The critical group of the Peisert graphs

Peter Sin
University of Florida

Discrete Mathematics Seminar, U. Delaware, October 22nd, 2015.

Outline

Critical group

- A integer $m \times n$ matrix defines an abelian group $\mathbb{Z}^m / \langle$ columns of A $\rangle$, whose cyclic decomposition is given by the Smith Normal Form of A.
- Let Γ be a graph.
- The group defined by its adjacency matrix A is called the *Smith group* of Γ.
- Let L be the Laplacian matrix of Γ. The torsion subgroup of the group defined by L is called the *critical group*, a.k.a *sandpile group*, *Picard group*, *Jacobian*, denoted $K(\Gamma)$.
- By Kirchhoff's Matrix-Tree Theorem, $|K(\Gamma)|$ is the number of spanning trees in Γ.

Critical group

- A integer $m \times n$ matrix defines an abelian group $\mathbb{Z}^m / \langle$ columns of A $\rangle$, whose cyclic decomposition is given by the Smith Normal Form of A.
- Let Γ be a graph.
- The group defined by its adjacency matrix A is called the *Smith group* of Γ.
- Let L be the Laplacian matrix of Γ. The torsion subgroup of the group defined by L is called the *critical group*, a.k.a *sandpile group*, *Picard group*, *Jacobian*, denoted $K(\Gamma)$.
- By Kirchhoff's Matrix-Tree Theorem, $|K(\Gamma)|$ is the number of spanning trees in Γ.

Critical group

- A integer $m \times n$ matrix defines an abelian group $\mathbb{Z}^m / \langle$ columns of A $\rangle$, whose cyclic decomposition is given by the Smith Normal Form of A.
- Let Γ be a graph.
- The group defined by its adjacency matrix A is called the *Smith group* of Γ.
- Let L be the Laplacian matrix of Γ. The torsion subgroup of the group defined by L is called the *critical group*, a.k.a *sandpile group*, *Picard group*, *Jacobian*, denoted $K(\Gamma)$.
- By Kirchhoff's Matrix-Tree Theorem, $|K(\Gamma)|$ is the number of spanning trees in Γ.

Critical group

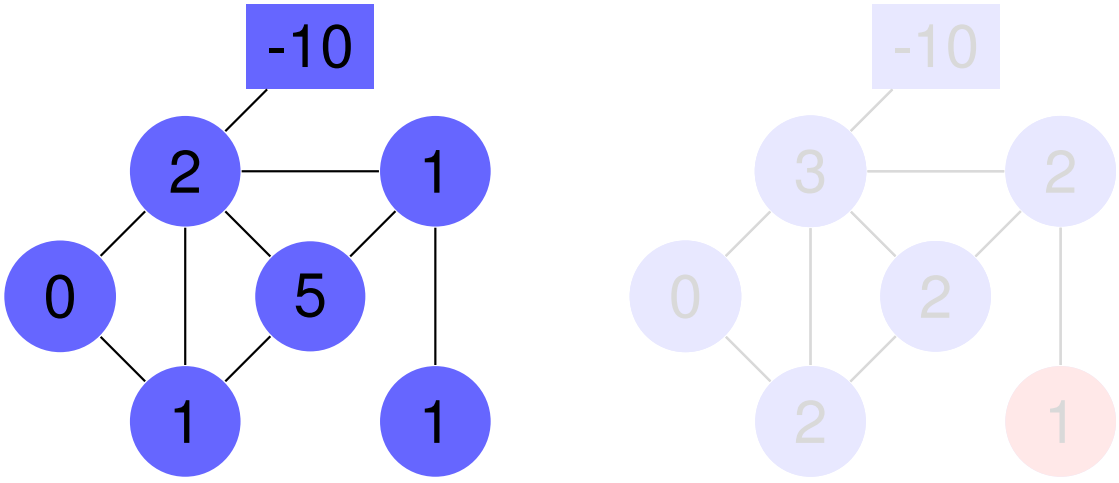
- A integer $m \times n$ matrix defines an abelian group $\mathbb{Z}^m / \langle$ columns of A $\rangle$, whose cyclic decomposition is given by the Smith Normal Form of A.
- Let Γ be a graph.
- The group defined by its adjacency matrix A is called the *Smith group* of Γ.
- Let L be the Laplacian matrix of Γ. The torsion subgroup of the group defined by L is called the *critical group*, a.k.a *sandpile group*, *Picard group*, *Jacobian*, denoted $K(\Gamma)$.
- By Kirchhoff's Matrix-Tree Theorem, $|K(\Gamma)|$ is the number of spanning trees in Γ.

Critical group

- A integer $m \times n$ matrix defines an abelian group $\mathbb{Z}^m / \langle$ columns of A $\rangle$, whose cyclic decomposition is given by the Smith Normal Form of A.
- Let Γ be a graph.
- The group defined by its adjacency matrix A is called the *Smith group* of Γ.
- Let L be the Laplacian matrix of Γ. The torsion subgroup of the group defined by L is called the *critical group*, a.k.a *sandpile group*, *Picard group*, *Jacobian*, denoted $K(\Gamma)$.
- By Kirchhoff's Matrix-Tree Theorem, $|K(\Gamma)|$ is the number of spanning trees in Γ.

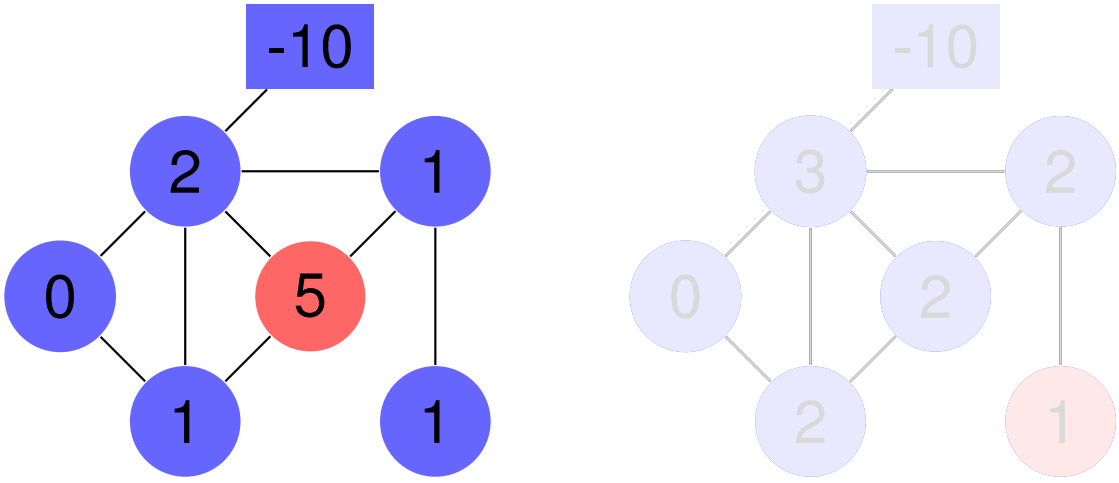
Outline

Rules



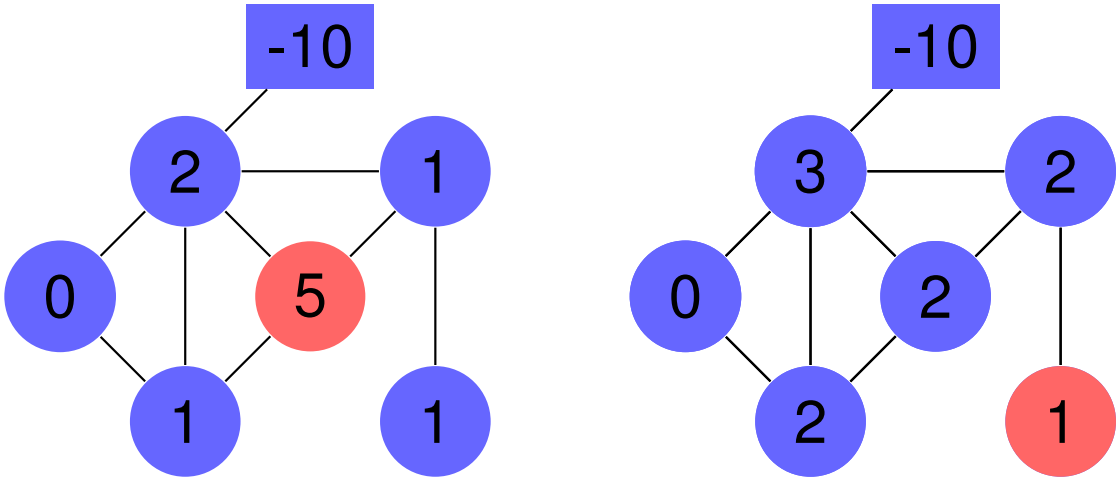
- A configuration is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.
- A round vertex v can be fired if it has at least $\deg(v)$ chips.
- The square vertex is fired only when no others can be fired.
- A configuration is *stable* if no round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

Rules



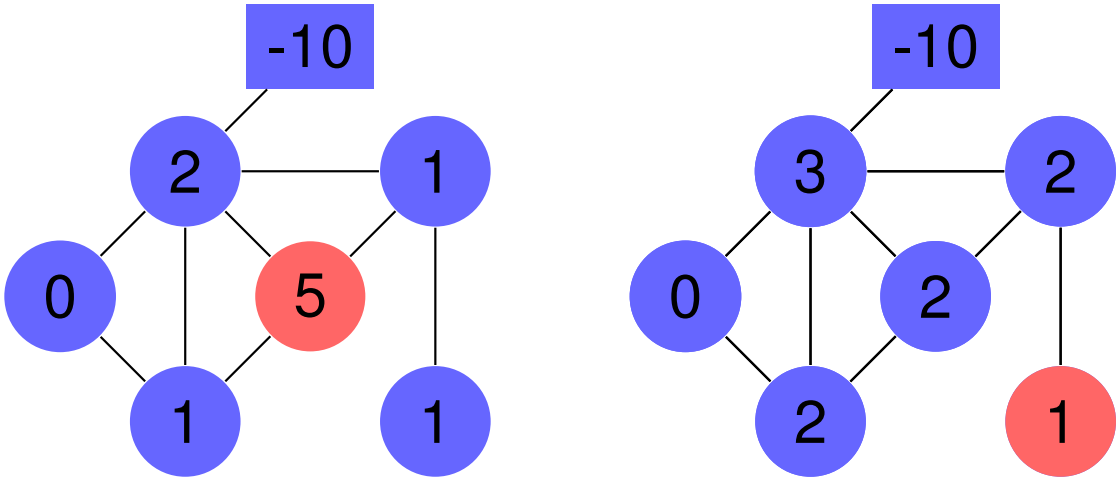
- A configuration is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.
- A round vertex v can be fired if it has at least $\deg(v)$ chips.
- The square vertex is fired only when no others can be fired.
- A configuration is *stable* if no round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

Rules



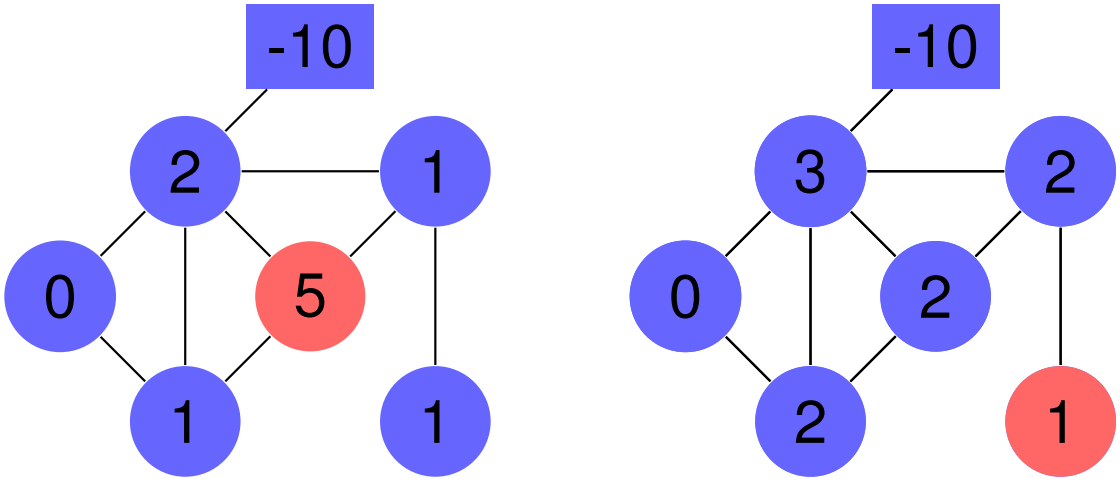
- A configuration is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.
- A round vertex v can be fired if it has at least $\deg(v)$ chips.
- The square vertex is fired only when no others can be fired.
- A configuration is *stable* if no round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

Rules



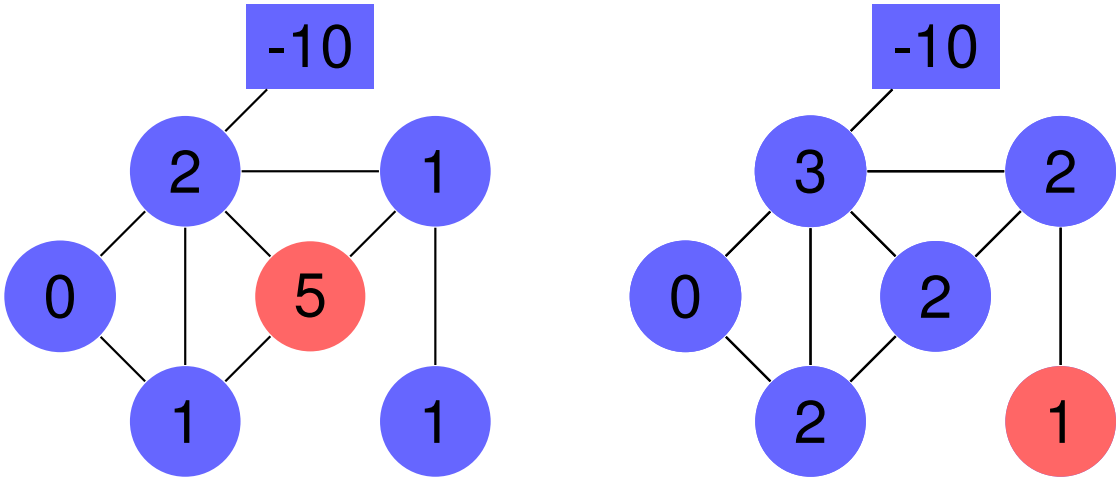
- A configuration is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.
- A round vertex v can be fired if it has at least $\deg(v)$ chips.
- The square vertex is fired only when no others can be fired.
- A configuration is *stable* if no round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

Rules



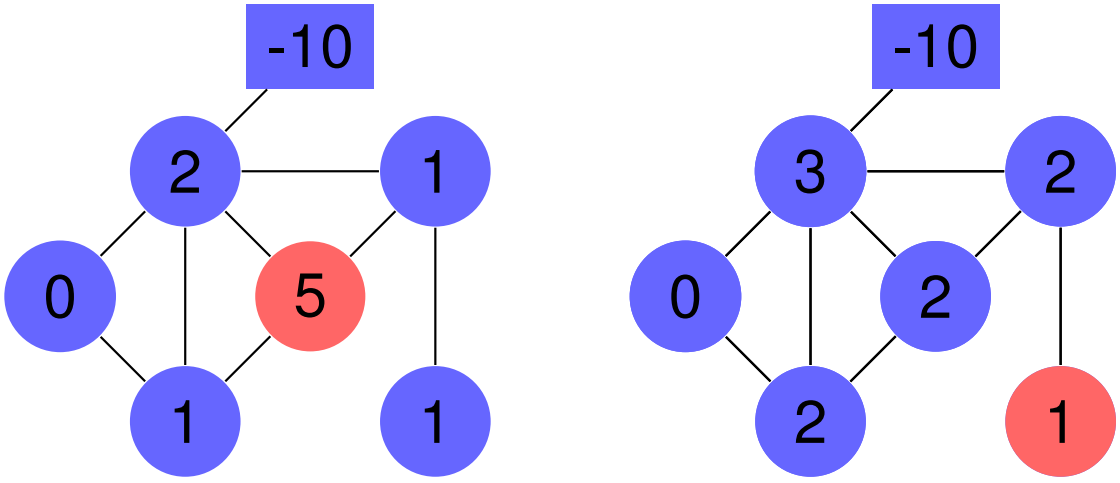
- A configuration is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.
- A round vertex v can be fired if it has at least $\deg(v)$ chips.
- The square vertex is fired only when no others can be fired.
- A configuration is *stable* if no round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

Rules



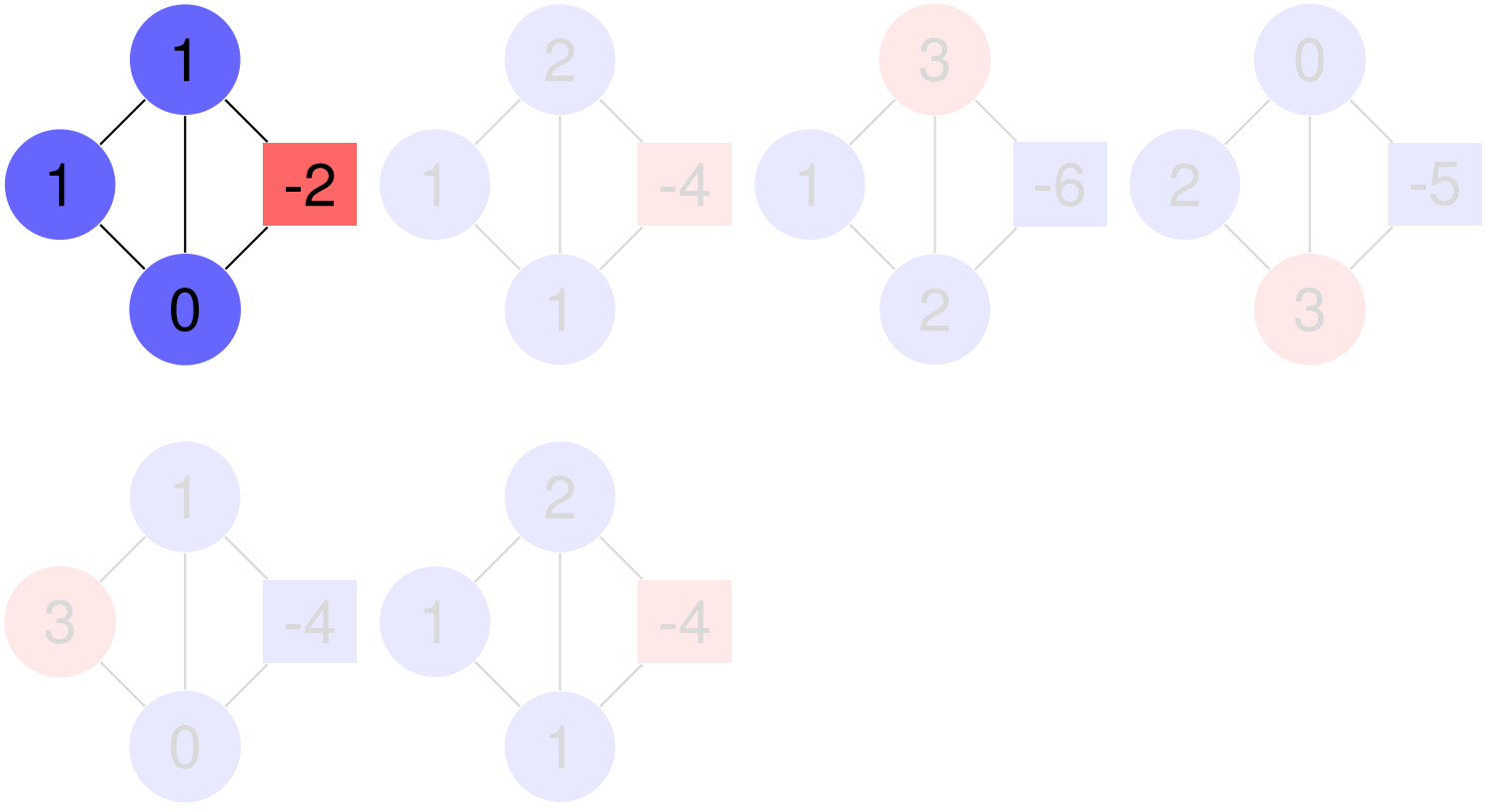
- A configuration is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.
- A round vertex v can be fired if it has at least $\deg(v)$ chips.
- The square vertex is fired only when no others can be fired.
- A configuration is *stable* if no round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

Rules

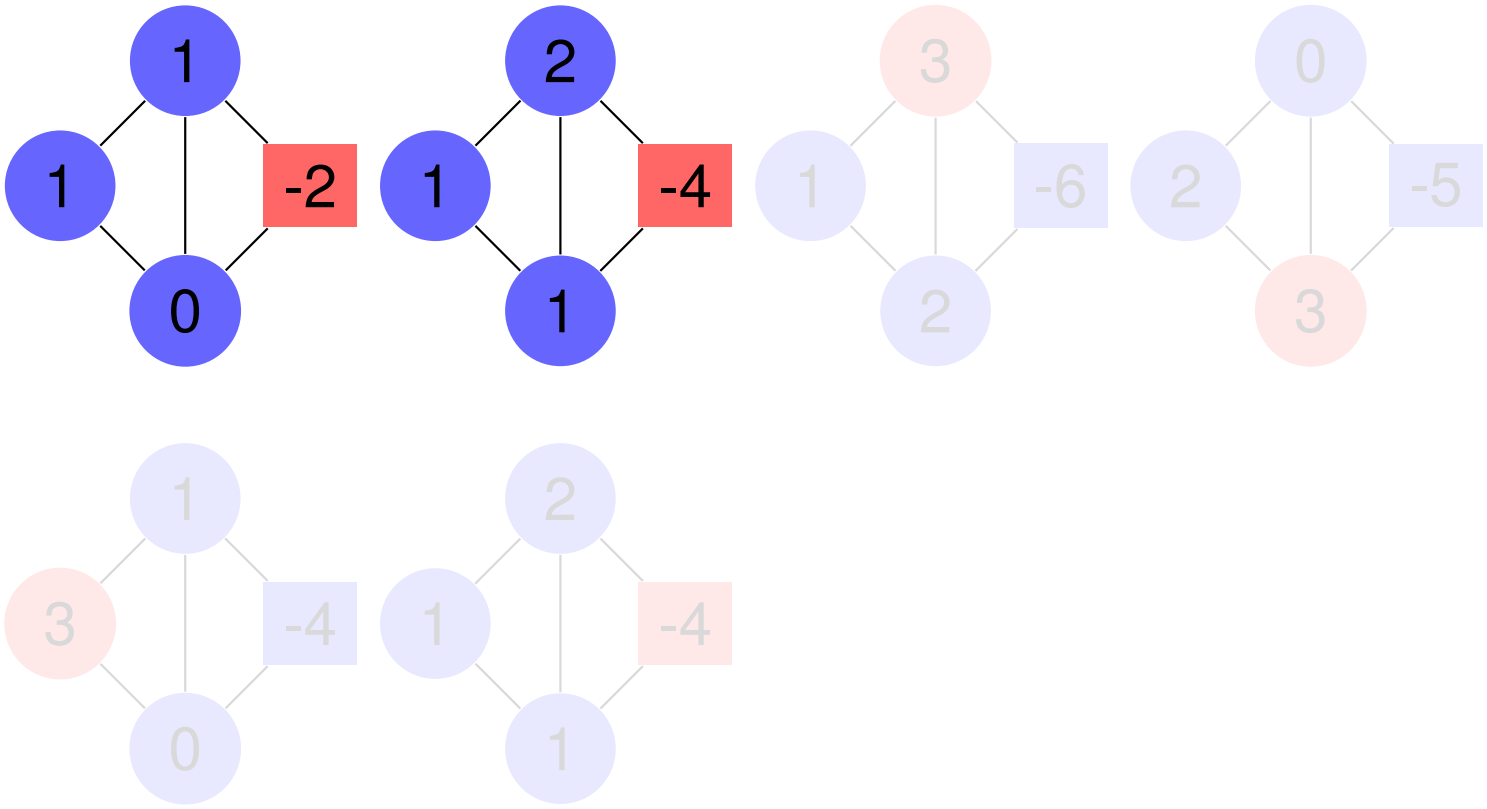


- A configuration is an assignment of a nonnegative integer $s(v)$ to each round vertex v and $-\sum_v s(v)$ to the square vertex.
- A round vertex v can be fired if it has at least $\deg(v)$ chips.
- The square vertex is fired only when no others can be fired.
- A configuration is *stable* if no round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

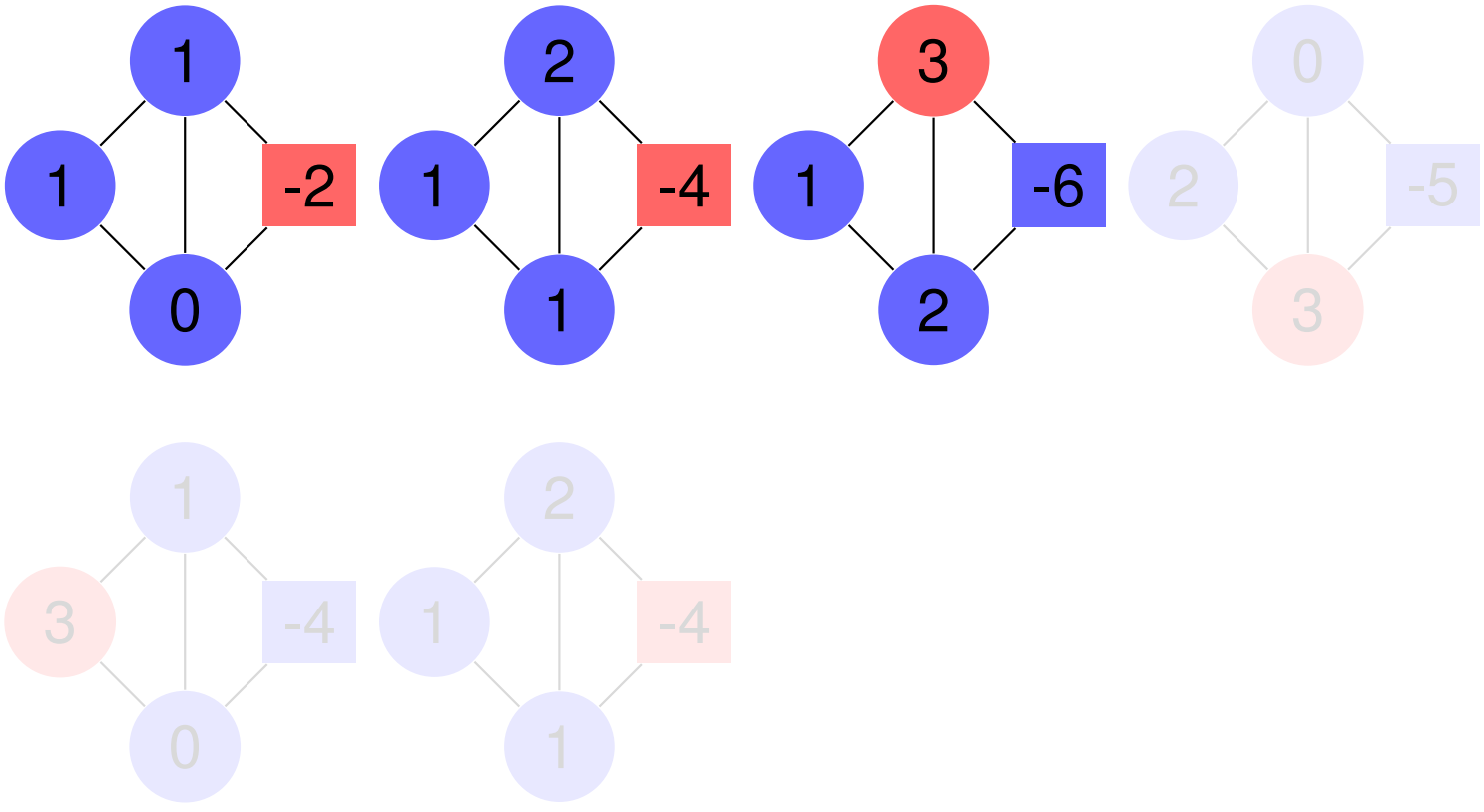
Sample game 1



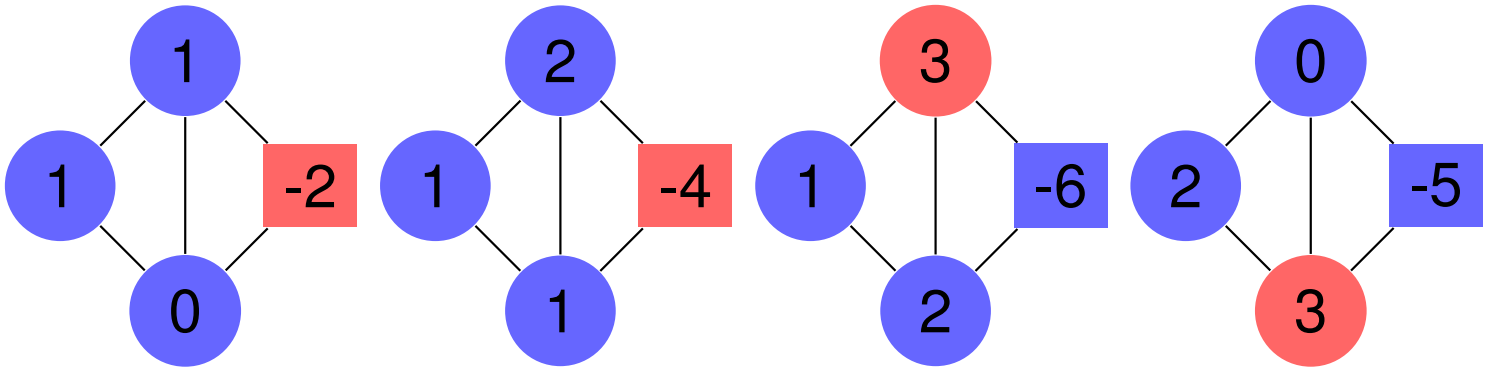
Sample game 1



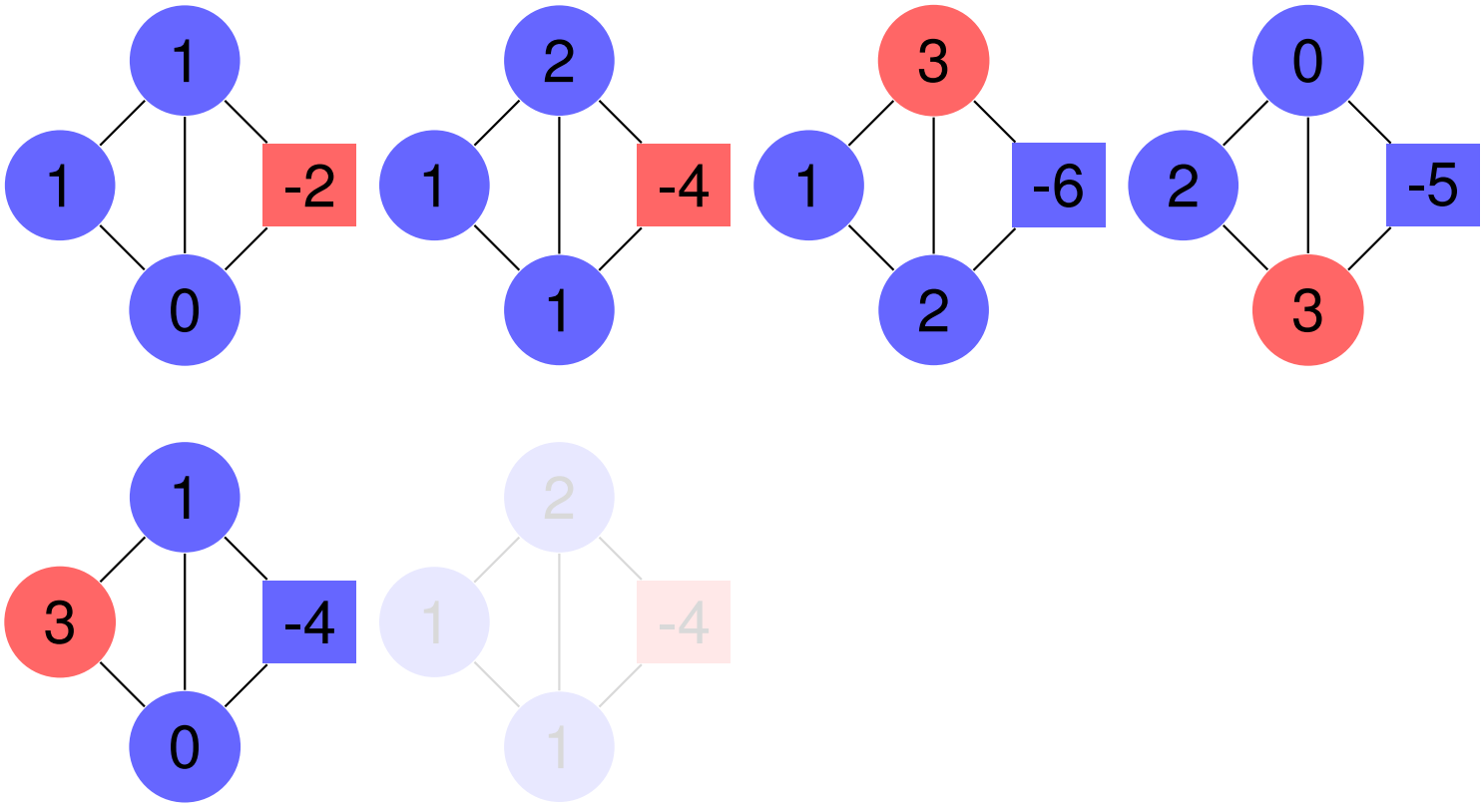
Sample game 1



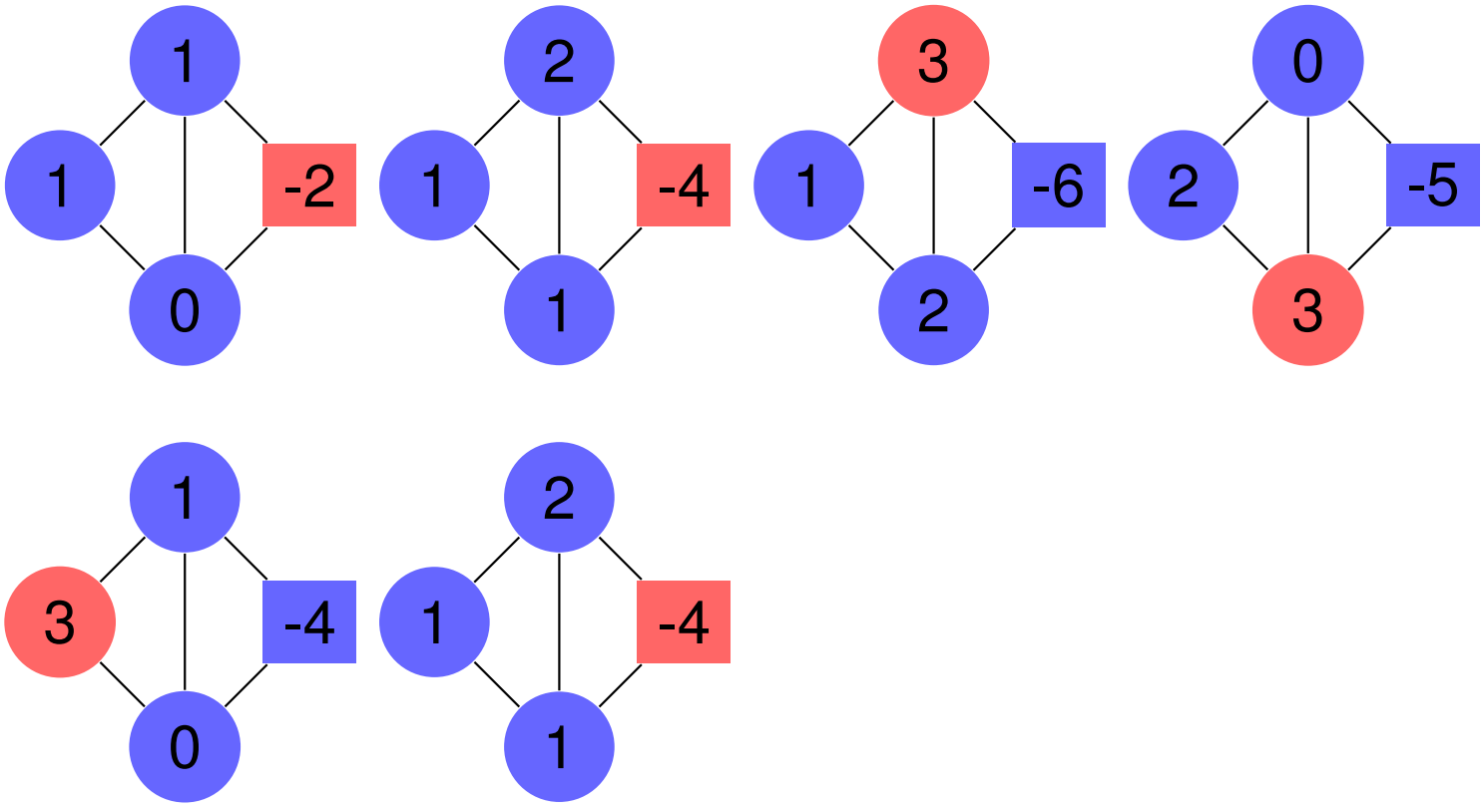
Sample game 1



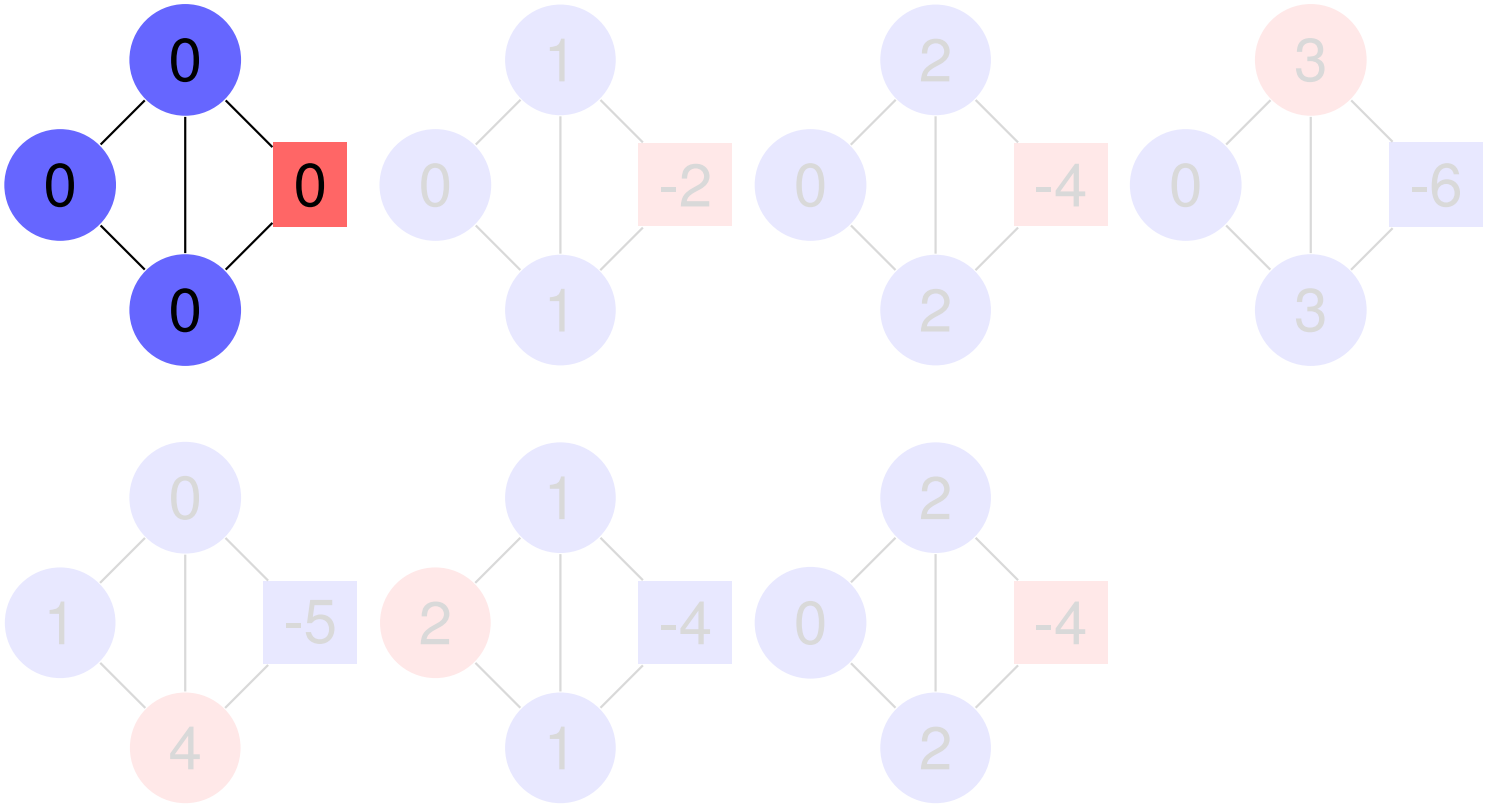
Sample game 1



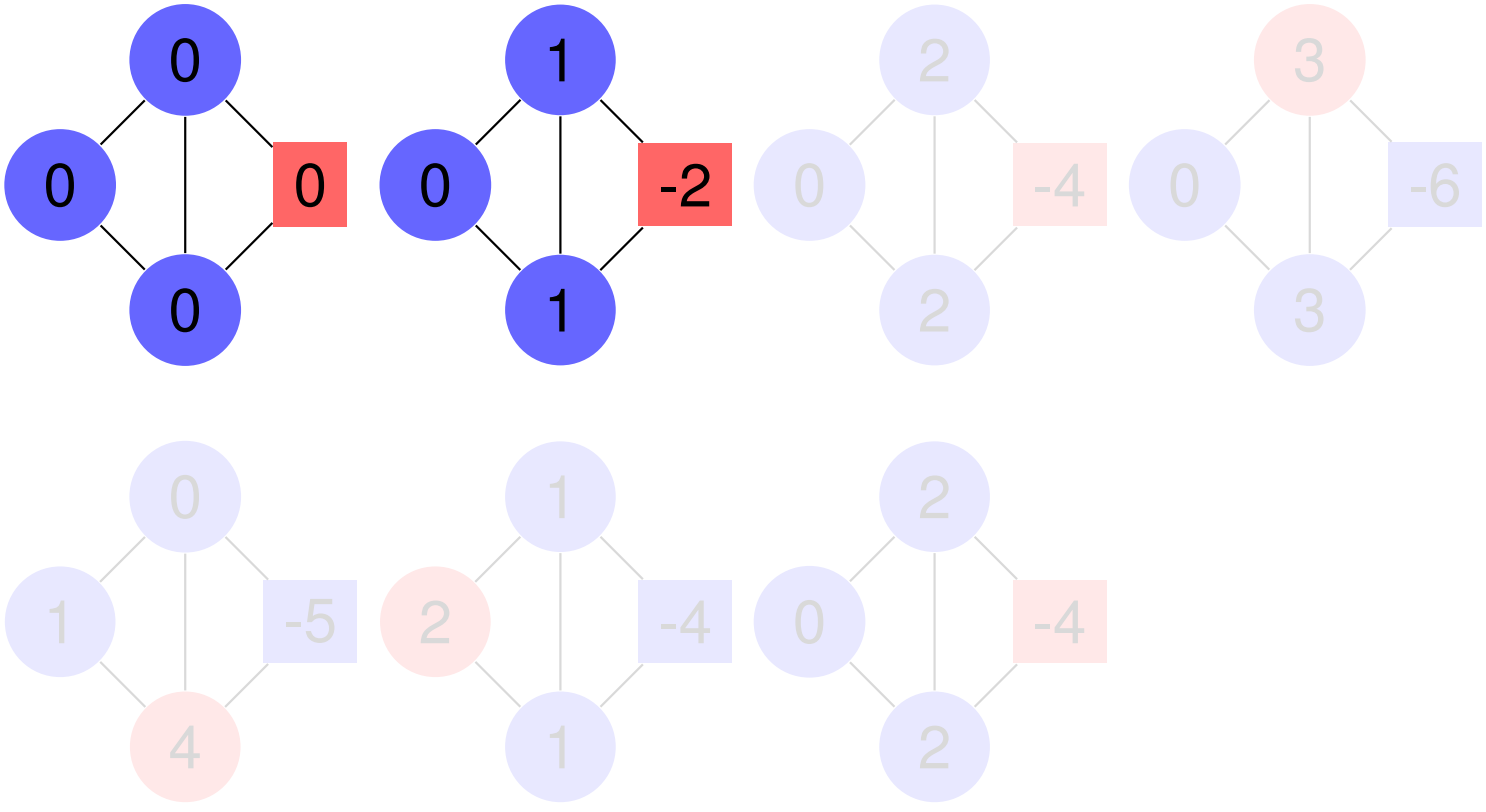
Sample game 1



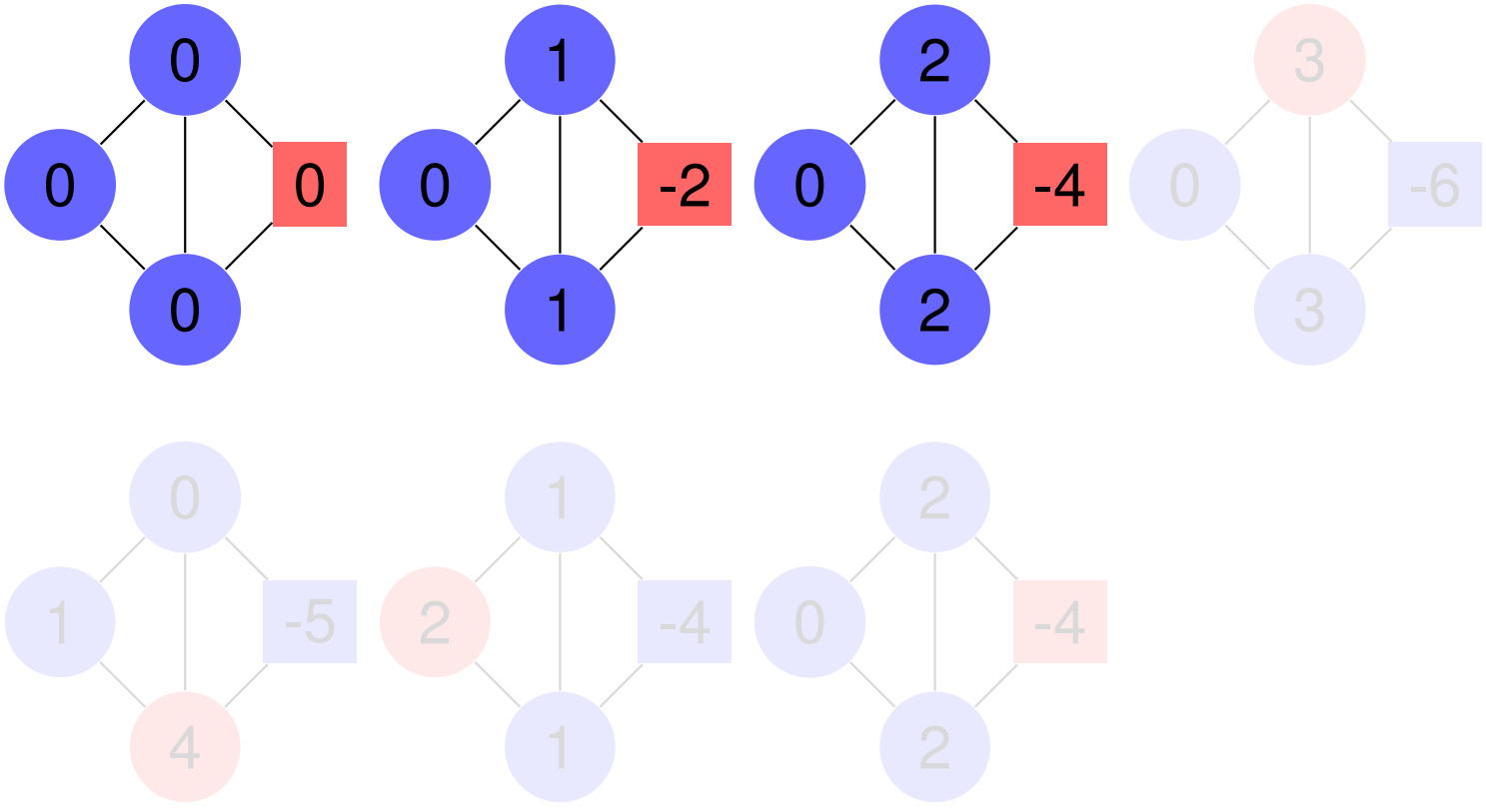
Sample game 2



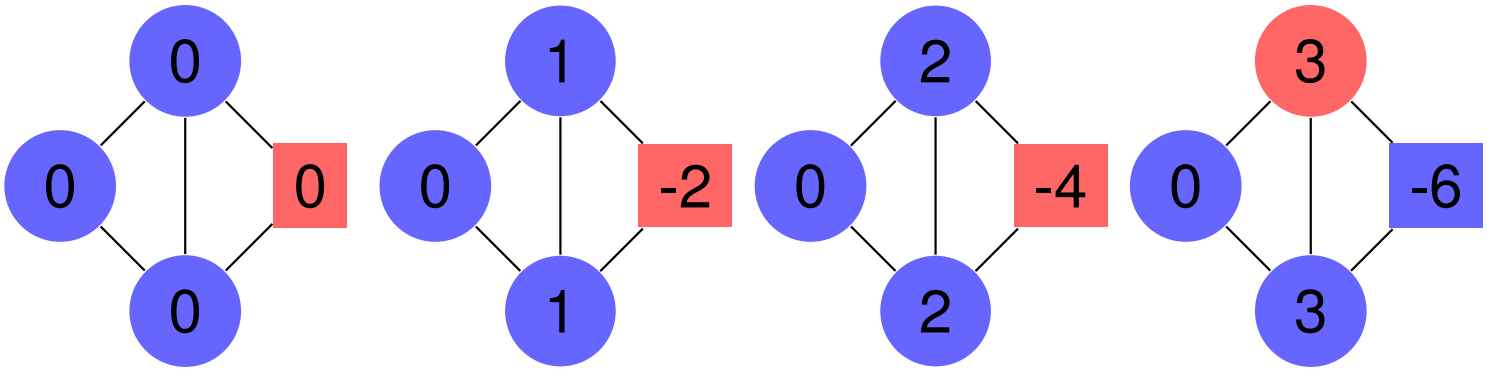
Sample game 2



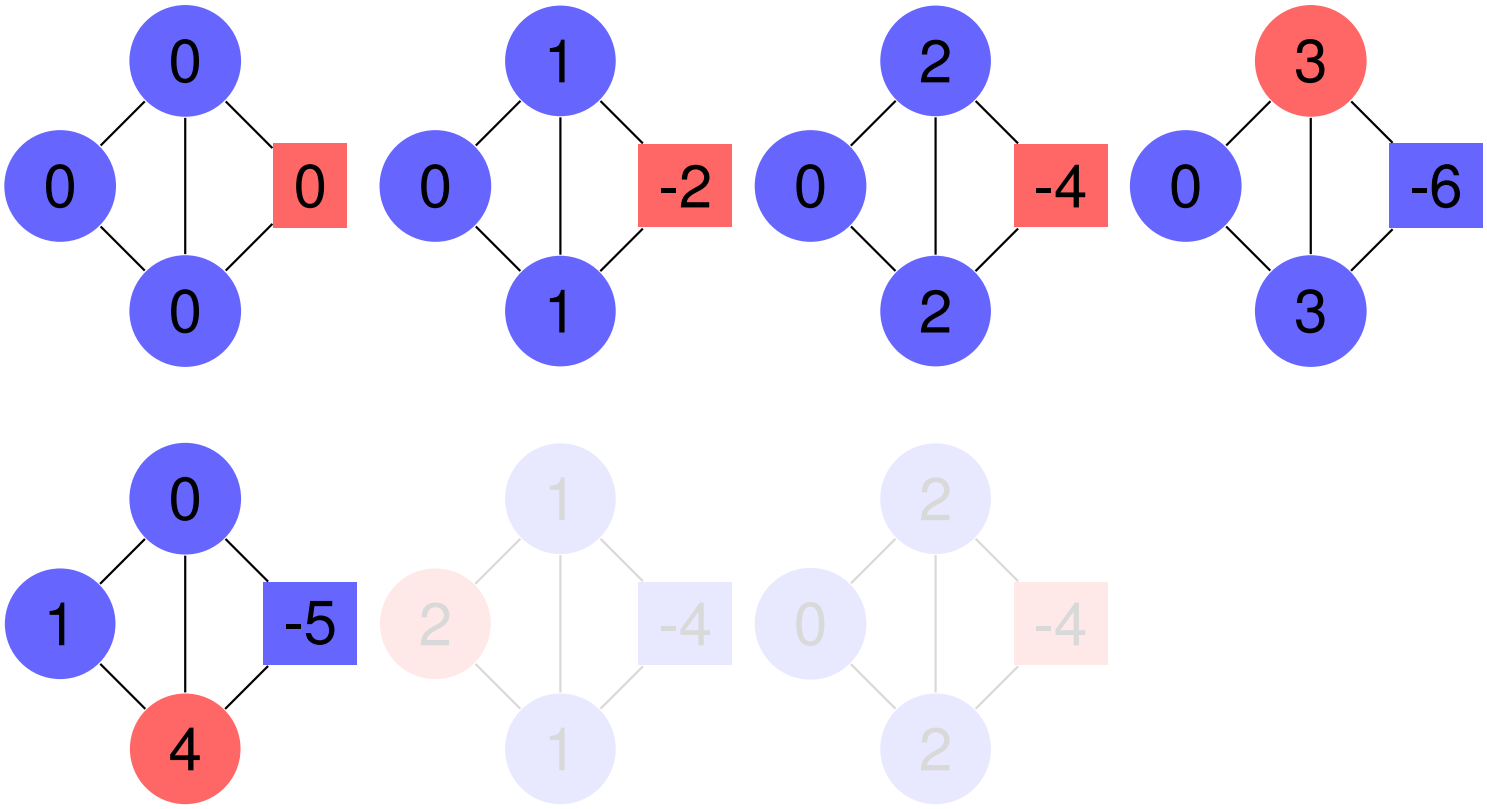
Sample game 2



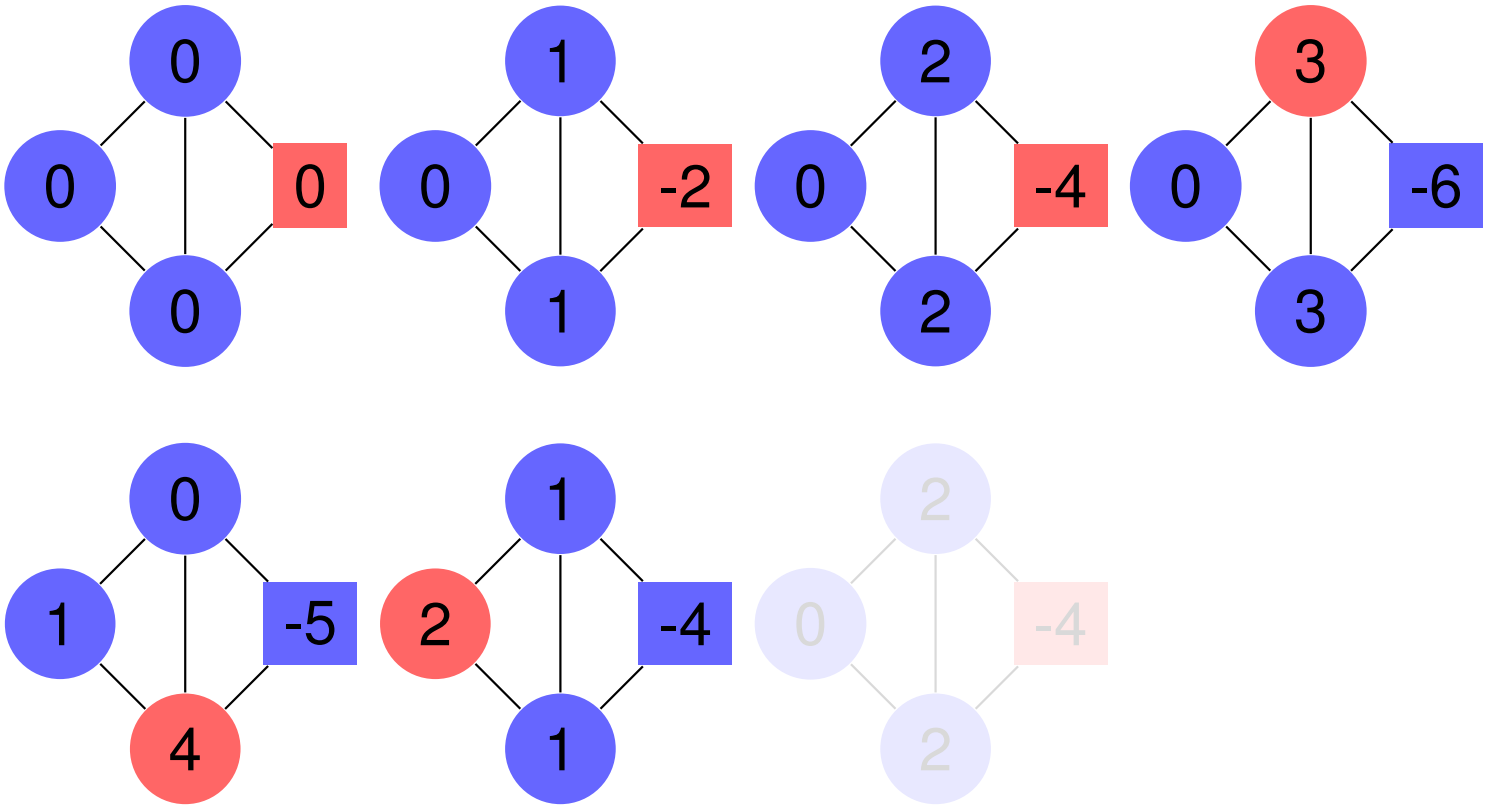
Sample game 2



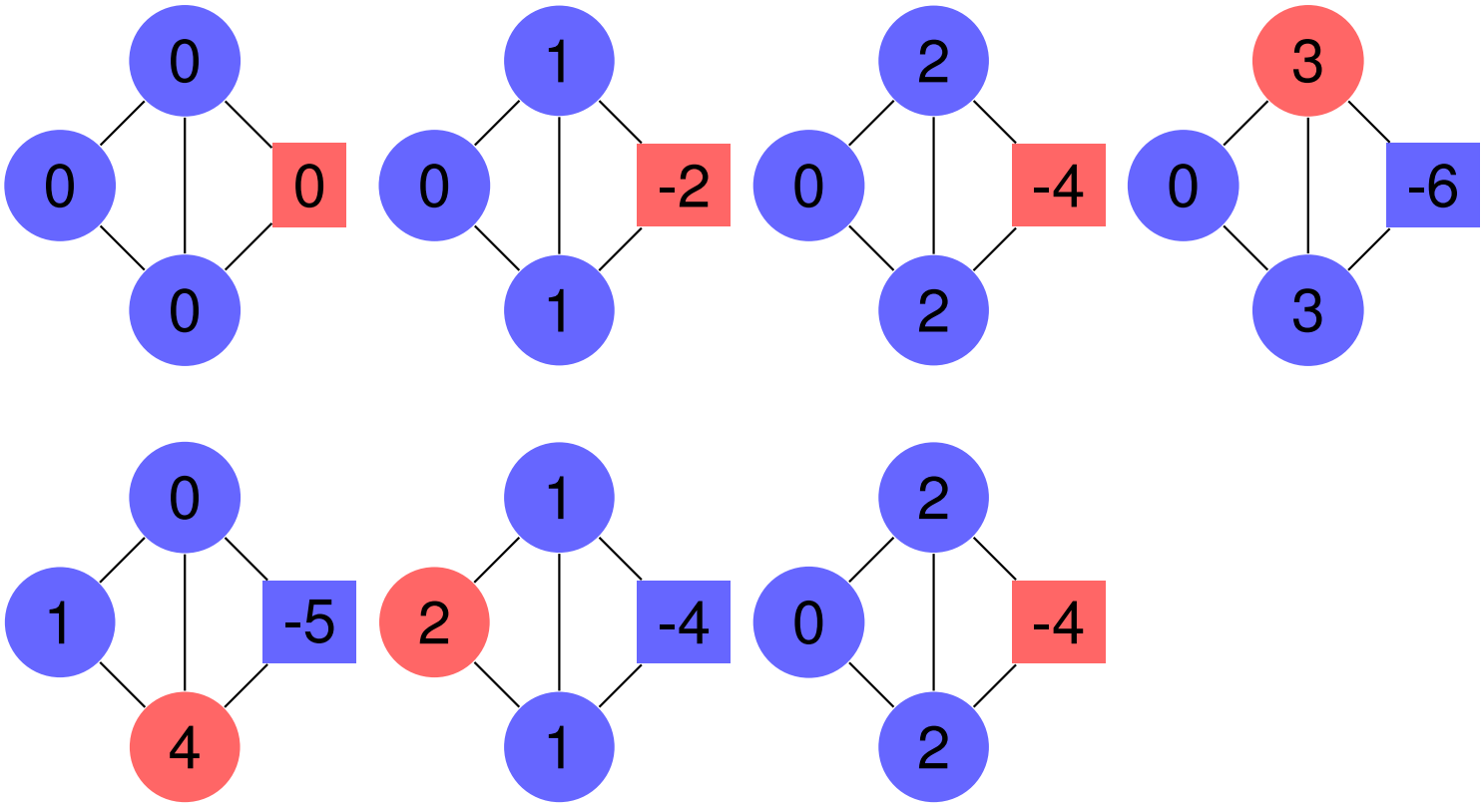
Sample game 2



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

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 $K(\Gamma)$.

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 $K(\Gamma)$.

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 $K(\Gamma)$.

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 $K(\Gamma)$.

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 $K(\Gamma)$.

Outline

Cayley graphs

- Let G be a group, and $S \subseteq G$ be a subset closed under inverses and not containing the identity.
- the Cayley graph $\Gamma(G, S)$ has vertex set G and (g, h) is an edge iff $g^{-1}h \in S$.
- G acts by left multiplication as a regular group of automorphisms of $\Gamma(G, S)$.

Cayley graphs

- Let G be a group, and $S \subseteq G$ be a subset closed under inverses and not containing the identity.
- the Cayley graph $\Gamma(G, S)$ has vertex set G and (g, h) is an edge iff $g^{-1}h \in S$.
- G acts by left multiplication as a regular group of automorphisms of $\Gamma(G, S)$.

Cayley graphs

- Let G be a group, and $S \subseteq G$ be a subset closed under inverses and not containing the identity.
- the Cayley graph $\Gamma(G, S)$ has vertex set G and (g, h) is an edge iff $g^{-1}h \in S$.
- G acts by left multiplication as a regular group of automorphisms of $\Gamma(G, S)$.

Paley graphs, Peisert graphs

- $G = \mathbb{F}_q$, $q \equiv 1 \pmod 4$, $S = \mathbb{F}_q^{\times 2}$. Then $\Gamma(G, S)$ is the *Paley graph* $\mathrm{Paley}(q)$.
- $G = \mathbb{F}_q$, $q = p^{2t}$, $p \equiv 3 \pmod 4$. and β a generator of $\mathbb{F}_q^{\times}$. Set $S' = \mathbb{F}_q^{\times 4} \cup \beta\mathbb{F}_q^{\times 4}$. Then $\Gamma(G, S')$ is the *Peisert graph* $P^*(q)$.
- Both types are *conference graphs* i.e. self-complementary strongly regular graphs. For the same q they are cospectral.
- The Smith and critical groups of $\mathrm{Paley}(q)$ were computed by Chandler-Sin-Xiang (2014) [1].
- All Cayley graphs on an elementary abelian group of order q that are cospectral with $\mathrm{Paley}(q)$ have isomorphic Smith groups. Also the p'-parts of their critical groups are isomorphic.
- Our problem is to determine the isomorphism type of $K(P^*(q))$.

Paley graphs, Peisert graphs

- $G = \mathbb{F}_q$, $q \equiv 1 \pmod 4$, $S = \mathbb{F}_q^{\times 2}$. Then $\Gamma(G, S)$ is the *Paley graph* $\mathrm{Paley}(q)$.
- $G = \mathbb{F}_q$, $q = p^{2t}$, $p \equiv 3 \pmod 4$. and β a generator of $\mathbb{F}_q^{\times}$. Set $S' = \mathbb{F}_q^{\times 4} \cup \beta\mathbb{F}_q^{\times 4}$. Then $\Gamma(G, S')$ is the *Peisert graph* $P^*(q)$.
- Both types are *conference graphs* i.e. self-complementary strongly regular graphs. For the same q they are cospectral.
- The Smith and critical groups of $\mathrm{Paley}(q)$ were computed by Chandler-Sin-Xiang (2014) [1].
- All Cayley graphs on an elementary abelian group of order q that are cospectral with $\mathrm{Paley}(q)$ have isomorphic Smith groups. Also the p'-parts of their critical groups are isomorphic.
- Our problem is to determine the isomorphism type of $K(P^*(q))$.

Paley graphs, Peisert graphs

- $G = \mathbb{F}_q$, $q \equiv 1 \pmod 4$, $S = \mathbb{F}_q^{\times 2}$. Then $\Gamma(G, S)$ is the *Paley graph* $\mathrm{Paley}(q)$.
- $G = \mathbb{F}_q$, $q = p^{2t}$, $p \equiv 3 \pmod 4$. and β a generator of $\mathbb{F}_q^{\times}$. Set $S' = \mathbb{F}_q^{\times 4} \cup \beta\mathbb{F}_q^{\times 4}$. Then $\Gamma(G, S')$ is the *Peisert graph* $P^*(q)$.
- Both types are *conference graphs* i.e. self-complementary strongly regular graphs. For the same q they are cospectral.
- The Smith and critical groups of $\mathrm{Paley}(q)$ were computed by Chandler-Sin-Xiang (2014) [1].
- All Cayley graphs on an elementary abelian group of order q that are cospectral with $\mathrm{Paley}(q)$ have isomorphic Smith groups. Also the p'-parts of their critical groups are isomorphic.
- Our problem is to determine the isomorphism type of $K(P^*(q))$.

Paley graphs, Peisert graphs

- $G = \mathbb{F}_q$, $q \equiv 1 \pmod 4$, $S = \mathbb{F}_q^{\times 2}$. Then $\Gamma(G, S)$ is the *Paley graph* $\mathrm{Paley}(q)$.
- $G = \mathbb{F}_q$, $q = p^{2t}$, $p \equiv 3 \pmod 4$. and β a generator of $\mathbb{F}_q^{\times}$. Set $S' = \mathbb{F}_q^{\times 4} \cup \beta\mathbb{F}_q^{\times 4}$. Then $\Gamma(G, S')$ is the *Peisert graph* $P^*(q)$.
- Both types are *conference graphs* i.e. self-complementary strongly regular graphs. For the same q they are cospectral.
- The Smith and critical groups of $\mathrm{Paley}(q)$ were computed by Chandler-Sin-Xiang (2014) [1].
- All Cayley graphs on an elementary abelian group of order q that are cospectral with $\mathrm{Paley}(q)$ have isomorphic Smith groups. Also the p'-parts of their critical groups are isomorphic.
- Our problem is to determine the isomorphism type of $K(P^*(q))$.

Paley graphs, Peisert graphs

- $G = \mathbb{F}_q$, $q \equiv 1 \pmod 4$, $S = \mathbb{F}_q^{\times 2}$. Then $\Gamma(G, S)$ is the *Paley graph* $\mathrm{Paley}(q)$.
- $G = \mathbb{F}_q$, $q = p^{2t}$, $p \equiv 3 \pmod 4$. and β a generator of $\mathbb{F}_q^{\times}$. Set $S' = \mathbb{F}_q^{\times 4} \cup \beta\mathbb{F}_q^{\times 4}$. Then $\Gamma(G, S')$ is the *Peisert graph* $P^*(q)$.
- Both types are *conference graphs* i.e. self-complementary strongly regular graphs. For the same q they are cospectral.
- The Smith and critical groups of $\mathrm{Paley}(q)$ were computed by Chandler-Sin-Xiang (2014) [1].
- All Cayley graphs on an elementary abelian group of order q that are cospectral with $\mathrm{Paley}(q)$ have isomorphic Smith groups. Also the p'-parts of their critical groups are isomorphic.
- Our problem is to determine the isomorphism type of $K(P^*(q))$.

Paley graphs, Peisert graphs

- $G = \mathbb{F}_q$, $q \equiv 1 \pmod 4$, $S = \mathbb{F}_q^{\times 2}$. Then $\Gamma(G, S)$ is the *Paley graph* $\mathrm{Paley}(q)$.
- $G = \mathbb{F}_q$, $q = p^{2t}$, $p \equiv 3 \pmod 4$. and β a generator of $\mathbb{F}_q^{\times}$. Set $S' = \mathbb{F}_q^{\times 4} \cup \beta\mathbb{F}_q^{\times 4}$. Then $\Gamma(G, S')$ is the *Peisert graph* $P^*(q)$.
- Both types are *conference graphs* i.e. self-complementary strongly regular graphs. For the same q they are cospectral.
- The Smith and critical groups of $\mathrm{Paley}(q)$ were computed by Chandler-Sin-Xiang (2014) [1].
- All Cayley graphs on an elementary abelian group of order q that are cospectral with $\mathrm{Paley}(q)$ have isomorphic Smith groups. Also the p'-parts of their critical groups are isomorphic.
- Our problem is to determine the isomorphism type of $K(P^*(q))$.

Outline

The module $R^{\mathbb{F}_q}$

- Recall $q = p^{2t}$ and $p \equiv 3 \pmod 4$.
- $R = \mathbb{Z}_p[\xi]$, ξ a primitive $(q-1)$-st root of unity.
- R is a local PID with maximal ideal pR.
- $R^{\mathbb{F}_q}$ has basis elements $[x]$ for $x \in \mathbb{F}_q$.
- $\mu_L : R^{\mathbb{F}_q} \to R^{\mathbb{F}_q}$, left multiplication by L.

The module $R^{\mathbb{F}_q}$

- Recall $q = p^{2t}$ and $p \equiv 3 \pmod 4$.
- $R = \mathbb{Z}_p[\xi]$, ξ a primitive $(q-1)$-st root of unity.
- R is a local PID with maximal ideal pR.
- $R^{\mathbb{F}_q}$ has basis elements $[x]$ for $x \in \mathbb{F}_q$.
- $\mu_L : R^{\mathbb{F}_q} \to R^{\mathbb{F}_q}$, left multiplication by L.

The module $R^{\mathbb{F}_q}$

- Recall $q = p^{2t}$ and $p \equiv 3 \pmod 4$.
- $R = \mathbb{Z}_p[\xi]$, ξ a primitive $(q-1)$-st root of unity.
- R is a local PID with maximal ideal pR.
- $R^{\mathbb{F}_q}$ has basis elements $[x]$ for $x \in \mathbb{F}_q$.
- $\mu_L : R^{\mathbb{F}_q} \to R^{\mathbb{F}_q}$, left multiplication by L.

The module $R^{\mathbb{F}_q}$

- Recall $q = p^{2t}$ and $p \equiv 3 \pmod 4$.
- $R = \mathbb{Z}_p[\xi]$, ξ a primitive $(q-1)$-st root of unity.
- R is a local PID with maximal ideal pR.
- $R^{\mathbb{F}_q}$ has basis elements $[x]$ for $x \in \mathbb{F}_q$.
- $\mu_L : R^{\mathbb{F}_q} \to R^{\mathbb{F}_q}$, left multiplication by L.

The module $R^{\mathbb{F}_q}$

- Recall $q = p^{2t}$ and $p \equiv 3 \pmod 4$.
- $R = \mathbb{Z}_p[\xi]$, ξ a primitive $(q-1)$-st root of unity.
- R is a local PID with maximal ideal pR.
- $R^{\mathbb{F}_q}$ has basis elements $[x]$ for $x \in \mathbb{F}_q$.
- $\mu_L : R^{\mathbb{F}_q} \to R^{\mathbb{F}_q}$, left multiplication by L.

- $T : \mathbb{F}_q^\times \to R^\times$, $T(\beta^j) = \xi^j$, Teichmüller character, generates $\mathrm{Hom}(\mathbb{F}_q^\times, R^\times)$.
- $\mathbb{F}_q^\times$ acts on $R^{\mathbb{F}_q} = R[0] \oplus R^{\mathbb{F}_q^\times}$
- $R^{\mathbb{F}_q^\times}$ decomposes further into the direct sum of $\mathbb{F}_q^\times$-invariant components of rank 1, affording the characters T^i, $i = 0, \ldots, q-2$.
- The component affording T^i is spanned by

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

- New basis $\{e_i \mid i = 1, \ldots q-2\} \cup \{e_0, [0]\}$,

- $T : \mathbb{F}_q^\times \to R^\times$, $T(\beta^j) = \xi^j$, Teichmüller character, generates $\mathrm{Hom}(\mathbb{F}_q^\times, R^\times)$.
- $\mathbb{F}_q^\times$ acts on $R^{\mathbb{F}_q} = R[0] \oplus R^{\mathbb{F}_q^\times}$
- $R^{\mathbb{F}_q^\times}$ decomposes further into the direct sum of $\mathbb{F}_q^\times$-invariant components of rank 1, affording the characters T^i, $i = 0, \ldots, q-2$.
- The component affording T^i is spanned by

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

- New basis $\{e_i \mid i = 1, \ldots q-2\} \cup \{e_0, [0]\}$,

- $T : \mathbb{F}_q^\times \to R^\times$, $T(\beta^j) = \xi^j$, Teichmüller character, generates $\mathrm{Hom}(\mathbb{F}_q^\times, R^\times)$.
- $\mathbb{F}_q^\times$ acts on $R^{\mathbb{F}_q} = R[0] \oplus R^{\mathbb{F}_q^\times}$
- $R^{\mathbb{F}_q^\times}$ decomposes further into the direct sum of $\mathbb{F}_q^\times$-invariant components of rank 1, affording the characters T^i, $i = 0, \ldots, q-2$.
- The component affording T^i is spanned by

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

- New basis $\{e_i \mid i = 1, \ldots q-2\} \cup \{e_0, [0]\}$,

- $T : \mathbb{F}_q^\times \to R^\times$, $T(\beta^j) = \xi^j$, Teichmüller character, generates $\mathrm{Hom}(\mathbb{F}_q^\times, R^\times)$.
- $\mathbb{F}_q^\times$ acts on $R^{\mathbb{F}_q} = R[0] \oplus R^{\mathbb{F}_q^\times}$
- $R^{\mathbb{F}_q^\times}$ decomposes further into the direct sum of $\mathbb{F}_q^\times$-invariant components of rank 1, affording the characters T^i, $i = 0, \ldots, q-2$.
- The component affording T^i is spanned by

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

- New basis $\{e_i \mid i = 1, \ldots q-2\} \cup \{e_0, [0]\}$,

- $T : \mathbb{F}_q^\times \to R^\times$, $T(\beta^j) = \xi^j$, Teichmüller character, generates $\mathrm{Hom}(\mathbb{F}_q^\times, R^\times)$.
- $\mathbb{F}_q^\times$ acts on $R^{\mathbb{F}_q} = R[0] \oplus R^{\mathbb{F}_q^\times}$
- $R^{\mathbb{F}_q^\times}$ decomposes further into the direct sum of $\mathbb{F}_q^\times$-invariant components of rank 1, affording the characters T^i, $i = 0, \ldots, q-2$.
- The component affording T^i is spanned by

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

- New basis $\{e_i \mid i = 1, \ldots q-2\} \cup \{e_0, [0]\}$,

$\mathbb{F}_q^{\times 4}$-decomposition

Next consider the action of the subgroup $H = \mathbb{F}_q^{\times 4}$.

- T^i, T^{i+r}, T^{i+2r}, and T^{i+3r} are equal on H
- For $i \notin \{0, r, 2r, 3r\}$ the elements e_i, e_{i+r}, e_{i+2r} and e_{i+3r} span the H-isotypic component

$$M_i = \{m \in R^{\mathbb{F}_q} \mid ym = T^i(y)m, \quad \forall y \in H\}$$

  of $R^{\mathbb{F}_q}$ for $1 \leq i \leq \frac{q-5}{4}$.
- M_0, the submodule of H-fixed points in $R^{\mathbb{F}_q}$. Basis elements $\mathbf{1} = \sum_{x \in \mathbb{F}_q} x = e_0 + [0]$, $[0]$, e_r, e_{2r} and $e_3 r$.
- $R^{\mathbb{F}_q} = M_0 \oplus \bigoplus_{i=1}^{\frac{q-5}{4}} M_i$.
- We have $\mu_L(M_i) \subseteq M_i$ as μ_L is an RH-module homomophism.
- Can re-order new basis so that the matrix of μ_L is block-diagonal with $\frac{q-5}{4}$ 4×4 blocks and a single 5×5 block.

$\mathbb{F}_q^{\times 4}$-decomposition

Next consider the action of the subgroup $H = \mathbb{F}_q^{\times 4}$.

- T^i, T^{i+r}, T^{i+2r}, and T^{i+3r} are equal on H
- For $i \notin \{0, r, 2r, 3r\}$ the elements e_i, e_{i+r}, e_{i+2r} and e_{i+3r} span the H-isotypic component

$$M_i = \{m \in R^{\mathbb{F}_q} \mid ym = T^i(y)m, \quad \forall y \in H\}$$

of $R^{\mathbb{F}_q}$ for $1 \leq i \leq \frac{q-5}{4}$.

- M_0, the submodule of H-fixed points in $R^{\mathbb{F}_q}$. Basis elements $\mathbf{1} = \sum_{x \in \mathbb{F}_q} x = e_0 + [0], [0], e_r, e_{2r}$ and $e_3 r$.
- $R^{\mathbb{F}_q} = M_0 \oplus \bigoplus_{i=1}^{\frac{q-5}{4}} M_i$.
- We have $\mu_L(M_i) \subseteq M_i$ as μ_L is an RH-module homomophism.
- Can re-order new basis so that the matrix of μ_L is block-diagonal with $\frac{q-5}{4}$ 4×4 blocks and a single 5×5 block.

$\mathbb{F}_q^{\times 4}$-decomposition

Next consider the action of the subgroup $H = \mathbb{F}_q^{\times 4}$.

- T^i, T^{i+r}, T^{i+2r}, and T^{i+3r} are equal on H
- For $i \notin \{0, r, 2r, 3r\}$ the elements e_i, e_{i+r}, e_{i+2r} and e_{i+3r} span the H-isotypic component

$$M_i = \{m \in R^{\mathbb{F}_q} \mid ym = T^i(y)m, \quad \forall y \in H\}$$

of $R^{\mathbb{F}_q}$ for $1 \leq i \leq \frac{q-5}{4}$.

- M_0, the submodule of H-fixed points in $R^{\mathbb{F}_q}$. Basis elements $\mathbf{1} = \sum_{x \in \mathbb{F}_q} x = e_0 + [0]$, $[0]$, e_r, e_{2r} and $e_3 r$.
- $R^{\mathbb{F}_q} = M_0 \oplus \bigoplus_{i=1}^{\frac{q-5}{4}} M_i$.
- We have $\mu_L(M_i) \subseteq M_i$ as μ_L is an RH-module homomophism.
- Can re-order new basis so that the matrix of μ_L is block-diagonal with $\frac{q-5}{4}$ 4×4 blocks and a single 5×5 block.

$\mathbb{F}_q^{\times 4}$-decomposition

Next consider the action of the subgroup $H = \mathbb{F}_q^{\times 4}$.

- T^i, T^{i+r}, T^{i+2r}, and T^{i+3r} are equal on H
- For $i \notin \{0, r, 2r, 3r\}$ the elements e_i, e_{i+r}, e_{i+2r} and e_{i+3r} span the H-isotypic component

$$M_i = \{m \in R^{\mathbb{F}_q} \mid ym = T^i(y)m, \quad \forall y \in H\}$$

  of $R^{\mathbb{F}_q}$ for $1 \leq i \leq \frac{q-5}{4}$.
- M_0, the submodule of H-fixed points in $R^{\mathbb{F}_q}$. Basis elements $\mathbf{1} = \sum_{x \in \mathbb{F}_q} x = e_0 + [0]$, $[0]$, e_r, e_{2r} and $e_3 r$.
- $R^{\mathbb{F}_q} = M_0 \oplus \bigoplus_{i=1}^{\frac{q-5}{4}} M_i$.
- We have $\mu_L(M_i) \subseteq M_i$ as μ_L is an RH-module homomophism.
- Can re-order new basis so that the matrix of μ_L is block-diagonal with $\frac{q-5}{4}$ 4×4 blocks and a single 5×5 block.

$\mathbb{F}_q^{\times 4}$-decomposition

Next consider the action of the subgroup $H = \mathbb{F}_q^{\times 4}$.

- T^i, T^{i+r}, T^{i+2r}, and T^{i+3r} are equal on H
- For $i \notin \{0, r, 2r, 3r\}$ the elements e_i, e_{i+r}, e_{i+2r} and e_{i+3r} span the H-isotypic component

$$M_i = \{m \in R^{\mathbb{F}_q} \mid ym = T^i(y)m, \quad \forall y \in H\}$$

  of $R^{\mathbb{F}_q}$ for $1 \leq i \leq \frac{q-5}{4}$.
- M_0, the submodule of H-fixed points in $R^{\mathbb{F}_q}$. Basis elements $\mathbf{1} = \sum_{x \in \mathbb{F}_q} x = e_0 + [0]$, $[0]$, e_r, e_{2r} and $e_3 r$.
- $R^{\mathbb{F}_q} = M_0 \oplus \bigoplus_{i=1}^{\frac{q-5}{4}} M_i$.
- We have $\mu_L(M_i) \subseteq M_i$ as μ_L is an RH-module homomophism.
- Can re-order new basis so that the matrix of μ_L is block-diagonal with $\frac{q-5}{4}$ 4×4 blocks and a single 5×5 block.

$\mathbb{F}_q^{\times 4}$-decomposition

Next consider the action of the subgroup $H = \mathbb{F}_q^{\times 4}$.

- T^i, T^{i+r}, T^{i+2r}, and T^{i+3r} are equal on H
- For $i \notin \{0, r, 2r, 3r\}$ the elements e_i, e_{i+r}, e_{i+2r} and e_{i+3r} span the H-isotypic component

$$M_i = \{m \in R^{\mathbb{F}_q} \mid ym = T^i(y)m, \quad \forall y \in H\}$$

  of $R^{\mathbb{F}_q}$ for $1 \leq i \leq \frac{q-5}{4}$.
- M_0, the submodule of H-fixed points in $R^{\mathbb{F}_q}$. Basis elements $\mathbf{1} = \sum_{x \in \mathbb{F}_q} x = e_0 + [0]$, $[0]$, e_r, e_{2r} and $e_3 r$.
- $R^{\mathbb{F}_q} = M_0 \oplus \bigoplus_{i=1}^{\frac{q-5}{4}} M_i$.
- We have $\mu_L(M_i) \subseteq M_i$ as μ_L is an RH-module homomophism.
- Can re-order new basis so that the matrix of μ_L is block-diagonal with $\frac{q-5}{4}$ 4×4 blocks and a single 5×5 block.

Outline

Jacobi Sums

Definition

Let θ and ψ be multiplicative characters of $\mathbb{F}_q^\times$ taking values in $R^\times$. The *Jacobi sum* is

$$J(\theta, \psi) = \sum_{x \in \mathbb{F}_q} \theta(x)\psi(1-x).$$

(At $x = 0$, nonprinc. chars take value 0, princ. char takes value 1.)

Notation

- $r = \frac{(q-1)}{4}$
- $\eta = \beta^r$, $\alpha = \frac{(\eta-1)}{2}$, $\overline{\alpha} = \frac{(\eta+1)}{2}$
- $\delta_0 : \mathbb{F}_q \to R$ takes the value 1 at 0 and 0 elsewhere.
- characteristic function of S' is

$$\delta_{S'} = \frac{1}{2}(T^0 - \delta_0 + \alpha T^r + \overline{\alpha} T^{-r}),$$

Notation

- $r = \frac{(q-1)}{4}$
- $\eta = \beta^r$, $\alpha = \frac{(\eta-1)}{2}$, $\overline{\alpha} = \frac{(\eta+1)}{2}$
- $\delta_0 : \mathbb{F}_q \to R$ takes the value 1 at 0 and 0 elsewhere.
- characteristic function of S' is

$$\delta_{S'} = \frac{1}{2}(T^0 - \delta_0 + \alpha T^r + \overline{\alpha} T^{-r}),$$

Notation

- $r = \frac{(q-1)}{4}$
- $\eta = \beta^r$, $\alpha = \frac{(\eta-1)}{2}$, $\overline{\alpha} = \frac{(\eta+1)}{2}$
- $\delta_0 : \mathbb{F}_q \to R$ takes the value 1 at 0 and 0 elsewhere.
- characteristic function of S' is

$$\delta_{S'} = \frac{1}{2}(T^0 - \delta_0 + \alpha T^r + \overline{\alpha} T^{-r}),$$

Notation

- $r = \frac{(q-1)}{4}$
- $\eta = \beta^r$, $\alpha = \frac{(\eta-1)}{2}$, $\overline{\alpha} = \frac{(\eta+1)}{2}$
- $\delta_0 : \mathbb{F}_q \to R$ takes the value 1 at 0 and 0 elsewhere.
- characteristic function of S' is

$$\delta_{S'} = \frac{1}{2}(T^0 - \delta_0 + \alpha T^r + \overline{\alpha} T^{-r}),$$

Lemma

Suppose $i \notin \{0, r, 3r\}$. Then

$$\mu_L(e_i) = \frac{1}{2}(qe_i - \overline{\alpha}J(T^{-i}, T^{-r})e_{i+r} - \alpha J(T^{-i}, T^{-3r})e_{i+3r}).$$

Proof.

$$2\mu_A(e_i) = 2\sum_{x\in\mathbb{F}_q^\times} T^{-i}(x) \sum_{y\in\mathbb{F}_q} \delta_{S'}(y)[x+y]$$

$$= \sum_{x\in\mathbb{F}_q^\times} T^{-i}(x) \sum_{y\in\mathbb{F}_q} (T^0(y) - \delta_0(y) + \alpha T^r(y) + \overline{\alpha} T^{-r}(y))[x+y]$$

$\ldots$

$\ldots$

Lemma

Suppose $i \notin \{0, r, 3r\}$. Then

$$\mu_L(e_i) = \frac{1}{2}(qe_i - \overline{\alpha}J(T^{-i}, T^{-r})e_{i+r} - \alpha J(T^{-i}, T^{-3r})e_{i+3r}).$$

Proof.

$$2\mu_A(e_i) = 2\sum_{x\in\mathbb{F}_q^\times} T^{-i}(x) \sum_{y\in\mathbb{F}_q} \delta_{S'}(y)[x+y]$$

$$= \sum_{x\in\mathbb{F}_q^\times} T^{-i}(x) \sum_{y\in\mathbb{F}_q} (T^0(y) - \delta_0(y) + \alpha T^r(y) + \overline{\alpha} T^{-r}(y))[x+y]$$

$\cdots$

$\cdots$

Lemma

Suppose $i \notin \{0, r, 3r\}$. Then

$$\mu_L(e_i) = \frac{1}{2}(qe_i - \overline{\alpha}J(T^{-i}, T^{-r})e_{i+r} - \alpha J(T^{-i}, T^{-3r})e_{i+3r}).$$

Proof.

$$2\mu_A(e_i) = 2\sum_{x\in\mathbb{F}_q^\times} T^{-i}(x) \sum_{y\in\mathbb{F}_q} \delta_{S'}(y)[x+y]$$

$$= \sum_{x\in\mathbb{F}_q^\times} T^{-i}(x) \sum_{y\in\mathbb{F}_q} (T^0(y) - \delta_0(y) + \alpha T^r(y) + \overline{\alpha} T^{-r}(y))[x+y]$$

$\ldots$

$\ldots$

The matrix of $\mu_{L|M_i}$ is

$$\begin{bmatrix} q & -\alpha J(T^{-i-r}, T^{-3r}) & 0 & -\overline{\alpha} J(T^{-i-3r}, T^{-r}) \\ -\overline{\alpha} J(T^{-i}, T^{-r}) & q & -\alpha J(T^{-i-2r}, T^{-3r}) & 0 \\ 0 & -\overline{\alpha} J(T^{-i-r}, T^{-r}) & q & -\alpha J(T^{-i-3r}, T^{-3r}) \\ -\alpha J(T^{-i}, T^{-3r}) & 0 & -\overline{\alpha} J(T^{-i-2r}, T^{-r}) & q \end{bmatrix}$$

The matrix $\mu_{L|M_0}$ is

$$\begin{bmatrix} 0 & -1 & \alpha & 0 & \overline{\alpha} \\ 0 & q & -q\alpha & 0 & -q\overline{\alpha} \\ 0 & -\overline{\alpha} & q & -\alpha J(T^{-2r}, T^{-3r}) & 0 \\ 0 & 0 & -\overline{\alpha} J(T^{-r}, T^{-r}) & q & -\alpha J(T^{-3r}, T^{-3r}) \\ 0 & -\alpha & 0 & -\overline{\alpha} J(T^{-2r}, T^{-r}) & q \end{bmatrix}$$

Outline

p-adic valuation of Jacobi Sums

- Let $j \in \mathbb{Z}$ with $j \not\equiv 0 \pmod{(q-1)}$.
- p-digit expresssion: $j = a_0 + a_1 p + a_2 p^2 + \cdots + a_{2t-1} p^{2t-1}$, $0 \leq a_i \leq p-1$.
- Write as $(a_0, a_1, \ldots, a_{2t-1})$.
- Let $s(j)$ denote the sum $\sum_i a_i$ of the p-digits of j modulo $q-1$.
- $r = \frac{q-1}{4} = (\frac{3p-1}{4}, \frac{p-3}{4}, \frac{3p-1}{4}, \frac{p-3}{4}, \ldots)$
- $3r = \frac{q-1}{4} = (\frac{p-3}{4}, \frac{3p-1}{4}, \frac{p-3}{4}, \frac{3p-1}{4}, \ldots)$
- $s(r) = s(3r) = t(p-1)$.

p-adic valuation of Jacobi Sums

- Let $j \in \mathbb{Z}$ with $j \not\equiv 0 \pmod{(q-1)}$.
- p-digit expresssion: $j = a_0 + a_1 p + a_2 p^2 + \cdots + a_{2t-1} p^{2t-1}$, $0 \leq a_i \leq p-1$.
- Write as $(a_0, a_1, \ldots, a_{2t-1})$.
- Let $s(j)$ denote the sum $\sum_i a_i$ of the p-digits of j modulo $q-1$.
- $r = \frac{q-1}{4} = (\frac{3p-1}{4}, \frac{p-3}{4}, \frac{3p-1}{4}, \frac{p-3}{4}, \ldots)$
- $3r = \frac{q-1}{4} = (\frac{p-3}{4}, \frac{3p-1}{4}, \frac{p-3}{4}, \frac{3p-1}{4}, \ldots)$
- $s(r) = s(3r) = t(p-1)$.

p-adic valuation of Jacobi Sums

- Let $j \in \mathbb{Z}$ with $j \not\equiv 0 \pmod{(q-1)}$.
- p-digit expresssion: $j = a_0 + a_1 p + a_2 p^2 + \cdots + a_{2t-1} p^{2t-1}$, $0 \leq a_i \leq p-1$.
- Write as $(a_0, a_1, \ldots, a_{2t-1})$.
- Let $s(j)$ denote the sum $\sum_i a_i$ of the p-digits of j modulo $q-1$.
- $r = \frac{q-1}{4} = (\frac{3p-1}{4}, \frac{p-3}{4}, \frac{3p-1}{4}, \frac{p-3}{4}, \ldots)$
- $3r = \frac{q-1}{4} = (\frac{p-3}{4}, \frac{3p-1}{4}, \frac{p-3}{4}, \frac{3p-1}{4}, \ldots)$
- $s(r) = s(3r) = t(p-1)$.

p-adic valuation of Jacobi Sums

- Let $j \in \mathbb{Z}$ with $j \not\equiv 0 \pmod{(q-1)}$.
- p-digit expresssion: $j = a_0 + a_1 p + a_2 p^2 + \cdots + a_{2t-1} p^{2t-1}$, $0 \leq a_i \leq p-1$.
- Write as $(a_0, a_1, \ldots, a_{2t-1})$.
- Let $s(j)$ denote the sum $\sum_i a_i$ of the p-digits of j modulo $q-1$.
- $r = \frac{q-1}{4} = (\frac{3p-1}{4}, \frac{p-3}{4}, \frac{3p-1}{4}, \frac{p-3}{4}, \ldots)$
- $3r = \frac{q-1}{4} = (\frac{p-3}{4}, \frac{3p-1}{4}, \frac{p-3}{4}, \frac{3p-1}{4}, \ldots)$
- $s(r) = s(3r) = t(p-1)$.

p-adic valuation of Jacobi Sums

- Let $j \in \mathbb{Z}$ with $j \not\equiv 0 \pmod{(q-1)}$.
- p-digit expresssion: $j = a_0 + a_1 p + a_2 p^2 + \cdots + a_{2t-1} p^{2t-1}$, $0 \leq a_i \leq p-1$.
- Write as $(a_0, a_1, \ldots, a_{2t-1})$.
- Let $s(j)$ denote the sum $\sum_i a_i$ of the p-digits of j modulo $q-1$.
- $r = \frac{q-1}{4} = (\frac{3p-1}{4}, \frac{p-3}{4}, \frac{3p-1}{4}, \frac{p-3}{4}, \ldots)$
- $3r = \frac{q-1}{4} = (\frac{p-3}{4}, \frac{3p-1}{4}, \frac{p-3}{4}, \frac{3p-1}{4}, \ldots)$
- $s(r) = s(3r) = t(p-1)$.

p-adic valuation of Jacobi Sums

- Let $j \in \mathbb{Z}$ with $j \not\equiv 0 \pmod{(q-1)}$.
- p-digit expresssion: $j = a_0 + a_1 p + a_2 p^2 + \cdots + a_{2t-1} p^{2t-1}$, $0 \leq a_i \leq p-1$.
- Write as $(a_0, a_1, \ldots, a_{2t-1})$.
- Let $s(j)$ denote the sum $\sum_i a_i$ of the p-digits of j modulo $q-1$.
- $r = \frac{q-1}{4} = (\frac{3p-1}{4}, \frac{p-3}{4}, \frac{3p-1}{4}, \frac{p-3}{4}, \ldots)$
- $3r = \frac{q-1}{4} = (\frac{p-3}{4}, \frac{3p-1}{4}, \frac{p-3}{4}, \frac{3p-1}{4}, \ldots)$
- $s(r) = s(3r) = t(p-1)$.

p-adic valuation of Jacobi Sums

- Let $j \in \mathbb{Z}$ with $j \not\equiv 0 \pmod{(q-1)}$.
- p-digit expresssion: $j = a_0 + a_1 p + a_2 p^2 + \cdots + a_{2t-1} p^{2t-1}$, $0 \leq a_i \leq p-1$.
- Write as $(a_0, a_1, \ldots, a_{2t-1})$.
- Let $s(j)$ denote the sum $\sum_i a_i$ of the p-digits of j modulo $q-1$.
- $r = \frac{q-1}{4} = (\frac{3p-1}{4}, \frac{p-3}{4}, \frac{3p-1}{4}, \frac{p-3}{4}, \ldots)$
- $3r = \frac{q-1}{4} = (\frac{p-3}{4}, \frac{3p-1}{4}, \frac{p-3}{4}, \frac{3p-1}{4}, \ldots)$
- $s(r) = s(3r) = t(p-1)$.

- By Stickelberger's Theorem and relation between Gauss sums and Jacobi sums, we know that when i, j and $i+j$ are not divisible by $q-1$ the p-adic valuation of $J(T^{-i}, T^{-j})$ is equal to

$$c(i,j) := \frac{1}{p-1}(s(i)+s(j)-s(i+j)),$$

- This valuation can be viewed as the number of carries, when adding the p-expansions of i and k, modulo $q-1$.

- By Stickelberger's Theorem and relation between Gauss sums and Jacobi sums, we know that when i, j and $i+j$ are not divisible by $q-1$ the p-adic valuation of $J(T^{-i}, T^{-j})$ is equal to

$$c(i,j) := \frac{1}{p-1}(s(i)+s(j)-s(i+j)),$$

- This valuation can be viewed as the number of carries, when adding the p-expansions of i and k, modulo $q-1$.

Outline

Main Theorem

Theorem

1. *The p-elementary divisors of* $(\mu_L)_{|M_0}$ *are* $0, 1, 1, p^t, p^t$.
2. *For* $1 \leq i \leq \frac{q-5}{4}$, *consider the two lists* $\{c(i,r), c(i+r,3r), c(i+2r,r), c(i+3r,3r)\}$ *and* $\{c(i,3r), c(i+r,r), c(i+2r,3r), c(i+3r,r)\}$ *and let* C_i *be the list that contains the smallest element. Then the four p-elementary divisors of* $(\mu_L)_{|M_i}$ *are* p^c *for* c *in* C_i.

General remarks on proof

- If X is a matrix with entries in R let $m_j(X)$ denote the multiplicity of p^j as a p-elementary divisor and let $\kappa(X)$ denote the product of the nonzero p-elementary divisors.
- $v_p(\kappa(X)) = \sum_j j m_j(X)$,
- $\kappa(L) = \kappa(\mu_L) = |K(P^*(q)|_p$ We first note that for any given power p^s, if two matrices X and X' over R are equal modulo p^s then $m_j(X) = m_j(X')$ for every $j < s$.
- $$v_p(\kappa(X)) \geq \sum_{j=0}^{s-1} j m_j(X) + s(\mathrm{rank}(X) - \sum_{j=0}^{s-1} m_j(X)).$$
- We shall obtain a lower bound for $v_p(\kappa(L))$ by looking at L modulo q.
- Then we shall see that as this lower bound coincides with the actual value of $v_p(\kappa(L))$ known from the Matrix-Tree Theorem.

General remarks on proof

- If X is a matrix with entries in R let $m_j(X)$ denote the multiplicity of p^j as a p-elementary divisor and let $\kappa(X)$ denote the product of the nonzero p-elementary divisors.
- $v_p(\kappa(X)) = \sum_j j m_j(X)$,
- $\kappa(L) = \kappa(\mu_L) = |K(P^*(q)|_p$ We first note that for any given power p^s, if two matrices X and X' over R are equal modulo p^s then $m_j(X) = m_j(X')$ for every $j < s$.
- $$v_p(\kappa(X)) \geq \sum_{j=0}^{s-1} j m_j(X) + s(\mathrm{rank}(X) - \sum_{j=0}^{s-1} m_j(X)).$$
- We shall obtain a lower bound for $v_p(\kappa(L))$ by looking at L modulo q.
- Then we shall see that as this lower bound coincides with the actual value of $v_p(\kappa(L))$ known from the Matrix-Tree Theorem.

General remarks on proof

- If X is a matrix with entries in R let $m_j(X)$ denote the multiplicity of p^j as a p-elementary divisor and let $\kappa(X)$ denote the product of the nonzero p-elementary divisors.
- $v_p(\kappa(X)) = \sum_j j m_j(X)$,
- $\kappa(L) = \kappa(\mu_L) = |K(P^*(q)|_p$ We first note that for any given power p^s, if two matrices X and X' over R are equal modulo p^s then $m_j(X) = m_j(X')$ for every $j < s$.
- $$v_p(\kappa(X)) \geq \sum_{j=0}^{s-1} j m_j(X) + s(\mathrm{rank}(X) - \sum_{j=0}^{s-1} m_j(X)).$$
- We shall obtain a lower bound for $v_p(\kappa(L))$ by looking at L modulo q.
- Then we shall see that as this lower bound coincides with the actual value of $v_p(\kappa(L))$ known from the Matrix-Tree Theorem.

General remarks on proof

- If X is a matrix with entries in R let $m_j(X)$ denote the multiplicity of p^j as a p-elementary divisor and let $\kappa(X)$ denote the product of the nonzero p-elementary divisors.
- $v_p(\kappa(X)) = \sum_j j m_j(X)$,
- $\kappa(L) = \kappa(\mu_L) = |K(P^*(q)|_p$ We first note that for any given power p^s, if two matrices X and X' over R are equal modulo p^s then $m_j(X) = m_j(X')$ for every $j < s$.
- $$v_p(\kappa(X)) \geq \sum_{j=0}^{s-1} j m_j(X) + s(\mathrm{rank}(X) - \sum_{j=0}^{s-1} m_j(X)).$$
- We shall obtain a lower bound for $v_p(\kappa(L))$ by looking at L modulo q.
- Then we shall see that as this lower bound coincides with the actual value of $v_p(\kappa(L))$ known from the Matrix-Tree Theorem.

General remarks on proof

- If X is a matrix with entries in R let $m_j(X)$ denote the multiplicity of p^j as a p-elementary divisor and let $\kappa(X)$ denote the product of the nonzero p-elementary divisors.
- $v_p(\kappa(X)) = \sum_j j m_j(X)$,
- $\kappa(L) = \kappa(\mu_L) = |K(P^*(q)|_p$ We first note that for any given power p^s, if two matrices X and X' over R are equal modulo p^s then $m_j(X) = m_j(X')$ for every $j < s$.
- $$v_p(\kappa(X)) \geq \sum_{j=0}^{s-1} j m_j(X) + s(\mathrm{rank}(X) - \sum_{j=0}^{s-1} m_j(X)).$$
- We shall obtain a lower bound for $v_p(\kappa(L))$ by looking at L modulo q.
- Then we shall see that as this lower bound coincides with the actual value of $v_p(\kappa(L))$ known from the Matrix-Tree Theorem.

General remarks on proof

- If X is a matrix with entries in R let $m_j(X)$ denote the multiplicity of p^j as a p-elementary divisor and let $\kappa(X)$ denote the product of the nonzero p-elementary divisors.
- $v_p(\kappa(X)) = \sum_j j m_j(X)$,
- $\kappa(L) = \kappa(\mu_L) = |K(P^*(q)|_p$ We first note that for any given power p^s, if two matrices X and X' over R are equal modulo p^s then $m_j(X) = m_j(X')$ for every $j < s$.
- $$v_p(\kappa(X)) \geq \sum_{j=0}^{s-1} j m_j(X) + s(\mathrm{rank}(X) - \sum_{j=0}^{s-1} m_j(X)).$$
- We shall obtain a lower bound for $v_p(\kappa(L))$ by looking at L modulo q.
- Then we shall see that as this lower bound coincides with the actual value of $v_p(\kappa(L))$ known from the Matrix-Tree Theorem.

Outline of proof of Theorem

If we work modulo q, this matrix is R-equivalent to

$$B = \begin{bmatrix} u_{11}J(T^{-i},T^{-r}) & u_{12}J(T^{-i-2r},T^{-3r}) & 0 & 0 \\ u_{21}J(T^{-i},T^{-3r}) & u_{22}J(T^{-i-2r},T^{-r}) & 0 & 0 \\ 0 & 0 & v_{11}J(T^{-i-3},T^{-3r}) & v_{12}J(T^{-i-3r},T^{-r}) \\ 0 & 0 & v_{21}J(T^{-i-r},T^{-r}) & v_{22}J(T^{-i-r},T^{-3r}), \end{bmatrix}$$

where the u_{mn} and v_{mn} are units of R.

Carries

Consider the matrix

$$C = \begin{bmatrix} c(i,r) & c(i+2r,3r) & \cdot & \cdot \\ c(i,3r) & c(i+2r,r) & \cdot & \cdot \\ \cdot & \cdot & c(i+3r,3r) & c(i+3r,r) \\ \cdot & \cdot & c(i+r,r) & c(i+r,3r) \end{bmatrix}$$

of the valuations of the nonzero entries of B. These entries are integers in the range $[0, 2t]$.

Lemma

Suppose $1 \leq i \leq q-2$ *and* $i \neq r, 2r, 3r$. *Then*

(i) $c(i,r) + c(q-1-i,r) = 2t.$

(ii) $c(i,r) + c(i+r,3r) + c(i+2r,r) + c(i+3r,3r) = 4t.$

(iii) $c(i,r) + c(i+2r,r) = c(i+2r,r) + c(i+2r,3r).$

Carries

Consider the matrix

$$C = \begin{bmatrix} c(i,r) & c(i+2r,3r) & \cdot & \cdot \\ c(i,3r) & c(i+2r,r) & \cdot & \cdot \\ \cdot & \cdot & c(i+3r,3r) & c(i+3r,r) \\ \cdot & \cdot & c(i+r,r) & c(i+r,3r) \end{bmatrix}$$

of the valuations of the nonzero entries of B. These entries are integers in the range $[0, 2t]$.

Lemma

Suppose $1 \leq i \leq q-2$ *and* $i \neq r, 2r, 3r$. *Then*

(i) $c(i,r) + c(q-1-i,r) = 2t.$

(ii) $c(i,r) + c(i+r,3r) + c(i+2r,r) + c(i+3r,3r) = 4t.$

(iii) $c(i,r) + c(i+2r,r) = c(i+2r,r) + c(i+2r,3r).$

Lower bounds on valuations

- By lemma, the diagonal sum of each 2×2 block is equal to the antidiagonal sum. This implies that

$$v_p(\kappa(\mu_{L|M_i})) \geq c(i,r)+c(i+r,3r)+c(i+2r,r)+c(i+3r,3r) = 4t.$$

- $$v_p(\kappa(\mu_{L|M_0})) \geq = 2t.$$
- Combining our bounds for $v_p(\kappa(\mu_{L|M_0}))$ and $v_p(\kappa(\mu_{L|M_i}))$ we see that

$$\begin{aligned} v_p(\kappa(\mu_L)) &= v_p(\kappa(\mu_{L|M_0})) + \sum_{i=1}^{\frac{q-5}{4}} v_p(\kappa(\mu_{L|M_i})) \\ &\geq 2t + \frac{q-5}{4}4t \\ &= (q-3)t \\ &= v_p(\kappa(\mu_L)), \end{aligned}$$

- All inequalities must be equalities!

Lower bounds on valuations

- By lemma, the diagonal sum of each 2×2 block is equal to the antidiagonal sum. This implies that

$$v_p(\kappa(\mu_{L|M_i})) \geq c(i,r)+c(i+r,3r)+c(i+2r,r)+c(i+3r,3r) = 4t.$$

- $$v_p(\kappa(\mu_{L|M_0})) \geq= 2t.$$

- Combining our bounds for $v_p(\kappa(\mu_{L|M_0}))$ and $v_p(\kappa(\mu_{L|M_i}))$ we see that

$$\begin{aligned} v_p(\kappa(\mu_L)) &= v_p(\kappa(\mu_{L|M_0})) + \sum_{i=1}^{\frac{q-5}{4}} v_p(\kappa(\mu_{L|M_i})) \\ &\geq 2t + \frac{q-5}{4}4t \\ &= (q-3)t \\ &= v_p(\kappa(\mu_L)), \end{aligned}$$

- All inequalities must be equalities!

Lower bounds on valuations

- By lemma, the diagonal sum of each 2×2 block is equal to the antidiagonal sum. This implies that

$$v_p(\kappa(\mu_{L|M_i})) \geq c(i,r)+c(i+r,3r)+c(i+2r,r)+c(i+3r,3r) = 4t.$$

- $$v_p(\kappa(\mu_{L|M_0})) \geq= 2t.$$

- Combining our bounds for $v_p(\kappa(\mu_{L|M_0}))$ and $v_p(\kappa(\mu_{L|M_i}))$ we see that

$$\begin{aligned} v_p(\kappa(\mu_L)) &= v_p(\kappa(\mu_{L|M_0})) + \sum_{i=1}^{\frac{q-5}{4}} v_p(\kappa(\mu_{L|M_i})) \\ &\geq 2t + \frac{q-5}{4}4t \\ &= (q-3)t \\ &= v_p(\kappa(\mu_L)), \end{aligned}$$

- All inequalities must be equalities!

Lower bounds on valuations

- By lemma, the diagonal sum of each 2×2 block is equal to the antidiagonal sum. This implies that

$$v_p(\kappa(\mu_{L|M_i})) \geq c(i,r)+c(i+r,3r)+c(i+2r,r)+c(i+3r,3r) = 4t.$$

- $$v_p(\kappa(\mu_{L|M_0})) \geq= 2t.$$

- Combining our bounds for $v_p(\kappa(\mu_{L|M_0}))$ and $v_p(\kappa(\mu_{L|M_i}))$ we see that

$$\begin{aligned} v_p(\kappa(\mu_L)) &= v_p(\kappa(\mu_{L|M_0})) + \sum_{i=1}^{\frac{q-5}{4}} v_p(\kappa(\mu_{L|M_i})) \\ &\geq 2t + \frac{q-5}{4}4t \\ &= (q-3)t \\ &= v_p(\kappa(\mu_L)), \end{aligned}$$

- All inequalities must be equalities!

Conclusion

The theorem now follows from the observations:

- The p-elementary divisors of each 2×2 block is determined by the miniumum p-adic valuation of an entry, and the determinant.
- Each entry in the lower block of C equal to the sum of the corresponding entry of the upper block plus $s(i) - s(i+r) + s(i+2r) - s(s+3r)$.

Conclusion

The theorem now follows from the observations:

- The p-elementary divisors of each 2×2 block is determined by the miniumum p-adic valuation of an entry, and the determinant.
- Each entry in the lower block of C equal to the sum of the corresponding entry of the upper block plus $s(i) - s(i + r) + s(i + 2r) - s(s + 3r)$.

Corollaries

Corollary

Let $m(i)$ denote the multiplicity of p^i as a p-elementary divisor of L. Then for $1 \leq i \leq 2t-1$ we have $m(i) = m(2t-i)$, and $m(0) = m(2t) + 2$.

Proof.

The corollary follows from the main theorem and part (i) of lemma on carries

We can get a formula for the p-rank (first obtained by Weng-Qiu-Wang-Xiang [2] (2007))

Corollary

$\operatorname{rank}_p L = 2(3^t - 1)(\frac{p+1}{4})^{2t}$

Outline

Example

Let $q = 9^2$. Then from [1], we have

$$K(\mathrm{Paley}(9^2)) \cong (\mathbb{Z}/20\mathbb{Z})^{40} \oplus [(\mathbb{Z}/3Z)^{16} \oplus (\mathbb{Z}/9\mathbb{Z})^{18} \oplus (\mathbb{Z}/27\mathbb{Z})^{16} \oplus (\mathbb{Z}/81\mathbb{Z})^{14}],$$

while our result shows

$$K(P^*(9^2)) \cong (\mathbb{Z}/20\mathbb{Z})^{40} \oplus [(\mathbb{Z}/3Z)^{20} \oplus (\mathbb{Z}/9\mathbb{Z})^{10} \oplus (\mathbb{Z}/27\mathbb{Z})^{20} \oplus (\mathbb{Z}/81\mathbb{Z})^{14}].$$

This is a new way to see that $P^*(9^2)$ and $\mathrm{Paley}(9^2)$ are not isomorphic.

Example

The critical group $K(P^*(3^{12}))$ is isomorphic to

$$(\mathbb{Z}/132860\mathbb{Z})^{265720} \oplus [(\mathbb{Z}/3\mathbb{Z})^{11376} \oplus (\mathbb{Z}/3^2\mathbb{Z})^{33408} \oplus (\mathbb{Z}/3^3\mathbb{Z})^{54176}$$
$$\oplus (\mathbb{Z}/3^4\mathbb{Z})^{66852} \oplus (\mathbb{Z}/3^5\mathbb{Z})^{66420} \oplus (\mathbb{Z}/3^6\mathbb{Z})^{64066}$$
$$\oplus (\mathbb{Z}/3^7\mathbb{Z})^{66420} \oplus (\mathbb{Z}/3^8\mathbb{Z})^{66852} \oplus (\mathbb{Z}/3^9\mathbb{Z})^{54176}$$
$$\oplus (\mathbb{Z}/3^{10}\mathbb{Z})^{33408} \oplus (\mathbb{Z}/3^{11}\mathbb{Z})^{11376} \oplus (\mathbb{Z}/3^{12}\mathbb{Z})^{1454}].$$

Thank you for your attention!

References

[1] David B. Chandler, Peter Sin, and Qing Xiang. “The Smith and critical groups of Paley graphs”. *J. Algebraic Combin.* 41.4 (2015), pp. 1013–1022.

[2] Guobiao Weng, Weisheng Qiu, Zeying Wang, and Qing Xiang. “Pseudo-Paley graphs and skew Hadamard difference sets from presemifields”. *Des. Codes Cryptogr.* 44.1-3 (2007), pp. 49–62.