Extremal Peisert-type graphs without strict-EKR property

Sergey Goryainov
(Hebei Normal University)

based on joint work in progress with

Chi Hoi Yip

The 8th Workshop "Algebraic Graph Theory and its Applications"

March 1st, 2023

Cayley graphs

Let p be a 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 the elements of G, such that two vertices g and h are adjacent if and only if $g - h \in S$.

Peisert-type graphs

Let $S \subset \mathbb{F}_{q^2}^*$ be a union of $m \leq q$ cosets of $\mathbb{F}_q^*$ in $\mathbb{F}_{q^2}^*$, that is,

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

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

Comments on the definition of Peisert-type graphs

While Peisert-type graphs were introduced formally recently [AY22], [AGLY22], they can date back to the construction of cyclotomic strongly regular graphs due to Brouwer, Wilson, and Xiang [BWX99] around 20 years ago.

The definition of Peisert-type graphs is motivated by the well-studied Paley graphs and Peisert graphs, which are only defined in finite fields with odd characteristic. However, the definition of Peisert-type graphs naturally extends to finite fields with characteristic 2.

[AGLY22] S. Asgarli, S. Goryainov, H. Lin, C. H. Yip, *The EKR-module property of pseudo-Paley graphs of square order*, Electron. J. Combin. **29** (2022), no. 4, #P4.33.

[AY22] S. Asgarli, C. H. Yip, *Van Lint-MacWilliams' conjecture and maximum cliques in Cayley graphs over finite fields*, J. Combin. Theory Ser. A **192** (2022), Paper No. 105667, 23 pp.

[BWX99] A. E. Brouwer, R. M. Wilson, and Q. Xiang, *Cyclotomy and strongly regular graphs*, J. Algebraic Combin. **10**(1),25–28, 1999.

Intersections of the the class of Peisert-type graphs with some other classes

- Paley graphs $P(q^2)$ of square order are Peisert-type graphs;
- Peisert graphs $P^*(q^2)$, where $q \equiv 3 \pmod 4$, are Peisert-type graphs (not all Peisert graphs are Peisert-type graphs);
- Generalised Paley graphs $GP(q^2, d)$, where $d \mid (q+1)$ and $d > 1$ (not all generalised Paley graphs are Peisert-type graphs);
- Generalised Peisert graphs $GP^*(q^2, d)$, where $d \mid (q+1)$ and d is even (not all generalised Peisert graphs are Peisert-type graphs).

Delsarte-Hoffman bound

For the clique number $\omega(X)$ of a strongly regular graph X, the Delsarte-Hoffman bound holds:

$$\omega(\Gamma) \leq 1 - \frac{k}{\theta_{\min}},$$

where $\theta_{\min}$ is the smallest eigenvalue of X.

A clique in a strongly regular graph is a Delsarte clique if its size is equal to the Delsarte-Hoffman bound.

Canonical cliques in Peisert-type graphs

Peisert-type graphs are strongly regular graphs.

Desarte-Hoffman bound implies that the clique number is at most q.

From the decomposition of the connection set into $\mathbb{F}_q^*$-cosets, it is clear that translates of $c_1\mathbb{F}_q, c_2\mathbb{F}_q, \ldots, c_m\mathbb{F}_q$ are Delsarte (in particular, maximum) cliques in X. These cliques are known as the canonical cliques in X and we say X has the strict-EKR property if all maximum cliques in X are canonical.

Such a terminology is reminiscent to the classical Erdős-Ko-Rado (EKR) theorem, where all maximum families of k-element subsets of $\{1, 2, \ldots, n\}$ are canonical intersecting whenever $n \geq 2k + 1$. There are lots of combinatorial objects where an analogue of the EKR theorem holds; we refer to the book by Godsil and Meagher [GM15] for a general discussion on EKR-type results.

[GM15] C. D. Godsil, K. Meagher, *Erdös-Ko-Rado Theorems: Algebraic Approaches*, Cambridge University Press (2015).

Subspace structure of Delsarte cliques in Peisert-type graphs

Theorem 1 ([AY22, Theorem 1.2])

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

[AY22] S. Asgarli, C. H. Yip, *Van Lint-MacWilliams' conjecture and maximum cliques in Cayley graphs over finite fields*, J. Combin. Theory Ser. A **192** (2022), Paper No. 105667, 23 pp.
https://doi.org/10.1016/j.jcta.2022.105667

Extremal Peisert-type graphs without strict-EKR property

Let X be a Peisert-type graph of type (m, q) without strict EKR-property. We say that X is extremal if all Peisert-type graphs of type $(m-1, q)$ have the strict-EKR property.

Theorem 2 ([AGLY22])

If $q > (m-1)^2$, then all Peisert-type graphs of type (m, q) have the strict-EKR property. Moreover, when q is a square, there exists an extremal Peisert-type graph of type $(\sqrt{q}+1, q)$ without the strict-EKR property.

However, an explicit construction of extremal Peisert-type graphs of type $(\sqrt{q}+1, q)$ without the strict-EKR property was not given in [AGLY22].

[AGLY22] S. Asgarli, S. Goryainov, H. Lin, C. H. Yip, *The EKR-module property of pseudo-Paley graphs of square order*, Electron. J. Combin. **29** (2022), no. 4, #P4.33.

Main problem

Problem 1

Determine all extremal Peisert-type graphs without strict-EKR property.

Outline

In this talk, we investigate extremal Peisert-type graphs of type (m, q) and consider the following cases:

- q is prime
- q is not prime
  - a bound $B(q)$ for m and its tightness
  - uniqueness of the extremal graphs in case when q is a square
  - uniqueness of the extremal graphs in case when q is a cube, but not a square
  - non-uniqueness of the extremal graphs in case $q = 2^5$

We also discuss some related problems.

The set of directions of a subsets of points of an affine plane

Let U be a subset of $\mathrm{AG}(2,q)$; the set of directions determined by U is defined to be

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

The theory of directions has been developed by Rédei [R73], Szőnyi [S99], and many other authors. It is of particular interest to estimate $|D(U)|$.

[R73] 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.

[S99] 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.

Summary of the results on the size of $D(U)$; q is prime

Theorem 3

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

- *(Rédei* [R73]*). If the points in U are not all collinear, then U determines at least $\frac{p+3}{2}$ directions.*
- *(Lovász and Schrijver* [LS83]*) 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* [G03]*) If U determines more than $\frac{p+3}{2}$ directions, then it determines at least $\lfloor \frac{2p+1}{3} \rfloor$ directions.*

[R73] 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.

[LS83] L. Lovász, A. Schrijver, *Remarks on a theorem of Rédei*, Studia Sci. Math. Hungar., 16 (1983) 449–454.

[G03] A. Gács, *On a generalization of Rédei's theorem.* Combinatorica, 23(4):585–598, 2003.

Exstremal Peisert-type graphs without strict EKR-property; q is prime

Corollary 1 (G., Yip, 2023+)

If q is prime and $q \geq 7$, then there exists a unique (up to isomorphism) Peisert-type graph of type $(\frac{q+3}{2}, q)$ that fails to have the strict-EKR property.

Bound for extremal Peisert-type graphs without strict-EKR property

Theorem 4 (G., Yip, 2023+)

Let $q = p^n$ with $n > 1$. Let k be the largest proper divisor of n. Then any Peisert-type graph of type (m, q) has the strict-EKR property provided that $m \leq p^{m-k}$. Moreover, in a Peisert-type graph of type $(p^{n-k}+1, q)$, each maximum clique containing 0 is a $\mathbb{F}_{p^k}$-subspace in $\mathbb{F}_{q^2}$.

Let $B(q) = p^{n-k}$.

Graphs $Y_{q,n}$

Let $q = r^n$, where r is a prime power and n is prime. Assume $\mathbb{F}_{q^2} = \{x + y\beta : x, y \in \mathbb{F}_q\}$, where β is a root of an irreducible polynomial $f(t) = t^2 - d \in \mathbb{F}_q[t]$.

Considering $\mathbb{F}_{r^n}$ as a n-dimensional $\mathbb{F}_r$-vector space underlying the affine space $\mathrm{AG}(n, r)$, let H be a an additive coset of a $(n-1)$-dimensional subspace in $\mathbb{F}_{r^n}$ (equivalently, let H be a hyperplane in $\mathrm{AG}(n, r)$). Note that $|H| = r^{n-1}$.

Let

$$S(H) = \mathbb{F}_q^* \cup \bigcup_{h \in H} (h + \beta)\mathbb{F}_q^*.$$

Let $Y_{q,n}(H)$ be the Peisert-type graph of type $(r^{n-1} + 1, r^n)$ defined by the generating set $S(H)$.

Proposition 1 (G., Yip, 2023+)

For any two hyperplanes H_1, H_2 in $AG(n, r)$, the graphs $Y_{q,n}(H_1)$ and $Y_{q,n}(H_2)$ are isomorphic.

We write $Y_{q,n}$ instead of $Y_{q,n}(H)$.

Given a prime power q, how many graphs $Y_{q,n}$ have we defined?

Let $q = p^m$, where p is prime and m is an integer, $m \geq 2$.

Let d be the number of different prime divisors of m. We have defined exactly d graphs of $Y_{q,n}$. Indeed, let $k_1, \ldots, k_d$ be the divisors of m such that

$$m/k_1, \ldots, m/k_d$$

are different primes and

$$m/k_1 < \ldots < m/k_d.$$

Put $n_i = m/k_i$ and $r_i = p^{k_i}$. Then, for any $i \in \{1, \ldots, d\}$, $q = r_i^{n_i}$ holds and we have defined the graphs $Y_{q,n_1}, \ldots, Y_{q,n_d}$.

Problem 2

Are these graphs minimal in terms of not having strict-EKR property?

Graphs $Y_{q,n}$ are Peisert-type graphs without strict-EKR property

Let $q = r^n$, where r is a prime power and n is prime. Consider the graph $Y_{q,n}$.

Theorem 5 (G., Yip, 2023+)

The following statements hold.
(1) *The graph $Y_{q,n}$ is a Peisert-type graph of type $(r^{n-1}+1, r^n)$.*
(2) *The graph $Y_{q,n}$ fails to have the strict-EKR property.*

Conjecture 1

The graph $Y_{q,n}$ has exactly $(r^n-1)/(r-1)$ non-canonical cliques containing 0.

A classification of extremal Peisert-type graphs without strict-EKR property

Theorem 6 (G., Yip, 2023+)

Let $q = p^m$, where p is prime and m is an integer $m \geq 2$. Let $k_1, \ldots, k_d$ be the divisors of m such that

$$m/k_1, \ldots, m/k_d$$

are different primes and

$$m/k_1 < \ldots < m/k_d.$$

Let $n_1 = m/k_1$ and $r_1 = p^{k_1}$. Then the following statements hold.
(1) Y_{q,n_1} is an extremal Peisert-type graph without strict-EKR property.
(2) If $n_1 \in \{2, 3\}$, then Y_{q,n_1} is the only (up to isomorphism) extremal Peisert-type graph without strict-EKR property.

Furher classification

If $q = 2^5$, then there exists exactly two non-isomorphic extremal graphs without strict-EKR property ($Y_{32,5}$ and one more).

Conjecture 2

If $n_1 \geq 5$, then there exist at least two non-isomorphic extremal graphs without strict-EKR property.

Graphs $Y_{q,2}(\mathbb{F}_r)$ and X_q

Let $q = r^2$. Note that $\mathbb{F}_r$ is a hyperplane (a line) in $\mathrm{AG}(2, r)$. Consider the extremal Peisert-type graph $Y_{q,2}(\mathbb{F}_r)$ of type $(r+1, q)$. We have put $H = \mathbb{F}_r$ in the definition of $Y_{q,2}(H)$.

Let $Q = \{\gamma \in \mathbb{F}_q^* \mid \gamma^{r+1} = 1\}$.

Let $S = \bigcup_{\delta \in Q} (\delta + \beta)\mathbb{F}_q^*$.

Let X_q be the Peisert-type graph of type $(r+1, q)$ defined by the generating set S.

Theorem 7 (G., Yip, 2023+)

The graphs $Y_{q,2}(\mathbb{F}_r)$ and X_q are isomorphic.

Proof.

The generating set $S(\mathbb{F}_r)$ can be obtained from S by multiplication (from the left) by any non-degenerate matrix $\begin{pmatrix} \sigma & \sigma^r \\ 1 & 1 \end{pmatrix}$, where $\sigma \neq \sigma^r$. $\square$

The graph X_q

The graph X_q has some interesting properties, and we devote the rest of the talk to this graph.

A non-canonical clique in X_q

Let ε be a primitive element of $\mathbb{F}_q$. Consider a 2-dimensional $\mathbb{F}_{\sqrt{q}}$-subspace in $\mathbb{F}_{q^2}$:

$$C_q = (1+\beta)\mathbb{F}_{\sqrt{q}} + (\varepsilon^{\sqrt{q}} + \varepsilon\beta)\mathbb{F}_{\sqrt{q}} =$$

$$= \{(1+\beta)a + (\varepsilon^{\sqrt{q}} + \varepsilon\beta)b \mid a, b \in \mathbb{F}_{\sqrt{q}}\} =$$

$$= \{a + b\varepsilon^{\sqrt{q}} + (a + b\varepsilon)\beta \mid a, b \in \mathbb{F}_{\sqrt{q}}\} =$$

$$= \{(a + b\varepsilon)^{\sqrt{q}} + (a + b\varepsilon)\beta \mid a, b \in \mathbb{F}_{\sqrt{q}}\} =$$

$$= \{\gamma^{\sqrt{q}} + \gamma\beta \mid \gamma \in \mathbb{F}_q\} =$$

$$= \{\gamma(\gamma^{\sqrt{q}-1} + \beta) \mid \gamma \in \mathbb{F}_q\} \subset S \cup \{0\}.$$

All non-canonical cliques in X_q

Proposition 2 (G., Yip, 2023+)

The subspace C_q induces a non-canonical clique in X_q. Moreover, the intersection of any canonical clique in X_q containing 0 *and C_q has exactly $\sqrt{q}-1$ nonzero elements (these elements are given by the elements $\gamma \in \mathbb{F}_q^*$ lying in the same coset of $\mathbb{F}_{\sqrt{q}}^*$ in $\mathbb{F}_q^*$.*

Corollary 2 (G., Yip, 2023+)

For any $i \in \{0, 1, \dots, \sqrt{q}\}$, the set $\varepsilon^i C_q$ induces a non-canonical clique in X_q, and, for any $i, j \in \{0, 1, \dots, \sqrt{q}\}$ such that $i \neq j$, we have $\varepsilon^i C_q \cap \varepsilon^j C_q = \{0\}$.

Proposition 3 (G., Yip, 2023+)

The $\sqrt{q}+1$ non-canonical cliques $\{C_q, \varepsilon C_q, \varepsilon^2 C_q, \dots, \varepsilon^{\sqrt{q}} C_q\}$ are the only non-canonical cliques in X_q containing 0.

Hyperbolic quadric

Let V be a $(2e)$-dimensional vector space over a finite field $\mathbb{F}_q$, where $e \geq 2$ and q is a prime power, provided with the hyperbolic quadratic form

$$HQ(x) = x_1x_2 + x_3x_4 + \ldots + x_{2e-1}x_{2e}.$$

The set HQ^+ of zeroes of HQ is called the hyperbolic quadric, where e is the maximal dimension of a subspace in Q^+.

Affine polar graphs $VO^+(2e, q)$

Denote by $VO^+(2e, q)$ the graph on V with two vectors x, y being adjacent if and only if $HQ(x - y) = 0$. The graph $VO^+(2e, q)$ is known as an affine polar graph.

Lemma 1 ([BV22])

The graph $VO^+(2e, q)$ is a vertex-transitive strongly regular graph with parameters

$$\begin{aligned} v &= q^{2e} \\ k &= (q^{e-1} + 1)(q^e - 1) \\ \lambda &= q(q^{e-2} + 1)(q^{e-1} - 1) + q - 2 \\ \mu &= q^{e-1}(q^{e-1} + 1) \end{aligned} \tag{1}$$

and eigenvalues $r = q^e - q^{e-1} - 1$, $s = -q^{e-1} - 1$.

[BV22] A. E. Brouwer and H. Van Maldeghem, *Strongly Regular Graphs*, Cambridge University Press, Cambridge (2022).

X_q is isomoprhic to $VO^+(4, \sqrt{q})$

Let $V(n,r)$ be a n-dimensional vector space over the finite field $\mathbb{F}_r$, where $n \geq 2$ and r is a prime power. Let $f(x_1, x_2, \ldots, x_n) : V(n,r) \mapsto \mathbb{F}_r$ be a quadratic form on $V(n,r)$. Define a graph G_f on the set of vectors of $V(n,r)$ as follows:

$$\text{for any } u, v \in V(n,r), u \sim v \text{ if any only if } f(u-v) = 0.$$

Two quadratic forms $f_1(x_1, x_2, \ldots, x_n)$ and $f_2(y_1, y_2, \ldots, y_n)$ are said to be equivalent if there exists an invertible matrix $B \in GL(n,r)$ such that $f_1(Bx) = f_2(y)$.

Lemma 2

Let f_1 and f_2 be two equivalent quadratic forms. Then the graphs G_{f_1} and G_{f_2} are isomorphic.

Corollary 3 (G., Yip, 2023+)

The graphs X_q and $VO^+(4, \sqrt{q})$ are isomorphic.

An induced complete bipartite subgraph in X_q

The fact that X_q is isomorphic to $VO^+(4, \sqrt{q})$ establishes a connection with the talk of Rhys Evans on extremal eigenfunctions of polar and affine polar graphs.

Let $T_0 = Q$ and $T_1 = Q\beta$. Note that T_0 and T_1 are subsets of the lines with slopes 1 and β in $AG(2, q)$. These lines do not intersect with S and thus are cocliques in X_q, which means that T_0 and T_1 are cocliques.

Let $\gamma_1 \in T_0$ and $\gamma_2\beta \in T_1$ be two arbitrary elements from the cocliques T_0 and T_1. Consider their difference and take into account that Q is a subgroup of order $\sqrt{q}+1$ in $\mathbb{F}_q^*$ and $-Q = Q$:

$$\gamma_2\beta - \gamma_1 = \gamma_2 + \gamma_1'\beta = \gamma_1'(\gamma_2(\gamma_1')^{-1} + \beta) = \gamma_1'(\gamma_2' + \beta) \in S,$$

where γ_1', γ_2' are uniquely determined elements from Q. This means that $T_0 \cup T_1$ induces a complete bipartite subgraph in X_q with parts T_0 and T_1 of size $\sqrt{q}+1$.

WDB is tight for the negative eigenvalue of $X_q \simeq VO^+(4, \sqrt{q})$

Define a function $f : \mathbb{F}_{q^2} \mapsto \mathbb{R}$ by the following rule:

$$f(\gamma) = \begin{cases} 1, & \gamma \in T_0; \\ -1, & \gamma \in T_1; \\ 0, & \gamma \notin T_0 \cup T_1. \end{cases}$$

Proposition 4 (G., Yip, 2023+)

The function f is a $(-\sqrt{q} - 1)$-eigenfunction of X_q whose cardinality of support is $2(\sqrt{q} + 1)$.

Corollary 4 (G., Yip, 2023+)

The weight-distribution bound is tight for the negative non-principal eigenvalue $-\sqrt{q} - 1$ of $X_q \simeq VO^+(4, \sqrt{q})$.

Problem 3

Characterise $(-\sqrt{q} - 1)$-eigenfunctions of X_q whose cardinality of support meets the weight-distribution bound $2(\sqrt{q} + 1)$.

Orthogonal arrays and their block graphs

An orthogonal array $OA(m, n)$ is an $m \times n^2$ array with entries from an n-element set W with the property that the columns of any $2 \times n^2$ subarray consist of all n^2 possible pairs.

The block graph of an orthogonal array $OA(m, n)$, denoted $D_{OA(m,n)}$, is defined to be the graph whose vertices are columns of the orthogonal array, where two columns are adjacent if there exists a row in which they have the same entry.

Let $S_{r,i}$ be the set of columns of $OA(m, n)$ that have the entry i in row r. These sets are cliques, and since each element of the n-element set W occurs exactly n times in each row, the size of $S_{r,i}$ is n for all i and r. These cliques are called the canonical cliques in the block graph $D_{OA(m,n)}$.

A simple combinatorial argument shows that the block graph of an orthogonal array is strongly regular (see [GM15, Theorem 5.5.1]).

[GM15] C. D. Godsil, K. Meagher, *Erdös-Ko-Rado Theorems: Algebraic Approaches*, Cambridge University Press (2015).

Peisert-type graphs are block graphs of orthogonal arrays

In [AGLY22, Theorem 4], we showed that each Peisert-type graph of type (m, q) can be realised as the block graph of an orthogonal array $OA(m, q)$. Moreover, there is a one-to-one correspondence between canonical cliques in the block graph and canonical cliques in a given Peisert-type graph. Note that the size of the canonical cliques in the block graphs of orthogonal arrays meets the Delsarte bound.

[AGLY22] S. Asgarli, S. Goryainov, H. Lin, C. H. Yip, *The EKR-module property of pseudo-Paley graphs of square order*, Electron. J. Combin. **29** (2022), no. 4, #P4.33.

A bound for block graphs of orthogonal arrays

Lemma 3 ([GM15, Corollary 5.5.3])

If $OA(m,n)$ is an orthogonal array with $n > (m-1)^2$, then the only cliques of size n in $D_{OA(m,n)}$ are canonical cliques.

Let $m-1$ be a prime power; then there exists an $OA(m, m-1)$ and, using MacNeish's construction [GM15, p. 98], it is possible to construct an $OA(m,(m-1)^2)$ from this array.

This larger orthogonal array has $OA(m, m-1)$ as a subarray, and thus the graph $D_{OA(m,(m-1)^2)}$ has the graph $D_{OA(m,m-1)}$ as an induced subgraph. Since this subgraph is isomorphic to $K_{(m-1)^2}$, it is a clique of size $(m-1)^2$ in $D_{OA(m,(m-1)^2}$ that is not canonical.

[GM15] C. D. Godsil, K. Meagher, *Erdös-Ko-Rado Theorems: Algebraic Approaches*, Cambridge University Press (2015).

Subarray structure of the non-canonical cliques in X_q

Problem 4 ([GM15, Problem 16.4.2])

Assume that $OA(m,(m-1)^2)$ *is an orthogonal array and its orthogonal array graph has non-canonical cliques of size* $(m-1)^2$. *Do these non-canonical cliques form subarrays that are isomorphic to orthogonal arrays with entries from* $\{1,\ldots,m-1\}$*?*

Theorem 8 (G., Yip, 2023+)

The non-canonical cliques in X_q *form subarrays that are isomorphic to orthogonal arrays with entries from* $\{1,\ldots,\sqrt{q}\}$.

[GM15] C. D. Godsil, K. Meagher, *Erdös-Ko-Rado Theorems: Algebraic Approaches*, Cambridge University Press (2015).

Thank you for your attention!