Paley Uniform Hypergraphs

Shonda Gosselin

University of Winnipeg

Algebraic Graph Theory Workshop
Banff International Research Station
April 29, 2011

Outline

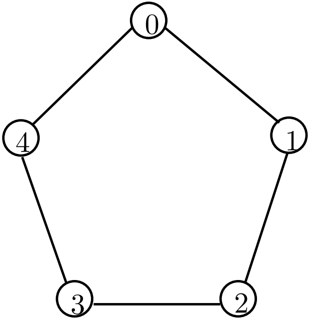
Outline

The Paley graph P_n

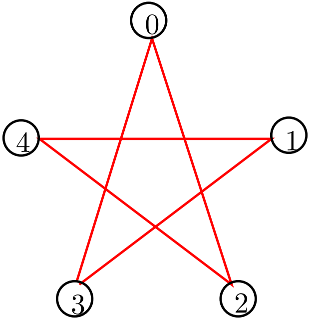
Definition

For a prime power $n \equiv 1 \pmod 4$ and a finite field $\mathbb{F}_n$, the **Paley graph of order n**, denoted by $\mathbf{P_n}$, is the simple graph with vertex set $V = \mathbb{F}_n$ and edge set E, where

$$\{x, y\} \in E \iff x - y \text{ is a nonzero square.}$$

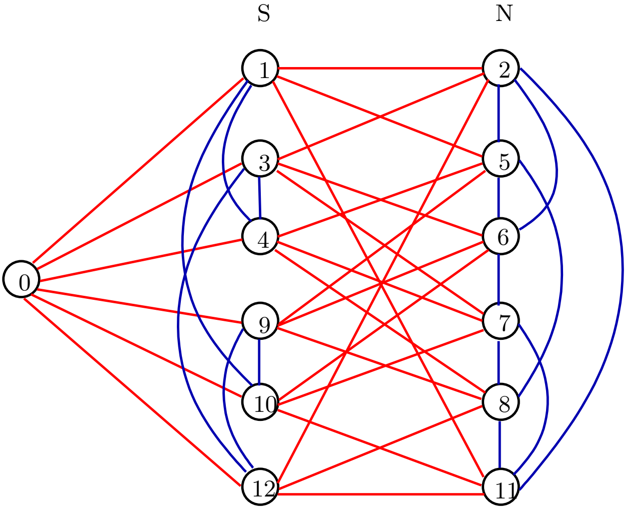


P_5

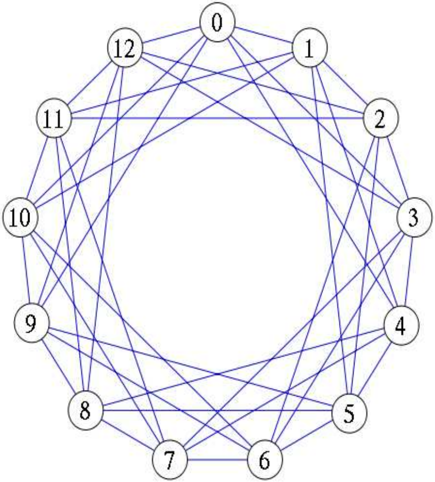


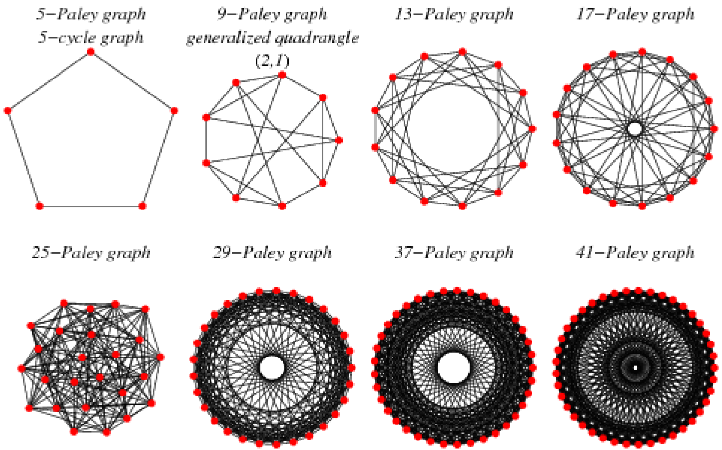
P_5^C

P_{13}



P_{13}




5−Paley graph
5−cycle graph
9−Paley graph
generalized quadrangle
(2,1)
13−Paley graph
17−Paley graph
25−Paley graph
29−Paley graph
37−Paley graph
41−Paley graph

P_n is self-complementary

If ω is a generator of $\mathbb{F}_n^*$, then

$$x - y \in \langle \omega^2 \rangle \iff \omega x - \omega y = \omega(x - y) \notin \langle \omega^2 \rangle.$$

$\mathbf{T}_{\omega,\mathbf{0}} : x \mapsto \omega x$ is an isomorphism from P_n to its complement. $\square$

Properties of the Paley graph P_n

- Cayley graph $Cay(\mathbb{F}_n; \langle \omega^2 \rangle)$ (vertex-transitive)
- self-complementary
- arc-transitive
- strongly regular $\left(n, \frac{n-1}{2}, \frac{n-5}{4}, \frac{n-1}{4}\right)$ (a conference graph)
- distance-transitive
- P_n and P_n^C are the relation graphs of a symmetric 2-class association scheme.
- $Aut(P_n)$ is an index-2 subgroup of the affine group $A\Gamma L(1, n)$

Outline

Definition

A simple k-uniform hypergraph X with vertex set V and edge set E is **(cyclically) q-complementary** if there is a permutation θ on V such that the sets

$$E, E^{\theta}, E^{\theta^2}, \ldots, E^{\theta^{q-1}}$$

partition the set of k-subsets of V.

θ is called a **q-antimorphism** of X (i.e., $\theta \in \mathbf{Ant_q(X)}$).

- The 2-complementary 2-uniform hypergraphs are the **self-complementary graphs**, which have been well studied due to their connection to the graph isomorphism problem.

- The q-complementary k-hypergraphs correspond to **cyclic edge decompositions (cyclotomic factorisations)** of the complete k-uniform hypergraph into q parts.

- The vertex-transitive q-complementary k-uniform hypergraphs correspond to **large sets of isomorphic designs** which are point-transitive.

- The strongly regular q-complementary graphs are the relation graphs of **symmetric q-class cyclotomic association schemes**.

Outline

The Paley graph P_n - revisited

Definition

For a prime power $n \equiv 1 \pmod 4$ and a finite field $\mathbb{F}_n$ of order n, the **Paley graph of order n**, denoted by $\mathbf{P_n} = (\mathbf{V}, \mathbf{E})$, is the simple graph with $\mathbf{V} = \mathbb{F}_\mathbf{n}$ and

$$\{\mathbf{x}, \mathbf{y}\} \in \mathbf{E} \iff \mathbf{x} - \mathbf{y} \in \langle \omega^\mathbf{2} \rangle$$

where ω is a generator of $\mathbb{F}_n^*$.

Generalized Paley Graphs

Definition

Let $\mathbb{F}_n$ be a finite field of order n, and let q be a divisor of $n-1$ where $q \geq 2$, and if n is odd then $(n-1)/q$ is even. Let $S \leq \mathbb{F}_n^*$ where $|S| = (n-1)/q$.

The **generalized Paley graph $\mathbf{GPaley(n,q)}$** is the graph with vertex set $\mathbb{F}_n$ and edge set all pairs $\{x, y\}$ with $x - y \in S$.

Generalized Paley Graphs

Definition

Let $\mathbb{F}_n$ be a finite field of order n, and let q be a divisor of $n-1$ where $q \geq 2$, and if n is odd then $(n-1)/q$ is even. Let $S \leq \mathbb{F}_n^*$ where $|S| = (n-1)/q$.

The **generalized Paley graph** $\mathbf{GPaley(n, q)}$ is the graph with vertex set $\mathbb{F}_n$ and edge set all pairs $\{x, y\}$ with $x - y \in S$.

- Cayley graph $Cay(\mathbb{F}_n; S = \langle \omega^q \rangle)$ (vertex-transitive)
- arc-transitive
- q-complementary ($x \mapsto \omega x$ is a q-antimorphism)
- the relation graphs of symmetric q-class cyclotomic association schemes.
- If $n = p^\alpha$ and q divides $p-1$, then $GPaley(n, q)$ is strongly regular, and $Aut(GPaley(n, q))$ is an index-q subgroup of $A\Gamma L(1, n)$.

Constructing q-complementary k-hypergraphs

Partition a group G into q sets

$$\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{q-1},$$

where each $\mathcal{C}_i$ is a union of cosets of a subgroup S of G.

Find an operation $\Psi : V^{(k)} \to G$ and a permutation $\theta : V \to V$ such that

$$\Psi(\{x_1, \ldots, x_k\}) \in \mathcal{C}_i \iff \Psi(\{x_1, \ldots, x_k\}^{\theta}) \in \mathcal{C}_{i+s}$$

for some s where $\gcd(s, q) = 1$.

Let $E_i = \{e \in V^{(k)} \mid \Psi(e) \in \mathcal{C}_i\}$.

Then $X_i = (V, E_i)$ is q-complementary with q-antimorphism θ.

Examples

1. Generalized Paley Graphs:
   - $V = \mathbb{F}_n$.
   - $G = \mathbb{F}_n^*$.
   - $S = \langle \omega^q \rangle$.
   - $\Psi(\{x, y\}) = x - y$.
2. q-Paley k-hypergraphs:
   - $V = \mathbb{F}_n$.
   - G is the group of squares of $\mathbb{F}_n^*$.
   - $S = \langle \omega^{2q\binom{k}{2}} \rangle$
   - Ψ: the square of the Van der Monde determinant,

$$VM^2(x_1, x_2, \ldots, x_k) = \prod_{i<j} (x_i - x_j)^2.$$

The q-Paley k-hypergraph $P^q_{n,k}$

Definition

q is prime, ℓ is the highest power of q dividing k or $k-1$.
n is a prime power, $n \equiv 1 \pmod{q^{\ell+1}}$
G is the group of squares in $\mathbb{F}_n^*$.
$S = \langle \omega^{2q\binom{k}{2}} \rangle$.
$c = \gcd(|G|, \binom{k}{2})$. ($qc$ is the number of cosets of S in G.)
F_i is the coset $\omega^{2i}\langle \omega^{2q\binom{k}{2}} \rangle$ in G $(0 \leq i \leq qc-1)$.
$\mathcal{C}_j = F_{jc+0} \cup F_{jc+1} \cup \cdots \cup F_{(j+1)c-1}$ $(0 \leq j \leq q-1)$.

The **q-Paley k-hypergraph of order n**, $\mathbf{P^q_{n,k}} = (V, E)$, is the simple k-hypergraph with $\mathbf{V} = \mathbb{F}_\mathbf{n}$ and

$$\{\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_k}\} \in \mathbf{E} \iff \prod_{\mathbf{i<j}} (\mathbf{x_i} - \mathbf{x_j})^2 \in \mathcal{C}_\mathbf{0}.$$

$P^q_{n,k}$ is q-complementary

$$
\begin{aligned}
& VM^2(x_1, x_2, \ldots, x_k) \in F_i \\
\iff & VM^2(\omega x_1, \omega x_2, \ldots, \omega x_k) = \omega^{2\binom{k}{2}} VM^2(x_1, x_2, \ldots, x_k) \in F_{i+sc},
\end{aligned}
$$

where $\gcd(q, s) = 1$.

$\mathbf{T}_{\omega,\mathbf{0}} : \mathbf{x} \to \omega\mathbf{x}$ is a q-antimorphism of $P^q_{n,k}$.

$P^q_{n,k}$ is vertex-transitive

For $b \in \mathbb{F}_n$,

$$\begin{aligned} & VM^2(x_1, x_2, \ldots, x_k) \in F_i \\ \iff & VM^2(x_1 + b, x_2 + b, \ldots, x_k + b) = VM^2(x_1, x_2, \ldots, x_k) \in F_i. \end{aligned}$$

$\mathbf{T_{1,b}} : \mathbf{x} \to \mathbf{x} + \mathbf{b}$ is an automorphism of $P^q_{n,k}$.

Automorphisms and q-antimorphisms of $P^q_{n,k}$

$$Aut(P^q_{n,k}) \geq \{T_{a,b} \mid a = \omega^s, s \equiv 0 \pmod{q}, b \in \mathbb{F}_n\}$$

$$Ant_q(P^q_{n,k}) \supseteq \{T_{a,b} \mid a = \omega^s, s \not\equiv 0 \pmod{q}, b \in \mathbb{F}_n\}.$$

$\mathbf{T_{a,b} : x \mapsto ax + b}$

$Aut(P^q_{n,k})$ contains an index-q subgroup of $A\Gamma L(1, n)$.

The q-Paley k-hypergraph $P^q_{n,k,r}$

Definition

q is prime, ℓ is the highest power of q dividing k or $k-1$.
n is a prime power, $n \equiv 1 \pmod{q^{\ell+1}}$
G is the group of squares in $\mathbb{F}_n^*$.
r is a divisor of $(n-1)/q^{\ell+1}$.
$S = \langle \omega^{2rq\binom{k}{2}} \rangle$.
$c = \gcd(|G|, r\binom{k}{2})$. ($qc$ is the number of cosets of S in G.)
F_i is the coset $\omega^{2i}\langle \omega^{2rq\binom{k}{2}} \rangle$ in G $(0 \leq i \leq qc-1)$.
$\mathcal{C}_j = F_{jc+0} \cup F_{jc+1} \cup \cdots \cup F_{(j+1)c-1} (0 \leq j \leq q-1)$.

The **q-Paley k-hypergraph of order n**, $\mathbf{P^q_{n,k,r}} = (V, E)$, is the simple k-hypergraph with $\mathbf{V} = \mathbb{F}_\mathbf{n}$ and

$$\{\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_k}\} \in \mathbf{E} \iff \prod_{\mathbf{i<j}} (\mathbf{x_i} - \mathbf{x_j})^2 \in \mathcal{C}_\mathbf{0}.$$

Automorphisms and q-antimorphisms of ${P_{n,k,r}}^q$

$$Aut(P^q_{n,k,r}) \geq \{T_{a,b} \mid a = \omega^{rs}, s \equiv 0 \pmod q, b \in \mathbb{F}_n\}$$

$$Ant_q(P^q_{n,k,r}) \supseteq \{T_{a,b} \mid a = \omega^{rs}, s \not\equiv 0 \pmod q, b \in \mathbb{F}_n\}$$

$\mathbf{T_{a,b} : x \mapsto ax + b}$

$Aut(P^q_{n,k,r})$ contains an index-qr subgroup of $A\Gamma L(1, n)$.

q-Paley k-hypergraph constructions

$q = 2,\ k = 2,\ r = 1$ (Paley)
$q = 2,\ k = 3,\ r = 1$, (Kocay, 1992)
$q = 2,\ k = 2$, any r (Peisert, 2001)
$q,\ k = 2$ (Li, Praeger 2003)(Li, Lim and Praeger 2009)
$q = 2$, any k, $r = 1$, (Potočnik and Šajna, 2009)
Odd prime q, any k, any r, (G. 2010)

Raymond Paley (1907-1933)