On maximal cliques in Paley graphs of square order

Sergey Goryainov
(Hebei Normal University)
based on joint works with
Vladislav Kabanov, Alexander Masley, Leonid Shalaginov, Alexandr Valyuzhenich, Chi Hoi Yip

The 22nd AHU-USTC-AHJZU Joint International Seminar on Algebraic Combinatorics

July 8, 2023

Erdős–Ko–Rado theorem

The Erdős–Ko–Rado theorem, one of the fundamental results in combinatorics, provides information about systems of intersecting sets. A family $\mathcal{A}$ of subsets of a ground set — it might as well be $\{1, \ldots, n\}$ — is intersecting if any two sets in $\mathcal{A}$ have at least one point in common.

Theorem 1 (Erdős–Ko–Rado, 1961)

Let k and n be integers with $n \geq 2k$. If $\mathcal{A}$ is an intersecting family of k-subsets of $\{1, \ldots, n\}$, then

$$|\mathcal{A}| \leq \binom{n-1}{k-1}.$$

Moreover, if $n > 2k$, equality holds if and only if $\mathcal{A}$ consists of all the k-subsets that contain a given point from $\{1, \ldots, n\}$.

Extensions of Erdős–Ko–Rado theorem

This theorem has two parts: a bound and a characterisation of families that meet the bound.

One reason this theorem is so important is that it has many interesting extensions. In particular, it can be translated to a question in graph theory. The Kneser graph $K(n, k)$ has all k-subsets of $\{1, \ldots, n\}$ as its vertices, and two k-subsets are adjacent if they are disjoint. (We assume $n \geq 2k$ to avoid trivialities.)

Then an intersecting family of k-subsets is a coclique in the Kneser graph, and we see that the EKR theorem characterises the cocliques of maximum size in the Kneser graph. An intersecting family consisting of all subsets containing a given point is called canonical.

So we can seek to extend the EKR theorem by replacing the Kneser graphs by other interesting families of graphs.

The Hilton-Milner theorem (I)

Erdős, Ko and Rado conjectured that the largest 1-intersecting system that was not a subset of the canonical intersecting set system is the set of all k-subsets that contain at least two elements from a fixed set of three elements. It turns out that this conjecture is not true; the actual maximum sets were given by Hilton and Milner.

Hilton and Milner proved that the largest intersecting system that is not a subset of a canonical intersecting system can be constructed as follows. Let $\mathcal{F}_0$ be the set system of all k-sets that contain the element 1, and let $A = \{2, 3, \ldots, k+1\}$. Define $\mathcal{F}'$ to be the system of all the sets in $\mathcal{F}_0$ that intersect A, together with the set A. This system is intersecting and has size

$$\binom{n-1}{k-1} - \binom{n-k-1}{k-1} + 1.$$

The Hilton-Milner theorem (II)

The next result is known as the Hilton–Milner theorem.

Theorem 2 (Hilton-Milner, 1967)

Let k and n be positive integers with $2 \leq k \leq \frac{n}{2}$. Let $\mathcal{A}$ be an intersecting k-set system on an n-set such that $\bigcap_{A \in \mathcal{A}} A = \emptyset$. Then

$$|\mathcal{A}| \leq \binom{n-1}{k-1} - \binom{n-k-1}{k-1} + 1.$$

Moreover, for $k > 3$, equality holds if and only if $\mathcal{A}$ is isomorphic to the system of all sets in $\mathcal{F}_0$ that intersect $\{2, \ldots, k+1\}$ together with the set $\{2, \ldots, k+1\}$; for $k = 3$ there are two non-isomorphic systems that meet this bound, the one described above and one more.

Comments on the Hilton-Milner theorem

- Similar to the EKR theorem, the Hilton-Milner theorem has two parts: a bound and a characterisation of families that meet the bound.
- In other words, the Hilton-Milner theorem shows what is second largest size of a maximal intersecting family (w.r.t. inclusion) and gives their characterisation.
- In terms of graphs, this theorem gives a characterisation of second largest maximal cocliques in the Kneser graph $K(n,k)$ (second largest maximal cliques in the complement).

Structure of the maximal intersecting family from the Hilton-Milner theorem in terms of graphs

In terms of the complement of the Kneser graph $K(n,k)$, $2 \leq k \leq \frac{n}{2}$, the general second largest clique can be constructed as follows:

1. Take a canonical clique C.
2. Take a vertex x outside of C.
3. Let C_x be the set of neighbours of x in C.
4. The second largest clique is $\{x\} \cup C_x$.

Hilton-Milner theorems for graphs

Problem 1

Whenever an analogue of the EKR-theorem is proved for some family of graphs, investigate whether there holds an analogue of the Hilton-Milner theorem, that is, determine the size of the second largest maximal cliques (if any) and characterise them.

We say that an analogue of the Hilton-Milner is exact if the structure of the second largest maximal cliques relies on the structure of the general second largest family of the intersecting sets (a vertex x outside of a canonical clique C joined with its neighbours C_x in C).

In this talk, we discuss two conjectures (verified for small values of parameters) for Paley graphs of square order and a subslass of Peisert graphs and why their statements can be viewed as exact analogues of the Hilton-Milner theorem.

Peisert-type graphs

Let q be a 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.

Peisert-type graphs are equivalent to the block graphs of orthogonal arrays obtained from the parallel classes of the affine plane $\mathrm{AG}(2, q)$.

Another way to look at Peisert-type graphs is to consider them as fusions of certain amorphic cyclotomic association schemes.

Basic properties of Peisert-type graphs

- Every Peisert-type graph of type (m, q) can be naturally defined on the points of the affine plane $\mathrm{AG}(2, q)$ with two points being adjacent whenever the line through these points belongs to one of m prescribed parallel classes of lines; the canonical cliques in a Peisert-type graph of type (m, q) are exactly the lines from m prescribed parallel classes defining the graph.
- The affine plane $\mathrm{AG}(2, q)$ can be viewed as an orthogonal $(q + 1) \times q^2$-array $OA(q + 1, q)$; every Peisert-type of type (m, q) graph can be viewed as the block graph of an orthogonal array $OA(m, q)$ obtained from this array $OA(q + 1, q)$ by choosing the subset of m rows corresponding the m prescribed classes of parallel classes.

Intersections of 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).

Maximal cliques in Paley graphs of square order

In [B84], Blokhuis proved a maximum clique in a Paley graph of square order is a canonical clique.

Problem 2

For a Paley graph of square order, what are maximal cliques that are not maximum? In particular, what are second largest maximal cliques?

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

Baker et al.' construction of maximal but not maximum cliques in Paley graphs of square order

In [BEHW96], a study of second largest maximal cliques in Paley graphs of square order $P(q^2)$ was initiated.

Given an odd prime power q, put $r(q) := \begin{cases} 1, & q \equiv 1(4); \\ 3, & q \equiv 3(4). \end{cases}$

In particular, the following construction of maximal cliques of size $\frac{q+r(q)}{2}$ in $P(q^2)$ was proposed.

Let β be a primitive element in a finite field $\mathbb{F}_{q^2}$, where q is an odd prime. Further, let

$$\varepsilon := \beta^{\frac{q+1}{2}}, S := \{x \in \mathbb{F}_q \mid x - \varepsilon \in (\mathbb{F}_{q^2}^*)^2\},$$

[BEHW96] R. D. Baker, G. L. Ebert, J. Hemmeter, A. J. Woldar, *Maximal cliques in the Paley graph of square order*, J. Statist. Plann. Inference **56** (1996) 33–38.

Baker et al.' construction of maximal but not maximum cliques in Paley graphs of square order

Let β be a primitive element in a finite field $\mathbb{F}_{q^2}$, where q is an odd prime. Further, let

$$\varepsilon := \beta^{\frac{q+1}{2}}, S := \{x \in \mathbb{F}_q \mid x - \varepsilon \in (\mathbb{F}_{q^2}^*)^2\},$$

Theorem 3 ([BEHW96])

1. *If* $q \equiv 1 \pmod 4$, *then* $S \cup \{\varepsilon\}$ *is a maximal clique in* $P(q^2)$ *of size* $\frac{q+1}{2}$;
2. *If* $q \equiv 3 \pmod 4$, *then* $S \cup \{\varepsilon, -\varepsilon\}$ *is a maximal clique in* $P(q^2)$ *of size* $\frac{q+3}{2}$.

However, their extensive searching for $q \leq 25$ showed that these are not the only maximal cliques of the such size (under the action of the full automorphism group of Paley graphs).

[BEHW96] R. D. Baker, G. L. Ebert, J. Hemmeter, A. J. Woldar, *Maximal cliques in the Paley graph of square order*, J. Statist. Plann. Inference **56** (1996) 33–38.

Bound for the possible analogue of the Hilton-Milner theorem for Paley graphs of square order

Conjecture 1 ([BEHW96])

For an odd prime power $q \geq 5$, the maximal cliques of size $\frac{q+r(q)}{2}$ in $P(q^2)$ are second largest. In other words, there are no maximal cliques of size s in $P(q^2)$ where $\frac{q+r(q)}{2} < s < q$.

This conjecture gives a reasonable bound for the size of second largest maximal cliques.

In this talk we discuss our recent developments related to this conjecture. Although the conjecture has not been confirmed yet, we were able to realise new interesting details and formulate a stronger conjecture whose statement is an exact analogue of the Hilton-Milner theorem.

[BEHW96] R. D. Baker, G. L. Ebert, J. Hemmeter, A. J. Woldar, *Maximal cliques in the Paley graph of square order*, J. Statist. Plann. Inference **56** (1996) 33–38.

A special oval Q

Let β be a primitive element in $\mathbb{F}_{q^2}$. Put $\omega := \beta^{q-1}$. Then $Q = \langle \omega \rangle$ is the subgroup of order $q+1$ in $\mathbb{F}_{q^2}^*$.

Facts about Q:

- Q is an oval in the corresponding affine plane (a set of points of size $q+1$ such that no three of them lie on a line);
- Q is the kernel of the norm mapping $N : \mathbb{F}_{q^2}^* \mapsto \mathbb{F}_q^*$, which means that $Q = \{\gamma \in \mathbb{F}_{q^2}^* \mid \gamma^{q+1} = 1\}$, or, equivalently, $Q = \{x + y\alpha \mid x, y \in \mathbb{F}_q, x^2 - y^2 d = 1\}$, where d is a non-square in $\mathbb{F}_q^*$ and $\alpha^2 = d$.

[GKSV18] S. Goryainov, V. Kabanov, L. Shalaginov, A. Valyuzhenich, *On eigenfunctions and maximal cliques of Paley graphs of square order*, Finite Fields and Their Applications 52 (2018) 361–369.

Another family of maximal cliques of second largest known size (I)

Knowing the structure of Q, we were also able to construct new maximal cliques of the second largest known size, that is $\frac{q+r(q)}{2}$, in Paley graphs of square order $P(q^2)$.

Theorem 4 ([GKSV18])

1. *If $q \equiv 1 \pmod 4$, then Q_0 and Q_1 induce maximal cocliques of size $\frac{q+1}{2}$ in $P(q^2)$ (maximal cliques of size $\frac{q+1}{2}$ in the complement of $P(q^2)$);*
2. *If $q \equiv 3 \pmod 4$, then $\{0\} \cup Q_0$ and $\{0\} \cup Q_1$ induce maximal cliques of size $\frac{q+3}{2}$ in $P(q^2)$.*

Another family of maximal cliques of second largest known size (II)

The full automorphism group of a Paley graph of square order is known to preserve the lines in the corresponding affine plane. This shows that our maximal cliques are not equivalent (under the full automorphism group) to the cliques constructed by Baker et al. Indeed, in our construction based on the oval Q, almost all triples of vertices of the clique are not collinear. On the other hand, almost all triples of vertices of the clique from Baker et al.'s construction are collinear.

[GKSV18] S. Goryainov, V. Kabanov, L. Shalaginov, A. Valyuzhenich, *On eigenfunctions and maximal cliques of Paley graphs of square order*, Finite Fields and Their Applications 52 (2018) 361–369.

Computer searching (2018): number of orbits on the maximal cliques of size $\frac{q+r(q)}{2}$ in $P(q^2)$

q	3	5	7	9	11	13	17	19	23	25
Clique size	3	3	5	5	7	7	9	11	13	13
#Orbits	1	1	1	3	3	4	9	4	4	2

Whenever $25 \leq q \leq 83$, the computations showed that the graph $P(q^2)$ contains exactly two non-equivalent (under the action of the full automorphism group) maximal cliques of size $\frac{q+r(q)}{2}$.

We thus formulate the following conjecture.

Conjecture 2

For $q \geq 25$, the graph $P(q^2)$ contains exactly two non-equivalent (under the action of the full automorphism group) maximal cliques of size $\frac{q+r(q)}{2}$, and these cliques are second largest.

The automorphism group of $P(q^2)$

The automorphism group of $P(q^2)$ acts arc-transitively, and the equality

$$\mathrm{Aut}\left(P(q^2)\right) = \left\{\, v \mapsto av^{\gamma} + b \mid a \in S,\ b \in \mathbb{F}_{q^2},\ \gamma \in \mathrm{Gal}(\mathbb{F}_{q^2}) \,\right\}$$

holds, where S is the set of square elements in $\mathbb{F}_{q^2}^*$.

The group $\mathrm{Aut}\left(P(q^2)\right)$ preserves the sets of quadratic and non-quadratic lines and acts on each of them transitively.

The group $\mathrm{Aut}\left(P(q^2)\right)$ has a subgroup that stabilises the quadratic line $\mathbb{F}_q$ and acts faithfully on the set of points that do not belong to $\mathbb{F}_q$; this subgroup is given by the affine transformations $x \mapsto ax + b$, where $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$.

General geometric structure of maximal cliques from the construction of Baker el al. (I)

Take an element $\gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

Since $\mathbb{F}_q$ is a quadratic line, the line through γ that is parallel to $\mathbb{F}_q$, is quadratic too.

The other $\frac{q-1}{2}$ quadratic lines through γ intersect $\mathbb{F}_q$ in $\frac{q-1}{2}$ points; denote this set of $\frac{q-1}{2}$ intersection points by X_γ.

For the conjugate element $\overline{\gamma}$, the equality $X_{\overline{\gamma}} = X_\gamma$ holds.

If $q \equiv 1(4)$, each of the sets $\{\gamma\} \cup X_\gamma$ and $\{\overline{\gamma}\} \cup X_\gamma$ induce a maximal clique of size $\frac{q+1}{2}$.

If $q \equiv 3(4)$, the set $\{\gamma, \overline{\gamma}\} \cup X_\gamma$ induces a maximal clique of size $\frac{q+3}{2}$.

General geometric structure of maximal cliques from the construction of Baker el al. (II)

In view of this, a general description of a Baker et al.' maximal cliques is as follows.

1. Take a quadratic line C (a canonical clique in $P(q^2)$).
2. Take a vertex x outside of C.
3. Let C_x be the set neighbours of x in C.
4. There exists a uniquely determined vertex x' outside of C such that $x \neq x'$ and $C_{x'} = C_x$.
5. Then $\{x\} \cup C_x$ and $\{x'\} \cup C_x$ are cliques. Moreover, if $q \equiv 1 \pmod 4$, then these cliques are maximal of size $\frac{q+1}{2}$; if $q \equiv 3 \pmod 4$, then these cliques are not maximal, but their union $\{x, x'\} \cup C_x$ is a maximal clique of size $\frac{q+3}{2}$.

Thus, if $q \equiv 1 \pmod 4$, we have the same structure of the maximal clique as in the Hilton-Milner theorem. If $q \equiv 3 \pmod 4$, the structure of the maximal clique relies on the structure of the maximal clique in the Hilton-Milner theorem.

What remains to regard Conjecture 2 as an exact analogue of the Hilton-Milner theorem?

The only thing needed to regard Conjecture 2 as an exact analogue of the Hilton-Milner theorem is to show that the two known constructions are equivalent even if they are not equivalent under the action of the full automorphism group of Paley graphs of square order.

Such an equivalence indeed exists, and we further discuss it in details.

To introduce the equivalence, let us reinterpret the two known constructions of maximal cliques of size $\frac{q+r(q)}{2}$ in $P(q^2)$. For each of the two constructions, we will consider two important incarnations. The required equivalence can be well understood for the resulting four instances.

Recall that we view $\mathbb{F}_{q^2}$ as a vector space over $\mathbb{F}_q$ generated by the elements 1 and α, where $\alpha^2 = d$ and d is a non-square in $\mathbb{F}_q^*$.

$(\mathbb{F}_q, \alpha)$-construction

Let us consider the quadratic line $\mathbb{F}_q$, the point $\alpha \notin \mathbb{F}_q$, and the pencil of quadratic lines through α. Each line of the pencil, except $\{c + \alpha : c \in \mathbb{F}_q\}$, intersects $\mathbb{F}_q$ at a point. Denote by $c_1, \ldots, c_{\frac{q-1}{2}}$ all the intersection points. So, the set $\{\alpha, c_1, \ldots, c_{\frac{q-1}{2}}\}$ is a clique of size $\frac{q+1}{2}$ in $P(q^2)$. The points $-\alpha$ and α have the same neighbours in $\mathbb{F}_q$. Therefore, the set $\{-\alpha, c_1, \ldots, c_{\frac{q-1}{2}}\}$ is also a clique. The first and the second cliques are equivalent under the field automorphism $\gamma \mapsto \gamma^q$ (an analogue of the complex conjugation), which acts as $\alpha \mapsto -\alpha$ and $c_k \mapsto c_k$. For $q \equiv 3(4)$, the line $\{c\alpha : c \in \mathbb{F}_q\}$, which contains $-\alpha$ and α, is quadratic. Hence the two cliques are combined into one.

Theorem 5

If $q \equiv 1(4)$, then $\{\alpha, c_1, \ldots, c_{\frac{q-1}{2}}\}$ is a maximal clique of size $\frac{q+1}{2}$ in $P(q^2)$; if $q \equiv 3(4)$, then $\{\pm\alpha, c_1, \ldots, c_{\frac{q-1}{2}}\}$ is a maximal clique of size $\frac{q+3}{2}$ in $P(q^2)$.

$(\alpha\mathbb{F}_q, 1)$-construction

The second interpretation uses the line $\alpha\mathbb{F}_q$ and the point $1 \notin \alpha\mathbb{F}_q$. For $q \equiv 1(4)$ (resp. $q \equiv 3(4)$), consider the pencil of non-quadratic (resp. quadratic) lines through 1. They all, except $\{1 + c\alpha : c \in \mathbb{F}_q\}$, intersect $\alpha\mathbb{F}_q$. Denote the intersection points by $c_1\alpha, \ldots, c_{\frac{q-1}{2}}\alpha$. The elements -1 and 1 have the same neighbours in $\alpha\mathbb{F}_q$. Thus $\{1, c_1\alpha, \ldots, c_{\frac{q-1}{2}}\alpha\}$ and $\{-1, c_1\alpha, \ldots, c_{\frac{q-1}{2}}\alpha\}$ are cocliques (resp. cliques) of size $\frac{q+1}{2}$ in $P(q^2)$. They are equivalent under the automorphism $\gamma \mapsto -\gamma^q$ and, if $q \equiv 3 \pmod 4$, combined into one.

Theorem 6

If $q \equiv 1(4)$, then $\{1, c_1\alpha, \ldots, c_{\frac{q-1}{2}}\alpha\}$ is a maximal independent set of size $\frac{q+1}{2}$ in $P(q^2)$; if $q \equiv 3(4)$, then $\{\pm 1, c_1\alpha, \ldots, c_{\frac{q-1}{2}}\alpha\}$ is a maximal clique of size $\frac{q+3}{2}$ in $P(q^2)$.

Connection between Theorem 6 and Theorem 5

Note that the sets from Theorem 6 are obtained from the sets from Theorem 5 by the mapping $\gamma \mapsto \alpha\gamma$, which is an isomorphism with the complement of $P(q^2)$ when $q \equiv 1 \pmod 4$ and an automorphism of $P(q^2)$ when $q \equiv 3 \pmod 4$.

Q-construction

Let β be a primitive element in $\mathbb{F}_{q^2}$ and $\omega = \beta^{q-1}$. Then ω is a square in $\mathbb{F}_{q^2}^*$, and $\langle\omega\rangle$ is a subgroup of order $q+1$ in $\mathbb{F}_{q^2}^*$. Denote it by Q. The points of Q form an oval in $\mathrm{AG}(2,q)$. Put

$$Q_0 := \langle\omega^2\rangle \quad \text{and} \quad Q_1 := \omega\langle\omega^2\rangle.$$

Obviously, $Q = Q_0 \cup Q_1$ and $Q_1 = \omega Q_0$.

Theorem 7

If $q \equiv 1(4)$, then Q_0 and Q_1 are maximal cocliques of size $\frac{q+1}{2}$ in $P(q^2)$; if $q \equiv 3(4)$, then $Q_0 \cup \{0\}$ and $Q_1 \cup \{0\}$ are maximal cliques of size $\frac{q+3}{2}$ in $P(q^2)$.

αQ-construction

The following construction is a corollary of Theorem 7 and the fact that the multiplication by α is an isomorphism with the complement when $q \equiv 1 \pmod 4$ and an automorphism of $P(q^2)$ when $q \equiv 3 \pmod 4$.

Theorem 8

If $q \equiv 1(4)$, then αQ_0 and αQ_1 are maximal cliques of size $\frac{q+1}{2}$ in $P(q^2)$; if $q \equiv 3(4)$, then $\alpha Q_0 \cup \{0\}$ and $\alpha Q_1 \cup \{0\}$ are maximal cliques of size $\frac{q+3}{2}$ in $P(q^2)$.

Correspondences between constructions

Further we introduce two linear fractional mappings, which establish correspondences between the sets from Theorems 7 and 6, and between the sets from Theorems 8 and 5.

Mapping φ

Let us define the first mapping $\varphi : \mathbb{F}_{q^2} \mapsto \mathbb{F}_{q^2}$ by the rule

$$\varphi(\gamma) := \begin{cases} \frac{\gamma+1}{\gamma-1} & \text{if} \;\; \gamma \neq 1, \\ 1 & \text{if} \;\; \gamma = 1. \end{cases}$$

Lemma 1

The mapping φ is a bijection and an involution.

Proposition 1 ([GMS22])

Let γ be an element from $Q \setminus \{1\}$, where $\gamma = x + y\alpha$ for some $x, y \in \mathbb{F}_q$. Then the following statements hold:

1. $\varphi(\gamma) = \frac{y}{x-1}\alpha$.
2. *The set $Q \setminus \{1\}$ is mapped to $\alpha\mathbb{F}_q$ by φ bijectively.*

[GMS22] S. Goryainov, A. Masley, L. V. Shalaginov, *On a correspondence between maximal cliques in Paley graphs of square order*, Discrete Math. **345** (2022), no. 6, 112853.
https://doi.org/10.1016/j.disc.2022.112853

φ is a correspondence

Proposition 2 ([GMS22])

Let γ be an element from $Q \setminus \{1, -1\}$, where $\gamma = x + y\alpha$ for some $x, y \in \mathbb{F}_q$. Then the following formula holds

$$\varphi(\gamma^2) = \frac{x}{yd}\alpha.$$

Theorem 9 ([GMS22])

Let Q_0 be the set from Theorem 7. If $q \equiv 1(4)$, then $\varphi(Q_0)$ coincides with the maximal coclique from Theorem 6, that is,

$$\varphi(Q_0) = \{1, c_1\alpha, \ldots, c_{\frac{q-1}{2}}\alpha\}.$$

If $q \equiv 3(4)$, then $\varphi(Q_0 \cup \{0\})$ coincides with the maximal clique from Theorem 6, that is,

$$\varphi(Q_0 \cup \{0\}) = \{\pm 1, c_1\alpha, \ldots, c_{\frac{q-1}{2}}\alpha\}.$$

Mapping ψ

Define the second mapping $\psi : \mathbb{F}_{q^2} \mapsto \mathbb{F}_{q^2}$ as

$$\psi(\gamma) := \alpha\varphi(\alpha^{-1}\gamma) = \begin{cases} \frac{\alpha\gamma+d}{\gamma-\alpha} & \text{if } \gamma \neq \alpha, \\ \alpha & \text{if } \gamma = \alpha. \end{cases}$$

Its properties are direct corollaries of the results on the correspondence φ and listed on the next slide.

Properties of ψ

Proposition 3 ([GMS22])

The following statements hold.

1. *The mapping ψ is a bijection and an involution.*
2. *Let γ be an element from $Q \setminus \{1\}$, where $\gamma = x + y\alpha$ for some $x, y \in \mathbb{F}_q$. Then*
$$\psi(\alpha\gamma) = \frac{yd}{x-1}.$$
3. *The set $\alpha Q \setminus \{\alpha\}$ is mapped to $\mathbb{F}_q$ by ψ bijectively.*
4. *Let γ be an element from $Q \setminus \{1, -1\}$, where $\gamma = x + y\alpha$ for some $x, y \in \mathbb{F}_q$. Then*
$$\psi(\alpha\gamma^2) = \frac{x}{y}.$$

ψ is a correspondence

Theorem 10 ([GMS22])

Let αQ_0 be the set from Theorem 8. If $q \equiv 1(4)$, then $\psi(\alpha Q_0)$ coincides with the maximal clique from Construction 5, that is,

$$\psi(\alpha Q_0) = \{\alpha, c_1, \dots, c_{\frac{q-1}{2}}\}.$$

If $q \equiv 3(4)$, then $\psi(\alpha Q_0 \cup \{0\})$ coincides with the maximal clique from Theorem 5, that is,

$$\psi(\alpha Q_0 \cup \{0\}) = \{\pm\alpha, c_1, \dots, c_{\frac{q-1}{2}}\}.$$

[GMS22] S. Goryainov, A. Masley, L. V. Shalaginov, *On a correspondence between maximal cliques in Paley graphs of square order*, Discrete Math. **345** (2022), no. 6, 112853.
`https://doi.org/10.1016/j.disc.2022.112853`

Comments on the correpondences φ and ψ (I)

Although we had established a correspondence between the construction by Baker et al. and our construction based on the oval, and showed that these constructions are related, our results were not enough to conclude that the constructions are equivalent. Indeed, as we discussed, these constructions are not equivalent under the full automorphism group.

At this stage, private communication with Andries E. Brouwer helped much. He recognised in the established correspondence $\varphi(\gamma) = \frac{\gamma+1}{\gamma-1}$ an automorphism of the subgraph of $P(q^2)$ induced by the first neighbourhood of the vertex 1.

Comments on the correpondences φ and ψ (II)

In [B00], Brouwer studied locally Paley graphs (that is, graphs in which the first neighbourhoods of vertices induce a Paley graph of the same size), reduced the problem of their determination to the problem of finding the automorphims group of the local subgraph of a Paley graph and showed that if the automorphims group of a local subgraph as he supposed, then a locally Paley graph is either the Taylor extension of a Paley graph or one exceptional graph (namely, the complement of 4×4-lattice).

Later, Muzychuk and Kovác confirmed [MK05] that the automorphism group of a local subgraph in a Paley graph is as Brouwer supposed.

[B00] A. E. Brouwer, *Locally Paley graphs*, Designs, Codes and Cryptography **21** (2000), 69–76.

[MK05] M. Muzychuk, I. Kovács, *A solution of a problem of A. E. Brouwer*, Designs, Codes and Cryptography **34**, 249–264 (2005).

The automorphism group of the local subgraph of a Paley graph

Let Γ_q denote the Paley graph of square order $P(q^2)$, where q is an odd prime power.

Let $\Delta = \Gamma_q(0)$ be the subgraph induced on the neighbours of 0. For $q > 9$, the automorphism group $\mathrm{Aut}(\Delta)$ of Δ is twice as large as the stabilizer of 0 in $\mathrm{Aut}(\Gamma_q)$ (see [B00, MK05]) since also $\gamma \mapsto \gamma^{-1}$ is an automorphism of Δ. This is the root of the stated correspondence. Indeed, since finding cliques is something that happens in a local graph, the linear fractional transformation acts.

[B00] A. E. Brouwer, *Locally Paley graphs*, Designs, Codes and Cryptography **21** (2000), 69–76.

[MK05] M. Muzychuk, I. Kovács, *A solution of a problem of A. E. Brouwer*, Designs, Codes and Cryptography **34**, 249–264 (2005).

Explicit expression of the correspondence φ in terms of $\gamma \mapsto \gamma^{-1}$

We have

$$\varphi(\gamma) = \frac{\gamma + 1}{\gamma - 1} = 1 + \frac{2}{\gamma - 1}.$$

This shows [B] that the correspondence φ is nothing more but the automorphism $\gamma \mapsto \frac{2}{\gamma}$ of $\Gamma_q(0)$ additively shifted by 1 (this shift gives an automorphism of the subgraph $\Gamma_q(1)$ of $P(q^2)$ induced on the neighbours of 1; this subgraph is isomorphic to $\Gamma_q(0)$).

Thus, the two known constructions of maximal cliques of size $\frac{q+r(q)}{2}$ in $P(q^2)$ are equivalent. This means the statement of Conjecture 2 is an exact analogue of the Hilton-Milner theorem [Y].

[B] A. E. Brouwer, private communication.

[Y] C. H. Yip, private communication.

Connection between maximal cliques in a graph Γ, maximal cliques in local subgraphs of Γ and graphs that are locally Γ

Since Paley graphs are vertex-transitive, the problem of determination maximal cliques of size t in them can be reduced the to the problem of determination maximal cliques of size $t-1$ in the subgraph induced by the neighbourhood of any vertex (note that the number of orbits on maximal cliques in the local subgraph can be larger).

On the other hand, if we know the graphs that are locally Paley graphs (we do know due to nice works by Brouwer and Muzychuk & Kovác), then the problem of determination maximal cliques of size t in Paley graphs can be reduced to the problem of determination maximal cliques of size $t+1$, containing a given vertex, in the locally Paley graphs.

Further we discuss the structure of locally Paley graphs.

Antipodal covers

A graph Γ is said to be locally $\mathcal{X}$ where $\mathcal{X}$ is a graph or a class of graphs, when for each $\gamma \in \Gamma$ the subgraph induced by $\Gamma(\gamma)$ is isomorphic to (respectively a member of) $\mathcal{X}$.

An antipodal graph is a connected graph Γ of diameter $d > 1$ for which the graph Γ_d (that is, the graph on the same vertex set with two vertices being adjacent whenever they are at distance d) is a disjoint union of cliques.

The folded graph of Γ is defined as the graph $\overline{\Gamma}$ whose vertices are the maximal cliques of Γ_d, adjacent if their union contains an edge of Γ. If, in addition, each $\gamma \in \Gamma$ has the same valency as its image under folding (so that, in particular, $d > 3$), then Γ is called an antipodal covering graph of $\overline{\Gamma}$. (Note that the folding map will be a local isomorphism precisely when $d > 3$.) If, moreover, all maximal cliques of Γ_d have the same size r then Γ is also called an antipodal r-cover (double cover if $r = 2$, triple cover if $r = 3$) of $\overline{\Gamma}$.

Taylor graphs

A distance-regular graph Γ with intersection array $\{k, \mu, 1; 1, \mu, k\}$ is called a Taylor graph. It follows from [BCN89,Proposition 4.2.2(ii)] that such a graph is an antipodal double cover of the complete graph K_{k+1}.

The local graphs $\Delta = \Gamma(x)$ of a Taylor graph Γ are strongly regular, and satisfy $v_\Delta = k$, $k_\Delta = \lambda_\Gamma = k - \mu - 1 = 2\mu_\Delta$, $\lambda_\Delta = \frac{1}{2}(3k_\Delta - k - 1)$.

[BCN89] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-Regular Graphs*, Springer-Verlag, Berlin (1989).

Locally Paley graphs

Given a graph Σ with vertex set X, its Taylor double is the graph with vertex set $\{x^\varepsilon | x \in X, \varepsilon = \pm 1\}$ and edges $x^\delta y^\varepsilon$ (for $x \neq y$) with $\delta\varepsilon = 1$ when $x \sim y$ and $\delta\varepsilon = -1$ otherwise.

Given a strongly regular graph Δ with $k_\Delta = 2\mu_\Delta$, its Taylor extension $\mathrm{T}\,\Delta$ is the Taylor double of $\{\infty\} + \Delta$. It is a Taylor graph.

Proposition 4 ([BCN89], For an explicit proof, see [B97])

The Taylor extension of a Paley graph is vertex-transitive and thus is locally Paley.

Theorem 11 ([B00,MK05])

A locally Paley graph is either the Taylor extension of a Paley graph or the complement of 4×4-lattice.

[B97] D. Buset, *Quelques conditions locales et extrémales en théorie des graphes*, Ph. D. Thesis, Université Libre de Bruxelles, December 1997.

Locally Paley graphs as Mathon graphs

Theorem 12 ([BCN89, Proposition 12.5.3])

Let $q = rm + 1$ be a prime power, where $r > 1$ and either m is even or q is a power of 2. Let V be a vector space of dimension 2 over $F = \mathbb{F}_q$ provided with a nondegenerate symplectic form B. Let K be the subgroup of the multiplicative group F^* of index r, and let $b \in F^*$. Then the graph $M(m, q)$ with vertex set $\{Kv \mid v \in V \setminus \{\overline{0}\}\}$ where $Ku \sim Kv$ if and only if $B(u, v) \in bK$ is distance-regular of diameter 3 with $r(q + 1)$ vertices and intersection array $\{q, q - m - 1, 1; 1, m, q\}$.

The graphs from Theorem 12 are called Mathon graphs

Proposition 5

The Mathon graphs with parameter $r = 2$ are isomorphic to the locally Paley Taylor graphs from Brouwer's classification.

Thus, all locally Paley graphs have a nice algebraic description.

Computer searching (2022): number of orbits on the maximal cliques of size $\frac{q+r(q)}{2}+1$ in the Taylor exstension of $P(q^2)$

q	3	5	7	9	11	13	17	19	23	25
Clique size	4	4	6	6	8	8	10	12	14	14
#Orbits	1	1	1	2	2	2	4	3	2	1

Whenever $25 \leq q \leq 47$, Brouwer's computations showed that the Taylor extension of $P(q^2)$ contains a unique (under the action of the full automorphism group) maximal clique of size $\frac{q+r(q)}{2}+1$.

The following conjecture is thus equivalent to Conjecture 2.

Conjecture 3

For $q \geq 25$, the Taylor exstension of $P(q^2)$ contains a unique (under the action of the full automorphism group) maximal clique of size $\frac{q+r(q)}{2}+1$, and this clique is second largest.

Comments

So we expect an exact analogue of the Hilton-Milner theorem for Paley graphs of square order $P(q^2)$ when $q \geq 25$.

According to computations, a conjecture similar to Conjecture 2 can be formulated for a subclass of Peisert graphs.

Peisert graphs

In [P01], Peisert gave a full description of self-complementary symmetric graphs and their automorphism groups. In particular, he proved that apart from the Paley graphs there is another infinite family of self-complementary symmetric graphs (now called Peisert graphs) and, in addition, one more graph not belonging to any of these families.

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 $\mathrm{Cay}(\mathbb{F}_q^+, M_q)$ with $M_q = \{g^j : j \equiv 0, 1 \pmod 4\}$, where g is a primitive root of the field $\mathbb{F}_q$.

[P01] W. Peisert, *All self-complementary symmetric graphs*, J. Algebra, 240(1):209–229, 2001.

Peisert graphs that are Peisert-type graphs

It can be shown that a Peisert graph $P^*(q^2)$ is a Peisert-type graph if and only if $q \equiv 3 \pmod 4$ (equivalently, if and only if the subfield $\mathbb{F}_q$ forms a (Delsarte) clique. Thus, if $q \equiv 3 \pmod 4$, canonical cliques are defined for the Peisert graph $P^*(q^2)$, and we can ask what are the corresponding EKR properties.

In [M09, Chapter 8], Mullin conjectured that if $q \equiv 3 \pmod 4$, then the Peisert graph with order q^2 has the strict-EKR property. In [AY22,Theorem 1.4], the conjecture was confirmed when $q = p^n$ and $p > 8.2n^2$.

[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.

[M09] N. Mullin, *Self-complementary arc-transitive graphs and their imposters*, 2009, Master's thesis, University of Waterloo. https://uwspace.uwaterloo.ca/handle/10012/4264

Second largest maximal cliques in small Peisert graphs $P^*(q^2)$, $q \equiv 1 \pmod 4$

The construction of the a clique supposed to be second largest maximal clique is simple and similar to what we had in the case of Paley graphs of square order. Note that the subfield $\mathbb{F}_q$ is a maximum (canonical) clique in the Peisert graph $P^*(q^2)$, where $q \equiv 3 \pmod 4$. Pick an element $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, and consider the clique $C = \{x\} \cup C_x$, where C_x is the set of neighbours of x in $\mathbb{F}_q$. Note that C has size $\frac{q+1}{2}$

Conjecture 4

Let q be an odd prime power, $q \equiv 3 \pmod 4$. Then C is a second largest maximal clique in the Peisert graph $P^*(q^2)$. Moreover, if $q \geq 23$, this clique is unique among maximal cliques of this size (under the action of the full automorphism group).

The existence part of Conjecture 4 has been computationally checked for $q \in \{7, 11, 19, 23, 27, 31, 43\}$. The uniqueness part has been computationally checked for $q \in \{23, 27, 31, 43\}$.

Possible exact analogue of the Hilton-Milner for Peisert graphs

It is clear that the statement of Conjecture 4 is an exact analogue of the Hilton-Milner for special class of Peisert graphs.

This analogue is even "more exact" than the one for Paley graphs of square order since we have only one general case, which exactly corresponds to the original Hilton-Milner theorem (we do not have an extra vertex in the maximal clique as in one of the cases for Paley graphs of square order).

Possible general construction for maximal cliques in Peisert-type graphs (I)

Let q be a prime power. Let H be a subgroup in $\mathbb{F}_q^*$ of size k and index m (in particular, $km = q-1$). Let $g_1H = H, g_2H, \dots, g_mH$ be the m cosets of H in $\mathbb{F}_q^*$. Let $1, \alpha$ be a basis of $\mathbb{F}_{q^2}$ considered as a vector space over $\mathbb{F}_q$.

Lemma 1

Let $i, j \in \{1, \dots, m\}$ be two, possibly equal, indices of the cosets. Consider the subsets $g_iH \subset \mathbb{F}_q$ and $g_jH\alpha \subset \alpha\mathbb{F}_q$ of the lines $\mathbb{F}_q$ and $\alpha\mathbb{F}_q$, respectively, and the set of points $U = g_iH \cup g_jH\alpha \cup \{0\}$. Then U determines exactly $k+2$ directions.

Possible general construction for maximal cliques in Peisert-type graphs (II)

Corollary 1

Let $I \subset \{1, \ldots, m\}$ be a nonempty subset of indices of the cosets, $|I| = s$, and $j \in \{1, \ldots, m\}$ be an index of a coset. Consider the subsets $\bigcup_{i \in I} g_i H \subset \mathbb{F}_q$ and $g_j H \alpha \subset \alpha \mathbb{F}_q$ of the lines $\mathbb{F}_q$ and $\alpha \mathbb{F}_q$, respectively, and the set of points $U = \bigcup_{i \in I} g_i H \cup g_j H \alpha \cup \{0\}$ of size $k(s+1)+1$. Then U has size $k(s+1)+1$ and determines exactly $ks+2$ directions.

Let X_U be the Peisert-type graph induced by the set U. Computations show that U is a maximal clique in X_U very often. Also, for many small q, if we choose appropriate values for k and s, then U is a second largest maximal clique in X_U.

Together with my colleague Chi Hoi Yip, we plan to investigate this construction further and expect that, for many Peisert-type graphs, maximal cliques of different sizes, including second largest, come from this construction.

Thank you for your attention!