Maximal cliques in the Paley graph of square order

aeb

September 22, 2022

Consider the Paley graph Γ of order q^2, where q is an odd prime power. The vertex set is the field $K = \mathbb{F}_{q^2}$. Two vertices are adjacent when they differ by a nonzero square in K. The graph Γ is self-complementary, and strongly regular with parameters $(v, k, \lambda, \mu) = (q^2, \frac{1}{2}(q^2-1), \frac{1}{4}(q^2-5), \frac{1}{4}(q^2-1))$.

Let $F = \mathbb{F}_q$ be the subfield of order q. It induces a clique, and by Blokhuis [2] all q-cliques in Γ look like this: they are affine images of a line in K, considered as affine plane over F.

Let $m_q = \frac{1}{2}(q+1)$ if $q \equiv 1 \pmod 4$, and $m_q = \frac{1}{2}(q+3)$ if $q \equiv 3 \pmod 4$. Baker et al. [1] construct maximal cliques of size m_q and conjecture that there are no maximal cliques of size strictly between m_q and q. (We checked that this is true for $q < 250$).

The clique F meets the Hoffman bound, so that each vertex outside is adjacent to precisely $\frac{1}{2}(q-1)$ vertices inside F. Let $z \in K \setminus F$. Let $S = \Gamma(z) \cap F$. If $q \equiv 1 \pmod 4$, then $S \cup \{z\}$ is a maximal clique in Γ of size $\frac{1}{2}(q+1)$, and if $q \equiv 3 \pmod 4$, then $S \cup \{z, z^q\}$ is a maximal clique in Γ of size $\frac{1}{2}(q+3)$. Details below.

Goryainov et al. [6] checked that the number of orbits of maximal cliques of size m_q equals 2 for $25 \le q \le 83$, and gave a second construction for cliques of this size. Goryainov et al. [7] gave a correspondence between the two classes of maximal cliques of size m_q.

(Let $\Delta = \Gamma(0)$ 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 $\mathrm{Aut}(\Gamma)$ (cf. [3, 9]) since also $x \mapsto x^{-1}$ is an automorphism of Δ. This gives the stated correspondence.)

0.1 Details

Let $q = p^e$, where p is an odd prime.

Proposition 0.1 (Baker et al. [1]) *Let $\gamma \in K \setminus F$ and let $S := \Gamma(\gamma) \cap F$. For $q \equiv 1 \pmod 4$ the set $S \cup \{\gamma\}$ is a maximal clique of size $\frac{1}{2}(q+1)$. For $q \equiv 3 \pmod 4$ the set $S \cup \{\gamma, \gamma^q\}$ is a maximal clique of size $\frac{1}{2}(q+3)$.*

Proof. Since F is a clique, $S \cup \{\gamma\}$ is a clique.

Let β be primitive in K, and put $\xi = \gamma^q - \gamma$. Then $\xi^q = -\xi$. If $\xi = \beta^i$ then $i \equiv \frac{1}{2}(q+1) \pmod{q+1}$, so that ξ is a square in K (and $\gamma \sim \gamma^q$) precisely when $q \equiv 3 \pmod 4$.

Let $\varepsilon = \beta^{(q+1)/2}$. Then $\varepsilon^q = -\varepsilon$ and $K = \{x + y\varepsilon \mid x, y \in F\}$. An element $\xi = x + y\varepsilon$ is a nonzero square in K if and only if $N(\xi) = \xi^{q+1} = x^2 - dy^2$ is a nonzero square in F, where $d := \varepsilon^2 \in F$.

The maps $\xi \mapsto a\xi + b$ with $a, b \in F$, $a \neq 0$ preserve Γ and F, commute with $\xi \mapsto \xi^q$, and $K \setminus F$ is a single orbit under the group they generate. So we may take $\gamma = \varepsilon$. Then $S = -S$. If $\eta \in K \setminus F$ is adjacent to all of $S \cup \{\gamma\}$, then $S = \Gamma(\eta) \cap F$. For $\eta = a\gamma + b$ with $a, b \in F$, $a \neq 0$, we find $S = aS + b$. The commutator of $\xi \mapsto a\xi + b$ and $\xi \mapsto -\xi$ is $\xi \mapsto \xi + \frac{2b}{a}$, but $|S|$ is not a multiple of p, so $b = 0$. Now $\eta \sim \gamma$ when $(a-1)\gamma$ is a square in K, that is, when γ is a square in K, that is, when $q \equiv 3 \pmod 4$. If this is the case, then $0 \in S$. The order i of a divides $q - 1$. Let r be a prime divisor of i. The set $S \setminus \{0\}$ of size $(q+1)/2$ is invariant for multiplication by the element $a^{i/r}$ of prime order r dividing $q - 1$. It follows that $r = 2$ and $i = 2$ (since $4 \nmid (q-1)$) and $a = -1$, so that $\eta = -\gamma = \gamma^q$. □

For $q > 7$, these maximal cliques have stabilizers (in Aut Γ) of order $2e$ if $q \equiv 1 \pmod 4$, and $4e$ if $q \equiv 3 \pmod 4$.

Let C be a maximal clique containing 0. Then, since $\xi \mapsto \xi^{-1}$ is an automorphism of $\Delta = \Gamma(0)$, also the set $C' = \{0\} \cup \{c^{-1} \mid c \in C \setminus \{0\}\}$ is a maximal clique, of the same size as C.

There is a more symmetric description of these latter cliques.

Proposition 0.2 (Goryainov et al. [6]) *Let β be primitive in K, and put $\omega := \beta^{q-1}$. Let $Q_0 := \langle \omega^2 \rangle$. If $q \equiv 1 \pmod 4$ the set Q_0 is a maximal coclique of size $(q+1)/2$. If $q \equiv 3 \pmod 4$ the set $Q_0 \cup \{0\}$ is a maximal clique of size $(q+3)/2$.*

Proof. Put $\varepsilon = \beta^{(q+1)/2}$, so that $\varepsilon^q = -\varepsilon$. Then $N(x + y\varepsilon) = x^2 - dy^2$ where $d = \varepsilon^2 \in F$. We see that $\langle \omega \rangle$ is the set of points on the conic $x^2 - dy^2 = 1$, and Q_0 consists of half of the points on this conic. Let $\omega^i = x + y\varepsilon$ with $x, y \in F$. Then $N(\omega^{2i} - 1) = ((x+y\varepsilon)^2 - 1)((x-y\varepsilon)^2 - 1) = -4dy^2$. Since $-d$ is a square in F if and only if $q \equiv 3 \pmod 4$, the given sets are (co)cliques as claimed. Maximality follows from the following proposition. □

For $q \geq 5$, these maximal cliques have stabilizers (in Aut Γ) of order $e(q+1)$.

Proposition 0.3 (Goryainov et al. [7]) *The map $\xi \mapsto \varepsilon^{-1}(1 + \frac{2}{\xi - 1})$, $1 \mapsto \varepsilon^{-1}$ maps Q_0 (resp. $Q_0 \cup \{0\}$) onto $S \cup \{\gamma\}$ (resp. $S \cup \{\gamma, \gamma^q\}$), where $\gamma = \varepsilon^{-1}$ and $S = \Gamma(\gamma) \cap F$.*

Proof. The given map maps 0, 1, $\eta = x + y\varepsilon \in \langle \omega \rangle$ to $-\varepsilon^{-1}$, ε^{-1}, and $\frac{y}{x-1}$, respectively. Let C be a maximal (co)clique containing Q_0 (resp. $Q_0 \cup \{0\}$). Then $1 \in C$, so $\xi \mapsto \frac{1}{\xi - 1}$ and $\xi \mapsto 1 + \frac{2}{\xi - 1}$ preserve adjacency on C, so $\xi \mapsto \varepsilon^{-1}(1 + \frac{2}{\xi - 1})$ flips or preserves adjacency when $q \equiv 1 \pmod 4$ or $q \equiv 3 \pmod 4$. □

Conjecture *For $q \geq 25$ the maximal cliques from Propositions 0.1 and 0.2 are all the 2nd largest cliques of Γ.*

Given two adjacent vertices, the line in AG$(2, q)$ they determine is a q-clique. Each point is on $\frac{q+1}{2}$ such 'quadratic lines'. Thus, cliques in Γ are subsets of AG$(2, q)$ that determine at most $\frac{q+1}{2}$ directions. Szőnyi [12] and Sziklai [11] give some information.

0.2 Numerical data

The table below gives the sizes of the maximal cliques in Paley(q^2) for $q \leq 47$. Exponents are the number of nonequivalent orbits of this size under the full group of the graph.

q	sizes
3	3^1
5	3^1, 5^1
7	5^1, 7^1
9	5^3, 9^1
11	7^3, 11^1
13	5^{10}, 7^4, 13^1
17	5^3, 7^{41}, 9^9, 17^1
19	7^{25}, 8^7, 9^{17}, 11^4, 19^1
23	7^{85}, 8^{108}, 9^{80}, 10^7, 11^9, 13^4, 23^1
25	7^{405}, 8^{226}, 9^{49}, 13^2, 25^1
27	7^{27}, 8^{411}, 9^{142}, 10^{50}, 11^{12}, 15^2, 27^1
29	7^{410}, 8^{1584}, 9^{2104}, 10^{148}, 11^{46}, 13^1, 15^2, 29^1
31	7^{60}, 8^{2004}, 9^{2734}, 10^{933}, 11^{199}, 12^{26}, 13^{46}, 17^2, 31^1
37	7^{103}, 8^{2505}, 9^{21556}, 10^{14002}, 11^{5712}, 12^{219}, 13^{222}, 19^2, 37^1
41	7^{168}, 8^{7801}, 9^{104495}, 10^{62070}, 11^{9583}, 12^{149}, 13^{128}, 14^{19}, 21^2, 41^1
43	7^{15}, 8^{1748}, 9^{54700}, 10^{109127}, 11^{54759}, 12^{9785}, 13^{1490}, 14^{156}, 15^{87}, 17^{20}, 23^2, 43^1
47	7^{12}, 8^{1097}, 9^{125545}, 10^{434029}, 11^{210725}, 12^{28533}, 13^{4904}, 14^{628}, 15^{230}, 16^{27}, 17^{50}, 25^2, 47^1

For $q \equiv 3 \pmod 4$, this confirms the values from Kiermaier & Kurz [8].

The table below gives the same information for the smallest maximal cliques for $q \leq 73$.

q	3	5	7	9	11	13	17	19	23	25	27	29
size	3^1	3^1	5^1	5^3	7^3	5^{10}	5^3	7^{25}	7^{85}	7^{405}	7^{27}	7^{410}
q	31	37	41	43	47	49	53	59	61	67	71	73
size	7^{60}	7^{103}	7^{168}	7^{15}	7^{12}	7^2	8^{455}	8^{113}	7^1	8^9	9^{119319}	9^{187566}

0.3 The Taylor extension

Given a strongly regular graph Γ on v vertices with $k = 2\mu$, its Taylor extension Σ is a distance-regular graph on $2(v+1)$ vertices with intersection array $\{v, v-k-1, 1; 1, v-k-1, v\}$ (cf. [4, §1.5], [5, §1.2.7]), an antipodal 2-cover of the complete graph K_{v+1}.

For the Paley graph of order r, the Taylor extension is distance-transitive on $2(r+1)$ vertices, with automorphism group $2{\times}P\Sigma L_2(r)$ (cf. [4, p. 228]). It follows that the maximal cliques in Σ have sizes that are 1 larger than those in Γ, while the number of orbits is smaller. Below a table for $r = q^2$, $q \leq 47$.

We see that the extra automorphisms of $\Delta = \Gamma(0)$ are those flipping the edge 0∞, for $\Gamma = \Sigma(\infty)$.

q	sizes
3	4^1
5	4^1, 6^1
7	6^1, 8^1
9	6^2, 10^1
11	8^2, 12^1
13	6^6, 8^2, 14^1
17	6^2, 8^{14}, 10^4, 18^1
19	8^8, 9^2, 10^5, 12^3, 20^1
23	8^{22}, 9^{16}, 10^{15}, 11^1, 12^4, 14^2, 24^1
25	8^{84}, 9^{29}, 10^{15}, 14^1, 26^1
27	8^6, 9^{50}, 10^{24}, 11^8, 12^6, 16^1, 28^1
29	8^{85}, 9^{180}, 10^{307}, 11^{18}, 12^{11}, 14^1, 16^1, 30^1
31	8^{17}, 9^{232}, 10^{324}, 11^{96}, 12^{43}, 13^3, 14^{13}, 18^1, 32^1
37	8^{31}, 9^{281}, 10^{2471}, 11^{1288}, 12^{640}, 13^{21}, 14^{36}, 20^1, 38^1
41	8^{42}, 9^{871}, 10^{11298}, 11^{5705}, 12^{1003}, 13^{17}, 14^{29}, 15^3, 22^1, 42^1
43	8^7, 9^{196}, 10^{5715}, 11^{10050}, 12^{4935}, 13^{840}, 14^{182}, 15^{15}, 16^{19}, 18^5, 24^1, 44^1
47	8^5, 9^{125}, 10^{12980}, 11^{39699}, 12^{18351}, 13^{2388}, 14^{516}, 15^{60}, 16^{38}, 17^3, 18^{12}, 26^1, 48^1

0.4 Peisert graphs

Peisert [10] characterized symmetric self-complementary graphs, and found (i) the Paley graphs on q vertices, $q \equiv 1 \pmod 4$ a prime power, and (ii) the graphs that are now called the Peisert graphs (of order $q^2 = p^{2e}$, $p \equiv 3 \pmod 4$, where two vertices are joined when their difference is β^i with $i \equiv 0, 1 \pmod 4$, β primitive in $\mathbb{F}_{q^2}$), and (iii) one further graph on 23^2 vertices. For this last graph, see [5, §10.70]. Sizes of cliques in small Peisert graphs (with number of orbits):

q	sizes
3	3^1
7	4^1, 7^1
9	5^1, 9^1
11	5^7, 6^2, 11^1
19	6^1, 7^{69}, 8^{40}, 9^{27}, 10^3, 19^1
23	6^1, 7^{222}, 8^{442}, 9^{186}, 10^{22}, 11^1, 12^1, 23^1
27	7^{205}, 8^{809}, 9^{273}, 10^{16}, 11^2, 14^1, 27^1
31	7^{157}, 8^{6099}, 9^{7998}, 10^{1629}, 11^{113}, 12^{11}, 13^{11}, 16^1, 31^1
43	7^2, 8^{4495}, 9^{121241}, 10^{258708}, 11^{121126}, 12^{21011}, 13^{2196}, 14^{195}, 15^{45}, 16^{19}, 17^8, 22^1, 43^1

If $q \equiv 3 \pmod 4$, the subfield $\mathbb{F}_q$ of $\mathbb{F}_{q^2}$ consists of $(q+1)$-th powers, so certainly of 4th powers, and hence induces a clique of size q (reaching the Hoffman bound). A vertex outside has $\frac{q-1}{2}$ neighbors inside, yielding a $\frac{q+1}{2}$-clique.

References

[1] 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.

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

[3] A. E. Brouwer, *Locally Paley graphs*, Des. Codes Cryptogr. **21** (2000) 69–76.

[4] A. E. Brouwer, A. M. Cohen & A. Neumaier, *Distance-regular graphs*, Springer, 1989.

[5] A. E. Brouwer & H. Van Maldeghem, *Strongly regular graphs*, Cambridge Univ. Press, 2022.

[6] S. Goryainov, V. V. Kabanov, L. Shalaginov & A. Valuzhenich, *On eigenfunctions and maximal cliques of Paley graphs of square order*, Finite Fields Appl. **52** (2018) 361–369.

[7] S. Goryainov, A. Masley & L. Shalaginov, *On a correspondence between maximal cliques in Paley graphs of square order*, Discr. Math. **345** (2022) 112853.

[8] M. Kiermaier & S. Kurz, *Maximal integral point sets in affine planes over finite fields*, Discr. Math. **309** (2009) 4564–4575.

[9] M. Muzychuk & I. Kovács, *A solution of a problem of A. E. Brouwer*, Des. Codes Cryptogr. **34** (2005) 249–264.

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

[11] P. Sziklai, *On subsets of* $\mathrm{GF}(q^2)$ *with dth power differences*, Discr. Math. **208/209** (1999) 547–555.

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