RIGIDITY OF MAXIMUM CLIQUES IN PSEUDO-PALEY GRAPHS FROM UNIONS OF CYCLOTOMIC CLASSES

SHAMIL ASGARLI AND CHI HOI YIP

ABSTRACT. Blokhuis showed that Paley graphs with square order have the Erdős-Ko-Rado (EKR) property in the sense that all maximum cliques are canonical. In our previous work, we extended the EKR property of Paley graphs to certain Peisert graphs and generalized Peisert graphs. In this paper, we propose a conjecture which generalizes the EKR property of Paley graphs, and can be viewed as an analogue of Chvátal’s Conjecture for families of set systems. As a partial progress, we prove that maximum cliques in pseudo-Paley graphs have a rigid structure.

1. INTRODUCTION

In this paper, we gather ideas from [AY21, Yip21a] and discuss the Erdős-Ko-Rado (EKR) property of pseudo-Paley graphs obtained from unions of semi-primitive cyclotomic classes. More precisely, we study the rigidity of the structure of maximum cliques in this family of graphs. The main motivation for this work is to extend the following result of Blokhuis [Blo84] to certain pseudo-Paley graphs. Blokhuis’ theorem is also known as the EKR property of Paley graphs according to Godsil and Meagher [GM16, Section 5.9]; see also Section 1.3 of this paper.

Theorem 1.1 ([Blo84]). Let \( q = p^{2r} \), where \( p \) is an odd prime. Then the only maximum clique in \( P_q \) containing \( \{0, 1\} \) is the subfield \( \mathbb{F}_{\sqrt{q}} \). Consequently, each maximum clique in \( P_q \) is the image of an affine transformation on the subfield \( \mathbb{F}_{\sqrt{q}} \).

In our previous work [AY21], we proved that Theorem 1.1 is essentially equivalent to asserting that each maximum clique has an affine subspace structure. Motivated by this observation, we investigate when a maximum clique of size \( \sqrt{q} \) in a pseudo-Paley graph is a subspace. See Conjecture 1.4 for a precise formulation.

1.1. Main results. Our main results concern pseudo-Paley graphs obtained from taking a union of \( d \) copies of \( 2d \)-Paley graphs. These graphs are similar to Paley graphs both globally as they share the same spectrum, and locally as the building blocks are generalized Paley graphs. We use \( I = \{m_1, m_2, \ldots, m_d\} \subset \{0, 1, 2, \ldots, 2d - 1\} \) to denote the set of indices of the cyclotomic classes. Let \( PP(q, 2d, I) \) denote the Cayley graph on \( \mathbb{F}_q^+ \), with the connection set being the union of \( 2d \)-th cyclotomic classes \( C_{m_1}, C_{m_2}, \ldots, C_{m_d} \); see Definitions 2.2 and 2.3. Usually, we work with the semi-primitive case, meaning that \( q = p^{2r} \) where \( r \) is the smallest integer such that \( p^r \equiv -1 \) (mod 2d). This additional hypothesis ensures that \( X = PP(q, 2d, I) \) is indeed a pseudo-Paley graph; see Lemma 2.13.

The first result guarantees that a maximum clique of size \( \sqrt{q} \) has equal contribution from each copy of the \( 2d \)-Paley graph, more precisely, from each cyclotomic class.

\[ \text{Date: October 15, 2021.} \]

\[ \text{2020 Mathematics Subject Classification.} \quad \text{Primary 05C25, 05C69; Secondary 11T22, 11T24, 05E30, 05C60.} \]

\[ \text{Key words and phrases.} \quad \text{Paley graph, maximum clique, Erdős-Ko-Rado theorem, Gauss sum, cyclotomy.} \]
Theorem 1.2. Let \( X = PP(q, 2d, I) \) be a semi-primitive pseudo-Paley graph with \( q = p^{2r} \) where \( r \) is even. Then \( \omega(X) \leq \sqrt{q} \). Moreover, if \( \omega(X) = \sqrt{q} \), and \( A \) is a maximum clique in \( X \) such that \( 0 \in A \), then

\[
|A \cap C_{m_1}| = |A \cap C_{m_2}| = \cdots = |A \cap C_{m_d}| = \frac{\sqrt{q} - 1}{d}. 
\] (1)

We remark that in the special case when \( X \) is the Paley graph, Theorem 1.2 follows from the EKR property of Paley graphs; see Lemma 2.14. Furthermore, Theorem 1.2 is a genuine extension: most graphs \( PP(q, 2d, I) \) are not isomorphic to the Paley graph \( P_q \); see Proposition 6.7. As a consequence, we find a new family of strongly regular self-complementary graphs, which is of independent interest.

Theorem 1.2 immediately implies the following upper bound on the clique number of a particular type of graphs.

Corollary 1.3. Let \( X = PP(q, 2d, I) \) be a semi-primitive pseudo-Paley graph with \( q = p^{2r} \) where \( r \) is even. Pick subsets \( D_{m_j} \subset C_j \) for each \( 1 \leq j \leq d \) such that \( |D_{m_k}| < (\sqrt{q} - 1)/d \) holds for some \( k \). Consider the Cayley graph \( X' = \text{Cay}(F_q^{+}, \bigcup_{j=1}^{n} D_{m_j}) \), which is a subgraph of \( X \). Then \( \omega(X') \leq \sqrt{q} - 1 \).

Proof. By Theorem 1.2, \( \omega(X') \leq \omega(X) \leq \sqrt{q} \). So, if \( \omega(X') = \sqrt{q} \), then \( \omega(X) = \sqrt{q} \) as well. Now, take a maximum clique \( A \) in \( X' \) containing 0, so that \( A \) is also a maximum clique in \( X \). By Theorem 1.2, \( |D_{m_j}| \geq |A \cap C_j| = \frac{\sqrt{q} - 1}{d} \) for each \( 1 \leq j \leq d \), contradicting the hypothesis. \( \square \)

The graphs considered in Corollary 1.3 include many important graphs. For example, by setting \( D_0 = C_0 \) and \( D_j = \emptyset \) for \( 1 \leq j \leq 2d - 1 \), we recover \( \omega(GP(q, 2d)) \leq \sqrt{q} - 1 \), which is a special case of the main result in [Yip21a]. In the case when the connection set of \( X' \) is contained in \( D' \), which is a union of at most \( d - 1 \) cyclotomic classes, the conclusion in Corollary 1.3 can be deduced using Delsarte’s bound on the strongly regular graph \( \text{Cay}(F_q^{+}, D') \); see Theorem 2.11 and Theorem 2.16. The graphs considered here could have poor algebraic structure, in which case the tools such as the Delsarte bound from algebraic graph theory seem inefficient.

Theorem 1.2 hints that any maximum clique \( A \) of size \( \sqrt{q} \) is rigid. In [AY21], we gave a simple proof of the EKR property of Paley graphs (see Theorem 1.1) by first showing that each maximum clique in \( P_q \) must be an affine subspace. This leads to the following conjecture, which we call the EKR property of semi-primitive pseudo-Paley graphs.

Conjecture 1.4. Let \( X = PP(q, 2d, I) \) be a semi-primitive pseudo-Paley graph with \( q = p^{2r} \) where \( r \) is even. If \( \omega(X) = \sqrt{q} \), then every maximum clique in \( X \) is an \( \mathbb{F}_{p^r} \)-affine subspace. In particular, if there is no \( \mathbb{F}_{p^r} \)-affine subspace which has size \( \sqrt{q} \) and forms a clique in \( X \), then \( \omega(X) \leq \sqrt{q} - 1 \).

We have verified Conjecture 1.4 experimentally for \( q \) up to \( 7^4 \). The algorithm is described in Section 7.

We also expect that most pseudo-Paley graphs (other than Paley graphs) on \( \mathbb{F}_q \) from a union of cyclotomic classes have clique number less than \( \sqrt{q} \); this is made precise in Proposition 5.6, where the density of graphs with clique number \( \sqrt{q} \) is shown to be zero. Our next main result provides an effective version of this statement.

Theorem 1.5. Let \( X = PP(q, 2d, I) \) be a semi-primitive pseudo-Paley graph with \( q = p^{2r} \) where \( r \) is even, and \( I \neq \{0, 2, \ldots, 2d - 2\} \) and \( I \neq \{1, 3, \ldots, 2d - 1\} \). Assuming Conjecture 1.4, \( \omega(X) \leq \sqrt{q} - 1 \) for \( p^t > 10.2r^2d \).  

2
As a concrete application, we can conditionally improve the trivial upper bound $\sqrt{q}$ for the clique number of generalized Peisert graphs; see the related discussion in Section 2.4. The result below contains as a special case the conjecture made by the second author on Peisert graphs [Yip21b, Conjecture 4.3].

**Theorem 1.6.** Suppose that Conjecture 1.4 is true. If $d \geq 2$, and $t$ is the smallest integer such that $p^t \equiv -1 \pmod{2d}$ and $p^t > 3$, then $\omega(GP^*(p^t, 2d)) \leq p^{2t} - 1$. In particular, $\omega(P^*_p) \leq p^2 - 1$ for any prime $p \equiv 3 \pmod{4}$ such that $p > 3$.

The key idea in the proof of Theorem 1.2 is to establish a system of linear equations in the expressions $|A \cap C_{m_1}|, |A \cap C_{m_2}|, \ldots, |A \cap C_{m_d}|$ and then find a way to solve the system. As preparation, we establish the following Fourier analytic characterization of maximum cliques in a pseudo-Paley graph from unions of cyclotomic classes, which is of independent interest.

Let $I = \{m_1, \ldots, m_d\}$ be a subset of $\{0, 1, \ldots, 2d - 1\}$ with size $d \geq 2$, and denote

$$D = \bigcup_{j=1}^d C_{m_j}, \quad D' = \bigcup_{j=1}^d C_{-m_j}, \quad D'' = \bigcup_{j=1}^d C_{-m_j-2d},$$

where all the indices are interpreted modulo $2d$.

**Proposition 1.7.** Let $X = PP(q, 2d, I)$ be a semi-primitive pseudo-Paley graph with $q = p^{2r+1}$. If $A$ is a clique in $X$, then $|A| \leq \sqrt{q}$; moreover, $|A| = \sqrt{q}$ if and only if $S(q, A; c) = 0$ for all $c \in B$, where $S(q, A; c)$ is defined in Definition 3.1, and

$$B = \begin{cases} \mathbb{F}_q \setminus D' & \text{if } r \text{ is odd and } p^t \equiv -1 \pmod{4d} \\
\mathbb{F}_q \setminus D'' & \text{if } r \text{ is odd and } p^t \equiv 2d - 1 \pmod{4d} \\
D' & \text{if } r \text{ is even} \end{cases}$$

and $D', D''$ are defined as in equation (2).

While we mainly focus on the case $r$ is even in all the previous statements, Proposition 1.7 includes the case $r$ is odd. When $r$ is odd and $0 \in I$ in the semi-primitive pseudo-Paley graph $X$, the subfield $\mathbb{F}_{\sqrt{q}}$ forms a maximum clique. We hope that the proposition above can be used to prove the EKR property of $X$ in this case: the only maximum clique containing 0, 1 is $\mathbb{F}_{\sqrt{q}}$. See the related discussion in [AY21] and [Yip21a, Section 4.4].

1.2. **Subspace structure of maximum cliques.** The subspace structure of maximum cliques is a phenomenon that has been observed in related Cayley graphs. For example, Paley graphs enjoy this property by Theorem 1.1. More generally, in [AY21, Theorem 1.2], we showed that maximum cliques of size $\sqrt{q}$ in a so-called Peisert-type graph (see [AY21, Definition 1.1]) must have a subspace structure. Most graphs considered in Conjecture 1.4 are not covered by the past results.

Proving Conjecture 1.4 in general seems to be out of reach. It is worth pointing out that neither Conjecture 1.4 nor Theorem 1.2 imply each other. However, let us discuss how Theorem 1.2 shows that a maximum clique containing 0 “behaves like” a subspace, thus lending some evidence towards Conjecture 1.4. Note that if $V$ is a vector space over $\mathbb{F}_p$, and $V$ is a maximum clique in $X$, then $|V \cap C_{m_j}| = |g^{-m_j}V \cap C_0|$ for each $1 \leq j \leq d$. Now, $g^{-m_j}V$ is again a vector space, and $C_0$ is a multiplicative subgroup of $\mathbb{F}_q$. The intersection of a subspace and a multiplicative subgroup can be modelled as the intersection of two random sets; this heuristic is close to the truth provided that the product of the sizes of the two sets is sufficiently large [Kop19, Lemma 11]. While in
our case $|V||C_0|$ is not sufficiently large, we still expect $|V \cap C_{m_j}| = |g^{-m_j}V \cap C_0|$ to be close to $|V||C_0|/q = (\sqrt{q} - 1)/d + O(1)$, and $(\sqrt{q} - 1)/d$ is exactly the size of the contribution in Theorem 1.2.

To give context for the present paper, we now turn attention to the well-known results related to Paley graphs. Blokhuis [Blo84] showed that Paley graphs of square order have the EKR property in the sense that all maximum cliques are canonical (with a subfield structure); see the related discussion on the history of the problem in [AY21, Section 2.1] and [GM16, Section 5.9].

Theorem 1.1 was later generalized by Sziklai [Szi99] to generalized Paley graphs $GP(q,d)$, where $d \mid (\sqrt{q} + 1)$. When $d \nmid (\sqrt{q} + 1)$, we do not expect that there is a simple characterization of maximum cliques in $GP(q,d)$, since $\omega(GP(q,d)) \leq \sqrt{q} - 1$; see [Yip21a] and [AY21, Remark 2.3]. A further generalization was recently discovered by the authors [AY21, Theorem 1.3].

Note that in Theorem 1.2, $\sqrt{q} \equiv 1 (\mod 2d)$, and so $2d \nmid (\sqrt{q} + 1)$. Thus, each copy of $GP(q,2d)$ appearing in $X$ has clique number $\leq \sqrt{q} - 1$, but it is not obvious how to control the clique number of $X$. In fact, $\omega(X) = \sqrt{q}$ can happen sometimes (see examples in Section 7). Theorem 1.2 and Conjecture 1.4 indicate that in such a graph $X$, any maximum clique $A$ of size $\sqrt{q}$ must have the same rigid structure observed in Paley graphs.

We also prove the following two theorems on the number of maximum cliques. Comparing these with Theorem 1.1, we see that pseudo-Paley graphs in general behave much differently compared to Paley graphs. Note that Theorem 1.8 generalizes Mullin’s theorem [Mul09, Lemma 3.3.6] for the Peisert graph.

**Theorem 1.8.** Let $X = PP(q,2d,I)$ be a semi-primitive pseudo-Paley graph with $q = p^{2rt}$ where $r$ is even. Suppose that $0 \in I$ and $I \neq \{0, 2, \ldots, 2d-2\}$. If $\omega(X) = \sqrt{q}$, then there are at least 2 maximum cliques in $X$ that contains $\{0, 1\}$.

**Theorem 1.9.** Let $X = PP(q,2d,I)$ be a semi-primitive pseudo-Paley graph with $q = p^{4t}$. Suppose that $0 \in I$ and $I \neq \{0, 2, \ldots, 2d-2\}$. Then $X$ has an even number of cliques (possibly zero) of size $\sqrt{q}$ that are subspaces defined over $\mathbb{F}_p$, containing 1. Furthermore, these maximum cliques come in pairs that are interchanged by the map $x \mapsto x\sqrt{q}$.

**1.3. Further motivation.** To give further motivation for Theorem 1.2 and Conjecture 1.4, and to see their connection with EKR-type results, we digress slightly to give an overview of EKR-type theorems.

The original Erdős-Ko-Rado (EKR) theorem [EKR61] states that each maximum intersecting family of $m$-subsets of $\{1, 2, \ldots, n\}$ is canonical in the sense that it is a star, provided $n \geq 2m + 1$. As one of the foundational results in extremal combinatorics, the EKR theorem has been widely studied. Moreover, its analogues have been successfully discovered in a wide range of combinatorial objects, including set systems, permutations, partitions, perfect matchings, orthogonal arrays, independent sets, cliques, vector spaces, and so on (see [GM16] for an extensive discussion). Typically EKR-type results state that the extremal configurations must have a rigid structure, and in most cases, they must be canonical in the sense that they have an extremely simple structure compared to the complicated ground space. For example, in the classical EKR theorem, the extremal configurations are stars, that is, families of sets containing a common element from the ground set. The classical EKR theorem can also be formulated in terms of graph theory: each maximum independent set in a Kneser graph is canonical (see [GM16, Chapter 2]). We can also phrase this phenomenon in terms of maximum cliques: each maximum clique in the complement of a Kneser graph is canonical. This explains why Theorem 1.1 is known as the EKR-property of Paley graphs.
There is a proposed algebraic graph theory approach for proving Theorem 1.1 in [GM16, Section 5.9] which remains open [GM16, Section 16.5]. Proving Conjecture 1.4 using this approach would be even more difficult. However, we should mention that the algebraic graph theory approach is powerful in proving EKR-type theorems; the book by Godsil and Meagher [GM16] provides an excellent survey.

Our next goal is to define a notion of canonical cliques in a semi-primitive pseudo-Paley graph $X$ so that we can speak about its EKR property. We will see in Section 2.4 that the trivial upper bound on the clique number of $X$ is $\sqrt{q}$, and yet it is difficult to improve this upper bound or classify the maximum cliques when the bound is tight. Note that $X$ is a Cayley graph $\text{Cay}(\mathbb{F}_q^+, D)$ for the set $D = \bigcup_j C_{m_j}$; the set $A$ forms a clique in $X$ if and only if $A - A \subset D \cup \{0\}$, where $A - A = \{a - a' : a, a' \in A\}$. We see that additive combinatorics plays an important role here because $A - A$ has a rich additive structure, whereas $D$, being a union of cyclotomic classes, has a rich multiplicative structure. This partially explains why estimating the clique number of Paley graphs, generalized Paley graphs, and other related graphs is a central open problem in additive combinatorics [CL07, Section 2.7]: the study of a clique is essentially the study of the interaction between additive structure and multiplicative structure of a set. See [AB14, Shk14] for related discussions. All results in this paper conditional on Conjecture 1.4 can be reformulated unconditionally based on such interaction; for instance, compare Theorem 1.5 and Corollary 5.9.

Let $K$ be a subfield of $\mathbb{F}_q$. Note that if $V$ is a $K$-subspace, then $V - V = V$; thus, the set $V$ forms a clique in $X$ if and only if $V \subset D \cup \{0\}$. Therefore, it is much easier for a subspace to form a clique in $X$, compared to a generic subset of $\mathbb{F}_q$. We would like to choose the subfield $K$ so that it serves the role of the prime subfield $\mathbb{F}_p$. In our case $q = p^{2rt} = (p^t)^{2r}$ and $t$ is the smallest integer with $p^t \equiv -1 \pmod{2d}$. In view of Stickelberger’s Theorem (Theorem 3.5), the choice $K = \mathbb{F}_{p^t}$ is the natural replacement of the prime subfield $\mathbb{F}_p$. Therefore, we call $V$ a canonical clique in $X$ if $V$ is a $\mathbb{F}_{p^t}$-affine subspace with $|V| = \sqrt{q}$ and $V$ forms a clique in $X$. Using this terminology, Conjecture 1.4 states that each maximum clique of size $\sqrt{q}$ in $X$ is canonical.

Note that we are working with a family of graphs simultaneously instead of working on a single graph, which significantly increases the difficulty of proving Conjecture 1.4. We remark that our conjecture is an analogue of the famous Chvátal’s Conjecture [Chv74] on families of set systems, which is a variant of the EKR theorem and is still widely open (see Chvátal’s webpage [Chv11] for related discussion and references on the conjecture). Chvátal’s Conjecture states that for any family $\mathcal{F}$ of subsets of a finite set that is closed under taking subsets (known as an ideal), there is a largest intersecting subfamily of $\mathcal{F}$ that is a star. In other words, in any nice set system, there is a canonical maximum intersecting family; our conjecture is actually stronger, because it implies that in any nice Pseudo-Paley graph (that is, with clique number $\sqrt{q}$), every maximum clique is canonical. In summary, Conjecture 1.4 can be viewed as a combination of both the Erdős-Ko-Rado Theorem and Chvátal’s conjecture in the context of pseudo-Paley graphs. The following table is a short dictionary between concepts in Chvátal’s Conjecture (first column) and in the present work (second column).
1.4. Structure of the paper. We outline the flowchart of the paper. In Section 2, we provide further background, introduce the relevant notations, and present preliminary properties. We also survey some results on strong regularity and the clique number. We introduce tools from Gauss sums and character sums in Section 3, and present the proof of Theorem 1.2, Proposition 1.7, and Theorem 1.8 in Section 4. In Section 5, we prove Theorem 1.5, Theorem 1.6, and Theorem 1.9. In Section 6, we prove that the families of graphs considered in this paper are almost always not isomorphic to Peisert graphs or Paley graphs. As a by-product, we obtain Corollary 6.8 which resolves Mullin’s conjecture on generalized Peisert graphs. Finally, in Section 7, we report results from our numerical experiments from SageMath, including two algorithms and sample code.

2. Preliminaries

2.1. Paley graphs and Peisert graphs. We begin with recalling a few fundamental definitions. Given an abelian group $G$ and a set $D \subset G \setminus \{0\}$ with $D = -D$, the Cayley graph $\text{Cay}(G, D)$ is the graph defined on $G$, such that two vertices $x, y \in G$ are adjacent if and only if $x - y \in D$. The set $D$ is called a connection set. Recall that a clique in a graph $X$ is a subset of vertices of $X$ such that any two of them are adjacent. Moreover, the clique number of $X$, denoted by $\omega(X)$, is the size of a maximum clique in $X$. Throughout the paper, $p$ denotes an odd prime, $q$ denotes a positive power of $p$, and $\mathbb{F}_q$ denotes the finite field with $q$ elements. For a finite field $\mathbb{F}_q$, $\mathbb{F}_q^*$ denotes its additive group, and $\mathbb{F}_q^+$ denotes its multiplicative group. We always assume that $q$ is a fixed primitive root of $\mathbb{F}_q$.

Paley graphs are the well-studied Cayley graphs $\text{Cay}(\mathbb{F}_q^+, (\mathbb{F}_q^*)^2)$, where $q \equiv 1 \pmod{4}$ and $(\mathbb{F}_q^*)^2$ is the set of squares in $\mathbb{F}_q$. In general, if $S$ is a proper subgroup of $\mathbb{F}_q^*$ such that $-1 \in S$, then $GP(q, d) = \text{Cay}(\mathbb{F}_q^+, S)$ is said to be a $d$-Paley graph, where $d = (q - 1)/|S|$; see for example [Coh88, LP09, Yip21c]. Since $q$ is odd, it is easy to see $-1 \in S$ if and only if $q \equiv 1 \pmod{2d}$. Alternatively, if $q \equiv 1 \pmod{2d}$, then $GP(q, d) = \text{Cay}(\mathbb{F}_q^+, (\mathbb{F}_q^*)^d)$.

The Peisert graph of order $q = p^r$, where $p$ is a prime such that $p \equiv 3 \pmod{4}$ and $r$ is even, denoted $P_q^*$, is the Cayley graph $\text{Cay}(\mathbb{F}_q^+, M_q)$ with

$$M_q := \{g^j : j \equiv 0, 1 \pmod{4}\},$$

where $g$ is a primitive root of the field $\mathbb{F}_q$. While the construction of $P_q^*$ depends on the primitive root $g$, the isomorphism type of $P_q^*$ is independent of the choice of $g$ [Pei01].

Motivated by the similarity shared among Paley graphs, generalized Paley graphs, and Peisert graphs, Mullin introduced generalized Peisert graphs; see for example [Mul09, Section 5.3] and [AY21, Definition 2.8].

**Definition 2.1** (generalized Peisert graph). Let $d$ be a positive integer, and $q$ a prime power such that $q \equiv 1 \pmod{4d}$. The $2d$-th power Peisert graph of order $q$, denoted $GP^*(q, 2d)$, is the Cayley graph $\text{Cay}(\mathbb{F}_q^+, M_2d)$ with

$$M_2d := \{g^{2d^j} : j \equiv 0, 1 \pmod{4d}\},$$

where $g$ is a primitive root of the field $\mathbb{F}_q$. While the construction of $P_q^*$ depends on the primitive root $g$, the isomorphism type of $P_q^*$ is independent of the choice of $g$ [Pei01].

Motivated by the similarity shared among Paley graphs, generalized Paley graphs, and Peisert graphs, Mullin introduced generalized Peisert graphs; see for example [Mul09, Section 5.3] and [AY21, Definition 2.8].

**Definition 2.1** (generalized Peisert graph). Let $d$ be a positive integer, and $q$ a prime power such that $q \equiv 1 \pmod{4d}$. The $2d$-th power Peisert graph of order $q$, denoted $GP^*(q, 2d)$, is the Cayley graph $\text{Cay}(\mathbb{F}_q^+, M_2d)$ with

$$M_2d := \{g^{2d^j} : j \equiv 0, 1 \pmod{4d}\},$$

where $g$ is a primitive root of the field $\mathbb{F}_q$. While the construction of $P_q^*$ depends on the primitive root $g$, the isomorphism type of $P_q^*$ is independent of the choice of $g$ [Pei01].

Motivated by the similarity shared among Paley graphs, generalized Paley graphs, and Peisert graphs, Mullin introduced generalized Peisert graphs; see for example [Mul09, Section 5.3] and [AY21, Definition 2.8].

**Definition 2.1** (generalized Peisert graph). Let $d$ be a positive integer, and $q$ a prime power such that $q \equiv 1 \pmod{4d}$. The $2d$-th power Peisert graph of order $q$, denoted $GP^*(q, 2d)$, is the Cayley graph $\text{Cay}(\mathbb{F}_q^+, M_2d)$ with

$$M_2d := \{g^{2d^j} : j \equiv 0, 1 \pmod{4d}\},$$

where $g$ is a primitive root of the field $\mathbb{F}_q$. While the construction of $P_q^*$ depends on the primitive root $g$, the isomorphism type of $P_q^*$ is independent of the choice of $g$ [Pei01].

Motivated by the similarity shared among Paley graphs, generalized Paley graphs, and Peisert graphs, Mullin introduced generalized Peisert graphs; see for example [Mul09, Section 5.3] and [AY21, Definition 2.8].
graph \( \text{Cay}(\mathbb{F}_q^+, M_{q,2d}) \), where

\[
M_{q,2d} = \left\{ g^{2dk+j} : 0 \leq j \leq d - 1, k \in \mathbb{Z} \right\},
\]

and \( g \) is a primitive root of \( \mathbb{F}_q \).

Observe that \( GP^*(q, 2) = P_q \) and \( GP^*(q, 4) = P_q^* \). This suggests that generalized Peisert graphs are also natural generalizations of Paley graphs. In fact, generalized Peisert graphs are more natural compared to generalized Paley graphs as they have the same edge density (namely, 1/2) as Paley graphs. Moreover, certain generalized Peisert graphs share the same eigenvalues as Paley graphs; see Example 2.5 and Lemma 2.13.

2.2. Cayley graphs from a union of cyclotomic classes. Next we revisit how to construct Cayley graphs from a union of cyclotomic classes; see for example [vLS81, BEW98, FX12]. The following is the definition of cyclotomic classes [FX12, Section 3]. Cyclotomic classes are closely related to Gauss sums. We will call a cyclotomic class \( \text{semi-primitive} \) if the corresponding Gauss sum is semi-primitive, in which case the associated Gauss sums can be evaluated explicitly by Stickelberger’s theorem (see Section 3 for a related discussion). We will restrict our attention to this case for the most part.

**Definition 2.2** (Cyclotomic classes). Let \( N \mid (q - 1) \). Let \( C_0 \) be the subgroup of \( \mathbb{F}_q^* \) with index \( N \), and let \( C_1, \ldots, C_{N-1} \) be all the cosets of \( C_0 \), where \( C_j = g^j C_0 \). The sets \( C_0, C_1, \ldots, C_{N-1} \) are called the \( N \)-th cyclotomic classes of \( \mathbb{F}_q \). Furthermore, we say that \( N \)-th cyclotomic classes are semi-primitive if \(-1 \) is a power of \( p \) modulo \( N \).

In the definition below and for the rest of the paper, we will fix the ground field \( \mathbb{F}_q \), and a choice of a primitive root \( g \) of \( \mathbb{F}_q \).

**Definition 2.3.** Suppose \( q \) is a prime power, \( d \) a positive integer such that \( 2d \mid (q - 1) \), and \( I = \{m_1, \ldots, m_d\} \subset \{0, 1, \ldots, 2d - 1\} \) with \( |I| = d \). Let \( C_0, C_1, \ldots, C_{2d-1} \) be the \( 2d \)-th cyclotomic classes of \( \mathbb{F}_q \). The graph \( PP(q, 2d, I) \) is defined to be the Cayley graph \( \text{Cay}(\mathbb{F}_q^+, D) \) where

\[
D = \bigcup_{j=1}^{d} C_{m_j}.
\]

Furthermore, we say that \( X = PP(q, 2d, I) \) is a semi-primitive pseudo-Paley graph if \(-1 \) is a power of \( p \) modulo \( 2d \). In this case, we always write \( q = p^{2rt} \) where \( t \in \mathbb{N} \) is the smallest integer satisfying \( p^t \equiv -1 \pmod{2d} \), and \( r \in \mathbb{N} \).

The notation “PP” stands for Pseudo-Paley; see Lemma 2.13 for more explanation. Observe that \( PP(q, 2d, I) \) is a union of \( d \) copies of \( GP(q, 2d) \), where the different copies are indexed by the set \( I \). While \( C_j \) clearly depends on the choice of \( g \), the isomorphism class of the resulting graph will only depend on \( q, d \) and the set \( I \). Indeed, any two primitive roots \( g \) and \( g' \) can be interchanged by a unique field automorphism which gives rise to a graph isomorphism.

**Remark 2.4.** If \( D' = yD \) for some \( y \in \mathbb{F}_q^* \), then the two Cayley graphs \( \text{Cay}(\mathbb{F}_q^+, D) \) and \( \text{Cay}(\mathbb{F}_q^+, D') \) are isomorphic via the map \( x \mapsto yx \). This observation allows us to assume \( m_1 = 0 \) without loss of generality. Indeed, we can replace \( X = \text{Cay}(\mathbb{F}_q^+, D) \) by the graph \( X' = \text{Cay}(\mathbb{F}_q^+, g^{-m_1}D) \).
In the following discussion, when we are talking about a cyclotomic class $C_j$ in $PP(q, 2d, I)$, we always assume $C_j$ is a $2d$-th cyclotomic classes of $\mathbb{F}_q$.

**Example 2.5.** By specializing the choice of the set $I$, we recover several important families of Cayley graphs we mentioned previously:

1. $PP(q, 2, \{0\})$ is the Paley graph $P_q = \text{Cay}(\mathbb{F}_q^+, C_0)$.
2. $PP(q, 4, \{0, 1\})$ is the Peisert graph $P^*_q = \text{Cay}(\mathbb{F}_q^+, C_0 \cup C_1)$.
3. $PP(q, 2d, \{0, 2, 4, \ldots, 2d - 2\})$ is also the Paley graph $P_q = \text{Cay}(\mathbb{F}_q^+, C_0 \cup C_2 \cup \ldots \cup C_{2d-2})$.
4. $PP(q, 2d, \{1, 3, 5, \ldots, 2d - 1\})$ is the complement of the Paley graph $P_q$, and it is isomorphic to $P_q$.
5. $PP(q, 2d, \{0, 1, 2, \ldots, d-1\})$ is the generalized Peisert graph $GP^*(q, 2d) = \text{Cay}(\mathbb{F}_q^+, C_0 \cup C_1 \cup \ldots \cup C_{d-1})$.
6. Suppose that $d = 2m$ is even. If $I = \{i, i+4, \ldots, i+4(m-1)\} \cup \{j, j+4, \ldots, j+4(m-1)\}$ for some $i < j \in \{0, 1, 2, 3\}$, then $PP(q, 2d, I)$ is isomorphic to the Paley graph $P_q$ when $j - i = 2$, and $PP(q, 2d, I)$ is isomorphic to the Peisert graph $P^*_q$ when $j - i \in \{1, 3\}$.
7. $PP(q, \sqrt{q} + 1, I)$ is a Peisert-type graph of order $q$ for square $q$: see [AY21, Definition 1.1]. The EKR property of these graphs was discussed in [AY21].

From Example 2.5, we see that two different choices of $(d, I)$ may represent the same graph. In general, if $d' | d$ and $I = \bigcup_{j \in I'} \{j + 2d'k : 0 \leq k \leq \frac{d}{d'} - 1\}$, then $PP(q, 2d, I) = PP(q, 2d', I')$. It is natural to work with the representation with the smallest value of $d$. This motivates the following definition.

**Definition 2.6 (Minimal representation).** We say $X = PP(q, 2d, I)$ is in its minimal representation if there is no $d' | d$ and $I' \subset \{0, 1, \ldots, 2d' - 1\}$ such that $d' < d$ and $X = PP(q, 2d', I')$.

It is clear that a minimal representation of $X$ is unique.

Note that if $d' | d$ and $I = \bigcup_{j \in I'} \{j + 2d'k : 0 \leq k \leq \frac{d}{d'} - 1\}$, then $I = I + 2d' n \pmod{2d}$ for any integer $n$. The converse is also true:

**Lemma 2.7.** Let $X = PP(q, 2d, I)$ and let $PP(q, 2d', I')$ be its minimal representation. If $I = I + k := \{j + k \pmod{2d} : j \in I\}$, then $k$ must be a multiple of $2d'$.

**Proof.** If $I = I + k$, then $I$ is a union of arithmetic progressions each with common difference $\gcd(2d, k)$. The length of each arithmetic progression appearing in the union is $\frac{2d}{\gcd(2d, k)}$. Therefore, $d = |I|$ is a multiple of $\frac{2d}{\gcd(2d, k)}$. It follows that $\gcd(2d, k)$ is even. Let $\gcd(2d, k) = 2e$.

In particular, $X = PP(q, 2d, I) = PP(q, 2e, J)$, where $J = \{j \pmod{2e} : j \in I\}$. Since $PP(q, 2d', I')$ is the minimal representation of $X$, it follows that $2d' | 2e$, and so $2d' | k$. □

**Remark 2.8.** The condition $I = I + k$ is connected to the symmetries of the graph $X$. More precisely, the map $x \mapsto g^k x$ induces a graph automorphism of $X$ if and only if $I + k = I$.

2.3. **Pseudo-Paley graphs.** The graphs constructed in Definition 2.3 enjoy properties such as being strongly regular. Brouwer and van Maldeghem [BvM21] provide a comprehensive reference on the topic of strongly regular graphs; see also [GM16, Chapter 5] for a detailed discussion on this topic with applications to finite geometry and Paley graphs. Recall that a graph is $k$-regular if each vertex has $k$ neighbors.
Definition 2.9 (Strongly regular graph). If \( Y \) is a \( k \)-regular graph with \( n \) vertices, such that any two adjacent vertices have \( \lambda \) common neighbors, and any two non-adjacent vertices have \( \mu \) common neighbors, then we say \( Y \) is a strongly regular graph with parameters \( (n, k, \lambda, \mu) \).

It is well-known that Paley graphs are strongly regular; see for example [GM16, Theorem 5.8.1].

Theorem 2.10. If \( q \equiv 1 \pmod{4} \), then \( P_q \) is a strongly regular \( (q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4}) \) graph. Moreover, the eigenvalues of \( P_q \) are \( \frac{q-1}{2} \) (with multiplicity 1), \( \frac{1}{2}(-1 \pm \sqrt{q}) \) (each with multiplicity \( \frac{q-1}{2} \)).

The following theorem, due to Brouwer, Wilson, and Xiang [BWX99], constructs a family of strongly regular Cayley graphs from union of semi-primitive cyclotomic classes. Recently, Feng and Xiang [FX12] gave constructions of strongly regular Cayley graphs by using union of cyclotomic classes and index 2 Gauss sums. For other constructions we refer to the survey [Xia12].

Theorem 2.11 ([BWX99, Theorem 2]). Let \( q = p^{2tr} \), where \( p \) is an odd prime such that \( t \) is the smallest integer satisfying \( p^t \equiv -1 \pmod{N} \). Choose \( m \) with \( 1 \leq m \leq N - 1 \) and \( D \) be a union of \( m \) distinct \( N \)-th cyclotomic classes. Then the graph \( Y = \text{Cay}(\mathbb{F}_q^+, D) \) is strongly regular with eigenvalues \( k = \frac{m}{N}(q - 1) \) (with multiplicity 1), \( \theta_1 = \frac{m}{N}(-1 + (-1)^r \sqrt{q}) \) (with multiplicity \( q - 1 - k \)) and \( \theta_2 = \frac{m}{N}(-1 + (-1)^r \sqrt{q}) + (-1)^{r+1} \sqrt{q} \) (with multiplicity \( k \)).

Weng, Qiu, Wang, and Xiang [WQWX07] first introduced the definition of pseudo-Paley graphs.

Definition 2.12 (Pseudo-Paley graph). A pseudo-Paley graph is a strongly regular graph with the same parameters \( n, k, \lambda, \mu \) as a Paley graph.

For (primitive) strongly regular graphs, there is a one-to-one correspondence between the spectra of the adjacency matrix and the parameters \( (n, k, \lambda, \mu) \); see for example [GM16, Section 5.2]. Thus, pseudo-Paley graphs can be alternatively defined as those graphs having the same multi-set of eigenvalues as the Paley graph. The following lemma explains the significance of the semi-primitive case, and justifies the notation \( PP(q, 2d, I) \).

Lemma 2.13 (Pseudo-Paley graphs from unions of semi-primitive cyclotomic classes). Let \( p \) be a prime such that \( t \) is the smallest integer such that \( p^t \equiv -1 \pmod{2d} \). If \( q = p^{2tr} \), then \( PP(q, 2d, I) \) is a pseudo-Paley graph for any \( I \subset \{0, 1, \ldots, 2d - 1\} \) with \( |I| = d \).

Proof. We apply Theorem 2.11 by setting \( N = 2d \) and \( m = d \) to find the eigenvalues \( k, \theta_1, \theta_2 \). The values we obtain are exactly the parameters described in Theorem 2.10, as desired.

There are many examples of pseudo-Paley graphs that are not isomorphic to the Paley graph. See Proposition 6.7 for a criterion on the set \( I \) such that \( PP(q, 2d, I) \not\cong P_q \).

One of our aims in the present paper is to draw parallels between Paley graphs and the graphs of the form \( PP(q, 2d, I) \). Lemma 2.13 already shows one such commonality. Another special property Paley graphs enjoy is the following “equal contribution” statement. Our main result, Theorem 1.2, extends this property to a larger family of pseudo-Paley graphs.

Lemma 2.14. Let \( X = PP(q, 2d, I) \) be a semi-primitive pseudo-Paley graph with \( q = p^{2rt} \) where \( r \) is even and \( I = \{0, 2, \ldots, 2d - 2\} \), so that \( X \) is the Paley graph \( P_q \). If \( A \) is a maximum clique in \( X \) such that \( 0 \in A \), then

\[
|A \cap C_0| = |A \cap C_2| = \cdots = |A \cap C_{2d-2}| = \frac{\sqrt{q} - 1}{d}.
\]
Proof. Note that \( g^{p^t+1} \) is a primitive root of the subfield \( \mathbb{F}_{\sqrt{q}} \). Since \( p^t \equiv -1 \pmod{2d} \) and \( r \) is even, \( p^t+1 \equiv 2 \pmod{2d} \). Let \( A \) be a maximum clique in \( X \) such that \( 0 \in A \). Since \( 0 \in A \), by Theorem 1.1, \( A = a\mathbb{F}_{\sqrt{q}} \) for some square \( a \in \mathbb{F}_q^* \). Observe that for each \( 0 \leq j \leq d-1 \),

\[
\mathbb{F}_{\sqrt{q}} \cap C_{2j} = \{(g^{p^t+1})^k : k \equiv j \pmod{d}\} \Rightarrow |\mathbb{F}_{\sqrt{q}} \cap C_{2j}| = \frac{\sqrt{q}-1}{d}. \tag{3}
\]

The same conclusion holds for \( A = a\mathbb{F}_{\sqrt{q}} \).

From Lemma 2.14, we see that the subfield \( \mathbb{F}_{\sqrt{q}} \) admits the following presentation

\[
\mathbb{F}_{\sqrt{q}} = \{0\} \cup \bigcup_{j=0}^{d-1} \{(g^{p^t+1})^k : k \equiv j \pmod{d}\} = \{0\} \cup \bigcup_{j=0}^{d-1} g^{2j} \langle g^{d(\sqrt{q}+1)} \rangle.
\]

This motivates the following construction of a set in \( PP(q, 2d, I) \):

\[
A(q, 2d, I) = \{0\} \cup \bigcup_{j=1}^{d} g^{m_j} \langle g^{d(\sqrt{q}+1)} \rangle. \tag{4}
\]

The following lemma shows this “naive construction” of \( A(q, 2d, I) \) does not give a clique in \( PP(q, 2d, I) \) with the exception of the Paley graph.

**Lemma 2.15.** Let \( X = PP(q, 2d, I) \) be a semi-primitive pseudo-Paley graph with \( q = p^{2rt} \) where \( r \) is even. Then \( A(q, 2d, I) \) defined in equation (4) is a clique in \( X \) if and only if \( I = \{0, 2, \ldots, 2d-2\} \) or \( I = \{1, 3, \ldots, 2d-1\} \).

**Proof.** If \( I = \{0, 2, \ldots, 2d-2\} \), then the conclusion follows from Lemma 2.14. The case \( I = \{1, 3, \ldots, 2d-1\} \) is similar.

Conversely, assume that \( I \) is different from \( \{0, 2, \ldots, 2d-2\} \) and \( \{1, 3, \ldots, 2d-1\} \). Given \( X = PP(q, 2d, I) \), we may assume without loss of generality that \( X \) is already in its minimal representation: indeed, if \( PP(q, 2d, I) = PP(q, 2d', I') \), then \( A(q, 2d', I') = A(q, 2d, I) \). By hypothesis, \( d \geq 2 \), and by Remark 2.4, we may assume that \( m_1 = 0 \).

Assume, to the contrary, that \( A(q, 2d, I) \) is a clique in \( X \). Let \( B_j = A(q, 2d, I) \cap (C_j \cup \{0\}) \) for each \( 0 \leq j \leq 2d-1 \). If \( x, y \in B_0 \) such that \( x - y \in C_k \) with \( 0 \leq k \leq 2d-1 \), then for each \( 1 \leq j \leq d \), we have \( g^{m_j} x, g^{m_j} y \in B_{m_j} \) and \( g^{m_j} x - g^{m_j} y \in C_{k+m_j} \). As a result, \( I + k = \{m_j + k \pmod{2d} : 1 \leq j \leq d\} = I \). By Lemma 2.7, \( 2d|k \) as \( PP(q, 2d, I) \) is the minimal representation of \( X \). Thus, \( k = 0 \) and \( B_0 - B_0 \subset B_0 \).

From \( B_0 - B_0 \subset B_0 \) we infer that \( B_0 \) is a subgroup of \( \mathbb{F}_q^+ \), and must have cardinality \( |B_0| = p^n \) for some \( n \geq 1 \). We show this is impossible by analyzing the equation:

\[
\frac{\sqrt{q}-1}{d} + 1 = |B_0| = p^n.
\]

Writing \( \sqrt{q} = p^t \), and rearranging the equation, we obtain \( p^t - 1 = d(p^n - 1) \). In particular, \( (p^n - 1) \mid (p^t - 1) \) and so \( n \mid rt \) and also \( n < rt \). As \( n \mid rt \), this yields \( d = 1 \pmod{p^n} \). Since \( p^t \equiv 1 \pmod{2d} \), we have \( p^t \geq 2d + 1 \). Combining \( d \leq \frac{1}{2}(p^t - 1) \) and \( p^t - 1 = d(p^n - 1) \), we must have \( n > (r - 1)t \), contradicting \( n \mid rt \). This shows that \( A(q, 2d, I) \) is not a clique in \( X \). \( \square \)

We will later see in Theorem 1.8 how Lemma 2.15 can help us distinguish \( X \) from the Paley graph.
2.4. Known results on the clique number. Delsarte, in his influential Ph.D. thesis [Del73], proved linear programming bounds for subsets in an association scheme. In particular, for a strongly regular graph, we have the following Delsarte bound on the clique number.

**Theorem 2.16** (Delsarte bound). For a $k$-regular strongly regular graph $Y$ with smallest eigenvalue $\alpha < 0$, we have $\omega(Y) \leq 1 - k/\alpha$.

**Corollary 2.17.** Let $p$ be a prime such that $t$ is the smallest integer such that $p^t \equiv -1 \pmod{2d}$. If $q = p^{2t}$, then $X = PP(q, 2d, I)$ is a pseudo-Paley graph with $\omega(X) \leq \sqrt{q}$.

**Proof.** By Lemma 2.13, $X$ is a pseudo-Paley graph. Thus $X$ is $\frac{q-1}{2}$-regular and the smallest eigenvalue of $X$ is $\frac{1}{2} \left(-1 - \sqrt{q}\right)$ by Theorem 2.10. Theorem 2.16 implies that

$$
\omega(X) \leq 1 - \frac{\frac{q-1}{2}}{\frac{1}{2} \left(-1 - \sqrt{q}\right)} = 1 + \left(\sqrt{q} - 1\right) = \sqrt{q}.
$$

We will call $\sqrt{q}$ the trivial upper bound (on the clique number) of a graph $PP(q, 2d, I)$. It is interesting to see if the trivial upper bound can be improved, or to classify maximum cliques if the trivial upper bound is tight.

In general, it is difficult to improve the Delsarte bound. Recently, a minor improvement on the Delsarte bound (from $\sqrt{q}$ to $\sqrt{q} - 1$) has been made by Greaves and Soicher [GS18] for infinitely many strongly regular graphs with non-square order, including infinitely many pseudo-Paley graphs with non-square order. It is notoriously difficult to improve the trivial upper bound $\sqrt{q}$ for $\omega(P_q)$. Recently, Hanson and Petridis [HP21] and the second author [Yip22] improved the $\sqrt{q}$ bound to $\sqrt{q}/2(1 + o(1))$ for $\omega(P_q)$ when $q$ is a non-square using Stepanov’s method. A similar method can be used to improve the bound on $\omega(GP(q, d))$ when $q$ is a non-square [HP21, Yip22, Yip21c]. This is still far from the conjectured bound $O(q^t)$ or even $O((\log q)^2)$; see the related discussion in [Yip22, Section 1] and [Yip21a, Section 1.3].

In this paper, we are mostly focusing on the case when $q$ is square. In general, it is hard to improve even the trivial upper bound $\sqrt{q}$ since it is possibly tight. For generalized Paley graphs with square order, the second author [Yip21a] used Gauss sums and character sums to establish a necessary and sufficient condition for $\omega(GP(q, d)) = \sqrt{q}$ to hold. In the current paper, we will borrow some ideas from [Yip21a]. Since we work with unions of copies of generalized Paley graphs of square order, it is even harder to check if the trivial upper bound is tight. We improve the trivial upper bound by 1 conditionally in Theorem 1.5. On the other hand, Proposition 1.7 and Theorem 1.2 unconditionally refine Corollary 2.17.

Regarding Peisert graphs, the best known upper bound on $\omega(P_q^{*})$ is still $\sqrt{q}$. Kisielewicz and Peisert [KP04, Theorem 5.1] showed that $\omega(P_{p^{2r}}^{*}) = p^r$ when $r$ is odd and $p^{r/2} \leq \omega(P_{p^{2r}}^{*}) \leq p^r$ when $r$ is even. When $r$ is even, Mullin [Mul09, Section 3.4] computed that $\omega(P_{p^{2r}}^{*}) = 9$ and $\omega(P_{2401}^{*}) = 17$. For Peisert graphs with large order, we do not know the right magnitude of their clique number. The second author [Yip21b, Conjecture 4.3] conjectured that $\omega(P_{p^{2r}}^{*}) < p^r$ when $r$ is even and $p^r > 9$. We prove this conjecture conditionally for the case $r = 2$ in Theorem 1.6.

3. Gauss sums and character sums

In this section, we work with Gauss sums and character sums over finite fields. We refer to [BEW98] and [LN97, Chapter 5] for a detailed discussion.
Theorem 3.2 implies that \( \chi \) is odd, then \( d \) follows from Theorem 3.2.

Theorem 3.5 using the connection between Gauss sums and maximum cliques in generalized Paley graphs.

\[ \theta \] is the canonical additive character \( e_p \) (\cite[Theorem 11.5.4]{BEW98}).

Proof. \[ \psi \] is understood according to the following classical theorem.

\[ \chi \] is the first non-trivial example is when \( \chi \) is a quadratic character; in this case, the Gauss sum is well-understood according to the following classical theorem.

**Theorem 3.2** (\cite[Theorem 11.5.4]{BEW98}). Let \( F_q \) be a finite field with \( q = p^s \), where \( p \) is an odd prime and \( s \) is a positive integer. Let \( \chi \) be the quadratic character of \( F_q \). Then

\[ G(\chi, \psi) = \sum_{c \in F_q} \chi(c) \psi(c). \]  

**Corollary 3.3.** Suppose \( p \) is a prime such that \( p^t \equiv -1 \) (mod \( 2d \)) with \( t \) minimal. Let \( q = p^{2rt} \), where \( r \) is even. If \( \chi \) be the quadratic character of \( F_q \), then \( G(\chi) = -\sqrt{q} \).

**Proof.** We can write \( q = p^s \) where \( s = 2rt \). Note that \( i^{2rt} = 1 \) since \( r \) is even. The corollary follows from Theorem 3.2.

**Corollary 3.4.** Suppose \( p \) is a prime such that \( p^t \equiv -1 \) (mod \( 2d \)) with \( t \) minimal. Let \( q = p^{2rt} \), where \( r \) is odd. Let \( \chi \) be the quadratic character of \( F_q \). If \( p^t \equiv -1 \) (mod \( 4d \)) or \( d \) is even, then \( G(\chi) = \sqrt{q} \); if \( p^t \equiv 2d - 1 \) (mod \( 4d \)) and \( d \) is odd, then \( G(\chi) = -\sqrt{q} \).

**Proof.** If \( p^t \equiv -1 \) (mod \( 4d \)) or \( d \) is even, then \( p^t \equiv 3 \) (mod \( 4 \)), and so \( p \equiv 3 \) (mod \( 4 \)). So, Theorem 3.2 implies that \( G(\chi) = (-1)^{2rt-1}i^{2rt} \sqrt{q} = \sqrt{q} \). If \( p^t \equiv 2d - 1 \) (mod \( 4d \)) and \( d \) is odd, then \( p^t \equiv 1 \) (mod \( 4 \)). If \( p \equiv 1 \) (mod \( 4 \)), then Theorem 3.2 implies that \( G(\chi) = (-1)^{2rt-1} \sqrt{q} = -\sqrt{q} \); if \( p \equiv 3 \) (mod \( 4 \)), then \( t \) must be even, and so Theorem 3.2 implies that \( G(\chi) = (-1)^{2rt-1}i^{2rt} \sqrt{q} = -\sqrt{q} \) as \( 2t \) is divisible by 4. In all cases, we get \( G(\chi) = -\sqrt{q} \).

Stickelberger’s theorem (see for example \cite[Theorem 11.6.3]{BEW98}) provides an explicit formula to compute semi-primitive Gauss sums. The original proof by Stickelberger \cite{Sti90} was based on algebraic geometry. The second author \cite{Yip21a} recently provided a new simple proof using the connection between Gauss sums and maximum cliques in generalized Paley graphs.

**Theorem 3.5** (Stickelberger’s theorem). Let \( p \) be an odd prime and let \( d > 2 \) be an integer. Suppose there exists a positive integer \( t \) such that \( -1 \equiv p^t \) (mod \( d \)), with \( t \) chosen minimal. Let \( \chi \) be a multiplicative character of \( F_{p^d} \) with order \( d \). Then \( v = 2ts \) for some positive integer \( s \), and

\[ p^{-v/2}G(\chi) = (-1)^{s-1+(p^t+1)s/d}. \]
Corollary 3.6. Let \( q = p^{2rt} \), where \( p^t \equiv -1 \pmod{2d} \) is a prime with \( t \) minimal. Let \( \chi \) be a multiplicative character in \( \mathbb{F}_q \) with order \( 2d \). Then for each \( 1 \leq k \leq 2d-1 \),

(1) \( G(\chi^k) = -\sqrt{q} \) if \( r \) is even;

(2) \( G(\chi^k) = \sqrt{q} \) if \( r \) is odd and \( p^t \equiv -1 \pmod{4d} \);

(3) \( G(\chi^k) = (-1)^k \sqrt{q} \) if \( r \) is odd and \( p^t \equiv 2d-1 \pmod{4d} \).

Proof. When \( k = d \), then \( \chi^d \) is the quadratic character. We consider three cases:

(i) if \( r \) is even, then \( G(\chi^d) = -\sqrt{q} \) by Corollary 3.3.

(ii) if \( r \) is odd and \( p^t \equiv -1 \pmod{4d} \), then \( G(\chi^d) = \sqrt{q} \) by Corollary 3.4.

(iii) if \( r \) is odd and \( p^t \equiv 2d-1 \pmod{4d} \), then we have two subcases.

(a) if \( d \) is even, then \( G(\chi) = \sqrt{q} = (-1)^d \sqrt{q} \) by Corollary 3.4.

(b) if \( d \) is odd, then \( G(\chi) = -\sqrt{q} = (-1)^d \sqrt{q} \) by Corollary 3.4.

Next we assume that \( d \nmid k \). Then \( \chi^k \) is a character with order \( e = 2d/\gcd(2d,k) > 2 \), where \( e \mid 2d \). Since \(-1\) is a power of \( p \pmod{2d} \), \(-1\) is also a power of \( p \pmod{e} \). Let \( t' \) be the smallest positive integer such that \( p^t \equiv -1 \pmod{e} \); then it is easy to check that the order of \( p \pmod{e} \) is \( 2t' \). Note that \( p^t \equiv -1 \pmod{2d} \), in particular, \( p^t \equiv -1 \pmod{e} \) and \( p^{t-t'} \equiv 1 \pmod{e} \). Thus, \( 2t' \mid (t-t') \) so that \( t/t' \) is an odd integer. Let \( r' \) be defined by the equation \( r't = r't' \) so that \( q = p^{2rt} = p^{2t'r'} \). It is clear that \( r \) and \( r' \) have the same parity.

We claim that \( p^t \equiv p^{r'} \pmod{2e} \). We consider two cases.

(i) Suppose that \( p^t \equiv -1 \pmod{2e} \). Since \( t/t' \) is odd, we also have \( p^t \equiv -1 \pmod{2e} \).

(ii) Suppose that \( p^t \equiv e-1 \pmod{2e} \).

(a) When \( e \) is even, observe that \( (e-1)^2 \equiv 1 \pmod{2e} \), and so \( (e-1)^{t/t'} \equiv e-1 \pmod{2e} \).

(b) When \( e \) is odd, \( (e-1)^2 \equiv e^2 + 1 \equiv e + 1 \pmod{2e} \); now, \( (e+1)^2 \equiv e^2 + 1 \equiv e + 1 \pmod{2e} \) and so \( (e-1)^{t/t'} \equiv (e+1)(e-1) \equiv e^2 - 1 \equiv e - 1 \pmod{2e} \).

In both sub-cases, \( (e-1)^{t/t'} \equiv e - 1 \pmod{2e} \). As a result, \( p^t \equiv e - 1 \pmod{2e} \).

This proves the claim. Consequently,

(i) If \( p^t \equiv -1 \pmod{4d} \), then \( p^t \equiv p^{r'} \equiv -1 \pmod{2e} \).

(ii) If \( p^t \equiv 2d-1 \pmod{4d} \), then we consider two subcases.

(a) if \( e \mid d \) (i.e., \( k \) is even), then \( p^{r'} \equiv p^t \equiv -1 \pmod{2e} \).

(b) if \( e \nmid d \) (i.e., \( k \) is odd), then \( p^{r'} \equiv p^t \equiv e - 1 \pmod{2e} \).

Finally, we apply Theorem 3.5 to obtain:

\[
G(\chi^k)/\sqrt{q} = (-1)^{r'-1+(p^{r'}+1)r}/e = \begin{cases} \((-1)^{r'-1} = (-1)^{r-1} = -1 \quad \text{in case (1)} \\ (-1)^{r'-1} = (-1)^{r-1} = 1 \quad \text{in case (2)} \\ (-1)^k \quad \text{in case (3)} \end{cases}
\]

as desired. \( \square \)

Weil sums are complete character sums with polynomial arguments. In general, it is difficult to evaluate a Weil sum explicitly. Luckily, a Weil sum with a monomial argument is known to be a linear combination of Gauss sums.
Corollary 3.8. Let $G$ be a multiplicative character of $\mathbb{F}_q$, $n \in \mathbb{N}$, and $\chi$ a multiplicative character of $\mathbb{F}_q$ of order $e = \gcd(n, q - 1)$. Then for any $a \in \mathbb{F}_q^*$,

$$\sum_{c \in \mathbb{F}_q} \psi(ac^n) = \sum_{j=1}^{e-1} \chi^j(a)G(\chi^j, \psi).$$

As an application of Theorem 3.7, we obtain the following result.

**Corollary 3.8.** Let $q = p^{2r}$, where $p^t \equiv -1 \pmod{2d}$ is a prime with $t$ minimal and $r$ is even. Let $C_0, C_1, \ldots, C_{2d-1}$ be the list of 2d-th cyclotomic classes of $\mathbb{F}_q$. Then

$$\sum_{c \in C_0} e_p(\text{Tr}_{\mathbb{F}_q}(c)) = -\frac{(2d - 1)\sqrt{q} + 1}{2d}, \quad \text{and} \quad \sum_{c \in C_k} e_p(\text{Tr}_{\mathbb{F}_q}(c)) = \frac{\sqrt{q} - 1}{2d}$$

for each $1 \leq k \leq 2d - 1$.

**Proof.** Let $\psi$ denote the canonical additive character of $\mathbb{F}_q$ and let $\chi$ be a multiplicative character such that $\chi(g) = \theta$, where $\theta$ is a primitive 2d-th root of unity. Then $\chi$ has order 2d, and $\chi^d$ is the quadratic character. By Corollary 3.3, $G(\chi^d) = -\sqrt{q}$ since $r$ is even. Together with Corollary 3.6, we conclude that $G(\chi^d) = -\sqrt{q}$ for each $1 \leq j \leq 2d - 1$.

Using Theorem 3.7 with $n = c = 2d$, for any $a \in \mathbb{F}_q^*$, we have

$$\sum_{c \in \mathbb{F}_q} e_p(\text{Tr}_{\mathbb{F}_q}(ac^{2d})) = \sum_{j=1}^{2d-1} \chi^j(a)G(\chi^j) = -\sqrt{q} \sum_{j=1}^{2d-1} \bar{\chi}^j(a) = \sqrt{q} - \sqrt{q} \sum_{j=0}^{2d-1} \bar{\chi}^j(a). \quad (6)$$

By the orthogonality relations,

$$\sum_{j=0}^{2d-1} \bar{\chi}^j(a) = \begin{cases} 1 & \text{if } a = 1 \\ 0 & \text{if } a \neq 1 \end{cases} \quad (7)$$

Combining (6) and (7), we obtain

$$\sum_{c \in \mathbb{F}_q} e_p(\text{Tr}_{\mathbb{F}_q}(c^{2d})) = -(2d - 1)\sqrt{q}, \quad \text{and} \quad \sum_{c \in \mathbb{F}_q} e_p(\text{Tr}_{\mathbb{F}_q}(g^k c^{2d})) = \sqrt{q}$$

for each $1 \leq k \leq 2d - 1$. The desired conclusion follows immediately from $e_p(\text{Tr}_{\mathbb{F}_q}(0)) = 1$. \qed

The following lemma allows us to compute character values using the associated Gauss sum.

**Lemma 3.9** ([LN97, Theorem 5.12]). Let $\chi$ be a multiplicative character of $\mathbb{F}_q$. Then for any $a \in \mathbb{F}_q$,

$$\overline{\chi(a)} = \frac{1}{G(\chi)} \sum_{c \in \mathbb{F}_q} \chi(c)e_p(\text{Tr}_{\mathbb{F}_q}(ac)).$$

**Lemma 3.10.** Let $q$ be an odd prime power. Let $A$ be a subset of $\mathbb{F}_q$, and let $\chi$ be a nontrivial multiplicative character of $\mathbb{F}_q$. Then

$$\sum_{a,b \in A} \chi(a-b) = \frac{1}{G(\chi)} \sum_{c \in \mathbb{F}_q} \chi(c)|S(q, A; c)|^2.$$
Proof. Recall that the trace map is linear. By Lemma 3.9,
\[
\sum_{a,b \in A} \chi(a-b) = \sum_{a,b \in A} \frac{1}{G(\chi)} \sum_{c \in \mathbb{F}_q^*} \chi(c) e_p(\text{Tr}_{\mathbb{F}_q}(a-b)c)
\]
\[
= \frac{1}{G(\chi)} \sum_{c \in \mathbb{F}_q^*} \chi(c) \left( \sum_{a,b \in A} e_p(\text{Tr}_{\mathbb{F}_q}(a-b)c) \right) \left( \sum_{b \in A} e_p(\text{Tr}_{\mathbb{F}_q}(-bc)) \right)
\]
\[
= \frac{1}{G(\chi)} \sum_{c \in \mathbb{F}_q^*} \chi(c) \left( \sum_{a \in A} e_p(\text{Tr}_{\mathbb{F}_q}(ac)) \right) \left( \sum_{b \in A} e_p(-\text{Tr}_{\mathbb{F}_q}(bc)) \right)
\]
\[
= \frac{1}{G(\chi)} \sum_{c \in \mathbb{F}_q^*} \chi(c) |S(q, A; c)|^2.
\]
\qed

Recall that \(S(q, A; c)\) is a scaled Fourier coefficient of the indicator function on \(A\). Thus, Plancherel’s identity implies the following lemma; see for example [Yip21a, Lemma 4.1].

**Lemma 3.11.** For any \(A \subset \mathbb{F}_q\),
\[
\sum_{c \in \mathbb{F}_q^*} |S(q, A; c)|^2 = q|A| - |A|^2,
\]
where \(S(q, A; c)\) is defined in equation (5).

The following theorem is a consequence of the main result in a recent paper by Reis [Rei20]. It states that there will be a lot cancellation in a character sum over a generic subspace \(V\) of \(\mathbb{F}_q\) provided that \(V\) is not the subfield \(\mathbb{F}_q^{\sqrt{q}}\). Consequently, if the character sum over a subset \(S\) is too large, then we can conclude that either \(S\) is not a subspace or \(S\) is the subfield \(\mathbb{F}_q^{\sqrt{q}}\). The first alternative in the previous sentence will be the key to prove Theorem 1.5. We also remark that the second alternative (the subfield case) was one of the main tools used in our previous paper [AY21].

**Theorem 3.12** ([AY21, Corollary 3.6]). Let \(n\) be an integer such that \(n \geq 2\), and \(q\) an odd prime power. Let \(V \subseteq \mathbb{F}_{q^n}\) be an \(\mathbb{F}_q\)-space of dimension \(n\), with \(1 \in V\), and \(V \neq \mathbb{F}_q^n\). Then for any non-trivial multiplicative character \(\chi\) of \(\mathbb{F}_{q^n}\),
\[
\left| \sum_{x \in V} \chi(x) \right| < \frac{2n}{\sqrt{q}} \cdot |V|.
\]  

4. PROOF OF THEOREM 1.2

In this section, we first prove Proposition 1.7 on the characterization of maximum cliques, and then use it to prove our main result Theorem 1.2.

**Proof.** Let \(A\) be a maximum clique in \(X\). Our aim is to show the following two statements:

1. \(|A| \leq \sqrt{q}\);
2. \(|A| = \sqrt{q}\) if and only if \(S(q, A; c) = 0\) for all \(c \in B\).
We have seen earlier in Corollary 2.17 that (1) can be proved independently using algebraic graph theory. The proof given here is genuinely different, and we include it as (1) and (2) naturally fit together. In the following, we use \( S(c) \) to denote \( S(q, A; c) \) for each \( c \in \mathbb{F}_q^{*} \), and use \( T_k = \sum_{c \in C_k} |S(c)|^2 \) as a shorthand for each \( 0 \leq k \leq 2d - 1 \).

Let \( \theta \) be a primitive \( 2d \)-th root of unity. Let \( \chi \) be the multiplicative character of \( \mathbb{F}_q \) such that \( \chi(g) = \theta \). Consider the following interpolation function \( f : \mathbb{F}_q \to \mathbb{R} \) defined by,

\[
  f(x) = \sum_{j=0}^{2d-1} c_j \chi^j(x), \quad \forall x \in \mathbb{F}_q
\]

where

\[
  c_j = \sum_{\ell=1}^{d} \theta^{jm_\ell}.
\]

We claim that

\[
  f(x) = \begin{cases} 
    2d, & \text{if } x \in D, \\
    0, & \text{if } x \notin D,
  \end{cases} 
\]

where \( D \) is defined in equation (2). To prove this claim, recall the orthogonality relations for the group of order \( |G| = 2d \) generated by the character \( \chi \):

\[
  \frac{1}{2d} \sum_{j=0}^{2d-1} \chi^j(g^k)\chi^j(g^\ell) = \begin{cases} 
    1 & \text{if } k = \ell, \\
    0 & \text{if } k \neq \ell.
  \end{cases}
\]

Next,

\[
  f(x) = \sum_{j=0}^{2d-1} \left( \sum_{\ell=1}^{d} \theta^{jm_\ell} \right) \chi^j(x) = \sum_{j=0}^{2d-1} \left( \sum_{\ell=1}^{d} \chi^j(g^{m_\ell}) \right) \chi^j(x) = \sum_{\ell=1}^{d} \left( \sum_{j=0}^{2d-1} \chi^j(g^{m_\ell}) \chi^j(x) \right).
\]

Given \( x \in D \), we have \( x = g^{2dk+m_\ell} \) for some \( k \geq 0 \) and for some \( 1 \leq \ell \leq d \); in this case, there will be exactly one non-zero inner sum, and so \( f(x) = f(g^{m_\ell}) = 2d \). If \( x = 0 \), then \( f(x) = 0 \). Given \( x \notin D \) such that \( x \neq 0 \), we have \( x = g^{2dk+m} \) for some \( k \geq 0 \) and \( m \neq m_\ell \) for any \( \ell \); in this case, all the inner sums will vanish and we get \( f(x) = f(g^m) = 0 \), establishing the claim above.

Since \( A \) is a clique, for any \( a, b \in A \), if \( a \neq b \), we have \( a - b \in D \); otherwise \( f(a-b) = 0 \). Thus, equation (9) implies that

\[
  \sum_{a,b \in A} f(a-b) = 2d(|A|^2 - |A|). 
\]

On the other hand, using Lemma 3.10, we have

\[
  \sum_{a,b \in A} f(a-b) = \sum_{a,b \in A} \sum_{j=0}^{2d-1} c_j \chi^j(a-b)
\]

\[
= \sum_{a,b \in A} c_0 \chi^0(a-b) + \sum_{j=1}^{2d-1} \sum_{a,b \in A} c_j \chi^j(a-b)
\]

\[
= d(|A|^2 - |A|) + \sum_{j=1}^{2d-1} \frac{c_j}{G(\chi^j)} \left( \sum_{c \in \mathbb{F}_q^{*}} \chi^j(c) |S(c)|^2 \right)
\]

16
\[ d(|A|^2 - |A|) + \sum_{j=1}^{2d-1} c_j G(\chi^j) \left( \sum_{k=0}^{2d-1} \sum_{c \in C_k} \chi^j(c) \left| S(c) \right|^2 \right) \]
\[ = d(|A|^2 - |A|) + \sum_{j=1}^{2d-1} c_j G(\chi^j) \left( \sum_{k=0}^{2d-1} \theta^{jk} T_k \right). \]

Next we proceed according to the sign of Gauss sums \( G(\chi^j) \) listed in Corollary 3.6.

**Case 1.** \( r \) is even.

In this case, by Corollary 3.6, \( G(\chi^j) = -\sqrt{q} \) for each \( 1 \leq j \leq 2d - 1 \). Thus,
\[ \sum_{a,b \in A} f(a - b) = d(|A|^2 - |A|) - \frac{1}{\sqrt{q}} \sum_{k=0}^{2d-1} \left( \sum_{j=1}^{2d-1} c_j \theta^{jk} \right) T_k. \] (11)

Observe that
\[ \sum_{j=1}^{2d-1} c_j \theta^{jk} = \sum_{j=1}^{2d-1} \sum_{\ell=1}^{d} \theta^{jm_\ell} \theta^{jk} = \sum_{\ell=1}^{d} \sum_{j=1}^{2d-1} \theta^{jm_\ell+k} \]
\[ = -d + \sum_{\ell=1}^{d} \sum_{j=0}^{2d-1} \theta^{jm_\ell+k} \]
\[ = \begin{cases} d, & \text{if } k \equiv -m_1, -m_2, \ldots, -m_d \pmod{2d}, \\ -d, & \text{otherwise}. \end{cases} \] (12)

For the last step, we used the following elementary fact based on the geometric series:
\[ \sum_{j=0}^{2d-1} \theta^{jm_\ell} = \begin{cases} 0 & \text{if } \ell \not\equiv 0 \pmod{2d}, \\ 2d & \text{if } \ell \equiv 0 \pmod{2d}. \end{cases} \]

Combining equations (11) and (12), we obtain that
\[ \sum_{a,b \in A} f(a - b) = d(|A|^2 - |A|) - \frac{d}{\sqrt{q}} \sum_{k \neq -m_\ell} T_k - \frac{d}{\sqrt{q}} \sum_{\ell=1}^{d} T_{-m_\ell} \]
\[ \leq d(|A|^2 - |A|) + \frac{d}{\sqrt{q}} \sum_{k=0}^{2d-1} T_k \]
\[ = d(|A|^2 - |A|) + \frac{d}{\sqrt{q}} (q|A| - |A|^2). \]

In the last step, we used Lemma 3.11. Comparing the inequality above with equation (10), it follows that for a clique \( A \), we have \( |A|^2 - |A| \leq \frac{1}{\sqrt{q}} (q|A| - |A|^2) \), which implies that \( |A| \leq \sqrt{q} \).

This completes the proof of (1). Moreover, the equality \( |A| = \sqrt{q} \) holds if and only if
\( T_{-m_1} = T_{-m_2} = \ldots = T_{-m_d} = 0. \) (13)

This implies that \( S(q, A; c) = 0 \) for all \( c \in D' = \bigcup_{\ell=1}^{d} C_{-m_\ell} \), proving (2).

**Case 2.** \( r \) is odd and \( p^r \equiv 2d - 1 \pmod{4d} \).
In this case, by Corollary 3.6, $G(\chi^j) = (-1)^j \sqrt{q}$ for each $1 \leq j \leq 2d - 1$. Thus,

$$
\sum_{a,b \in A} f(a-b) = d(|A|^2 - |A|) + \frac{1}{\sqrt{q}} \sum_{k=0}^{2d-1} \left( \sum_{j=1}^{2d-1} (-1)^j c_j \theta^{jk} \right) T_k.
$$

Similar to Case 1, observe that $(-1)^j = (\theta^d)^j = \theta^{jd}$, and so

$$
\sum_{j=1}^{2d-1} (-1)^j c_j \theta^{jk} = \sum_{j=1}^{2d-1} c_j \theta^{j(k+d)} = \sum_{j=1}^{2d-1} \theta^{j(m_\ell+k+d)} = \sum_{\ell=1}^{d} \sum_{j=1}^{2d-1} \theta^{j(m_\ell+k+d)}
$$

$$
= -d + \sum_{\ell=1}^{d} \sum_{j=0}^{2d-1} \theta^{j(m_\ell+k+d)}
$$

$$
= \begin{cases} 
  d, & \text{if } k \equiv -m_1 - d, -m_2 - d, \ldots, -m_d - d \pmod{2d}, \\
  -d, & \text{otherwise}.
\end{cases}
$$

Continuing as in Case 1, we obtain

$$
\sum_{a,b \in A, a \neq b} f(a-b) = d(|A|^2 - |A|) - \frac{d}{\sqrt{q}} \sum_{k \neq -m_\ell - d} T_k + \frac{d}{\sqrt{q}} \sum_{\ell=1}^{d} T_{-m_\ell - d}
$$

$$
\leq d(|A|^2 - |A|) + \frac{d}{\sqrt{q}} \sum_{k=0}^{2d-1} T_k
$$

$$
= d(|A|^2 - |A|) + \frac{d}{\sqrt{q}} (q|A| - |A|^2).
$$

In the same way as before, we get $|A| \leq \sqrt{q}$. Moreover, the equality $|A| = \sqrt{q}$ holds if and only if $T_k = 0$ for each $k \neq -m_\ell - d$. This implies that $S(q, A; c) = 0$ for all $c \in \mathbb{F}_q^* \setminus D''$.

Case 3. $r$ is odd and $p^r \equiv -1 \pmod{4d}$.

In this case, by Corollary 3.6, $G(\chi^j) = \sqrt{q}$ for each $1 \leq j \leq 2d - 1$. Thus,

$$
\sum_{a,b \in A} f(a-b) = d(|A|^2 - |A|) + \frac{1}{\sqrt{q}} \sum_{k=0}^{2d-1} \left( \sum_{j=1}^{2d-1} c_j \theta^{jk} \right) T_k.
$$

The analysis is basically the same as the first case, and we obtain $|A| \leq \sqrt{q}$. Moreover, the equality $|A| = \sqrt{q}$ holds if and only if $T_k = 0$ for each $k \neq -m_\ell$. This implies that $S(q, A; c) = 0$ for all $c \in \mathbb{F}_q^* \setminus D'$.

\[ \square \]

Proof of Theorem 1.2. Let $A$ be a clique of size $\sqrt{q}$ such that $0 \in A$. Let $A_j = A \cap C_j$ for each $0 \leq j \leq 2d - 1$. Since $A$ is a clique in $X$ and $0 \in A$, we have $A \setminus \{0\} = \cup_{j=1}^{d} A_{m_j}$, and thus

$$
\sum_{j=1}^{d} |A_{m_j}| = \sqrt{q} - 1. \quad (14)
$$

By Proposition 1.7, $S(q, A; c) = 0$ for all $c \in D'$ where $D' = C_{m_1} \cup C_{m_2} \cup \cdots \cup C_{m_d}$. Without loss of generality, we may assume that $m_1 = 0$ (see Remark 2.4). In particular, we have
\[ S(q, A; c) = 0 \] for each \( c \in C_0 \), implying the following:

\[
0 = \sum_{c \in C_0} S(q, A; c) = \sum_{c \in C_0} \sum_{a \in A} e_p(\text{Tr}_{F_q}(ac)) = \sum_{a \in A} \sum_{c \in C_0} e_p(\text{Tr}_{F_q}(ac))
\]

\[
= |C_0| + \sum_{j=1}^{d} \sum_{a \in A_m, c \in C_0} e_p(\text{Tr}_{F_q}(ac)).
\]

Note that if \( a \in A_{m_j} \), then as \( c \) runs over \( C_0 \), \( ac \) runs over \( C_{m_j} \). Therefore,

\[
0 = |C_0| + \sum_{j=1}^{d} |A_{m_j}| \sum_{c \in C_{m_j}} e_p(\text{Tr}_{F_q}(c)).
\]

We can apply the similar argument to \( C_{-m_k} \) for each \( k \geq 2 \) to obtain:

\[
0 = \sum_{c \in C_{-m_k}} S(q, A; c) = \sum_{a \in A} \sum_{c \in C_{-m_k}} e_p(\text{Tr}_{F_q}(ac))
\]

\[
= |C_{-m_k}| + \sum_{j=1}^{d} |A_{m_j}| \sum_{c \in C_{m_j} - m_k} e_p(\text{Tr}_{F_q}(c)).
\]

Recall that the index \( j \) in \( C_j \) is defined up to modulo 2d, which allows us to consider \( C_{m_j - m_k} \) even when \( m_j - m_k < 0 \). For convenience, we define

\[
\lambda := \sum_{c \in C_0} e_p(\text{Tr}_{F_q}(c)), \quad \text{and} \quad \mu := \sum_{c \in C_k} e_p(\text{Tr}_{F_q}(c))
\]

for each \( 1 \leq k \leq 2d - 1 \). The value of \( \mu \) is well-defined in view of Corollary 3.8.

Given a fixed integer \( k \) satisfying \( 1 \leq k \leq d \), there is a unique value of \( j \) such that \( m_j - m_k \equiv 0 \) (mod 2d), namely, \( j = k \). Therefore, the equation

\[
0 = |C_{-m_k}| + \sum_{j=1}^{d} |A_{m_j}| \sum_{c \in C_{m_j} - m_k} e_p(\text{Tr}_{F_q}(c))
\]

becomes

\[
0 = |C_0| + \lambda |A_{m_k}| + \sum_{1 \leq j \leq d} \mu |A_{m_j}|
\]

(15)

where we also used the fact that \( |C_{-m_k}| = |C_0| \). Note that equation (15) is valid for each \( 1 \leq k \leq d \), and so these \( d \) linear equations correspond to the matrix equation \( Mx = b \) where

\[
M = \begin{pmatrix}
\lambda & \mu & \mu & \cdots & \mu \\
\mu & \lambda & \mu & \cdots & \mu \\
\mu & \mu & \lambda & \cdots & \mu \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\mu & \mu & \mu & \cdots & \lambda
\end{pmatrix}, \quad x = \begin{pmatrix}
|A_{m_1}| \\
|A_{m_2}| \\
|A_{m_3}| \\
\vdots \\
|A_{m_d}|
\end{pmatrix} \quad \text{and} \quad b = -\begin{pmatrix}
|C_0| \\
|C_0| \\
|C_0| \\
\vdots \\
|C_0|
\end{pmatrix}
\]

Note that \( M = (\lambda - \mu)I_d + \mu J_d \), where \( I_d \) is the \( d \times d \) identity matrix and \( J_d \) is the \( d \times d \) all 1’s matrix. It is straightforward to see that \( M \) has eigenvalue \( \lambda - \mu \) with multiplicity \( d - 1 \), and
eigenvalue $\lambda + (d - 1)\mu$ with multiplicity 1. By Corollary 3.8, we know that $\lambda \neq \mu$ and

$$\lambda + (d - 1)\mu = -\frac{(2d - 1)\sqrt{q} + 1}{2d} + (d - 1) \cdot \frac{\sqrt{q} - 1}{2d} = -\frac{\sqrt{q} + 1}{2}.$$

Therefore, $\mathbf{M}$ is invertible. Thus, $\mathbf{Mx} = \mathbf{b}$ has a unique solution given by

$$\mathbf{x} = \left( \begin{array}{c} \gamma \\ \gamma \\ \vdots \\ \gamma \end{array} \right),$$

where $\gamma = -|C_0|/(\lambda + (d - 1)\mu)$. We deduce that

$$|A_{m_j}| = \gamma = -\frac{|C_0|}{\lambda + (d - 1)\mu} = \frac{2|C_0|}{\sqrt{q} + 1} = \frac{2(q - 1)}{2d(\sqrt{q} + 1)} = \frac{\sqrt{q} - 1}{d}$$

for each $1 \leq j \leq d$. It is easy to verify that $|A_{m_1}|, |A_{m_2}|, \ldots, |A_{m_d}|$ satisfy the equation (14). \qed

Now that the main Theorem 1.2 is proved, we continue with an application on the number of maximum cliques. Recall that in the Paley graph $P_q$, there is a unique maximum clique that contains $\{0, 1\}$, namely the subfield $\mathbb{F}_{q^2}$. In contrast, Mullin [Mul09, Lemma 3.3.6] shows that if $r$ is even and $q = p^{2r}$ for some prime $p \equiv 3 \pmod{4}$ such that $\omega(P_q) = \sqrt{q}$, then there are at least 2 maximum cliques in $P_q^*$ that contains $\{0, 1\}$. We extend this result in the Theorem 1.8 and present the proof below.

**Proof of Theorem 1.8.** Suppose $\omega(X) = \sqrt{q}$, and that there is a unique maximum clique $A$ in $X$ that contains $\{0, 1\}$. We will show that $A = A(q, 2d, I)$ defined in equation (4), which contradicts Lemma 2.15 and thus establishes the theorem.

Let $A_j = A \cap C_j$ for each $0 \leq j \leq 2d - 1$. By Theorem 1.2, $|A_{m_j}| = \frac{\sqrt{q} - 1}{d}$ for each $1 \leq j \leq d$. For each $y \in A_0$, the map $x \mapsto y^{-1}x$ induces a graph automorphism of $X$, so $y^{-1}A$ is a maximum clique: moreover, $1 = y^{-1}y \in y^{-1}A$, and so $y^{-1}A = A$ by the uniqueness of the maximum clique containing $\{0, 1\}$. In particular, for each $x, y \in A_0$, we have $xy^{-1} \in y^{-1}A_0 = A_0$. Hence $A_0$ is a subgroup of $\mathbb{F}_q^*$. Since $|A_0| = \frac{\sqrt{q} - 1}{d}$, we conclude that $A_0 = \langle g^{d(\sqrt{q} + 1)} \rangle$. For each $1 \leq j \leq d$, we can apply the same argument to $g^{-m_j}A_{m_j}$ to conclude that $A_{m_j} = g^{m_j}\langle g^{d(\sqrt{q} + 1)} \rangle$. Therefore,

$$A = \{0\} \cup \bigcup_{j=1}^{d} A_{m_j} = \{0\} \cup \bigcup_{j=1}^{d} g^{m_j}\langle g^{d(\sqrt{q} + 1)} \rangle = A(q, 2d, I).$$

\qed

As an immediate consequence, we have the following characterization.

**Corollary 4.1.** Let $X = PP(q, 2d, I)$ be a semi-primitive pseudo-Paley graph with $q = p^{2rt}$ where $r$ is even. Then $X$ is isomorphic to the Paley graph $P_q$ if and only if $I = \{0, 2, \ldots, 2d - 2\}$ or $I = \{1, 3, \ldots, 2d - 1\}$.

**Proof.** If $I = \{0, 2, \ldots, 2d - 2\}$ or $I = \{1, 3, \ldots, 2d - 1\}$, then $X \cong P_q$ by Example 2.5.

Conversely, suppose that $I$ is different from $\{0, 2, \ldots, 2d - 2\}$ and $\{1, 3, \ldots, 2d - 1\}$. Assume, to the contrary, that $X$ is isomorphic to the Paley graph $P_q$. Then $\omega(X) = \sqrt{q}$. By Remark 2.4, we may assume that $0 \in I$. If $f : X \to P_q$ is a graph isomorphism, then after composing $f$ with a suitable automorphism $h : P_q \to P_q$, we may assume that $f(0) = 0$ and $f(1) = 1$. This would imply...
that the number of maximum cliques containing \( \{0,1\} \) must be the same in both graphs; however, there is a unique such maximum clique in \( P_2 \) by Theorem 1.1, while there are at least two such cliques in \( X \) by Theorem 1.8. This contradiction shows that \( X \) is not isomorphic to \( P_2 \). \( \Box \)

The corollary above shows that almost all the graphs of the form \( PP(q,2d,I) \) in the semi-primitive case are not isomorphic to the Paley graph. In Section 6, we will prove a stronger result without the semi-primitive assumption.

5. Subspace Structure of Maximum Cliques

The goal of this section is to prove three of our main results. In Section 5.1, we establish Theorem 1.9 which concerns the parity on the number of maximum cliques having a subspace structure. In Section 5.2, we discuss the density of the graphs achieving the trivial upper bound on the clique number. Finally, in Section 5.3, we prove Theorem 1.5 and Theorem 1.6, which improve the previously known upper bound \( \sqrt{q} \) on the clique number conditionally (assuming Conjecture 1.4).

5.1. Maximum Cliques Come in Pairs. We will see in this subsection that if \( X \) is a semi-primitive pseudo-Paley graph on \( q = p^{2rt} \) vertices with \( r \) even, is different from the Paley graph, then the maximum cliques of size \( \sqrt{q} \) in \( X \) with the subspace structure come in pairs. Furthermore, in each pair, the two maximum cliques are interchanged by the Galois automorphism \( x \mapsto x^q \).

**Lemma 5.1.** If \( p^t \equiv -1 \pmod{2d} \), and \( q = p^{2rt} \), then \( \mathbb{F}_{p^t}^* \subset C_0 = \langle g^{2d} \rangle \).

**Proof.** Note that \( g^k \) is a primitive root of \( \mathbb{F}_{p^t}^* \), where

\[
k = \frac{p^{2rt} - 1}{p^t - 1} = \sum_{j=0}^{2r-1} p^{jt} \equiv \sum_{j=0}^{2r-1} (-1)^j \equiv 0 \pmod{2d}
\]

since \( p^t \equiv -1 \pmod{2d} \). Thus, \( g^k \in \langle g^{2d} \rangle \), it follows that \( \mathbb{F}_{p^t}^* \subset C_0 \). \( \Box \)

The following lemma is a simple consequence of Theorem 1.2 and Lemma 2.14.

**Lemma 5.2.** Let \( X = PP(q,2d,I) \) be a semi-primitive pseudo-Paley graph with \( q = p^{2rt} \) where \( r \) is even, and \( I \neq \{0,2,\ldots,2d-2\} \). Then the subfield \( \mathbb{F}_{\sqrt{q}} \) is not a clique in \( X \).

**Proof.** If \( \mathbb{F}_{\sqrt{q}} \) were to be a clique in \( X \), then it would be a maximum clique. Comparing the two equations (1) and (3), we get \( I = \{0,2,\ldots,2d-2\} \), a contradiction. \( \Box \)

**Lemma 5.3.** Consider the finite field \( \mathbb{F}_q \) where \( q = p^{4t} \) and \( p^t \equiv -1 \pmod{2d} \). Let \( g \) be the primitive root of \( \mathbb{F}_q \) and \( C_0 = \langle g^{2d} \rangle \). Let \( x \in C_0 \). If \( \{x,x^{p^{2t}}\} \) is linearly dependent over \( \mathbb{F}_{p^t} \), then \( x \in \langle g^{(p^{2t}+1)d} \rangle \).

**Proof.** If \( \{x,x^{p^{2t}}\} \) is linearly dependent over \( \mathbb{F}_{p^t} \), then \( x^{p^{2t}-1} \in \mathbb{F}_{p^t}^* \). After expressing \( x = g^k \) for some integer \( k \), we obtain \( g^{(p^{2t}-1)k} \in \mathbb{F}_{p^t}^* \). As \( \mathbb{F}_{p^t}^* = \langle g^{(q-1)/(p^t-1)} \rangle \), and \( q = p^{4t} \) we must have

\[
\frac{q-1}{p^t-1} | (p^{2t}-1)k \Rightarrow (p^{2t}+1)(p^t+1) | (p^{2t}-1)k \Rightarrow p^{2t} + 1 | (p^t-1)k.
\]

Using \( \gcd(p^{2t} + 1,p^t - 1) = 2 \), we obtain \( \frac{p^{2t}+1}{2} | k \). Next, \( x = g^k \in C_0 = \langle g^{2d} \rangle \) implies that \( 2d | k \). We will now combine these two divisibility relations \( \frac{p^{2t}+1}{2} | k \) and \( 2d | k \).
Observe that \( p^t \equiv -1 \pmod{2d} \) implies \( p^{2t} \equiv 1 \pmod{4d} \), so that \( \frac{p^{2t}+1}{2} \equiv 1 \pmod{2d} \). Therefore, \( \gcd(\frac{p^{2t}+1}{2}, 2d) = 1 \). Combining \( \frac{p^{2t}+1}{2} \mid k \) and \( 2d \mid k \), we conclude \((p^{2t} + 1)d \mid k \) and hence \( x = g^k \in (g^{|p^{2t}+1|d})\).

\[ \square \]

Now we are ready to present the proof of Theorem 1.9.

**Proof of Theorem 1.9.** Without loss of generality, we may assume \( m_1 = 0 \); see Remark 2.4. By assumption, \( X \) is a Cayley graph on \( q = p^d \) many vertices where \( p^t \equiv -1 \pmod{2d} \). Note that the map \( f : \mathbb{F}_q \to \mathbb{F}_q \) given by \( f(x) = x^{\sqrt{q}} \) preserves the edges of the graph: if \( x, y \in \mathbb{F}_q \) and \( x - y \in D \), then

\[
f(x) - f(y) = x^{\sqrt{q}} - y^{\sqrt{q}} = (x - y)^{\sqrt{q}} \in D
\]

because \( \sqrt{q} = p^{2t} \equiv 1 \pmod{2d} \). Note that \( f \) fixes each element of \( \mathbb{F}_{\sqrt{q}} \) pointwise; in particular, \( f \) fixes \( \mathbb{F}_{p^t} \). It is also evident that \( f \) is a bijection on the vertex set \( \mathbb{F}_q \). We conclude that \( f \) is a graph automorphism of \( X \) which fixes \( \mathbb{F}_{p^t} \), and hence should send maximum cliques containing \( \mathbb{F}_{p^t} \) to maximum cliques containing \( \mathbb{F}_{p^t} \). Let \( A \) be a clique of size \( \sqrt{q} \), such that \( A \) is a \( \mathbb{F}_{p^t} \)-subspace containing \( \mathbb{F}_{p^t} \). We claim that \( f(A) \neq A \). The theorem follows immediately from this claim, because \( f \) is an involution and so the maximum cliques containing \( \mathbb{F}_{p^t} \) must come in pairs \( \{A, f(A)\} \).

We assume, to the contrary, that \( f(A) = A \). Since \( I \) is different from \( \{0, 2, \ldots, 2d - 2\} \), the subfield \( \mathbb{F}_{\sqrt{q}} \) is not a clique in \( X \) by Lemma 5.2. Since \( A \subset \mathbb{F}_q = \mathbb{F}_{p^t} \) is a 2-dimensional subspace over \( \mathbb{F}_{p^t} \) containing \( \mathbb{F}_{p^t} \) and \( A \neq \mathbb{F}_{\sqrt{q}} \mathbb{F}_{p^t} \), we must have \( A \cap \mathbb{F}_{\sqrt{q}} = \mathbb{F}_{p^t} \). The idea behind the proof is to estimate the number of \( x \in C_0 \cap A \) such that \( x \) and \( f(x) = x^{p^{2t}} \) are linearly independent over \( \mathbb{F}_{p^t} \), and use Theorem 1.2 to show that there are too many such elements when \( f(A) = A \).

Let \( V \) be the set of elements \( x \in C_0 \cap A \) such that \( \{x, x^{p^{2t}}\} \) are dependent over \( \mathbb{F}_{p^t} \). By Lemma 5.3, we have \( V \subset \langle g^{p^{2t}+1}d \rangle \). As \( g^{p^{2t}+1}d \in \langle g^{p^{2t}+1}d \rangle = \mathbb{F}_{\sqrt{q}} \), we have \( V \subset \mathbb{F}_{\sqrt{q}} \). In particular, \( V \subset A \cap \mathbb{F}_{\sqrt{q}} = \mathbb{F}_{p^t} \). On the other hand, it is clear that \( \mathbb{F}_{p^t} \subset V \) and \( 0 \notin V \).

Therefore, \( V = \mathbb{F}_{p^t}^* \). Theorem 1.2 states that \( |C_0 \cap A| = \frac{p^t - 1}{d} \), which implies that there are \( \frac{p^t-1}{d} - (p^t - 1) \) elements \( x \in C_0 \cap A \) such that \( \{x, x^{p^{2t}}\} \) are independent over \( \mathbb{F}_{p^t} \), i.e., the complement \( V' := C_0 \cap (A \setminus V) \) has \( \frac{p^t-1}{d} - (p^t - 1) \) elements.

Since \( f \) fixes \( A \) and \( A \) is a \( \mathbb{F}_{p^t} \)-subspace, we can apply Lemma 5.1 to obtain the following inclusion of sets:

\[
\bigcup_{x \in V'} (x^{p^t} \cup x^{p^{2t}F_{p^t}^*}) \subset C_0 \cap (A \setminus \mathbb{F}_{p^t}^*).
\]

Note that \( |x^{p^t} \cup x^{p^{2t}F_{p^t}^*}| = 2(p^t - 1) \) for each \( x \in V' \). If \( x, y \in V' \), such that \( x^{p^t} \cup x^{p^{2t}F_{p^t}^*} = y^{p^t} \cup y^{p^{2t}F_{p^t}^*} \), then \( y \in x^{p^t} \cup x^{p^{2t}F_{p^t}^*} \). Therefore,

\[
\frac{p^{2t} - 1}{d} - (p^t - 1) = |C_0 \cap (A \setminus \mathbb{F}_{p^t}^*)| \geq \left| \bigcup_{x \in V'} (x^{p^t} \cup x^{p^{2t}F_{p^t}^*}) \right| \geq 2(p^t - 1) \left\lceil \frac{|V'|}{2(p^t - 1)} \right\rceil.
\]

Note that \( \frac{|V'|}{2(p^t - 1)} = \frac{p^t+1}{2d} - \frac{1}{2} \) has fractional part \( \frac{1}{2} \) since \( p^t \equiv -1 \pmod{2d} \). This means \( \left\lceil \frac{|V'|}{2(p^t - 1)} \right\rceil = \frac{p^t+1}{2d} \), contradicting the inequality above. We conclude that \( f(A) \neq A \).

\[ \square \]

**Example 5.4.** If \( X \) is the Peisert graph with order \( q = p^4 \) where \( p > 3 \), then there are 0 maximum cliques of size \( \sqrt{q} \) with the subspace structure because \( \mathbb{F}_p \) forms a maximal clique in \( P_q^* \) [AY21, Theorem 1.5].
Example 5.5 (Graphs of order 625 and 2401). If $X = PP(5^4, 6, I)$ with $I \neq \{0, 2, 4\}, \{1, 3, 5\}$ then $X$ contains either 0 or 2 maximum cliques of the kind described in Theorem 1.9. A similar conclusion holds for $X = PP(7^4, 8, I)$. More numerical evidence is presented in Section 7.

5.2. The density result. Fix a positive integer $N$. Define $\mathcal{PP}(N)$ to be collection of all the semi-primitive pseudo-Paley graphs of the form $X = PP(q, 2d, I)$ with $q = p^{2rt} \leq N$ and $r$ even. Let $\mathcal{F}(N)$ be the subset of $\mathcal{PP}(N)$ consisting of those graphs $X = PP(q, 2d, I)$ with $\omega(X) = \sqrt{q}$. Since $\omega(X) \leq \sqrt{q}$ always holds, the graphs in $\mathcal{F}(N)$ are the precisely those that attain the trivial upper bound on the clique number.

Proposition 5.6. Assume that Conjecture 1.4 is true. The density of graphs attaining the trivial upper bound on the clique number inside the family of semi-primitive pseudo-Paley graphs is zero, that is,

$$\lim_{N \to \infty} \frac{\# \mathcal{F}(N)}{\# \mathcal{PP}(N)} = 0.$$

Proof. Given a prime power $q = p^{2rt} \leq N$, with $r$ even, let $\mathcal{PP}(N, p, t) \subset \mathcal{PP}(N)$ be the subset consisting of graphs $PP(q, 2d, I)$ with $q = p^{2rt}$ vertices such that $t$ is the smallest positive integer such that $p^t \equiv -1 \pmod{2d}$. Similarly, define $\mathcal{F}(N, p, t) = \mathcal{F}(N) \cap \mathcal{PP}(N, p, t)$. We can decompose

$$\mathcal{PP}(N) = \bigsqcup_{p^t \leq N} \mathcal{PP}(N, p, t), \quad \text{and} \quad \mathcal{F}(N) = \bigsqcup_{p^t \leq N} \mathcal{F}(N, p, t),$$

This is a disjoint union because for any $PP(q, 2d, I) \in \mathcal{PP}(N)$, there is a unique $(p, t)$ such that $PP(q, 2d, I) \in \mathcal{PP}(N, p, t)$. Indeed, $q$ determines the value of $p$, and the congruence $p^t \equiv -1 \pmod{2d}$ uniquely determines the value of smallest such $t$.

Recall that the Grassmannian $Gr(r, 2r)(\mathbb{F}_{p^t})$ is the set of all $r$-dimensional $\mathbb{F}_{p^t}$-subspaces inside $\mathbb{F}_{(p^t)^2r} = \mathbb{F}_q$. Given a graph $X = PP(q, 2d, I) \in \mathcal{F}(N, p, t)$ with $q = p^{2rt}$, Conjecture 1.4 implies that the set of maximum cliques in $X$ containing 0 gives a subset $S_X \subset Gr(r, 2r)(\mathbb{F}_{p^t})$ with $S_X \neq \emptyset$. If $Y \in \mathcal{F}(N, p, t)$ with $Y = PP(q, 2d, J)$, and $I \neq J$, then we claim that $S_X \cap S_Y = \emptyset$. Indeed, by Theorem 1.2, a maximum clique $V \in S_X$ uniquely determines $I$ because $I = \{j : 0 \leq j \leq 2d - 1 \text{ and } |C_j \cap V| = \frac{q - 1}{d}\}$, and hence the graph $X$. If $V \in S_X \cap S_Y$, then $X = Y$. The claim is proved, and we obtain:

$$\# \mathcal{F}(N, p, t) \leq \# \bigsqcup_{p^t \leq N} Gr(r, 2r)(\mathbb{F}_{p^t}).$$

The cardinality of the Grassmannian can be bounded as follows:

$$\# Gr(r, 2r)(\mathbb{F}_{p^t}) = \frac{(p^{2rt} - 1)(p^{2rt} - p^t) \cdots (p^{2rt} - p^{(r - 1)t})}{(p^t - 1)(p^t - p^t) \cdots (p^t - p^{(r - 1)t})} \leq p^{2r^2t}.$$

Thus,

$$\# \mathcal{F}(N, p, t) \leq \sum_{p^{2rt} \leq N} (p^t)^{2r^2} \leq \ln(N) \cdot N^r \leq \ln(N) \cdot N^{\ln(N)} = \ln(N) \cdot e^{(\ln(N))^2},$$

which implies,

$$\# \mathcal{F}(N) = \sum_{p^{rt} \leq N} \# \mathcal{F}(N, p, t) \leq N \cdot \ln(N) \cdot e^{(\ln(N))^2}. \quad (16)$$
On the other hand, the number of graphs of the form $PP(q, 2d, I) \in PP(N, p, t)$ with $q = p^{2t}$ and $d = (p^t + 1)/2$ is given by the binomial coefficient $\binom{2d}{d} = \binom{p^t + 1}{(p^t + 1)/2}$ since $I \subset \{0, 1, \ldots, 2d - 1\}$ with $\#I = d$. Using Stirling’s approximation,

$$\#PP(N, p, t) \geq \left( \frac{p^t + 1}{(p^t + 1)/2} \right) \geq \frac{4p^t}{\sqrt{4p^t}}.$$ 

By Chebyshev’s Theorem, there exists a prime $p_0$ such that $\frac{1}{2}N^{1/4} < p_0 < N^{1/4}$ for $N$ large. As a result,

$$\#PP(N) \geq \#PP(N, p_0, 1) \geq \frac{4p_0}{\sqrt{4p_0}} \geq \frac{2N^{1/4}}{\sqrt{2N^{1/4}}}.$$ 

Combining (16) and (17),

$$\limsup_{N \to \infty} \frac{\#F(N)}{\#PP(N)} \leq \limsup_{N \to \infty} \frac{N \cdot \ln(N) \cdot e^{(\ln(N))^2}}{2^{N^{1/4}}/\sqrt{2N^{1/4}}} = 0,$$ 

as desired. \qed

Despite the density of $F(N)$ being zero, we still expect that $F(N)$ will contain infinitely many examples that are non-isomorphic to the Paley graph.

**Conjecture 5.7.** For each prime $p \geq 3$, there is a subset $I \subset \{0, 1, \ldots, p\}$ with $0, 1 \in I$ and $|I| = \frac{p+1}{2}$ such that $\omega(PP(p^4, p+1, I)) = p^2$.

Using SageMath, Conjecture 5.7 has been checked to hold for all primes $p \leq 5000$. The algorithm for verifying Conjecture 5.7 is given in Algorithm 2 in Section 7.

We remark that Proposition 5.6 can be phrased unconditionally. The argument shows that union zero a union of at most $d$ distinct $2d$-th semi-primitive cyclotomic classes of $\mathbb{F}_q$ almost surely does not contain a subspace of size $\sqrt{q}$, as $q \to \infty$.

### 5.3. **Conditional improvement on the trivial upper bound.** The following lemma is useful for obtaining a lower bound on the character sum as we will see in the proof of Theorem 1.5 below.

**Lemma 5.8.** Let $d \geq 2$ be a positive integer and $\theta$ be a primitive $2d$-th root of unity. Given a subset $I = \{m_1, m_2, \ldots, m_d\} \subset \{0, 1, \ldots, 2d - 1\}$, there exists an integer $1 \leq k \leq 2d - 1$ such that $|\sum_{j=1}^d \theta^{km_j}| > \sqrt{d}/2$.

**Proof.** We have

$$\left| \sum_{k=0}^{2d-1} \sum_{j=1}^d \theta^{km_j} \right|^2 = \sum_{k=0}^{2d-1} \sum_{1 \leq j, j' \leq d} \theta^{k(m_j - m_{j'})} = \sum_{1 \leq j, j' \leq d} \sum_{k=0}^{2d-1} \theta^{k(m_j - m_{j'})} = 2d^2.$$ 

It follows that

$$\max_{1 \leq k \leq 2d-1} \left| \sum_{j=1}^d \theta^{km_j} \right| \geq \sqrt{\frac{2d^2 - d^2}{2d - 1}} = \sqrt{\frac{d^2}{2d - 1}} > \sqrt{\frac{d}{2}}.$$ 

Next we use the character sum estimates to prove Theorem 1.5.
Proof of Theorem 1.5. Assume, to the contrary, that $\omega(X) = \sqrt{q}$ and $p^t > 10.2r^2d$. Without loss of generality, we may assume $m_1 = 0$ (Remark 2.4). Since $X$ is a Cayley graph, we can restrict attention to maximum cliques containing 0. If $A$ is a maximum clique in $X$ containing 0, Theorem 1.2 implies that $C_0 \cap A \neq \emptyset$ and thus we can further assume that $1 \in A$. Indeed, any $y \in C_0 \cap A$ yields another maximum clique $B = y^{-1}A$ containing both 0 and 1. By Lemma 5.2, $A \neq \mathbb{F}_q$.

By Lemma 5.8, we can find $1 \leq k \leq 2d - 1$, such that $|\sum_{j=1}^d \theta^{km_j}| > \sqrt{d/2}$. Let $\chi$ be the multiplicative character of $\mathbb{F}_q$ such that $\chi(g) = \theta^k$. Then $\chi$ is a nontrivial character with order dividing $2d$. Suppose that $A$ is a subspace over $\mathbb{F}_p$; then by Theorem 3.12 and Theorem 1.2, we have

$$\frac{\sqrt{q} - 1}{d} \left| \sum_{j=1}^d \theta^{km_j} \right| = \left| \sum_{j=1}^d \chi(x) \right| = \left| \sum_{x \in A} \chi(x) \right| < \frac{2r}{\sqrt{p}} \sqrt{q}, \quad (18)$$

Thus,

$$\frac{\sqrt{q} - 1}{\sqrt{2d}} \leq \frac{\sqrt{q} - 1}{d} \left| \sum_{j=1}^d \theta^{km_j} \right| < \frac{2r}{\sqrt{p}} \sqrt{q}.$$ 

However, the above inequality implies $p^t \leq 10.2r^2d$, a contradiction. This finishes the proof. □

While Theorem 1.5 is stated conditionally in terms of the clique number of certain Cayley graphs, it can also be phrased unconditionally with additive combinatorics flavor as follows.

Corollary 5.9. Let $q = p^{2rt}$, where $r$ is even, and $t$ is the smallest positive integer such that $p^t \equiv -1 \pmod{2d}$. Let $D$ be the union of at most $d$ distinct $2d$-th cyclotomic classes of $\mathbb{F}_q$. Assume that $D$ contains at least one square and one non-square element. If $p^t > 10.2r^2d$, then there is no $\mathbb{F}_p$-subspace $V$ of $\mathbb{F}_q$, with dimension at least $r$, such that $V \subseteq D \cup \{0\}$.

When the set $I$ has a simple structure, the above lower bound on $p$ can be further improved. We illustrate this by analyzing the case of generalized Peisert graphs, where we can compute the sum of roots of unity explicitly.

Corollary 5.10. Let $q = p^{2rt}$, where $r$ is even and $t$ is the smallest positive integer such that $p^t \equiv -1 \pmod{2d}$. Assuming Conjecture 1.4, the generalized Peisert graph $GP^*(q, 2d)$ has clique number less than $\sqrt{q}$ when $p^t \geq 12.5r^2$.

Proof. We will assume that $\omega(GP^*(q, 2d)) = \sqrt{q}$ and show that $p^t < 12.5r^2$ must hold. Recall that $GP^*(q, 2d) = PP(q, 2d, I)$, where $I = \{0, 1, \ldots, d - 1\}$; see Example 2.5.

Let $\theta = e^{2\pi i/2d} = e^{i\pi/d}$. Let $\chi$ be the multiplicative character of $\mathbb{F}_q$ such that $\chi(g) = \theta$. We have

$$\sum_{j=1}^d \theta^{m_j} = \sum_{j=1}^d \theta^{d-1} = \frac{1 - \theta^d}{1 - \theta} = \frac{2}{1 - \theta}.$$ 

Using the inequality $\cos x \geq 1 - \frac{x^2}{2}$ for all real $x$, we have

$$|1 - \theta| = \sqrt{2 - 2 \cos \frac{\pi}{d}} \leq \sqrt{2 - 2(1 - \frac{\pi^2}{2d^2})} = \frac{\pi}{d},$$

and so,

$$\left| \frac{2}{1 - \theta} \right| \geq \frac{2d}{\pi}. \quad (19)$$
Combining the inequalities (18) and (19) yields
\[
\frac{\sqrt{q} - 1}{d} \cdot \frac{2d}{\pi} \leq \frac{\sqrt{q} - 1}{d} \left| \sum_{j=1}^{d} g^{m_j} \right| < \frac{2r}{\sqrt{p^d}} \sqrt{q}.
\]
This last inequality rearranges into:
\[
\sqrt{p^d} < \frac{r\pi \sqrt{q}}{\sqrt{q} - 1} \Rightarrow p^d < \frac{r^2 \pi^2 q}{(\sqrt{q} - 1)^2} \leq \left( \frac{81}{64} \right) r^2 \pi^2 < 12.5r^2
\]
(20) since \( q \geq 81 \).

To prove Theorem 1.6, we apply the above corollary, and then use SageMath [Sag21] to verify the cases when \( q \) is small.

**Proof of Theorem 1.6.** We assume the clique number is \( \sqrt{q} \) and apply the contrapositive of Corollary 5.10 in the special case \( r = 2 \) to conclude that \( p^d < 50 \). Note that when \( p^d \geq 41 \), \( q = p^d \geq 41^4 \), and inequality (20) implies that
\[
p^d < 4\pi^2 \left( \frac{1681}{1680} \right)^2 < 40,
\]
a contradiction. Therefore,

\[
p^d \in \{ 5, 7, 9, 11, 13, 17, 19, 23, 25, 27, 29, 31, 37 \}.
\]
Recall that \( p^d \equiv -1 \ (\text{mod} \ 2d) \) and \( d \geq 2 \). We verified each choice of \( (p^d, d) \) in the following list using Algorithm 1 (described in Section 7) via SageMath:

\[
\{(5, 3), (7, 2), (7, 4), (9, 5), (11, 2), (11, 3), (11, 6), (13, 7), (17, 3), (17, 9),
(19, 5), (19, 10), (23, 2), (23, 3), (23, 4), (23, 6), (23, 12), (25, 13), (27, 7),
(27, 14), (29, 3), (29, 5), (29, 15), (31, 2), (31, 4), (31, 8), (31, 16), (37, 19)\}.
\]
The largest case \( (p^d, d) = (37, 19) \) took about 16 hours. \( \square \)

6. NON-ISOMORPHISM

The goal of this section is to show that most graphs of the form \( PP(q, 2d, I) \) are not isomorphic to the Paley graph \( P_q \) or the Peisert graph \( P_q^* \). In contrast to Corollary 4.1, we do not assume the semi-primitive condition.

Peisert [Pei01] proved that \( P_q \) and \( P_q^* \) are non-isomorphic except when \( q = 3^2 \) by studying their respective automorphism groups. Another approach to distinguish these graphs is to study their \( p \)-ranks [BvE92]; this was carried out successfully in [WQWX07, Proposition 3.6]. We are going to use ideas in Peisert’s paper [Pei01] to establish our key criterion in Proposition 6.7.

The following definition is standard. For instance, see [dLF11, Section 3.6] for the definition of \( \Gamma L_n(F) \) for any field \( F \); we are primarily interested in the case when \( F = \mathbb{F}_q \) and \( n = 1 \). In this case, we often write \( \Gamma L_1(F) \) instead of \( \Gamma L_1(\mathbb{F}_q) \).

**Definition 6.1** (general semilinear group). Let \( \Gamma L_1(q) := \mathbb{F}_q^* \rtimes \text{Gal}(\mathbb{F}_q/\mathbb{F}_p) \) be the semi-direct product obtained via the natural action of \( \text{Gal}(\mathbb{F}_q/\mathbb{F}_p) \) on \( \mathbb{F}_q^* \). This group is called the general semilinear group of degree 1 over the finite field \( \mathbb{F}_q \).
Let \( g \) be a fixed primitive root of \( \mathbb{F}_q \), and let \( \zeta : \mathbb{F}_q \rightarrow \mathbb{F}_q \) be the map \( x \mapsto gx \). Since \( \zeta^k : \mathbb{F}_q \rightarrow \mathbb{F}_q \) is given by \( x \mapsto g^kx \), we see that \( \langle \zeta \rangle \cong \mathbb{F}_q^* \). Thus, the elements of \( \Gamma L_1(q) \) can be viewed as functions \( f : \mathbb{F}_q \rightarrow \mathbb{F}_q \) satisfying \( f(x + y) = f(x) + f(y) \) for all \( x, y \in \mathbb{F}_q \) and \( f(cx) = c^p f(x) \) for some \( j \) and for all \( x, c \in \mathbb{F}_q \). Since the Galois group \( \text{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle \alpha \rangle \) is generated by the Frobenius map \( \alpha : x \mapsto x^p \), we can also write \( \Gamma L_1(q) = \mathbb{F}_q^* \rtimes \langle \alpha \rangle = \langle \zeta \rangle \rtimes \langle \alpha \rangle \). Thus, \( \Gamma L_1(q) = \langle \zeta, \alpha \rangle \) and in particular, \( \Gamma L_1(q) \) is a permutation group. We remark that other authors (for example Peisert [Pei01], and Foulser and Kallaher [FK78]) use \( \omega \) to denote the map \( x \mapsto gx \).

We use \( \zeta \) for this purpose as \( \omega \) is reserved for the clique number throughout the paper.

Peisert [Pei01] classified all self-complementary symmetric graphs. Recall that a graph is self-complementary if it is isomorphic to its complement, and a graph is symmetric if its automorphism group acts transitively on the ordered pairs of adjacent vertices.

**Theorem 6.2 ([Pei01]).** A graph \( G \) is self-complementary and symmetric if and only if \( |G| = p^n \) for some prime \( p \) with \( p^n \equiv 1 \ (\text{mod } 4) \), and \( G \) is isomorphic to a Paley graph or a Peisert graph or is isomorphic to the exceptional graph \( G(23^2) \).

The key to proving Theorem 6.2 is the classification of the automorphism groups of all possible self-complementary symmetric graphs [Pei01, Theorem 4.2]. For our purposes, we state a slight variation of this result.

**Theorem 6.3.** Let \( X \) be a self-complementary symmetric Cayley graph defined on \( \mathbb{F}_{p^n} \) with \( \mathcal{A} = \text{Aut}(X) \), and \( \mathcal{A}_0 \) be the subgroup of \( \mathcal{A} \) which fixes 0. If \( p^n \notin \{9, 49, 81, 529\} \), then \( \mathcal{A}_0 \) is a subgroup of \( \Gamma L_1(p^n) \) and \( \mathcal{A} \cong \mathbb{F}_{p^n} \rtimes \mathcal{A}_0 \).

**Proof.** Each automorphism \( f \in \mathcal{A} \) can be decomposed as \( f_2 \circ f_1 \) where \( f_1 \in \mathcal{A}_0 \) and \( f_2 \) is a translation by an element of \( \mathbb{F}_{p^n} \). This explains the identity \( \mathcal{A} \cong \mathbb{F}_{p^n} \rtimes \mathcal{A}_0 \).

The proof given in [Pei01, Theorem 4.2] classifies the automorphism group of any such graph \( G \). There are four different cases in Peisert’s proof. Case 1 corresponds exactly to \( \mathcal{A}_0 \leq \Gamma L_1(p^n) \). Next, Case 2 corresponds to \( p^n = 9 \), while Cases 3 and 4 correspond to \( p^n \in \{49, 81, 529\} \). By the hypothesis, we must be in Case 1.

The following lemma shows that a subgroup of \( \Gamma L_1(p^n) \) has a simple structure. The sentence starting with “Moreover” is not literally part of [FK78, Lemma 2.1], but appears on page 117 of [FK78] and also on page 220 of [Pei01].

**Lemma 6.4 ([FK78, Lemma 2.1]).** If \( \mathcal{A}_0 \) is a subgroup of \( \Gamma L_1(p^n) \), then \( \mathcal{A}_0 = \langle \zeta^d, \zeta^e \alpha^s \rangle \) for some integers \( d, e, s \) satisfying the following conditions:

\[
s \mid n, d \mid (p^n - 1), \quad e \left( \frac{p^n - 1}{p^s - 1} \right) \equiv 0 \pmod{d}.
\]

Such a representation \( \mathcal{A}_0 = \langle \zeta^d, \zeta^e \alpha^s \rangle \) is unique when \( d, s > 0 \) and \( 0 \leq e < d \) and it is called the standard form. Moreover, if \( \mathcal{A}_0 = \langle \zeta^d, \zeta^e \alpha^s \rangle \) is in standard form, then \( |\mathcal{A}_0| = n(p^n - 1)/sd \).

The automorphism group of Paley graphs and Peisert graphs were first determined by Carlitz [Car60] and Peisert [Pei01], respectively.

**Theorem 6.5 ([Car60]).** Let \( q = p^n \). Then \( \text{Aut}(P_q) \cong \mathbb{F}_{p^n} \rtimes \langle \zeta^2, \alpha \rangle \) and \( |\text{Aut}(P_q)| = np^n(p^n - 1)/2 \).

**Theorem 6.6 ([Pei01, Corollary 6.3]).** Let \( q = p^n \), where \( p \equiv 3 \pmod{4} \) and \( n \) is even. If \( q \neq 3^2, 7^2, 3^4, 23^2 \), then \( \text{Aut}(P_q^*) \cong \mathbb{F}_{p^n} \rtimes \langle \zeta^4, \zeta \alpha \rangle \) and \( |\text{Aut}(P_q^*)| = np^n(p^n - 1)/4 \).
For a generalized Paley graph, it is much more difficult to determine its automorphism group. In [LP09], Lim and Praeger used association scheme to study the automorphism groups of certain generalized Paley graphs. We expect in general it is even harder to determine the automorphism group of $X = PP(q, 2d, I)$ since it is a union of copies of generalized Paley graphs. While determining the automorphism group of $X$ is challenging, we show that $X$ is not isomorphic to $P_q$ and $P_q^*$ in general.

**Proposition 6.7.** Let $X = PP(q, 2d, I)$ be in its minimal representation such that $q = p^n \notin \{3^2, 7^2, 3^4, 23^2\}$.

1. If $d = 1$, then $X$ is isomorphic to the Paley graph $P_q$.
2. If $d = 2$, then $X$ is isomorphic to the Peisert graph $P_q^*$.
3. If $d \geq 3$, then $X$ is not isomorphic to $P_q$ or $P_q^*$.

**Proof.** It is straightforward to prove the cases $d = 1$ and $d = 2$. See Example 2.5.

Next we assume $d \geq 3$. Assume, to the contrary, that $X$ is isomorphic to $P_q$ or to $P_q^*$. In particular, $X$ is symmetric and self-complementary by Theorem 6.2. Let $\mathcal{A} = \text{Aut}(X)$ and $\mathcal{A}_0 \leq \mathcal{A}$ be the subgroup fixing 0. By Theorem 6.3, $\mathcal{A}_0$ is a subgroup of $\Gamma L_1(\mathbb{F}_q)$.

By Lemma 2.7 and Remark 2.8, $\zeta^k : x \mapsto g^k x$ induces a graph automorphism of $X$ if and only if $2d \mid k$. Therefore, each $\zeta^k \in \mathcal{A}_0$ with $k > 0$ must satisfy $k \geq 2d \geq 6$. Using Lemma 6.4, we have $\mathcal{A}_0 = \langle \zeta^d, \zeta^e \alpha \rangle$ in its standard form for some $d', e \geq 0$ and $s \geq 1$. Consequently,

$$|\mathcal{A}| = |\mathbb{F}_p^n| |\mathcal{A}_0| = \frac{np^n(p^n - 1)}{sd'} \leq \frac{np^n(p^n - 1)}{6}.$$ 

The automorphism group of $X$ has a smaller size than the automorphism group of both the Paley graph $P_q$ and the Peisert graph $P_q^*$ (if $n$ is even) shown in Theorem 6.5 and Theorem 6.6, which is a contradiction.

Mullin [Mul09, Chapter 8] conjectured that generalized Peisert graphs are distinct from Peisert and Paley graphs for infinitely many prime powers. She verified the conjecture computationally for small prime powers [Mul09, Section 5.4]. We confirm this conjecture below.

**Corollary 6.8.** If $d \geq 3$ and $q \equiv 1 \mod 4d$ and $q \notin \{3^2, 7^2, 3^4, 23^2\}$, then $GP^*(q, 2d)$ is not isomorphic to $P_q$ or $P_q^*$. In fact, $GP^*(q, 2d)$ is self-complementary but not symmetric.

**Proof.** By Example 2.5, we identify $GP^*(q, 2d)$ with $PP(q, 2d, \{0, 1, \ldots, d - 1\})$ which is in its minimal representation, and the complement of $GP^*(q, 2d)$ corresponds to $PP(q, 2d, \{d, d + 1, \ldots, 2d - 1\})$. The first assertion follows directly from Proposition 6.7. Consider the graph homomorphism:

$$f : PP(q, 2d, \{0, 1, \ldots, d - 1\}) \to PP(q, 2d, \{d, d + 1, \ldots, 2d - 1\})$$

induced by $x \mapsto g^d x$ on the set of vertices. Then $f$ is an isomorphism from $GP^*(q, 2d)$ to its complement. Thus, $GP^*(q, 2d)$ is self-complementary. Since $GP^*(q, 2d)$ is not isomorphic to the Paley graph and the Peisert graph, $GP^*(q, 2d)$ cannot be symmetric by Theorem 6.2.

Mathon [Mat88] asked whether there is an infinite family of self-complementary strongly regular graphs of non-Paley type. This was already settled affirmatively by Peisert in Theorem 6.2 as Peisert graphs are of non-Paley type. Klin, Kriger and Woldar [KKW16] also answered Mathon’s question for graphs of order $p^2$. Corollary 6.8 gives another answer to this question. Indeed, it follows from Lemma 2.13 that when $q = p^{2r}$ with $r$ even and $p^t \equiv -1 \mod 2d)$, the generalized Peisert graph $GP^*(q, 2d)$ is strongly regular, self-complementary but not isomorphic to $P_q$ or $P_q^*$. 

28
7. Algorithms and Numerical Computations

In this section, we present algorithms to find and classify maximum cliques in pseudo-Paley graphs. We also report results from our numerical experiments using SageMath \cite{Sag21} to support the conjectures in this paper.

Using SageMath, we can find several examples of pseudo-Paley graphs of order \( q \) coming from a union of semi-primitive cyclotomic classes with clique number \( \sqrt{q} \). The following table summarizes some of these examples. The set \( I \) indicates the choice of \( C_i \)'s in the connection set. For example, the second row corresponds to the Cayley graph \( \text{Cay}(\mathbb{F}_{5^4}, D) \) where \( D = C_0 \cup C_1 \cup C_3 \) and \( C_j = \{ g^{6i+j} \mid 0 \leq i \leq \frac{5^4-1}{6} \} \) and \( g \) is a primitive root of \( \mathbb{F}_{5^4} \).

<table>
<thead>
<tr>
<th>( q )</th>
<th>( d )</th>
<th>( I )</th>
<th>( \omega(X) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 5^4 )</td>
<td>3</td>
<td>{0, 1, 3}</td>
<td>25</td>
</tr>
<tr>
<td>( 7^4 )</td>
<td>4</td>
<td>{0, 1, 2, 4}</td>
<td>49</td>
</tr>
<tr>
<td>( 7^4 )</td>
<td>4</td>
<td>{0, 1, 3, 6}</td>
<td>49</td>
</tr>
<tr>
<td>( 3^8 )</td>
<td>5</td>
<td>{0, 1, 2, 3, 5}</td>
<td>81</td>
</tr>
<tr>
<td>( 3^8 )</td>
<td>5</td>
<td>{0, 1, 3, 6, 7}</td>
<td>81</td>
</tr>
<tr>
<td>( 11^4 )</td>
<td>6</td>
<td>{0, 1, 2, 3, 6, 7}</td>
<td>121</td>
</tr>
<tr>
<td>( 11^4 )</td>
<td>6</td>
<td>{0, 1, 2, 4, 5, 8}</td>
<td>121</td>
</tr>
<tr>
<td>( 11^4 )</td>
<td>6</td>
<td>{0, 1, 2, 3, 5, 10}</td>
<td>121</td>
</tr>
<tr>
<td>( 13^4 )</td>
<td>7</td>
<td>{0, 1, 2, 3, 5, 6, 9}</td>
<td>169</td>
</tr>
<tr>
<td>( 13^4 )</td>
<td>7</td>
<td>{0, 1, 2, 4, 7, 8, 10}</td>
<td>169</td>
</tr>
<tr>
<td>( 13^4 )</td>
<td>7</td>
<td>{0, 1, 2, 5, 7, 9, 10}</td>
<td>169</td>
</tr>
</tbody>
</table>

Table 1. Graphs \( X \) with \( \omega(X) = \sqrt{q} \)

With the help of SageMath, we also notice that in each of the graphs listed above, there are exactly 2 cliques of size \( \sqrt{q} \) containing \( \mathbb{F}_{p^r} \). Both cliques are subspaces over \( \mathbb{F}_{p^r} \) which supports Conjecture 1.4. This leads us to conjecture the following refined version of Theorem 1.9.

**Conjecture 7.1.** Let \( X = PP(q, 2d, I) \) be a semi-primitive pseudo-Paley graph with \( q = p^{2rt} \) where \( r \) is even. If \( \omega(X) = \sqrt{q} \), then the number of maximum cliques containing \( \mathbb{F}_{p^r} \) is 2.

In general, finding the clique number of a Cayley graph is NP-hard \cite{GR17}. It is not possible to compute the exact clique number of \( X = PP(q, 2d, I) \) for \( q > 2000 \) using the current computational power. In contrast, finding the common neighbors of \( \mathbb{F}_p \) inside \( X \) takes only polynomial-time, and SageMath can return the clique number of a graph with < 700 vertices in a few minutes. Therefore, we employ the following algorithm.

**Algorithm 1:** Find the size of a maximum clique containing \( \mathbb{F}_p \) inside \( PP(q, 2d, I) \)

\[
k = \min\{n \in \mathbb{N} : q/2^n < 700\}
\]

\[
V = \{0, 1, \ldots, k - 1\} \cup \bigcap_{j=0}^{k-1} \text{Neighbors}(j) \quad \text{// Finding the set of common neighbors}
\]

\[
Y = PP(q, 2d, I)[V] \quad \text{// Taking the induced subgraph}
\]

\[
\text{return } \omega(Y)
\]

Since the graph is \( q^{-1/2} \)-regular, we expect that the subgraph \( Y \) has roughly \( q/2^k \) many vertices. This heuristic can be proved rigorously using character sums and Weil’s bound, see for example \cite{GS71}; essentially, the graphs we are working on are pseudo-random \cite{CGW89, KP04}. Since
\[ q/2^k < 700, \] SageMath can return the clique number of \( Y \) quickly. We used this algorithm to handle the exceptional cases in Theorem 1.6.

In general, it suffices to consider maximum cliques containing \( \{0, 1\} \). The reasoning is given at the beginning of the proof of Theorem 1.5. When \( q \leq 7^4 \), we have \( q/2^2 < 700 \), and we can perform the algorithm outlined above with \( k = 2 \) to find the clique number of all possible \( PP(q, 2d, I) \). This verifies the main Conjecture 1.4 for values of \( q \) up to \( 7^4 \).

In the final part of the paper, we present an efficient algorithm to verify Conjecture 5.7 for a given prime \( p \). The strategy is to fix a \( \mathbb{F}_p \)-subspace \( V \subset \mathbb{F}_{p^4} \) with basis \( \{1, a\} \) with \( a \in C_1 \), and search for an index set \( I \subset \{0, 1, \ldots, p\} \) with \(|I| = (p + 1)/2\) such that \( V \setminus \{0\} \subset \bigcup_{j \in I} C_j \). In order for \( V \) to form a clique in \( PP(p^4, p + 1, I) \), by Theorem 1.2, we must have

\[ I = \{j : |V \cap C_j| = \frac{p^2 - 1}{p + 1}/2 = 2(p - 1)\}. \quad (21) \]

Since \( 1, a \in V \), it follows that \( 0, 1 \in I \). Note that \( V \setminus \{0\} \) is a disjoint union of \( (p + 1) \) many \( \mathbb{F}_p^* \)-cosets with representatives \( R = \{1, a, a + 1, a + 2, \ldots, a + (p - 1)\} \). By Lemma 5.1, \( \mathbb{F}_p^* \) is a subgroup of \( C_0 \), and so each cyclotomic class \( C_j \) is a disjoint union of \( \mathbb{F}_p^* \)-cosets. As a result, we can decompose \( (V \setminus \{0\}) \cap C_j \) into \( \mathbb{F}_p^* \)-cosets. Therefore, equation (21) is equivalent to the statement that \( C_j \) contains exactly two \( \mathbb{F}_p^* \)-coset representatives in \( R \) for each \( j \in I \). Applying this idea, we can design a polynomial-time algorithm as follows:

**Algorithm 2:** Count the number of \( I \) such that \( 0, 1 \in I \) and \( \omega(PP(p^4, p + 1, I)) = p^2 \).

```plaintext
ValidSets ← ∅
for k ← 0 to \( p^2 \) do
    a ← \( g^{(p+1)k+1} \)
    L ← [] // initiating an empty list
    R ← \{1, a, a + 1, \ldots, a + (p - 1)\}
    for r ∈ R do
        t ← \( \log_g(r) \) // finding exponent t with \( g^t = r \) using the discrete logarithm
        L ← L append \{t (mod p + 1)\}
    I ← set(L) // remove duplicates from the list L to get the set I
    flag ← 1 // assume I is a valid set
    for j ∈ I do
        if L.count(j) ≠ 2 then
            flag ← 0 // I is not valid
            break
    if flag = 1 then
        ValidSets ← ValidSets ∪\{I\}
return #ValidSets // return cardinality
```

A slight variation of the algorithm above can be used to verify Conjecture 7.1 for \( PP(p^4, p + 1, I) \) for any given prime \( p \); we verified it for all odd primes up to 100. The table below lists the result of Algorithm 2 for odd primes \( p \) up to 100. From Table 2, we predict that the number of such sets \( I \) is roughly \( p^2/8 \).
Sample Sage code. An example of a SageMath code for Algorithm 1 in the case $q = 11^4, d = 3$ and $X = PP(q, 6, \{0, 1, 2\})$ is given below. We pick $k = 5$ and compute the size of a maximum clique in $X$ containing $\{0, 1, 2, 3, 4\}$. The aforementioned heuristic tells us that the subgraph $Y$ should have size approximately $11^4/2^5 \approx 458$. In fact, $Y$ has 449 vertices, so the heuristic is fairly accurate.

```python
> q=11^4;
> Fq.<g>=GF(q, modulus="primitive");
> V=[0+g-g,1+g-g,2+g-g,3+g-g,4+g-g]
> D = [g^(6*i+j) for i in [0..(q-1)/6-1] for j in [0, 1, 2]]
> for x in D:
    if (x-1 in D) and (x-2 in D) and (x-3 in D) and (x-4 in D):
        V.append(x)
> Y=Graph([V, lambda i,j: i != j and i-j in D]);
> Y.clique_number()
```

The particular code above took around 2 minutes and the output is 19. Thus, $PP(11^4, 6, \{0, 1, 2\})$ does not have a clique with size $\sqrt{q} = 11^2$ which contains $\{0, 1, 2, 3, 4\}$.

ACKNOWLEDGEMENTS

The authors thank Gabriel Currier, Greg Martin, Zinovy Reichstein, József Solymosi, and Joshua Zahl for helpful discussions. The research of the first author was supported by a postdoctoral research fellowship from the University of British Columbia. The research of the second author was supported in part by a Four Year Doctoral Fellowship from the University of British Columbia.

REFERENCES


DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, 1984 MATHEMATICS ROAD, CANADA V6T 1Z2

Email address: sasgarli@math.ubc.ca

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, 1984 MATHEMATICS ROAD, CANADA V6T 1Z2

Email address: kyleyip@math.ubc.ca