The critical group of a graph

Peter Sin

Millican Colloquium, UNT, March 24th, 2014.

- 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;

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

Pierre-Simon Laplace (1749-1827)

- $\Gamma = (V, E)$ simple, connected graph.

- $\Gamma = (V, E)$ simple, connected graph.
- $L = D - A$, A adjacency matrix, D degree matrix.

- $\Gamma = (V, E)$ simple, connected graph.
- $L = D - A$, A adjacency matrix, D degree matrix.
- Think of L as a linear map $L : \mathbf{Z}^V \to \mathbf{Z}^V$.

- $\Gamma = (V, E)$ simple, connected graph.
- $L = D - A$, A adjacency matrix, D degree matrix.
- Think of L as a linear map $L : \mathbf{Z}^V \to \mathbf{Z}^V$.
- $\mathrm{rank}(L) = |V| - 1$.

Critical group

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

Critical group

- $\mathbf{Z}^V / \operatorname{Im}(L) \cong \mathbf{Z} \oplus K(\Gamma)$
- The finite group $K(\Gamma)$ is called the critical group of Γ.

Critical group

- $\mathbf{Z}^V / \operatorname{Im}(L) \cong \mathbf{Z} \oplus K(\Gamma)$
- The finite group $K(\Gamma)$ is called the critical group of Γ.
- Let $\varepsilon : \mathbf{Z}^V \to \mathbf{Z}$, $\sum_{v \in V} a_v v \mapsto \sum_{v \in V} a_v$.

Critical group

- $\mathbf{Z}^V / \mathrm{Im}(L) \cong \mathbf{Z} \oplus K(\Gamma)$
- The finite group $K(\Gamma)$ is called the critical group of Γ.
- Let $\varepsilon : \mathbf{Z}^V \to \mathbf{Z}$, $\sum_{v \in V} a_v v \mapsto \sum_{v \in V} a_v$.
- $L(\ker(\varepsilon)) \subseteq \ker(\varepsilon)$, and $K(\Gamma) \cong \mathrm{Ker}(\varepsilon)/L(\mathrm{Ker}(\varepsilon))$

Kirchhoff's Matrix-Tree Theorem

Gustav Kirchhoff (1824-1887)

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

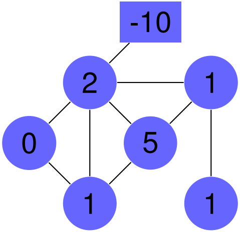
Gustav Kirchhoff (1824-1887)

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.*

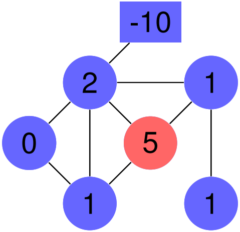
Also, $\det(\tilde{L}) = |K(\Gamma)| = \frac{1}{|V|}\prod_{j=2}^{|V|}\lambda_j$.

Rules



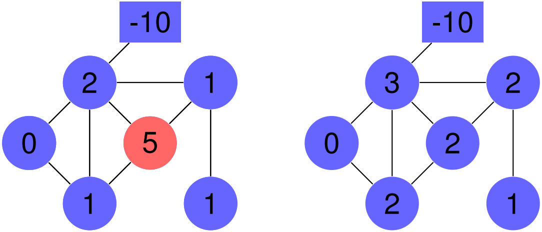
- A configuration is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.

Rules



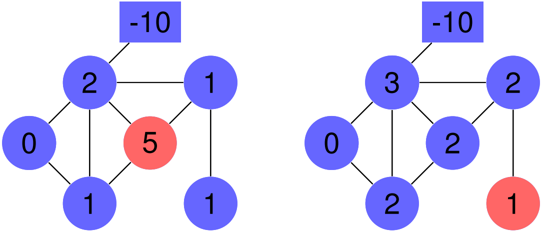
- A configuration is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.
- A round vertex v can be fired if it has at least $\deg(v)$ chips.

Rules



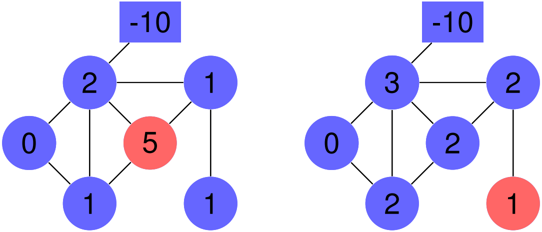
- A configuration is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.
- A round vertex v can be fired if it has at least $\deg(v)$ chips.

Rules



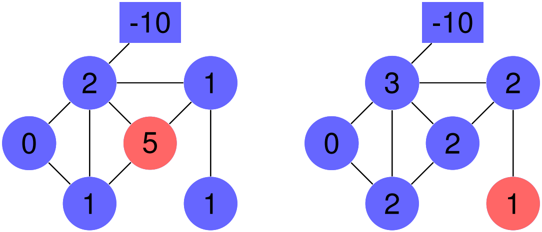
- A configuration is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.
- A round vertex v can be fired if it has at least $\deg(v)$ chips.

Rules



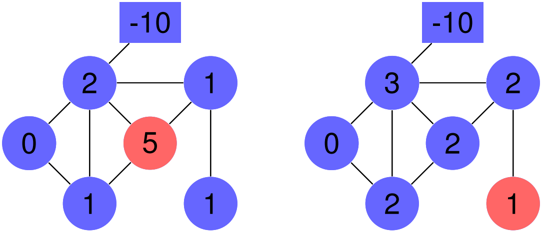
- A configuration is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.
- A round vertex v can be fired if it has at least $\deg(v)$ chips.
- The square vertex is fired only when no others can be fired.

Rules



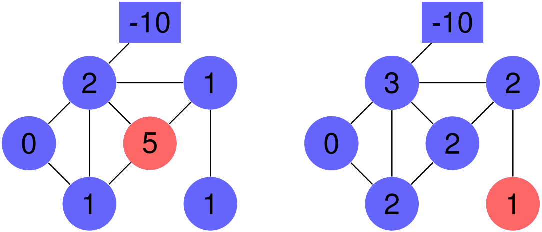
- A configuration is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.
- A round vertex v can be fired if it has at least $\deg(v)$ chips.
- The square vertex is fired only when no others can be fired.
- A configuration is *stable* if no round vertex can be fired.

Rules



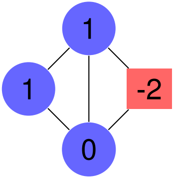
- A configuration is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.
- A round vertex v can be fired if it has at least $\deg(v)$ chips.
- The square vertex is fired only when no others can be fired.
- A configuration is *stable* if no round vertex can be fired.
- A configuration is *recurrent* if there is a sequence of firings that lead to the same configuration.

Rules

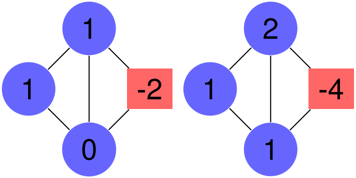


- A configuration is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.
- A round vertex v can be fired if it has at least $\deg(v)$ chips.
- The square vertex is fired only when no others can be fired.
- A configuration is *stable* if no round 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.

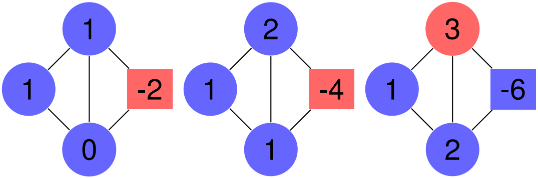
Sample game 1



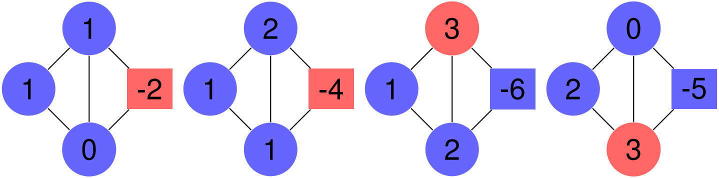
Sample game 1



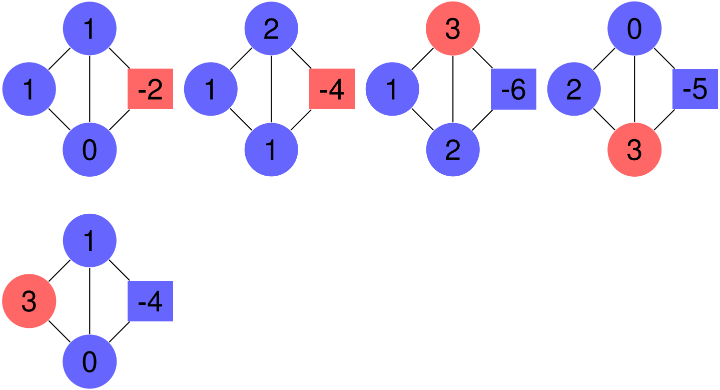
Sample game 1



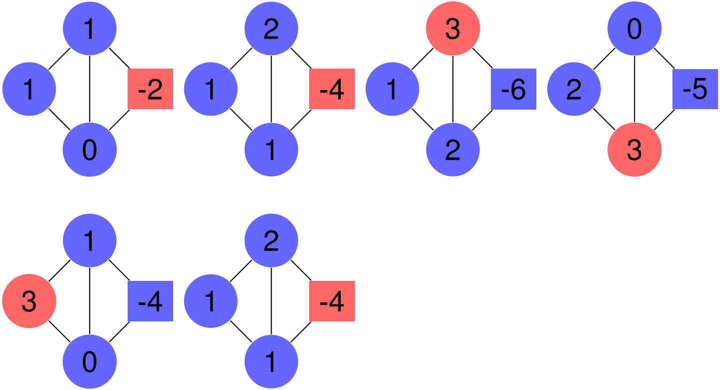
Sample game 1



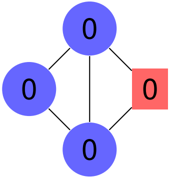
Sample game 1



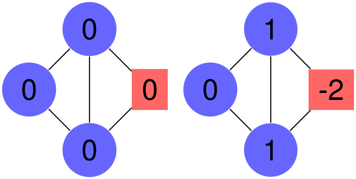
Sample game 1



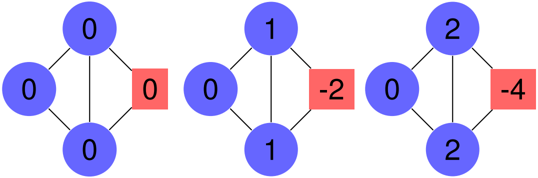
Sample game 2



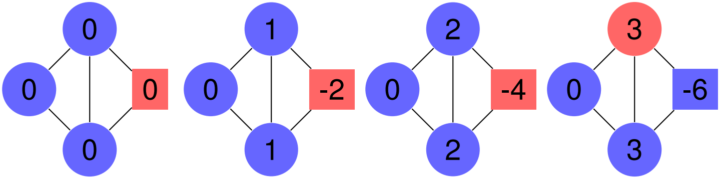
Sample game 2



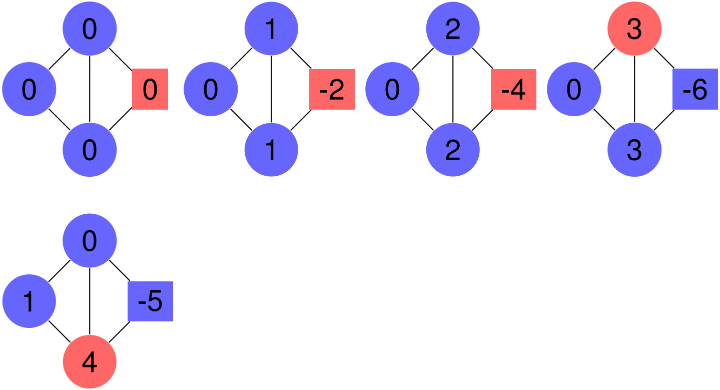
Sample game 2



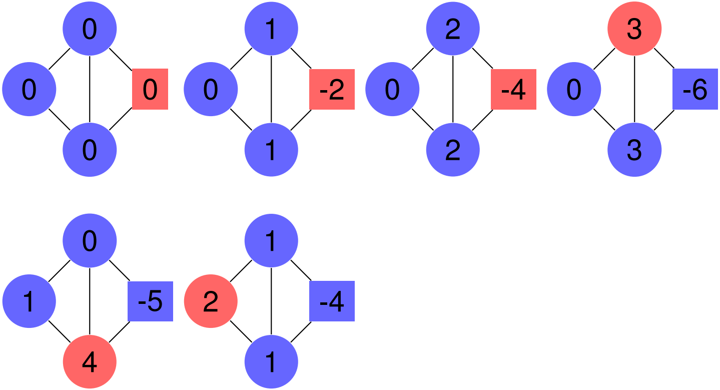
Sample game 2



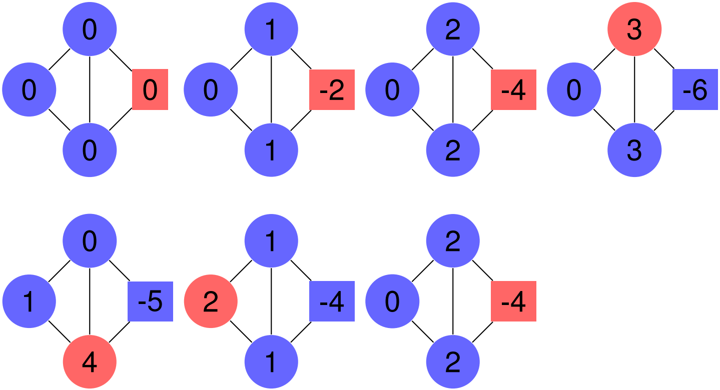
Sample game 2



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

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

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

Theorem

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

Theorem

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

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

Equivalence and Smith normal form

Henry John Stephen Smith (1826-1883)

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

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

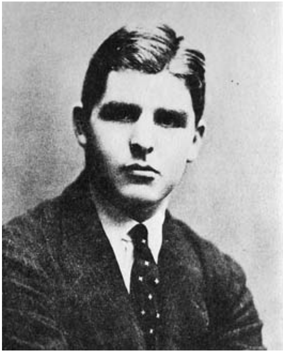
- Trees, $K(\Gamma) = \{0\}$.

- 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).

- 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).
- Conference graphs on a square-free number of vertices (Lorenzini).



Raymond E. A. C. Paley (1907-33)

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

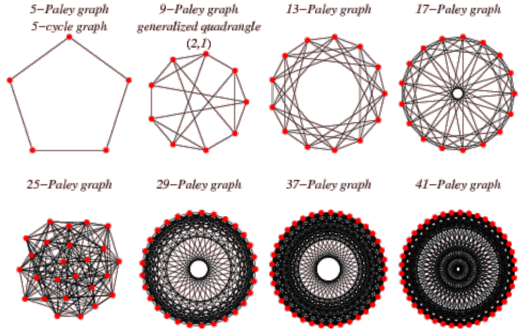
- Vertex set is $\mathbb{F}_q$, $q = p^t \equiv 1 \pmod 4$

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 $\mathrm{P}(q)$

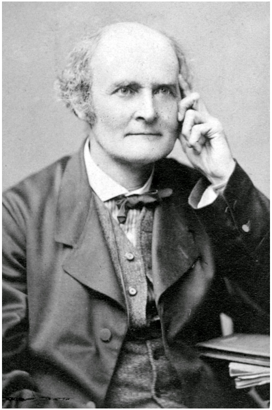
- Vertex set is $\mathbb{F}_q$, $q = p^t \equiv 1 \pmod 4$
- $S =$ set of nonzero squares in $\mathbb{F}_q$
- two vertices x and y are joined by an edge iff $x - y \in S$.



Some Paley graphs (from Wolfram Mathworld)

Paley graphs are Cayley graphs

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



Arthur Cayley (1821-95)

Paley graphs are strongly regular graphs

It is well known and easily checked that $\mathrm{P}(q)$ 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.

David Chandler and Qing Xiang

Symmetries

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

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

Symmetries

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

  where $\mu = \frac{q-1}{4}$.
- $\mathrm{Aut}(\mathrm{P}(q)) \geq \mathbb{F}_q \rtimes S$.

Symmetries

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

  where $\mu = \frac{q-1}{4}$.
- $\mathrm{Aut}(\mathrm{P}(q)) \geq \mathbb{F}_q \rtimes S$.
- $K(\mathrm{P}(q)) = K(\mathrm{P}(q))_p \oplus K(\mathrm{P}(q))_{p'}$

Symmetries

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

  where $\mu = \frac{q-1}{4}$.
- $\mathrm{Aut}(\mathrm{P}(q)) \geq \mathbb{F}_q \rtimes S$.
- $K(\mathrm{P}(q)) = K(\mathrm{P}(q))_p \oplus K(\mathrm{P}(q))_{p'}$
- Use $\mathbb{F}_q$-action to help compute p'-part.

Symmetries

- $$|K(\mathrm{P}(q))| = \frac{1}{q}\left(\frac{q+\sqrt{q}}{2}\right)^k\left(\frac{q-\sqrt{q}}{2}\right)^k = q^{\frac{q-3}{2}}\mu^k,$$
  where $\mu = \frac{q-1}{4}$.
- $\mathrm{Aut}(\mathrm{P}(q)) \geq \mathbb{F}_q \rtimes S$.
- $K(\mathrm{P}(q)) = K(\mathrm{P}(q))_p \oplus K(\mathrm{P}(q))_{p'}$
- Use $\mathbb{F}_q$-action to help compute p'-part.
- Use S-action to help compute p-part.

p'-part

Joseph Fourier (1768-1830)

Discrete Fourier Transform

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

Discrete Fourier Transform

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

Discrete Fourier Transform

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

Discrete Fourier Transform

- X, complex character table of $(\mathbb{F}_q, +)$
- X is a matrix over $\mathbf{Z}[\zeta]$, ζ a complex primitive p-th root of unity.
- $\frac{1}{q}X\overline{X}^t = I$.
- $$\frac{1}{q}XL\overline{X}^t = \mathrm{diag}(k - \psi(S))_\psi, \tag{1}$$

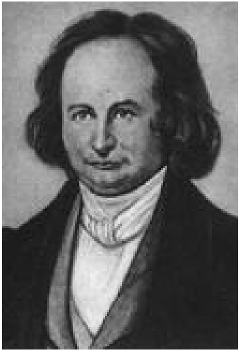
Discrete Fourier Transform

- X, complex character table of $(\mathbb{F}_q, +)$
- X is a matrix over $\mathbf{Z}[\zeta]$, ζ a complex primitive p-th root of unity.
- $\frac{1}{q} X \overline{X}^t = I$.
- $$\frac{1}{q} X L \overline{X}^t = \mathrm{diag}(k - \psi(S))_{\psi}, \tag{1}$$
- Interpret this as PLQ-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



Carl Gustav Jacob Jacobi (1804-51)

$\mathbb{F}_q^\times$-action

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

$\mathbb{F}_q^\times$-action

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

$\mathbb{F}_q^\times$-action

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

$\mathbb{F}_q^\times$-action

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

$\mathbb{F}_q^\times$-action

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

$\mathbb{F}_q^\times$-action

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

$\mathbb{F}_q^\times$-action

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

$\mathbb{F}_q^\times$-action

- $R = \mathbf{Z}_p[\xi_{q-1}]$, pR maximal ideal of R, $R/pR \cong \mathbb{F}_q$.
- $T : \mathbb{F}_q^\times \to R^\times$ 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 2-dimensional.

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 2-dimensional.
- $\{e_i, e_{i+k}\}$ 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 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 $\{\mathbf{1}, [0], e_k\}$.

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 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 $\{\mathbf{1}, [0], e_k\}$.
- 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 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 $\{\mathbf{1}, [0], e_k\}$.
- 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.

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

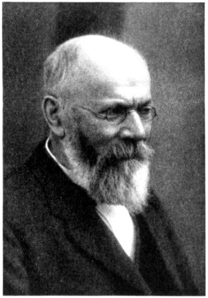
(i) $L(\mathbf{1}) = 0$.

(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.



Carl Friedrich Gauss (1777-1855) Ludwig Stickelberger (1850-1936)

Gauss and Jacobi

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

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 $a_0 + a_1 + \cdots + a_{t-1}$.

Theorem

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*.

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*.
- 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*.
- 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 $L(\mathrm{P}(q))$ which are equal to $p^\lambda,\ 0 \leq \lambda < t$, 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: $K(\mathrm{P}(5^3))$

- $f(3,0) = 3^3 = 27$

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

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

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

- $f(4,0) = 3^4 = 81$.

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

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

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

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

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

Thank you for your attention!