The Smith and critical groups of a graph

Qing Xiang
Department of Mathematical Sciences
University of Delaware
Newark, DE 19716

The 8th Shanghai Conference on Combinatorics
May 26, 2014
Critical groups of graphs

Outline

Laplacian matrix of a graph

Smith normal form

Some families of graphs with known critical groups

Paley graphs

Smith group of Paley graphs

Critical group of Paley 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 several contexts;

- in physics: the Abelian Sandpile model (Bak-Tang-Wiesenfeld, Dhar);
- its combinatorial variant: the Chip-firing game (Björner-Lovasz-Shor, Biggs);
- in arithmetic geometry: Picard group, graph Jacobian (Lorenzini).

We'll consider the problem of computing the critical group for families of graphs.

The Paley graphs are a very important class of strongly regular graphs arising from finite fields.

We'll say something about the computation of their critical groups, which involves groups, characters and number theory.
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 several contexts;

- in physics: the *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 several contexts;

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

- in physics: the *Abelian Sandpile model* (Bak-Tang-Wiesenfeld, Dhar);
- its combinatorial variant: the *Chip-firing game* (Björner-Lovasz-Shor, Biggs);
- in arithmetic geometry: Picard group, graph Jacobian (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 several contexts;

- in physics: the Abelian Sandpile model (Bak-Tang-Wiesenfeld, Dhar);
- its combinatorial variant: the Chip-firing game (Björner-Lovasz-Shor, Biggs);
- in arithmetic geometry: Picard group, graph Jacobian (Lorenzini).

We’ll consider the problem of computing the critical group for families of graphs.
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 several contexts:

- in physics: the *Abelian Sandpile model* (Bak-Tang-Wiesenfeld, Dhar);
- its combinatorial variant: the *Chip-firing game* (Björner-Lovasz-Shor, Biggs);
- in arithmetic geometry: Picard group, graph Jacobian (Lorenzini).

We’ll consider the problem of computing the critical group for families of graphs.

The Paley graphs are a very important class of strongly regular graphs arising from finite fields.
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 several contexts;

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

its combinatorial variant: the Chip-firing game (Björner-Lovasz-Shor, Biggs);

in arithmetic geometry: Picard group, graph Jacobian (Lorenzini).

We’ll consider the problem of computing the critical group for families of graphs.

The Paley graphs are a very important class of strongly regular graphs arising from finite fields.

We’ll say something about the computation of their critical groups, which involves groups, characters and number theory.
Critical groups of graphs

Outline

Laplacian matrix of a graph

Smith normal form

Some families of graphs with known critical groups

Paley graphs

Smith group of Paley graphs

Critical group of Paley graphs
\( \Gamma = (V, E) \) simple, connected graph.
\( \Gamma = (V, E) \) simple, connected graph.

\( L = D - A, A \) adjacency matrix, \( D = \text{diag}(d_1, d_2, \ldots, d_v) \): degree matrix.
- $\Gamma = (V, E)$ simple, connected graph.
- $L = D - A$, $A$ adjacency matrix, $D = \text{diag}(d_1, d_2, \ldots, d_v)$: degree matrix.
- Think of both $A$ and $L$ as linear maps $\mathbb{Z}^V \rightarrow \mathbb{Z}^V$. 
- $\Gamma = (V, E)$ simple, connected graph.
- $L = D - A$, $A$ adjacency matrix, $D = \text{diag}(d_1, d_2, \ldots, d_v)$: degree matrix.
- Think of both $A$ and $L$ as linear maps $\mathbb{Z}^V \to \mathbb{Z}^V$.
- $\text{rank}(L) = |V| - 1$ (the smallest eigenvalue of $L$ is 0).
Smith group and Critical group

\[ \mathbb{Z}^V / \text{Im}(A) := S(\Gamma) \text{ the } Smith \text{ group of } \Gamma. \]
Smith group and Critical group

- $\mathbb{Z}^V / \text{Im}(A) := S(\Gamma)$ the *Smith group* of $\Gamma$.
- $\mathbb{Z}^V / \text{Im}(L) \cong \mathbb{Z} \oplus K(\Gamma)$
Smith group and Critical group

- \( \mathbb{Z}^V / \text{Im}(A) := S(\Gamma) \) the *Smith group* of \( \Gamma \).
- \( \mathbb{Z}^V / \text{Im}(L) \cong \mathbb{Z} \oplus K(\Gamma) \)
- The finite group \( K(\Gamma) \) is called the *critical group* of \( \Gamma \).
Kirchhoff’s Matrix Tree Theorem

For any connected graph $\Gamma$, the number of spanning trees is equal to $\det(\tilde{L})$, where $\tilde{L}$ is obtained from $L$ by deleting the row and column corresponding to any chosen vertex.
Kirchhoff’s Matrix-Tree Theorem

For any connected graph \( \Gamma \), the number of spanning trees is equal to \( \det(\tilde{L}) \), where \( \tilde{L} \) is obtained from \( L \) by deleting the row and column corresponding to any chosen vertex.

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

Outline

Laplacian matrix of a graph

Smith normal form

Some families of graphs with known critical groups

Paley graphs

Smith group of Paley graphs

Critical group of Paley graphs
Equivalence and Smith normal form

Given an integer matrix $X$, there exist unimodular integer matrices $P$ and $Q$ such that

$$PXQ = \begin{pmatrix} Y & 0 \\ 0 & 0 \end{pmatrix}, \quad Y = \text{diag}(s_1, s_2, \ldots s_r), \quad s_1 | s_2 | \cdots | s_r.$$
Critical groups of graphs

Outline

Laplacian matrix of a graph

Smith normal form

Some families of graphs with known critical groups

Paley graphs

Smith group of Paley graphs

Critical group of Paley graphs
- Trees, $K(\Gamma) = \{0\}$. 
Trees, $K(\Gamma) = \{0\}$.

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

Outline

Laplacian matrix of a graph

Smith normal form

Some families of graphs with known critical groups

Paley graphs

Smith group of Paley graphs

Critical group of Paley graphs
Paley graphs $P(q)$

- Vertex set is $\mathbb{F}_q$, $q = p^t \equiv 1 \pmod{4}$
Paley graphs $P(q)$

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

- 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 are Cayley graphs

We can view $P(q)$ as a Cayley graph on $(\mathbb{F}_q, +)$ with connecting set $S$
Paley graphs are strongly regular graphs

It is well known and easily checked that $P(q)$ is a strongly regular graph and that 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.
Critical groups of graphs

Outline

Laplacian matrix of a graph

Smith normal form

Some families of graphs with known critical groups

Paley graphs

Smith group of Paley graphs

Critical group of Paley graphs
\[ |S(P(q))| = k(k/2)^k, \text{ so } \gcd(|S(P(q))|, q) = 1. \]
\[ |S(P(q))| = k(k/2)^k, \text{ so } \gcd(|S(P(q))|, q) = 1. \]

\[ X, \text{ complex character table of } (\mathbb{F}_q, +) \]
\[ |S(P(q))| = k(k/2)^k, \text{ so } \gcd(|S(P(q))|, q) = 1. \]

- \( X \), complex character table of \((\mathbb{F}_q, +)\)
- \( X \) is a matrix over \( \mathbb{Z}[\zeta] \), \( \zeta \) a complex primitive \( p \)-th root of unity.
\[ |S(P(q))| = k(k/2)^k, \text{ so } \gcd(|S(P(q))|, q) = 1. \]

- \( X \), complex character table of \( (\mathbb{F}_q, +) \)
- \( X \) is a matrix over \( \mathbb{Z}[\zeta] \), \( \zeta \) a complex primitive \( p \)-th root of unity.
- \( \frac{1}{q}XX^t = I \).
\[ |S(P(q))| = k(k/2)^k, \text{ so } \gcd(|S(P(q))|, q) = 1. \]

1. \(X\), complex character table of \((\mathbb{F}_q, +)\)

2. \(X\) is a matrix over \(\mathbb{Z}[\zeta]\), \(\zeta\) a complex primitive \(p\)-th root of unity.

3. \(\frac{1}{q}X \overline{X}^t = I.\)

4. 

\[
\frac{1}{q}X \overline{X}^t = \text{diag}(\psi(S))_\psi, \tag{1}
\]

where \(\psi\) runs through the additive characters of \(\mathbb{F}_q\).
Theorem
$S(P(q)) \cong \mathbb{Z}/2\mu \mathbb{Z} \oplus (\mathbb{Z}/\mu \mathbb{Z})^{2\mu}$, where $\mu = \frac{q-1}{4}$.

Remark
This theorem was conjectured by Joe Rushanan in his Caltech PhD thesis (1988).
Critical groups of graphs

Outline

Laplacian matrix of a graph

Smith normal form

Some families of graphs with known critical groups

Paley graphs

Smith group of Paley graphs

Critical group of Paley graphs
Symmetries

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

where \( \mu = \frac{q-1}{4} \).
Symmetries

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

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

\[ \text{Aut}(P(q)) \supseteq \mathbb{F}_q \rtimes S. \]
Symmetries

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

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

\[ \text{Aut}(P(q)) \geq \mathbb{F}_q \rtimes S. \]

\[ K(P(q)) = K(P(q))_p \oplus K(P(q))_{p'} \]
Symmetries

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

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

- \( \text{Aut}(P(q)) \geq \mathbb{F}_q \rtimes S \).
- \( K(P(q)) = K(P(q))_p \oplus K(P(q))_{p'} \).
- Use \( \mathbb{F}_q \)-action to help compute \( p' \)-part.
Symmetries

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

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

\[ Aut(P(q)) \geq \mathbb{F}_q \rtimes S. \]

\[ K(P(q)) = K(P(q))_p \oplus K(P(q))_{p'} \]

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

Use \( S \)-action to help compute \( p \)-part.
$p'$-part

- $X$, complex character table of $(\mathbb{F}_q, +)$
$p'$-part

- $X$, complex character table of $(\mathbb{F}_q, +)$
- $X$ is a matrix over $\mathbb{Z}[\zeta]$, $\zeta$ a complex primitive $p$-th root of unity.
$p'$-part

- $X$, complex character table of $(\mathbb{F}_q, +)$
- $X$ is a matrix over $\mathbb{Z}[\zeta]$, $\zeta$ a complex primitive $p$-th root of unity.
- $\frac{1}{q} X \overline{X}^t = I$. 
\( p' \)-part

- \( X \), complex character table of \((\mathbb{F}_q, +)\)
- \( X \) is a matrix over \( \mathbb{Z}[\zeta] \), \( \zeta \) a complex primitive \( p \)-th root of unity.
- \( \frac{1}{q}X \overline{X}^t = I \).
- \[
    \frac{1}{q}X L \overline{X}^t = \text{diag}(k - \psi(S))_\psi,
\] (2)
$p'$-part

- $X$, complex character table of $(\mathbb{F}_q, +)$
- $X$ is a matrix over $\mathbb{Z}[\zeta]$, $\zeta$ a complex primitive $p$-th root of unity.
- $\frac{1}{q} X \overline{X}^t = I$.

\[ \frac{1}{q} X L \overline{X}^t = \text{diag}(k - \psi(S))_{\psi} \]  

(2)

- Interpret this as $PLQ$-equivalence over suitable local rings of integers.
Theorem
\[ K(P(q))_{p'} \cong (\mathbb{Z}/\mu\mathbb{Z})^{2\mu}, \text{ where } \mu = \frac{q-1}{4}. \]
The \( p \)-part
$\mathbb{F}_q^\times$-action

$R = \mathbb{Z}_p[\xi_{q-1}]$, $\mathfrak{p}R$ maximal ideal of $R$, $R/\mathfrak{p}R \cong \mathbb{F}_q$. 
$F_q^\times$-action

- $R = \mathbb{Z}_p[\xi_{q-1}]$, $pR$ maximal ideal of $R$, $R/pR \cong F_q$.
- $T : F_q^\times \rightarrow R^\times$ Teichmüller character.
\( \mathbb{F}_q^\times \) -action

- \( R = \mathbb{Z}_p[\xi_{q-1}] \), \( \mathfrak{p}R \) maximal ideal of \( R \), \( R/\mathfrak{p}R \cong \mathbb{F}_q \).
- \( T : \mathbb{F}_q^\times \to R^\times \) Teichmüller character.
- \( T \) generates the cyclic group \( \text{Hom}(\mathbb{F}_q^\times, R^\times) \).
$\mathbb{F}_q^\times$-action

- $R = \mathbb{Z}_p[\xi_{q-1}]$, $\mathfrak{p}R$ maximal ideal of $R$, $R/\mathfrak{p}R \cong \mathbb{F}_q$.
- $T : \mathbb{F}_q^\times \rightarrow R^\times$ Teichmüller character.
- $T$ generates the cyclic group $\text{Hom}(\mathbb{F}_q^\times, R^\times)$.
- 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 $[x]$. 
$\mathbb{F}_q^\times$-action

- $R = \mathbb{Z}_p[\xi_{q-1}]$, $pR$ maximal ideal of $R$, $R/pR \cong \mathbb{F}_q$.
- $T : \mathbb{F}_q^\times \to R^\times$ Teichmüller character.
- $T$ generates the cyclic group $\text{Hom}(\mathbb{F}_q^\times, R^\times)$.
- 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,
$\mathbb{F}_q^\times$-action

- $R = \mathbb{Z}_p[\xi_{q-1}]$, $\mathfrak{p}R$ maximal ideal of $R$, $R/\mathfrak{p}R \cong \mathbb{F}_q$.
- $T : \mathbb{F}_q^\times \rightarrow R^\times$ Teichmüller character.
- $T$ generates the cyclic group $\text{Hom}(\mathbb{F}_q^\times, R^\times)$.
- 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 $\mathbb{F}_q^\times$. 
$F_q^\times$-action

- $R = \mathbb{Z}_p[\xi_{q-1}], \mathfrak{p}R$ maximal ideal of $R$, $R/\mathfrak{p}R \cong F_q$.
- $T : F_q^\times \to R^\times$ Teichmüller character.
- $T$ generates the cyclic group $\text{Hom}(F_q^\times, R^\times)$.
- Let $R_{F_q}$ be the free $R$-module with basis indexed by the elements of $F_q$; write the basis element corresponding to $x \in F_q$ as $[x]$.
- $F_q^\times$ acts on $R_{F_q}$, permuting the basis by field multiplication,
- $R_{F_q}$ decomposes as the direct sum $R[0] \oplus R_{F_q}^{\times}$ of a trivial module with the regular module for $F_q^\times$.
- $R_{F_q}^{\times} = \bigoplus_{i=0}^{q-2} E_i$, $E_i$ affording $T^i$. 
\(F_q^\times\)-action

- \(R = \mathbb{Z}_p[\xi_{q-1}], \) \(pR\) maximal ideal of \(R, \) \(R/pR \cong \mathbb{F}_q.\)
- \(T : F_q^\times \rightarrow R^\times\) Teichmüller character.
- \(T\) generates the cyclic group \(\text{Hom}(F_q^\times, R^\times)\).
- Let \(R^{F_q}\) be the free \(R\)-module with basis indexed by the elements of \(F_q;\) write the basis element corresponding to \(x \in F_q\) as \([x]\).
- \(F_q^\times\) acts on \(R^{F_q}\), permuting the basis by field multiplication,
- \(R^{F_q}\) decomposes as the direct sum \(R[0] \oplus R^{F_q^\times}\) of a trivial module with the regular module for \(F_q^\times\).
- \(R^{F_q^\times} = \bigoplus_{i=0}^{q-2} E_i, E_i\) affording \(T^i.\)
- A basis element for \(E_i\) is

\[e_i = \sum_{x \in F_q^\times} T^i(x^{-1})[x].\]
Consider action $S$ on $R^\times_{F_q}$. $T^i = T^{i+k}$ on $S$. 
Consider action $S$ on $R^{\mathbb{F}_q}$: $T^i = T^{i+k}$ on $S$.

$S$-isotypic components on $R^{\mathbb{F}_q}$ are each 2-dimensional.
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 2-dimensional.
- $\{e_i, e_{i+k}\}$ is basis of $M_i = E_i + E_{i+k}$
Consider action $S$ on $R_{F q}$. $T_i = T^{i+k}$ on $S$.

- $S$-isotypic components on $R_{F q}$ are each 2-dimensional.
- $\{e_i, e_{i+k}\}$ is basis of $M_i = E_i + E_{i+k}$
- The $S$-fixed subspace $M_0$ has basis $\{1, [0], e_k\}$. 

$L$ is $S$-equivariant endomorphisms of $R_{F q}$, $L([x]) = k[x] - \sum_{s \in S} [x + s]$, $x \in F_q$. $L$ maps each $M_i$ to itself.
Consider action $S$ on $\mathbb{F}_q^\times$. $T^i = T^{i+k}$ on $S$.

- $S$-isotypic components on $\mathbb{F}_q^\times$ are each 2-dimensional.
- $\{e_i, e_{i+k}\}$ is basis of $M_i = E_i + E_{i+k}$
- The $S$-fixed subspace $M_0$ has basis $\{1, [0], e_k\}$.
- $L$ is $S$-equivariant endomorphisms of $\mathbb{F}_q^\times$,

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

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

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

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

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

- $L$ maps each $M_i$ to itself.
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) $L(1) = 0$.
(ii) $L(e_k) = \frac{1}{2} (1 - q([0] - e_k))$.
(iii) $L([0]) = \frac{1}{2} (q[0] - e_k - 1)$. 

Corollary

The Laplacian matrix $L$ is equivalent over $\mathbb{R}$ 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

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

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

where $\zeta$ is a primitive $p$-th root of unity in some extension of $R$. 
Gauss and Jacobi

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

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

where $\zeta$ is a primitive $p$-th root of unity in some extension of $R$.

Lemma

If $\chi$ and $\psi$ 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 Theorem

**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 Theorem

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

$$a = a_0 + a_1p + \cdots + a_{t-1}p^{t-1}.$$  

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

Theorem
Let $a, b \in \mathbb{Z}/(q - 1)\mathbb{Z}$, with $a, b, a + b \not\equiv 0 \pmod{q - 1}$. Then the 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 \( \lambda \) 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 \( \lambda \) carries?
- This problem can be solved by applying the transfer matrix method.
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 \( \lambda \) carries?
- This problem can be solved by applying the \textit{transfer matrix method}.
- 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 $\lambda$ carries?

- This problem can be solved by applying the transfer matrix method.

- 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

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

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

The number of $p$-adic elementary divisors of $L(P(q))$ which are equal to $p^t$ is $\left(\frac{p+1}{2}\right)^t - 2$. 
Example: $K(P(5^3))$

- $f(3, 0) = 3^3 = 27$
Example: $K(P(5^3))$

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

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

$$K(P(5^3)) \cong (\mathbb{Z}/31\mathbb{Z})^6 \oplus (\mathbb{Z}/5\mathbb{Z})^{36} \oplus (\mathbb{Z}/25\mathbb{Z})^{36} \oplus (\mathbb{Z}/125\mathbb{Z})^{25}.$$
Example: $K(P(5^4))$

- $f(4, 0) = 3^4 = 81$. 
Example: $K(P(5^4))$

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

Example: $K(P(5^4))$

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

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

$K(P(5^4)) \cong (\mathbb{Z}/156\mathbb{Z})^{312} \oplus (\mathbb{Z}/5\mathbb{Z})^{144} \oplus (\mathbb{Z}/25\mathbb{Z})^{176} \oplus (\mathbb{Z}/125\mathbb{Z})^{144} \oplus (\mathbb{Z}/625\mathbb{Z})^{79}.$
Thank you for your attention!