Isomorphism problem for Cayley combinatorial objects

M. Muzychuk,

Netanya Academic College,
Israel

,
August, 2016, Novosibirsk, Russia

Combinatorial objects.

A combinatorial object over a finite set Ω is a pair (Ω, O) where O is an arbitrary relational structure on Ω.

Combinatorial objects.

A combinatorial object over a finite set Ω is a pair (Ω, O) where O is an arbitrary relational structure on Ω.

1. graphs and digraphs;

Combinatorial objects.

A combinatorial object over a finite set Ω is a pair (Ω, O) where O is an arbitrary relational structure on Ω.

1. graphs and digraphs;
2. colored digraphs;

Combinatorial objects.

A combinatorial object over a finite set Ω is a pair (Ω, O) where O is an arbitrary relational structure on Ω.

1. graphs and digraphs;
2. colored digraphs;
3. block-designs;

Combinatorial objects.

A combinatorial object over a finite set Ω is a pair (Ω, O) where O is an arbitrary relational structure on Ω.

1. graphs and digraphs;
2. colored digraphs;
3. block-designs;
4. combinatorial maps;

Combinatorial objects.

A combinatorial object over a finite set Ω is a pair (Ω, O) where O is an arbitrary relational structure on Ω.

1. graphs and digraphs;
2. colored digraphs;
3. block-designs;
4. combinatorial maps;
5. etc

Graphs

A graph is a pair $\Gamma = (\Omega, E)$ where Ω is a finite set of vertices and $E \subset \Omega \times \Omega$ is the set of (directed) edges/arcs.

Graphs

A graph is a pair $\Gamma = (\Omega, E)$ where Ω is a finite set of vertices and $E \subset \Omega \times \Omega$ is the set of (directed) edges/arcs.

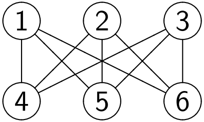
Graph Isomorphism.

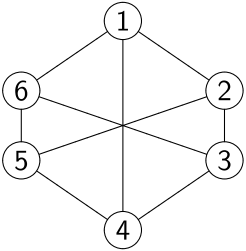
$\Gamma_1 = (\Omega_1, E_1) \cong \Gamma_2 = (\Omega_2, E_2)$ iff there exists a bijection (an isomorphism) $f : \Omega_1 \to \Omega_2$ such that

$$\forall \alpha_1, \beta_1 \in \Omega_1 : \quad (\alpha_1^f, \beta_1^f) \in E_2 \quad \Leftrightarrow \quad (\alpha_1, \beta_1) \in E_1.$$

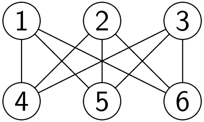
$\mathrm{Aut}(\Gamma_1)$ is the automorphism group of Γ_1.

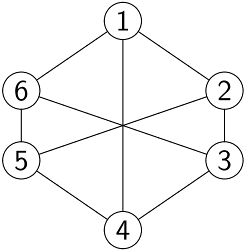
Example





Example

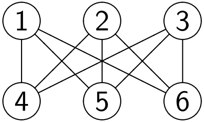


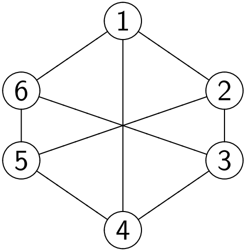


An isomorphism

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 2 & 4 & 6 \end{pmatrix}$$

Example





An isomorphism

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 2 & 4 & 6 \end{pmatrix}$$

$$\mathrm{Aut}(\Gamma) = (S_3 \times S_3).S_2.$$

The Graph Isomorphism Problem (GIP).

GIP is to find the computational complexity of the problem:

The Graph Isomorphism Problem (GIP).

GIP is to find the computational complexity of the problem:

GIP(Γ_1, Γ_2): given graphs Γ_1 and Γ_2 test whether or not $\Gamma_1 \cong \Gamma_2$.

The Graph Isomorphism Problem (GIP).

GIP is to find the computational complexity of the problem:

GIP(Γ_1, Γ_2): given graphs Γ_1 and Γ_2 test whether or not $\Gamma_1 \cong \Gamma_2$.

- Given graphs Γ_1 and Γ_2 of order n, and a bijection $f : \Omega_1 \to \Omega_2$ one can test in time $O(n^2)$ whether f is an isomorphism.

The Graph Isomorphism Problem (GIP).

GIP is to find the computational complexity of the problem:

GIP(Γ_1, Γ_2): given graphs Γ_1 and Γ_2 test whether or not $\Gamma_1 \cong \Gamma_2$.

- Given graphs Γ_1 and Γ_2 of order n, and a bijection $f : \Omega_1 \to \Omega_2$ one can test in time $O(n^2)$ whether f is an isomorphism.
- Therefore GIP$\in$**NP**.

The Graph Isomorphism Problem (GIP).

GIP is to find the computational complexity of the problem:

GIP(Γ_1, Γ_2): given graphs Γ_1 and Γ_2 test whether or not $\Gamma_1 \cong \Gamma_2$.

- Given graphs Γ_1 and Γ_2 of order n, and a bijection $f : \Omega_1 \to \Omega_2$ one can test in time $O(n^2)$ whether f is an isomorphism.
- Therefore GIP$\in$**NP**.
- An exhaustive search of all the possible bijections runs in exponential time $O(n!)$.

The Graph Isomorphism Problem (GIP).

GIP is to find the computational complexity of the problem:

GIP(Γ_1, Γ_2): given graphs Γ_1 and Γ_2 test whether or not $\Gamma_1 \cong \Gamma_2$.

- Given graphs Γ_1 and Γ_2 of order n, and a bijection $f : \Omega_1 \to \Omega_2$ one can test in time $O(n^2)$ whether f is an isomorphism.
- Therefore GIP$\in$**NP**.
- An exhaustive search of all the possible bijections runs in exponential time $O(n!)$.
- At present it is not known whether GIP$\in$**P**.

The Graph Isomorphism Problem (GIP).

GIP is to find the computational complexity of the problem:

GIP(Γ_1, Γ_2): given graphs Γ_1 and Γ_2 test whether or not $\Gamma_1 \cong \Gamma_2$.

- Given graphs Γ_1 and Γ_2 of order n, and a bijection $f : \Omega_1 \to \Omega_2$ one can test in time $O(n^2)$ whether f is an isomorphism.
- Therefore GIP$\in$**NP**.
- An exhaustive search of all the possible bijections runs in exponential time $O(n!)$.
- At present it is not known whether GIP$\in$**P**.

Theorem (L.Babai, 2015).

The isomorphism of n-vertex graphs can be tested in time $\exp(O((\log n)^c))$.

Cayley graphs

Definition

A Cayley graph over a finite group H defined by a connection set $S \subseteq H$ has H as a set of nodes and arc set

$$\mathrm{Cay}(H, S) := \{(x, y) \mid xy^{-1} \in S\}.$$

Cayley graphs

Definition

A Cayley graph over a finite group H defined by a connection set $S \subseteq H$ has H as a set of nodes and arc set

$$\mathrm{Cay}(H, S) := \{(x, y) \mid xy^{-1} \in S\}.$$

A circulant graph is a Cayley graph over a cyclic group.

Cayley graphs

Definition

A Cayley graph over a finite group H defined by a connection set $S \subseteq H$ has H as a set of nodes and arc set

$$\mathrm{Cay}(H,S) := \{(x,y) \mid xy^{-1} \in S\}.$$

A circulant graph is a Cayley graph over a cyclic group.

Proposition

1. For any $h \in H$ the permutation $h_R : x \mapsto xh$ is an automorphism of $\mathrm{Cay}(H,S)$;

Cayley graphs

Definition

A Cayley graph over a finite group H defined by a connection set $S \subseteq H$ has H as a set of nodes and arc set

$$\mathrm{Cay}(H, S) := \{(x, y) \,|\, xy^{-1} \in S\}.$$

A circulant graph is a Cayley graph over a cyclic group.

Proposition

1. For any $h \in H$ the permutation $h_R : x \mapsto xh$ is an automorphism of $\mathrm{Cay}(H, S)$;
2. The set $H_R := \{h_R \,|\, h \in H\}$ is a regular subgroup of $\mathrm{Aut}(\mathrm{Cay}(S, H))$.

Cayley graphs

Definition

A Cayley graph over a finite group H defined by a connection set $S \subseteq H$ has H as a set of nodes and arc set

$$\mathrm{Cay}(H, S) := \{(x, y) \,|\, xy^{-1} \in S\}.$$

A circulant graph is a Cayley graph over a cyclic group.

Proposition

1. For any $h \in H$ the permutation $h_R : x \mapsto xh$ is an automorphism of $\mathrm{Cay}(H, S)$;
2. The set $H_R := \{h_R \,|\, h \in H\}$ is a regular subgroup of $\mathrm{Aut}(\mathrm{Cay}(S, H))$.

Cayley objects and regular subgroups.

Definition

A transitive subgroup of $\mathrm{Sym}(\Omega)$ is called regular iff it's point stabilizer is trivial. An H-regular subgroup is a regular subgroup isomorphic to H.

Cayley objects and regular subgroups.

Definition

A transitive subgroup of $\mathrm{Sym}(\Omega)$ is called regular iff it's point stabilizer is trivial. An H-regular subgroup is a regular subgroup isomorphic to H.

Theorem (Sabidussi)

A graph is isomorphic to a Cayley graph over a group H iff its automorphism group contains an H-regular subgroup.

Cayley objects and regular subgroups.

Definition

A transitive subgroup of $\mathrm{Sym}(\Omega)$ is called regular iff it's point stabilizer is trivial. An H-regular subgroup is a regular subgroup isomorphic to H.

Theorem (Sabidussi)

A graph is isomorphic to a Cayley graph over a group H iff its automorphism group contains an H-regular subgroup.

Definition

Any combinatorial object (H, O) is called a Cayley object if it is H_R-invariant.

Theorem

Subidussi's Theorem is true for any combinatorial object.

Cayley graphs isomorphism problem

CGIP

Given two Cayley graphs Cay(H, S) and Cay(H, T). Find whether they are isomorphic.

Cayley graphs isomorphism problem

CGIP

Given two Cayley graphs $\mathrm{Cay}(H, S)$ and $\mathrm{Cay}(H, T)$. Find whether they are isomorphic.

CGIP for a group class

Given a class $\mathcal{H}$ of finite groups. Does there exists a polynomial algorithm which solves a CGIP for groups in $\mathcal{H}$.

Cayley graphs isomorphism problem

CGIP

Given two Cayley graphs $\mathrm{Cay}(H, S)$ and $\mathrm{Cay}(H, T)$. Find whether they are isomorphic.

CGIP for a group class

Given a class $\mathcal{H}$ of finite groups. Does there exists a polynomial algorithm which solves a CGIP for groups in $\mathcal{H}$.

Cayley graph automorphism group

Given a Cayley graphs $\mathrm{Cay}(H, S)$. Find generators of $\mathrm{Aut}(\mathrm{Cay}(H, S))$.

Cayley graphs isomorphism problem

CGIP

Given two Cayley graphs $\mathrm{Cay}(H, S)$ and $\mathrm{Cay}(H, T)$. Find whether they are isomorphic.

CGIP for a group class

Given a class $\mathcal{H}$ of finite groups. Does there exists a polynomial algorithm which solves a CGIP for groups in $\mathcal{H}$.

Cayley graph automorphism group

Given a Cayley graphs $\mathrm{Cay}(H, S)$. Find generators of $\mathrm{Aut}(\mathrm{Cay}(H, S))$.

Cayley graph recognition problem

Given a graph Γ of order n and a finite group $H, |H| = n$. Find whether Γ is isomorphic to a Cayley graph over H.

Cayley isomorphic graphs

Definition

Two Cayley graphs $\mathrm{Cay}(H, S)$ and $\mathrm{Cay}(H, T)$ are Cayley isomorphic, notation $\mathrm{Cay}(H, S) \cong_{Cay} \mathrm{Cay}(H, T)$, iff

$$\exists_{f \in \mathrm{Aut}(H)} \ \mathrm{Cay}(H, S)^f = \mathrm{Cay}(H, T)$$

Cayley isomorphic graphs

Definition

Two Cayley graphs $\mathrm{Cay}(H, S)$ and $\mathrm{Cay}(H, T)$ are Cayley isomorphic, notation $\mathrm{Cay}(H, S) \cong_{Cay} \mathrm{Cay}(H, T)$, iff

$$\exists_{f \in \mathrm{Aut}(H)} \ \mathrm{Cay}(H, S)^f = \mathrm{Cay}(H, T) \iff \exists_{f \in \mathrm{Aut}(H)} \ S^f = T.$$

Cayley isomorphic graphs

Definition

Two Cayley graphs $\mathrm{Cay}(H, S)$ and $\mathrm{Cay}(H, T)$ are Cayley isomorphic, notation $\mathrm{Cay}(H, S) \cong_{Cay} \mathrm{Cay}(H, T)$, iff

$$\exists_{f \in \mathrm{Aut}(H)} \ \mathrm{Cay}(H, S)^f = \mathrm{Cay}(H, T) \iff \exists_{f \in \mathrm{Aut}(H)} \ S^f = T.$$

Observation

$\mathrm{Cay}(H, S) \cong_{Cay} \mathrm{Cay}(H, T) \implies \mathrm{Cay}(H, S) \cong \mathrm{Cay}(H, T)$

Cayley isomorphic graphs

Definition

Two Cayley graphs $\mathrm{Cay}(H,S)$ and $\mathrm{Cay}(H,T)$ are Cayley isomorphic, notation $\mathrm{Cay}(H,S) \cong_{Cay} \mathrm{Cay}(H,T)$, iff

$$\exists_{f\in \mathrm{Aut}(H)} \ \mathrm{Cay}(H,S)^f = \mathrm{Cay}(H,T) \iff \exists_{f\in \mathrm{Aut}(H)} \ S^f = T.$$

Observation

$\mathrm{Cay}(H,S) \cong_{Cay} \mathrm{Cay}(H,T) \implies \mathrm{Cay}(H,S) \cong \mathrm{Cay}(H,T)$

Example

Take $H = \mathbb{Z}_2 \times \mathbb{Z}_4$, $S = H \setminus K$, $T = H \setminus C$ where K, C are order 4 subgroups, $K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, $C \cong \mathbb{Z}_4$. Then

$$\mathrm{Cay}(H,S) \cong K_{4,4} \cong \mathrm{Cay}(H,T).$$

CI-property

CI-property

CI-property

A subset $S \subseteq H$ of group H is called a CI-subset if for any subset $T \subseteq H$ the following equivalence holds

$$\mathrm{Cay}(H, S) \cong_{Cay} \mathrm{Cay}(H, T) \iff \mathrm{Cay}(H, S) \cong \mathrm{Cay}(H, T)$$

CI-property

CI-property

A subset $S \subseteq H$ of group H is called a CI-subset if for any subset $T \subseteq H$ the following equivalence holds

$$\mathrm{Cay}(H, S) \cong_{Cay} \mathrm{Cay}(H, T) \iff \mathrm{Cay}(H, S) \cong \mathrm{Cay}(H, T)$$

CIG-groups

A group H is called a CI-group with respect to graphs, CIG-group for short, if any subset of H is a CI-subset.

Isomorphism problem for circulant graphs

Ádám's conjecture (1967): $\mathbb{Z}_n$ is a CI-group for every n

Isomorphism problem for circulant graphs

Ádám's conjecture (1967): $\mathbb{Z}_n$ is a CI-group for every n

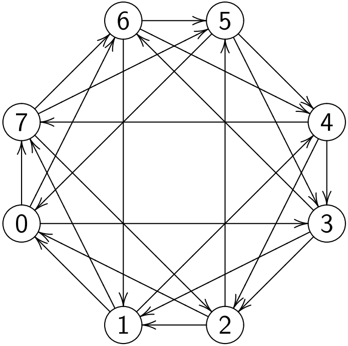
$$\mathrm{Cay}(\mathbb{Z}_n, S) \cong \mathrm{Cay}(\mathbb{Z}_n, T) \iff \exists_{m \in \mathbb{Z}_n^*} T = mS.$$

Isomorphism problem for circulant graphs

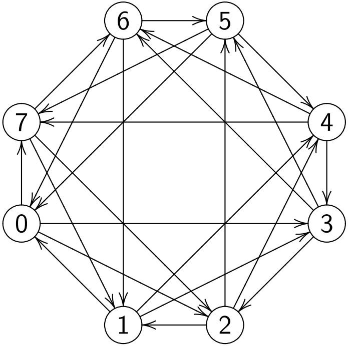
Ádám's conjecture (1967): $\mathbb{Z}_n$ is a CI-group for every n

$\mathrm{Cay}(\mathbb{Z}_n, S) \cong \mathrm{Cay}(\mathbb{Z}_n, T) \iff \exists_{m \in \mathbb{Z}_n^*} T = mS.$

Minimal Counterexample (Elspas and Turner, 1970).



$\mathrm{Cay}(\mathbb{Z}_8, \{1, 2, 5\})$



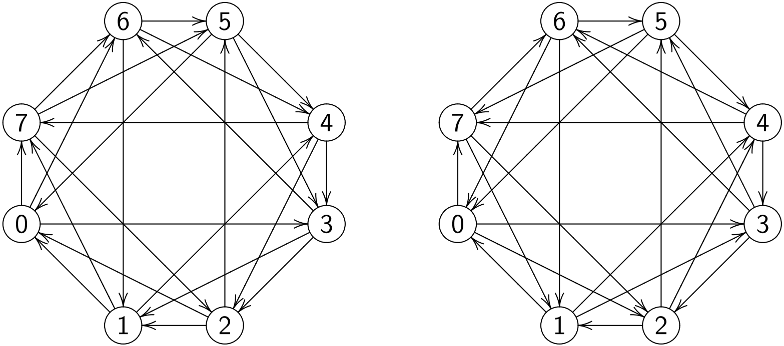
$\mathrm{Cay}(\mathbb{Z}_8, \{1, 6, 5\})$

Isomorphism problem for circulant graphs

Ádám's conjecture (1967): $\mathbb{Z}_n$ is a CI-group for every n

$\mathrm{Cay}(\mathbb{Z}_n, S) \cong \mathrm{Cay}(\mathbb{Z}_n, T) \iff \exists_{m \in \mathbb{Z}_n^*} T = mS.$

Minimal Counterexample (Elspas and Turner, 1970).



$\mathrm{Cay}(\mathbb{Z}_8, \{1, 2, 5\}) \xrightarrow{(2,6)(3,7)} \mathrm{Cay}(\mathbb{Z}_8, \{1, 6, 5\})$

Ádám's conjecture

Theorem (Alspach & Parsons and Egorov & Markov, 1979)

Ádám's conjecture fails if n is divisible by 8 or by odd square.

Ádám's conjecture

Theorem (Alspach & Parsons and Egorov & Markov, 1979)

Ádám's conjecture fails if n is divisible by 8 or by odd square.

Ádám's conjecture is true if

1. n is a prime - Elspas & Parsons;
2. $n = 2p, 3p, 4p$ - Babai 1977;
3. $n = pq, p \neq q$ are primes - C. Godsil (1977), Klin & Pöschel (1978), Alspach & Parsons (1979)

Ádám's conjecture

Theorem (Alspach & Parsons and Egorov & Markov, 1979)

Ádám's conjecture fails if n is divisible by 8 or by odd square.

Ádám's conjecture is true if

1. n is a prime - Elspas & Parsons;
2. $n = 2p, 3p, 4p$ - Babai 1977;
3. $n = pq, p \neq q$ are primes - C. Godsil (1977), Klin & Pöschel (1978), Alspach & Parsons (1979)

Pálfy's correction of Ádám's conjecture (1987):

Ádám conjecture is true if n is a square free or twice square free number.

Ádám's conjecture

Theorem (Pálfy, 1987)

Ádám's conjecture is true if $n = 4$ or $\gcd(n, \varphi(n)) = 1$.

Ádám's conjecture

Theorem (Pálfy, 1987)

Ádám's conjecture is true if $n = 4$ or $\gcd(n, \varphi(n)) = 1$.

Pálfy's result holds for ANY type of cyclic combinatorial objects.

Ádám's conjecture

Theorem (Pálfy, 1987)

Ádám's conjecture is true if $n = 4$ or $\gcd(n, \varphi(n)) = 1$.

Pálfy's result holds for ANY type of cyclic combinatorial objects.

Theorem (Muzychuk, 1995-97)

The corrected Ádám's conjecture is true.

CI-groups w.r.t. digraphs

CI-groups w.r.t. digraphs

During last 40 years the classification of CIG-groups was studied by many researches: B. Alspach, L.Babai, M.Conder, E. Dobson, B. Elspas, V.N.Egorov, P.Frankl, C. Godsil, M. Hirasaka, M. Klin, I. Kovacs, C.H.Li, Z.P. Lu, A.I.Markov, L. Nowitz, T.D. Parsons, P. Pálfy, R. Pöschel, C. Praeger, P. Spiga, G. Somlai, J. Turner.

Theorem (necessary conditions to be a CIG-group)

If H is a CI-group w.r.t. digraphs, then H is a coprime product of groups from the following list:

$$\mathbb{Z}_p^e, \quad \mathbb{Z}_4, Q_8, A_4, E(M,2), E(M,3), E(M,4).$$

where M is a direct product of elementary abelian groups of odd order.

CI-groups w.r.t. digraphs (sufficient conditions)

Theorem

The following groups are CI-groups w.r.t. digraphs

1. $\mathbb{Z}_n$ where n is square-free or twice square-free number;
2. $\mathbb{Z}_p^e, e \leq 4$ and $\mathbb{Z}_2^5$;
3. $\mathbb{Z}_p^2 \times \mathbb{Z}_q, \mathbb{Z}_p^3 \times \mathbb{Z}_q$ where p and q are distinct primes;
4. $D_{2p}, \mathbb{F}_{3p}, \mathbb{Z}_p \rtimes \mathbb{Z}_4$;
5. Q_8, A_4.

1. C.H. Li, On isomorphisms of finite Cayley graphs - survey, DM 256 (2002),
2. C.H. Li, Z.P. Lu, P. Pálfy, Further restrictions on the struture of finite CI-groups, JACO 26 (2007).

Open Problems

1. Given a prime p, find a minimal $n(p)$ such that $\mathbb{Z}_p^n$ is not a CIG-group,

Open Problems

1. Given a prime p, find a minimal $n(p)$ such that $\mathbb{Z}_p^n$ is not a CIG-group, $n(p) \geq 5$,

Open Problems

1. Given a prime p, find a minimal $n(p)$ such that $\mathbb{Z}_p^n$ is not a CIG-group, $n(p) \geq 5$, $n(p) < 2p + 3$ (G. Somlai);

Open Problems

1. Given a prime p, find a minimal $n(p)$ such that $\mathbb{Z}_p^n$ is not a CIG-group, $n(p) \geq 5$, $n(p) < 2p + 3$ (G. Somlai); $n(2) = 6$ (L. Nowitz), $6 \leq n(3) \leq 8$ (P. Spiga).

Open Problems

1. Given a prime p, find a minimal $n(p)$ such that $\mathbb{Z}_p^n$ is not a CIG-group, $n(p) \geq 5$, $n(p) < 2p + 3$ (G. Somlai); $n(2) = 6$ (L. Nowitz), $6 \leq n(3) \leq 8$ (P. Spiga).
2. Does there exists n_0 such that $\mathbb{Z}_p^{n_0}$ is not a CIG-group for any prime p?

Open Problems

1. Given a prime p, find a minimal $n(p)$ such that $\mathbb{Z}_p^n$ is not a CIG-group, $n(p) \geq 5$, $n(p) < 2p + 3$ (G. Somlai); $n(2) = 6$ (L. Nowitz), $6 \leq n(3) \leq 8$ (P. Spiga).
2. Does there exists n_0 such that $\mathbb{Z}_p^{n_0}$ is not a CIG-group for any prime p?
3. Is $\mathbb{Z}_p^5$ a CIG-group?

Open Problems

1. Given a prime p, find a minimal $n(p)$ such that $\mathbb{Z}_p^n$ is not a CIG-group, $n(p) \geq 5$, $n(p) < 2p + 3$ (G. Somlai); $n(2) = 6$ (L. Nowitz), $6 \leq n(3) \leq 8$ (P. Spiga).
2. Does there exists n_0 such that $\mathbb{Z}_p^{n_0}$ is not a CIG-group for any prime p?
3. Is $\mathbb{Z}_p^5$ a CIG-group?
4. Is a coprime product of CIG-groups a CIG-group?

Open Problems

1. Given a prime p, find a minimal $n(p)$ such that $\mathbb{Z}_p^n$ is not a CIG-group, $n(p) \geq 5$, $n(p) < 2p + 3$ (G. Somlai); $n(2) = 6$ (L. Nowitz), $6 \leq n(3) \leq 8$ (P. Spiga).
2. Does there exists n_0 such that $\mathbb{Z}_p^{n_0}$ is not a CIG-group for any prime p?
3. Is $\mathbb{Z}_p^5$ a CIG-group?
4. Is a coprime product of CIG-groups a CIG-group?
5. Is a dihedral group of a square-free order a CIG-group?

Open Problems

1. Given a prime p, find a minimal $n(p)$ such that $\mathbb{Z}_p^n$ is not a CIG-group, $n(p) \geq 5$, $n(p) < 2p + 3$ (G. Somlai);
$n(2) = 6$ (L. Nowitz), $6 \leq n(3) \leq 8$ (P. Spiga).
2. Does there exists n_0 such that $\mathbb{Z}_p^{n_0}$ is not a CIG-group for any prime p?
3. Is $\mathbb{Z}_p^5$ a CIG-group?
4. Is a coprime product of CIG-groups a CIG-group?
5. Is a dihedral group of a square-free order a CIG-group?
6. Find a polynomial algorithm which solves a recognition problem for Cayley graphs over $\mathbb{Z}_p^2$.

Non-CI groups: the cyclic case

Non-CI groups: the cyclic case

1. $n = p^2$, Alspach & Parsons, 1978;

Non-CI groups: the cyclic case

1. $n = p^2$, Alspach & Parsons, 1978;
2. $n = p^m, p > 2$, Klin & Pöschel, 1978;

Non-CI groups: the cyclic case

1. $n = p^2$, Alspach & Parsons, 1978;
2. $n = p^m, p > 2$, Klin & Pöschel, 1978;
3. $n = 2^m$, Muzychuk & Pöschel, 1999;

Non-CI groups: the cyclic case

1. $n = p^2$, Alspach & Parsons, 1978;
2. $n = p^m, p > 2$, Klin & Pöschel, 1978;
3. $n = 2^m$, Muzychuk & Pöschel, 1999;
4. arbitrary n, Evdokimov & Ponomarenko - 2003, Muzychuk, 2004.

An isomorphism problem for arbitrary cyclic combinatorial objects of orders p^2 and pq was solved by Job, Huffman and Pless in 1993,1996.

Solving sets

Definition

A subset $P \subset \mathrm{Sym}(H)$ is called a solving set for a Cayley digraph $\mathrm{Cay}(H, S)$ iff

$$\forall_{T \subseteq H} \mathrm{Cay}(H, S) \cong \mathrm{Cay}(H, T) \iff$$

$$\iff \exists_{p \in P} \mathrm{Cay}(H, S)^p = \mathrm{Cay}(H, T).$$

A solving set of minimal cardinality is called a minimal solving set. A set of permutations $P \subseteq \mathrm{Sym}(H)$ is called solving set for the group H iff it is a solving set for all Cayley digraphs over H.

Solving sets

Definition

A subset $P \subset \mathrm{Sym}(H)$ is called a solving set for a Cayley digraph $\mathrm{Cay}(H, S)$ iff

$$\forall_{T \subseteq H} \mathrm{Cay}(H, S) \cong \mathrm{Cay}(H, T) \iff$$

$$\iff \exists_{p \in P} \mathrm{Cay}(H, S)^p = \mathrm{Cay}(H, T).$$

A solving set of minimal cardinality is called a minimal solving set. A set of permutations $P \subseteq \mathrm{Sym}(H)$ is called solving set for the group H iff it is a solving set for all Cayley digraphs over H.

A group H is a CIG-group iff $\mathrm{Aut}(H)$ is a solving set for H.

"Individual" solving set

"Individual" solving set

Theorem (Babai, 1977)

A subset $S \subset H$ is a CI-subset iff any regular subgroup of $\mathrm{Aut}(\mathrm{Cay}(H, S))$ isomorphic to H is conjugate to H_R in $\mathrm{Aut}(\mathrm{Cay}(H, S))$.

"Individual" solving set

Theorem (Babai, 1977)

A subset $S \subset H$ is a CI-subset iff any regular subgroup of $\mathrm{Aut}(\mathrm{Cay}(H,S))$ isomorphic to H is conjugate to H_R in $\mathrm{Aut}(\mathrm{Cay}(H,S))$.

Definition

Let $G \leq \mathrm{Sym}(H)$ be an arbitrary group. A set $F_i, i \in I$ of H-regular subgroups of G is called an H-base of G iff any H-regular subgroup of G is conjugate in G to exactly one F_i.

"Individual" solving set

Theorem (Babai, 1977)

A subset $S \subset H$ is a CI-subset iff any regular subgroup of $\mathrm{Aut}(\mathrm{Cay}(H,S))$ isomorphic to H is conjugate to H_R in $\mathrm{Aut}(\mathrm{Cay}(H,S))$.

Definition

Let $G \leq \mathrm{Sym}(H)$ be an arbitrary group. A set $F_i, i \in I$ of H-regular subgroups of G is called an H-base of G iff any H-regular subgroup of G is conjugate in G to exactly one F_i.

Theorem

Let S be an arbitrary subset of H. Let $F_i, i \in I$ be an H-base of the group $G := \mathrm{Aut}(\mathrm{Cay}(H,S)))$. Denote by $f_i \in \mathrm{Sym}(H)$ permutations such that $H_R = F_i^{f_i}, i \in I$. Then $\cup_{i \in I} f_i \mathrm{Aut}(H)$ is a solving set for $\mathrm{Cay}(H,S)$.

Example

1. Let $H = \mathbb{Z}_8$ and $\Gamma := \mathrm{Cay}(\mathbb{Z}_8, \{1, 2, 5\})$;

Example

1. Let $H = \mathbb{Z}_8$ and $\Gamma := \mathrm{Cay}(\mathbb{Z}_8, \{1, 2, 5\})$;
2. Then $G := \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_8, \{1, 2, 5\})) = \langle \rho \rangle \rtimes \langle \tau \rangle$ where $x^\rho = x + 1, x^\tau = 5x$;

Example

1. Let $H = \mathbb{Z}_8$ and $\Gamma := \mathrm{Cay}(\mathbb{Z}_8, \{1,2,5\})$;
2. Then $G := \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_8, \{1,2,5\})) = \langle \rho \rangle \rtimes \langle \tau \rangle$ where $x^\rho = x + 1, x^\tau = 5x$;
3. G contains exactly two regular cyclic subgroups G:
   $(\mathbb{Z}_8)_R = \langle \rho \rangle$ and
   $\langle \sigma \rangle, x^\sigma = 5x + 1 \implies \sigma = (0,1,6,7,4,5,2,3)$

Example

1. Let $H = \mathbb{Z}_8$ and $\Gamma := \mathrm{Cay}(\mathbb{Z}_8, \{1, 2, 5\})$;
2. Then $G := \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_8, \{1, 2, 5\})) = \langle \rho \rangle \rtimes \langle \tau \rangle$ where $x^\rho = x + 1, x^\tau = 5x$;
3. G contains exactly two regular cyclic subgroups G:
   $(\mathbb{Z}_8)_R = \langle \rho \rangle$ and
   $\langle \sigma \rangle, x^\sigma = 5x + 1 \implies \sigma = (0, 1, 6, 7, 4, 5, 2, 3)$
4. $\langle \rho \rangle$ and $\langle \sigma \rangle$ is a $\mathbb{Z}_8$-base of G;

Example

1. Let $H = \mathbb{Z}_8$ and $\Gamma := \mathrm{Cay}(\mathbb{Z}_8, \{1, 2, 5\})$;
2. Then $G := \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_8, \{1, 2, 5\})) = \langle\rho\rangle \rtimes \langle\tau\rangle$ where $x^\rho = x + 1, x^\tau = 5x$;
3. G contains exactly two regular cyclic subgroups G:
   $(\mathbb{Z}_8)_R = \langle\rho\rangle$ and
   $\langle\sigma\rangle, x^\sigma = 5x + 1 \implies \sigma = (0, 1, 6, 7, 4, 5, 2, 3)$
4. $\langle\rho\rangle$ and $\langle\sigma\rangle$ is a $\mathbb{Z}_8$-base of G;
5. $\langle\rho\rangle = \langle\sigma\rangle^{(2,6)(3,7)} \implies \mathrm{Aut}(\mathbb{Z}_8) \cup (2, 6)(3, 7)\,\mathrm{Aut}(\mathbb{Z}_8)$ is a solving set for $\mathrm{Cay}(\mathbb{Z}_8, \{1, 2, 5\})$.

How to construct a solving set for all Cayley graphs over H

How to construct a solving set for all Cayley graphs over H

1. Find the automorphism groups of all Cayley graphs over H;

How to construct a solving set for all Cayley graphs over H

1. Find the automorphism groups of all Cayley graphs over H;
2. Too many graphs - $2^{|H|-1}$;-(

How to construct a solving set for all Cayley graphs over H

1. Find the automorphism groups of all Cayley graphs over H;
2. Too many graphs - $2^{|H|-1}$;-(
3. Different graphs may have the same automorphism group!

How to construct a solving set for all Cayley graphs over H

1. Find the automorphism groups of all Cayley graphs over H;
2. Too many graphs - $2^{|H|-1}$;-(
3. Different graphs may have the same automorphism group!

   If $|H|$ is prime, then the number of distinct automorphism groups is less than $|H|$.

How to construct a solving set for all Cayley graphs over H

1. Find the automorphism groups of all Cayley graphs over H;
2. Too many graphs - $2^{|H|-1}$;-(
3. Different graphs may have the same automorphism group!

   If $|H|$ is prime, then the number of distinct automorphism groups is less than $|H|$.
4. Klin-Pöschel approach - use the method of Schur rings to find all possible automorphism groups.

Automorphism groups of Cayley graphs

Proposition

Let $G = \text{Aut}(\text{Cay}(H, S))$ and $\mathcal{S} = \{S_0, S_1, ..., S_d\}$ be the set of orbits of the point stabilizer G_e. Then

Automorphism groups of Cayley graphs

Proposition

Let $G = \mathrm{Aut}(\mathrm{Cay}(H, S))$ and $\mathcal{S} = \{S_0, S_1, ..., S_d\}$ be the set of orbits of the point stabilizer G_e. Then

1. $S_0 = \{e\}$;

Automorphism groups of Cayley graphs

Proposition

Let $G = \mathrm{Aut}(\mathrm{Cay}(H, S))$ and $\mathcal{S} = \{S_0, S_1, ..., S_d\}$ be the set of orbits of the point stabilizer G_e. Then

1. $S_0 = \{e\}$;
2. S is a union of some orbits $S_i \in \mathcal{S}$;

Automorphism groups of Cayley graphs

Proposition

Let $G = \mathrm{Aut}(\mathrm{Cay}(H, S))$ and $\mathcal{S} = \{S_0, S_1, ..., S_d\}$ be the set of orbits of the point stabilizer G_e. Then

1. $S_0 = \{e\}$;
2. S is a union of some orbits $S_i \in \mathcal{S}$;
3. $G = \bigcap_{i=0}^{d} \mathrm{Aut}(\mathrm{Cay}(H, S_i))$

Automorphism groups of Cayley graphs

Proposition

Let $G = \mathrm{Aut}(\mathrm{Cay}(H, S))$ and $\mathcal{S} = \{S_0, S_1, ..., S_d\}$ be the set of orbits of the point stabilizer G_e. Then

1. $S_0 = \{e\}$;
2. S is a union of some orbits $S_i \in \mathcal{S}$;
3. $G = \bigcap_{i=0}^{d} \mathrm{Aut}(\mathrm{Cay}(H, S_i)) =: \mathrm{Aut}(\mathcal{S})$.

Theorem, I. Schur (1933)

The partition $\mathcal{S}$ gives rise to a subalgebra of a group algebra $\mathbb{Q}[H]$.

These special partitions will be called Schur partitions of H.

Schur rings (algebras)

Definition (Wielandt)

Let $S \subseteq H$. An element $\underline{S} := \sum_{s \in S} s \in \mathbb{Q}[H]$ is called a simple quantity. We abbreviate $\underline{\{g\}}$ as g .

Schur rings (algebras)

Definition (Wielandt)

Let $S \subseteq H$. An element $\underline{S} := \sum_{s \in S} s \in \mathbb{Q}[H]$ is called a simple quantity. We abbreviate $\underline{\{g\}}$ as $\underline{g}$.

Schur partitions

A partitition $\mathcal{S}$ of a group H is called Schur partition if it satisfies the following conditions

Schur rings (algebras)

Definition (Wielandt)

Let $S \subseteq H$. An element $\underline{S} := \sum_{s \in S} s \in \mathbb{Q}[H]$ is called a simple quantity. We abbreviate $\underline{\{g\}}$ as $\underline{g}$.

Schur partitions

A partitition $\mathcal{S}$ of a group H is called Schur partition if it satisfies the following conditions

1. $\{e\} \in \mathcal{S}$;

Schur rings (algebras)

Definition (Wielandt)

Let $S \subseteq H$. An element $\underline{S} := \sum_{s \in S} s \in \mathbb{Q}[H]$ is called a simple quantity. We abbreviate $\underline{\{g\}}$ as $\underline{g}$.

Schur partitions

A partitition $\mathcal{S}$ of a group H is called Schur partition if it satisfies the following conditions

1. $\{e\} \in \mathcal{S}$;
2. $\mathcal{S}^{(-1)} = \mathcal{S}$ where $\mathcal{S}^{(-1)} := \{S^{(-1)} \mid S \in \mathcal{S}\}$;

Schur rings (algebras)

Definition (Wielandt)

Let $S \subseteq H$. An element $\underline{S} := \sum_{s \in S} s \in \mathbb{Q}[H]$ is called a simple quantity. We abbreviate $\underline{\{g\}}$ as g .

Schur partitions

A partitition $\mathcal{S}$ of a group H is called Schur partition if it satisfies the following conditions

1. $\{e\} \in \mathcal{S}$;
2. $\mathcal{S}^{(-1)} = \mathcal{S}$ where $\mathcal{S}^{(-1)} := \{S^{(-1)} \mid S \in \mathcal{S}\}$;
3. the linear span $\underline{\mathcal{S}} := \langle \underline{S} \rangle_{S \in \mathcal{S}}$ is a subalgebra of of $\mathbb{Q}[H]$

Schur rings (algebras)

Definition (Wielandt)

Let $S \subseteq H$. An element $\underline{S} := \sum_{s \in S} s \in \mathbb{Q}[H]$ is called a simple quantity. We abbreviate $\underline{\{g\}}$ as g .

Schur partitions

A partitition $\mathcal{S}$ of a group H is called Schur partition if it satisfies the following conditions

1. $\{e\} \in \mathcal{S}$;
2. $\mathcal{S}^{(-1)} = \mathcal{S}$ where $\mathcal{S}^{(-1)} := \{S^{(-1)} \mid S \in \mathcal{S}\}$;
3. the linear span $\underline{\mathcal{S}} := \langle \underline{S} \rangle_{S \in \mathcal{S}}$ is a subalgebra of of $\mathbb{Q}[H]$

A subalgebra $\mathcal{A}$ of $\mathbb{Q}[H]$ arising in this way is called a Schur algebra/ring.

Klin-Pöschel scheme for a solution of IPCG.

Klin-Pöschel scheme for a solution of IPCG.

1. Find the set $\mathfrak{S}$ of all Schur partitions of H;

Klin-Pöschel scheme for a solution of IPCG.

1. Find the set $\mathfrak{S}$ of all Schur partitions of H;
2. For each $\mathcal{S} \in \mathfrak{S}$ find the automorphism group $G := \mathrm{Aut}(\mathcal{S})$. Then

Klin-Pöschel scheme for a solution of IPCG.

1. Find the set $\mathfrak{S}$ of all Schur partitions of H;
2. For each $\mathcal{S} \in \mathfrak{S}$ find the automorphism group $G := \mathrm{Aut}(\mathcal{S})$. Then
    1. Find an H-base of G: $F_1, ..., F_k$;

Klin-Pöschel scheme for a solution of IPCG.

1. Find the set $\mathfrak{S}$ of all Schur partitions of H;
2. For each $\mathcal{S} \in \mathfrak{S}$ find the automorphism group $G := \mathrm{Aut}(\mathcal{S})$. Then
   1. Find an H-base of G: $F_1, ..., F_k$;
   2. Find $f_i \in \mathrm{Sym}(H)$ with $H_R = F_i^{f_i}, i = 1, ..., k$;

Klin-Pöschel scheme for a solution of IPCG.

1. Find the set $\mathfrak{S}$ of all Schur partitions of H;
2. For each $\mathcal{S} \in \mathfrak{S}$ find the automorphism group $G := \mathrm{Aut}(\mathcal{S})$. Then
   1. Find an H-base of G: $F_1, ..., F_k$;
   2. Find $f_i \in \mathrm{Sym}(H)$ with $H_R = F_i^{f_i}, i = 1, ..., k$;
   3. Set $P(\mathcal{S}) := \bigcup_{i=1}^{k} f_i \, \mathrm{Aut}(H)$;

Klin-Pöschel scheme for a solution of IPCG.

1. Find the set $\mathfrak{S}$ of all Schur partitions of H;
2. For each $\mathcal{S} \in \mathfrak{S}$ find the automorphism group $G := \mathrm{Aut}(\mathcal{S})$. Then
   1. Find an H-base of G: $F_1, ..., F_k$;
   2. Find $f_i \in \mathrm{Sym}(H)$ with $H_R = F_i^{f_i}, i = 1, ..., k$;
   3. Set $P(\mathcal{S}) := \bigcup_{i=1}^{k} f_i \,\mathrm{Aut}(H)$;
3. Take $\bigcup_{\mathcal{S} \in \mathfrak{S}} P(\mathcal{S})$ as a solving set for Cayley digraphs over H.

This scheme successfully worked for $\mathbb{Z}_n$ if n is a power of an odd prime or a product of two distinct primes.

Example: solving set for circulant graphs of order 8

The following list was generated by the computer program COCO (thanks to Misha Klin).

$\{0\}$, $\{1, 2, 3, 4, 5, 6, 7\}$;
$\{0\}$, $\{1, 3, 5, 7\}$, $\{2, 6, 4\}$;
$\{0\}$, $\{1, 3, 5, 7, 2, 6\}$, $\{4\}$;
$\{0\}$, $\{1, 3, 5, 7\}$, $\{2, 6\}$, $\{4\}$;
$\{0\}$, $\{1, 3, 5, 7\}$, $\{2\}$, $\{6\}$, $\{4\}$;
$\{0\}$, $\{1, 5\}$, $\{3, 7\}$, $\{2\}$, $\{6\}$, $\{4\}$;
$\{0\}$, $\{1, 5\}$, $\{3, 7\}$, $\{2, 6\}$, $\{4\}$;
$\{0\}$, $\{1, 3\}$, $\{5, 7\}$, $\{2, 6\}$, $\{4\}$;
$\{0\}$, $\{1, 7\}$, $\{3, 5\}$, $\{2, 6\}$, $\{4\}$;
$\{0\}$, $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$, $\{5\}$, $\{6\}$, $\{7\}$;

Example

N	S-partition $\mathcal{S}$	Aut. group	cyclic bases	Solving set
1	$\{0\}, \{1,2,3,4,5,6,7\}$	S_8	$\langle\rho\rangle$	$\mathbb{Z}_8^*$
2	$\{0\}, \{1,3,5,7\}, \{2,6,4\}$	$S_2 \wr S_4$	$\langle\rho\rangle$	$\mathbb{Z}_8^*$
3	$\{0\}, \{1,3,5,7,2,6\}, \{4\}$	$S_4 \wr S_2$	$\langle\rho\rangle$	$\mathbb{Z}_8^*$
4	$\{0\}, \{1,3,5,7\}, \{2,6\}, \{4\}$	$S_2 \wr S_2 \wr S_2$	$\langle\rho\rangle$	$\mathbb{Z}_8^*$
5	$\{0\}, \{1,3,5,7\}, \{2\}, \{6\}, \{4\}$	$S_2 \wr \mathbb{Z}_4$	$\langle\rho\rangle$	$\mathbb{Z}_8^*$
6	$\{0\}, \{1,5\}, \{3,7\}, \{2\}, \{6\}, \{4\}$	$\mathbb{Z}_8.Z_2$	$\langle\rho\rangle, \langle\sigma\rangle$	$\mathbb{Z}_8^* \cup \alpha\mathbb{Z}_8^*$
7	$\{0\}, \{1,5\}, \{3,7\}, \{2,6\}, \{4\}$	$\mathbb{Z}_4 \wr S_2$	$\langle\rho\rangle$	$\mathbb{Z}_8^*$
8	$\{0\}, \{1,3\}, \{5,7\}, \{2,6\}, \{4\}$	$\mathbb{Z}_8.\mathbb{Z}_2$	$\langle\rho\rangle$	$\mathbb{Z}_8^*$
9	$\{0\}, \{1,7\}, \{3,5\}, \{2,6\}, \{4\}$	D_{16}	$\langle\rho\rangle$	$\mathbb{Z}_8^*$
10	$\{0\}, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}, \{7\}$	$\mathbb{Z}_8$	$\langle\rho\rangle$	$\mathbb{Z}_8^*$

Here $\alpha = (2,6)(3,7)$. Thus $\mathbb{Z}_8^* \cup \alpha\mathbb{Z}_8^*$ is a solving set for circulant graphs over $\mathbb{Z}_8$.

Solution of the isomorphism problem for circulant digraphs.

Solution of the isomorphism problem for circulant digraphs.

Theorem (Klin-Pöschel, 1978)

Let n be an odd prime power. Then

1. the number of Schur rings over $\mathbb{Z}_n$ is bounded by $n^C, 2 \leq C < 2.5$;

Solution of the isomorphism problem for circulant digraphs.

Theorem (Klin-Pöschel, 1978)

Let n be an odd prime power. Then

1. the number of Schur rings over $\mathbb{Z}_n$ is bounded by $n^C, 2 \leq C < 2.5$;
2. there exists an efficiently constructed solving set P_n for circulant graphs of order n s.t. $|P_n| \leq n^C \varphi(n)$

Solution of the isomorphism problem for circulant digraphs.

Theorem (Klin-Pöschel, 1978)

Let n be an odd prime power. Then

1. the number of Schur rings over $\mathbb{Z}_n$ is bounded by $n^C, 2 \leq C < 2.5$;
2. there exists an efficiently constructed solving set P_n for circulant graphs of order n s.t. $|P_n| \leq n^C \varphi(n)$

Theorem (Muzychuk-Pöschel, 1999)

Let $n = 2^m$. Then there exists an efficiently constructed solving set P_n for circulant graphs of order n s.t. $|P_n| \leq n^C \varphi(n)$.

But if n is a square-free number, the number of Schur partitions growes exponentially!

Control of H-bases

Definition

Let $H_R \leq X \leq Y \leq \operatorname{Sym} H$ be arbitrary subgroups. We say that X controls H-bases of Y, notation $X \preceq_H Y$, if there exists an H-base of X which contains an H-base of Y.

Control of H-bases

Definition

Let $H_R \leq X \leq Y \leq \operatorname{Sym} H$ be arbitrary subgroups. We say that X controls H-bases of Y, notation $X \preceq_H Y$, if there exists an H-base of X which contains an H-base of Y.

Proposition

The following are equivalent

1. $X \preceq_H Y$;
2. for any H-regular subgroup $F \leq Y$ there exists $y \in Y$ s.t. $F^y \leq X$;
3. any H-base of X contains an H-base of Y.

Control of H-bases

Definition

Let $H_R \leq X \leq Y \leq \operatorname{Sym} H$ be arbitrary subgroups. We say that X controls H-bases of Y, notation $X \preceq_H Y$, if there exists an H-base of X which contains an H-base of Y.

Proposition

The following are equivalent

1. $X \preceq_H Y$;
2. for any H-regular subgroup $F \leq Y$ there exists $y \in Y$ s.t. $F^y \leq X$;
3. any H-base of X contains an H-base of Y.

Proposition

The relation $\preceq_H$ is a partial order on the lattice $[H_R, \operatorname{Sym}(H)]$.

$\preceq_H$-minimal subgroups.

Proposition

If H is a p-group, then every $\preceq_H$-minimal subgroup of $\operatorname{Sym} H$ is a p-group too.

$\preceq_H$-minimal subgroups.

Proposition

If H is a p-group, then every $\preceq_H$-minimal subgroup of $\operatorname{Sym} H$ is a p-group too.

Example. The symmetric group $\operatorname{Sym}(8)$ has two $\prec_{\mathbb{Z}_8}$-minimal subgroups: $\mathbb{Z}_8$ and $\mathbb{Z}_8 \rtimes \langle \sigma \rangle$ where $\sigma(x) = 5x$.

$\preceq_H$-minimal subgroups.

Proposition

If H is a p-group, then every $\preceq_H$-minimal subgroup of Sym H is a p-group too.

Example. The symmetric group Sym(8) has two $\prec_{\mathbb{Z}_8}$-minimal subgroups: $\mathbb{Z}_8$ and $\mathbb{Z}_8 \rtimes \langle \sigma \rangle$ where $\sigma(x) = 5x$.

Theorem (Palfy, 1987)

If H is a cyclic group of order n, then H_R is a unique $\preceq_H$-minimal subgroup iff $n = 4$ or $\gcd(n, \varphi(n)) = 1$.

$\preceq_H$-minimal subgroups.

Proposition

If H is a p-group, then every $\preceq_H$-minimal subgroup of $\mathrm{Sym}\, H$ is a p-group too.

Example. The symmetric group Sym(8) has two $\prec_{\mathbb{Z}_8}$-minimal subgroups: $\mathbb{Z}_8$ and $\mathbb{Z}_8 \rtimes \langle \sigma \rangle$ where $\sigma(x) = 5x$.

Theorem (Palfy, 1987)

If H is a cyclic group of order n, then H_R is a unique $\preceq_H$-minimal subgroup iff $n = 4$ or $\gcd(n, \varphi(n)) = 1$.

Theorem (M., 1999)

If H is cyclic, then each $\prec_H$-minimal subgroup of $X \in [H_R, \mathrm{Sym}\, H]$ is solvable and $\pi(X) = \pi(H)$.

Isomorphism problem for cyclic combinatorial objects

Theorem (M., 2004)

The automorphism group G of a colored circulant digraph contains a nilpotent subgroup which controls cyclic bases.

Remark. The original statement is formulated in the language of Schur rings.

Isomorphism problem for cyclic combinatorial objects

Theorem (M., 2004)

The automorphism group G of a colored circulant digraph contains a nilpotent subgroup which controls cyclic bases.

Remark. The original statement is formulated in the language of Schur rings.

Theorem (M. 2004)

Let $n = p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}$ be a decomposition of n into a product of prime powers. Denote by $P_{p_i^{m_i}}$ a solving set for colored circulant digraphs over $\mathbb{Z}_{p_i^{m_i}}$.Then the set $P_n := P_{p_1^{m_1}} \times \ldots \times P_{p_k^{m_k}}$ is a solving set for colored Cayley digraphs over $\mathbb{Z}_n$. In particular, $|P_n| < n^C \varphi(n)$.

Non-graphical cyclic combinatorial objects

Theorem (M., 2011)

The set P_n is also a solving set for a semisimple cyclic codes of length n. In other words, two semisimple cyclic codes $C, D \leq \mathbb{F}_q^n$ are permutation equivalent iff there exists $g \in P_n$ s.t. $C^g = D$.

Non-graphical cyclic combinatorial objects

Theorem (M., 2011)

The set P_n is also a solving set for a semisimple cyclic codes of length n. In other words, two semisimple cyclic codes $C, D \leq \mathbb{F}_q^n$ are permutation equivalent iff there exists $g \in P_n$ s.t. $C^g = D$.

Theorem (I. Kovacs, D. Marušič and M. Muzychuk, 2015)

A cyclic group is a CI-group with respect to balanced configurations.

Non-graphical combinatorial objects: Cayley maps

Definition

A Cayley map is a triple $M(H, S, \rho)$ where

1. H is a finite group;
2. $S \subseteq H$ is a symmetric subset of H;
3. $\rho \in \mathrm{Sym}(S)$ is a rotation of S (full cycle permutation).

Non-graphical combinatorial objects: Cayley maps

Definition

A Cayley map is a triple $M(H, S, \rho)$ where

1. H is a finite group;
2. $S \subseteq H$ is a symmetric subset of H;
3. $\rho \in \mathrm{Sym}(S)$ is a rotation of S (full cycle permutation).

A rotation ρ determines a 2-cell embeding of the Cayley graph $\mathrm{Cay}(H, S)$ into a surface.

Non-graphical combinatorial objects: Cayley maps

Definition

A Cayley map is a triple $M(H, S, \rho)$ where

1. H is a finite group;
2. $S \subseteq H$ is a symmetric subset of H;
3. $\rho \in \mathrm{Sym}(S)$ is a rotation of S (full cycle permutation).

A rotation ρ determines a 2-cell embeding of the Cayley graph $\mathrm{Cay}(H, S)$ into a surface.

Example: $H = \mathbb{Z}_2 \times \mathbb{Z}_2, S = \{01, 10, 11\}, \rho = (01, 10, 11)$.

Non-graphical combinatorial objects: Cayley maps

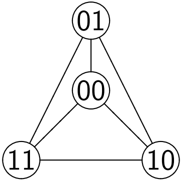
Definition

A Cayley map is a triple $M(H, S, \rho)$ where

1. H is a finite group;
2. $S \subseteq H$ is a symmetric subset of H;
3. $\rho \in \mathrm{Sym}(S)$ is a rotation of S (full cycle permutation).

A rotation ρ determines a 2-cell embeding of the Cayley graph $\mathrm{Cay}(H, S)$ into a surface.

Example: $H = \mathbb{Z}_2 \times \mathbb{Z}_2, S = \{01, 10, 11\}, \rho = (01, 10, 11)$.



Map isomorphisms

Definition

Two Cayley maps $M(H, S, \rho)$ and $M(H, S', \rho')$ are isomorphic iff there exists a bijection $f \in \mathrm{Sym}(H)$ s.t.

$$\{(h, sh, \rho(s)h) \mid s \in S, h \in H\}^f = \{(h, sh, \rho'(s)h) \mid s \in S', h \in H\}.$$

Cayley isomorphism

Two Cayley maps $M(H, S, \rho)$ and $M(H, S', \rho')$ are Cayley isomorphic iff there exists $f \in \mathrm{Aut}(H)$ s.t. $S^f = S$ and $f_S\rho = \rho' f_S$.

Problem

Classify all finite groups with CI-property with respect to maps.

CI-groups with respect to maps

Theorem (M and G. Somlai, 2015)

Let H be a CI-group with respect to Cayley maps. Then H is isomorphic to one of the following groups

1. $\mathbb{Z}_2^r \times \mathbb{Z}_m, \mathbb{Z}_4 \times \mathbb{Z}_m, \mathbb{Z}_8 \times \mathbb{Z}_m, Q_8 \times \mathbb{Z}_m$;
2. $\mathbb{Z}_m \rtimes \mathbb{Z}_{2^e}, e = 1, 2, 3$.

where m is a square-free odd number.

CI-groups with respect to maps

Theorem (M and G. Somlai, 2015)

Let H be a CI-group with respect to Cayley maps. Then H is isomorphic to one of the following groups

1. $\mathbb{Z}_2^r \times \mathbb{Z}_m, \mathbb{Z}_4 \times \mathbb{Z}_m, \mathbb{Z}_8 \times \mathbb{Z}_m, Q_8 \times \mathbb{Z}_m$;
2. $\mathbb{Z}_m \rtimes \mathbb{Z}_{2^e}, e = 1, 2, 3.$

where m is a square-free odd number.

Theorem (M and G. Somlai, 2015)

The following groups are CI with respect to Cayley maps.

$$\mathbb{Z}_m \times \mathbb{Z}_4, \mathbb{Z}_m \times \mathbb{Z}_2^r, \mathbb{Z}_m \times Q_8.$$