid y, 1-y, 1-xy\} &\to \{z \in \mathbb{Z}_{p^\alpha} : p \nmid z, 1-z, 1-xz\} \\
y &\mapsto (1-y)(1-xy)^{-1}
\end{aligned}
$$

We substitute $z = (1-y)(1-xy)^{-1}$ in the sum in Definition 7.4 to obtain

$$
\begin{aligned}
{}_2F_1\left(\begin{matrix} A, & B \\ & D \end{matrix}\middle| x\right) &= \frac{\varepsilon(x)BD(-1)}{p^\alpha} \sum_{\substack{p\nmid z,1-z,\\ 1-xz}} [B((1-z)(1-xz)^{-1}) \\
&\qquad \times \overline{B}D(z(1-x)(1-xz)^{-1})\overline{A}((1-x)(1-xz)^{-1})] \\
&= \frac{\varepsilon(x)BD(-1)}{p^\alpha}\overline{AB}D(1-x) \sum_{\substack{p\nmid z,1-z,\\ 1-xz}} \overline{B}D(z)B(1-z)A\overline{D}(1-xz).
\end{aligned} \tag{7.21}
$$

As a result, Definition 7.4 and (7.21) yield (7.20). Now, using Lemma 7.7 and (7.20) we find that

$$
\begin{aligned}
&{}_3F_2\left(\begin{matrix} A, & B, & C \\ & D, & E \end{matrix}\middle| 1\right) \\
&= \frac{CE(-1)}{p^\alpha} \sum_{p\nmid y,1-y} {}_2F_1\left(\begin{matrix} A, & B \\ & D \end{matrix}\middle| y\right) C(y)\overline{C}E(1-y) \\
&= \frac{CDE(-1)}{p^\alpha} \sum_{p\nmid y,1-y} {}_2F_1\left(\begin{matrix} \overline{A}D, & \overline{B}D \\ & D \end{matrix}\middle| y\right) C(y)\overline{ABC}DE(1-y) \\
&= AB(-1){}_3F_2\left(\begin{matrix} \overline{A}D, & \overline{B}D, & C \\ & D, & \overline{AB}DE \end{matrix}\middle| 1\right).
\end{aligned}
$$

This completes the proof of the lemma. ■

8

On a Peisert-like graph on $\mathbb{Z}_n$

8.1 Introduction

Besides Paley graphs, their relatives the Peisert graphs have also been generalized into graphs called *generalized Peisert* or *Peisert type* graphs, addressed in [8, 9, 31, 44]. In this chapter, we investigate into the generalization of the Peisert graph for the commutative ring $\mathbb{Z}_n$, much like how we defined the Paley-type graph in Chapter 2. Note that for $q \equiv 1 \pmod 4$, where q is an even power of a prime $p \equiv 3 \pmod 4$ and $\mathbb{F}_q^* = \langle g \rangle$, the edges of the Paley graph are determined by the cosets $\langle g^4 \rangle \cup g^2\langle g^4 \rangle$, while those of the Peisert graph depend on the cosets $\langle g^4 \rangle \cup g\langle g^4 \rangle$.

[1]Contents of this chapter have been published in *La Matematica* (2023).

In this chapter, we introduce a *Peisert-like* graph on the commutative ring $\mathbb{Z}_n$, for suitable n. Computing the number of cliques in the Paley and Peisert graphs has been of interest, for instance see [1, 26]. Our primary focus is to evaluate the number of triangles and cliques of order four in the Peisert-like graph by evaluating certain character sums involving Dirichlet characters. To this end, we make use of the hypergeometric functions containing Dirichlet characters as arguments that were defined in Chapter 7, and then use these functions to compute the number of cliques of order 4 in the Peisert-like graph.

8.2 Defining a Peisert-like graph on $\mathbb{Z}_n$

We begin by considering n such that $\mathbb{Z}_n^*$ is cyclic, omitting the trivial cases $n = 2, 4$. By Proposition 1.1, $n = p^\alpha$ or $2p^\alpha$, where p is an odd prime and α is a positive integer. Since we attempt to define an analogue of the Peisert graph, we consider the possibilities of constructing graphs by considering two cosets out of the four cosets of the subgroup $\langle g^4\rangle$ in $\mathbb{Z}_n^* = \langle g\rangle$. We find that the order of g^4 is equal to

$$o(g^4) = \frac{o(g)}{\gcd(4, o(g))} = \frac{p^{\alpha-1}(p-1)}{\gcd(4, p^{\alpha-1}(p-1))} = \frac{p^{\alpha-1}(p-1)}{2\gcd(2, \frac{p-1}{2})}.$$

If $\gcd(2, \frac{p-1}{2}) = 1$ then $o(g^4) = \frac{o(g)}{2}$ and so $\langle g^4\rangle$ has two distinct cosets in $\langle g\rangle$, whereby $\mathbb{Z}_n^*$ becomes the union of the two distinct cosets. So, in order that the edge set of the graph we construct depends on a proper subset of $\mathbb{Z}_n^*$, we need that $\gcd(2, \frac{p-1}{2}) \neq 1$, and hence $2 \mid \frac{p-1}{2}$, that is, $p \equiv 1 \pmod 4$. Then there are four distinct cosets of $\langle g^4\rangle$ in $\langle g\rangle$. Subsequently, we assume that $n = p^\alpha$ or $n = 2p^\alpha$, where p is an odd prime such that $p \equiv 1 \pmod 4$ and $\alpha \geq 1$. Now, we look at the possible pairs of cosets of $\langle g^4\rangle$ that can be taken to construct the edge set of a well-defined graph. Let the cosets be $g^i\langle g^4\rangle$ and $g^j\langle g^4\rangle, i \neq j$ and $i, j \in \{0, 1, 2, 3\}$. To ensure that an edge is well-defined for an undirected graph, we need the property that, for $x \in \mathbb{Z}_n$, if $x \in g^i\langle g^4\rangle \cup\ g^j\langle g^4\rangle$ then $-x \in g^i\langle g^4\rangle \cup\ g^j\langle g^4\rangle$. Let $G_{i,j}$ denote

the graph constructed, if possible, by taking the vertex set to be $\mathbb{Z}_n$, where $G_{i,j}$ has an edge xy if $x - y \in g^i\langle g^4\rangle \cup g^j\langle g^4\rangle$.

Case 1: If $i = 0$ or $j = 0$ then the cosets are $\langle g^4\rangle$ and $g^a\langle g^4\rangle$ where $a \in \{1, 2, 3\}$. If $a = 2$ then we get back the Paley-type graph, and so we do not consider $G_{0,2}$. Then, we have $a = 1$ or $a = 3$. However, $G_{0,1}$ and $G_{0,3}$, if well defined, are isomorphic due to the following isomorphism:

$$V(G_{0,1}) \to V(G_{0,3})$$
$$x \mapsto g^3x.$$

So, it is enough to study $G_{0,1}$. Note that if $p \equiv 1 \pmod 8$ then $G_{0,1}$ and $G_{0,3}$ are well defined, but if $p \equiv 5 \pmod 8$ then $1 \in \langle g^4\rangle$ but $-1 \notin \langle g^4\rangle$ so an edge is not well defined in both $G_{0,1}$ and $G_{0,3}$. Hence, it is enough to study $G_{0,1}$ when $p \equiv 1 \pmod 8$.

Case 2: Let $i, j \geq 1$. The possible graphs considered are $G_{1,2}, G_{1,3}$ and $G_{2,3}$. We observe the following.

- $p \equiv 1 \pmod 8$ if and only if there exists some $x \in \mathbb{Z}_n^*$ such that $x, -x \in g^i\langle g^4\rangle$.
- If $G_{0,1}, G_{0,2}, G_{1,2}, G_{1,3}$ and $G_{2,3}$ are well defined, we find that $G_{1,2}$ is isomorphic to $G_{0,1}$ by the isomorphism

$$V(G_{1,2}) \to V(G_{0,1})$$
$$x \mapsto g^3x,$$

  and this map provides isomorphisms from $G_{2,3}$ to $G_{1,2}$ and from $G_{1,3}$ to $G_{0,2}$ as well.

Based on the above observations, we have the following subcases.

Subcase 1: $p \equiv 1 \pmod 8$. Then, $G_{0,1}, G_{0,2}, G_{1,2}, G_{1,3}$ and $G_{2,3}$ are well defined. Ignoring the case for $G_{1,3}$ (since it is isomorphic to the Paley-type graph

$G_{0,2}$), we obtain that it is enough to study $G_{0,1}$.

Subcase 2: $p \equiv 5 \pmod 8$. In order that the graph becomes well defined, for any $x \in \mathbb{Z}_n$, $x \in g^i\langle g^4\rangle$ should imply that $-x \in g^j\langle g^4\rangle$, so that $-1 \in g^{j-i}\langle g^4\rangle$. This yields, $-1 = g^{j-i+4h}$ for some $h \in \mathbb{Z}$, which implies $1 = g^{2(j-i+4h)}$, so $p^{\alpha-1}(p-1) \mid 2(j-i+4h)$. Then, $2 \mid j-i$ since $\frac{p-1}{2}$ is even. Hence $i \equiv j \pmod 2$. So, we only consider $G_{1,3}$. Note that in this case $-1 \in g^2\langle g^4\rangle$.

Out of the aforementioned cases, we choose the first case since it seems to mimic the definition of the Peisert graph the most. Thus, we have the following definition.

Definition 8.1 (Peisert-like graph $G^*(n)$)**.** *Let $n = p^\alpha$ or $n = 2p^\alpha$, where p is an odd prime such that $p \equiv 1 \pmod 8$ and α is a positive integer. Let $\mathbb{Z}_n^* = \langle g\rangle$. Then, the Peisert-like graph is the graph $G^*(n) = (V, E)$, where $V = \mathbb{Z}_n$ and $E = \{xy | x - y \in \langle g^4\rangle \cup g\langle g^4\rangle\}$.*

The definition of the graph is independent of the choice of the generator g, like in the Peisert graph. To see this, let h be another generator of $\mathbb{Z}_n^*$. Then $h = g^t$ for some $t \in \mathbb{Z}$. If t is even then $h = (g^{\frac{t}{2}})^2 \in (\mathbb{Z}_n^*)^2$, which implies $\mathbb{Z}_n^* \subseteq (\mathbb{Z}_n^*)^2$, which is not possible. So, $t \equiv 1$ or $3 \pmod 4$. If $t \equiv 1 \pmod 4$, then $\langle g^4\rangle = \langle h^4\rangle$ since both are subgroups of order $\frac{p^{\alpha-1}(p-1)}{4}$ and $\mathbb{Z}_n^*$ is cyclic, and $h\langle h^4\rangle = g^t\langle g^4\rangle = g\langle g^4\rangle$. So the edge set remains unchanged. If $t \equiv 3 \pmod 4$, we define the graph $G'(n)$ as $G'(n) = (V', E')$, where $V' = \mathbb{Z}_n$ and $E' = \{xy | x - y \in \langle h^4\rangle \cup h\langle h^4\rangle\}$. Then,

$$V(G^*(n)) \to V(G'(n))$$
$$x \mapsto hx$$

is an isomorphism.

The Peisert-like graph $G^*(17)$ is shown in Figure 8.1. The vertex 0 is adjacent to the vertices $1, 3, 4, 5, 12, 13, 14$ and 16.

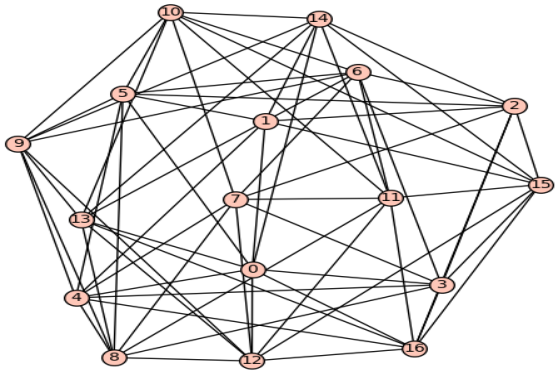

Figure 8.1: The Peisert-like graph of order 17

8.3 Some properties of the Peisert-like graph

We begin by fixing some notation. Let $n = p^\alpha$ or $2p^\alpha$, where $p \equiv 1 \pmod 8$ and $\alpha \geq 1$, and let $G^*(n)$ be the Peisert-like graph of order n. Since 4 divides the order of $\mathbb{Z}_n^*$ and $\mathbb{Z}_n^*$ is cyclic, there exists a character of order 4 in $\widehat{\mathbb{Z}_n^*}$; let us fix such a character and call it χ_4. Let $\varphi = \chi_4^2$ be the quadratic character. The trivial character is denoted by ε. Let $\mathbb{Z}_n^* = \langle g \rangle$ and let $h = 1 - \chi_4(g)$. Then, for $x \in \mathbb{Z}_n^*$, we observe that

$$\frac{2 + h\chi_4(x) + \overline{h}\overline{\chi_4}(x)}{4} = \begin{cases} 1, & \text{if } x \in \langle g^4 \rangle \cup g\langle g^4 \rangle; \\ 0, & \text{otherwise.} \end{cases} \tag{8.1}$$

Now, we prove some basic properties of $G^*(n)$.

Proposition 8.2. *Let $n = p^\alpha$ or $2p^\alpha$, where $p \equiv 1 \pmod 8$ and α is a positive integer. Let $G^*(n)$ be the Peisert-like graph of order n. Then, $G^*(n)$ is regular of degree $\frac{p^{\alpha-1}(p-1)}{2}$. Also, the number of edges in $G^*(n)$ is equal to $\frac{n\phi(n)}{4}$.*

Proof. By the definition of $G^*(n)$, the degree of a vertex is equal to the cardinality of the set $\langle g^4 \rangle \cup g\langle g^4 \rangle$. Alternatively, we may use a character sum to deduce the

same. Let $a \in \mathbb{Z}_n$. Then, using (8.1), we find that the degree of the vertex a is

$$deg(a) = \sum_{x-a \in \mathbb{Z}_n^*} \frac{2 + h\chi_4(a-x) + \overline{h}\overline{\chi_4}(a-x)}{4} = \frac{p^{\alpha-1}(p-1)}{2}.$$

The last equality is obtained by using $\sum_{x-a \in \mathbb{Z}_n^*} \chi_4(a-x) = \sum_{x-a \in \mathbb{Z}_n^*} \overline{\chi_4}(a-x) = 0$. The number of edges in $G^*(n)$ is $\frac{1}{2} \times \sum \deg = \frac{1}{2}\frac{p^{\alpha-1}(p-1)}{2} \times n = \frac{n\phi(n)}{4}$. This completes the proof of the proposition. ■

Alternatively, one can find the number of edges in $G^*(n)$ by evaluating the following character sum:

$$\frac{1}{2}\sum_{x} \sum_{y-x \in \mathbb{Z}_n^*} \frac{2 + h\chi_4(y-x) + \overline{h}\overline{\chi_4}(y-x)}{4}.$$

Proposition 8.3. *Let $n = p^\alpha$ or $2p^\alpha$, where $p \equiv 1 \pmod 8$ and $\alpha \geq 1$, and let $G^*(n)$ be the Peisert-like graph of order n. Then, $G^*(n)$ is vertex-transitive.*

Proof. $G^*(n)$ being a Cayley graph, is vertex-transitive; see [28, Theorem 3.1.2]. We have the following explicit automorphism to demonstrate the same. Let $a \in \mathbb{Z}_n$. Then, the map

$$V(G^*(n)) \to V(G^*(n))$$
$$x \mapsto x + a$$

is an automorphism. This completes the proof. ■

We note here that unlike the Peisert graph, the Peisert-like graph is not self-complementary unless the number of vertices in the graph is a prime. This is because a self complementary graph on n vertices must necessarily have $\frac{n(n-1)}{4}$ edges, but for $n = p^\alpha$ or $n = 2p^\alpha$, $\phi(n) \neq n-1$ unless n is a prime. We also observe that the Peisert-like graph, although never a cycle graph, has a spanning cycle. So, it is a

connected graph. This is because, for each vertex $x \in \mathbb{Z}_n$, the vertices $x+1$ and $x-1$ are both adjacent to x.

8.4 Triangles and cliques of order four in the graph

The Peisert-like graph $G^*(n)$ is defined for $n = p^\alpha$ or $n = 2p^\alpha$, where $p \equiv 1 \pmod 8$ is a prime and α is a positive integer. However, to calculate the number of triangles and cliques of order four in the graph, we consider only the case $n = p^\alpha$. This is because there cannot exist cliques of order more than two if $n = 2p^\alpha$, and we see why. Let $n = 2p^\alpha$, and if possible let x, y and z be vertices in $G^*(n)$ which form a clique. Then $x-y, y-z$ and $x-z$ are necessarily elements in $\mathbb{Z}_n^*$, and therefore, are odd integers, which contradicts that $x - z = x - y + y - z$. Thus, we consider only the case $n = p^\alpha$. In the following theorem, we compute the number of triangles in the Peisert-like graph.

Theorem 8.4. *Let $p \equiv 1 \pmod 8$ be a prime and let α be a positive integer. Let $G^*(p^\alpha)$ be the Peisert-like graph of order p^α. Then,*

$$\mathcal{K}_3(G^*(p^\alpha)) = \frac{p^{3\alpha-2}(p-1)(p-5)}{2^4 \times 3}.$$

Comparing Theorem 3.1 and Theorem 8.4, we observe that for a prime $p \equiv 1 \pmod 8$ and a positive integer α, the number of triangles in the Peisert-like graph of order p^α equals the number of triangles in the Paley-type graph of order p^α.

To find the number of cliques of order 4 in the Peisert-like graph $G^*(p^\alpha)$, one needs to compute certain character sums involving Dirichlet characters modulo p^α. We simplify such character sums by the hypergeometric functions for Dirichlet characters that were introduced in Chapter 7. Thus, we have the following theorem.

Theorem 8.5. *Let $q = p^\alpha$, where $p \equiv 1 \pmod 8$ is a prime and α is a positive integer. Let $G^*(q)$ be the Peisert-like graph of order q. Let χ_4 be a character mod q*

of order 4, *and let* φ *and* ε *be the quadratic and trivial characters mod* q, *respectively. Then,*

$$\mathcal{K}_4(G^*(q)) = \frac{p^{2\alpha-1}(p-1)}{2^{10}\times 3}[2p^{2\alpha-2}(p^2-20p+81)+2Im(\rho)^2+4Im(\rho)\cdot Im(\xi) - Re(M_3)+3M_5],$$

where $\rho := J(\chi_4,\chi_4)$ *and* $\xi := J(\chi_4,\varphi)$; *and* $M_3 = q^2\cdot {}_3F_2\left(\begin{matrix}\chi_4, & \overline{\chi_4}, & \overline{\chi_4}\\ \varphi, & \varepsilon & \end{matrix}\middle|1\right)$ *and* $M_5 = q^2\cdot {}_3F_2\left(\begin{matrix}\chi_4, & \chi_4, & \overline{\chi_4}\\ \varepsilon, & \varepsilon & \end{matrix}\middle|1\right)$ *are the hypergeometric terms.*

It is evident from the theorem that M_5 is a real number, since $\mathcal{K}_4(G^*(q))$ is a real number. Using `Python`, we numerically verify Theorem 8.5 for certain values of p and α. We list some of the values in Table 8.1. We find that for each of the values of p^α listed below, $\rho=\xi$. The `Python` code that we used is provided in the appendix.

$q=p^\alpha$	$\mathcal{K}_4(G^*(q))$	$\rho=\xi$	M_3	M_5	$\mathcal{K}_4(G^*(q))$ (by Thm 8.5)
$17^1=17$	17	$-1+4i$	$-6-24i$	10	17
$41^1=41$	1025	$-5+4i$	$-30-24i$	-30	1025
$73^1=73$	14235	$3+8i$	$-6+16i$	10	14235
$89^1=89$	32307	$-5+8i$	$90+144i$	-22	32307
$97^1=97$	44426	$-9-4i$	$90-40i$	-150	44426
$17^2=289$	1419857	$-17+68i$	$-1734-6936i$	2890	1419857

Table 8.1: Numerical data for Theorem 8.5

Before proceeding with the proofs of the main results, we prove the following lemma which will be recalled in the proofs of Theorem 8.4 and Theorem 8.5.

Lemma 8.6. *Let* $n=p^\alpha$, *where* $p\equiv 1 \pmod 8$ *is a prime and* α *is a positive integer. Let* χ_4 *be a character on* $\mathbb{Z}_n^*$ *of order* 4. *Then,* χ_4 *has period* p.

Proof. The proof goes along similar lines as in Lemmas 2.8 and 2.9 in Chapter 2. Let $\mathbb{Z}_n^* = \langle g \rangle$ and let $x \in \mathbb{Z}_n$. The result holds if $p \mid x$, so let us assume that $x \in \mathbb{Z}_n^*$. Let x^{-1} denote the multiplicative inverse of x in $\mathbb{Z}_n^*$. Then by the binomial theorem,

$$(1 + px^{-1})^{\frac{\phi(n)}{4}} = \sum_{i=0}^{\frac{\phi(n)}{4}} \binom{\frac{\phi(n)}{4}}{i} (px^{-1})^i. \tag{8.2}$$

Now, we show that

$$p^\alpha \mid \binom{\frac{\phi(n)}{4}}{i} (px^{-1})^i \text{ for } i = 1, \ldots, \frac{\phi(n)}{4}. \tag{8.3}$$

For $\alpha \leq i \leq \frac{\phi(n)}{4}$, (8.3) is evident. So, we assume that $1 \leq i \leq \alpha - 1$. To this end, we observe that

$$\binom{\frac{\phi(n)}{4}}{i} = \frac{\frac{\phi(n)}{4}\left(\frac{\phi(n)}{4} - 1\right) \cdots \left(\frac{\phi(n)}{4} - i + 1\right)}{i!}$$

where $\frac{\phi(n)}{4} = p^{\alpha - i} p^{i-1} \left(\frac{p-1}{4}\right)$, therefore to show (8.3) it is sufficient to show that p^i does not divide $i!$. Let $\sigma_p(i)$ be the sum of digits of the base-p representation of i. Recalling Definition 2.6, we have by Lemma 2.7, $v_p(i!) = \sum_{k=1}^{\infty} \lfloor \frac{i}{p^k} \rfloor$, from which it can be deduced that $v_p(i!) = \frac{i - \sigma_p(i)}{p-1}$. If p^i divides $i!$ then $v_p(i) \geq i$, that is, $\frac{i - v_p(i)}{p-1} \geq i$, which is not possible. This proves (8.3). Thus, (8.2) yields $(1 + px^{-1})^{\frac{\phi(n)}{4}} \equiv 1 \pmod{p^\alpha}$. So, if $1 + px^{-1} = g^t$ in $\mathbb{Z}_n^*$ for some $t \in \mathbb{Z}$, then $1 = (1 + px^{-1})^{\frac{\phi(n)}{4}} = g^{\frac{t\phi(n)}{4}}$, which implies that $\phi(n) \mid \frac{t\phi(n)}{4}$, which gives $4 \mid t$ and hence, $1 + px^{-1} \in \langle g^4 \rangle$. This means that $\chi_4(1 + px^{-1}) = 1$, that is, $\chi_4(x + p) = \chi_4(x)$, completing the proof of the lemma. ■

8.4.1 Proof of Theorem 8.4

In this subsection, we prove Theorem 8.4. Note that we use Notation 1.57.

Proof of Theorem 8.4. Let $\mathcal{K}_3(G^*(p^\alpha), 0)$ denote the number of triangles in $G^*(p^\alpha)$ containing the vertex 0. Since $G^*(p^\alpha)$ is vertex-transitive, so

$$\mathcal{K}_3(G^*(p^\alpha)) = \frac{p^\alpha}{3} \times \mathcal{K}_3(G^*(p^\alpha), 0). \tag{8.4}$$

Recall that $\mathbb{Z}_{p^\alpha}^* = \langle g \rangle$ and $h = 1 - \chi_4(g)$. Now, using (8.1) we have

$$\mathcal{K}_3(G^*(p^\alpha), 0) = \frac{1}{2} \sum_{x \in \mathbb{Z}_{p^\alpha}^*} \sum_{y, x-y \in \mathbb{Z}_{p^\alpha}^*} \left[\frac{2 + h\chi_4(x) + \overline{h}\overline{\chi_4}(x)}{4} \times \frac{2 + h\chi_4(y) + \overline{h}\overline{\chi_4}(y)}{4} \right.$$
$$\left. \times \frac{2 + h\chi_4(x-y) + \overline{h}\overline{\chi_4}(x-y)}{4} \right]. \tag{8.5}$$

We shall use the fact that $\chi_4(-1) = 1$ since $-1 \in \langle g^4 \rangle$. We also make use of Theorem 1.19 as needed. Firstly, we evaluate the sum in (8.5) indexed by y. We have

$$\sum_{y, x-y \in \mathbb{Z}_{p^\alpha}^*} [2 + h\chi_4(y) + \overline{h}\overline{\chi_4}(y)][2 + h\chi_4(x-y) + \overline{h}\overline{\chi_4}(x-y)]$$
$$= \sum_{y, x-y \in \mathbb{Z}_{p^\alpha}^*} [4 + 2h\chi_4(y) + 2\overline{h}\overline{\chi_4}(y) + 2h\chi_4(x-y) + 2\overline{h}\overline{\chi_4}(x-y) + h^2\chi_4(y(x-y))$$
$$+ |h|^2\chi_4(y)\overline{\chi_4}(x-y) + |h|^2\overline{\chi_4}(y)\chi_4(x-y) + \overline{h}^2\overline{\chi_4}(y(x-y))]. \tag{8.6}$$

Using Lemma 8.6, we find that

$$\sum_{y, x-y \in \mathbb{Z}_{p^\alpha}^*} \chi_4(x-y) = \sum_{x-y \in \mathbb{Z}_{p^\alpha}^*} \chi_4(x-y) - \sum_{\substack{x-y \in \mathbb{Z}_{p^\alpha}^* \\ p \mid y}} \chi_4(x-y)$$
$$= -\sum_{t=0}^{p^{\alpha-1}-1} \chi_4(x-pt) = -\sum_{t=0}^{p^{\alpha-1}-1} \chi_4(x) = -p^{\alpha-1}\chi_4(x), \tag{8.7}$$

and similarly

$$\sum_{y, x-y \in \mathbb{Z}_{p^\alpha}^*} \chi_4(y) = -p^{\alpha-1}\chi_4(x). \tag{8.8}$$

Using the substitution $y \mapsto xy$ in the following sum, we have

$$\sum_{y,x-y\in\mathbb{Z}_{p^\alpha}^*} \chi_4(y(x-y)) = \sum_{y\in\mathbb{Z}_{p^\alpha}} \chi_4(y(x-y)) = \varphi(x)J(\chi_4,\chi_4). \tag{8.9}$$

Also, we find that

$$\sum_{y,x-y\in\mathbb{Z}_{p^\alpha}^*} \chi_4(y)\overline{\chi_4}(x-y) = \sum_{p\nmid y} \overline{\chi_4}\left(xy^{-1}-1\right), \tag{8.10}$$

where y^{-1} denotes the multipicative inverse of y in $\mathbb{Z}_n^*$. The following map

$$\{y \in \mathbb{Z}_{p^\alpha} : p \nmid y, x-y\} \to \{z \in \mathbb{Z}_{p^\alpha} : p \nmid z, z+1\}$$
$$y \mapsto xy^{-1} - 1$$

is a bijection, and hence, (8.10) yields

$$\sum_{y,x-y\in\mathbb{Z}_{p^\alpha}^*} \chi_4(y)\overline{\chi_4}(x-y) = \sum_{p\nmid z+1} \overline{\chi_4}(z) = -\sum_{p\mid z+1} \overline{\chi_4}(z) = -p^{\alpha-1}. \tag{8.11}$$

Lastly, we have

$$\sum_{y,x-y\in\mathbb{Z}_{p^\alpha}^*} 1 = \sum_{p\nmid y} 1 - \sum_{\substack{p\nmid y \\ p\mid x-y}} 1 = p^{\alpha-1}(p-2). \tag{8.12}$$

Employing (8.7) - (8.12) in (8.6), and then combining with (8.5) we find that

$$\mathcal{K}_3(G^*(p^\alpha),0) = \frac{1}{2^7}\sum_{p\nmid x}[2+h\chi_4(x)+\overline{h}\overline{\chi_4}(x)][A-B\chi_4(x)-\overline{B}\overline{\chi_4}(x)+C\varphi(x)], \tag{8.13}$$

where

$$A = 4(p-3)p^{\alpha-1},$$
$$B = 4hp^{\alpha-1}, \text{ and}$$
$$C = h^2 \cdot J(\chi_4, \chi_4) + \overline{h}^2 \cdot \overline{J(\chi_4, \chi_4)}.$$

After expanding the expression inside the sum over x and proceeding similarly as shown above, (8.13) yields

$$\mathcal{K}_3(G^*(p^\alpha), 0) = \frac{1}{2^7}[2A - \overline{B}h - B\overline{h}]\phi(p^\alpha) = \frac{1}{2^4}p^{2\alpha-2}(p-1)(p-5). \tag{8.14}$$

Finally, combining (8.14) and (8.4), we obtain the required result. ■

8.4.2 Proof of Theorem 8.5

Before proceeding with the proof of the theorem, we evaluate some character sums which we come across in the proof of Theorem 8.5. The following three lemmas are analogues of Lemmas 6.5 to 6.9 in Chapter 6.

Lemma 8.7. *For a prime $p \equiv 1 \pmod 8$ and an integer $\alpha \geq 1$, let χ_4 be a Dirichlet character mod p^α of order 4 and let φ be the quadratic character mod p^α. Let $x \in \mathbb{Z}_{p^\alpha}^*$ be such that $p \nmid 1-x$. Let $\rho := J(\chi_4, \chi_4)$. Then, we have*

$$\sum_{\substack{y \in \mathbb{Z}_{p^\alpha}^* \\ p \nmid 1-y, x-y}} \chi_4^{i_1}(x-y)\chi_4^{i_2}(1-y)\chi_4^{i_3}(y)$$

$$= \begin{cases} p^{\alpha-1}(p-3), & \text{if } (i_1,i_2,i_3) = (0,0,0); \\ -p^{\alpha-1}(1+\chi_4(x)), & \text{if } (i_1,i_2,i_3) = (0,0,1); \\ -p^{\alpha-1}(1+\chi_4(1-x)), & \text{if } (i_1,i_2,i_3) = (0,1,0); \\ -p^{\alpha-1}(\chi_4(1-x)+\chi_4(x)), & \text{if } (i_1,i_2,i_3) = (1,0,0); \\ \rho - p^{\alpha-1}\chi_4(1-x)\chi_4(x), & \text{if } (i_1,i_2,i_3) = (0,1,1); \\ \varphi(x)\rho - p^{\alpha-1}\chi_4(1-x), & \text{if } (i_1,i_2,i_3) = (1,0,1); \\ \varphi(x-1)\rho - p^{\alpha-1}\chi_4(x), & \text{if } (i_1,i_2,i_3) = (1,1,0); \\ -p^{\alpha-1}(1+\overline{\chi_4}(1-x)\chi_4(x)), & \text{if } (i_1,i_2,i_3) = (0,-1,1); \\ -p^{\alpha-1}(1+\overline{\chi_4}(1-x)), & \text{if } (i_1,i_2,i_3) = (-1,0,1); \\ -p^{\alpha-1}(1+\overline{\chi_4}(x)), & \text{if } (i_1,i_2,i_3) = (-1,1,0). \end{cases}$$

Proof. The proofs are straightforward, and we give one such instance. Let $(i_1,i_2,i_3) = (0,-1,1)$. Since χ_4 is of period p, we have

$$\sum_{\substack{y\in\mathbb{Z}_{p^\alpha}^* \\ p\nmid 1-y, x-y}} \chi_4(y)\overline{\chi_4}(1-y) = \sum_{p\nmid y,1-y} \chi_4(y)\overline{\chi_4}(1-y) - p^{\alpha-1}\chi_4(x)\overline{\chi_4}(1-x). \tag{8.15}$$

Now, the following map

$$\{y \in \mathbb{Z}_{p^\alpha} : p \nmid y, y-1\} \to \{z \in \mathbb{Z}_{p^\alpha} : p \nmid z, 1+z\}$$
$$y \mapsto y(1-y)^{-1}$$

is a bijection. Hence,

$$\sum_{p\nmid y,1-y} \chi_4(y)\overline{\chi_4}(1-y) = -p^{\alpha-1}. \tag{8.16}$$

Combining (8.15) and (8.16), we complete the proof of the lemma when $(i_1,i_2,i_3) = (0,-1,1)$. ∎

The proofs of the following two lemmas are similar to that of Lemma 8.7 and

involve the same techniques, so we state them without proofs.

Lemma 8.8. *Let $p \equiv 1 \pmod 8$ be a prime and let $\alpha \geq 1$ be an integer. Let χ_4 be a Dirichlet character mod p^α of order 4 and let φ be the quadratic character mod p^α. Let $\xi := J(\chi_4, \varphi)$. Then, we have*

$$\sum_{p\nmid x,1-x} \sum_{p\nmid y,1-y,x-y} \chi_4^{i_1}(y)\chi_4^{i_2}(1-y)\chi_4^{i_3}(x-y)$$
$$= \begin{cases} -2\xi p^{\alpha-1}, & \text{if } (i_1,i_2,i_3) = (1,1,1); \\ 2p^{2\alpha-2}, & \text{if } (i_1,i_2,i_3) = (1,1,-1); \\ -p^{\alpha-1}(\overline{\xi} - p^{\alpha-1}), & \text{if } (i_1,i_2,i_3) = (1,-1,1); \\ -p^{\alpha-1}(\xi - p^{\alpha-1}), & \text{if } (i_1,i_2,i_3) = (1,-1,-1). \end{cases}$$

Lemma 8.9. *Let $p \equiv 1 \pmod 8$ be a prime and let $\alpha \geq 1$ be an integer. Let χ_4 be a Dirichlet character mod p^α of order 4 and let φ be the quadratic character mod p^α. Let $\rho := J(\chi_4, \chi_4)$, $\xi := J(\chi_4, \varphi)$, $S_1 := -p^{\alpha-1}(\rho + \xi)$, $S_2 := -p^{\alpha-1}\rho + p^{2\alpha-2}$, $S_3 := |\rho|^2 + p^{2\alpha-2}, S_4 := p^{2\alpha-2} - p^{\alpha-1}\xi, S_5 := \rho^2 - p^{\alpha-1}\overline{\xi}$ and $S_6 := 2p^{2\alpha-2}$. Then, for $i_1, i_2, i_3 \in \{\pm 1\}$, we have the following tabulation of the values of the expression given below:*

$$\sum_{\substack{x,y\in\mathbb{Z}_{p^\alpha}, \\ p\nmid x,1-x}} A_x \cdot \chi_4^{i_1}(y)\chi_4^{i_2}(1-y)\chi_4^{i_3}(x-y). \tag{8.17}$$

For $w \in \{1, \ldots, 8\}$ and $z \in \{1, 2, \ldots, 7\}$, the (w, z)-th entry in the table corresponds to (8.17), where A_x is either $\chi_4(x), \overline{\chi_4}(x), \chi_4(1-x)$ or $\overline{\chi_4}(1-x)$ and the tuple

(i_1, i_2, i_3) *depends on* w.

			A_x			
i_1	i_2	i_3	$\chi_4(x)$	$\overline{\chi_4}(x)$	$\chi_4(1-x)$	$\overline{\chi_4}(1-x)$
1	1	1	S_1	S_1	S_1	S_1
1	1	−1	S_2	$\overline{S_2}$	S_2	$\overline{S_2}$
1	−1	1	S_3	S_6	S_5	$\overline{S_4}$
1	−1	−1	S_4	$\overline{S_5}$	S_6	S_3
−1	1	1	S_5	$\overline{S_4}$	S_3	S_6
−1	1	−1	S_6	S_3	S_4	$\overline{S_5}$
−1	−1	1	S_2	$\overline{S_2}$	S_2	$\overline{S_2}$
−1	−1	−1	$\overline{S_1}$	$\overline{S_1}$	$\overline{S_1}$	$\overline{S_1}$

For example, the $(3, 6)$*-th position contains the value* $S_5 = \rho^2 - p^{\alpha-1}\overline{\xi}$. *Here* $w = 3$ *corresponds to* $i_1 = 1, i_2 = -1, i_3 = 1$*;* $z = 6$ *corresponds to the column* $A_x = \chi_4(1-x)$.

In Chapter 6, we used Lemma 6.11 (due to [21]) therein, in the proof of finding cliques of order 4 in the Peisert graph. The purpose was to have a group action, which ultimately concluded that certain hypergeometric functions (over finite fields) would yield the same value. Here, we do the same but for hypergeometric functions with Dirichlet characters as arguments. The lemmas listed in Section 7.3 in Chapter 7 allow us to do so. The following lemma looks essentially the same as Lemma 6.11 in Chapter 6, except that the hypergeometric functions here involve the Dirichlet characters modulo p^α.

Lemma 8.10. *Let* $X = \{(t_1, t_2, t_3, t_4, t_5) \in \mathbb{Z}_4^5 : t_1, t_2, t_3 \neq 0, t_4, t_5;\ t_1 + t_2 + t_3 \neq t_4, t_5\}$. *Define the functions* $f_i : X \to X,\ i \in \{1, 2, \ldots, 7\}$ *in the following manner:*

$$f_1(t_1, t_2, t_3, t_4, t_5) = (t_2 - t_4, t_1 - t_4, t_3 - t_4, -t_4, t_5 - t_4),$$

$$f_2(t_1,t_2,t_3,t_4,t_5) = (t_1, t_1-t_4, t_1-t_5, t_1-t_2, t_1-t_3),$$
$$f_3(t_1,t_2,t_3,t_4,t_5) = (t_2-t_4, t_2, t_2-t_5, t_2-t_1, t_2-t_3),$$
$$f_4(t_1,t_2,t_3,t_4,t_5) = (t_1, t_2, t_5-t_3, t_1+t_2-t_4, t_5),$$
$$f_5(t_1,t_2,t_3,t_4,t_5) = (t_1, t_4-t_2, t_3, t_4, t_1+t_3-t_5),$$
$$f_6(t_1,t_2,t_3,t_4,t_5) = (t_4-t_1, t_2, t_3, t_4, t_2+t_3-t_5),$$
$$f_7(t_1,t_2,t_3,t_4,t_5) = (t_4-t_1, t_4-t_2, t_3, t_4, t_4+t_5-t_1-t_2).$$

Then the group generated by $f_1,\ldots,f_7$, with operation composition of functions, is the set

$$\mathcal{F} = \{f_0, f_i, f_j\circ f_l, f_4\circ f_1, f_6\circ f_2, f_5\circ f_3, f_1\circ f_4\circ f_1 : 1\le i\le 7,\ 1\le j\le 3,\ 4\le l\le 7\},$$

where f_0 is the identity map. Moreover, the group $\mathcal{F}$ acts on the set X, and X contains eleven orbits with representatives $(1,1,1,0,0)$, $(3,3,3,0,0)$, $(1,3,3,2,0)$, $(3,1,1,2,0)$, $(2,1,3,0,0)$, $(1,3,2,0,0)$, $(2,3,1,0,0)$, $(1,2,2,0,0)$, $(2,2,1,0,0)$, $(1,1,3,0,0)$ and $(2,2,2,0,0)$.

Now, let $p\equiv 1 \pmod 8$ be a prime and α be a positive integer. Let χ_4 be a Dirichlet character mod p^α of order 4. If we associate the 5-tuple $(t_1,t_2,\ldots,t_5)\in X$ to the hypergeometric function ${}_3F_2\left(\begin{matrix}\chi_4^{t_1}, & \chi_4^{t_2}, & \chi_4^{t_3}\\ & \chi_4^{t_4}, & \chi_4^{t_5}\end{matrix}\middle|1\right)$, then each orbit of the group action consists of a number of 5-tuples $(t_1,t_2,\ldots,t_5)$, and the corresponding ${}_3F_2$ terms have the same value.

Proof. As observed in Lemma 6.11, $\mathcal{F}$ acts on X. Now, for each of the Lemmas 7.8 to 7.14, we associate the maps f_1 to f_7. For example, the transformation in Lemma 7.8 gives that

$${}_3F_2\left(\begin{matrix}\chi_4^{t_1}, & \chi_4^{t_2}, & \chi_4^{t_3}\\ & \chi_4^{t_4}, & \chi_4^{t_5}\end{matrix}\middle|1\right) = {}_3F_2\left(\begin{matrix}\chi_4^{t_2-t_4}, & \chi_4^{t_1-t_4}, & \chi_4^{t_3-t_4}\\ & \chi_4^{-t_4}, & \chi_4^{t_5-t_4}\end{matrix}\middle|1\right),$$

and hence, it induces the map $f_1 : X \to X$ given by

$$f_1(t_1, t_2, t_3, t_4, t_5) = (t_2 - t_4, t_1 - t_4, t_3 - t_4, -t_4, t_5 - t_4).$$

Similarly, the other transformations in Lemmas 7.9 to 7.14 correspond to the maps f_2 to f_7. Due to the equality of the ${}_3F_2(\cdot)$ hypergeometric functions in these lemmas and the fact that $\mathcal{F}$ acts on X, the value of ${}_3F_2(\cdot)$ is constant in each orbit. ■

We are now ready to prove Theorem 8.5. We recall that $\mathbb{Z}_{p^\alpha}^* = \langle g \rangle$, χ_4 is a fixed character of order 4 and $h = 1 - \chi_4(g)$. Since $-1 \in \langle g^4 \rangle$, we have $\chi_4(-1) = 1$. Let $H = \langle g^4 \rangle \cup g\langle g^4 \rangle$. We make use of Theorem 1.19 as needed. Note that we use Notation 1.57.

Proof of Theorem 8.5. Since $G^*(p^\alpha)$ is vertex-transitive, we find that

$$\begin{aligned} \mathcal{K}_4(G^*(p^\alpha)) &= \frac{p^\alpha}{4} \times \text{ number of cliques of order 4 in } G^*(p^\alpha) \text{ containing } 0 \\ &= \frac{p^\alpha}{4} \times \mathcal{K}_3(\langle H \rangle). \end{aligned} \tag{8.18}$$

So, our task is to find $\mathcal{K}_3(\langle H \rangle)$. We proceed as in the proof of Theorem 6.3 in Chapter 6. Let $a, b \in H$ be such that $\chi_4(ab^{-1}) = 1$. We note that

$$\mathcal{K}_3(\langle H \rangle, a) = \frac{1}{2} \times \sum \sum_{\chi_4(x-y) \in \{1, \chi_4(g)\}} 1, \tag{8.19}$$

where the first sum is taken over all x such that $\chi_4(x), \chi_4(a-x) \in \{1, \chi_4(g)\}$ and the second sum is taken over all y such that $p \nmid y - x$ and $\chi_4(y), \chi_4(a-y) \in \{1, \chi_4(g)\}$. Hence, using (8.1) in (8.19), we find that

$$\begin{aligned} &\mathcal{K}_3(\langle H \rangle, a) \\ &= \frac{1}{2 \times 4^5} \sum_{p \nmid x, x-a} \sum_{p \nmid y, y-a, x-y} [(2 + h\chi_4(a-x) + \overline{h}\overline{\chi_4}(a-x)) \end{aligned}$$

$$\times (2 + h\chi_4(a-y) + \overline{h}\overline{\chi_4}(a-y))(2 + h\chi_4(x-y) + \overline{h}\overline{\chi_4}(x-y))$$
$$\times (2 + h\chi_4(x) + \overline{h}\overline{\chi_4}(x))(2 + h\chi_4(y) + \overline{h}\overline{\chi_4}(y))]. \tag{8.20}$$

Now,

$$\{y \in \mathbb{Z}_{p^\alpha} : p \nmid y, y-a, x-y\} \to \{Y \in \mathbb{Z}_{p^\alpha} : p \nmid Y, b-Y, Y-ba^{-1}x\}$$
$$y \mapsto ba^{-1}y$$

is a bijection. Therefore, using the substitution $y \mapsto ba^{-1}y$ in the inner sum in (8.20) indexed by y yields

$$\begin{aligned}
&\mathcal{K}_3(\langle H\rangle, a)\\
&= \frac{1}{2\times 4^5} \sum_{p\nmid x, x-a} \sum_{p\nmid Y, b-Y, Y-ba^{-1}x} [(2 + h\chi_4(a-x) + \overline{h}\overline{\chi_4}(a-x))\\
&\times (2 + h\chi_4(b-Y) + \overline{h}\overline{\chi_4}(b-Y))(2 + h\chi_4(x-ab^{-1}Y) + \overline{h}\overline{\chi_4}(x-ab^{-1}Y))\\
&\times (2 + h\chi_4(x) + \overline{h}\overline{\chi_4}(x))(2 + h\chi_4(Y) + \overline{h}\overline{\chi_4}(Y))]\\
&= \frac{1}{2\times 4^5} \sum_{p\nmid Y, b-Y} \sum_{p\nmid x, x-a, x-ab^{-1}Y} [(2 + h\chi_4(a-x) + \overline{h}\overline{\chi_4}(a-x)\\
&\times (2 + h\chi_4(b-Y) + \overline{h}\overline{\chi_4}(b-Y))(2 + h\chi_4(x-ab^{-1}Y) + \overline{h}\overline{\chi_4}(x-ab^{-1}Y))\\
&\times (2 + h\chi_4(x) + \overline{h}\overline{\chi_4}(x))(2 + h\chi_4(Y) + \overline{h}\overline{\chi_4}(Y))].
\end{aligned} \tag{8.21}$$

Again, we find that

$$\{x \in \mathbb{Z}_{p^\alpha} : p \nmid x, x-a, x-ab^{-1}y\} \to \{X \in \mathbb{Z}_{p^\alpha} : p \nmid X, X-b, X-Y\}$$
$$x \mapsto ba^{-1}x$$

is a bijection, and hence, employing the substitution $x \mapsto ba^{-1}x$ in the inner sum in

(8.21) indexed by x yields

$$\begin{aligned}
&\mathcal{K}_3(\langle H\rangle, a)\\
&= \frac{1}{2\times 4^5}\sum_{\substack{p\nmid Y,\\ Y-b}}\sum_{\substack{p\nmid X, X-b,\\ X-Y}}[(2+h\chi_4(X-b)+\overline{h}\overline{\chi_4}(X-b))\\
&\times(2+h\chi_4(Y-b)+\overline{h}\overline{\chi_4}(Y-b))(2+h\chi_4(X-Y)+\overline{h}\overline{\chi_4}(X-Y))\\
&\times(2+h\chi_4(X)+\overline{h}\overline{\chi_4}(X))(2+h\chi_4(Y)+\overline{h}\overline{\chi_4}(Y))]\\
&= \mathcal{K}_3(\langle H\rangle, b).
\end{aligned}$$

Thus, if $a, b \in H$ are such that $\chi_4(ab^{-1}) = 1$, then

$$\mathcal{K}_3(\langle H\rangle, a) = \mathcal{K}_3(\langle H\rangle, b). \tag{8.22}$$

Let $\langle g^4\rangle = \{x_1, \ldots, x_{p^{\alpha-1}\left(\frac{p-1}{4}\right)}\}$ with $x_1 = 1$ and $g\langle g^4\rangle = \{y_1, \ldots, y_{p^{\alpha-1}\left(\frac{p-1}{4}\right)}\}$ with $y_1 = g$. Then,

$$\sum_{i=1}^{p^{\alpha-1}\left(\frac{p-1}{4}\right)} \mathcal{K}_3(\langle H\rangle, x_i) + \sum_{i=1}^{p^{\alpha-1}\left(\frac{p-1}{4}\right)} \mathcal{K}_3(\langle H\rangle, y_i) = 3\times\mathcal{K}_3(\langle H\rangle). \tag{8.23}$$

By (8.22), we have

$$\mathcal{K}_3(\langle H\rangle, x_1) = \mathcal{K}_3(\langle H\rangle, x_2) = \cdots = \mathcal{K}_3(\langle H\rangle, x_{p^{\alpha-1}\left(\frac{p-1}{4}\right)})$$

and

$$\mathcal{K}_3(\langle H\rangle, y_1) = \mathcal{K}_3(\langle H\rangle, y_2) = \cdots = \mathcal{K}_3(\langle H\rangle, y_{p^{\alpha-1}\left(\frac{p-1}{4}\right)}).$$

Hence, (8.23) yields

$$\mathcal{K}_3(\langle H\rangle) = \frac{p^{\alpha-1}(p-1)}{12}[\mathcal{K}_3(\langle H\rangle, 1) + \mathcal{K}_3(\langle H\rangle, g)]. \tag{8.24}$$

Thus, we need to find only $\mathcal{K}_3(\langle H\rangle, 1)$ and $\mathcal{K}_3(\langle H\rangle, g)$. We first find $\mathcal{K}_3(\langle H\rangle, 1)$.

Employing (8.1), we have

$$\begin{aligned}
&\mathcal{K}_3(\langle H\rangle, 1)\\
&= \frac{1}{2\times 4^5}\sum_{\substack{p\nmid x,\\ 1-x}}[(2+h\chi_4(1-x)+\overline{h}\overline{\chi_4}(1-x))(2+h\chi_4(x)+\overline{h}\overline{\chi_4}(x))]\\
&\qquad \sum_{\substack{p\nmid y,1-y,\\ x-y}}[(2+h\chi_4(1-y)+\overline{h}\overline{\chi_4}(1-y))(2+h\chi_4(x-y)+\overline{h}\overline{\chi_4}(x-y))\\
&\qquad\qquad \times(2+h\chi_4(y)+\overline{h}\overline{\chi_4}(y))]. \qquad (8.25)
\end{aligned}$$

Let $i_1, i_2, i_3 \in \{\pm 1\}$ and let F_{i_1,i_2,i_3} denote the term $\chi_4^{i_1}(y)\chi_4^{i_2}(1-y)\chi_4^{i_3}(x-y)$. Next, we expand and evaluate the inner summation in (8.25). We have

$$\begin{aligned}
&\sum_{\substack{p\nmid y,1-y,\\ x-y}}[2+h\chi_4(y)+\overline{h}\overline{\chi_4}(y)][2+h\chi_4(1-y)+\overline{h}\overline{\chi_4}(1-y)][2+h\chi_4(x-y)+\overline{h}\overline{\chi_4}(x-y)]\\
&= \sum_{\substack{p\nmid y,1-y,\\ x-y}}[8+4h\chi_4(y)+4\overline{h}\overline{\chi_4}(y)+4h\chi_4(1-y)+4\overline{h}\overline{\chi_4}(1-y)+4h\chi_4(x-y)\\
&+4\overline{h}\overline{\chi_4}(x-y)+4\chi_4(y)\overline{\chi_4}(1-y)+4\overline{\chi_4}(y)\chi_4(1-y)+4\chi_4(y)\overline{\chi_4}(x-y)\\
&+4\overline{\chi_4}(y)\chi_4(x-y)+4\chi_4(1-y)\overline{\chi_4}(x-y)+4\overline{\chi_4}(1-y)\chi_4(x-y)\\
&+2h^2\chi_4(y)\chi_4(1-y)+2\overline{h}^2\overline{\chi_4}(y)\overline{\chi_4}(1-y)+2h^2\chi_4(y)\chi_4(x-y)\\
&+2\overline{h}^2\overline{\chi_4}(y)\overline{\chi_4}(x-y)+2h^2\chi_4(1-y)\chi_4(x-y)+2\overline{h}^2\overline{\chi_4}(1-y)\overline{\chi_4}(x-y)\\
&+h^3F_{1,1,1}+2hF_{1,1,-1}+2hF_{1,-1,1}+2\overline{h}F_{1,-1,-1}+2hF_{-1,1,1}+2\overline{h}F_{-1,1,-1}\\
&+2\overline{h}F_{-1,-1,1}+\overline{h}^3F_{-1,-1,-1}]. \qquad (8.26)
\end{aligned}$$

Now, referring to Lemma 8.7, (8.26) yields

$$\sum_{\substack{p\nmid y,1-y,\\ x-y}}[2+h\chi_4(y)+\overline{h}\overline{\chi_4}(y)][2+h\chi_4(1-y)+\overline{h}\overline{\chi_4}(1-y)][2+h\chi_4(x-y)+\overline{h}\overline{\chi_4}(x-y)]$$

$$
\begin{aligned}
&= A + B\chi_4(x) + \overline{B}\overline{\chi_4}(x) + B\chi_4(x-1) + \overline{B}\overline{\chi_4}(x-1) - 4p^{\alpha-1}\chi_4(x)\overline{\chi_4}(x-1)\\
&- 4p^{\alpha-1}\overline{\chi_4}(x)\chi_4(x-1) - 2h^2p^{\alpha-1}\chi_4(x)\chi_4(x-1) - 2\overline{h}^2p^{\alpha-1}\overline{\chi_4}(x)\overline{\chi_4}(x-1) + C\varphi(x)\\
&+ C\varphi(x-1)\\
&+ \sum_{\substack{p\nmid y,1-y,\\ x-y}} [h^3F_{1,1,1} + 2hF_{1,1,-1} + 2hF_{1,-1,1} + 2\overline{h}F_{1,-1,-1} + 2hF_{-1,1,1}\\
&+ 2\overline{h}F_{-1,1,-1} + 2\overline{h}F_{-1,-1,1} + \overline{h}^3F_{-1,-1,-1}]\\
&=: \mathcal{I}, \qquad (8.27)
\end{aligned}
$$

where $A := 8p^{\alpha-1}(p-8) + 4\,\mathrm{Re}(h^2\rho)$, $B := -12hp^{\alpha-1}$ and $C := 4\,\mathrm{Re}(h^2\rho)$.

Next, we introduce some notation. Let

$$
\begin{aligned}
A_1 &:= 32(p-15)p^{\alpha-1} + 16\,\mathrm{Re}(h^2\rho),\\
B_1 &:= 16(p-15)hp^{\alpha-1} + 16\,\mathrm{Re}(h^2\rho),\\
C_1 &:= 16\,\mathrm{Re}(h^2\rho),\\
D_1 &:= 8h\,\mathrm{Re}(h^2\rho),\\
E_1 &:= 8(p-15)h^2p^{\alpha-1} + (4h^2+16)\mathrm{Re}(h^2\rho), \text{ and}\\
F_1 &:= 16(p-15)p^{\alpha-1} + 8\,\mathrm{Re}(h^2\rho).
\end{aligned}
$$

For $i \in \{1,2,3,4\}$ and $j \in \{1,2,\ldots,8\}$, we define the following character sums.

$$
\begin{aligned}
T_j &:= \sum_{p\nmid x,1-x}\sum_{y}\chi_4^{i_1}(y)\chi_4^{i_2}(1-y)\chi_4^{i_3}(x-y),\\
U_{ij} &:= \sum_{p\nmid x,1-x}\chi_4^{l}(m)\sum_{y}\chi_4^{i_1}(y)\chi_4^{i_2}(1-y)\chi_4^{i_3}(x-y),\\
V_{ij} &:= \sum_{x}\chi_4^{l_1}(x)\chi_4^{l_2}(1-x)\sum_{y}\chi_4^{i_1}(y)\chi_4^{i_2}(1-y)\chi_4^{i_3}(x-y),
\end{aligned}
$$

where

$$l = \begin{cases} 1, & \text{if } i \text{ is odd,} \\ -1, & \text{otherwise;} \end{cases}$$

$$m = \begin{cases} x, & \text{if } i \in \{1, 2\}, \\ 1 - x, & \text{otherwise;} \end{cases}$$

and

$$(l_1, l_2) = \begin{cases} (1, 1), & \text{if } i = 1, \\ (1, -1), & \text{if } i = 2, \\ (-1, 1), & \text{if } i = 3, \\ (-1, -1), & \text{if } i = 4. \end{cases}$$

Also, corresponding to each j, let (i_1, i_2, i_3) take the value according to the following:

$$(i_1, i_2, i_3) = \begin{cases} (1, 1, 1), & \text{if } j = 1, \\ (1, 1, -1), & \text{if } j = 2, \\ (1, -1, 1), & \text{if } j = 3, \\ (1, -1, -1), & \text{if } j = 4, \\ (-1, 1, 1), & \text{if } j = 5, \\ (-1, 1, -1), & \text{if } j = 6, \\ (-1, -1, 1), & \text{if } j = 7, \\ (-1, -1, -1), & \text{if } j = 8. \end{cases}$$

Then, using (8.27) and the notation we just described, (8.25) yields

$$\mathcal{K}_3(\langle H \rangle, 1) = \frac{1}{2^{11}} \sum_{p \nmid x, 1-x} [(2 + h\chi_4(x) + \overline{h}\overline{\chi_4}(x))(2 + h\chi_4(1 - x) + \overline{h}\overline{\chi_4}(1 - x)) \times \mathcal{I}]$$

$$
\begin{aligned}
=&\frac{1}{2^{11}}\sum_{p\nmid x,1-x}(A_1+B_1\chi_4(x)+\overline{B_1}\overline{\chi_4}(x)+B_1\chi_4(x-1)+\overline{B_1}\overline{\chi_4}(x-1)\\
&+C_1\varphi(x)+C_1\varphi(x-1)+D_1\chi_4(x)\varphi(x-1)+\overline{D_1}\overline{\chi_4}(x)\varphi(x-1)\\
&+D_1\varphi(x)\chi_4(x-1)+\overline{D_1}\varphi(x)\overline{\chi_4}(x-1)+E_1\chi_4(x)\chi_4(x-1)+\overline{E_1}\overline{\chi_4}(x)\overline{\chi_4}(x-1)\\
&+F_1\chi_4(x)\overline{\chi_4}(1-x)+\overline{F_1}\overline{\chi_4}(x)\chi_4(x-1))\\
&+\frac{1}{2^{11}}(4h^3T_1+8hT_2+8hT_3+8\overline{h}T_4+8hT_5+8\overline{h}T_6+8\overline{h}T_7+4\overline{h}^3T_8\\
&+2h^4U_{11}+4h^2U_{12}+4h^2U_{13}+8U_{14}+4h^2U_{15}+8U_{16}+8U_{17}+4\overline{h}^2U_{18}\\
&+4h^2U_{21}+8U_{22}+8U_{23}+4\overline{h}^2U_{24}+8U_{25}+4\overline{h}^2U_{26}+4\overline{h}^2U_{27}+2\overline{h}^4U_{28}\\
&+2h^4U_{31}+4h^2U_{32}+4h^2U_{33}+8U_{34}+4h^2U_{35}+8U_{36}+8U_{37}+4\overline{h}^2U_{38}\\
&+4h^2U_{41}+8U_{42}+8U_{43}+4\overline{h}^2U_{44}+8U_{45}+4\overline{h}^2U_{46}+4\overline{h}^2U_{47}+2\overline{h}^4U_{48}\\
&+h^5V_{11}+2h^3V_{12}+2h^3V_{13}+4hV_{14}+2h^3V_{15}+4hV_{16}+4hV_{17}+4\overline{h}V_{18}\\
&+2h^3V_{21}+4hV_{22}+4hV_{23}+4\overline{h}V_{24}+4hV_{25}+4\overline{h}V_{26}+4\overline{h}V_{27}+2\overline{h}^3V_{28}\\
&+2h^3V_{31}+4hV_{32}+4hV_{33}+4\overline{h}V_{34}+4hV_{35}+4\overline{h}V_{36}+4\overline{h}V_{37}+2\overline{h}^3V_{38}\\
&+4hV_{41}+4\overline{h}V_{42}+4\overline{h}V_{43}+2\overline{h}^3V_{44}+4\overline{h}V_{45}+2\overline{h}^3V_{46}+2\overline{h}^3V_{47}+\overline{h}^5V_{48}).
\end{aligned}
$$

Employing Lemmas 8.8 and 8.9, we find that

$$
\begin{aligned}
\mathcal{K}_3(\langle H\rangle,1)=&\frac{1}{2^{11}}\left[16(p-9)p^{\alpha-1}\mathrm{Re}(h^2\rho)+32p^{2\alpha-2}(p^2-20p+81)\right.\\
&+2\mathrm{Re}\{\rho(8h^2(p-17)p^{\alpha-1}+4(h^2+4)\mathrm{Re}(h^2\rho))\}+32\mathrm{Re}(h^2\rho)\mathrm{Re}(\xi h)+16\mathrm{Re}(h^2\rho^2)\\
&+h^5V_{11}+2h^3V_{12}+2h^3V_{13}+4hV_{14}+2h^3V_{15}+4hV_{16}+4hV_{17}+4\overline{h}V_{18}\\
&+2h^3V_{21}+4hV_{22}+4hV_{23}+4\overline{h}V_{24}+4hV_{25}+4\overline{h}V_{26}+4\overline{h}V_{27}+2\overline{h}^3V_{28}\\
&+2h^3V_{31}+4hV_{32}+4hV_{33}+4\overline{h}V_{34}+4hV_{35}+4\overline{h}V_{36}+4\overline{h}V_{37}+2\overline{h}^3V_{38}\\
&\left.+4hV_{41}+4\overline{h}V_{42}+4\overline{h}V_{43}+2\overline{h}^3V_{44}+4\overline{h}V_{45}+2\overline{h}^3V_{46}+2\overline{h}^3V_{47}+\overline{h}^5V_{48}\right]. \qquad (8.28)
\end{aligned}
$$

Now, we convert each term of the form V_{ij} $[i\in\{1,2,3,4\},j\in\{1,2,\ldots,8\}]$ into its equivalent $p^{2\alpha}\cdot{}_3F_2$ form. We use the notation $(t_1,t_2,\ldots,t_5)\in\mathbb{Z}_4^5$ for the term

$p^{2\alpha}\cdot {}_3F_2\left(\begin{matrix}\chi_4^{t_1}, & \chi_4^{t_2}, & \chi_4^{t_3}\\ & \chi_4^{t_4}, & \chi_4^{t_5}\end{matrix}\Big|1\right)$. Then, (8.28) yields

$$\begin{aligned}\mathcal{K}_3(\langle H\rangle,1) &= \frac{1}{2^{11}}\big[16(p-9)p^{\alpha-1}\mathrm{Re}(h^2\rho)+32p^{2\alpha-2}(p^2-20p+81)\\ &+2\mathrm{Re}\{\rho(8h^2(p-17)p^{\alpha-1}+4(h^2+4)\mathrm{Re}(h^2\rho))\}+32\mathrm{Re}(h^2\rho)\mathrm{Re}(\xi h)+16\mathrm{Re}(h^2\rho^2)\\ &+h^5(3,1,1,2,2)+2h^3(1,1,3,2,0)+2h^3(3,1,1,0,2)+4h(1,1,3,0,0)\\ &+2h^3(3,3,1,0,2)+4h(1,3,3,0,0)+4h(3,3,1,2,2)+4\overline{h}(1,3,3,2,0)\\ &+2h^3(3,1,3,2,2)+4h(1,1,1,2,0)+4h(3,1,3,0,2)+4\overline{h}(1,1,1,0,0)\\ &+4h(3,3,3,0,2)+4\overline{h}(1,3,1,0,0)+4\overline{h}(3,3,3,2,2)+2\overline{h}^3(1,3,1,2,0)\\ &+2h^3(3,1,3,2,0)+4h(1,1,1,2,2)+4h(3,1,3,0,0)+4\overline{h}(1,1,1,0,2)\\ &+4h(3,3,3,0,0)+4\overline{h}(1,3,1,0,2)+4\overline{h}(3,3,3,2,0)+2\overline{h}^3(1,3,1,2,2)\\ &+4h(3,1,1,2,0)+4\overline{h}(1,1,3,2,2)+4\overline{h}(3,1,1,0,0)+2\overline{h}^3(1,1,3,0,2)\\ &+4\overline{h}(3,3,1,0,0)+2\overline{h}^3(1,3,3,0,2)+2\overline{h}^3(3,3,1,2,0)+\overline{h}^5(1,3,3,2,2)\big]. \end{aligned}\tag{8.29}$$

Next, we list the tuples $(t_1,t_2,\ldots,t_5)$ in each orbit of the group action of $\mathcal{F}$ on X, and then group the corresponding terms in (8.29) together (this is possible due to Lemma 8.10). The orbit representatives $(1,1,1,0,0)$, $(3,3,3,0,0)$, $(1,3,3,2,0)$, $(3,1,1,2,0)$ and $(1,1,3,0,0)$ mentioned in Lemma 8.10 are the ones whose orbits exhaust the hypergeometric terms in (8.29). We denote the $p^{2\alpha}\cdot {}_3F_2$ terms corresponding to these orbit representatives as $M_1,M_2,\ldots,M_5$, respectively. Then, (8.29) yields

$$\begin{aligned}\mathcal{K}_3(\langle H\rangle,1) &= \frac{1}{2^{11}}\big[16(p-9)p^{\alpha-1}\mathrm{Re}(h^2\rho)+32p^{2\alpha-2}(p^2-20p+81)\\ &+2\mathrm{Re}\{\rho(8h^2(p-17)p^{\alpha-1}+4(h^2+4)\mathrm{Re}(h^2\rho))\}+32\mathrm{Re}(h^2\rho)\mathrm{Re}(\xi h)+16\mathrm{Re}(h^2\rho^2)\\ &+h^5M_4+2h^3M_1+2h^3M_1+4hM_5+2h^3M_1+4hM_5+4hM_1+4\overline{h}M_3\\ &+2h^3M_4+4hM_5+4hM_2+4\overline{h}M_1+4hM_5+4\overline{h}M_5+4\overline{h}M_5+2\overline{h}^3M_3\\ &+2h^3M_4+4hM_5+4hM_5+4\overline{h}M_5+4hM_2+4\overline{h}M_1+4\overline{h}M_5+2\overline{h}^3M_3\end{aligned}$$

$$+ 4hM_4 + 4\overline{h}M_2 + 4\overline{h}M_5 + 2\overline{h}^3M_2 + 4\overline{h}M_5 + 2\overline{h}^3M_2 + 2\overline{h}^3M_2 + \overline{h}^5M_3\Big]. \tag{8.30}$$

Simplifying (8.30), we have the reduced expression of $\mathcal{K}_3(\langle H\rangle, 1)$ as follows.

$$\begin{aligned}\mathcal{K}_3(\langle H\rangle, 1) = \frac{1}{2^{11}}[&16(p-9)p^{\alpha-1}\mathrm{Re}(h^2\rho) + 32p^{2\alpha-2}(p^2-20p+81)\\ &+ 2\mathrm{Re}\{\rho(8h^2(p-17)p^{\alpha-1} + 4(h^2+4)\mathrm{Re}(h^2\rho))\} + 32\mathrm{Re}(h^2\rho)\mathrm{Re}(\xi h)\\ &+ 16\mathrm{Re}(h^2\rho^2) + 8(1-\overline{h})M_1 + 8(1-h)M_2 - 8hM_3 - 8\overline{h}M_4 + 48M_5].\end{aligned} \tag{8.31}$$

Returning back to (8.24), we are now left to calculate $\mathcal{K}_3(\langle H\rangle, g)$. Again, by employing (8.1), we have

$$\begin{aligned}&\mathcal{K}_3(\langle H\rangle, g)\\ &= \frac{1}{2^{11}}\sum_{\substack{p\nmid x,\\ g-x}}\sum_{\substack{p\nmid y, g-y,\\ x-y}}\big[(2+h\chi_4(g-x)+\overline{h}\overline{\chi_4}(g-x))(2+h\chi_4(g-y)+\overline{h}\overline{\chi_4}(g-y))\\ &\times(2+h\chi_4(x-y)+\overline{h}\overline{\chi_4}(x-y))(2+h\chi_4(x)+\overline{h}\overline{\chi_4}(x))(2+h\chi_4(y)+\overline{h}\overline{\chi_4}(y))\big].\end{aligned} \tag{8.32}$$

Using the substitutions $Y = yg^{-1}$ and $X = xg^{-1}$, and then using the fact that $h\chi_4(g) = \overline{h}$, (8.32) yields

$$\begin{aligned}&\mathcal{K}_3(\langle H\rangle, g)\\ &= \frac{1}{2^{11}}\sum_{\substack{p\nmid x,\\ 1-x}}\sum_{\substack{p\nmid y, 1-y,\\ x-y}}\big[(2+\overline{h}\chi_4(1-x)+h\overline{\chi_4}(1-x))(2+\overline{h}\chi_4(1-y)+h\overline{\chi_4}(1-y))\\ &\times(2+\overline{h}\chi_4(x-y)+h\overline{\chi_4}(x-y))(2+\overline{h}\chi_4(x)+h\overline{\chi_4}(x))(2+\overline{h}\chi_4(y)+h\overline{\chi_4}(y))\big].\end{aligned}$$

Cmparing this with (8.25), we see that the expansion of the expression inside this summation will consist of the same summation terms as in (8.25), except that the coefficient corresponding to each summation term in this case, will become the

complex conjugate of the corresponding coefficient of the same summation term that we obtain by expanding (8.25). So, we proceed to evaluate $\mathcal{K}_3(\langle H\rangle, g)$ in the same manner as we did for $\mathcal{K}_3(\langle H\rangle, 1)$ and find that for the step analogous to (8.27), there is a change in the value of the constants A and C: $\mathrm{Re}(\overline{h}^2\rho)$ takes the place of $\mathrm{Re}(h^2\rho)$; the other coefficients remain unchanged except for complex conjugation. Eventually, we have that the expression for $\mathcal{K}_3(\langle H\rangle, g)$ can be written by replacing $\mathrm{Re}(h^2\rho)$ by $\mathrm{Re}(\overline{h}^2\rho)$ and taking the complex conjugate of the coefficients of ρ, ξ as well as the complex conjugate of the coefficients of the hypergeometric terms corresponding to $\mathcal{K}_3(\langle H\rangle, 1)$ in (8.31). In particular, we have

$$\begin{aligned}\mathcal{K}_3(\langle H\rangle, g) = \frac{1}{2^{11}}[&16(p-9)p^{\alpha-1}\mathrm{Re}(\overline{h}^2\rho) + 32p^{2\alpha-2}(p^2-20p+81)\\ &+ 2\mathrm{Re}\{\rho(8\overline{h}^2(p-17)p^{\alpha-1} + 4(\overline{h}^2+4)\mathrm{Re}(\overline{h}^2\rho))\} + 32\mathrm{Re}(\overline{h}^2\rho)\mathrm{Re}(\xi\overline{h})\\ &+ 16\mathrm{Re}(\overline{h}^2\rho^2) + 8(1-h)M_1 + 8(1-\overline{h})M_2 - 8\overline{h}M_3 - 8hM_4 + 48M_5].\end{aligned} \tag{8.33}$$

Finally, using (8.31) and (8.33) in (8.24), we have

$$\begin{aligned}\mathcal{K}_3(\langle H\rangle) = \frac{p^{\alpha-1}(p-1)}{2^8\times 3}\big[&2p^{2\alpha-2}(p^2-20p+81) + 2(\mathrm{Im}\rho)^2 + 4\mathrm{Im}\rho\cdot\mathrm{Im}\xi\\ &-\mathrm{Re}(M_3) + 3M_5\big].\end{aligned}$$

Substituting the above value in (8.18), we complete the proof of the theorem. ■

Bibliography

[1] J. Alexander. Designs from Paley graphs and Peisert graphs. *arXiv preprint arXiv:1507.01289*, 2015.

[2] J. Alexander. *Selected results in combinatorics and graph theory.* ProQuest LLC, Ann Arbor, MI, 2016. Thesis (Ph.D)–University of Delaware.

[3] W. Ananchuen. On the adjacency properties of generalized Paley graphs. *Australas. J. Combin.*, 24:129–147, 2001.

[4] W. Ananchuen and L. Caccetta. On the adjacency properties of Paley graphs. *Networks*, 23(4):227–236, 1993.

[5] W. Ananchuen and L. Caccetta. Cubic and quadruple Paley graphs with the n-e.c. property. *Discrete Math.*, 306(22):2954–2961, 2006.

[6] T. M. Apostol. *Analytic number theory.* Springer-Verlag New York Inc., 1976.

[7] S. Asgarli, S. Goryainov, H. Lin, and C. H. Yip. The EKR-module property of pseudo-paley graphs of square order. *Electron. J. Combin.*, 29(4):19 pp., 2022.

[8] S. Asgarli and C. H. Yip. The subspace structure of maximum cliques in pseudo-paley graphs from unions of cyclotomic classes. *arXiv preprint arXiv:2110.07176*, 2021.

[9] S. Asgarli and C. H. Yip. Van Lint–MacWilliams' conjecture and maximum cliques in Cayley graphs over finite fields. *J. Combin. Theory Ser. A*, 192:Paper No. 105667, 23 pp., 2022.

[10] N. Ashrafi, H. R. Maimani, M. R. Pournaki, and S. Yassemi. Unit graphs associated with rings. *Comm. Algebra*, 38(8):2851–2871, 2010.

[11] R. Atanasov, M. Budden, J. Lambert, K. Murphy, and A. Penland. On certain induced subgraphs of Paley graphs. *Acta Univ. Apulensis Math. Inform.*, (40):51–65, 2014.

[12] B. C. Berndt and R. J. Evans. Sums of Gauss, Jacobi, and Jacobsthal. *J. Number Theory*, 11(3, S. Chowla Anniversary Issue):349–398, 1979.

[13] B. C. Berndt, R. J. Evans, and K. S. Williams. *Gauss and Jacobi sums*. Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons, Inc., New York, 1998. A Wiley-Interscience Publication.

[14] A. E. Brouwer and W. J. Martin. Triple intersection numbers for the paley graphs. *Finite Fields and Their Applications*, 80:102010, 2022.

[15] A. E. Brouwer, R. M. Wilson, and Q. Xiang. Cyclotomy and strongly regular graphs. *J. Algebraic Combin.*, 10(1):25–28, 1999.

[16] M. Budden, N. Calkins, W. N. Hack, J. Lambert, and K. Thompson. Dirichlet character difference graphs. *Acta Mathematica Universitatis Comenianae*, 82(1):21–28, 2017.

[17] A. Cayley. Desiderata and suggestions: No. 2. the theory of groups: graphical representation. *Amer. J. Math.*, 1(2):174–176, 1878.

[18] C. Chao. On the classification of symmetric graphs with a prime number of vertices. *Trans. Amer. Math. Soc.*, 158:247–256, 1971.

[19] K. Conrad. Characters of finite abelian groups. *Lecture Notes*, 17, 2010.

[20] A. Das. Paley-type graphs of order a product of two distinct primes. *Algebra Discrete Math.*, 28(1):44–59, 2019.

[21] M. L. Dawsey and D. McCarthy. Generalized Paley graphs and their complete subgraphs of orders three and four. *Res. Math. Sci.*, 8(2):Paper No. 18, 23 pp., 2021.

[22] D. S. Dummit and R. M. Foote. *Abstract algebra*, volume 3. Wiley Hoboken, 2004.

[23] A. N. Elsawy. Paley graphs and their generalizations. *arXiv preprint arXiv:1203.1818*, 2012.

[24] P. Erdős. On the number of complete subgraphs contained in certain graphs. *Magyar Tud. Akad. Mat. Kutató Int. Közl.*, 7:459–464, 1962.

[25] P. Erdős and A. Rényi. Asymmetric graphs. *Acta Math. Acad. Sci. Hungar.*, 14:295–315, 1963.

[26] R. J. Evans, J. R. Pulham, and J. Sheehan. On the number of complete subgraphs contained in certain graphs. *J. Combin. Theory Ser. B*, 30(3):364–371, 1981.

[27] J. Fuselier, L. Long, R. Ramakrishna, H. Swisher, and F. T. Tu. Hypergeometric functions over finite fields. *2017 MATRIX Annals*, pages 461–466, 2019.

[28] C. Godsil and G. F. Royle. *Algebraic graph theory*, volume 207. Springer Science & Business Media, 2001.

[29] A. W. Goodman. On sets of acquaintances and strangers at any party. *Amer. Math. Monthly*, 66:778–783, 1959.

[30] S. Goryainov, L. Shalaginov, and C. H. Yip. On eigenfunctions and maximal cliques of generalised paley graphs of square order. *Finite Fields Appl.*, 87(102150), 2023.

[31] S. Goryainov and C. H. Yip. Extremal peisert-type graphs without the strict-ekr property. *arXiv preprint arXiv:2306.00391*, 2023.

[32] J. Greene. *Character sum analogues for hypergeometric and generalized hypergeometric functions over finite fields*. ProQuest LLC, Ann Arbor, MI, 1984. Thesis (Ph.D.)–University of Minnesota.

[33] J. Greene. Hypergeometric functions over finite fields. *Trans. Amer. Math. Soc.*, 301(1):77–101, 1987.

[34] F. Harary. *Graph Theory*. Addison-Wesley, Reading, MA, 1969.

[35] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[36] G. A. Jones. Paley and the Paley graphs. In *Isomorphisms, symmetry and computations in algebraic graph theory*, volume 305 of *Springer Proc. Math. Stat.*, pages 155–183. Springer, Cham, [2020] ©2020.

[37] S. A. Katre and A. R. Rajwade. Resolution of the sign ambiguity in the determination of the cyclotomic numbers of order 4 and the corresponding Jacobsthal sum. *Math. Scand.*, 60(1):52–62, 1987.

[38] J. D. Key and B. G. Rodrigues. Special LCD codes from Peisert and generalized Peisert graphs. *Graphs Combin.*, 35(3):633–652, 2019.

[39] A. Kisielewicz and W. Peisert. Pseudo-random properties of self-complementary symmetric graphs. *J. Graph Theory*, 47(4):310–316, 2004.

[40] J. Kraft and L. Washington. *An introduction to number theory with cryptography*. CRC press, 2014.

[41] T. K. Lim and C. E. Praeger. On generalized Paley graphs and their automorphism groups. *Michigan Math. J.*, 58(1):293–308, 2009.

[42] D. McCarthy. Transformations of well-poised hypergeometric functions over finite fields. *Finite Fields Appl.*, 18(6):1133–1147, 2012.

[43] J. Mináč, L. Muller, T. T. Nguyen, and N. D. Tân. On the paley graph of a quadratic character. *arXiv preprint arXiv:2212.02005*, 2022.

[44] N. E. Mullin. Self-complementary arc-transitive graphs and their imposters. Master's thesis, University of Waterloo, 2009.

[45] K. Ono. Values of Gaussian hypergeometric series. *Trans. Amer. Math. Soc.*, 350(3):1205–1223, 1998.

[46] K. Ono. *The web of modularity: arithmetic of the coefficients of modular forms and q-series*, volume 102 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 2004.

[47] R. E. A. C. Paley. On orthogonal matrices. *Journal of Mathematics and Physics*, 12(1-4):311–320, 1933.

[48] W. Peisert. Direct product and uniqueness of automorphism groups of graphs. *Discrete mathematics*, 207(1-3):189–197, 1999.

[49] W. Peisert. All self-complementary symmetric graphs. *J. Algebra*, 240(1):209–229, 2001.

[50] L. Reis. Paley-like graphs over finite fields from vector spaces. *Finite Fields and Their Applications*, 88:102171, 2023.

[51] Horst Sachs. Über selbstkomplementäre Graphen. *Publ. Math. Debrecen*, 9:270–288, 1962.

[52] W. M. Schmidt. *Equations over finite fields: an elementary approach*, volume 536. Springer, 2006.

[53] P. Sin. The critical groups of the Peisert graphs. *J. Algebraic Combin.*, 48(2):227–245, 2018.

[54] L. Sze. The number of edges on generalizations of paley graphs. *International Journal of Mathematics and Mathematical Sciences*, 27:111–123, 2001.

[55] A. G. Thomason. *Partitions of graphs*. PhD thesis, University of Cambridge, 1980.

[56] N. Wage. Character sums and Ramsey properties of generalized Paley graphs. *Integers*, 6:A18, 16 pp., 2006.

[57] C. H. Yip. *On the clique number of Paley graphs and generalized Paley graphs*. PhD thesis, University of British Columbia, 2021.

[58] C. H. Yip. On maximal cliques of Cayley graphs over fields. *J. Algebraic Combin.*, 56(2):323–333, 2022.

[59] C. H. Yip. On the clique number of paley graphs of prime power order. *Finite Fields and Their Applications*, 77:101930, 2022.

[60] C. H. Yip. Refined estimates on the clique number of generalized paley graphs. *arXiv preprint arXiv:2304.13213*, 2023.

[61] H. Zhang. Self-complementary symmetric graphs. *J. Graph Theory*, 16(1):1–5, 1992.

Appendix: Python Code

We have used Python to verify Theorem 8.5 numerically. We refer to the theorem for the notation of ρ, ξ, M_3 and M_5. The code takes a prime $p \equiv 1 \pmod 8$ and a positive integer r as inputs, and computes the number of cliques of order four in the Peisert-like graph $G^*(p^r)$, the Jacobi sums (denoted by ρ and ξ), and the hypergeometric terms (denoted by M_3 and M_5). This Python code can be found in the following link:
https://github.com/AnwitaB/cliques_of_order_four_in_Peisert-like_graph
Alternatively, the SageMath code for the Peisert-like graph can be found in the following link:
https://github.com/AnwitaB/Peisert-like-graph-SageMath/blob/main/Peisert-like
For sake of completeness, we have provided the Python code below.

```
from sympy.ntheory.factor_ import totient
from math import gcd
import cmath
import numpy as np

#the function below calculates the number of cliques of order four in the
Peisert-like graph G^*(n) where n=p^r
def cliques_four (n,H):      #H is the connection set of the graph
```

```
  b1=(int)(totient(n)/2)
  number=0
  flag1, flag2, flag3, flag4, flag5, flag6=0,0,0,0,0,0
  temp1, temp2, temp3, temp4, temp5, temp6=0,0,0,0,0,0

#now, checking if each tuple (i,j,k,l) forms a clique
 for i in range (n):
  for j in range(i+1,n):  #checking if ij is an edge
   temp1, flag1=(i-j)%n,0
   for m in range (b1):
    if temp1==H[m]:
     flag1=1
     break
   if flag1==0:
    continue
   for k in range(j+1,n):  #checking if ik and jk are edges
    temp2, temp3, flag2, flag3=(i-k)%n, (j-k)%n, 0, 0
    for m in range (b1):
     if temp2==H[m]:
      flag2=1
      break
    for m in range (b1):
     if temp3==H[m]:
      flag3=1
      break
    if flag2==0 or flag3==0:
     continue
    for l in range(k+1,n):  #checking if il,jl,kl are edges
```

```
        temp4, temp5, temp6=(i-l)%n, (j-l)%n, (k-l)%n
        flag4, flag5, flag6= 0, 0, 0
        for m in range (b1):
         if temp4==H[m]:
           flag4=1
           break
        for m in range (b1):
         if temp5==H[m]:
           flag5=1
           break
        for m in range (b1):
         if temp6==H[m]:
           flag6=1
           break
        if flag4==0 or flag5==0 or flag6==0:
         continue
        number=number+1   #counts the number of tuples (i,j,k,l)
                          #forming a clique

 print("The number of cliques of order four in the Peisert-like graph
G^*(p^r) is ",number)
 return 1


def raised(k):  #this returns the value of i^k
 if (k%4)==0:
  return 1
 elif (k%4)==1:
```

```
   return complex(0,1)
  elif (k%4)==2:
   return -1
  else:
   return complex(0,1)*(-1)

#the function below calculates the Jacobi sums rho:=J(chi_4,chi_4)
#and zi:=J(chi_4,phi) where chi_4(g)=i, a primitive fourth root of
#unity and phi is the quadratic character, and g is the generator
# of Z_n^*
def jacobi_sums(n,zn,a):

  pos_x, pos_x1=0,0
  rho, zi=0,0
  for i in range(totient(n)):
   x=zn[i]
   x1=(1-x)%n
   if gcd(x1,n)==1:
    for j in range(totient(n)):  #finds pos_x such that g^pos_x=x
     if a[j]==x:
      pos_x=j
      break
    for j in range(totient(n)):  #finds pos_x1 such that
     if a[j]==x1:                #g^pos_x1=1-x
      pos_x1=j
      break
    rho=rho+raised(pos_x+pos_x1)
    zi=zi+raised(pos_x+2*pos_x1)
```

```
 print("The Jacobi sum rho:=J(chi_4,chi_4) is ",rho)
 print("The Jacobi sum zi:=J(chi_4,phi) is ",zi)
 return 1


def hypergeom_sums(n,zn,a):  #this function calculates the
                        #hypergeometric terms M_3 and M_5
 x,x1=0,0
 pos_x, pos_x1=0,0
 sum3,sum5=0,0,
 temp=0
 pos_y, pos_y1, pos_xy=0,0,0
# For calculating the hypergeometric terms, which are double
#summations, we assume that the outer summation is indexed by
#x and the inner summation is indexed by y
 for i in range(totient(n)):
  x=zn[i]
  x1=(1-x)%n
  if gcd(x1,n)==1:
   for j in range(totient(n)):  #finds pos_x such that
    if a[j]==x:                  #g^pos_x=x
     pos_x=j
     break
   for j in range(totient(n)):  #finds pos_x1 such that
    if a[j]==x1:               #g^pos_x1=1-x
     pos_x1=j
     break
   temp=raised(pos_x+pos_x1)         #chi_4(x(1-x))
```

```
temp1, tempo1=0,0
for k in range(totient(n)):
 y=zn[k]
 y1=(1-y)%n
 xy=(x-y)%n
 if (gcd(y1,n)!=1) or (gcd(xy,n)!=1):
  continue
 for l in range(totient(n)):  #finds pos_y such that
  if a[l]==y:                 #g^pos_y=y
   pos_y=l
   break
 for l in range(totient(n)):  #finds pos_y1 such that
  if a[l]==y1:                #g^pos_y1=1-y
   pos_y1=l
   break
 for l in range(totient(n)):  #finds pos_xy such that
  if a[l]==xy:                #g^pos_xy=x-y
   pos_xy=l
   break
 temp1=temp1+raised(pos_y+pos_y1+pos_xy)
                             #chi_4(y(1-y)(x-y))
 tempo1=tempo1+raised(pos_y)*np.conj(raised(pos_y1+pos_xy))
         #chi_4(y)overline(chi_4(1-y)(x-y))) for M_5
temp1=np.conj(temp1) #overline(chi_4(y(1-y)(x-y))) for M_3
sum3=sum3+temp*temp1 #calculates M_3 which involves the
         #sum chi_4(x(1-x))overline(chi_4(y(1-y)(x-y)))
sum5=sum5+temp*tempo1 #calculates M_5 which involves the
     #sum chi_4(x(1-x))chi_4(y)overline(chi_4((1-y)(x-y)))
```

```
 print("The hypergeometric sum M_3 is ",sum3)
 print("The hypergeometric sum M_5 is ",sum5)
 return 1

def main():
 print("enter a prime p congruent to 1 modulo 8")
 p = int(input())
 print("enter a positive integer r")
 r = int(input())
 n=int(pow(p,r))
 zn=list()
 div=list()
 g = 0

 for i in range(1,n):
  if gcd(i,n)==1:
   zn.append(i)          #zn contains the elements of Z_n^*

 for i in range(1, int(totient(n)/2)+1):
  if totient(n)%i==0:
   div.append(i)     #div contains all the positive divisors
 ldiv=len(div)         #of phi(n), except phi(n)

 for i in range(totient(n)):  #this loop finds g, a generator
  var=0                    #of Z_n^*.  Each element a in
  a1=zn[i]                  #Z_n^* is considered, and if
  for d in range (ldiv):     #a^dd=1 in Z_n^* for some dd
```

```
    dd=div[d]              #in div, then a is discarded
    if (pow(a1,dd)%n)==1:
     var=1
     break
   if var==0:
    g=a1
    break
  g1=(g*g*g*g)%n

  H=list()      #H is the connection set of the graph G(p^r)
  for i in range(1, int(totient(n)/4)+1):
   temp=1
   for j in range(1, i+1):
    temp=temp*g1
   H.append(temp%n) #powers of g^4, that is, elements of <g^4>,
                #are appended to H
  for i in range(int(totient(n)/4)):
   H.append((H[i]*g)%n) #elements of g<g^4> are appended to H
  a=list()
  for i in range(totient(n)):
   s=(int)(pow(g,i))
   a.append(s%n)   #a stores all the powers of the generator g,
                #that is, 1,g,g^2,..,g^(totient(n)-1)
  cliques_four(n, H)
  jacobi_sums(n,zn,a)
  hypergeom_sums(n,zn,a)
main()
```

The following link contains the `SageMath` code for the Paley-type graph:
https://github.com/AnwitaB/Paley-type-SageMath/blob/main/Paley-type

Publications

Publications from Thesis work

1. A. Bhowmik and R. Barman, *On a Paley-type graph on* $\mathbb{Z}_n$, Graphs and Combinatorics 38 (2022), no. 2, Paper No. 41, 25 pp.

2. A. Bhowmik and R. Barman, *Number of complete subgraphs of Peisert graphs and finite field hypergeometric functions*, arXiv preprint arXiv:2205.03928 [math.CO; math.NT] (2022), minor revisions submitted to Research in Number Theory.

3. A. Bhowmik and R. Barman, *Hypergeometric functions for Dirichlet characters and Peisert-like graphs*, La Matematica (2023). https://doi.org/10.1007/s44007-023-00075-w.

4. A. Bhowmik and R. Barman, *Cliques of orders three and four in the Paley-type graphs*, arXiv preprint arXiv:2301.07021 [math.CO; math.NT] (2023).