On a correspondence between maximal cliques in Paley graphs of square order

Sergey Goryainov

Chelyabinsk State University

Based on a joint project with
Alexander Masley and Leonid Shalaginov

Graphs and Groups, Geometries and GAP (G2G2-2021)
June 24th, 2021
1 Preliminary
2 Two families of maximal cliques in Paley graphs of square order
3 Correspondence between two known families of maximal cliques
Let $q$ be an odd prime power, $q \equiv 1(4)$.

The **Paley graph** of order $q$ (denoted by $P(q)$) is a graph defined as follows:

- the vertex set is the finite field $\mathbb{F}_q$;
- two vertices $\gamma_1, \gamma_2$ are adjacent iff $\gamma_1 - \gamma_2$ is a square in $\mathbb{F}_q^*$.

Since $-1$ is a square in $\mathbb{F}_q^*$ iff $q \equiv 1(4)$, the graph $P(q)$ is undirected.
A clique (resp. coclique) in an undirected graph is a set of pairwise adjacent (resp. non-adjacent) vertices.

Problem 1

What are maximum cliques (cocliques) in $P(q)$?

Since $P(q)$ is self-complementary, the studying cliques and the studying cocliques in $P(q)$ are equivalent.

Since $P(q)$ is strongly regular, we can apply Delsarte-Hoffman bound to $P(q)$. It says that a clique (coclique) in $P(q)$ has at most $\sqrt{q}$ vertices.

Problem 1 is unsolved in general.
The case of Paley graphs of square order $q^2$

Let $q$ be an odd prime power.

According to the Delsarte-Hoffman bound, a clique in $P(q^2)$ has at most $q$ vertices.

Since every element from $\mathbb{F}_q^*$ is a square in $\mathbb{F}_{q^2}^*$, the subfield $\mathbb{F}_q$ induces a clique of size $q$ in $P(q^2)$, which implies the tightness of the Delsarte-Hoffman bound.

In 1984, Blokhuis classified maximum cliques in $P(q^2)$ and proved [1] that such a clique is an affine image of the subfield $\mathbb{F}_q$.

Problem 2

What are maximal but not maximum cliques in $P(q^2)$?

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

In 1996, Baker et al. found [2] maximal cliques of size $\frac{q + r(q)}{2}$ in $P(q^2)$ for any odd prime power $q$. Let us say that these cliques are of Type I.

In 2018, Goryainov et al. found [3] one more family of maximal cliques in $P(q^2)$ with the same size $\frac{q + r(q)}{2}$. Let us say that these cliques are of Type II.


Computations on maximal cliques of size $\frac{q+r(q)}{2}$ in $P(q^2)$

<table>
<thead>
<tr>
<th>$q$</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>9</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clique size</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>5</td>
<td>7</td>
<td>7</td>
<td>9</td>
<td>11</td>
<td>13</td>
</tr>
<tr>
<td>#Orbits</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$q$</th>
<th>25</th>
<th>27</th>
<th>29</th>
<th>31</th>
<th>37</th>
<th>41</th>
<th>43</th>
<th>47</th>
<th>49</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clique size</td>
<td>13</td>
<td>15</td>
<td>15</td>
<td>17</td>
<td>19</td>
<td>21</td>
<td>23</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>#Orbits</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$q$</th>
<th>53</th>
<th>59</th>
<th>61</th>
<th>67</th>
<th>71</th>
<th>73</th>
<th>79</th>
<th>81</th>
<th>83</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clique size</td>
<td>27</td>
<td>31</td>
<td>31</td>
<td>35</td>
<td>37</td>
<td>37</td>
<td>41</td>
<td>41</td>
<td>43</td>
</tr>
<tr>
<td>#Orbits</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Conjecture

For $q \geq 25$, the graph $P(q^2)$ contains exactly two non-equivalent cliques of size $\frac{q+r(q)}{2}$. 
Fix a non-square $d \in \mathbb{F}_q^*$. 

Consider the polynomial $f(t) = t^2 - d \in \mathbb{F}_q[t]$. 

Then
\[
\mathbb{F}_{q^2} = \{x + y\alpha \mid x, y \in \mathbb{F}_q\},
\]
where $\alpha$ is a root of $f(t)$. 

Let $\beta$ be a primitive element of $\mathbb{F}_{q^2}$. 

Note that the elements from $\mathbb{F}_q^* = \langle \beta^{q+1} \rangle$ are squares in $\mathbb{F}_{q^2}^*$. 

Let $V(2, q)$ be a 2-dimensional vector space over $\mathbb{F}_q$.

Consider the affine plane $A(2, q)$ whose

- points are vectors of $V(2, q)$;
- lines are all cosets of 1-dimensional subspaces in $V(2, q)$;
- incidence relation is natural (whether a vector belongs to a coset).

Since $\mathbb{F}_{q^2}$ can viewed as a 2-dimensional vector space over $\mathbb{F}_q$, the points of $A(2, q)$ can be matched with the elements of $\mathbb{F}_{q^2}$ as follows:

$$(x, y) \leftrightarrow x + y\alpha.$$
Given a line $\ell$ in $A(2, q)$, there exist elements $x_1 + y_1\alpha$ and $x_2 + y_2\alpha$ such that

$$\ell = \{x_1 + y_1\alpha + c(x_2 + y_2\alpha) \mid c \in \mathbb{F}_q\}.$$ 

The line $\ell$ is called quadratic (rep. non-quadratic) if $x_2 + y_2\alpha$ is a square (resp. non-square) in $\mathbb{F}_{q^2}^*$. 

- The subfield $\mathbb{F}_q$ is a quadratic line.
- There are precisely $q + 1$ lines through a point: $\frac{q+1}{2}$ quadratic and $\frac{q+1}{2}$ non-quadratic lines.
For any distinct $\gamma_1, \gamma_2 \in \mathbb{F}_{q^2}$, the difference $\gamma_1 - \gamma_2$ is a square in $\mathbb{F}_{q^2}^*$ (equivalently, $\gamma_1 \sim \gamma_2$ in $P(q^2)$) iff the line connecting $\gamma_1$ and $\gamma_2$ is quadratic.
The automorphism group of $P(q^2)$ acts arc-transitively, and the following equality

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

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

The group $\text{Aut}(P(q^2))$ preserves the sets of quadratic and non-quadratic lines.

The group $\text{Aut}(P(q^2))$ 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 $b \in \mathbb{F}_q$. 
Take an element $\gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

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

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

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

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

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

The subgroup $Q$ of order $q + 1$ in $\mathbb{F}_{q^2}^*$

Put

$$\omega := \beta^{q-1}, \quad Q := \langle \omega \rangle,$$

$$Q_0 := \langle \omega^2 \rangle, \quad Q_1 := \omega \langle \omega^2 \rangle.$$

- $Q$ is a subgroup of order $q + 1$ in $\mathbb{F}_{q^2}^*$
- $Q$ is the kernel of the norm mapping $N : \mathbb{F}_{q^2}^* \mapsto \mathbb{F}_q^*$; given an element $\gamma = x + y\alpha \in \mathbb{F}_{q^2}^*$,

$$N(\gamma) := \gamma^{q+1} = \gamma\gamma^q = \gamma\overline{\gamma} = x^2 - y^2d$$

- $Q$ forms an oval in $A(2, q)$ (that is a set of $q + 1$ points with no three on a line)
- $Q$ is included to the neighbourhood of 0
- If $q \equiv 1(4)$, then $Q$ induces the complete bipartite graph with parts $Q_0$ and $Q_1$
- If $q \equiv 3(4)$, then $Q$ induces a pair of disjoint cliques $Q_0$ and $Q_1$
If $q \equiv 1(4)$, each of the sets $Q_0$ and $Q_1$ induces a maximal coclique of size $\frac{q+1}{2}$ in $P(q^2)$ (a maximal clique of size $\frac{q+1}{2}$ in $\overline{P(q^2)}$).

If $q \equiv 3(4)$, each of the sets $\{0\} \cup Q_0$ and $\{0\} \cup Q_1$ induces a maximal clique of size $\frac{q+3}{2}$ in $P(q^2)$.

Consider the mapping \( \varphi : \mathbb{F}_{q^2} \rightarrow \mathbb{F}_{q^2} \) defined by the rule:

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

**Proposition 1**
For any \( \gamma = x + y\alpha \in Q, \gamma \neq 1 \), the equality \( \varphi(\gamma) = \frac{y}{x-1}\alpha \) holds.

It means that \( \varphi \) maps \( Q \setminus \{1\} \) to the line \( \{c\alpha \mid c \in \mathbb{F}_q\} \).

**Proposition 2**
For any \( \gamma = x + y\alpha \in Q, \gamma \neq 1 \), the equality \( \varphi(\gamma^2) = \frac{x}{yd}\alpha \) holds.

**Theorem**
If \( q \equiv 1(4) \), then \( \varphi(Q_0) \) is a coclique of size \( \frac{q+1}{2} \) and of Type I; if \( q \equiv 3(4) \), then \( \varphi(Q_0 \cup \{0\}) \) is a maximal clique of size \( \frac{q+3}{2} \) and of Type I.
We are interested to find a generalisation of Theorem for 3-Paley graphs of square order (two vertices are adjacent iff their difference is a cube in $\mathbb{F}_{q^2}^*$).

Computations show that, for $q = 11, 17, 23, 29, 41, 47, 53$, an analogue of Theorem holds for 3-Paley graphs of square order $q^2$. 
Thank you for your attention!