Association schemes, Schur rings and Cayley graph isomorphism problem

Misha Muzychuk

Netanya Academic College,
Israel

Rogla, June 2011

Isomorphism Problem for Cayley graphs

Cayley graphs

Let H be a finite group and $S \subseteq H$. A Cayley graph over H generated by a connection set S has H as a vertex set, and two vertices $x, y \in H$ are connected iff $xy^{-1} \in S$. Notation $\mathrm{Cay}(H, S)$. A Cayley graph over cyclic group is called circulant.

Isomorphism Problem for Cayley graphs

Cayley graphs

Let H be a finite group and $S \subseteq H$. A Cayley graph over H generated by a connection set S has H as a vertex set, and two vertices $x, y \in H$ are connected iff $xy^{-1} \in S$. Notation $\mathrm{Cay}(H, S)$. A Cayley graph over cyclic group is called circulant.

Cayley graphs isomorphism problem (CGIP)

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

Isomorphism Problem for Cayley graphs

Cayley graphs

Let H be a finite group and $S \subseteq H$. A Cayley graph over H generated by a connection set S has H as a vertex set, and two vertices $x, y \in H$ are connected iff $xy^{-1} \in S$. Notation $\mathrm{Cay}(H, S)$. A Cayley graph over cyclic group is called circulant.

Cayley graphs isomorphism problem (CGIP)

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

Input: a group H of order n (given by its Cayley table), two subsets S, T. We are looking for an algorithm which recognizes an isomoprhism between $\mathrm{Cay}(H, S)$ and $\mathrm{Cay}(H, T)$ with running time $n^{O(1)}$.

Cayley isomorphism

Definition

Cayley graphs $\mathrm{Cay}(H, S)$ and $\mathrm{Cay}(H, T)$ are called Cayley isomorphic, notation $\mathrm{Cay}(H, T) \cong_{Cay} \mathrm{Cay}(H, S)$, if $\exists\ \varphi \in \mathrm{Aut}(H)$ such that $S^{\varphi} = T$. Clearly that

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

Definition

A subset $S \subseteq H$ is called a CI-subset if any Cayley graph over H isomorphic to $\mathrm{Cay}(H, S)$ is also Cayley isomorphic. A group H is called a CI-group with respect to graphs if each subset of H is a CI-subsets.

Related problems

Cayley isomorphism problem

Given two subsetes $S, T \subseteq H$. Find whether they are conjugate by an element of $\mathrm{Aut}(H)$. Related problem: find a stabiliser of S in $\mathrm{Aut}(H)$.

Related problems

Cayley isomorphism problem

Given two subsetes $S, T \subseteq H$. Find whether they are conjugate by an element of $\mathrm{Aut}(H)$. Related problem: find a stabiliser of S in $\mathrm{Aut}(H)$.

Automorphism group of a Cayley graph

Given a Cayley graph $\mathrm{Cay}(H, S)$. Find its automorphism group (the generators).

Related problems

Cayley isomorphism problem

Given two subsetes $S, T \subseteq H$. Find whether they are conjugate by an element of $\mathrm{Aut}(H)$. Related problem: find a stabiliser of S in $\mathrm{Aut}(H)$.

Automorphism group of a Cayley graph

Given a Cayley graph $\mathrm{Cay}(H, S)$. Find its automorphism group (the generators).

Recognizing being a Cayley graph over a given group

Given a graph Γ of order n and a concrete group H of order n. Is Γ isomorphic to a Cayley graph over H? In other words, does $\mathrm{Aut}(\Gamma)$ contain a regular subgroup isomorphic to H.

Problems summary

1. Cayley isomorphism.
2. Usual isomorphism (ISO).
3. Automorphism group (AGEN).
4. Cayley graph recognition.

Coherent closure of a Cayley graph

Let H be a finite group. For each $h \in H$ we set

- $h_L := \{(x, hx) \mid x \in H\}, H_L = \{h_L \mid h \in H\}$;
- $h_R := \{(x, xh) \mid x \in H\}, H_R = \{h_R \mid h \in H\}$

Both H_L and H_R are regular subgroups of $\mathrm{Sym}(H)$ isomorphic to H.

Well-known fact

Each Cayley graph over H is H_R-invariant. In particular it is vertex transitive.

Corollary

A coherent closure $\langle\langle \mathrm{Cay}(H, S) \rangle\rangle$ is an association scheme.

Association schemes

Definition

Recall that an association scheme is a pair $\mathcal{X} = (\Omega, S)$ satisfying the following conditions

1. S is a partition of Ω^2;
2. $1_\Omega \in S$ and $S^* = S$;
3. for any triple of relations $r, s, t \in S$ and any pair $(\alpha, \beta) \in t$ the intersection number $c_{rs}^t := |\alpha r \cap \beta s^*|$ depends only on r, s, t.

The elements of S are called basic relations of $\mathcal{X}$. The adjacency matrix of $\mathcal{X}$: $A(S)_{\alpha,\beta} := s \iff (\alpha, \beta) \in s$.

Recall that the numbers $|\Omega|$,$|S|$ and $|S| - 1$ are called the degree, rank and class number of $\mathcal{X}$.

Association schemes

Basic (di)graphs

For each non-reflexive $s \in S$ the pair (Ω, s) is called a basic graph of $\mathcal{X}$. The valency of the graph (Ω, s) is denoted as n_s ($n_s = c_{ss^*}^1$). For a given subset $T \subseteq S$ we set $n_T = \sum_{t \in T} n_t$.

Association schemes

Basic (di)graphs

For each non-reflexive $s \in S$ the pair (Ω, s) is called a basic graph of $\mathcal{X}$. The valency of the graph (Ω, s) is denoted as n_s ($n_s = c_{ss^*}^1$). For a given subset $T \subseteq S$ we set $n_T = \sum_{t \in T} n_t$.

Adjacency (Bose-Mesner) algebra

The adjacency matrix of a basic graph (Ω, s) is denoted as $A(s)$. It follows from

$$A(s)A(t) = \sum_{r \in S} c_{st}^r A(r)$$

that the linear span of the matrices $A(s), s \in S$ is a subalgebra of $M_\Omega(\mathbb{C})$ - complex adjacency algebra of $\mathcal{X}$, notation $\mathbb{C}[S]$. A scheme is called commutative if $\mathbb{C}[S]$ is commutative.

Association schemes

Product of relations

Given $s, t \in T$, we set $st := \{r \in S \mid c_{st}^{r} \neq 0\}$. If $A, B \subseteq S$, then $AB := \bigcup_{a\in A, b\in B} ab$. A relational product of $s, t \in S$ is denoted as $s \cdot t$.

Association schemes

Product of relations

Given $s, t \in T$, we set $st := \{r \in S \mid c_{st}^{r} \neq 0\}$. If $A, B \subseteq S$, then $AB := \bigcup_{a \in A, b \in B} ab$. A relational product of $s, t \in S$ is denoted as $s \cdot t$.

Exercise

Prove that $s \cdot t = \cup_{r \in st} r$

Association schemes

Product of relations

Given $s, t \in T$, we set $st := \{r \in S \mid c^r_{st} \neq 0\}$. If $A, B \subseteq S$, then $AB := \bigcup_{a \in A, b \in B} ab$. A relational product of $s, t \in S$ is denoted as $s \cdot t$.

Exercise

Prove that $s \cdot t = \cup_{r \in st} r$

A scheme is called symmetric (antisymmetric) if all its non-reflexive basic relations are symmetric (antisymmetric).

Exercise

Prove that a symmetric scheme is commutative. Hint: use $A(s^*) = A(s)^T$.

Schurian schemes

Let G be a finite group acting transitively on the set Ω. Extending this action to a diagonal action on Ω^2: $(\alpha, \beta)^g := (\alpha^g, \beta^g)$ we obtain a partition of Ω^2 into G-orbits (they are called 2-orbits (orbitals) of G). The set of 2-orbits will be denoted as Ω^2/G.

Known fact

A pair $Inv(G) = (\Omega, \Omega^2/G)$ is an association scheme. Association schemes of this type are called Schurian.

Recall that the scheme $Inv(G)$ as a 2-orbit (orbital) scheme of G.

Thin schemes

Definition

A basic relation $s \in S$ is called thin if $n_s = 1$ (in other words s is a permutation on Ω). A scheme is thin if every basic relation is thin.

Examples

Consider a 2-orbit scheme $Inv(H_R)$ of the group $H_R \leq \mathrm{Sym}(H)$ where H is a finite group. In this case $\Omega = H$ and the basic relations are of the form $h_L = \{(x, hx) \mid x \in H\}$ where h runs through H. All basic relations of this scheme are thin.

Theorem

Any thin scheme is isomorphic to a scheme (H, H_L) for some finite group H.

Flag scheme of a projective planes

Let $\mathcal{P} = (P, L)$ be a projective plane of order n. Denote by $\mathcal{F}$ the set of flags (p, ℓ) of the plane $\mathcal{P}$. Define two relations on $\mathcal{F}$ as following

$$\begin{aligned} s &:= \{((p_1, \ell_1), (p_2, \ell_2)) \,|\, p_1 = p_2, \ell_1 \neq \ell_2\}, \\ t &:= \{((p_1, \ell_1), (p_2, \ell_2)) \,|\, p_1 \neq p_2, \ell_1 = \ell_2\}. \end{aligned}$$

Then the relations $1, s, t, s \cdot t, t \cdot s, s \cdot t \cdot s$ form an association scheme of rank 6 on $\mathcal{F}$ called the flag scheme of a projective plane. Notice that $s \cdot t \cdot s = t \cdot s \cdot t$.

Flag scheme of a projective planes

Let $\mathcal{P} = (P, L)$ be a projective plane of order n. Denote by $\mathcal{F}$ the set of flags (p, ℓ) of the plane $\mathcal{P}$. Define two relations on $\mathcal{F}$ as following

$$\begin{aligned} s &:= \{((p_1, \ell_1), (p_2, \ell_2)) \mid p_1 = p_2, \ell_1 \neq \ell_2\}, \\ t &:= \{((p_1, \ell_1), (p_2, \ell_2)) \mid p_1 \neq p_2, \ell_1 = \ell_2\}. \end{aligned}$$

Then the relations $1, s, t, s \cdot t, t \cdot s, s \cdot t \cdot s$ form an association scheme of rank 6 on $\mathcal{F}$ called the flag scheme of a projective plane. Notice that $s \cdot t \cdot s = t \cdot s \cdot t$.

Exercise

Compute $s(s \cdot t)$.

Affine schemes

Let $A = (P, L)$ be an affine plane of order n. Define a partition of $P \times P \setminus 1_P$ by putting two pairs $(p_1, p_2), (q_1, q_2)$ into the same class iff the lines p_1p_2, q_1q_2 are parallel or coincide. In this way we obtain a partition of $P^2 \setminus 1_P$ into $n + 1$ binary relations which are in one-to-one correspondence with parallel classes of lines in A. These relations together with the identity 1_P form a symmetric association scheme of degree n^2 and rank $n + 2$.

Fusions and fissions

Let $\mathcal{X} = (\Omega, S)$ and $\mathfrak{Y} = (\Omega, T)$ be two schemes. We say that $\mathfrak{Y}$ is a fusion of $\mathcal{X}$ (and $\mathcal{X}$ is a fission of $\mathfrak{Y}$) if each basic relation of $\mathfrak{Y}$ is a union of some basic relations of $\mathcal{X}$. Thus $\mathfrak{Y}$ is a fusion of $\mathcal{X}$ iff the $\mathbb{C}[T] \subseteq \mathbb{C}[S]$, or, equivalently, $T \sqsubseteq S$ (that is the partition S is a refinement of T) .

Proposition

Let Γ be a G-invariant (di)graph where $G \leq \mathrm{Sym}(\Omega)$ is a transitive permutation group. Then the coherent closure $\langle\langle\Gamma\rangle\rangle$ is a fusion of the scheme $Inv(G) = (\Omega, \Omega^2/G)$.

Corollary

A coherent closure of a Cayley graph $\mathrm{Cay}(H, S)$ is a fusion scheme of $Inv(H_R) = (H, H_L)$. Any fusion of this scheme is called a Cayley scheme over H.

Fusions and fissions

A fusion $\mathfrak{Y}$ of $\mathcal{X}$ is uniquely determined by a partition $\mathcal{P}$ of S where two basic relations of S belong to the same class of $\mathcal{P}$ iff they are fused in $\mathfrak{Y}$. This partition has the following properties $\mathcal{P}(1) = \{1\}, \mathcal{P}(s^*) = \mathcal{P}(s)^*$. A partition $\mathcal{P}$ of S satisfying these conditions is usually called admissible. Notice that not every admissible partition determines a scheme.

Proposition

All partitions determining fusions of $\mathcal{X}$ form a sublattice of a partition lattice of S. It has a unique maximal element - $\mathcal{X}$ and unique minimal one - the trivial scheme.

Fusions in the flag scheme of a projective plane

Theorem

Let $(\mathcal{F}, \{1, s, t, s \cdot t, t \cdot s, s \cdot t \cdot s\})$ be the flag scheme of a projective plane of order $n > 1$. Then it admits the following non-trivial fusions

1. $\{1\}, \{s\}, \{t, s \cdot t, t \cdot s, s \cdot t \cdot s\}$;
2. $\{1\}, \{t\}, \{s, s \cdot t, t \cdot s, s \cdot t \cdot s\}$;
3. $\{1\}, \{s, t\}, \{s \cdot t, t \cdot s\}, \{s \cdot t \cdot s\}$.

The latter fusion determines the scheme of a d.r.g. of diameter 3.

Fusions in the affine scheme

Theorem

Let (P, S) be an affine scheme of rank $n + 2$ which corresponds to an affine plane of order n. Then any admissible partition of S determines a fusion scheme of (P, S).

Cayley schemes

Let H be an arbitrary finite, multiplicatively written, group with identity e. Then (H, H_L) is a 2-orbit scheme of the regular permutation group H_R. Any fusion scheme of (H, H_L) is called a Cayley scheme over H. A Cayley scheme over cyclic group is called a circulant scheme.

Example

Let $\mathcal{X}$ be a circulant scheme of degree 4. Its adjacency matrix is

$$A(\mathcal{X}) = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 0 & 1 & 2 \\ 2 & 3 & 0 & 1 \\ 1 & 2 & 3 & 0 \end{pmatrix}$$

Merging of classes 3 and 1 yields a fusion scheme $\mathcal{X}'$.

Cayley schemes

$$A(\mathcal{X}') = \begin{pmatrix} 0 & 1 & 2 & 1 \\ 1 & 0 & 1 & 2 \\ 2 & 1 & 0 & 1 \\ 1 & 2 & 1 & 0 \end{pmatrix}$$

Cayley schemes

Each Cayley scheme is invariant under the action of H_R.

Theorem

An association scheme is isomorphic to a Cayley scheme over group H iff the automorphism group of a scheme contains a regular subgroup isomorphic to H.

Since each fusion of a scheme is uniquely determined by an admissible partition of scheme's basic relations, any fusion of a Cayley scheme is completely determined by a partition of H.

Fusion of Cayley schemes

Schur partitions

Let $\mathcal{S} = \{\mathcal{S}_0, ..., \mathcal{S}_d\}$ be a partition of a finite group H. It is called Schur partition (S-partition, for short) if it satisfies the following conditions

1. $\mathcal{S}_0 = \{e\}$;
2. for each $i \in [0, d]$ there exists $i' \in [0, d]$ such that $\mathcal{S}_i^{(-1)} := \{h^{-1} \mid h \in \mathcal{S}_i\} = \mathcal{S}_{i'}$;
3. for each triple $i, j, k \in [0, d]$ and $a \in \mathcal{S}_k$ the number of pairs $(x, y) \in \mathcal{S}_i \times \mathcal{S}_j$ satisfying $xy = a$ depends only on a triple i, j, k.

Schur partitions

Example

$H = \mathbb{Z}_4, \mathcal{S} = \{\{0\}, \{2\}, \{1, 3\}\}$.

Let $\mathcal{S}$ be an arbitrary partition of H. Denote by $\mathrm{Cay}(H, \mathcal{S})$ the partition of $H \times H$ into the disjoint union of binary relations $\mathrm{Cay}(H, S), S \in \mathcal{S}$ where $\mathrm{Cay}(H, S) = \{(x, y) \in H \times H \,|\, xy^{-1}\}$.

Theorem

A pair $(H, \mathrm{Cay}(H, \mathcal{S}))$ is a scheme iff $\mathcal{S}$ is a Schur partition. Thus there is a one-to-one correspondence between Cayley schemes over H and Schur partitions of H.

Schur rings/algebras

Let $\mathbb{C}[H]$ be the group algebra of H over $\mathbb{C}$. It consists of all formal sums $\sum_{h\in H}\alpha_h h$, $\alpha_h \in \mathbb{C}$ which are multiplied according to the following rule:

$$(\sum_{h\in H}\alpha_h h)(\sum_{h\in H}\beta_h h) = \sum_{h\in H}\sum_{f\in H}(\alpha_h\beta_f)(hf).$$

The Schur-Hadamard product in $\mathbb{C}[H]$ is defined as follows:

$$(\sum_{h\in H}\alpha_h h)\circ(\sum_{h\in H}\beta_h h) = \sum_{h\in H}(\alpha_h\beta_h)h.$$

For each $m \in \mathbb{Z}$ and $x = \sum_{h\in H} x_h h$ let $x^{(m)} := \sum_{h\in H} x_h h^m$. We also write $T^{(m)}$ for $\{t^m \mid t \in T\}$ where $T \subseteq H$.

Schur rings

A simple quantity is an element of the form $\underline{T} := \sum_{t \in T} t$ where $T \subseteq H$. In what follows we write g instead of $\underline{\{g\}}$. $\underline{T}$ is called symmetric if $T^{(-1)} = T$.

Given a partition $\mathcal{T}$ of H we set $\underline{\mathcal{T}}$ to be a subspace of $\mathbb{C}[H]$ spanned $\underline{T}$, $T \in \mathcal{T}$.

Definition

A subalgebra $\mathcal{A}$ of the group algebra $\mathbb{C}[H]$ is called a Schur ring/algebra (more briefly, an S-ring) if it satisfies the following axioms:

(S1) $\mathcal{A}$ has a basis of simple quantities $\underline{T_0}, \ldots, \underline{T_r}$, where $T_0 = \{e\}$,

(S2) $T_i \cap T_j = \emptyset$ for $i \neq j$, and $\bigcup_{j=0}^{r} T_j = H$,

(S3) For each $i \in \{0, 1, \ldots, r\}$ there exists $i' \in \{0, 1, \ldots, r\}$ such that $T_{i'} = T_i^{(-1)}$.

Schur rings

By (S1) and (S2), the basis $\underline{T_0}, \ldots, \underline{T_r}$ is unique and it is called the standard basis of $\mathcal{A}$. The number $r+1$ is called the rank of $\mathcal{A}$. The sets T_i, $0 \leq i \leq r$, are called the basic sets of $\mathcal{A}$ and the notation $\mathcal{A} = \langle \underline{T_0}, \ldots, \underline{T_r} \rangle$ will be used if $\mathcal{A}$ is an S-ring over H whose basic sets are $T_0, \ldots, T_r$. Since $\mathcal{A}$ is a subalgebra, the product $\underline{T_i}\,\underline{T_j}$ is a linear combination of $\underline{T_0}, \ldots, \underline{T_r}$. That is

$$\underline{T_i}\,\underline{T_j} = \sum_k c_{ij}^k \underline{T_k}$$

where c_{ij}^k are structure constants of the S-ring $\mathcal{A}$. It is easy to check that

$$c_{ij}^k = |\{(x, y) \in T_i \times T_j \mid xy = g\}|,$$

where $g \in T_k$ is arbitrary.

Schur rings

There is a trivial S-ring over an arbitrary group H, namely $\langle \underline{e}, \underline{H \setminus \{e\}} \rangle$. A subset S of H is called an $\mathcal{A}$-subset or an $\mathcal{A}$-set if S is a union of basic sets of $\mathcal{A}$. Note that an intersection and union of two $\mathcal{A}$-subsets is once more an $\mathcal{A}$-subset.
Note that the group algebra by itself is a Schur ring, the basic sets of which are singletones. Any S-ring different from $\mathbb{C}[H]$ is called proper.

Simple fact

There is one-to-one correspondence between S-partitions of H and S-rings over H.

Schur rings - algebraic approach

It follows from the definition that each S-ring contains e,$\underline{H}$ (note that e and $\underline{H}$ the units with respect to the multiplications $\cdot$ and $\circ$, respectively) and is closed with respect to the operations $\cdot, \circ, ^{(-1)}$. It turns out this is a characteristic property of S-rings.

Theorem

A vector subspace $\mathcal{A} \subseteq \mathbb{C}[H]$ is an S-ring over H if and only if $e \in \mathcal{A}$, $\underline{H} \in \mathcal{A}$ and $\mathcal{A}$ is closed with respect to $\cdot, \circ$ and $^{(-1)}$.

It follows from this result that the intersection of S-rings over H is an S-ring over the same group. Given $x_1, \ldots, x_k \in \mathbb{C}[H]$, we define $\langle\langle x_1, \ldots, x_k \rangle\rangle$ to be the least S-ring which contains the elements $x_1, \ldots, x_k$.

Examples

Theorem (Schur)

Let $G = AH$ be a factorization of a finite group G into a product of two trivially intersecting subgroups. Then the centralizer $\mathcal{A}$ of $\underline{A}$ in $\mathbb{C}[H]$ is a Schur ring over H. The basic sets of $\mathcal{A}$ have a form $AgA \cap H$.

A concrete example

A simple group $SL_3(2)$ 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.

Examples

Corollary of Schur's Theorem

Let $\Phi \leq \mathrm{Aut}(H)$ be an arbitrary group of automorphisms. Then the set of Φ- orbits H/Φ is a Schur partition.

Corollary

Conjugacy classes of a finite group form an S-partition.

Subgroup S-ring

Let $\mathcal{L}$ be a sublattice of the subgroup lattice of a group H such that $\{e\}, H \in \mathcal{L}$. Assume that any two subgroups $A, B \in \mathcal{L}$ are permutable, that is $AB = BA$. Then the linear span of $\underline{A}, A \in \mathcal{L}$ is a Schur ring over H.

Examples

Below there is a complete list of proper Schur rings over $\mathbb{Z}_8$ computed by the package COCO.

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

Isomorphisms between S-rings

Let $\mathcal{A}$ and $\mathcal{B}$ be two S-rings over groups H and K resp. Let $S_0 = \{e\}, ..., S_d$ and $T_0 = \{e\}, ..., T_d$ be their basic sets.

Definition

We say that $\mathcal{A}$ and $\mathcal{B}$ are

1. Cayley isomorphic if there exists a group isomorphism from H to K which maps $\mathcal{A}$ bijectively onto $\mathcal{B}$;
2. (combinatorially) isomorphic iff there exists a scheme isomorphism between Cayley schemes $\mathrm{Cay}(H, \{S_0, ..., S_d\})$ and $\mathrm{Cay}(K, \{T_0, ..., T_d\})$;
3. algebraically isomorphic iff there exists an algebra isomorphism between $\mathcal{A}$ and $\mathcal{B}$ which maps the standard basis of $\mathcal{A}$ onto a standard basis of $\mathcal{B}$

Isomorphisms between S-rings

An algebraic isomorphism induces a bijection f between the basic sets (or index sets) such that $c_{ij}^{k} = c_{i^f j^f}^{k^f}$.

Theorem

Let $f : H \to K$ be a bijection which maps e_H to e_K. Then f is a combinatorial isomorphism iff it satisfies the conditions

$$(hS)^f = h^f S^f \text{ for each } h \in H \text{ and } S \in \mathcal{S}.$$

A combinatorial isomorphism $f : H \to K$ is called normalized if $e_H^f = e_K$. Notice that two S-rings are comb. isom. iff there exists a normalized comb. isom between them.

Connections between isomorphisms

Lemma

If $f : H \to K$ is normalized combinatorial isomorphism from $\mathcal{A}$ onto $\mathcal{B}$, then its restriction onto $\mathcal{A}$ is an algebraic isomorphism between $\mathcal{A}$ and $\mathcal{B}$.

$$\mathcal{A} \cong_{Cay} \mathcal{B} \Rightarrow \mathcal{A} \cong \mathcal{B} \Rightarrow \mathcal{A} \cong_{alg} \mathcal{B}.$$

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

Examples

Cayley isomorphism

The partitions $\{\{00\},\{10\},\{01,11\}\}$ and $\{\{00\},\{01\},\{10,11\}\}$ are two Schur partitions of $\mathbb{Z}_2^2$ which are Cayley isomorphic by an automorphism $xy \mapsto yx$.

Combinatorial isomorphism

The partitions $\{\{00\},\{11\},\{10,01\}\}$ and $\{\{0\},\{2\},\{1,3\}\}$ are Schur partitions of $\mathbb{Z}_2^2$ and $\mathbb{Z}_4$ respectively. The mapping

$$00 \mapsto 0,\ 11 \mapsto 2,\ 01 \mapsto 1,\ 10 \mapsto 3$$

is a combinatorial isomorphism between the S-rings known in coding theory as Gray map.

Examples

Let K_4 be the Klein four group (i.e. $K_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$) and $H = K_4 \times K_4$. Let Φ be an order two subgroup of $\mathrm{Aut}(H)$ generated by an involution interchanging the coordinaties. Then H/Φ is an S-partition with 4 orbits of length one and 6 orbits of length two.
Let $K = \mathbb{Z}_4 \times \mathbb{Z}_4$ and $\Psi \leq \mathrm{Aut}(H)$ be an order two subgroup generated by an automorphism $x \mapsto -x$. Then K/Ψ be an S-partition with 4 orbits of length one and 6 orbits of kength two.

Proposition

S-rings $\underline{H/\Phi}$ and $\underline{K/\Psi}$ are isomorphic algebraically but not isomorphic combinatorially.

Automorphisms of an S-ring

Automorphism group of an S-ring

Let $\mathcal{A}$ be an S-ring over H and $\mathcal{S}$ the corresponding S-partition. The group $G := \mathrm{Aut}(\mathrm{Cay}(H, \mathcal{S}))$ is called the automorphism group of $\mathcal{A}$.

- $H_R \leq G$;
- $G = \bigcap_{S \in \mathcal{S}} \mathrm{Aut}(\mathrm{Cay}(H, S))$;
- each basic set $S \in \mathcal{S}$ is G_e-invariant.

We say that $\mathcal{A}$ is Schurian if $\mathrm{Cay}(H, \mathcal{S})$ is Schurian, that is each basic set $S \in \mathcal{S}$ is an orbit of G_e.

Application of S-rings to the CGIP

Solving sets

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

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

A graph $\mathrm{Cay}(H, S)$ is a CI iff $\mathrm{Aut}(H)$ is a solving set. A set S is a solving set w.r.t Cayley graphs over H iff it is a solving set for each Cayley graph over H.

Theorem (Babai)

Let $G = \mathrm{Aut}(\mathrm{Cay}(H, S))$. A graph $\mathrm{Cay}(H, S)$ is CI iff any regular subgroup K of G isomorphic to H is conjugate in G to H_R.

Constructing individual solving sets

Definition

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

Theorem

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

$$\bigcup_{i \in I} f_i Aut(H)$$

is a solving set for $\mathrm{Cay}(H, S)$.

Appearence of S-rings

Let $S \subseteq H$ be an arbitrary subset. Denote by $\mathcal{S}$ an S-partition of H corresponding to the S-ring $\langle\langle \underline{S} \rangle\rangle$. Then the association scheme $\mathrm{Cay}(H, \mathcal{S})$ is a coherent closure of a Cayley graph $\mathrm{Cay}(H, S)$.

Corollary

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

Constructing global solving set

Klin - Pöschel approach

1. Enumerate all Schur rings over H: - $\mathcal{A}_1, ..., \mathcal{A}_N$;
2. Compute the automorphism group of every S-ring $\mathcal{A}_i, i = 1, ..., N$ and find its solving set;
3. Unify the solving sets found in the previous step.

As an example, we consider application of this process to $\mathbb{Z}_8$. We denote the cyclic shift $x \mapsto x + 1, x \in \mathbb{Z}_8$ as ρ. Thus $(\mathbb{Z}_8)_R = \langle \rho \rangle$.

Example

N	S-partition	Aut	$\mathbb{Z}_8$ – bases
1	$\{0\}, \{1,2,3,4,5,6,7\}$	S_8	$\langle\rho\rangle$
2	$\{0\}, \{1,3,5,7\}, \{2,6,4\}$	$S_4 \wr S_2$	$\langle\rho\rangle$
3	$\{0\}, \{1,3,5,7,2,6\}, \{4\}$	$S_2 \wr S_4$	$\langle\rho\rangle$
4	$\{0\}, \{1,3,5,7\}, \{2,6\}, \{4\}$	$S_2 \wr S_2 \wr S_2$	$\langle\rho\rangle$
5	$\{0\}, \{1,3,5,7\}, \{2\}, \{6\}, \{4\}$	$\mathbb{Z}_4 \wr S_2$	$\langle\rho\rangle$
6	$\{0\}, \{1,5\}, \{3,7\}, \{2\}, \{6\}, \{4\}$	$\mathbb{Z}_8 \rtimes \langle 5\rangle$	$\langle\rho\rangle, \langle\sigma\rangle$
7	$\{0\}, \{1,5\}, \{3,7\}, \{2,6\}, \{4\}$	$S_2 \wr \mathbb{Z}_4$	$\langle\rho\rangle$
8	$\{0\}, \{1,3\}, \{5,7\}, \{2,6\}, \{4\}$	$\mathbb{Z}_8 \rtimes \langle 3\rangle$	$\langle\rho\rangle$
9	$\{0\}, \{1,7\}, \{3,5\}, \{2,6\}, \{4\}$	$\mathbb{Z}_8 \rtimes \langle 7\rangle$	$\langle\rho\rangle$

Here σ denotes a pemutation $x \mapsto 5x + 1, x \in \mathbb{Z}_8$. Notice that $\langle\sigma\rangle^{(26)(37)} = \langle\rho\rangle$. So, a solving set for Cayley digraphs over $\mathbb{Z}_8$ is a union of two $\mathrm{Aut}(\mathbb{Z}_8)$-cosets: $\mathrm{Aut}(\mathbb{Z}_8) \cup (2,6)(3,7)\,\mathrm{Aut}(\mathbb{Z}_8)$.

Fusion control

Definition

Let $H_R \leq Y \leq Z \leq \mathrm{Sym}(H)$ be a chain of subgroups. We say that Y controls fusion of H_R in Z if for any regular H-isomorphic subgroup K of Z there exists $z \in Z$ such that $K^z \leq Y$. Notation $Y \preceq_{H_R} Z$.

Lemma

Let $\mathcal{A} \subseteq \mathcal{B}$ be two Schur rings over H. If $\mathrm{Aut}(\mathcal{B}) \preceq_{H_R} \mathrm{Aut}(\mathcal{A})$, then any solving set for $\mathcal{B}$ is a solving set for $\mathcal{A}$.

We'll write $\mathcal{A} \sqsubseteq_i \mathcal{B}$ iff $\mathrm{Aut}(\mathcal{B}) \preceq_{H_R} \mathrm{Aut}(\mathcal{A})$.

Constructing global solving set

Notice that $\sqsubseteq_i$ is a partial order on the set of all S-rings over H.

Modified Klin - Pöschel approach

1. Find all Schur rings over H which are maximal with respect to $\sqsubseteq_i$: - $\mathcal{A}_1, ..., \mathcal{A}_N$;
2. Compute the automorphism group of every S-ring $\mathcal{A}_i, i = 1, ..., N$ and find its solving set;
3. Unify the solving sets found in the previous step.

$\sqsubseteq_i$-maximal S-rings may be classified up to Cayley isomorphism.

How to find $\sqsubseteq_i$-maximal S-partitions

All $\sqsubseteq_i$-maximal S-ring are Schurian.

p-groups

If H is a p-group, then $\sqsubseteq_i$-maximal S-ring are so-called p-S-rings, that is cardinalities of basic sets are p-powers.

In the considered example of the group $\mathbb{Z}_8$ there are 7 2-S-rings, among them only two are $\sqsubseteq_i$-maximal partitions: the singltone one and $\{1,5\},\{3,7\},\{0\},\{2\},\{4\},\{6\}$.

H is a p-group

$|H| = p$

$\mathbb{C}[H]$ is the only p-S-ring over H

$|H| = p^2$

There are exactly two p-S-rings over H (up to Cayley isomorphism). If H is cyclic, both of them are $\sqsubseteq_i$-maximal. If H is elementary abelian, then only $\mathbb{C}[H]$ is $\sqsubseteq_i$-maximal.

$|H| = p^3$

If H is cyclic, then there are 5 p-S-rings over H. All of them are $\sqsubseteq_i$-maximal. If H is elementary abelian, then there are 6 p-S-rings over H and $\mathbb{C}[H]$ is the only one which is $\sqsubseteq_i$-maximal.