On EKR properties of Peisert-type graphs

Sergey Goryainov
(Hebei Normal University)

based on joint work with

Shamil Asgarli, Huiqiu Lin and Chi Hoi Yip

6th Workshop on Algebraic Graph Theory and its Applications

Mathematical Center in Akademgorodok

March 23rd, 2022

Basic definitions

Let p be an odd prime, 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 of X such that any two of them are adjacent. For a graph X, the clique number of X, denoted $\omega(X)$, is the size of a maximum clique of X.

EKR properties

Given any graph X for which we can describe its canonical cliques (that is, typically cliques with large size and simple structure), we can ask whether X has any of the following three related Erdős-Ko-Rado (EKR) properties:

- EKR property: the clique number of X equals the size of canonical cliques.
- EKR-module property: the characteristic vector of each maximum clique in X is a $\mathbb{Q}$-linear combination of characteristic vectors of canonical cliques in X.
- strict-EKR property: each maximum clique in X is a canonical clique.

EKR-type results

The classical Erdős-Ko-Rado theorem [EKR61] classified maximum intersecting families of k-element subsets of $\{1, 2, ..., n\}$ when $n \geq 2k + 1$.

Since then, EKR-type results refer to understanding maximum intersecting families in a broader context, and more generally, classifying extremal configurations in other domains. The book [GM15] by Godsil and Meagher provides an excellent survey on the modern algebraic approaches to proving EKR-type results for permutations, set systems, orthogonal arrays, and so on.

[EKR61] P. Erdős, C. Ko, and R. Rado, Intersection theorems for systems of finite sets, Quart. J. Math. Oxford Ser. (2) 12 (1961), 313–320.

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

EKR-module property (I)

The EKR-type problems related to a transitive permutation group G can be reformulated in terms of the EKR properties of cocliques of the derangement graph $\Gamma(G)$, or equivalently, the cliques of the complement. Once we define canonical cocliques (or cliques), we can discuss the EKR properties of G after identifying G with $\Gamma(G)$.

The EKR-module property was first formally defined by Meagher [M19] in this context: a permutation group G naturally acts on the vector space W spanned by the characteristic vectors of canonical cliques, which makes W a G-module.

[M19] K. Meagher, *An Erdős-Ko-Rado theorem for the group* $PSU(3, q)$, Des. Codes Cryptogr. 87 (2019), no. 4, 717–744.

EKR-module property (II)

Each finite 2-transitive group has the EKR property [MSP16].

Meagher and Sin [MS21] recently showed that all finite 2-transitive groups have the EKR-module property. However, the strict-EKR property does not hold for permutations groups in general; recently, Meagher and Razafimahatratra [MR21] have shown that the general linear group $GL(2, q)$ is such a counterexample.

[MR21] K. Meagher and A. S. Razafimahatratra, *Erdős-Ko-Rado results for the general linear group, the special linear group and the affine general linear group*, arXiv:2110.08972

[MS21] K. Meagher and P. Sin, *All 2-transitive groups have the EKR-module property*, J. Combin. Theory Ser. A 177 (2021), Paper No. 105322, 21.

[MST16] K. Meagher, P. Spiga, and P. H. Tiep, *An Erdős-Ko-Rado theorem for finite 2-transitive groups*, European J. Combin. 55 (2016), 100–118.

EKR-module property (III)

We remark that our results are of similar flavour, although in our context of Peisert-type graphs, the corresponding vector space W does not carry a natural module structure. However, we remark that the definition of EKR-module property (even for permutation groups) does not need the additional G-module structure.

Module method

In general, the module method (see [AM15, Section 4]) refers to the strategy of proving that a graph Γ satisfies the strict-EKR property in two steps:

- show that Γ satisfies the EKR-module property
- show that EKR-module property implies the strict-EKR property

As an example of the module method, [AM15, Theorem 4.5] provides a sufficient condition for the second step above for 2-transitive permutation groups.

[AM15] B. Ahmadi and K. Meagher, *The Erdős-Ko-Rado property for some 2-transitive groups*, Ann. Comb. 19 (2015), no. 4, 621–640.

Blokhuis' result in terms of ERK properties

Consider the Paley graph P_{q^2} which is the Cayley graph defined on the additive group of $\mathbb{F}_{q^2}$, with the connection set being the set of squares in $\mathbb{F}^*_{q^2}$. Clearly, the subfield $\mathbb{F}_q$ forms a clique. Moreover, $a\mathbb{F}_q + b$ also forms a clique for each $a, b \in \mathbb{F}_{q^2}$ where a is a nonzero square. Such square translates of $\mathbb{F}_q$ are the canonical cliques [GM15, Section 5.9] in this example. Blokhuis proved that these are precisely the maximum cliques in P_{q^2}.

Theorem 1 ([B84, Theorem])

Let q be an odd prime power. The Paley graph P_{q^2} satisfies the strict-EKR property.

Godsil and Meagher [GM15, Section 5.9] call Theorem 1 the EKR theorem for Paley graphs.

[B84] A. Blokhuis, *On subsets of $GF(q^2)$ with square differences*, Indag. Math. **46** (1984) 369–372.

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

Extensions and generalizations of Blokhuis' result

Extensions and generalizations of Theorem 1 can be found in [BF91],[S99],[M09],[AY21] and [AY21a]. A Fourier analytic approach was recently proposed in [Y21, Section 4.4].

[BF91] A. A. Bruen and J. C. Fisher, *The Jamison method in Galois geometries*, Des. Codes Cryptogr. 1 (1991), no. 3, 199–205.

[S99] P. Sziklai, *On subsets of* $GF(q^2)$ *with* d*th power differences*, Discrete Math. 208/209 (1999), 547–555.

[M09] N. Mullin, *Self-complementary arc-transitive graphs and their imposters* (2009). Master's thesis, University of Waterloo.

[AY21] S. Asgarli and C. H. Yip, *Rigidity of maximum cliques in pseudo-Paley graphs from unions of cyclotomic classes*, arXiv:2110.07176

[AY21a] S. Asgarli and C. H. Yip, *Van Lint-MacWilliams' conjecture and maximum cliques in Cayley graphs over finite fields*, arXiv:2106.01522

[Y21] C. H. Yip, *Gauss sums and the maximum cliques in generalized Paley graphs of square order*, Funct. Approx. Comment. Math. (2021)

Peisert-type graphs

While we have at least three different proofs of Theorem 1, all known proofs rely heavily on advanced tools such as the polynomial method over finite fields.

Instead, in this work, we follow a purely combinatorial approach. Although we are not able to give a simple proof of Theorem 1, we prove that a weaker version of Theorem 1 extends to a larger family of Cayley graphs, namely Peisert-type graphs.

Let q be an odd prime power. Let $S \subset \mathbb{F}_{q^2}^*$ be a union of $m \leq q$ cosets of $\mathbb{F}_q^*$ in $\mathbb{F}_{q^2}^*$ such that $\mathbb{F}_q^* \subset S$, 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). A clique in X is called a canonical clique if it is the image of the subfield $\mathbb{F}_q$ under an affine transformation.

Some important examples of Peisert-type graphs

The following families of Cayley graphs are Peisert-type graphs (see [AY21a, Lemma 2.10]):

- Paley graphs of square order;
- Peisert graph with order q^2, where $q \equiv 3 \pmod 4$;
- Generalised Paley graphs $GP(q^2, d)$, where $d \mid (q+1)$ and $d > 1$;
- Generalised Peisert graphs $GP^*(q^2, d)$, where $d \mid (q+1)$ and d is even.

[AY21a] S. Asgarli and C. H. Yip, *Van Lint-MacWilliams' conjecture and maximum cliques in Cayley graphs over finite fields*, arXiv:2106.01522

Peisert-type graphs satisfy the EKR-module property

Blokhuis' theorem already implies that Paley graphs of square order possess the EKR-module property. In their book, Godsil and Meagher ask for an algebraic proof of this statement [GM15, Problem 16.5.1], which motivates our work.

Our main result answers this problem for a larger family of Cayley graphs:

Theorem 2 ([9, Theorem 1.3])
Peisert-type graphs satisfy the EKR-module property.

[AGLY22] S. Asgarli, S. Goryainov, H. Lin, C. H. Yip, *The EKR-module property of pseudo-Paley graphs of square order*, arXiv:2201.03100

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

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 T 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 $X_{OA(m,n)}$, 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 T 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 $X_{OA(m,n)}$. A simple combinatorial argument shows that the block graph of an orthogonal array is strongly regular.

A sufficient condition for the block graph of an orthogonal array to have strict-EKR property

Theorem 3 ([GM16, Corollary 5.5.3], [AGLY22, Theorem 2.8])
Let $X = X_{OA(m,n)}$ be the block graph of an orthogonal array $OA(m,n)$ with $n > (m-1)^2$. Then X has the strict-EKR property: the only maximum cliques in X are the columns that have entry i in row r for some $1 \leq i \leq n$ and $1 \leq r \leq m$.

[AGLY22] S. Asgarli, S. Goryainov, H. Lin, C. H. Yip, *The EKR-module property of pseudo-Paley graphs of square order*, arXiv:2201.03100

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

Connection between Peisert-type graphs and orthogonal arrays

The main ingredient in the proof of Theorem 2 is the following connection between Peisert-type graphs and orthogonal arrays, which is of independent interest.

Theorem 4 ([AGLY22, Theorem 1.4])

Each Peisert-type graph of type (m, q) can be realized 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.

We then were able to find two explicit eigenbases for the positive non-principal eigenvalue of the block graph of an orthogonal array, which led us to the result of Theorem 2 (more generally, it led us to the establishing of EKR-module property for the block graphs of orthogonal arrays).

[AGLY22] S. Asgarli, S. Goryainov, H. Lin, C. H. Yip, *The EKR-module property of pseudo-Paley graphs of square order*, arXiv:2201.03100

We remark that the idea of viewing certain Cayley graphs geometrically has appeared in the past; see for example [M09, Construction 5.2.1] and [AY21a, Section 4.2] for related discussion. However, Paley graphs and block graphs of orthogonal arrays are often treated independently; see for example [GR01, Chapter 5], and [AFMNSR21, Section 5]. Theorem 4 is the first to make an explicit connection between Peisert-type graphs and orthogonal arrays, and allows us to treat them in a uniform manner.

[M09] N. Mullin, *Self-complementary arc-transitive graphs and their imposters* (2009). Master's thesis, University of Waterloo.

[AY21a] S. Asgarli and C. H. Yip, *Van Lint-MacWilliams' conjecture and maximum cliques in Cayley graphs over finite fields*, arXiv:2106.01522

[GR01] C. Godsil and G. Royle, *Algebraic graph theory*, Graduate Texts in Mathematics, vol. 207, Springer-Verlag, New York, 2001.

[AFMNSR21] M. Adm, S. Fallat, K. Meagher, S. Nasserasr, M. N. Shirazi, and A. S. Razafimahatratra, Weakly Hadamard diagonalizable graphs, Linear Algebra Appl. 610 (2021), 86–119

Strongly regular graphs due to Brouwer, Wilson, and Xiang that generalise Peisert-type graphs

It is known that the block graph of an orthogonal array is strongly regular. Thus, Theorem 4 also implies the same conclusion for the Peisert-type graphs. We remark that Peisert-type graphs form a subfamily of a well-known family of strongly regular Cayley graphs defined on finite fields due to Brouwer, Wilson, and Xiang [12]: the connection set is a union of semi-primitive cyclotomic classes of $\mathbb{F}_{q^2}$. However, their proof heavily relied on the fact we can compute semi-primitive Gauss sums explicitly using Stickelberger's theorem and its variants; see [BWX99, Proposition 1] and [AY21, Corollary 3.6]. Theorem 4 can be proved using a purely combinatorial argument, thus giving an elementary proof of the corollary below.

[AY21] S. Asgarli and C. H. Yip, *Rigidity of maximum cliques in pseudo-Paley graphs from unions of cyclotomic classes*, arXiv:2110.07176

[BWX99] A. E. Brouwer, R. M. Wilson, and Q. Xiang, *Cyclotomy and strongly regular graphs*, J. Algebraic Combin. 10 (1999), no. 1, 25–28.

Peisert-type graphs are strongly regular

Corollary 1 ([AGLY22, Corollary 1.5])

A Peisert-type graph of type (m, q) is strongly regular with parameters $(q^2, m(q-1), (m-1)(m-2)+q-2, m(m-1))$ and eigenvalues $k = m(q-1)$ (with multiplicity 1), $-m$ (with multiplicity q^2-1-k) and $q-m$ (with multiplicity k). In particular, a Peisert-type graph of type $(\frac{q+1}{2}, q)$ is a pseudo-Paley graph.

[AGLY22] S. Asgarli, S. Goryainov, H. Lin, C. H. Yip, *The EKR-module property of pseudo-Paley graphs of square order*, arXiv:2201.03100

On Peisert-type graphs with strict-EKR property (I)

Corollary 2 ([AGLY22, Corollary 1.8])
If $q > (m-1)^2$, then all Peisert-type graphs of type (m, q) satisfy the strict-EKR property. In particular, if $d > \frac{q+1}{\sqrt{q}+1}$ and $d \mid (q+1)$, then the d-Paley graph $GP(q^2, d)$ has the strict-EKR property.

[AGLY22] S. Asgarli, S. Goryainov, H. Lin, C. H. Yip, *The EKR-module property of pseudo-Paley graphs of square order*, arXiv:2201.03100

On Peisert-type graphs with strict-EKR property (II)

It is natural to examine when a Peisert-type graph X enjoys the strict-EKR property. While we do not have a general answer to this problem, we exhibit an infinite family of Peisert-type graphs which fail to satisfy the strict-EKR property. The following theorem shows that the condition $q > (m-1)^2$ in Corollary 2 is sharp when q is a square.

Theorem 5 ([AGLY22, Theorem 1.9])

Let q be an odd prime power which is not a prime. Then there exists a Peisert-type graph X of order q^2 such that X fails to have the strict-EKR property. In particular, if q is a square, then there exists a Peisert-type graph X of type $(\sqrt{q}+1, q)$ which fails to have the strict-EKR property.

[AGLY22] S. Asgarli, S. Goryainov, H. Lin, C. H. Yip, *The EKR-module property of pseudo-Paley graphs of square order*, arXiv:2201.03100

Hadamard matrices and Hadamard diagonalisable graphs

Recall that a Hadamard matrix is a square matrix with entries 1 or -1 such that any two columns are mutually orthogonal.

Given an undirected graph G, the Laplacian matrix of G is defined as $L(G) = D(G) - A(G)$, where $D(G)$ is the diagonal matrix of vertex degrees of G and $A(G)$ is the adjacency matrix of G.

A graph G is called Hadamard diagonalisable if the Laplacian matrix of G can be diagonalised by a Hadamard matrix [BFK11].

[BFK11] S. Barik, S. Fallat, and S. Kirkland, *On Hadamard diagonalizable graphs*, Linear Algebra Appl. 435 (2011), no. 8, 1885–1902.

Weakly Hadamard matrices and weakly Hadamard diagonalisable graphs

Recently, Adm et al. [AFMNSR21] studied a larger class of graphs which contains some families of strongly regular graphs. In order to present this result, they introduced a broader class of matrices which include Hadamard matrices.

A square matrix is called weakly Hadamard if it satisfies the following two conditions:

- The entries of the matrix are from the set $\{-1, 0, 1\}$.
- There is an ordering of the columns of the matrix so that the non-consecutive columns are orthogonal.

A graph is weakly Hadamard diagonalisable if its Laplacian matrix can be diagonalised with a weakly Hadamard matrix.

[AFMNSR21] M. Adm, S. Fallat, K. Meagher, S. Nasserasr, M. N. Shirazi, and A. S. Razafimahatratra, *Weakly Hadamard diagonalizable graphs*, Linear Algebra Appl. 610 (2021), 86–119.

A sufficient condition of the block graph of an orthogonal array to be weakly Hadamard diagonalisable

A large class of block graphs of orthogonal arrays satisfy the definition of weakly Hadamard diagonalisable graphs according to the following theorem.

Theorem 6 ([AFMNSR21, Theorem 5.19])
Let $O = OA(m, n)$ be an orthogonal array that can be extended to an orthogonal array with $n + 1$ rows. Then its block graph X_O is weakly Hadamard diagonalisable.

[AFMNSR21] M. Adm, S. Fallat, K. Meagher, S. Nasserasr, M. N. Shirazi, and A. S. Razafimahatratra, *Weakly Hadamard diagonalizable graphs*, Linear Algebra Appl. 610 (2021), 86–119.

Peisert-type graphs are weakly Hadamard diagonalisable

Paley graphs are known to have a close connection with Paley's construction of Hadamard matrices [P33]. In [AFMNSR21, Theorem 5.9], it was shown that Paley graphs of square order are weakly Hadamard diagonalisable.

Our following theorem generalises their result.

Theorem 7 ([AGLY22, Theorem 1.6])
Peisert-type graphs are weakly Hadamard diagonalisable.

[AGLY22] S. Asgarli, S. Goryainov, H. Lin, C. H. Yip, *The EKR-module property of pseudo-Paley graphs of square order*, arXiv:2201.03100

[AFMNSR21] M. Adm, S. Fallat, K. Meagher, S. Nasserasr, M. N. Shirazi, and A. S. Razafimahatratra, Weakly Hadamard diagonalizable graphs, Linear Algebra Appl. 610 (2021), 86–119

[P33] R. E. A. C. Paley, *On orthogonal matrices*, J. Math. Phys., Mass. Inst. Techn. 12 (1933), 311–320.

Chromatic number and ERK theorem

The chromatic number of a graph X, denoted $\chi(X)$, is the smallest number of colours needed to colour the vertices of X so that no two adjacent vertices share the same colour.

We remark that one can prove the original EKR theorem using the (fractional) chromatic number of Kneser graphs [GR01, Theorem 7.8.1].

It is known that the chromatic number is lower bounded by the clique number, that is, $\omega(X) \leq \chi(X)$.

[GR01] C. Godsil and G. Royle, *Algebraic graph theory*, Graduate Texts in Mathematics, vol. 207, Springer-Verlag, New York, 2001.

On chromatic and clique numbers of generalised Paley graphs

Broere, Döman, and Ridley [BDR88] showed that if $d > 1$ and $d \mid (q+1)$, then both the chromatic number and the clique number of the generalized Paley graph $GP(q^2, d)$ is q.

The converse of this result was proved by Schneider and Silva [SS15, Theorem 4.7].

A stronger converse was proved recently in [Y21].

[BDR88] I. Broere, D. Dőman, and J. N. Ridley, *The clique numbers and chromatic numbers of certain Paley graphs*, Quaestiones Math. 11 (1988), no. 1, 91–93.

[SS15] C. Schneider and A. C. Silva, *Cliques and colorings in generalized Paley graphs and an approach to synchronization*, J. Algebra Appl. 14 (2015), no. 6, 1550088, 13.

[Y21] C. H. Yip, Gauss sums and the maximum cliques in generalized Paley graphs of square order, Funct. Approx. Comment. Math. (2021)

Chromatic and clique numbers of Peisert-type graphs graphs

Our following theorem computes both the chromatic and the clique number of all Peisert-type graphs, hence extending the first result on generalised Paley graphs since $GP(q^2, d)$ with $d \mid (q+1)$ is a Peisert-type graph.

Theorem 8 ([AGLY22, Theorem 1.7])
Let X be a Peisert-type graph of order q^2. Then $\omega(X) = \chi(X) = q$.

[AGLY22] S. Asgarli, S. Goryainov, H. Lin, C. H. Yip, *The EKR-module property of pseudo-Paley graphs of square order*, arXiv:2201.03100

Open problems (I)

Let X be a Peisert-type graph, and W be the vector space generated by the characteristic vectors of the canonical cliques in X. As we mentioned above, there is no obvious choice of a non-trivial group action on W. Finding such a group action, already in the case of the Paley graph, may give new insights on the EKR theorems.

Problem 1

Does there exist a 2-transitive permutation group G that acts linearly on the vector space W generated by the characteristic vectors of canonical cliques in the Paley graph P_{q^2}?

Another problem, motivated by the counterexamples found in Theorem 5, is the following.

Problem 2

Characterize Peisert-type graphs with the strict-EKR property.

Open problems (II)

Peisert-type graphs of order q^2 can be analogously defined in the case when q is a power of 2.

Problem 3

Investigate EKR properties of Peisert-type graphs in characteristic 2.

Note that we already have some progress on Problem 3.

Thank you for your attention!