The critical group of a graph

Peter Sin, U. of Florida

Gainesville International Number Theory Conference,
March 20th, 2016
in honor of Krishna Alladi's 60th birthday

Critical groups of graphs

This talk is about the *critical group*, a finite abelian group associated with a finite graph.

This talk is about the *critical group*, a finite abelian group associated with a finite graph.

The critical group is defined using the *Laplacian matrix* of the graph.

This talk is about the *critical group*, a finite abelian group associated with a finite graph.

The critical group is defined using the *Laplacian matrix* of the graph.

The critical group arises in various contexts;

This talk is about the *critical group*, a finite abelian group associated with a finite graph.

The critical group is defined using the *Laplacian matrix* of the graph.

The critical group arises in various contexts;

- in statistical physics: *Abelian Sandpile model* (Bak-Tang-Wiesenfeld, Dhar);

This talk is about the *critical group*, a finite abelian group associated with a finite graph.

The critical group is defined using the *Laplacian matrix* of the graph.

The critical group arises in various contexts;

- in statistical physics: *Abelian Sandpile model* (Bak-Tang-Wiesenfeld, Dhar);
- its combinatorial variant: the *Chip-firing game* (Björner-Lovasz-Shor, Gabrielov, Biggs);

This talk is about the *critical group*, a finite abelian group associated with a finite graph.

The critical group is defined using the *Laplacian matrix* of the graph.

The critical group arises in various contexts;

- in statistical physics: *Abelian Sandpile model* (Bak-Tang-Wiesenfeld, Dhar);
- its combinatorial variant: the *Chip-firing game* (Björner-Lovasz-Shor, Gabrielov, Biggs);
- in arithmetic geometry: Néron models (Lorenzini)

This talk is about the *critical group*, a finite abelian group associated with a finite graph.

The critical group is defined using the *Laplacian matrix* of the graph.

The critical group arises in various contexts;

- in statistical physics: *Abelian Sandpile model* (Bak-Tang-Wiesenfeld, Dhar);
- its combinatorial variant: the *Chip-firing game* (Björner-Lovasz-Shor, Gabrielov, Biggs);
- in arithmetic geometry: Néron models (Lorenzini)
- Riemann-Roch for graphs: graph jacobian (Baker-Norine).

This talk is about the *critical group*, a finite abelian group associated with a finite graph.

The critical group is defined using the *Laplacian matrix* of the graph.

The critical group arises in various contexts;

- in statistical physics: *Abelian Sandpile model* (Bak-Tang-Wiesenfeld, Dhar);
- its combinatorial variant: the *Chip-firing game* (Björner-Lovasz-Shor, Gabrielov, Biggs);
- in arithmetic geometry: Néron models (Lorenzini)
- Riemann-Roch for graphs: graph jacobian (Baker-Norine).

We'll discuss the general problem of computing the critical group for families of graphs, and the specific case of the Paley graphs.

Laplacian matrix and critical group

Let $\Gamma = (V, E)$ be a simple, connected graph.

Laplacian matrix and critical group

Let $\Gamma = (V, E)$ be a simple, connected graph.

$A :=$ adjacency matrix, $D :=$ degree matrix, $L = D - A$ is the *Laplacian matrix*.

Laplacian matrix and critical group

Let $\Gamma = (V, E)$ be a simple, connected graph.

$A :=$ adjacency matrix, $D :=$ degree matrix, $L = D - A$ is the *Laplacian matrix*.

Think of L as a linear map $L : \mathbf{Z}^V \to \mathbf{Z}^V$.

Laplacian matrix and critical group

Let $\Gamma = (V, E)$ be a simple, connected graph.

$A :=$ adjacency matrix, $D :=$ degree matrix, $L = D - A$ is the *Laplacian matrix*.

Think of L as a linear map $L : \mathbf{Z}^V \to \mathbf{Z}^V$.

$\mathrm{rank}(L) = |V| - 1$.

Laplacian matrix and critical group

Let $\Gamma = (V, E)$ be a simple, connected graph.

$A :=$ adjacency matrix, $D :=$ degree matrix, $L = D - A$ is the *Laplacian matrix*.

Think of L as a linear map $L : \mathbf{Z}^V \to \mathbf{Z}^V$.

$\mathrm{rank}(L) = |V| - 1$.

$\mathbf{Z}^V / \mathrm{Im}(L) \cong \mathbf{Z} \oplus K(\Gamma)$

Laplacian matrix and critical group

Let $\Gamma = (V, E)$ be a simple, connected graph.

$A :=$ adjacency matrix, $D :=$ degree matrix, $L = D - A$ is the *Laplacian matrix*.

Think of L as a linear map $L : \mathbf{Z}^V \to \mathbf{Z}^V$.

$\mathrm{rank}(L) = |V| - 1$.

$\mathbf{Z}^V / \mathrm{Im}(L) \cong \mathbf{Z} \oplus K(\Gamma)$

The finite group $K(\Gamma)$ is called the *critical group* of Γ.

Kirchhoff's Matrix-Tree Theorem

Kirchhoff's Matrix Tree Theorem

For any connected graph Γ*, the number of spanning trees is equal to* $\det(\tilde{L})$*, where* $\tilde{L}$ *is obtained from L be deleting the row and column corrresponding to any chosen vertex.*

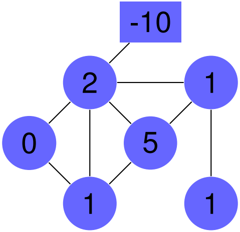
Kirchhoff's Matrix-Tree Theorem

Kirchhoff's Matrix Tree Theorem

For any connected graph Γ*, the number of spanning trees is equal to* $\det(\tilde{L})$*, where* $\tilde{L}$ *is obtained from L be deleting the row and column corrresponding to any chosen vertex.*

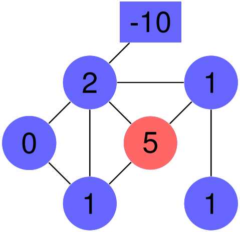
Also, $\det(\tilde{L}) = |K(\Gamma)| = \frac{1}{|V|}\prod_{j=2}^{|V|}\lambda_j$.

Rules



A *configuration* is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.

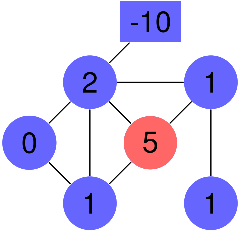
Rules

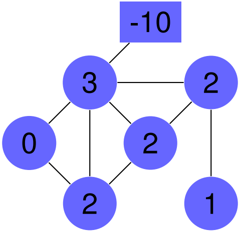


A *configuration* is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.

A round vertex v can be fired if it has at least $\deg(v)$ chips.

Rules

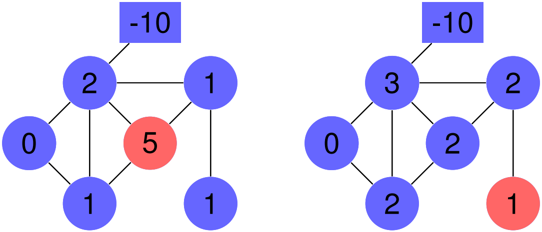




A *configuration* is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.

A round vertex v can be fired if it has at least $\deg(v)$ chips.

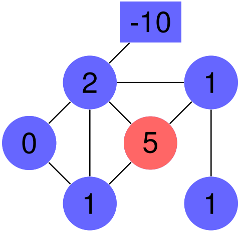
Rules

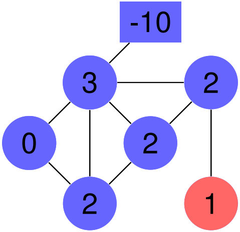


A *configuration* is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.

A round vertex v can be fired if it has at least $\deg(v)$ chips.

Rules



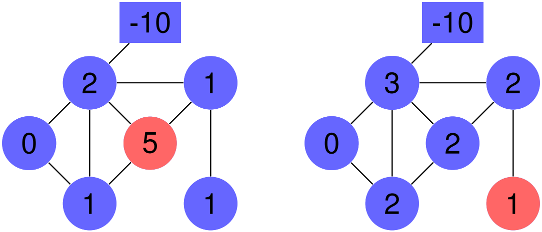


A *configuration* is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.

A round vertex v can be fired if it has at least $\deg(v)$ chips.

The square vertex is fired only when no others can be fired.

Rules



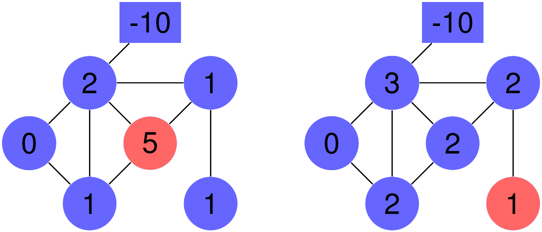
A *configuration* is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.

A round vertex v can be fired if it has at least $\deg(v)$ chips.

The square vertex is fired only when no others can be fired.

A configuration is *stable* if no round vertex can be fired.

Rules



A *configuration* is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.

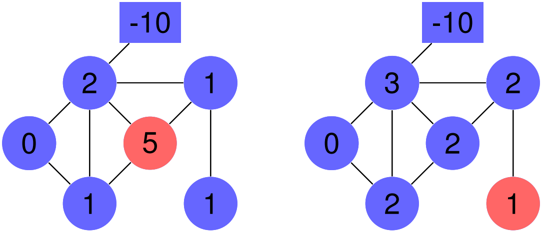
A round vertex v can be fired if it has at least $\deg(v)$ chips.

The square vertex is fired only when no others can be fired.

A configuration is *stable* if no round vertex can be fired.

A configuration is *recurrent* if there is a sequence of firings that lead to the same configuration.

Rules



A *configuration* is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.

A round vertex v can be fired if it has at least $\deg(v)$ chips.

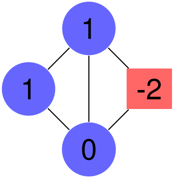
The square vertex is fired only when no others can be fired.

A configuration is *stable* if no round vertex can be fired.

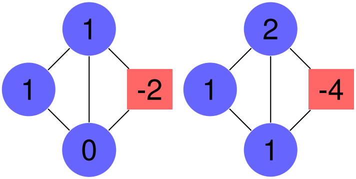
A configuration is *recurrent* if there is a sequence of firings that lead to the same configuration.

A configuration is *critical* if it is both recurrent and stable.

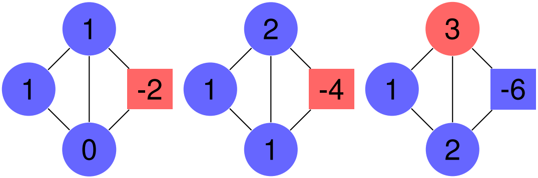
Sample game 1



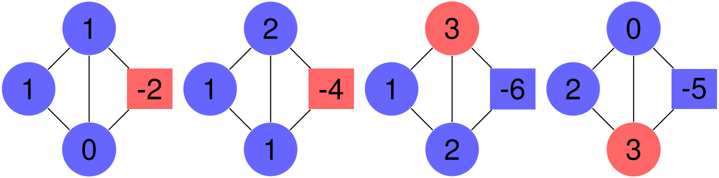
Sample game 1



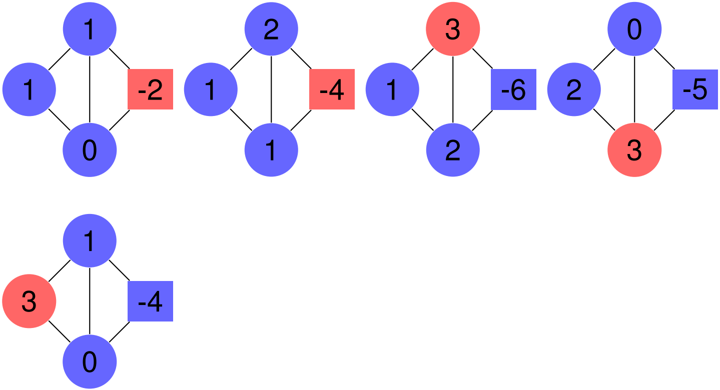
Sample game 1



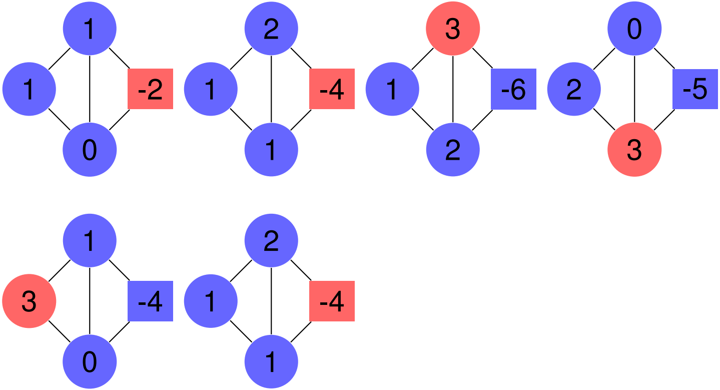
Sample game 1



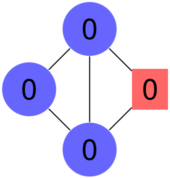
Sample game 1



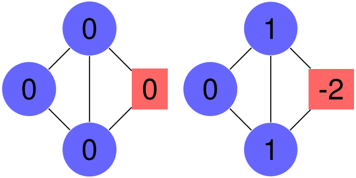
Sample game 1



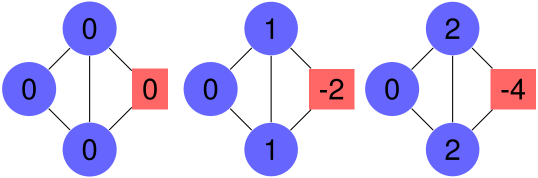
Sample game 2



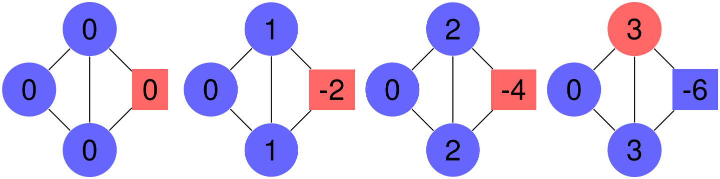
Sample game 2



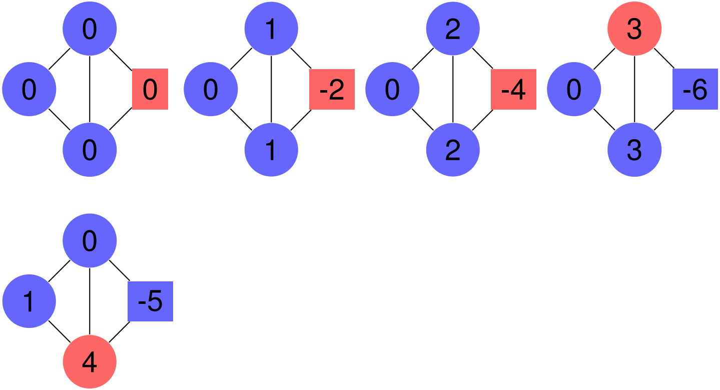
Sample game 2



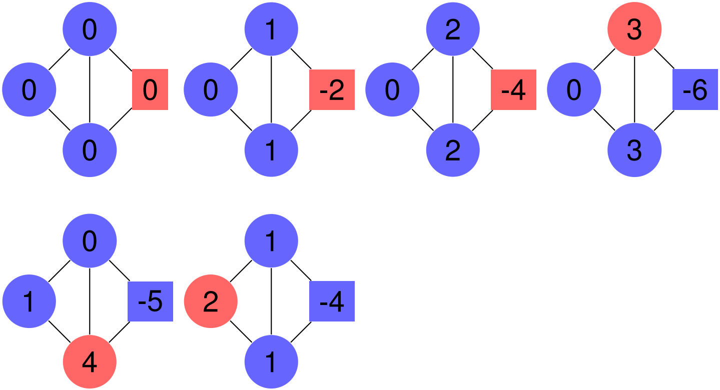
Sample game 2



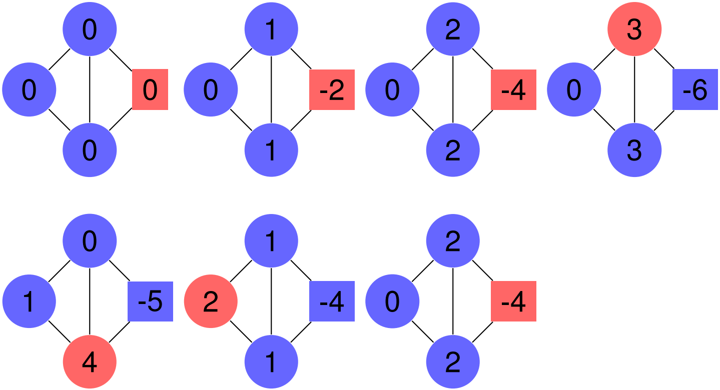
Sample game 2



Sample game 2



Sample game 2



Relation with Laplacian

Start with a configuration s and fire vertices in a sequence where each vertex v is fired $x(v)$ times, ending up with configuration s'.

Relation with Laplacian

Start with a configuration s and fire vertices in a sequence where each vertex v is fired $x(v)$ times, ending up with configuration s'.

$s'(v) = s(v) - x(v)\deg(v) + \sum_{(v,w)\in E} x(w)$

Relation with Laplacian

Start with a configuration s and fire vertices in a sequence where each vertex v is fired $x(v)$ times, ending up with configuration s'.

$s'(v) = s(v) - x(v)\deg(v) + \sum_{(v,w)\in E} x(w)$

$s' = s - Lx$

Relation with Laplacian

Start with a configuration s and fire vertices in a sequence where each vertex v is fired $x(v)$ times, ending up with configuration s'.

$s'(v) = s(v) - x(v)\deg(v) + \sum_{(v,w)\in E} x(w)$

$s' = s - Lx$

Theorem (Biggs)

Let s be a configuration in the chip-firing game on a connected graph G. Then there is a unique critical configuration which can be reached from s.

Relation with Laplacian

Start with a configuration s and fire vertices in a sequence where each vertex v is fired $x(v)$ times, ending up with configuration s'.

$s'(v) = s(v) - x(v)\deg(v) + \sum_{(v,w)\in E} x(w)$

$s' = s - Lx$

Theorem (Biggs)

Let s be a configuration in the chip-firing game on a connected graph G. Then there is a unique critical configuration which can be reached from s.

Theorem (Biggs)

The set of critical configurations has a natural group operation making it isomorphic to the critical group $K(\Gamma)$.

Smith normal form

Two integer matrices X and Y are *equivalent* iff there exist unimodular integer matrices P and Q such that $PXQ = Y$

Smith normal form

Two integer matrices X and Y are *equivalent* iff there exist unimodular integer matrices P and Q such that $PXQ = Y$

Each equivalence class contains a *Smith normal form*

$$\left[\begin{array}{c:c} H & 0 \\ \hdashline 0 & 0 \end{array}\right], \quad H = \mathrm{diag}(s_1, s_2, \ldots s_r), \quad s_1 | s_2 | \cdots | s_r.$$

Smith normal form

Two integer matrices X and Y are *equivalent* iff there exist unimodular integer matrices P and Q such that $PXQ = Y$

Each equivalence class contains a *Smith normal form*

$$\left[\begin{array}{c:c} H & 0 \\ \hdashline 0 & 0 \end{array}\right], \quad H = \mathrm{diag}(s_1, s_2, \ldots s_r), \quad s_1 | s_2 | \cdots | s_r.$$

Similarly for PIDs.

Smith normal form

Two integer matrices X and Y are *equivalent* iff there exist unimodular integer matrices P and Q such that $PXQ = Y$

Each equivalence class contains a *Smith normal form*

$$\left[\begin{array}{c:c} H & 0 \\ \hdashline 0 & 0 \end{array}\right], \quad H = \mathrm{diag}(s_1, s_2, \ldots s_r), \quad s_1 | s_2 | \cdots | s_r.$$

Similarly for PIDs.

The SNF of the Laplacian gives the structure of the critical group.

- Trees, $K(\Gamma) = \{0\}$.

- Trees, $K(\Gamma) = \{0\}$.
- Complete graphs, $K(K_n) \cong (\mathbf{Z}/n\mathbf{Z})^{n-2}$.

- Trees, $K(\Gamma) = \{0\}$.
- Complete graphs, $K(K_n) \cong (\mathbf{Z}/n\mathbf{Z})^{n-2}$.
- Wheel graphs W_n, $K(\Gamma) \cong (\mathbf{Z}/\ell_n)^2$, if n is odd (Biggs). Here ℓ_n is a *Lucas* number.

- Trees, $K(\Gamma) = \{0\}$.
- Complete graphs, $K(K_n) \cong (\mathbf{Z}/n\mathbf{Z})^{n-2}$.
- Wheel graphs W_n, $K(\Gamma) \cong (\mathbf{Z}/\ell_n)^2$, if n is odd (Biggs). Here ℓ_n is a *Lucas* number.
- Complete multipartite graphs (Jacobson, Niedermaier, Reiner 2003).

- Trees, $K(\Gamma) = \{0\}$.
- Complete graphs, $K(K_n) \cong (\mathbf{Z}/n\mathbf{Z})^{n-2}$.
- Wheel graphs W_n, $K(\Gamma) \cong (\mathbf{Z}/\ell_n)^2$, if n is odd (Biggs). Here ℓ_n is a *Lucas* number.
- Complete multipartite graphs (Jacobson, Niedermaier, Reiner 2003).
- Conference graphs on a square-free number of vertices (Lorenzini 2008).

- Trees, $K(\Gamma) = \{0\}$.
- Complete graphs, $K(K_n) \cong (\mathbf{Z}/n\mathbf{Z})^{n-2}$.
- Wheel graphs W_n, $K(\Gamma) \cong (\mathbf{Z}/\ell_n)^2$, if n is odd (Biggs). Here ℓ_n is a *Lucas* number.
- Complete multipartite graphs (Jacobson, Niedermaier, Reiner 2003).
- Conference graphs on a square-free number of vertices (Lorenzini 2008).
- Incidence graph of Lines in finite Projective space (Brouwer-Ducey-S 2012).

- Trees, $K(\Gamma) = \{0\}$.
- Complete graphs, $K(K_n) \cong (\mathbf{Z}/n\mathbf{Z})^{n-2}$.
- Wheel graphs W_n, $K(\Gamma) \cong (\mathbf{Z}/\ell_n)^2$, if n is odd (Biggs). Here ℓ_n is a *Lucas* number.
- Complete multipartite graphs (Jacobson, Niedermaier, Reiner 2003).
- Conference graphs on a square-free number of vertices (Lorenzini 2008).
- Incidence graph of Lines in finite Projective space (Brouwer-Ducey-S 2012).
- Erdös-Renyi Random graphs (Wood, 2014)

- Trees, $K(\Gamma) = \{0\}$.
- Complete graphs, $K(K_n) \cong (\mathbf{Z}/n\mathbf{Z})^{n-2}$.
- Wheel graphs W_n, $K(\Gamma) \cong (\mathbf{Z}/\ell_n)^2$, if n is odd (Biggs). Here ℓ_n is a *Lucas* number.
- Complete multipartite graphs (Jacobson, Niedermaier, Reiner 2003).
- Conference graphs on a square-free number of vertices (Lorenzini 2008).
- Incidence graph of Lines in finite Projective space (Brouwer-Ducey-S 2012).
- Erdös-Renyi Random graphs (Wood, 2014)
- Square Rook's graph and complement (Berget 1991, Ducey-Gerhard-Watson 2015)

- Trees, $K(\Gamma) = \{0\}$.
- Complete graphs, $K(K_n) \cong (\mathbf{Z}/n\mathbf{Z})^{n-2}$.
- Wheel graphs W_n, $K(\Gamma) \cong (\mathbf{Z}/\ell_n)^2$, if n is odd (Biggs). Here ℓ_n is a *Lucas* number.
- Complete multipartite graphs (Jacobson, Niedermaier, Reiner 2003).
- Conference graphs on a square-free number of vertices (Lorenzini 2008).
- Incidence graph of Lines in finite Projective space (Brouwer-Ducey-S 2012).
- Erdös-Renyi Random graphs (Wood, 2014)
- Square Rook's graph and complement (Berget 1991, Ducey-Gerhard-Watson 2015)
- Paley graphs (Chandler-S-Xiang 2015)

- Trees, $K(\Gamma) = \{0\}$.
- Complete graphs, $K(K_n) \cong (\mathbf{Z}/n\mathbf{Z})^{n-2}$.
- Wheel graphs W_n, $K(\Gamma) \cong (\mathbf{Z}/\ell_n)^2$, if n is odd (Biggs). Here ℓ_n is a *Lucas* number.
- Complete multipartite graphs (Jacobson, Niedermaier, Reiner 2003).
- Conference graphs on a square-free number of vertices (Lorenzini 2008).
- Incidence graph of Lines in finite Projective space (Brouwer-Ducey-S 2012).
- Erdös-Renyi Random graphs (Wood, 2014)
- Square Rook's graph and complement (Berget 1991, Ducey-Gerhard-Watson 2015)
- Paley graphs (Chandler-S-Xiang 2015)
- Peisert graphs (S. 2015)

Paley graphs $\mathrm{P}(q)$

Vertex set is $\mathbb{F}_q$, $q = p^t \equiv 1 \pmod 4$

Paley graphs $\mathrm{P}(q)$

Vertex set is $\mathbb{F}_q$, $q = p^t \equiv 1 \pmod 4$
$S =$ set of nonzero squares in $\mathbb{F}_q$

Paley graphs $\mathrm{P}(q)$

Vertex set is $\mathbb{F}_q$, $q = p^t \equiv 1 \pmod 4$

$S =$ set of nonzero squares in $\mathbb{F}_q$

Two vertices x and y are joined by an edge iff $x - y \in S$.

Paley graphs $\mathrm{P}(q)$

Vertex set is $\mathbb{F}_q$, $q = p^t \equiv 1 \pmod 4$

$S =$ set of nonzero squares in $\mathbb{F}_q$

Two vertices x and y are joined by an edge iff $x - y \in S$.

$\mathrm{P}(q)$ is a Cayley graph on $(\mathbb{F}_q, +)$ with connecting set S

Paley graphs are strongly regular graphs

$\mathrm{P}(q)$ is a *strongly regular graph*, self-complementary, with parameters $(v = q, k = \frac{(q-1)}{2}, \lambda = \frac{(q-5)}{4}, \mu = \frac{q-1}{4})$. Its eigenvalues are $k = \frac{q-1}{2}$, $r = \frac{-1+\sqrt{q}}{2}$ and $s = \frac{-1-\sqrt{q}}{2}$, with multiplicities 1, $\frac{q-1}{2}$ and $\frac{q-1}{2}$, respectively.

Automorphisms

$$\mathrm{Aut}(\mathrm{P}(q)) \geq \mathbb{F}_q \rtimes S.$$

Automorphisms

$$\mathrm{Aut}(\mathrm{P}(q)) \geq \mathbb{F}_q \rtimes S.$$

$$|K(\mathrm{P}(q))| = \frac{1}{q}\left(\frac{q+\sqrt{q}}{2}\right)^k \left(\frac{q-\sqrt{q}}{2}\right)^k = q^{\frac{q-3}{2}}\mu^k,$$

where $\mu = \frac{q-1}{4}$.

Automorphisms

$$\mathrm{Aut}(\mathrm{P}(q)) \geq \mathbb{F}_q \rtimes S.$$

$$|K(\mathrm{P}(q))| = \frac{1}{q}\left(\frac{q+\sqrt{q}}{2}\right)^k \left(\frac{q-\sqrt{q}}{2}\right)^k = q^{\frac{q-3}{2}}\mu^k,$$

where $\mu = \frac{q-1}{4}$.

$K(\mathrm{P}(q)) = K(\mathrm{P}(q))_p \oplus K(\mathrm{P}(q))_{p'}$

Automorphisms

$$\mathrm{Aut}(\mathrm{P}(q)) \geq \mathbb{F}_q \rtimes S.$$

$$|K(\mathrm{P}(q))| = \frac{1}{q}\left(\frac{q+\sqrt{q}}{2}\right)^k \left(\frac{q-\sqrt{q}}{2}\right)^k = q^{\frac{q-3}{2}}\mu^k,$$

where $\mu = \frac{q-1}{4}$.

$K(\mathrm{P}(q)) = K(\mathrm{P}(q))_p \oplus K(\mathrm{P}(q))_{p'}$

Use $\mathbb{F}_q$-action to help compute p'-part.

Automorphisms

$$\mathrm{Aut}(\mathrm{P}(q)) \geq \mathbb{F}_q \rtimes S.$$

$$|K(\mathrm{P}(q))| = \frac{1}{q}\left(\frac{q+\sqrt{q}}{2}\right)^k \left(\frac{q-\sqrt{q}}{2}\right)^k = q^{\frac{q-3}{2}}\mu^k,$$

where $\mu = \frac{q-1}{4}$.

$K(\mathrm{P}(q)) = K(\mathrm{P}(q))_p \oplus K(\mathrm{P}(q))_{p'}$

Use $\mathbb{F}_q$-action to help compute p'-part.

Use S-action to help compute p-part.

p'-part: Discrete Fourier Transform

Let X be the complex character table of $(\mathbb{F}_q, +)$

p'-part: Discrete Fourier Transform

Let X be the complex character table of $(\mathbb{F}_q, +)$

X is a matrix over $\mathbf{Z}[\zeta]$, ζ a complex primitive p-th root of unity.

p'-part: Discrete Fourier Transform

Let X be the complex character table of $(\mathbb{F}_q, +)$

X is a matrix over $\mathbf{Z}[\zeta]$, ζ a complex primitive p-th root of unity.

$\frac{1}{q} X \overline{X}^t = I$.

p'-part: Discrete Fourier Transform

Let X be the complex character table of $(\mathbb{F}_q, +)$

X is a matrix over $\mathbf{Z}[\zeta]$, ζ a complex primitive p-th root of unity.

$\frac{1}{q} X \overline{X}^t = I$.

(MacWilliams-Mann)

$$\frac{1}{q} X L \overline{X}^t = \mathrm{diag}(k - \psi(S))_\psi, \tag{1}$$

p'-part: Discrete Fourier Transform

Let X be the complex character table of $(\mathbb{F}_q, +)$

X is a matrix over $\mathbf{Z}[\zeta]$, ζ a complex primitive p-th root of unity.

$\frac{1}{q}X\overline{X}^t = I$.

(MacWilliams-Mann)

$$\frac{1}{q}XL\overline{X}^t = \mathrm{diag}(k - \psi(S))_\psi, \tag{1}$$

This equation can be viewed as matrix similarity, hence equivalence, over suitable local rings of integers.

Theorem

$K(\mathrm{P}(q))_{p'} \cong (\mathbf{Z}/\mu\mathbf{Z})^{2\mu}$, *where* $\mu = \frac{q-1}{4}$.

The p-part: $\mathbb{F}_q^\times$-action

$R = \mathbf{Z}_p[\xi_{q-1}]$, pR maximal ideal of R, $R/pR \cong \mathbb{F}_q$.

The p-part: $\mathbb{F}_q^\times$-action

$R = \mathbf{Z}_p[\xi_{q-1}]$, pR maximal ideal of R, $R/pR \cong \mathbb{F}_q$.

$T : \mathbb{F}_q^\times \to R^\times$, $\beta \mapsto \xi_{q-1}$, Teichmüller character.

The p-part: $\mathbb{F}_q^\times$-action

$R = \mathbf{Z}_p[\xi_{q-1}]$, pR maximal ideal of R, $R/pR \cong \mathbb{F}_q$.

$T : \mathbb{F}_q^\times \to R^\times$, $\beta \mapsto \xi_{q-1}$, Teichmüller character.

T generates the cyclic group $\mathrm{Hom}(\mathbb{F}_q^\times, R^\times)$.

The p-part: $\mathbb{F}_q^\times$-action

$R = \mathbf{Z}_p[\xi_{q-1}]$, pR maximal ideal of R, $R/pR \cong \mathbb{F}_q$.

$T : \mathbb{F}_q^\times \to R^\times$, $\beta \mapsto \xi_{q-1}$, Teichmüller character.

T generates the cyclic group $\mathrm{Hom}(\mathbb{F}_q^\times, R^\times)$.

Let $R^{\mathbb{F}_q}$ be the free R-module with basis indexed by the elements of $\mathbb{F}_q$; write the basis element corresponding to $x \in \mathbb{F}_q$ as $[x]$.

The p-part: $\mathbb{F}_q^\times$-action

$R = \mathbf{Z}_p[\xi_{q-1}]$, pR maximal ideal of R, $R/pR \cong \mathbb{F}_q$.

$T : \mathbb{F}_q^\times \to R^\times$, $\beta \mapsto \xi_{q-1}$, Teichmüller character.

T generates the cyclic group $\mathrm{Hom}(\mathbb{F}_q^\times, R^\times)$.

Let $R^{\mathbb{F}_q}$ be the free R-module with basis indexed by the elements of $\mathbb{F}_q$; write the basis element corresponding to $x \in \mathbb{F}_q$ as $[x]$.

$\mathbb{F}_q^\times$ acts on $R^{\mathbb{F}_q}$, permuting the basis by field multiplication,

The p-part: $\mathbb{F}_q^\times$-action

$R = \mathbf{Z}_p[\xi_{q-1}]$, pR maximal ideal of R, $R/pR \cong \mathbb{F}_q$.

$T : \mathbb{F}_q^\times \to R^\times$, $\beta \mapsto \xi_{q-1}$, Teichmüller character.

T generates the cyclic group $\mathrm{Hom}(\mathbb{F}_q^\times, R^\times)$.

Let $R^{\mathbb{F}_q}$ be the free R-module with basis indexed by the elements of $\mathbb{F}_q$; write the basis element corresponding to $x \in \mathbb{F}_q$ as $[x]$.

$\mathbb{F}_q^\times$ acts on $R^{\mathbb{F}_q}$, permuting the basis by field multiplication,

$R^{\mathbb{F}_q}$ decomposes as the direct sum $R[0] \oplus R^{\mathbb{F}_q^\times}$ of a trivial module with the regular module for $\mathbb{F}_q^\times$.

The p-part: $\mathbb{F}_q^\times$-action

$R = \mathbf{Z}_p[\xi_{q-1}]$, pR maximal ideal of R, $R/pR \cong \mathbb{F}_q$.

$T : \mathbb{F}_q^\times \to R^\times$, $\beta \mapsto \xi_{q-1}$, Teichmüller character.

T generates the cyclic group $\mathrm{Hom}(\mathbb{F}_q^\times, R^\times)$.

Let $R^{\mathbb{F}_q}$ be the free R-module with basis indexed by the elements of $\mathbb{F}_q$; write the basis element corresponding to $x \in \mathbb{F}_q$ as $[x]$.

$\mathbb{F}_q^\times$ acts on $R^{\mathbb{F}_q}$, permuting the basis by field multiplication,

$R^{\mathbb{F}_q}$ decomposes as the direct sum $R[0] \oplus R^{\mathbb{F}_q^\times}$ of a trivial module with the regular module for $\mathbb{F}_q^\times$.

$R^{\mathbb{F}_q^\times} = \oplus_{i=0}^{q-2} E_i$, E_i affording T^i.

The p-part: $\mathbb{F}_q^\times$-action

$R = \mathbf{Z}_p[\xi_{q-1}]$, pR maximal ideal of R, $R/pR \cong \mathbb{F}_q$.

$T : \mathbb{F}_q^\times \to R^\times$, $\beta \mapsto \xi_{q-1}$, Teichmüller character.

T generates the cyclic group $\mathrm{Hom}(\mathbb{F}_q^\times, R^\times)$.

Let $R^{\mathbb{F}_q}$ be the free R-module with basis indexed by the elements of $\mathbb{F}_q$; write the basis element corresponding to $x \in \mathbb{F}_q$ as $[x]$.

$\mathbb{F}_q^\times$ acts on $R^{\mathbb{F}_q}$, permuting the basis by field multiplication,

$R^{\mathbb{F}_q}$ decomposes as the direct sum $R[0] \oplus R^{\mathbb{F}_q^\times}$ of a trivial module with the regular module for $\mathbb{F}_q^\times$.

$R^{\mathbb{F}_q^\times} = \oplus_{i=0}^{q-2} E_i$, E_i affording T^i.

A basis element for E_i is

$$e_i = \sum_{x \in \mathbb{F}_q^\times} T^i(x^{-1})[x].$$

S-action

Consider action S on $R^{\mathbb{F}_q^\times}$. $T^i = T^{i+k}$ on S.

S-action

Consider action S on $R^{\mathbb{F}_q^\times}$. $T^i = T^{i+k}$ on S.

S-isotypic components on $R^{\mathbb{F}_q^\times}$ are each free R-modules of rank 2.

S-action

Consider action S on $R^{\mathbb{F}_q^\times}$. $T^i = T^{i+k}$ on S.

S-isotypic components on $R^{\mathbb{F}_q^\times}$ are each free R-modules of rank 2.

$\{e_i, e_{i+k}\}$ is basis of $M_i = E_i + E_{i+k}$

S-action

Consider action S on $R^{\mathbb{F}_q^\times}$. $T^i = T^{i+k}$ on S.

S-isotypic components on $R^{\mathbb{F}_q^\times}$ are each free R-modules of rank 2.

$\{e_i, e_{i+k}\}$ is basis of $M_i = E_i + E_{i+k}$

The S-fixed subspace M_0 has basis $\{\mathbf{1}, [0], e_k\}$.

S-action

Consider action S on $R^{\mathbb{F}_q^\times}$. $T^i = T^{i+k}$ on S.

S-isotypic components on $R^{\mathbb{F}_q^\times}$ are each free R-modules of rank 2.

$\{e_i, e_{i+k}\}$ is basis of $M_i = E_i + E_{i+k}$

The S-fixed subspace M_0 has basis $\{\mathbf{1}, [0], e_k\}$.

L is S-equivariant endomorphisms of $R^{\mathbb{F}_q}$,

$$L([x]) = k[x] - \sum_{s \in S} [x+s], \; x \in \mathbb{F}_q.$$

S-action

Consider action S on $R^{\mathbb{F}_q^\times}$. $T^i = T^{i+k}$ on S.

S-isotypic components on $R^{\mathbb{F}_q^\times}$ are each free R-modules of rank 2.

$\{e_i, e_{i+k}\}$ is basis of $M_i = E_i + E_{i+k}$

The S-fixed subspace M_0 has basis $\{\mathbf{1}, [0], e_k\}$.

L is S-equivariant endomorphisms of $R^{\mathbb{F}_q}$,

$$L([x]) = k[x] - \sum_{s\in S}[x+s],\ x \in \mathbb{F}_q.$$

L maps each M_i to itself.

$$L(e_i) = \sum_{x\in\mathbb{F}_q^\times} T^i(x^{-1})L([x]).$$

Jacobi Sums

The *Jacobi sum* of two nontrivial characters T^a and T^b is

$$J(T^a, T^b) = \sum_{x \in \mathbb{F}_q} T^a(x) T^b(1 - x).$$

Jacobi Sums

The *Jacobi sum* of two nontrivial characters T^a and T^b is

$$J(T^a, T^b) = \sum_{x \in \mathbb{F}_q} T^a(x) T^b(1-x).$$

Lemma

Suppose $0 \leq i \leq q-2$ *and* $i \neq 0, k$*. Then*

$$L(e_i) = \frac{1}{2}(qe_i - J(T^{-i}, T^k)e_{i+k})$$

Jacobi Sums

The *Jacobi sum* of two nontrivial characters T^a and T^b is

$$J(T^a, T^b) = \sum_{x \in \mathbb{F}_q} T^a(x) T^b(1-x).$$

Lemma

Suppose $0 \leq i \leq q-2$ *and* $i \neq 0, k$. *Then*

$$L(e_i) = \frac{1}{2}(qe_i - J(T^{-i}, T^k)e_{i+k})$$

Lemma

(i) $L(\mathbf{1}) = 0$.

(ii) $L(e_k) = \frac{1}{2}(\mathbf{1} - q([0] - e_k))$.

(iii) $L([0]) = \frac{1}{2}(q[0] - e_k - \mathbf{1})$.

Corollary

The Laplacian matrix L is equivalent over R to the diagonal matrix with diagonal entries $J(T^{-i}, T^k)$, for $i = 1, \ldots, q-2$ and $i \neq k$, two 1s and one zero.

Gauss and Jacobi sums

Gauss sums: If $1 \neq \chi \in \mathrm{Hom}(\mathbb{F}_q^\times, R^\times)$,

$$g(\chi) = \sum_{y \in \mathbb{F}_q^\times} \chi(y)\zeta^{\mathrm{tr}(y)},$$

where ζ is a primitive p-th root of unity in some extension of R.

Gauss and Jacobi sums

Gauss sums: If $1 \neq \chi \in \mathrm{Hom}(\mathbb{F}_q^\times, R^\times)$,

$$g(\chi) = \sum_{y \in \mathbb{F}_q^\times} \chi(y)\zeta^{\mathrm{tr}(y)},$$

where ζ is a primitive p-th root of unity in some extension of R.

Lemma

If χ and ψ are nontrivial multiplicative characters of $\mathbb{F}_q^\times$ such that $\chi\psi$ is also nontrivial, then

$$J(\chi, \psi) = \frac{g(\chi)g(\psi)}{g(\chi\psi)}.$$

Stickelberger's Congruence

Theorem

For $0 < a < q - 1$, write a p-adically as

$$a = a_0 + a_1 p + \cdots + a_{t-1} p^{t-1}.$$

Then the number of times that p divides $g(T^{-a})$ is $a_0 + a_1 + \cdots + a_{t-1}$.

Stickelberger's Congruence

Theorem

For $0 < a < q-1$*, write a p-adically as*

$$a = a_0 + a_1 p + \cdots + a_{t-1} p^{t-1}.$$

Then the number of times that p divides $g(T^{-a})$ *is* $a_0 + a_1 + \cdots + a_{t-1}$*.*

Corollary

Let $a, b \in \mathbf{Z}/(q-1)\mathbf{Z}$*, with* $a, b, a+b \not\equiv 0 \pmod{q-1}$*. Then number of times that p divides* $J(T^{-a}, T^{-b})$ *is equal to the number of carries in the addition* $a+b \pmod{q-1}$ *when a and b are written in p-digit form.*

The Counting Problem

$$k = \frac{1}{2}(q-1)$$

The Counting Problem

$k = \frac{1}{2}(q-1)$

What is the number of i, $1 \leq i \leq q-2$, $i \neq k$ such that adding i to $\frac{q-1}{2}$ modulo $q-1$ involves exactly λ carries?

The Counting Problem

$k = \frac{1}{2}(q-1)$

What is the number of i, $1 \leq i \leq q-2$, $i \neq k$ such that adding i to $\frac{q-1}{2}$ modulo $q-1$ involves exactly λ carries?

This problem can be solved by applying the *transfer matrix method*. (See Stanley's book.)

The Counting Problem

$k = \frac{1}{2}(q-1)$

What is the number of i, $1 \leq i \leq q-2$, $i \neq k$ such that adding i to $\frac{q-1}{2}$ modulo $q-1$ involves exactly λ carries?

This problem can be solved by applying the *transfer matrix method*. (See Stanley's book.)

Reformulate as a count of closed walks on a certain directed graph.

The Counting Problem

$k = \frac{1}{2}(q-1)$

What is the number of i, $1 \leq i \leq q-2$, $i \neq k$ such that adding i to $\frac{q-1}{2}$ modulo $q-1$ involves exactly λ carries?

This problem can be solved by applying the *transfer matrix method*. (See Stanley's book.)

Reformulate as a count of closed walks on a certain directed graph.

Transfer matrix method yields the generating function for our counting problem from the adjacency matrix of the digraph.

Theorem (CSX, 2015)

Let $q = p^t$ be a prime power congruent to 1 modulo 4. Then the number of p-adic elementary divisors of $L(\mathrm{P}(q))$ which are equal to p^λ, $0 \leq \lambda < t$, is

$$f(t,\lambda) = \sum_{i=0}^{\min\{\lambda, t-\lambda\}} \frac{t}{t-i}\binom{t-i}{i}\binom{t-2i}{\lambda-i}(-p)^i\left(\frac{p+1}{2}\right)^{t-2i}.$$

The number of p-adic elementary divisors of $L(\mathrm{P}(q))$ which are equal to p^t is $\left(\frac{p+1}{2}\right)^t - 2$.

Example: $K(\mathrm{P}(5^3))$

$$f(3,0) = 3^3 = 27,\ f(3,1) = \binom{3}{1} \cdot 3^3 - \tfrac{3}{2}\binom{2}{1}\binom{1}{0} \cdot 5 \cdot 3 = 36.$$

Example: $K(\mathrm{P}(5^3))$

$$f(3,0) = 3^3 = 27,\ f(3,1) = \binom{3}{1} \cdot 3^3 - \frac{3}{2}\binom{2}{1}\binom{1}{0} \cdot 5 \cdot 3 = 36.$$

$$K(\mathrm{P}(5^3)) \cong (\mathbf{Z}/31\mathbf{Z})^{62} \oplus (\mathbf{Z}/5\mathbf{Z})^{36} \oplus (\mathbf{Z}/25\mathbf{Z})^{36} \oplus (\mathbf{Z}/125\mathbf{Z})^{25}.$$

Example:$K(\mathrm{P}(5^4))$

$$f(4,0) = 3^4 = 81,\ f(4,1) = \binom{4}{1} \cdot 3^4 - \frac{4}{3}\binom{3}{1}\binom{2}{0} \cdot 5 \cdot 3^2 = 144,$$
$$f(4,2) = \binom{4}{2} \cdot 3^4 - \frac{4}{3}\binom{3}{1}\binom{2}{1} \cdot 5 \cdot 3^2 + \frac{4}{2}\binom{2}{2}\binom{0}{0} \cdot 5^2 = 176.$$

Example: $K(\mathrm{P}(5^4))$

$$f(4,0) = 3^4 = 81,\ f(4,1) = \binom{4}{1}\cdot 3^4 - \tfrac{4}{3}\binom{3}{1}\binom{2}{0}\cdot 5\cdot 3^2 = 144,$$
$$f(4,2) = \binom{4}{2}\cdot 3^4 - \tfrac{4}{3}\binom{3}{1}\binom{2}{1}\cdot 5\cdot 3^2 + \tfrac{4}{2}\binom{2}{2}\binom{0}{0}\cdot 5^2 = 176.$$

$$\begin{aligned} K(\mathrm{P}(5^4)) \cong (\mathbf{Z}/156\mathbf{Z})^{312} \oplus (\mathbf{Z}/5\mathbf{Z})^{144} \oplus (\mathbf{Z}/25\mathbf{Z})^{176} \\ \oplus (\mathbf{Z}/125\mathbf{Z})^{144} \oplus (\mathbf{Z}/625\mathbf{Z})^{79}. \end{aligned}$$

Peisert graphs $\mathrm{P}^*(q)$

Similar construction to Paley. $q = p^{2t}$, $p \equiv 3 \pmod 4$.

Peisert graphs $\mathrm{P}^*(q)$

Similar construction to Paley. $q = p^{2t}$, $p \equiv 3 \pmod 4$.
$\mathbb{F}_q{}^\times = \langle \beta \rangle$, $C = \langle \beta^4 \rangle$.

Peisert graphs $\mathrm{P}^*(q)$

Similar construction to Paley. $q = p^{2t}$, $p \equiv 3 \pmod 4$.
${\mathbb{F}_q}^\times = \langle \beta \rangle$, $C = \langle \beta^4 \rangle$.
$S' = C \cup \beta C$. Note $-1 \in C$.

Peisert graphs $\mathrm{P}^*(q)$

Similar construction to Paley. $q = p^{2t}$, $p \equiv 3 \pmod 4$.
${\mathbb{F}_q}^\times = \langle \beta \rangle$, $C = \langle \beta^4 \rangle$.
$S' = C \cup \beta C$. Note $-1 \in C$.
$\mathrm{P}^*(q)$ is a strongly regular graph , with same parameters as $\mathrm{P}(q)$.

Peisert graphs $\mathrm{P}^*(q)$

Similar construction to Paley. $q = p^{2t}$, $p \equiv 3 \pmod 4$.
${\mathbb{F}_q}^\times = \langle \beta \rangle$, $C = \langle \beta^4 \rangle$.
$S' = C \cup \beta C$. Note $-1 \in C$.
$\mathrm{P}^*(q)$ is a strongly regular graph , with same parameters as $\mathrm{P}(q)$.
Let A^* be the adjacency matrix, $L^* = kI - A^*$ the Laplacian.

Peisert graphs $\mathrm{P}^*(q)$

Similar construction to Paley. $q = p^{2t}$, $p \equiv 3 \pmod 4$.
${\mathbb{F}_q}^\times = \langle \beta \rangle$, $C = \langle \beta^4 \rangle$.
$S' = C \cup \beta C$. Note $-1 \in C$.
$\mathrm{P}^*(q)$ is a strongly regular graph , with same parameters as $\mathrm{P}(q)$.
Let A^* be the adjacency matrix, $L^* = kI - A^*$ the Laplacian.
By similar techniques we can compute the SNF of A^*, L^*.

Peisert graphs $\mathrm{P}^*(q)$

Similar construction to Paley. $q = p^{2t}$, $p \equiv 3 \pmod 4$.
${\mathbb{F}_q}^\times = \langle \beta \rangle$, $C = \langle \beta^4 \rangle$.
$S' = C \cup \beta C$. Note $-1 \in C$.
$\mathrm{P}^*(q)$ is a strongly regular graph , with same parameters as $\mathrm{P}(q)$.
Let A^* be the adjacency matrix, $L^* = kI - A^*$ the Laplacian.
By similar techniques we can compute the SNF of A^*, L^*.
When $q = p^2$, A and A^* have same SNF, so do L and L^*.

Peisert graphs $\mathrm{P}^*(q)$

Similar construction to Paley. $q = p^{2t}$, $p \equiv 3 \pmod 4$.
${\mathbb{F}_q}^\times = \langle\beta\rangle$, $C = \langle\beta^4\rangle$.
$S' = C \cup \beta C$. Note $-1 \in C$.
$\mathrm{P}^*(q)$ is a strongly regular graph , with same parameters as $\mathrm{P}(q)$.
Let A^* be the adjacency matrix, $L^* = kI - A^*$ the Laplacian.
By similar techniques we can compute the SNF of A^*, L^*.
When $q = p^2$, A and A^* have same SNF, so do L and L^*.
In fact more is true.

Peisert graphs $\mathrm{P}^*(q)$

Similar construction to Paley. $q = p^{2t}$, $p \equiv 3 \pmod 4$.
$\mathbb{F}_q{}^{\times} = \langle \beta \rangle$, $C = \langle \beta^4 \rangle$.
$S' = C \cup \beta C$. Note $-1 \in C$.
$\mathrm{P}^*(q)$ is a strongly regular graph , with same parameters as $\mathrm{P}(q)$.
Let A^* be the adjacency matrix, $L^* = kI - A^*$ the Laplacian.
By similar techniques we can compute the SNF of A^*, L^*.
When $q = p^2$, A and A^* have same SNF, so do L and L^*.
In fact more is true.

Theorem

Assume $q = p^2$

(a) *There is a number field K such that A and A^* are similar as matrices over $\mathcal{O}_K$. (Uses local-global principle for similarity of matrices (Guralnick).)*

(b) *For all $c \in \mathbf{Z}$, the matrices $A + cI$ and $A^* + cI$ have the same SNF.*

Thank you for your attention!