ERDŐS–KO–RADO THEOREM IN PEISERT-TYPE GRAPHS

CHI HOI YIP

ABSTRACT. The celebrated Erdős–Ko–Rado (EKR) theorem for Paley graphs of square order states that all maximum cliques are canonical in the sense that each maximum clique arises from the subfield construction. Recently, Asgarli and Yip extended this result to Peisert graphs and other Cayley graphs which are Peisert-type graphs with nice algebraic properties on the connection set. On the other hand, there are Peisert-type graphs for which the EKR theorem fails to hold. In this paper, we show that the EKR theorem of Paley graphs extends to almost all pseudo-Paley graphs of Peisert-type. Furthermore, we establish the stability results of the same flavor.

1. INTRODUCTION

Throughout the paper, let p be an odd prime and q a power of p. Let $\mathbb{F}_q$ be the finite field with q elements, $\mathbb{F}_q^+$ be its additive group, and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ be its multiplicative group.

Given an abelian group G and a connection set $S \subset G \setminus \{0\}$ with $S = -S$, the *Cayley graph* $\mathrm{Cay}(G, S)$ is the undirected graph whose vertices are elements of G, such that two vertices g and h are adjacent if and only if $g - h \in S$. A *clique* in a graph X is a subset of vertices in which every two distinct vertices are adjacent. Note that a subset C of vertices in $X = \mathrm{Cay}(G, S)$ is a clique if and only if $C - C \subset S \cup \{0\}$. This naturally connects the concept of cliques in Cayley graphs with many interesting problems from additive combinatorics.

Next, we introduce the main object in this paper, defined in [1, 2]:

Definition 1.1 (Peisert-type graphs). Let q be an odd prime power. Let $S \subset \mathbb{F}_{q^2}^*$ be a union of $m \leq q$ [1] cosets of $\mathbb{F}_q^*$ in $\mathbb{F}_{q^2}^*$, that is,

$$S = c_1 \mathbb{F}_q^* \cup c_2 \mathbb{F}_q^* \cup \cdots \cup c_m \mathbb{F}_q^*. \tag{1}$$

Then the Cayley graph $X = \mathrm{Cay}(\mathbb{F}_{q^2}^+, S)$ is said to be a Peisert-type graph of type (m, q).

The classical Erdős-Ko-Rado theorem [9] concerns the classification of maximum intersecting families of k-element subsets of $\{1, 2, ..., n\}$: when $n \geq 2k + 1$, all maximum families are canonically intersecting (also known as stars) in the sense that all sets in the family contain a fixed element. Unsurprisingly, in many extremal problems, the only extremal configurations are given by those obvious constructions. The book [12] by Godsil and Meagher consists of many modern algebraic approaches to proving various EKR-type results.

In this paper we study the structure of maximum cliques in Peisert-type graphs; equivalently, we study the interaction between the addition operation (coming from $C - C$) and the multiplication operation (coming from those $\mathbb{F}_q^*$-cosets forming S) over finite fields. From the perspective of EKR, Peisert-type graphs are nice objects to study as they admit obvious choices of maximum cliques.

[1]The definition in [2] has the stronger assumption that $m \leq \frac{q+1}{2}$. Readers are warned to keep this in mind when consulting the results in [2].

Indeed, one can read from the connection set S that $c_1\mathbb{F}_q, c_2\mathbb{F}_q, \ldots, c_m\mathbb{F}_q$ are cliques in X containing 0. Moreover, Peisert-type graphs are based on cyclotomic constructions (due to Brouwer, Wilson, and Xiang [8]) so that they are strongly regular, which implies that $c_1\mathbb{F}_q, c_2\mathbb{F}_q, \ldots, c_m\mathbb{F}_q$ are maximum cliques because of the Delsarte bound (see [1, Theorem 7] for a different proof). Thus, translates of $c_1\mathbb{F}_q, c_2\mathbb{F}_q, \ldots, c_m\mathbb{F}_q$ can be regarded as *canonical cliques* in X. Since there are no other obvious maximum cliques in X, in view of EKR-type results, we say *the EKR theorem holds for X*, or equivalently, X has *the strict-EKR property*, provided that all maximum cliques in X are canonical.

The story of the EKR theorem in our setting begins with a celebrated result by Blokhuis [6], who showed that the only maximum clique (containing 0,1) in the Paley graph of order q^2 is given by the subfield $\mathbb{F}_q$. Recall that the *Paley graph of order q^2* is $\mathrm{Cay}(\mathbb{F}_{q^2}^+, (\mathbb{F}_{q^2}^*)^2)$, where $(\mathbb{F}_{q^2}^*)^2$ is the subset of squares in $\mathbb{F}_{q^2}^*$. One can easily show that the subset of squares can be decomposed as the union of $\mathbb{F}_q^*$-cosets, and verify that Blokhuis' result is equivalent to the EKR theorem for Paley graphs; see [12, Section 5.9] for a related discussion. Later, Sziklai [19] generalized the proof of Blokhuis, and showed that if $d \mid (q+1)$ and $d \geq 3$, then the *d-Paley graph* $\mathrm{Cay}(\mathbb{F}_{q^2}^+, (\mathbb{F}_{q^2}^*)^d)$ has the strict-EKR property, in the same spirit. We refer to [2, Section 2.1] for more historical discussion. Recently, Mullin [15] studied the same question for the Peisert graph $\mathrm{Cay}(\mathbb{F}_{q^2}^+, (\mathbb{F}_{q^2}^*)^4 \cup g(\mathbb{F}_{q^2}^*)^4)$ (where $q \equiv 3 \pmod 4$ and g is a primitive root of $\mathbb{F}_{q^2}$) and conjectured that the EKR theorem also holds. However, she remarked (see also [2, Remark 2.19]) that it seems the idea of Blokhuis and Sziklai relies on the subgroup structure of the connection set (which precisely corresponds to Paley graphs and d-Paley graphs) and thus fails to extend to Peisert graphs. When d is even, one can also ask the same question for the d-th power Peisert graphs (see for example [2, Definition 2.11]), defined similarly as d-Paley graphs.

The attempt to find a unified approach to prove the EKR theorem of these graphs eventually led to the definition of Peisert-type graphs in [2]; indeed, the above four families of graphs are special Peisert-type graphs [2, Lemma 2.10]. In [2, Theorem 1.3], Asgarli and Yip showed that the strict-EKR property holds for a Peisert-type graph X of type (m,q) (with $m \leq \frac{q+1}{2}$ and q sufficiently large) provided the existence of a multiplicative character such that the character sum over each subset of the connection set of X admits a small cancellation. When X is a Paley graph, Peisert graph, or their generalizations, the choice of such a character is obvious; thus this criterion gives rise to a new proof of the result by Blokhuis and by Sziklai, as well as resolves the conjecture by Mullin (except for the case when p is small compared to $\log_p q$). However, it is not clear how to apply such a criterion to an abstractly defined Peisert-type graph. Furthermore, given a Peisert-type graph, it seems difficult to predict if it has the strict-EKR property by staring at its connection set. Indeed, one can systematically construct an infinite family of Peisert-type graphs for which the strict-EKR property fails [1, Section 5].

The stability of canonical cliques in Peisert-type graphs has also been studied. For simplicity, we say a Peisert-type graph X with order q^2 has *the property* $\mathrm{ST}(k)$ if each clique in X with size at least $q - k$ is contained in a canonical clique in X. From the definition, it is clear that the strict-EKR property is equivalent to the property $\mathrm{ST}(0)$. Thus, the property $\mathrm{ST}(k)$ (for $k \geq 1$) refines the strict-EKR property. One widely open conjecture, due to by Baker, Ebert, Hemmeter, and Woldar [3], states that the second largest maximal clique in the Paley graph with order q^2 has size $\frac{q+r(q)}{2}$, where $r(q) = 1$ or 3, depending on q modulo 4. In other words, Paley graphs of order q^2 has the property $\mathrm{ST}(\frac{q-r(q)}{2} - 1)$. To the best knowledge of the author, no partial progress has been made for this conjecture. For d-Paley graphs of order q^2 with $d \geq 3$, Sziklai [19, Theorem

1.3] showed they have the property $\mathrm{ST}(c\sqrt{q})$ for some positive constant c (depending on d); we refer to [2, Corollary 4.4] and [13, Section 6] for some generalization and improvement on his results. However, all known results in this direction assume the edge density of the graph being strictly less than $1/2$. In general, such type of stability questions is widely open for Peisert-type graphs.

In [1, Section 6], Asgarli, Goryainov, Lin, and Yip asked for a complete classification of Peisert-type graphs with the strict-EKR property. This question is potentially very challenging; indeed, it turns out to be a special case of a widely open problem regarding the strict-EKR property of block graphs of orthogonal arrays [12, Problem 16.4.1]. In this paper, we give some partial answers to this question by estimating the number of Peisert-type graphs with the strict-EKR property. In other words, we study how likely the strict-EKR property holds for a "random" Peisert-type graph. From the probabilistic viewpoint, it seems plausible that there should be a threshold in terms of m and q determining the prevalence (or not) of the strict-EKR property among Peisert-type graphs of type (m, q). We remark that questions of a similar flavor have been studied previously; for example, Balogh, Bohman, and Mubayi [5] studied EKR-type results in random hypergraphs.

Our first main result shows that the strict-EKR property is prevalent when the edge density of the graph is at most $\frac{1}{2}$. It is known that Peisert-type graphs with edge density $\frac{1}{2}$ are pseudo-Paley graphs [1, Corollary 5], that is, graphs that share the same spectrum with some Paley graphs. Thus, our result shows that the EKR theorem for Paley graphs extends to almost all pseudo-Paley graphs of Peisert-type; moreover, we can say something stronger on the stability of canonical cliques.

Theorem 1.2. *As $q \to \infty$, almost all Peisert-type graphs of type $(\frac{q+1}{2}, q)$ have the property* $\mathrm{ST}(\sqrt{q}/2)$.

In many problems defined over finite fields, working over a prime field $\mathbb{F}_p$ is much easier than working over a general finite field. Essentially, this is due to the existence of subfield obstructions over a general finite field. The same situation occurs in our settings. When p is a prime, it is known that all Peisert-type graphs of type $(\frac{p+1}{2}, p)$ have the strict-EKR property [2] (see also Theorem 2.1). Our second main result refines Theorem 1.2 when $q = p$ is a prime.

Theorem 1.3. *As $p \to \infty$, almost all Peisert-type graphs of type $(\lfloor \frac{2p-2}{3} \rfloor, p)$ have the strict-EKR property, and almost all Peisert-type graphs of type $(\frac{p+1}{2}, p)$ have the property* $\mathrm{ST}(p/20)$.

On the other hand, we show that if the edge density of a Peisert-type graph is too large, then the strict-EKR property almost surely fails.

Theorem 1.4. *Let $n \geq 2$ with the largest proper divisor being t and let $q = p^n$. As $p \to \infty$, almost all Peisert-type graphs of type $(q - o(p^t), q)$ do not have the strict-EKR property.*

As suggested by numerical computations, the structure of maximum cliques could be very complicated in Peisert-type graphs with the edge density strictly greater than $1/2$. This is probably why the strict-EKR property of these graphs has not been studied in the literature.

Structure of the paper. In Section 2, we provide additional background and prove some preliminary results. In Section 3, we study the strict-EKR property of Peisert-type graphs. Finally, in Section 4, we study the stability of canonical cliques. The proof of Theorem 1.2 and Theorem 1.3 will be presented in Section 4, and the proof of Theorem 1.4 will be presented in Section 3.

2. PRELIMINARIES

2.1. EKR properties of Peisert-type graphs.
In this subsection, we provide extra background on the known EKR properties of Peisert-type graphs.

Theorem 2.1 (Asgarli and Yip [2, Theorem 1.2]). *Let X be a Peisert-type graph of type (m, q) with $m \leq \frac{q+1}{2}$, where q is a power of an odd prime p. Then each maximum clique in X containing 0 is an $\mathbb{F}_p$-subspace of $\mathbb{F}_{q^2}$.*

In particular, the above theorem immediately implies the strict-EKR property for each Peisert-type graph of type (m, p) with $m \leq \frac{p+1}{2}$, which has been implicitly observed by Lovász and Schrijver [14]. When q is a proper prime power and the connection set of X has a nice algebraic structure (which is the case for Paley graphs, Peisert graphs, and their generalizations), it turns out that Theorem 2.1 implies the strict-EKR property [2, Theorem 1.3].

The following theorem shows that all Peisert-type graphs with small edge density have the strict-EKR property.

Theorem 2.2 (Asgarli, Goryainov, Lin, and Yip [1, Corollary 8]). *If $q > (m - 1)^2$, then all Peisert-type graphs of type (m, q) have the strict-EKR property.*

Theorem 2.2 is best possible if q is a square; see the counterexamples constructed in [1, Theorem 9]. We refer to [2, Corollary 4.1] for a slightly stronger statement.

The following corollary is equivalent to the above theorem. We record it here as it has potential applications in number theory and additive combinatorics. The realization of this equivalence is also helpful in proving our main results.

Corollary 2.3. *Let $V \subset \mathbb{F}_{q^2}$ be an $\mathbb{F}_p$-subspace with size q. If V is not an $\mathbb{F}_q$-subspace, then at least $\sqrt{q} + 1$ many $\mathbb{F}_q^*$-cosets are needed to cover $V \setminus \{0\}$.*

Proof. Suppose that the minimum number of $\mathbb{F}_q^*$-cosets needed to cover $V \setminus \{0\}$ is m; say $V \setminus \{0\} \subset S := \cup_{i=1}^m c_i \mathbb{F}_q^*$. Then V is a clique in $X = \text{Cay}(\mathbb{F}_{q^2}^+, S)$ since $V - V = V \subset S \cup \{0\}$. It follows that V is a non-canonical clique in the Peisert-type graph X that is of type (m, q), and thus X fails to satisfy the strict-EKR property. It follows from Theorem 2.2 that $m \geq \sqrt{q} + 1$. $\qquad\square$

2.2. Connection with finite geometry.
In this subsection, we recall some celebrated results from the theory of directions and then discuss their connection with Peisert-type graphs.

We begin with some standard terminologies. Let $\text{AG}(2, q)$ and $\text{PG}(1, q)$ denote the affine plane and the projective line over $\mathbb{F}_q$, respectively. Let U be a subset of $\text{AG}(2, q)$; the *set of directions determined* by U is defined to be

$$D(U) := \{[a - c : b - d] : (a, b), (c, d) \in U, (a, b) \neq (c, d)\} \subset \text{PG}(1, q).$$

Let $D \subset \text{PG}(1, q)$ be a set of directions. We say that a subset U of $\text{AG}(2, q)$ is a *D-set* if $D(U) = D$, and U is said to be *maximal with respect to D* if $D(U) \subset D$ and $D(U \cup \{v\}) \not\subset D$ for any $v \in \text{AG}(2, q) \setminus U$.

The theory of directions has been developed by multiple authors, notably Rédei [16] and Szőnyi [18]. It is of particular interest to estimate $|D(U)|$; the following theorem summarizes the best-known results on the size of $D(U)$ when $q = p$ is a prime.

Theorem 2.4. *Let U be a subset of $\text{AG}(2, p)$ with $|U| = p$.*

- *(Rédei and Megyesi [16]) If the points in U are not all collinear, then U determines at least $\frac{p+3}{2}$ directions.*
- *(Lovász and Schrijver [14]) If U determines exactly $(p+3)/2$ directions, then U is affinely equivalent to the set $\{(x, x^{(p+1)/2}) : x \in \mathbb{F}_p\}$.*
- *(Gács [10]) If U determines more than $\frac{p+3}{2}$ directions, then it determines at least $\lfloor \frac{2p+1}{3} \rfloor$ directions.*

The following theorem is analogous to Theorem 2.4 for $q = p^2$.

Theorem 2.5 (Gács, Lovász, and Szőnyi [11]). *Let U be a subset of $\mathrm{AG}(2, p^2)$ with $|U| = p^2$. If $|D(U)| \geq \frac{p^2+3}{2}$, then either U is affinely equivalent to the set $\{(x, x^{(p^2+1)/2}) : x \in \mathbb{F}_{p^2}\}$, or $|D(U)| \geq \frac{p^2+p}{2} + 1$.*

Proving direction results over $\mathrm{AG}(2, q)$ for general prime powers q appears to be much harder. Indeed the subfield obstructions would provide a major barrier in proving extensions of Theorem 2.4; see [4, 7] for a celebrated result of Blokhuis, Ball, Brouwer, Storme, and Szőnyi. It is known that results similar to Theorem 2.4 can be very helpful in studying cliques in Paley graphs and more generally Peisert-type graphs. In the literature, geometric properties of Peisert-type graphs have been explored; see [1, 2, 6, 13, 14, 19]. Such geometrical interpretations of Peisert-type graphs turn out to play an important role in proving their EKR-type properties; we refer to Section 4.1 for a different connection, which is crucial in the proof of our stability result.

There are also stability results in the theory of directions. Here we list two results by Szőnyi [17], whose proofs use tools from algebraic geometry.

Theorem 2.6 (Szőnyi [17]). *Let U be a D-set of $\mathrm{AG}(2, q)$ consisting of $q - n$ points with $1 \leq n \leq \sqrt{q}/2$. If $|D| < (q+1)/2$, then U can be extended to a D-set V with $|V| = q$. Moreover, when q is a prime p, the assumption $n \leq \sqrt{q}/2$ can be weakened to $n < (p + 45)/20$.*

Proof. This is essentially [17, Theorem 4]. When $q = p$ is a prime, one can use the Stöhr-Voloch bound (instead of the Hasse-Weil bound) to get an improved upper bound on the number of rational points of a curve so that [17, Theorem 4] can be refined; see [17, Remark 3] and also [18, Theorem 5.1]. $\square$

Theorem 2.7 (Szőnyi [17]). *Let $D \subset \mathrm{PG}(1, q)$ with $|D| = \frac{q+1}{2}$. Suppose that there is a D-set $U \subset \mathrm{AG}(2, q)$ such that U is maximal with respect to D and $|U| = q - n$ with $1 \leq n \leq \sqrt{q}/2$. Then $\mathrm{PG}(1, q) \setminus D$ is the projection of an irreducible conic (with the form $X^2 + aY^2 + bZ^2 + cXY + dYZ + eZX = 0$ defined in the projective plane) onto the YZ projective line. Moreover, when q is a prime p, the assumption $n \leq \sqrt{q}/2$ can be weakened to $n < (p + 45)/20$.*

Proof. This is essentially [17, Proposition 6]. Note that in the original statement of [17, Proposition 6], it was implicitly assumed that the infinity direction $\infty := [0 : 1]$ is in D (which was assumed at the beginning of the proof in [17, Theorem 4]); in general, one needs to slightly modify the statement. The form of the conic is explicit from the proof of [17, Proposition 6].

When $q = p$ is a prime, although it is not explicitly stated in [17], one can derive the same conclusion using [17, Remark 3] (see also the proof of Theorem 2.6). $\square$

We will call a subset $D \subset \mathrm{PG}(1, q)$ *bad* if it satisfies the assumptions of Theorem 2.7. We define $\mathcal{B}_q$ to be the collection of bad direction sets. The following two corollaries are consequences of the above two theorems.

Corollary 2.8. *The collection $\mathcal{B}_q$ of bad direction sets in $\mathrm{PG}(1,q)$ has size at most q^5.*

Proof. This follows from Theorem 2.7. Note that each $D \in \mathcal{B}_q$ arises from the projection of a conic with the form $X^2 + aY^2 + bZ^2 + cXY + dYZ + eZX = 0$, with $a, b, c, d, e \in \mathbb{F}_q$. Since the number of such conics is at most q^5 and each conic with the above form gives rise to at most one bad direction set, the statement follows. $\qquad\square$

Remark 2.9. One can get a better upper bound on $|\mathcal{B}_q|$ using the transitive property of projective general linear group $\mathrm{PGL}_2(\mathbb{F}_q)$, but it is not needed for our applications.

Corollary 2.10. *Let U be a D-set of $\mathrm{AG}(2,q)$ consisting of $q - n$ points with $n \leq \sqrt{q}/2$. If $|D| \leq (q+1)/2$ and $D \notin \mathcal{B}_q$, then U can be extended to a D-set V with $|V| = q$. Moreover, when $q = p$ is a prime, the assumption $n \leq \sqrt{q}/2$ can be weakened to $n < (p + 45)/20$.*

Proof. When $|D| < (q+1)/2$, this follows from Theorem 2.6.

Next assume that $|D| = (q+1)/2$ and $D \notin \mathcal{B}_q$. Let U be a D-set with the above assumption. Then Theorem 2.7 implies that U is not maximal with respect to D, that is, U can be extended to a D-set U' with $|U'| = |U| + 1$, provided that $|U| < q$. We can then apply the same reasoning to U' since U' is still a D-set with $D \notin \mathcal{B}_q$. Thus, U' can be extended to a D-set U'' with $|U''| = |U'| + 1$, provided that $|U'| < q$. Applying the same argument repeatedly yields a D-set V with $|V| = q$. $\quad\square$

3. PREVALENCE OF THE STRICT-EKR PROPERTY

Proposition 3.1. *As $q \to \infty$, almost all Peisert-type graphs of type $(\frac{q+1}{2}, q)$ have the strict-EKR property. In particular, we have the EKR theorem for almost all pseudo-Paley graphs of Peisert-type.*

Proof. Let $q = p^n$. We need to estimate the number of graphs that fail to have the strict-EKR property. Since Cayley graphs are vertex-transitive, it suffices to consider maximum cliques containing 0. Thus, it is equivalent to estimating the number of graphs admitting at least one non-canonical maximum clique containing 0.

By Theorem 2.1, all non-canonical maximum cliques containing 0 are $\mathbb{F}_p$-subspaces. The number of $\mathbb{F}_p$-subspaces of size q in $\mathbb{F}_{q^2}$ is given by the Grassmannian

$$\# \mathrm{Gr}(n, 2n)(\mathbb{F}_p) = \frac{(p^{2n} - 1)(p^{2n} - p) \cdots (p^{2n} - p^{n-1})}{(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})} \leq p^{2n^2} = q^{2n}.$$

Let V be an $\mathbb{F}_p$-subspace of size q in $\mathbb{F}_{q^2}$, such that V does not have the subfield structure in the sense that V is not an $\mathbb{F}_q$-subspace. By Corollary 2.3, we need at least $\sqrt{q} + 1$ many $\mathbb{F}_q^*$-cosets to cover $V \setminus \{0\}$. Let $X = \mathrm{Cay}(\mathbb{F}_{q^2}^+, S)$ be a Peisert-type graph of type $(\frac{q+1}{2}, q)$, such that V is a (maximum) clique in X. Then $V = V - V \subset S \cup \{0\}$. It follows that S must be the union of $\frac{q+1}{2}$ many $\mathbb{F}_q^*$-cosets, with at least $\sqrt{q} + 1$ of them having been prescribed. It follows that the number of such graphs X is at most

$$\binom{q + 1 - (\sqrt{q} + 1)}{\frac{q+1}{2} - (\sqrt{q} + 1)},$$

which accounts for the number of graphs that fails to satisfy the strict-EKR property due to the appearance of the non-canonical maximum clique V.

To conclude, the density of graphs that fails to satisfy the strict-EKR property is at most

$$\frac{q^{2n} \cdot \binom{q+1-(\sqrt{q}+1)}{\frac{q+1}{2}-(\sqrt{q}+1)}}{\binom{q+1}{\frac{q+1}{2}}} = q^{2n} \cdot \prod_{j=0}^{\sqrt{q}} \frac{\frac{q+1}{2}-j}{q+1-j} \le \frac{q^{2n}}{2^{\sqrt{q}}}$$

$$= \exp(2n \log q - \sqrt{q}\log 2) \le \exp(2(\log q)^2 - \sqrt{q}\log 2),$$

which tends to 0 as $q \to \infty$. This completes the proof. $\qquad\square$

The proof of Theorem 1.4 is similar to the proof of Proposition 3.1, but we instead consider the "most efficient" non-canonical maximum clique in terms of the number of $\mathbb{F}_q^*$-cosets needed to cover it.

Proof of Theorem 1.4. Let $V \subset \mathbb{F}_{q^2}$ be an $\mathbb{F}_{p^t}$-subspace of size q such that V is not an $\mathbb{F}_q$-subspace. Note that the intersection between V and an $\mathbb{F}_q^*$-coset (together with 0) is an $\mathbb{F}_{p^t}$-subspace. Thus, the intersection between V and each $\mathbb{F}_q^*$-coset has size 0 or at least $p^t - 1$. It follows that at most $\frac{q-1}{p^t-1}$ many $\mathbb{F}_q^*$-cosets are needed to cover $V \setminus \{0\}$.

We consider the family of Peisert-type graphs of type (m, q). Let $X = \mathrm{Cay}(\mathbb{F}_{q^2}^+, S)$ be a Peisert-type graph of type (m, q), such that V is a (maximum) clique in X. Note that V is a non-canonical clique in X provided that S is the union of m many $\mathbb{F}_q^*$-cosets, with at most $\frac{q-1}{p^t-1}$ of them having been prescribed in order to cover $V \setminus \{0\}$. It follows that the density of Peisert-type graphs of type (m, q) without the strict-EKR property (due to V) is at least

$$\frac{\binom{q+1-(q-1)/(p^t-1)}{m-(q-1)/(p^t-1)}}{\binom{q+1}{m}} = \prod_{j=0}^{(q-1)/(p^t-1)-1} \frac{m-j}{q+1-j} \ge \left(\frac{m-(q-1)/(p^t-1)+1}{q+1-(q-1)/(p^t-1)+1} \right)^{(q-1)/(p^t-1)}$$

$$= \left(1 - \frac{q+1-m}{q+2-(q-1)/(p^t-1)} \right)^{(q-1)/(p^t-1)}$$

$$\ge 1 - \frac{q-1}{p^t-1} \cdot \frac{q+1-m}{q+2-(q-1)/(p^t-1)},$$

where we used Bernoulli's inequality for the last step. If $q - m = o(p^t)$, then the above lower bound approaches to 1 as $p \to \infty$. This shows that almost surely the strict-EKR property fails to hold under the given assumptions. $\qquad\square$

The following corollary follows from Theorem 1.4 immediately.

Corollary 3.2. *As $q \to \infty$ with q being a square, almost all Peisert-type graphs of type $(q - o(\sqrt{q}), q)$ do not have the strict-EKR property.*

4. STABILITY OF CANONICAL CLIQUES

4.1. **An explicit correspondence.** Let q be a fixed odd prime power. We establish an explicit connection between the structure of maximum cliques of Peisert-type graphs and the direction sets determined by subsets $U \subset \mathrm{AG}(2, q)$ with $|U| = q$. The observation is based on the idea of realizing a Peisert-type graph projectively (as opposed to affinely, which was the idea in the previous works [1, 2]). We start by picking a fixed $v \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ so that $\{1, v\}$ forms a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. This allows us to identify $\mathbb{F}_{q^2}$ and $\mathrm{AG}(2, q)$ via the embedding $\pi \colon \mathbb{F}_{q^2} \to \mathrm{AG}(2, q)$, where

$$\pi(a + bv) = (a, b), \quad \forall a, b \in \mathbb{F}_q.$$

We also define the map $\sigma\colon \mathrm{AG}(2,q) \setminus \{(0,0)\} \to \mathrm{PG}(1,q)$ such that

$$\sigma((a,b)) = [a:b], \quad \forall (a,b) \in \mathrm{AG}(2,q) \setminus \{(0,0)\}.$$

Let X be a Peisert-type graph $X = \mathrm{Cay}(\mathbb{F}_{q^2}^+, S)$ of type (m,q). We define *the direction set determined by* X to be $\mathcal{D}(X) := \sigma(\pi(S))$. Since S is the union of m many $\mathbb{F}_q^*$-cosets in $\mathbb{F}_{q^2}^*$, it follows that $\mathcal{D}(X)$ is a subset of $\mathrm{PG}(1,q)$ with size m. The following proposition describes the explicit connection that will be very helpful in establishing our main results.

Proposition 4.1. *Let* $X = \mathrm{Cay}(\mathbb{F}_{q^2}^+, S)$ *be a Peisert-type graph and let* $C \subset \mathbb{F}_{q^2}$. *Then we have the following correspondences:*

- *C is a clique in X if and only if $D(\pi(C)) \subset \mathcal{D}(X)$, equivalently, $\pi(C)$ is a D-set for some $D \subset \mathcal{D}(X)$.*
- *If $|C| = q$, then C is a canonical clique in X if and only $|D(\pi(C))| = 1$ and $D(\pi(C)) \subset \mathcal{D}(X)$.*

Proof. Let C be a clique. Let $x, y \in C$ with $x \neq y$. Let $\pi(x) = (a,b)$ and $\pi(y) = (c,d)$. Since C is a clique, it follows that $x - y = (a - c) + (b - d)v \in S$. Therefore, the direction

$$[a - c : b - d] = \sigma((a - c, b - d)) = \sigma(\pi(x - y)) \in \sigma(\pi(S)) = \mathcal{D}(X).$$

This shows that $D(\pi(C)) \subset \mathcal{D}(X)$. Conversely, it is also easy to verify that $D(\pi(C)) \subset \mathcal{D}(X)$ implies that C is a clique.

If C is a canonical clique, then $C - C = \alpha \mathbb{F}_q$ for some $\alpha \in \mathbb{F}_{q^2}^*$, so

$$D(\pi(C)) = \sigma(\pi((C - C) \setminus \{0\})) = \sigma(\pi(\alpha))$$

is a singleton set. Conversely, if $|D(\pi(C))| = 1$, then all points in $\pi(C)$ are collinear, and it is easy to verify that $C = \pi^{-1}(\pi(C))$ is a canonical clique. $\qquad\square$

Remark 4.2. Proposition 4.1, together with [2, Theorem 3.2], immediately imply Theorem 2.1. This new proof is much simpler than the original proof in [2, Theorem 1.2].

4.2. **Proof of Theorem 1.2 and Theorem 1.3.** In Proposition 3.1, we have shown that almost all Peisert-type graphs of type $(\frac{q+1}{2}, q)$ have the strict-EKR property. The next proposition shows that the strict-EKR property can be strengthened to the property $\mathrm{ST}(\sqrt{q}/2)$ in the generic case.

Proposition 4.3. *Let* X *be a Peisert-type graph of type* $(\frac{q+1}{2}, q)$ *with the strict-EKR property. If* $\mathcal{D}(X) \notin \mathcal{B}_q$, *then* X *has the property* $\mathrm{ST}(\sqrt{q}/2)$. *Moreover, if* $q = p$ *is a prime, then* X *has the property* $\mathrm{ST}(p/20)$.

Proof. Let C be a clique in X with $|C| \geq q - \sqrt{q}/2$. To show X has the property $\mathrm{ST}(\sqrt{q}/2)$, it suffices to show that C is contained in a canonical clique. Let $U = \pi(C)$ and let $D = D(U)$; Proposition 4.1 implies that U is a D-set with $D \subset \mathcal{D}(X)$. Thus, $|D| \leq \frac{q+1}{2}$ and $D \notin \mathcal{B}_q$. It follows from Corollary 2.10 that U can be extended a D-set V with $|V| = q$. In particular, by Proposition 4.1, $C' := \pi^{-1}(V)$ is a maximum clique in X with $C \subset C'$. Since X has the strict-EKR property, C' must be a canonical clique. Therefore, X has the property $\mathrm{ST}(\sqrt{q}/2)$. The proof for the case that $q = p$ is a prime is similar. $\qquad\square$

Remark 4.4. Let X be the Paley graph of order q^2. We know that X has the strict-EKR property [6]. If we can show that $\mathcal{D}(X) \notin \mathcal{B}_q$, then one can apply Proposition 4.3 to get the first nontrivial progress towards the conjecture by Baker et. al [3] mentioned in the introduction. However, it

seems more inputs from algebraic geometry are needed to understand the distribution of rational points of conics.

Now we are ready to present the proof of Theorem 1.2.

Proof of Theorem 1.2. By Proposition 3.1, as $q \to \infty$, almost all Peisert-type graphs of type $(\frac{q+1}{2}, q)$ have the strict-EKR property. By Corollary 2.8, as $q \to \infty$, almost all Peisert-type graphs X of type $(\frac{q+1}{2}, q)$ satisfies $\mathcal{D}(X) \notin \mathcal{B}_q$ since the map $X \mapsto \mathcal{D}(X)$ is injective, and $q^5/\binom{q+1}{(q+1)/2} \to 0$. Therefore, Proposition 4.3 allows us to conclude that as $q \to \infty$, almost all Peisert-type graphs of type $(\frac{q+1}{2}, q)$ have the property $\mathrm{ST}(\sqrt{q}/2)$. $\qquad\square$

Finally, we discuss the situation where $q = p$ is a prime. In this case, we can prove stronger results with the help of Theorem 2.4.

Proposition 4.5. *As $p \to \infty$, almost all Peisert-type graphs of type $(\lfloor \frac{2p-2}{3} \rfloor, p)$ have the strict-EKR property.*

Proof. Let C be a non-canonical clique (containing 0) in a Peisert-type graph X of type $(\lfloor \frac{2p-2}{3} \rfloor, p)$. By Proposition 4.1, $U = \pi(C)$ is a D-set for some $D \subset \mathcal{D}(X)$ with $|D| \geq 2$. Note that if $|D| > \frac{p+3}{2}$, then $|D| \geq \lfloor \frac{2p+1}{3} \rfloor$ by Theorem 2.4, which is impossible since $|\mathcal{D}(X)| = \lfloor \frac{2p-2}{3} \rfloor$. Therefore, in view of Theorem 2.4, we must have $|D(U)| = \frac{p+3}{2}$; furthermore, U is affinely equivalent to the set $\{(x, x^{(p+1)/2}) : x \in \mathbb{F}_p\}$. It follows that there exists an invertible matrix $M \in \mathrm{GL}_2(\mathbb{F}_p)$ such that

$$U = M\{(x, x^{(p+1)/2}) : x \in \mathbb{F}_p\}.$$

Since $|\mathrm{GL}_2(\mathbb{F}_p)| < p^4$, the number of possible direction sets $D = D(U)$ is at most p^4.

As a quick summary, if X is a Peisert-type graph X of type $(\lfloor \frac{2p-2}{3} \rfloor, p)$ without the strict-EKR property, then it must contain a non-canonical clique C such that $|D(\pi(C))| = \frac{p+3}{2}$ and $D(\pi(C)) \subset \mathcal{D}(X)$; furthermore, the number of possible candidates for $D(\pi(C))$ is at most p^4. This allows us to mimic the proof of Proposition 3.1 and conclude that the density of Peisert-type graphs X of type (m, p) with $m = \lfloor \frac{2p-2}{3} \rfloor$ such that the strict-EKR property fails is at most

$$p^4 \cdot \frac{\binom{(p+1) - \frac{p+3}{2}}{m - \frac{p+3}{2}}}{\binom{p+1}{m}} < \frac{p^4}{(\frac{p+1}{m})^{(p+3)/2}} < \frac{p^4}{(\frac{3}{2})^{(p+3)/2}} \to 0$$

as $p \to \infty$. This completes the proof. $\qquad\square$

When $q = p^2$, we can also provide the following improvement on Proposition 3.1:

Proposition 4.6. *As $p \to \infty$, almost all Peisert-type graphs of type $(\frac{p^2+p}{2}, p^2)$ have the strict-EKR property.*

Proof. By Proposition 3.1, as $p \to \infty$, almost all Peisert-type graphs of type $(\frac{p^2+1}{2}, p^2)$ have the strict-EKR property. To prove the stronger result, one can mimic the proof of Proposition 3.1 and Proposition 4.5 with the help of Theorem 2.5. We omit the detailed analysis since the proof would be very similar. $\qquad\square$

We conclude the paper by proving Theorem 1.3.

Proof of Theorem 1.3. It follows from Proposition 3.1, Proposition 4.3, and Proposition 4.5. The proof is similar to the proof of Theorem 1.2. $\qquad\square$

ACKNOWLEDGEMENT

REFERENCES

[1] S. Asgarli, S. Goryainov, H. Lin, and C. H. Yip. The EKR-Module Property of Pseudo-Paley Graphs of Square Order. *Electron. J. Combin.*, 29(4):Paper No. 4.33, 2022.

[2] S. Asgarli and C. H. Yip. Van Lint–MacWilliams' conjecture and maximum cliques in Cayley graphs over finite fields. *J. Combin. Theory Ser. A*, 192:Paper No. 105667, 23, 2022.

[3] R. D. Baker, G. L. Ebert, J. Hemmeter, and A. Woldar. Maximal cliques in the Paley graph of square order. *J. Statist. Plann. Inference*, 56(1):33–38, 1996. Special issue on orthogonal arrays and affine designs, Part I.

[4] S. Ball. The number of directions determined by a function over a finite field. *J. Combin. Theory Ser. A*, 104(2):341–350, 2003.

[5] J. Balogh, T. Bohman, and D. Mubayi. Erdős-Ko-Rado in random hypergraphs. *Combin. Probab. Comput.*, 18(5):629–646, 2009.

[6] A. Blokhuis. On subsets of $GF(q^2)$ with square differences. *Nederl. Akad. Wetensch. Indag. Math.*, 46(4):369–372, 1984.

[7] A. Blokhuis, S. Ball, A. E. Brouwer, L. Storme, and T. Szőnyi. On the number of slopes of the graph of a function defined on a finite field. *J. Combin. Theory Ser. A*, 86(1):187–196, 1999.

[8] A. E. Brouwer, R. M. Wilson, and Q. Xiang. Cyclotomy and strongly regular graphs. *J. Algebraic Combin.*, 10(1):25–28, 1999.

[9] P. Erdős, C. Ko, and R. Rado. Intersection theorems for systems of finite sets. *Quart. J. Math. Oxford Ser. (2)*, 12:313–320, 1961.

[10] A. Gács. On a generalization of Rédei's theorem. *Combinatorica*, 23(4):585–598, 2003.

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

[12] C. Godsil and K. Meagher. *Erdős-Ko-Rado theorems: algebraic approaches*, volume 149 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2016.

[13] S. Goryainov, L. Shalaginov, and C. H. Yip. On eigenfunctions and maximal cliques of generalised Paley graphs of square order. *Finite Fields Appl.*, 87:Paper No. 102150, 2023.

[14] L. Lovász and A. Schrijver. Remarks on a theorem of Rédei. *Studia Sci. Math. Hungar.*, 16(3-4):449–454, 1983.

[15] N. Mullin. Self-complementary arc-transitive graphs and their imposters. Master's thesis, University of Waterloo, 2009.

[16] L. Rédei. *Lacunary polynomials over finite fields*. North-Holland Publishing Co., Amsterdam-London; American Elsevier Publishing Co., Inc., New York, 1973. Translated from the German by I. Földes.

[17] T. Szőnyi. On the number of directions determined by a set of points in an affine Galois plane. *J. Combin. Theory Ser. A*, 74(1):141–146, 1996.

[18] T. Szőnyi. Around Rédei's theorem. *Discrete Math.*, 208/209:557–575, 1999.

[19] P. Sziklai. On subsets of $GF(q^2)$ with dth power differences. *Discrete Math.*, 208/209:547–555, 1999.

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

Email address: kyleyip@math.ubc.ca