On the Isomorphism Problem for Cayley combinatorial objects

M. Muzychuk

Ben-Gurion University of the Negev,
Israel

July, 2018, Pilsen, Czech Republick

Combinatorial Objects

Definition (L. Babai, 1977)

Combinatorial objects are objects of a concrete category, i.e. the category with a forgetful functor to the category of sets.

Definition (P. Pálfy, 1987)

A combinatorial object on a (finite) set Ω is a relational structure, i.e. a (finite) subset of $\Omega \cup \Omega^2 \cup \Omega^3 \dots$.

Definition (N. Brand, 1991)

A finite subset O of $\Omega \cup 2^{\Omega} \cup 2^{2^{\Omega}} \dots$.

In what follows a combinatorial object will mean an ordered tuple $O := (R_1, \dots, R_d)$ where $R_i \subset \Omega \cup \Omega^2 \cup \Omega^3 \dots$.
Isomorphisms and automorphisms are defined in a natural way.

Cayley Combinatorial Objects

If $G \leq \mathrm{Sym}(\Omega)$, then $\mathrm{Obj}(G)$ stands for the set of all G-invariant combinatorial objects.

Cayley Combinatorial Objects

If $G \leq \mathrm{Sym}(\Omega)$, then $\mathrm{Obj}(G)$ stands for the set of all G-invariant combinatorial objects.

Definition

Let H be a finite group, $H_R \leq \mathrm{Sym}(H)$ its right regular representation. A combinatorial object O over H invariant under the subgroup H_R is called a Cayley combinatorial object.

Cayley Combinatorial Objects

If $G \leq \mathrm{Sym}(\Omega)$, then $\mathrm{Obj}(G)$ stands for the set of all G-invariant combinatorial objects.

Definition

Let H be a finite group, $H_R \leq \mathrm{Sym}(H)$ its right regular representation. A combinatorial object O over H invariant under the subgroup H_R is called a Cayley combinatorial object.

- Cayley (di)graphs, colored Cayley digraphs,

Cayley Combinatorial Objects

If $G \leq \mathrm{Sym}(\Omega)$, then $\mathrm{Obj}(G)$ stands for the set of all G-invariant combinatorial objects.

Definition

Let H be a finite group, $H_R \leq \mathrm{Sym}(H)$ its right regular representation. A combinatorial object O over H invariant under the subgroup H_R is called a Cayley combinatorial object.

- Cayley (di)graphs, colored Cayley digraphs,
- Translation designs,

Cayley Combinatorial Objects

If $G \leq \mathrm{Sym}(\Omega)$, then $\mathrm{Obj}(G)$ stands for the set of all G-invariant combinatorial objects.

Definition

Let H be a finite group, $H_R \leq \mathrm{Sym}(H)$ its right regular representation. A combinatorial object O over H invariant under the subgroup H_R is called a Cayley combinatorial object.

- Cayley (di)graphs, colored Cayley digraphs,
- Translation designs,
- Cayley configurations,

Cayley Combinatorial Objects

If $G \leq \mathrm{Sym}(\Omega)$, then $\mathrm{Obj}(G)$ stands for the set of all G-invariant combinatorial objects.

Definition

Let H be a finite group, $H_R \leq \mathrm{Sym}(H)$ its right regular representation. A combinatorial object O over H invariant under the subgroup H_R is called a Cayley combinatorial object.

- Cayley (di)graphs, colored Cayley digraphs,
- Translation designs,
- Cayley configurations,
- Group codes,

Cayley Combinatorial Objects

If $G \leq \mathrm{Sym}(\Omega)$, then $\mathrm{Obj}(G)$ stands for the set of all G-invariant combinatorial objects.

Definition

Let H be a finite group, $H_R \leq \mathrm{Sym}(H)$ its right regular representation. A combinatorial object O over H invariant under the subgroup H_R is called a Cayley combinatorial object.

- Cayley (di)graphs, colored Cayley digraphs,
- Translation designs,
- Cayley configurations,
- Group codes,
- Cayley maps,
- etc.

Isomorphism problem for Cayley combinatorial objects

Problem

Given a finite group H and combinatorial objects $O, O' \in \mathrm{O}bj(H_R)$, find whether they are isomorphic and (if so) find an isomorphism between them.

Isomorphism problem for Cayley combinatorial objects

Problem

Given a finite group H and combinatorial objects $O, O' \in \mathrm{O}bj(H_R)$, find whether they are isomorphic and (if so) find an isomorphism between them.

For any $O \in \mathrm{Obj}(H_R)$ and $f \in \mathrm{Aut}(H)$, the object O^f is a Cayley object over H isomorphic to O. We say that O^f is Cayley isomorphic/equivalent to O. Notation $O \cong_{Cay} O^f$.

Isomorphism problem for Cayley combinatorial objects

Problem

Given a finite group H and combinatorial objects $O, O' \in \mathrm{O}bj(H_R)$, find whether they are isomorphic and (if so) find an isomorphism between them.

For any $O \in \mathrm{Obj}(H_R)$ and $f \in \mathsf{Aut}(H)$, the object O^f is a Cayley object over H isomorphic to O. We say that O^f is Cayley isomorphic/equivalent to O. Notation $O \cong_{Cay} O^f$.

CI-property (Babai, 1977)

A Cayley object O is called a CI-object iff

$$\forall\ O' \in \mathrm{Obj}(H_R)\ \ O' \cong O \iff O' \cong_{Cay} O.$$

Isomorphism problem for Cayley combinatorial objects

Problem

Given a finite group H and combinatorial objects $O, O' \in \mathrm{O}bj(H_R)$, find whether they are isomorphic and (if so) find an isomorphism between them.

For any $O \in \mathrm{Obj}(H_R)$ and $f \in \mathsf{Aut}(H)$, the object O^f is a Cayley object over H isomorphic to O. We say that O^f is Cayley isomorphic/equivalent to O. Notation $O \cong_{Cay} O^f$.

CI-property (Babai, 1977)

A Cayley object O is called a CI-object iff

$$\forall\ O' \in \mathrm{Obj}(H_R)\ \ O' \cong O \iff O' \cong_{Cay} O.$$

Definition

Let $\mathfrak{K}$ be a class of combinatorial objects. A group H is called a CI-group w.r.t a class $\mathfrak{K}$ ($\mathfrak{K}$-CI-group for short) if any object $O \in \mathfrak{K}$ is a CI-object.

Cayley digraphs

Definition

Let $S \subseteq H$ be a subset of a finite group H. A Cayley digraph $\mathrm{Cay}(H, S)$ has H as a vertex set; two vertices $x, y \in H$ are connected iff $xy^{-1} \in S$. If $S = S^{(-1)}$ and $1_H \notin S$, then $\mathrm{Cay}(H, S)$ is a simple undirected graph.

A colored Cayley digraph is a tuple $(\mathrm{Cay}(H, S_0), \ldots, \mathrm{Cay}(H, S_d))$ where $S_0, \ldots, S_d$ are pairwise disjoint non-empty subsets of H. Notation, $\mathrm{Cay}(H, \mathcal{S}), \mathcal{S} = (S_0, \ldots, S_d)$.

Cayley digraphs

Definition

Let $S \subseteq H$ be a subset of a finite group H. A Cayley digraph $\mathrm{Cay}(H, S)$ has H as a vertex set; two vertices $x, y \in H$ are connected iff $xy^{-1} \in S$. If $S = S^{(-1)}$ and $1_H \notin S$, then $\mathrm{Cay}(H, S)$ is a simple undirected graph.

A colored Cayley digraph is a tuple $(\mathrm{Cay}(H, S_0), \ldots, \mathrm{Cay}(H, S_d))$ where $S_0, \ldots, S_d$ are pairwise disjoint non-empty subsets of H. Notation, $\mathrm{Cay}(H, \mathcal{S}), \mathcal{S} = (S_0, \ldots, S_d)$.

Isomorphism between colored Cayley digraphs

Two colored Cayley digraphs $\mathrm{Cay}(H, (S_0, \ldots, S_d))$ and $\mathrm{Cay}(H, (S_0', \ldots, S_d'))$ are isomorphic iff there exists $g \in \mathrm{Sym}(H)$ s.t. $\mathrm{Cay}(H, S_i)^g = \mathrm{Cay}(H, S_i'), i = 0, \ldots, d$. If $g \in \mathrm{Aut}(H)$, then the digraphs are called Cayley isomorphic.

IP for Cayley digraphs

IP for Cayley graphs v. 1.0

Given a group H of order n and $S, T \subseteq H$, decide whether $\mathrm{Cay}(H, S)$ and $\mathrm{Cay}(H, T)$ are isomorphic.

IP for Cayley digraphs

IP for Cayley graphs v. 1.0

Given a group H of order n and $S, T \subseteq H$, decide whether $\mathrm{Cay}(H, S)$ and $\mathrm{Cay}(H, T)$ are isomorphic.

IP for Cayley graphs v. 2.0

Given two groups H, K of order n and $S \subseteq H$, $T \subseteq K$, decide whether $\mathrm{Cay}(H, S)$ and $\mathrm{Cay}(K, T)$ are isomorphic.

IP for Cayley digraphs

IP for Cayley graphs v. 1.0

Given a group H of order n and $S, T \subseteq H$, decide whether $\mathrm{Cay}(H, S)$ and $\mathrm{Cay}(H, T)$ are isomorphic.

IP for Cayley graphs v. 2.0

Given two groups H, K of order n and $S \subseteq H$, $T \subseteq K$, decide whether $\mathrm{Cay}(H, S)$ and $\mathrm{Cay}(K, T)$ are isomorphic.

Proposition

If there exists an algorithm that solves version 1.0 for all groups in a time $f(n)$, then

1. it solves version 2.0 in $f(n^2)$;
2. it solves the Group Isomorphism Problem in a time $f(n^4)$

Isomorphism problem for circulant graphs

Ádám's conjecture (1967): $\mathbb{Z}_n$ is a CI-group w.r.t. graphs for every n.

Isomorphism problem for circulant graphs

Ádám's conjecture (1967): $\mathbb{Z}_n$ is a CI-group w.r.t. graphs for every n.

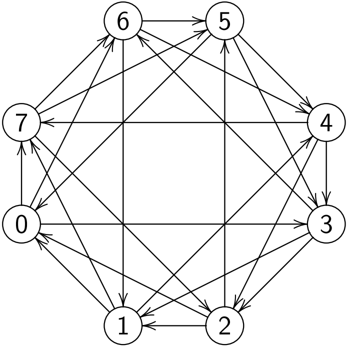
$\mathrm{Cay}(\mathbb{Z}_n, S) \cong \mathrm{Cay}(\mathbb{Z}_n, T) \iff \exists_{m \in \mathbb{Z}_n^*} T = mS.$

Isomorphism problem for circulant graphs

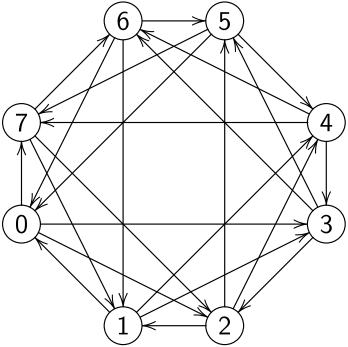
Ádám's conjecture (1967): $\mathbb{Z}_n$ is a CI-group w.r.t. graphs for every n.

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

Minimal Counterexample (Elspas and Turner, 1970).



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



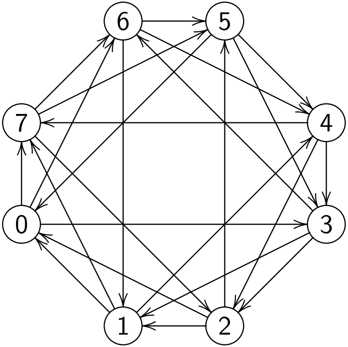
$\mathrm{Cay}(\mathbb{Z}_8, \{1, 6, 5\})$

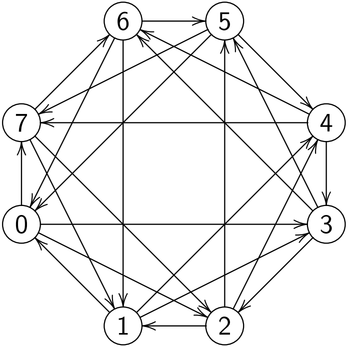
Isomorphism problem for circulant graphs

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 (M. 1995-97)

The corrected Ádám's conjecture is true.

CI-groups w.r.t. digraphs ($\vec{\mathfrak{G}}$-groups)

CI-groups w.r.t. digraphs ($\vec{\mathfrak{G}}$-groups)

During last 50 years the classification of CI-groups w.r.t. digraphs was studied by many researches: B. Alspach, L.Babai, M.Conder, E. Dobson, B. Elspas, V.N.Egorov, P.Frankl, C. Godsil, M. Hirasaka, Y.-Q. Feng, 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 CI-group w.r.t. digraphs)

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

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

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. $\mathbb{Z}_p^e, e \leq 5$;
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. $D_{2p}, \mathbb{Z}_p \rtimes \mathbb{Z}_4$;
5. $Q_8, Q_8 \times \mathbb{Z}_p, A_4$;
6. $D_{2n}, \mathbb{Z}_p^2 \times \mathbb{Z}_n, \mathbb{Z}_p^2 \times \mathbb{Z}_q \times \mathbb{Z}_n$ with $\gcd(n, \varphi(n)) = 1$

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 $\vec{\mathfrak{G}}$-group,

Open Problems

1. Given a prime p, find a minimal $n(p)$ such that $\mathbb{Z}_p^n$ is not a $\vec{\mathfrak{G}}$-group, $n(p) \geq 6$ (Y.-Q. Feng & I. Kovacs);

Open Problems

1. Given a prime p, find a minimal $n(p)$ such that $\mathbb{Z}_p^n$ is not a $\vec{\mathfrak{G}}$-group, $n(p) \geq 6$ (Y.-Q. Feng & I. Kovacs); $n(p) < 2p + 3$ (G. Somlai);

Open Problems

1. Given a prime p, find a minimal $n(p)$ such that $\mathbb{Z}_p^n$ is not a $\vec{\mathfrak{G}}$-group, $n(p) \geq 6$ (Y.-Q. Feng & I. Kovacs); $n(p) < 2p+3$ (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 $\vec{\mathfrak{G}}$-group, $n(p) \geq 6$ (Y.-Q. Feng & I. Kovacs); $n(p) < 2p + 3$ (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 $\vec{\mathfrak{G}}$-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 $\vec{\mathfrak{G}}$-group, $n(p) \geq 6$ (Y.-Q. Feng & I. Kovacs); $n(p) < 2p + 3$ (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 $\vec{\mathfrak{G}}$-group for any prime p?
3. Is $\mathbb{Z}_p^6$ a $\vec{\mathfrak{G}}$-group?

Open Problems

1. Given a prime p, find a minimal $n(p)$ such that $\mathbb{Z}_p^n$ is not a $\vec{\mathfrak{G}}$-group, $n(p) \geq 6$ (Y.-Q. Feng & I. Kovacs); $n(p) < 2p + 3$ (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 $\vec{\mathfrak{G}}$-group for any prime p?
3. Is $\mathbb{Z}_p^6$ a $\vec{\mathfrak{G}}$-group?
4. Is a coprime product of $\vec{\mathfrak{G}}$-groups a $\vec{\mathfrak{G}}$-group?

Open Problems

1. Given a prime p, find a minimal $n(p)$ such that $\mathbb{Z}_p^n$ is not a $\vec{\mathfrak{G}}$-group, $n(p) \geq 6$ (Y.-Q. Feng & I. Kovacs); $n(p) < 2p + 3$ (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 $\vec{\mathfrak{G}}$-group for any prime p?
3. Is $\mathbb{Z}_p^6$ a $\vec{\mathfrak{G}}$-group?
4. Is a coprime product of $\vec{\mathfrak{G}}$-groups a $\vec{\mathfrak{G}}$-group?
5. Is a dihedral group of a square-free order a $\vec{\mathfrak{G}}$-group?

Open Problems

1. Given a prime p, find a minimal $n(p)$ such that $\mathbb{Z}_p^n$ is not a $\vec{\mathfrak{G}}$-group, $n(p) \geq 6$ (Y.-Q. Feng & I. Kovacs); $n(p) < 2p + 3$ (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 $\vec{\mathfrak{G}}$-group for any prime p?
3. Is $\mathbb{Z}_p^6$ a $\vec{\mathfrak{G}}$-group?
4. Is a coprime product of $\vec{\mathfrak{G}}$-groups a $\vec{\mathfrak{G}}$-group?
5. Is a dihedral group of a square-free order a $\vec{\mathfrak{G}}$-group?

Non-CI groups: the cyclic case

Non-CI groups: the cyclic case

1. $n = p^2$, Alspach & Parsons, 1979;

Non-CI groups: the cyclic case

1. $n = p^2$, Alspach & Parsons, 1979;
2. $n = p^m, p > 2$, Klin & Pöschel, 1978;

Non-CI groups: the cyclic case

1. $n = p^2$, Alspach & Parsons, 1979;
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, 1979;
2. $n = p^m, p > 2$, Klin & Pöschel, 1978;
3. $n = 2^m$, Muzychuk & Pöschel, 1999;
4. arbitrary n, Evdokimov & Ponomarenko - 2003, M.-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 $\vec{\mathfrak{G}}$-group iff $\mathrm{Aut}(H)$ is a solving set for H.

"Individual" solving set

"Individual" solving set

Theorem (Babai, 1977)

A Cayley object $O \in \mathrm{Obj}(H_R)$ is CI iff any regular subgroup of $\mathrm{Aut}(O)$ isomorphic to H is conjugate to H_R in $\mathrm{Aut}(O)$.

"Individual" solving set

Theorem (Babai, 1977)

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

"Individual" solving set

Theorem (Babai, 1977)

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

Coherent closure of a Cayley graph

Coherent closure of a Cayley graph

1. A coherent closure of a Cayley digraph is an H_R-invariant association scheme (homogeneous coherent configuration) $(H, \mathcal{R} = \{R_0, ..., R_d\})$;

Coherent closure of a Cayley graph

1. A coherent closure of a Cayley digraph is an H_R-invariant association scheme (homogeneous coherent configuration) $(H, \mathcal{R} = \{R_0, ..., R_d\})$;
2. $R_i = \mathrm{Cay}(H, S_i)$ for some $S_i \subseteq H$;

Coherent closure of a Cayley graph

1. A coherent closure of a Cayley digraph is an H_R-invariant association scheme (homogeneous coherent configuration) $(H, \mathcal{R} = \{R_0, ..., R_d\})$;
2. $R_i = \mathrm{Cay}(H, S_i)$ for some $S_i \subseteq H$;
3. $S_0 = \{e\}$ and $\mathcal{S} = \{S_0, ..., S_d\}$ is a partition of H;

Coherent closure of a Cayley graph

1. A coherent closure of a Cayley digraph is an H_R-invariant association scheme (homogeneous coherent configuration) $(H, \mathcal{R} = \{R_0, ..., R_d\})$;
2. $R_i = \mathrm{Cay}(H, S_i)$ for some $S_i \subseteq H$;
3. $S_0 = \{e\}$ and $\mathcal{S} = \{S_0, ..., S_d\}$ is a partition of H;
4. S is a union of some S_i's;

Coherent closure of a Cayley graph

1. A coherent closure of a Cayley digraph is an H_R-invariant association scheme (homogeneous coherent configuration) $(H, \mathcal{R} = \{R_0, ..., R_d\})$;
2. $R_i = \mathrm{Cay}(H, S_i)$ for some $S_i \subseteq H$;
3. $S_0 = \{e\}$ and $\mathcal{S} = \{S_0, ..., S_d\}$ is a partition of H;
4. S is a union of some S_i's;
5. $\mathrm{Aut}(\mathrm{Cay}(H, S)) = \bigcap_{i=0}^{d} \mathrm{Aut}(\mathrm{Cay}(H, S_i))$

Coherent closure of a Cayley graph

1. A coherent closure of a Cayley digraph is an H_R-invariant association scheme (homogeneous coherent configuration) $(H, \mathcal{R} = \{R_0, ..., R_d\})$;
2. $R_i = \mathrm{Cay}(H, S_i)$ for some $S_i \subseteq H$;
3. $S_0 = \{e\}$ and $\mathcal{S} = \{S_0, ..., S_d\}$ is a partition of H;
4. S is a union of some S_i's;
5. $\mathrm{Aut}(\mathrm{Cay}(H, S)) = \bigcap_{i=0}^{d} \mathrm{Aut}(\mathrm{Cay}(H, S_i)) =: \mathrm{Aut}(\mathrm{Cay}(H, \mathcal{S}))$.

Coherent closure of a Cayley graph

1. A coherent closure of a Cayley digraph is an H_R-invariant association scheme (homogeneous coherent configuration) $(H, \mathcal{R} = \{R_0, ..., R_d\})$;
2. $R_i = \mathrm{Cay}(H, S_i)$ for some $S_i \subseteq H$;
3. $S_0 = \{e\}$ and $\mathcal{S} = \{S_0, ..., S_d\}$ is a partition of H;
4. S is a union of some S_i's;
5. $\mathrm{Aut}(\mathrm{Cay}(H, S)) = \bigcap_{i=0}^{d} \mathrm{Aut}(\mathrm{Cay}(H, S_i)) =: \mathrm{Aut}(\mathrm{Cay}(H, \mathcal{S}))$.

These special partitions are called S-partitions of H. They are in 1-1 correspondence with Schur rings over 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 $\underline{g}$.

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 g .

Schur partitions

A partition $\mathcal{S}$ of a group H is called an S-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 partition $\mathcal{S}$ of a group H is called an S-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 g .

Schur partitions

A partition $\mathcal{S}$ of a group H is called an S-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 partition $\mathcal{S}$ of a group H is called an S-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 $\mathbb{Q}[H]$

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 partition $\mathcal{S}$ of a group H is called an S-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 $\mathbb{Q}[H]$

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 S-partitions of H;

Klin-Pöschel scheme for a solution of IPCG.

1. Find the set $\mathfrak{S}$ of all S-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 S-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 S-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 S-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 S-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: $F_1, \ldots, F_k$;
   2. Find $f_i \in \mathrm{Sym}(H)$ with $H_R = F_i^{f_i}, i = 1, \ldots, k$;
   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 colored circulant digraphs 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 colored circulant digraphs 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 colored circulant digraphs of order n s.t. $|P_n| \leq n^C \varphi(n)$.

But if n is a square-free number, the number of S-partitions is not polynomial in n.

Control of H-bases

Definition

Let $H_R \le X \le Y \le \operatorname{Sym} H$ be arbitrary subgroups. We say that X controls H-bases of Y, notation $X \preceq_H Y$, if 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 any H-base of X 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. $F^y \leq X$;

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 any H-base of X 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. $F^y \leq X$;

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 $\mathrm{Sym}\, H$ 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 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 $\mathrm{Sym}\, H$ is a p-group too.

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

Theorem (Pálfy, 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 $\operatorname{Sym} H$ 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 $\sigma(x) = 5x$.

Theorem (Pálfy, 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 $X \in [H_R, \operatorname{Sym} H]$ is solvable and $\pi(X) = \pi(H)$.

Isomorphism problem for circulant graphs

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 circulant graphs

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, $|P_n| < n^C \varphi(n)$.

Isomorphism problem for cyclic combinatorial objects

Denote $\overline{n} := \{0, ..., n-1\} \subseteq \mathbb{Z}$, $c = (0, 1, 2, ..., n-1)$, $C = \langle c \rangle$.

Isomorphism problem for cyclic combinatorial objects

Denote $\overline{n} := \{0, ..., n-1\} \subseteq \mathbb{Z}$, $c = (0, 1, 2, ..., n-1)$, $C = \langle c \rangle$.

Problem

Given two cyclic combinatorial objects $O, O' \in \mathrm{O}bj(C)$, find whether they are isomorphic and (if so) find an isomorphism between them.

Isomorphism problem for cyclic combinatorial objects

Denote $\overline{n} := \{0, ..., n-1\} \subseteq \mathbb{Z}$, $c = (0, 1, 2, ..., n-1)$, $C = \langle c \rangle$.

Problem

Given two cyclic combinatorial objects $O, O' \in \mathrm{O}bj(C)$, find whether they are isomorphic and (if so) find an isomorphism between them.

Let $n = p_1 \cdots p_k$ be a prime decomposition of $n, p_1 \geq ... \geq p_k$.
Define a subgroup W_n inductively:

$$W_n := \begin{cases} AGL_1(p_k) & \text{if } k = 1; \\ AGL_1(p_k) \wr W_{n/p_k} & \text{if } k > 1. \end{cases}$$

The action of $AGL_1(p_k) \wr W_{n/p_k}$ on $\overline{n}$ is defined via the bijection:

$$\overline{n} \ni i \leftrightarrow (q, r) \in \overline{p_k} \times \overline{n/p_k}, \text{ where } i = q\frac{n}{p_k} + r, 0 \leq r < n/p_k.$$

Isomorphism problem for cyclic combinatorial objects

Theorem (M. & Ponomarenko, 2017)

The group W_n is a solving set for all C-invariant combinatorial objects. In other words, $O, O' \in \mathrm{O}bj(C)$ are isomorphic iff there exists an element $f \in W_n$ s.t. $O^f = O'$.

Isomorphism problem for cyclic combinatorial objects

Theorem (M. & Ponomarenko, 2017)

The group W_n is a solving set for all C-invariant combinatorial objects. In other words, $O, O' \in \mathrm{O}bj(C)$ are isomorphic iff there exists an element $f \in W_n$ s.t. $O^f = O'$.

Unfortunately, $|W_n|$ is not polynomial in n.

Isomorphism problem for cyclic combinatorial objects

Theorem (M. & Ponomarenko, 2017)

The group W_n is a solving set for all C-invariant combinatorial objects. In other words, $O, O' \in \mathrm{O}bj(C)$ are isomorphic iff there exists an element $f \in W_n$ s.t. $O^f = O'$.

Unfortunately, $|W_n|$ is not polynomial in n. But the group W_n is solvable. This yields the following result.

Theorem (M. & Ponomarenko 2017)

The isomorphism of any two cyclic objects can be tested in time polynomial in their sizes.

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/symmetric 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

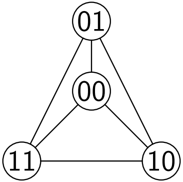
Definition

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.

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