Cayley schemes and Schur rings

M. Muzychuk

Ben-Gurion University of the Negev,
Israel

10th PhD Summer School in Discrete Mathematics , Rogla
Slovenia, June 2022

Thin (regular) schemes.

Definition

A scheme $(\Omega, \mathcal{S})$ is called thin if $n_S = 1$ for each $S \in \mathcal{S}$.

Thin (regular) schemes.

Definition

A scheme $(\Omega, \mathcal{S})$ is called thin if $n_S = 1$ for each $S \in \mathcal{S}$.

Proposition

A scheme $(\Omega, \mathcal{S})$ is thin iff $\mathcal{S}$ is a regular subgroup of $\mathrm{Sym}(\Omega)$.

Thin (regular) schemes.

Definition

A scheme $(\Omega, \mathcal{S})$ is called thin if $n_S = 1$ for each $S \in \mathcal{S}$.

Proposition

A scheme $(\Omega, \mathcal{S})$ is thin iff $\mathcal{S}$ is a regular subgroup of $\mathrm{Sym}(\Omega)$.

Proposition

The schemes $(H, H_R), (H, H_L)$ are pairwise isomorphic thin schemes. They commute elementwise and

$$\begin{gathered}
\mathrm{Inv}(H_R) = H_L,\ \mathrm{Inv}(H_L) = H_R, \\
\mathrm{Aut}(H_L) = H_R, \mathrm{Aut}(H_R) = H_L, \\
\mathrm{Iso}(H_L) = H_R\,\mathrm{Aut}(H),\ \mathrm{Iso}(H_R) = H_L\,\mathrm{Aut}(H).
\end{gathered}$$

Cayley schemes

Defintion

An association scheme which is a fusion of $(H; H_L)$ is called a Cayley scheme over H.

If $(H, \mathcal{S})$ is a Cayley scheme over H, then each basic relation $S \in \mathcal{S}$ is a Cayley graph with generating set $Se = \{h \in H \,|\, (h, e) \in S\}$. Notice that $Se = (eS)^{(-1)} = \{h^{-1} \,|\, h \in Se\}$.

Proposition. Let $(H, \mathcal{R})$ be a Cayley scheme. Then the set

$\mathcal{S} := \{Re \,|\, R \in \mathcal{R}\}$ is a partition of H with the following properties

- $\{e\} \in \mathcal{S}$;
- $S \in \mathcal{S} \implies S^{(-1)} \in \mathcal{S}$;
- for any triple $R, S, T \in \mathcal{S}$ and any $t \in T$ the number $c_{RS}^T := |S \cap R^{(-1)}t|$ does not depend on a choice $t \in T$.

Cayley schemes and Schur partitions

Defintion. A partition $\mathcal{S}$ of H is called Schur partition iff

it satifies the above conditions, that is

- $\{e\} \in \mathcal{S}$;
- $S \in \mathcal{S} \implies S^{(-1)} \in \mathcal{S}$;
- for any triple $R, S, T \in \mathcal{S}$ and any $t \in T$ the number $c_{RS}^{T} := |S \cap R^{(-1)}t|$ does not depend on a choice $t \in T$.

Notice that $|S \cap R^{(-1)}t| = \{(x, y) \in R \times S \mid xy = t\}$.

Proposition

Let $\mathcal{S}$ be a partition of H. A partition

$$\mathrm{Cay}(H, \mathcal{S}) := \{\mathrm{Cay}(H, S) \mid S \in \mathcal{S}\}$$

is an association scheme iff $\mathcal{S}$ is a Schur partition.

Schur partitions and Schur rings (algebras)

Notation

- $R[H]$ the group algebra over a unitary ring R.
- If $x = \sum_{h \in H} x_h h \in R[H], y = \sum_{h \in H} y_h h \in R[H]$, then their group product (convolution) is $xy = \sum_{h,f \in H} x_h y_f (hf)$;
- Schur-Hadamard product $x \circ y = \sum_{h \in H} (x_h y_h) h$;
- $\circ$-idemotents have a form $\underline{S} := \sum_{s \in S} s$ where $S \subseteq H$, they are called simple quantities;
- $\underline{\{h\}}$ is abbreviated as h;
- if $\mathcal{S} \vdash H$, then $\underline{\mathcal{S}} := \langle \underline{S} \,|\, S \in \mathcal{S} \rangle$;
- for each $m \in \mathbb{Z}$ and $x \in R[H]$ we denote $x^{(m)} := \sum_{h \in H} x_h h^m$;

Schur partitions and Schur rings (algebras)

Proposition

Let $\mathcal{S} \vdash H$ be s.t. $\{e\} \in \mathcal{S}$ and $\mathcal{S}^{(-1)} = \mathcal{S}$. Then $\mathcal{S}$ is a Schur partition iff the linear span $\langle \underline{\mathcal{S}} \rangle$ is a subalgebra of $\mathbb{Q}[H]$.

Definition

A subalgebra $\mathcal{A} \leq \mathbb{Q}[H]$ is called a Schur ring/algebra over H if there exists a Schur partition $\mathcal{S} \vdash H$ such that $\mathcal{A} = \langle \underline{\mathcal{S}} \rangle$. The elements of $\mathcal{S}$ are called basic sets of $\mathcal{A}$ while the elements of $\mathcal{S}^{\cup}$ are called $\mathcal{A}$-(sub)sets.

Theorem

A vector space $\mathcal{A} \leq \mathbb{Q}[H]$ is a Schur ring iff $e, \underline{H} \in \mathcal{A}$ and $\mathcal{A}$ closed w.r.t. convolution, $\circ$ and ${}^{(-1)}$.

Generating S-ring

Proposition

If $\mathcal{A} = \langle \underline{\mathcal{S}} \rangle$ and $\mathcal{B} = \langle \underline{\mathcal{T}} \rangle$ are S-rings, then

- $\mathcal{A} \subseteq \mathcal{B} \iff \mathcal{S} \sqsubseteq \mathcal{T}$;
- $\mathcal{A} \cap \mathcal{B} = \underline{\mathcal{S} \cap \mathcal{T}} = \langle \underline{\mathcal{S} \wedge \mathcal{T}} \rangle$

The intersection of all S-rings containing elements $x, y, z, \ldots \in \mathbb{Q}[H]$ is denoted as $\langle\langle x, y, z, \ldots \rangle\rangle$.

Theorem

Let $S \subseteq H$ be an arbitrary subset. Let $\mathcal{A} = \langle\langle \underline{S} \rangle\rangle$ be a Schur ring generated by $\underline{S}$ and $\mathcal{S}$ the corresponding S-paritition (that is $\langle \underline{\mathcal{S}} \rangle = \mathcal{A}$). Then $\langle\langle \mathrm{Cay}(H, S) \rangle\rangle = \mathrm{Cay}(H, \mathcal{S})$ and $S \in \mathcal{S}^{\cup}$.

Generating S-ring

Proposition (Schur-Wielandt principle)

Let $f : \mathbb{Q} \to \mathbb{Q}$ be an arbitrary function. Then for any element $x = \sum_{h \in H} x_h h$ of an S-ring $\mathcal{A}$ the element $f[x] := \sum_{h \in H} f(x_h) h$ also belongs to $\mathcal{A}$.

In the case when $f = \delta_r, r \in \mathbb{Q}$ (the Kronecker delta-function) we obtain the following

Corollary

Let $\mathcal{A}$ be an S-ring over H and $x = \sum_{h \in H} x_h h$. If $x \in \mathcal{A}$ then for any $r \in Q$ the simple quantity $\delta_r[x] = \underline{\{h \in H \,|\, x_h = r\}}$ belongs to $\mathcal{A}$ (equivalently, $\{h \in H \,|\, x_h = r\}$ is an $\mathcal{A}$-subset).

Computation of $\langle\langle \underline{S} \rangle\rangle$. A concrete example: $S = \{1, 4, 7\} \subseteq \mathbb{Z}_8$.

It's better to write $\underline{S} = \underline{\{1, 4, 7\}}$ as $\underline{S} = c + c^4 + c^7$ where $c^8 = 1$.

Computation of $\langle\langle \underline{S} \rangle\rangle$. A concrete example: $S = \{1,4,7\} \subseteq \mathbb{Z}_8$.

It's better to write $\underline{S} = \underline{\{1,4,7\}}$ as $\underline{S} = c + c^4 + c^7$ where $c^8 = 1$.
Then $\underline{S}^2 = 3c^0 + c^2 + c^6 + 2c^5 + 2c^3 \in \langle\langle \underline{S} \rangle\rangle \implies 1 = c^0 \in \langle\langle \underline{S} \rangle\rangle$,

Computation of $\langle\langle \underline{S} \rangle\rangle$. A concrete example: $S = \{1, 4, 7\} \subseteq \mathbb{Z}_8$.

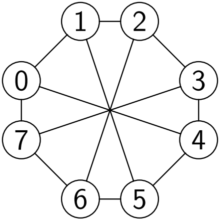
It's better to write $\underline{S} = \underline{\{1, 4, 7\}}$ as $\underline{S} = c + c^4 + c^7$ where $c^8 = 1$.
Then $\underline{S}^2 = 3c^0 + c^2 + c^6 + 2c^5 + 2c^3 \in \langle\langle \underline{S} \rangle\rangle \implies 1 = c^0 \in \langle\langle \underline{S} \rangle\rangle$,
$\underline{T} := c^5 + c^3, \underline{R} = c^2 + c^6 \in \langle\langle \underline{S} \rangle\rangle \implies \underline{R}^2 = 2c^0 + 2c^4 \in \langle\langle \underline{S} \rangle\rangle$

Computation of $\langle\langle \underline{S} \rangle\rangle$. A concrete example: $S = \{1, 4, 7\} \subseteq \mathbb{Z}_8$.

It's better to write $\underline{S} = \underline{\{1, 4, 7\}}$ as $\underline{S} = c + c^4 + c^7$ where $c^8 = 1$.
Then $\underline{S}^2 = 3c^0 + c^2 + c^6 + 2c^5 + 2c^3 \in \langle\langle \underline{S} \rangle\rangle \implies 1 = c^0 \in \langle\langle \underline{S} \rangle\rangle$,
$\underline{T} := c^5 + c^3, \underline{R} = c^2 + c^6 \in \langle\langle \underline{S} \rangle\rangle \implies \underline{R}^2 = 2c^0 + 2c^4 \in \langle\langle \underline{S} \rangle\rangle$
$\implies c^4 \in \langle\langle \underline{S} \rangle\rangle \implies \langle\langle \underline{S} \rangle\rangle = \langle c^0, c + c^7, c^2 + c^6, c^3 + c^5 \rangle$.

Computation of $\langle\!\langle \underline{S} \rangle\!\rangle$. A concrete example: $S = \{1, 4, 7\} \subseteq \mathbb{Z}_8$.

It's better to write $\underline{S} = \underline{\{1, 4, 7\}}$ as $\underline{S} = c + c^4 + c^7$ where $c^8 = 1$.
Then $\underline{S}^2 = 3c^0 + c^2 + c^6 + 2c^5 + 2c^3 \in \langle\!\langle \underline{S} \rangle\!\rangle \implies 1 = c^0 \in \langle\!\langle \underline{S} \rangle\!\rangle$,
$\underline{T} := c^5 + c^3, \underline{R} = c^2 + c^6 \in \langle\!\langle \underline{S} \rangle\!\rangle \implies \underline{R}^2 = 2c^0 + 2c^4 \in \langle\!\langle \underline{S} \rangle\!\rangle$
$\implies c^4 \in \langle\!\langle \underline{S} \rangle\!\rangle \implies \langle\!\langle \underline{S} \rangle\!\rangle = \langle c^0, c + c^7, c^2 + c^6, c^3 + c^5 \rangle$.
Thus $\langle\!\langle \mathrm{Cay}(\mathbb{Z}_8, \{1, 4, 7\}) \rangle\!\rangle = \mathrm{Cay}(\mathbb{Z}_8, \{\{0\}, \{1, 7\}, \{2, 6\}, \{3, 5\}\})$.
In other words, the right hand side is the coherent closure of the graph depictered below.



$\mathrm{Cay}(\mathbb{Z}_8, \{1, 4, 7\})$

Examples: Schur partitions over the group $\mathbb{Z}_8$

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

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

Further examples

Proposition

Let $F \leq \mathrm{Aut}(H) \leq \mathrm{Sym}(H)$. Then the orbit partition $\mathrm{Orb}(F, H)$ is a Schur partition. The corresponding S-ring coincides with $\mathbb{Q}[H]^F$.

Partial cases

- $F = \mathrm{Inn}(H) \implies \mathbf{Z}(\mathbb{Q}[H])$ is an S-ring. Its basic sets coincide with conjugacy classes of H. Fusion S-rings of $\mathbf{Z}(\mathbb{Q}[H])$ are in one-to-one correspondence with supercharacters introduced recently by Isaacs et. el.
- let R be a ring, $H = (R, +)$ and $K \leq R^\times$. The corresponding S-ring $\mathbb{Q}[H]^K$ is called cyclotomic. Its basic sets have a form $Kr, r \in R$.

Further examples

Proposition (subgroup S-rings)

$\mathcal{L}$ be a sublattice of a subgroup lattice of H which contains $\{e\}$ and H. If any two subgroup $K, L \in \mathcal{L}$ are permutable, then $\langle \underline{L} \rangle_{L \in \mathcal{L}}$ is a Schur ring.

Hecke algebras

Let $K \leq H$ be an abritrary subgroup and $\mathcal{S} = \{KhK \mid h \in H\}$ be a partition of H into double cosets of K. The linear span $\underline{\mathcal{S}}$ is known as Hecke algebra w.r.t. K. It is closed w.r.t. $^{(-1)}, \circ, \cdot$ but doesn't contain 1.

Properties of S-rings

Proposition

Let $\mathcal{S}$ be a Schur partition of H and $\mathrm{Cay}(H, \mathcal{S})$ the corresponding Cayley scheme. Then $\mathrm{Cay}(H, \mathcal{S})^{\cup} = \mathrm{Cay}(H, \mathcal{S}^{\cup})$ and

- the set $\mathcal{S}^{\cup}$ is closed w.r.t. boolean operations;
- $\{e\}, H \in \mathcal{S}^{\cup}$;
- $(\mathcal{S}^{\cup})^* = \mathcal{S}^{\cup}$;
- $\mathcal{S}$ is closed w.r.t. group product;
- $S \in \mathcal{S}^{\cup} \implies \langle S \rangle \in \mathcal{S}^{\cup}$;

A relation $E = \mathrm{Cay}(H, S), S \in \mathcal{S}^{\cup}$ is an equivalence iff S is a subgroup of H.

Definition

A subgroup $F \leq H$ is called an $\mathcal{A}$-subgroup if $\underline{F} \in \mathcal{A}$. An S-ring is called primitive iff $\{e\}, H$ are the only $\mathcal{A}$-subgroups.

Schurian S-rings

Theorem (Schur)

Let H be a group and $H_R \leq G \leq \mathrm{Sym}(H)$. Then the orbits of G_e form an S-partition.

Proof.

Set $\mathcal{S} := \mathrm{Inv}(G)$. Then $H_R \leq G \implies \mathcal{S} \sqsubseteq \mathrm{Inv}(H_R) = H_L$. Thus $\mathcal{S}$ is a Cayley scheme. Hence $e\mathcal{S} = \{eS \mid S \in \mathcal{S}\}$ is a Schur partition of H. Since $\mathcal{S}$ is schurian, $e\mathcal{S} = \mathrm{Orb}(G_e, H)$. $\square$

An S-partition is called Schurian if it has a form $\mathrm{Orb}(G_e, H)$ for some G, $H_R \leq G \leq \mathrm{Sym}(H)$

Subgroup factorization and Schur rungs

Theorem (Schur)

Let $G = AH$ be a factorization into a subgroup product with $A \cap H = \{e\}$. Then the subalgebra

$$\mathbf{C}_{\mathbb{Q}[H]}(\underline{A}) := \{x \in \mathbb{Q}[H] \,|\, x\underline{A} = \underline{A}x\}.$$

is a Schur ring the basic sets of which have the form $AhA \cap H$.

A concrete example

A simple group $PSL_3(2)$ has a decomposition into a product AH where $A \cong D_8$ and $H \cong F_{21}$. The corresponding S-ring over H has rank six and its Cayley scheme is isomorphic to a flag scheme of a projective plane of order 2.

Isomorphisms between Schur rings

Let $\mathcal{S} \vdash H$ and $\mathcal{T} \vdash K$ be two S-partitions of groups H and K resp. The S-rings $\mathcal{A} := \langle \underline{\mathcal{S}} \rangle, \mathcal{B} := \langle \underline{\mathcal{T}} \rangle$ are

- Cayley isomorphic, notation $\cong_{Cay}$, if there exists a group isomorphism $f : H \to K$ s.t. $\mathcal{S}^f = \mathcal{T}$;
- combinatorially isomorphic if the schemes $\mathrm{Cay}(H, \mathcal{S})$ and $\mathrm{Cay}(K, \mathcal{T})$ are isomorphic (as schemes);
- algebraically isomorphic if the schemes $\mathrm{Cay}(H, \mathcal{S})$ and $\mathrm{Cay}(K, \mathcal{T})$ are algebraically isomorphic.

In what follows we abbreviate

$$\mathrm{Aut}(\mathcal{A}) := \mathrm{Aut}(\mathrm{Cay}(H, \mathcal{S})), \mathrm{Iso}(\mathcal{A}) := \mathrm{Iso}(\mathrm{Cay}(H, \mathcal{S})).$$

Isomorphisms between S-rings

Proposition

$\mathcal{A} \cong_{alg} \mathcal{B}$ iff there exists a bijection $f : \mathcal{S} \to \mathcal{T}$ s.t. $c_{PQ}^{R} = c_{P^f Q^f}^{R^f}$.

Proposition

$\mathcal{A} \cong_{com} \mathcal{B}$ iff there exists a bijection $f : H \to K$ s.t. $(e_H)^f = e_K$ and

- for any $h \in H$ and $S \in \mathcal{S}$ it holds that $(hS)^f = h^f S^f$;
- $\mathcal{S}^f = \mathcal{T}$;
- $f|_{\mathcal{S}}$ is an algebraic isomorphism between $\mathcal{A}$ and $\mathcal{B}$

$$\mathcal{A} \cong_{Cay} \mathcal{B} \Rightarrow \mathcal{A} \cong \mathcal{B} \Rightarrow \mathcal{A} \cong_{alg} \mathcal{B}.$$
$$\mathcal{A} \cong_{Cay} \mathcal{B} \not\Leftarrow \mathcal{A} \cong \mathcal{B} \not\Leftarrow \mathcal{A} \cong_{alg} \mathcal{B}.$$

Application to Cayley graph isomorphism problem.

- Let $f : \mathrm{Cay}(H, S) \to \mathrm{Cay}(H, T)$ be an isomorphism s.t. $f(e) = e$;
- then $\mathcal{S}^f = \mathcal{T}$ where $\mathcal{S}$ and $\mathcal{T}$ are S-partitions generated by $\underline{S}$ and $\underline{T}$ resp.;
- f^* is an algebraic isomorphism between S-rings $\underline{\mathcal{S}}$ and $\underline{\mathcal{T}}$.

Klin-Pöschel approach.

How to solve GIP for Cayley graphs over a finite group H.

Klin-Pöschel approach.

How to solve GIP for Cayley graphs over a finite group H.

- Find all S-rings over H.

Klin-Pöschel approach.

How to solve GIP for Cayley graphs over a finite group H.

- Find all S-rings over H. Let $\mathcal{A}_1, ..., \mathcal{A}_N$ be the complete list of them;

Klin-Pöschel approach.

How to solve GIP for Cayley graphs over a finite group H.

- Find all S-rings over H. Let $\mathcal{A}_1, ..., \mathcal{A}_N$ be the complete list of them;
- For all pairs i, j find the set Φ_{ij} of algebraic isomorphisms between them;

Klin-Pöschel approach.

How to solve GIP for Cayley graphs over a finite group H.

- Find all S-rings over H. Let $\mathcal{A}_1, ..., \mathcal{A}_N$ be the complete list of them;
- For all pairs i, j find the set Φ_{ij} of algebraic isomorphisms between them;
- For each $\phi \in \Phi_{ij}$ find a combinatorial isomorphism f between $\mathcal{A}_i$ and $\mathcal{A}_j$ s.t. $f^* = \phi$ (if such f exists);

Klin-Pöschel approach.

How to solve GIP for Cayley graphs over a finite group H.

- Find all S-rings over H. Let $\mathcal{A}_1, \ldots., \mathcal{A}_N$ be the complete list of them;
- For all pairs i, j find the set Φ_{ij} of algebraic isomorphisms between them;
- For each $\phi \in \Phi_{ij}$ find a combinatorial isomorphism f between $\mathcal{A}_i$ and $\mathcal{A}_j$ s.t. $f^* = \phi$ (if such f exists);
- Collect all permutations f found on the previous stage. Let P be the set of all those permutations.

Klin-Pöschel approach.

How to solve GIP for Cayley graphs over a finite group H.

- Find all S-rings over H. Let $\mathcal{A}_1, ..., \mathcal{A}_N$ be the complete list of them;
- For all pairs i, j find the set Φ_{ij} of algebraic isomorphisms between them;
- For each $\phi \in \Phi_{ij}$ find a combinatorial isomorphism f between $\mathcal{A}_i$ and $\mathcal{A}_j$ s.t. $f^* = \phi$ (if such f exists);
- Collect all permutations f found on the previous stage. Let P be the set of all those permutations.

Proposition

The set P constructed above is a solving set for the Cayely graphs over H, that is two Cayley graphs $\mathrm{Cay}(H, S)$ and $\mathrm{Cay}(H, T)$ are isomorphic iff there exists $f \in P$ s.t. $\mathrm{Cay}(H, S)^f = \mathrm{Cay}(H, T)$.

Example

N	S-partition $\mathcal{S}$	$\lvert\mathrm{Alg}(\mathcal{S})\rvert$	$\mathrm{Iso}(\mathcal{S})/\mathrm{Aut}(\mathcal{S})$ transversal
1	$\{0\}, \{1,2,3,4,5,6,7\}$	1	μ_1
2	$\{0\}, \{1,3,5,7\}, \{2,6,4\}$	1	μ_1
3	$\{0\}, \{1,3,5,7,2,6\}, \{4\}$	1	μ_1
4	$\{0\}, \{1,3,5,7\}, \{2,6\}, \{4\}$	1	μ_1
5	$\{0\}, \{1,3,5,7\}, \{2\}, \{6\}, \{4\}$	2	μ_1, μ_3
6	$\{0\}, \{1,5\}, \{3,7\}, \{2\}, \{6\}, \{4\}$	4	$\mu_1, \mu_3, \sigma, \sigma\mu_3$
7	$\{0\}, \{1,5\}, \{3,7\}, \{2,6\}, \{4\}$	2	μ_1, μ_3
8	$\{0\}, \{1,3\}, \{5,7\}, \{2,6\}, \{4\}$	2	μ_1, μ_5
9	$\{0\}, \{1,7\}, \{3,5\}, \{2,6\}, \{4\}$	2	μ_1, μ_3
10	$\{0\}, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}, \{7\}$	4	$\mu_1, \mu_3, \mu_5, \mu_7$

Here $\sigma = (2,6)(3,7)$ and μ_a is an automorphism of $\mathbb{Z}_8$: $x \mapsto ax$. Thus $\{\mu_1, \mu_3, \mu_5, \mu_7, \sigma, \sigma\mu_3\}$ is a solving set for $\mathbb{Z}_8$.

Solving sets for cyclic groups

Theorem

Two S-rings over cyclic groups are algebraically isomorphic iff they coincide.

This implies the following modification of the original Klin-Pöschel approach

- Find all S-rings over $\mathbb{Z}_n$, let $\mathcal{A}_1, ..., \mathcal{A}_N$ be the complete list of them;
- For each $\mathcal{A}_i$ find a transversal T_i of $\mathrm{Iso}(\mathcal{A}_i)/\mathrm{Aut}(\mathcal{A}_i)$
- Then the union of T_i produces a solving set for $\mathbb{Z}_n$.

Theorem

Given a number n, one can construct a solving set for $\mathbb{Z}_n$ of at most n^3 permutations in time $n^{O(1)}$.

CI-property (L. Babai, 1976)

Definition

A Cayley (di)graph $\mathrm{Cay}(H, S)$ has a Cayley Isomorphism property (CI-property for short) iff $\mathrm{Aut}(H)$ is a solving set for $\mathrm{Cay}(H, S)$,

$$\forall_{T \subseteq H}\ \mathrm{Cay}(H, T) \cong \mathrm{Cay}(H, S) \iff \exists_{\varphi \in \mathrm{Aut}(H)}\ T = S^{\varphi}.$$

H is a DCI-group if every subset S has CI-property.
H is a CI-group if every symmetric subset S has CI-property.
H is a $\mathrm{CI}^{(2)}$-group if it has CI-property for all colored Cayley digraphs over H.

$$\mathrm{CI}^{(2)} - \text{property} \implies \text{DCI-property} \implies \text{CI-property}$$

Problem (L. Babai & P. Frankl, 1976)

Which are the CI-groups?

Graph Isomorphism problem for (D)CI-groups

Proposition

Let $\mathfrak{G}$ be a class of (D)CI-groups. If $|\operatorname{Aut}(H)| = |H|^c$ for every $H \in \mathfrak{G}$ and some for some constant c, then GIP for Cayley graphs over groups from $\mathfrak{G}$ belongs to **P**.

Problem

Given two subsets $S, T \subseteq \mathbb{Z}_p^k$, find whether there exists $\varphi \in \operatorname{Aut}(\mathbb{Z}_p^k)$ such that $S^\varphi = T$.

Graph Isomorphism problem for (D)CI-groups

Proposition

Let $\mathfrak{G}$ be a class of (D)CI-groups. If $|\operatorname{Aut}(H)| = |H|^c$ for every $H \in \mathfrak{G}$ and some for some constant c, then GIP for Cayley graphs over groups from $\mathfrak{G}$ belongs to **P**.

Problem

Given two subsets $S, T \subseteq \mathbb{Z}_p^k$, find whether there exists $\varphi \in \operatorname{Aut}(\mathbb{Z}_p^k)$ such that $S^\varphi = T$.
Does there exists a polynomial (in p^k) algorithm which answers the above question?

Code equivalence Problem

Two generating subsets $S = \{s_1, ..., s_n\}, T = \{t_1, ..., t_n\} \subseteq \mathbb{Z}_p^k$ are equivalent iff the linear codes with generating matrices $\mathrm{S} = (s_1|...|s_n), \mathrm{T} = (t_1|...|t_n)$ are permutation equivalent.