Association schemes, Schur rings and the isomorphism problem for circulant graphs. Part 1.

M. Muzychuk and I. Ponomarenko

Contents

- Graph isomorphism problem and Weisfeiler-Leman algorithm.
- Coherent configurations and coherent (cellular) algebras.
- Association schemes.
- Cayley schemes and Schur rings.
- Schur rings and Cayley graphs isomorphism problem.
- Theory of Schur rings.

References. Coherent configurations and algebras

- D. G. Higman, Coherent configurations I, Rend. Sem. Mat. Univ. Padova, 44 (1970), 1-25;
- D. G. Higman, Coherent algebras, Linear Alg. and Its Applications, 93 (1987), 209-239;
- B. Weisfeiler, On Construction and Identification of Graphs, LNM 558 (1976);
- M. Klin, C. Rücker, G. Rücker and G. Tinhofer, Algebraic Combinatorics in Mahematical Chemistry, 1997;
- I.A. Faradžev, M.H. Klin, M.E. Muzychuk, Cellular rings and groups of automorphisms of graphs, in: I.A. Faradžev (Ed.), Investigations In Algebraic Theory Of Combinatorial Objects, Kluwer Acad. Publ, Dordrecht, 1994, pp. 1-152;
- S. Evdokimov and I. Ponomarenko, Permutation group approach to association schemes, Europ. J. of Combin. 30(2009), 1456-1476.

References. Association Schemes

- E. Bannai, T. Ito, Algebraic Combinatorics I: Association Schemes, Benjamin/Cummings, Menlo Park, CA, 1984;
- R.A. Bailey, Association Schemes: Designed Experiments, Algebra and Combinatorics, Cambridge University Press, Cambridge, 2004;
- P.-H. Zieschang, An algebraic approach to association schemes, Springer-Verlag, Berlin,1996;
- P.-H. Zieschang, Theory of Association Schemes, Springer-Verlag, Berlin, 2005;
- A.E. Brouwer, A.M. Cohen, A. Neumaier, Distance-Regular Graphs, Springer-Verlag, Berlin, 1989.

References. Schur rings

- H. Wielandt, Finite Permutation Groups, Academic press, New York, London, 1964;
- W.R. Scott, Group Theory, Prentice-Hall, 1964;
- M. Klin, M. Muzychuk, R.Pöschel, The isomorphism problem for circulant graphs via Schur rings theory, DIMACS, Ser. Discrete Math. Theor. Comput. Sci. 56, 2001;
- M.Muzychuk and I.Ponomarenko, Schur rings, Europ. J. of Comb., 30 (2009), 1526-1539.

Lecture 1.

Notation: binary relations

Let $R, S \subseteq \Omega^2$ be binary relations. Then

- $S^* := \{(\alpha, \beta) : \ (\beta, \alpha) \in S\}$;
- S is symmetric (antisymmetric) if $S = S^*$ ($S \cap S^* = \emptyset$ resp.);
- $\alpha S := \{\beta \in \Omega : \ (\alpha, \beta) \in S\}$, $S\alpha := \alpha S^*$;
- $D(S) := \{\alpha \in \Omega : \ \alpha S \neq \emptyset\}$, $R(S) := D(S^*)$;
- $RS = \{(\alpha, \beta) : \ \alpha R \cap S\beta \neq \emptyset\}$;
- $R^+ = \bigcup_{i=0}^{\infty} R^i$ is the transitive closure of R;
- $1_\Omega := \{(\omega, \omega) : \ \omega \in \Omega\}$.

Each permutation $g \in \mathrm{Sym}(\Omega)$ is considered as a binary relation. Thus $\alpha g = \{\alpha^g\}$ and $g^* = g^{-1}$.

Notation: partitions

- $\mathcal{P} \vdash \Omega$ means that $\mathcal{P}$ is a partition of Ω.
- $\mathcal{P} \sqsubseteq \mathcal{C} \iff \mathcal{C}$ is a refinement of $\mathcal{P}$;
- Lattice operations are denoted as $\mathcal{P} \vee \mathcal{C}$ and $\mathcal{P} \wedge \mathcal{C}$ ($\mathcal{P} \vee \mathcal{C}$ is the partition the classes of which are the intersections of classes of $\mathcal{P}$ and $\mathcal{C}$);
- if $\mathcal{P} \vdash \Omega$ then $\mathcal{P}^\cup$ denotes the set of all possible unions of elements in $\mathcal{P}$;
- $\mathcal{C} \vdash \Omega^2 \implies \mathcal{C}^* := \{C^* : \ C \in \mathcal{C}\}$.

Algorithms

- an algorithm can be thought as a sequence of steps from what we have (input) to what we want to get (output),
- depending on a computational model one has to define the size of the input/output, and possible "elementary" steps,
- the complexity of an algorithm is the number of "elementary" steps as the function of the input size.

Example: transitivity test

Input: a group $G \leq \mathrm{Sym}(\Omega)$ given by a generator set S.
Output: "YES" or "NO" depending on whether G is transitive.
Step 1. Take $\alpha \in \Omega$ and set $\Omega_0 := \{\alpha\}$. Set $S := S \cup \{1_G\}$.
Step 2. While $(\Omega_0)^S \neq \Omega_0$ do $\Omega_0 := (\Omega_0)^S$.
Step 3. Output "YES" if $\Omega_0 = \Omega$, and "NO" otherwise.

Exercise: The complexity of the algorithm is $O(nm)$ where $n = |\Omega|$ and $m = |S|$.

Graphs

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

Definition.
Graphs $\Gamma_1 = (\Omega_1, E_1)$ and $\Gamma_2 = (\Omega_2, E_2)$ are called isomorphic, $\Gamma_1 \cong \Gamma_2$, if there is a bijection $f : \Omega_1 \to \Omega_2$ such that

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

Such a bijection is called the isomorphism from Γ_1 to Γ_2; the set of all of them is denoted by $\mathrm{Iso}(\Gamma_1, \Gamma_2)$.The automorphism group of Γ is defined to be $\mathrm{Aut}(\Gamma) := \mathrm{Iso}(\Gamma, \Gamma)$.

The Graph Isomorphism Problem (ISO)

Problem ISO
Input: graphs Γ_1 and Γ_2
Output: "YES" or "NO" depending on whether or not $\Gamma_1 \cong \Gamma_2$.

- Given n-vertex graphs Γ_1 and Γ_2, and a bijection $f : \Omega_1 \to \Omega_2$ one can test in time $O(n^2)$ whether $f \in \mathrm{Iso}(\Gamma_1, \Gamma_2)$.
- Therefore ISO$\in$**NP**.
- An exhaustive search of all the possible bijections runs in exponential time $O(n!)$.
- At present it is not known whether ISO$\in$**P**.

The proof of the time bound of the best algorithm (up to now) for the ISO depends on the Classification of Finite Simple Groups.

Theorem (L.Babai, E.Luks and W.Kantor, 1984)
The isomorphism of n-vertex graphs can be tested in time $\exp(O(\sqrt{n \log n}))$.

Some problems equivalent to the ISO

The problems equivalent to the ISO (Mathon,1979):

- IMAP: given Γ and Γ' find $f \in \mathrm{Iso}(\Gamma, \Gamma')$ (if it exists),
- ICOUNT: given Γ and Γ' find $|\mathrm{Iso}(\Gamma, \Gamma')|$,
- ACOUNT: given Γ find $|\mathrm{Aut}(\Gamma)|$,
- AGEN: given Γ find a generators of the group $\mathrm{Aut}(\Gamma)$,
- APART: given Γ find its automorphic partition $\mathrm{Orb}(\mathrm{Aut}(\Gamma))$.

Isomorphism problem for colored graphs

Definition
A triple (Ω, Y, c) where $c : \Omega^2 \to Y$ is a surjection, is called a colored graph with the coloring function c.

The color classes form a partition $\mathcal{C} := \{c^{-1}(y) \mid y \in Y\}$ of Ω^2.

Definition
Two colored graphs (Ω, Y, c) and (Δ, Z, d) are isomorphic if there exists a bijection $f : \Omega \to \Delta$ such that

$$d(\alpha^f, \beta^f) = c(\alpha, \beta).$$

Remarks

- The ISO for colored graphs is equivalent to the ISO.
- One can consider a colored graph also as a partition.

Configurations and their isomorphisms

Definition.
A pair $(\Omega, \mathcal{C})$ where $\mathcal{C} \vdash \Omega^2$ is called a configuration on Ω. The elements of $\mathcal{C}$ are called basic relations or color classes.

Let $\mathcal{X} = (\Omega, \mathcal{C})$ and $\mathcal{X}' = (\Omega', \mathcal{C}')$ be two configurations. Then

- $\mathrm{Iso}(\mathcal{X}, \mathcal{X}') := \{f : \Omega \to \Omega' : \ f \text{ is a bijection and } \mathcal{C}^f = \mathcal{C}'\}$;
- $\mathcal{X} \cong \mathcal{X}' \iff \mathrm{Iso}(\mathcal{X}, \mathcal{X}') \neq \emptyset$;
- each $f \in \mathrm{Iso}(\mathcal{X}, \mathcal{X}')$ induces a bijection f^* between $\mathcal{C}$ and $\mathcal{C}'$ via $C^{f^*} = C^f$, $C \in \mathcal{C}$;
- $\mathrm{Iso}(\mathcal{X}) := \mathrm{Iso}(\mathcal{X}, \mathcal{X}) = \{g \in \mathrm{Sym}(\Omega) : \ \mathcal{C}^g = \mathcal{C}\}$;
- $\mathrm{Aut}(\mathcal{X}) := \{g \in \mathrm{Sym}(\Omega) : \ \forall C \in \mathcal{C} : \ C^g = C\}$.

Cayley graphs and their isomorphisms

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

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

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

Definition
Two Cayley graphs $\mathrm{Cay}(H,S)$ and $\mathrm{Cay}(K,T)$ are Cayley isomorphic if there exists a group isomorphism $f : H \to K$ which is a graph isomorphism too, that is

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

The graphs $\mathrm{Cay}(\{\pm 1\}, \mathbb{Z}_5)$ and $\mathrm{Cay}(\{\pm 2\}, \mathbb{Z}_5)$ are Cayley isomorphic.

A characterization of Cayley graphs

The automorphism group of a Cayley graph $\mathrm{Cay}(H,S)$ contains a regular subgroup $H_R \leq \mathrm{Sym}(H)$ consisting the right translations

$$h_R : x \mapsto xh$$

for all $h \in H$.

Theorem (Sabidussi)
A graph $\Gamma = (\Omega, E)$ is isomorphic to a Cayley graph over a group H if and only if $\mathrm{Aut}(\Gamma)$ contains a regular subgroup isomorphic to H.

Proof.

- Pick a base point $\omega \in \Omega$.
- Define a bijection $f : \Omega \to H$, $\alpha \mapsto \bar{\alpha}$ where $\omega^{\bar{\alpha}} = \alpha$.
- Set $S = \{\bar{\alpha} : \ \alpha \in E\omega\}$.
- Now $f \in \mathrm{Iso}(\Gamma, \mathrm{Cay}(H,S))$:

$$(\alpha,\beta) \in E \ \Leftrightarrow \ (\omega^{\bar{\alpha}}, \omega^{\bar{\beta}}) \in E \ \Leftrightarrow \ (\omega^{\bar{\alpha}\bar{\beta}^{-1}}, \omega) \in E \ \Leftrightarrow \ \bar{\alpha}\bar{\beta}^{-1} \in S.$$

Cayley representations of graphs

Definition
Under a Cayley representation of a graph Γ over a group H we mean any graph $\mathrm{Cay}(H,S)$ isomorphic to Γ.

Remark: graph can have Cayley representations over non-isomorphic groups.

Exercise:

- What happens with S if one replaces the base point?
- Find all Cayley representations of $\mathrm{Cay}(\mathbb{Z}_6, \{\pm 1, 3\})$ and 3-dim cube.

Lecture 2.

Isomorphism problems for Cayley graphs

Problems
Given a group H and graphs $\Gamma = \mathsf{Cay}(H,S)$ and $\Gamma' = \mathsf{Cay}(H,S')$ we have the following problems:

- IMAP: find $f \in \mathrm{Iso}(\Gamma,\Gamma')$ (if it exists),
- ICOUNT: find $|\mathrm{Iso}(\Gamma,\Gamma')|$,
- ACOUNT: find $|\mathrm{Aut}(\Gamma)|$,
- AGEN: find generators of the group $\mathrm{Aut}(\Gamma)$.

Recognizing problem:
CGR: given a graph Θ test whether it is a Cayley graph over H.

Isomorphism problem for finite groups
Construction
For a finite group K set $\Gamma(K)$ to be a graph with vertex set $K \times K$ such that

$$(a,b) \sim (c,d) \iff a = c \ \vee \ b = d \ \vee \ ab = cd.$$

Theorem (Moorhouse, 1991)
$K_1 \cong K_2 \iff \Gamma(K_1) \cong \Gamma(K_2)$.

Exercise

- $\Gamma(K)$ is a Cayley graph over $K \times K$.
- $\Gamma(\mathbb{Z}_4) \ncong \Gamma(\mathbb{Z}_2 \times \mathbb{Z}_2)$:

$$\mathbb{Z}_4 \to \begin{matrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{matrix} \qquad \mathbb{Z}_2 \times \mathbb{Z}_2 \to \begin{matrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{matrix}$$

Naive vertex classification
Denote by $d_\Gamma(\alpha)$ the valency of the vertex α in the graph Γ, and by $d_\Gamma(\alpha, C)$ the valency of α in a vertex color class C .

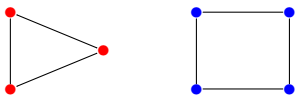
Naive vertex classification
Given a graph Γ we construct an $\mathrm{Aut}(\Gamma)$-invariant vertex coloring.

- Put vertices α and β in the same class iff $d_\Gamma(\alpha) = d_\Gamma(\beta)$;
- Iteratively, put vertices α and β in the same class iff $d_\Gamma(\alpha, C) = d_\Gamma(\beta, C)$ for all color classes C.

Comments

- The algorithm correctly finds $\mathrm{Orb}(\mathrm{Aut}(\Gamma))$ for the class of trees (G.Tinhofer, 1985), for almost all graphs (L.Babai, P.Erdös, S.Selkow, 1980).
- The algorithm fails when Γ is regular and $\mathrm{Aut}(\Gamma)$ is intransitive.

The Weisfeiler-Leman algorithm
No automorphism moves red points to blue ones:



To distinguish vertices we need to color edges of Γ.
WL-algorithm (Weisfeiler-Leman (1968)
Input: graph $\Gamma = (\Omega, E)$.
Output: an $\mathrm{Aut}(\Gamma)$-invariant coloring of Ω^2.

Step 1. Set $\mathcal{C} = \{1_\Omega\} \cup \{E\} \cup \{\Omega^2 \setminus (E \cup 1_\Omega)\}$.

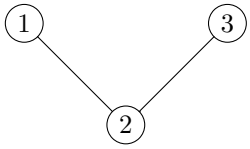
Step 2. For all $(\alpha, \beta) \in \Omega \times \Omega$ and $R, S \in \mathcal{C}$ find the number

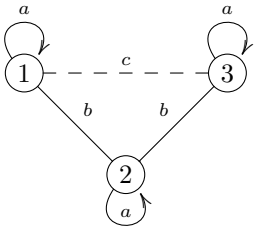
$$c(\alpha, \beta; R, S) = |\alpha R \cap S\beta|.$$

Step 3. Build a new partition $\mathcal{C} := \mathrm{bl}(\mathcal{C})$ by putting (α, β) and (α', β') to the same class if $|\alpha R \cap S\beta| = |\alpha' R \cap S\beta'|$ for all $R, S \in \mathcal{C}$.

Step 4. Repeat the procedure till $|\mathcal{C}|$ stop to increase.

The WL-algorithm: very small example





Initial coloring

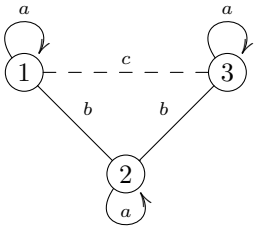
Graph:

Adjacency matrix:

$$A = \begin{pmatrix} a & b & c \\ b & a & b \\ c & b & a \end{pmatrix}.$$

First iteration

Graph:

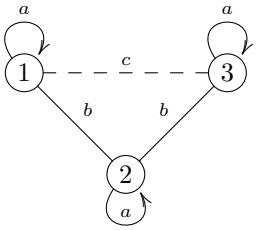


Adjacency matrix:

$$A^2 = \begin{pmatrix} a^2+b^2+c^2 & ab+ba+cb & ac+b^2+ca \\ ba+ab+bc & 2b^2+a^2 & bc+ab+ba \\ ca+b^2+ac & cb+ba+ab & c^2+b^2+a^2 \end{pmatrix}.$$

First iteration

Graph:



Adjacency matrix:

$$A^2 = \begin{pmatrix} a^2+b^2+c^2 & ab+ba+cb & ac+b^2+ca \\ bc+ab+ba & 2b^2+a^2 & bc+ab+ba \\ ac+b^2+ca & ab+ba+cb & c^2+b^2+a^2 \end{pmatrix}.$$

Second iteration

Graph:

Adjacency matrix:

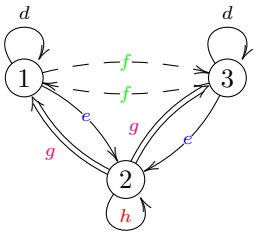
$$A = \begin{pmatrix} d & e & f \\ g & h & g \\ f & e & d \end{pmatrix}$$

WL-refinement (operation WL)

The correctness of the WL-algorithm (i.e. that it is stopped) follows from the following statements.

Lemma

1. $\mathcal{C} \sqsubseteq \mathcal{S} \implies \mathsf{WL}(\mathcal{C}) \sqsubseteq \mathsf{WL}(\mathcal{S})$,
2. $\mathcal{C}^* = \mathcal{C} \implies \mathsf{WL}(\mathcal{C})^* = \mathsf{WL}(\mathcal{C})$,
3. $1_\Omega \in \mathcal{C}^\cup \implies \mathcal{C} \sqsubseteq \mathsf{WL}(\mathcal{C})$.



Theorem
If a partition $\mathcal{C} \vdash \Omega^2$ satisfies the conditions $1_\Omega \in \mathcal{C}$ and $\mathcal{C}^* = \mathcal{C}$, then $\text{Ы}(\mathcal{C})$ satisfies the same conditions and $\mathcal{C} \sqsubseteq \text{Ы}(\mathcal{C})$.

Canonical WL-refinement

Proposition
Let $f : \Omega \to \Delta$ be a bijection that maps a partition $\mathcal{C}$ of Ω^2 onto a partition $\mathcal{T}$ of Δ^2 (i.e. $\mathcal{C}^f = \mathcal{T}$). Then $\text{Ы}(\mathcal{C})^f = \text{Ы}(\mathcal{T})$.

Corollary
Let Γ be a graph and $\mathcal{C}$ the stable partition obtained by the WL-algorithm. Then $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\mathcal{C})$.

Given an ordered partition $\vec{\mathcal{C}} = (S_1, ..., S_m)$ of Ω^2 the WL-algorithm produces a unique (canonical) ordering of the refinement $\text{Ы}(\mathcal{C})$ (denoted as $\text{Ы}(\vec{\mathcal{C}})$), i.e.

$$\vec{\mathcal{C}}^f = \vec{\mathcal{T}} \implies \text{Ы}(\vec{\mathcal{C}})^f = \text{Ы}(\vec{\mathcal{T}})$$

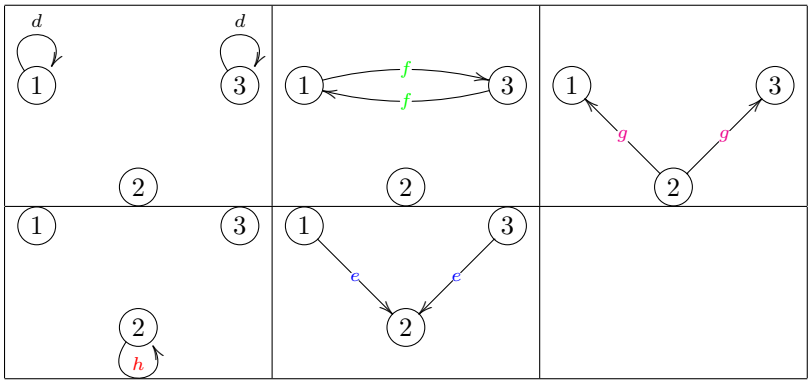
Coherent configurations (D. Higman, 1970)
The output partition of the Weisfeiler-Leman algorithm forms a coherent configuration, i.e. a pair $\mathcal{X} = (\Omega, \mathcal{C})$ such that:

1. $\mathcal{C}$ is a partition of $\Omega \times \Omega$,
2. $1_\Omega \in \mathcal{C}^\cup$,
3. $\mathcal{C}^* = \mathcal{C}$,
4. $\mathcal{C} = \text{Ы}(\mathcal{C})$, or, equivalently, for all $R, S, T \in \mathcal{C}$ the intersection number $c_{RS}^T = |\alpha R \cap S\beta|$ does not depend on the choice of $(\alpha, \beta) \in T$.

Terminology:

- the degree and rank of $\mathcal{X}$ are the numbers $|\Omega|$ and $|\mathcal{C}|$,
- the basic relations and relations of $\mathcal{X}$ are the elements of $\mathcal{C}$ and of $\mathcal{C}^\cup$,
- the configuration $\mathcal{X}$ is homogeneous (or association scheme, or scheme), if $1_\Omega \in \mathcal{C}$.

Coherent configurations: a concrete example.



Coherent configurations: relations

Proposition
Let $\mathcal{X} = (\Omega, \mathcal{C})$ be a coherent configuration. Then

- the set $\mathcal{C}^\cup$ is closed with repect to boolean operations;
- $1_\Omega, \Omega^2 \in \mathcal{C}^\cup$;
- $(\mathcal{C}^\cup)^* = \mathcal{C}^\cup$;
- $\mathcal{C}^\cup$ is closed with respect to relational product.

Coherent configurations: fibers

Definition
A fiber of $\mathcal{X}$ is a set $\Delta \subset \Omega$ such that $1_\Delta \in \mathcal{C}$; the set of all fibers is denoted by $\Phi = \Phi(\mathcal{X})$.

Proposition

- $\mathcal{X}$ is a scheme if and only if $|\Phi| = 1$,
- $\Omega = \bigcup_{\Delta\in\Phi} \Delta$,
- for any $S \in \mathcal{C}$ the sets $D(S)$ and $R(S)$ are fibers of $\mathcal{X}$,
- for any $S \in \mathcal{C}$ and $\alpha \in D(S)$ we have $|\alpha S| = c^T_{SS^*}$ where $T = 1_{D(S)}$; the number $n_S = c^T_{SS^*}$ is called the valency of S,
- for any $\Delta \in \Phi$ the set $\mathcal{C}_\Delta := \{C \in \mathcal{C} : \ D(C) = \Delta, R(C) = \Delta\}$ form a homogeneous cc on Δ, called a homogeneous constituent of $\mathcal{C}$.

Exercises

Exercises:

- Prove that if the symmetrization $\{C \cup C^* \,|\, C \in \mathcal{C}\}$ of a cc $\mathcal{X} = (\Omega, \mathcal{C})$ is a cc then $\mathcal{C}$ is a scheme.
- Enumerate up to an isomorphism all cc of degree $2, 3, 4$.
- Prove that for any triple $R, S, T \in \mathcal{C}$ it holds that
$$c^{T^*}_{RS}|T^*| = c^{R^*}_{ST}|R^*| = c^{S^*}_{TR}|S^*|.$$

Isomorphisms between coherent configurations

Definition
Two coherent configuration $\mathcal{X} = (\Omega, \mathcal{C})$ and $\mathcal{X}' = (\Omega', \mathcal{C}')$ are called (combinatorially) isomorphic if there exist bijections $f : \Omega \to \Omega'$ and $\phi : \mathcal{C} \to \mathcal{C}'$ such that
$$\forall_{\alpha,\beta\in\Omega} \ \ (\alpha, \beta) \in C \iff (\alpha^f, \beta^f) \in C^\phi.$$
The set of all isomorphisms between $\mathcal{X}$ and $\mathcal{X}'$ is denoted as $\mathrm{Iso}(\mathcal{X}, \mathcal{X}')$.

Comments

- ϕ is induced by f, and hence is usually omitted;
- $\mathrm{Iso}(\mathcal{X}) := \mathrm{Iso}(\mathcal{X}, \mathcal{X})$;
- $\mathrm{Aut}(\mathcal{X}) = \{f \in \mathrm{Sym}(\Omega) : \ S^f = S \text{ for all } S \in \mathcal{C}\}$,
- $\mathrm{Aut}(\mathcal{X}) \trianglelefteq \mathrm{Iso}(\mathcal{X})$.

Lecture 3.

Coherent configurations generated by a graph

Theorem
Let $\langle\!\langle \Gamma \rangle\!\rangle \vdash \Omega^2$ be the WL-closure of a graph $\Gamma = (\Omega, E)$ obtained by applying WL-algorithm to Γ. Then

1. $E \in \langle\!\langle \Gamma \rangle\!\rangle^\cup$;
2. $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\langle\!\langle \Gamma \rangle\!\rangle)$.

Examples: strongly regular graphs

Definition
An undirected graph $\Gamma = (\Omega, E)$ is called strongly regular if its WL-closure has rank three. In other words, WL-algorithm stops at the first iteration and $\langle\langle\Gamma\rangle\rangle = \{1_\Omega, E, E^c\}$.

Proposition
A graph $\Gamma = (\Omega, E)$ is strongly regular if and only if there exist non-negative integers k, λ, μ such that

1. Γ is k-regular,
2. any two adjacent vertices have exactly λ common neighbors,
3. any two non-adjacent vertices have exactly μ common neighbors.

Exercises
Let $\Gamma = (\Omega, E)$ be a strongly regular graph with parameters v, k, λ, μ. Then

- the complement to Γ is strongly regular;
- $(k - \lambda - 1)k = (v - k - 1)\mu$;
- Γ is disconnected iff $\lambda = k - 1$ iff Γ is a disjoint union of K_k;
- the graph $\Gamma(K)$ built from the Cayley table of a group K is strongly regular;
- the complements to $\Gamma(\mathbb{Z}_4)$ and $\Gamma(\mathbb{Z}_2 \times \mathbb{Z}_2)$ are the only strongly regular graph with parameters $v = 16$, $k = 6$ and $\lambda = \mu = 2$.

Examples: permutation groups
Let $G \le \mathrm{Sym}(\Omega)$ be a permutation group. It acts on $\Omega \times \Omega$:

$$(\alpha, \beta)^g := (\alpha^g, \beta^g), \qquad \alpha, \beta \in \Omega,\ g \in G.$$

Proposition
Set $\mathcal{C} := \mathrm{Orb}(G, \Omega \times \Omega)$. Then

1. $\mathrm{Inv}(G) := (\Omega, \mathcal{C})$ is a coherent configuration (of G),
2. the basic relations of $\mathcal{X}$ are the 2-orbits of G,
3. $\Phi(\mathcal{X}) = \mathrm{Orb}(G, \Omega)$,
4. $\mathcal{X}$ is a scheme if and only if G is transitive.

Definition.
A coherent configuration $\mathcal{X}$ is schurian if $\mathcal{X} = \mathrm{Inv}(G)$ for some G.

The Schurity problem is to check whether or not given a coherent configuration is schurian.

Exercise
Let $G = \mathbb{Z}_2^3$ and $G_1 = \langle(1,0,0)\rangle, G_2 = \langle(0,1,0)\rangle, G_3 = \langle(0,0,1)\rangle$.

Set $\Omega = G/G_1 \cup G/G_2 \cup G/G_3$ and $\mathcal{C} = \mathrm{Orb}(G, \Omega^2)$.

- what is the rank of $\mathcal{X} = (\Omega, \mathcal{C})$?
- find the fibers and describe the basic graphs of $\mathcal{X}$;
- find homogeneous constituents;
- find $\mathrm{Iso}(\mathcal{X})$ and $\mathrm{Aut}(\mathcal{X})$;

Galois correspondence between cc and groups

Definition
Let $\mathcal{X} = (\Omega, \mathcal{C}), \mathcal{X}' = (\Omega, \mathcal{C}')$ be two coherent configurations. We say that $\mathcal{X}$ is a fusion of $\mathcal{X}'$ (equivalently $\mathcal{X}'$ is a fission of $\mathcal{X}$), notation $\mathcal{X} \sqsubseteq \mathcal{X}'$ if $\mathcal{C} \sqsubseteq \mathcal{C}'$.

Proposition
Let $\mathcal{X}, \mathcal{X}'$ be two coherent configurations on Ω and $G, H \leq \mathrm{Sym}(\Omega)$. Then

- $\mathcal{X} \sqsubseteq \mathcal{X}' \implies \mathrm{Aut}(\mathcal{X}) \geq \mathrm{Aut}(\mathcal{X}')$;
- $H \leq G \implies \mathrm{Inv}(H) \sqsupseteq \mathrm{Inv}(G)$;
- $G \leq \mathrm{Aut}(\mathrm{Inv}(G))$ and $\mathcal{X} \sqsubseteq \mathrm{Inv}(\mathrm{Aut}(\mathcal{X}))$.

Thus the mappings $\mathcal{X} \mapsto \mathrm{Aut}(\mathcal{X})$ and $G \mapsto \mathrm{Inv}(G)$ form a Galois correspondence between coherent configurations on Ω and permutation groups on Ω.

Galois closed objects

Definition

- The group $G^{(2)} := \mathrm{Aut}(\mathrm{Inv}(G))$ is called a 2-closure of $G \leq \mathrm{Sym}(\Omega)$; G is 2-closed if $G = G^{(2)}$.
- The cc $\mathrm{Sch}(\mathcal{X}) := \mathrm{Inv}(\mathrm{Aut}(\mathcal{X}))$ is called a schurian closure of a cc $\mathcal{X} = (\Omega, \mathcal{C})$; $\mathcal{X}$ is schurian if $\mathrm{Sch}(\mathcal{X}) = \mathcal{X}$.

Theorem
The mappings $(\mathrm{Aut}, \mathrm{Inv})$ are bijections between schurian coherent configurations on Ω and 2-closed subgroups of $\mathrm{Sym}(\Omega)$.

The ISO is polynomially equivalent to the problem of finding the schurian closure of a coherent configuration.

Matrix operations

Notation
Let $A, B \in M_\Omega(\mathbb{F})$ be arbitrary matrices. We denote by

- AB (or $A \cdot B$) the usual matrix product;
- $A \circ B$ the Schur-Hadamard (component-wise) product, i.e. $(A \circ B)_{\alpha\beta} := A_{\alpha\beta} B_{\alpha\beta}$;
- $A^\top$ the transposed of A;
- I_Ω the identity matrix;
- J_Ω the all one matrix.

Proposition
The algebra $(M_\Omega(\mathbb{F}), \circ)$ is a commutative associative algebra with identity J_Ω. It is isomorphic to $\mathbb{F}^n$ where $n = |\Omega|^2$.

Idempotents
Let $(\mathcal{A}, \star)$ be finite dimensional algebra over field $\mathbb{F}$.
Definition

- $e \in \mathcal{A}, e \neq 0$ is $\star$-idempotent if $e \star e = e$;
- idempotents e, f are orthogonal if $e \star f = f \star e = 0$;
- idempotent e is minimal if it is not a sum $e = e_1 + e_2$ of pairwise orthogonal idempotents e_1, e_2.

Exercise:

- a matrix $E \in M_\Omega(\mathbb{F})$ is $\cdot$-idempotent iff E is similar to a $(0,1)$-diagonal matrix;
- a matrix $E \in M_\Omega(\mathbb{F})$ is $\circ$-idempotent iff E is $(0,1)$-matrix iff $E = A(S)$ is the adjacency matrix of some $S \subseteq \Omega^2$;
- a symmetric matrix is $\cdot$- and $\circ$-idempotent iff it's $(0,1)$-diagonal matrix.

Coherent (cellular) algebras

Definition.
A subspace $\mathcal{A} \leq M_\Omega(\mathbb{F})$ is called a coherent (or cellular) algebra if it contains I_Ω, J_Ω and is closed with respect to $\cdot, \circ, {}^\top$.

Examples: $\langle I_\Omega, J_\Omega \rangle$ and $M_\Omega(\mathbb{F})$.

Proposition
Let $\mathcal{X} = (\Omega, \mathcal{C})$ be a coherent configuration. Then the linear span $\mathbb{F}\mathcal{X} = \mathbb{F}\mathcal{C} := \langle A(C) \rangle_{C \in \mathcal{C}}$ is a coherent algebra of dimension $|\mathcal{C}|$. It is called the adjacency (or Bose-Mesner) algebra of $\mathcal{X}$.

The basis $\{A(C) : C \in \mathcal{C}\}$ is called the standard basis of $\mathbb{F}\mathcal{X}$; it consists of $(0,1)$-matrices and they are minimal $\circ$-idempotents. Moreover,

$$A(S)A(T) = \sum_{R \in \mathcal{C}} c_{ST}^R A(R), \qquad S, T \in \mathcal{C}.$$

Coherent algebras are adjacency algebras

Theorem
Every coherent algebra $\mathcal{A} \leq M_\Omega(\mathbb{F})$ has a unique basis consisting of minimal $\circ$-idempotents which are pairwise orthogonal. If $\mathsf{char}(\mathbb{F}) = 0$ then $\mathcal{A}$ is the adjacency algebra of a uniquely determined coherent configuration.

Proof. $\mathcal{A}$ is a $\circ$-subalgebra of $(M_\Omega(\mathbb{F}), \circ) \cong (\mathbb{F}^n, \circ), n = |\Omega|^2$.

Lemma
Let $\mathcal{A}$ be a k-dimensional subalgebra of $(\mathbb{F}^n, \circ)$. Then there exists a unique basis $A_1, ..., A_k$ of $\mathcal{A}$ consisting of minimal, pairwise orthogonal, $\circ$-idempotents. Each $\circ$-idemoptent of $\mathcal{A}$ is a $(0,1)$-linear combination of $A_1, ..., A_k$ and $A_1 + ... + A_k$ is the unit of $\mathcal{A}$.

Proof of the Theorem (the end)

- $A_i = A(R_i), R_i \subseteq \Omega^2$;
- $i \neq j \implies A_i \circ A_j = 0 \implies R_i \cap R_j = \emptyset$;
- $\sum_{i=1}^k A_i = J_\Omega \implies \bigcup_i R_i = \Omega^2$;
- $I_\Omega = \sum_i A_i \implies 1_\Omega = \bigcup_i R_i$;
- $A_i A_j = \sum_k c_{ij}^k A_k$ for some $c_{ij}^k \in \mathbb{F}$;
- $(A_i A_j)_{\alpha\beta} = c_{ij}^k$ where k is defined by $(\alpha, \beta) \in R_k$;
- if $\mathrm{char}(\mathbb{F}) = 0$, then $(A_i A_j)_{\alpha\beta} = |\alpha R_i \cap R_j \beta| \implies |\alpha R_i \cap R_j \beta| = c_{ij}^k$.

Thus coherent configurations and coherent algebras are the same objects presented by different languages. In what follows we'll switch between the languages freely.

Lecture 4.

Isomorphisms between coherent algebras

Definition
Given two coherent algebras $\mathcal{A} \leq M_\Omega(\mathbb{F}), \mathcal{A}' \leq M_{\Omega'}(\mathbb{F})$, a linear bijection $L : \mathcal{A} \to \mathcal{A}'$ is called an (algebraic) isomorphism if

- $L(XY) = L(X)L(Y)$;
- $L(X \circ Y) = L(X) \circ L(Y)$;
- $L(X^\top) = L(X)^\top$.

Proposition
Let $L : \mathbb{F}\mathcal{X} \to \mathbb{F}\mathcal{X}'$ be an algebraic isomorphism between the adjacency algebras of coherent configurations $\mathcal{X}$ and $\mathcal{X}'$. Then there exists a bijection $\varphi : \mathcal{C} \to \mathcal{C}'$ such that $L(A(C)) = A(C^\varphi)$ and $c_{RS}^T = c'^{T^\varphi}_{R^\varphi S^\varphi}$. Vice versa, any such φ extends uniquely up to an algebraic isomorphism between $\mathbb{F}\mathcal{X}$ and $\mathbb{F}\mathcal{X}'$; φ is called an algebraic isomorphism from $\mathcal{X}$ onto $\mathcal{X}'$.

Properties of algebraic isomorphisms

Proposition
Let φ be an algebraic isomorphism from a coherent configuration $\mathcal{X} = (\Omega, \mathcal{C})$ to a coherent configuration $\mathcal{X}' = (\Omega', \mathcal{C}')$. Then

- $(RS)^\varphi = R^\varphi S^\varphi$ for any $R, S \in \mathcal{C}^\cup$;
- for each $\Delta \in \Phi(\mathcal{X})$ there exists a unique $\Delta' \in \Phi(\mathcal{X}')$ such that $(1_\Delta)^\varphi = 1_{\Delta'}$;
- the mapping $\Delta \mapsto \Delta'$ is a bijection from $\Phi(\mathcal{X})$ onto $\Phi(\mathcal{X}')$;
- $D(S^\varphi) = D(S)^\varphi$ and $R(S^\varphi) = R(S)^\varphi$ for all $S \in \mathcal{C}$;
- $|n_{S^\varphi}| = |n_S|$ for each $S \in \mathcal{C}$;
- $|\Delta^\varphi| = |\Delta|$ for any $\Delta \in \Phi(\mathcal{X})$.

Isomorphisms between coherent algebras

Proposition
Given $f \in \mathrm{Iso}(\mathcal{X}, \mathcal{X}')$ the mapping $\varphi_f : S \mapsto S^f$ is an algebraic isomorphism from $\mathcal{X}$ onto $\mathcal{X}'$; we say that φ_f is induced by the isomorphism f.

All algebraic automorphisms of $\mathcal{X}$ to itself form a subgroup of $\mathrm{Sym}(\mathcal{C})$ denoted as $\mathsf{Alg}(\mathcal{X})$. Notice that

$$\mathrm{Iso}(\mathcal{X})/\mathrm{Aut}(\mathcal{X}) \hookrightarrow \mathsf{Alg}(\mathcal{X}).$$

Proposition
Given $A \le \mathsf{Alg}(\mathcal{X})$ the subspace

$$(\mathbb{F}\mathcal{X})^A := \{x \in \mathbb{F}\mathcal{X} : \ x^a = x \text{ for all } a \in A\}$$

is a coherent algebra; the corresponding coherent configuration is denoted by $\mathcal{X}^A$ and is called an algebraic fusion of $\mathcal{X}$.

Coherent closure: definition

Proposition
Let $\mathcal{X} = (\Omega, \mathcal{C})$ and $\mathcal{X}' = (\Omega, \mathcal{C}')$ be coherent configurations. Then

- $\mathbb{F}\mathcal{X} \subseteq \mathbb{F}\mathcal{X}'$ if and only if $\mathcal{C} \sqsubseteq \mathcal{C}'$;
- $\mathbb{F}\mathcal{X} \cap \mathbb{F}\mathcal{X}' = \mathbb{F}(\mathcal{C} \wedge \mathcal{C}')$ is a coherent algebra.

In general, $\mathbb{F}(\mathcal{C} \vee \mathcal{C}')$ is not necessarily coherent algebra.

Proposition
Let $A_1, ..., A_m \in M_\Omega(\mathbb{F})$. Then the intersection of all coherent algebras containing $A_1, ..., A_m$ is a coherent algebra; it is called the coherent closure of $A_1, ..., A_m$ and denoted by $\langle\langle A_1, ..., A_m \rangle\rangle$.

The definition of the coherent closure is not constructive; the constructive one is given by means of the WL-algorithm.

Coherent closure: properties

Definition
Given matrices $A_1, ..., A_k \in M_\Omega(\mathbb{F})$ we define a partition $\mathcal{P}(A_1, ..., A_k)$ of Ω^2 via the following equivalence relation:

$$(\alpha, \beta) \sim (\gamma, \delta) \iff (A_i)_{\alpha\beta} = (A_i)_{\gamma\delta} \text{ for all } 1 \le i \le k.$$

Proposition
Let $\mathcal{X} = (\Omega, \mathcal{C})$ be a coherent configuration. Then

1. if $A_1, ..., A_k \in \mathbb{F}\mathcal{X}$, then $\mathcal{P}(A_1, ..., A_k) \sqsubseteq \mathcal{C}$,
2. if $\mathcal{S} \vdash \Omega^2$ and $\mathcal{S} \sqsubseteq \mathcal{C}$, then $\mathsf{Bl}(\mathcal{S}) \sqsubseteq \mathcal{C}$.

Coherent closure: computation

Finding coherent closure by means of the WL-algorithm:
Given matrices $A_1, ..., A_k \in M_\Omega(\mathbb{F})$ do:

Step 1. Set $\mathcal{S}_0 := \mathcal{P}(A_1, ..., A_k, A_1^\top, ..., A_k^\top, I_\Omega)$ and $i := 0$;

Step 2. While $\mathcal{S}_i \neq \text{Ы}(\mathcal{S}_i)$ do $i := i + 1$ and $\mathcal{S}_i := \text{Ы}(\mathcal{S}_i)$;

Step 3. Output $\mathbb{F}\mathcal{S}$ where $\mathcal{S} = \mathcal{S}_i$.

Theorem
The above algorithm computes the coherent closure $\langle\langle A_1, ..., A_k \rangle\rangle$ of the matrices $A_1, ..., A_k$.

Proof. Let $\mathcal{X} = (\Omega, \mathcal{C})$ be the underlying coherent configuration of $\langle\langle A_1, ..., A_k \rangle\rangle$, i.e. $\langle\langle A_1, ..., A_k \rangle\rangle = \mathbb{F}\mathcal{X}$. Then $\mathcal{S}_0 \sqsubseteq \mathcal{C}$.

- Moreover, if $\mathcal{S}_i^* = \mathcal{S}_i$, $1_\Omega \in (\mathcal{S}_i)^\cup$ and $\mathcal{S}_i \sqsubseteq \mathcal{C}$ for $i \geq 0$, then the same holds for $i = i + 1$.
- Thus $\mathcal{S} \sqsubseteq \mathcal{C}$, and hence $\mathcal{S} = \mathcal{C}$.

The main property of the WL-algorithm

Theorem
Let

- $\vec{\mathcal{S}} = (S_1, ..., S_m)$ and $\vec{\mathcal{T}} = (T_1, ..., T_m)$ be ordered partitions of Ω^2 and Δ^2,
- $\langle\langle\vec{\mathcal{S}}\rangle\rangle = (P_1, ..., P_k)$ and $\langle\langle\vec{\mathcal{T}}\rangle\rangle = (Q_1, ..., Q_\ell)$ be the canonical ordering of the coherent closures produced by WL-algorithm,
- $f \in \mathrm{Iso}(\mathcal{S}, \mathcal{T})$ be such that $S_i^f = T_i$, $i = 1, \ldots, m$.

Then $k = \ell$ and $P_i^f = Q_i$, $i = 1, ..., k$. In particular, the mapping $P_i \mapsto Q_i$ is an algebraic isomorphism from $\langle\langle\mathcal{S}\rangle\rangle$ onto $\langle\langle\mathcal{T}\rangle\rangle$.

Thus the ISO can be reformulated as follows: test whether given an algebraic isomorphism is induced by a combinatorial one.

Coherent closure of a Cayley graph

Problem
Given a finite group H and two subsets $S, T \subseteq H$, decide whether $\mathsf{Cay}(H, S) \cong \mathsf{Cay}(H, T)$.

Proposition
The coherent closure $\mathcal{X} = \langle\langle\mathsf{Cay}(H, S)\rangle\rangle$ of the Cayley graph $\mathsf{Cay}(H, S)$ is a fusion scheme of $\mathrm{Inv}(H_R)$.

Proof.

- We have $\mathrm{Aut}(\mathcal{X}) = \mathrm{Aut}(\mathsf{Cay}(H, S)) \geq H_R$.
- Therefore $\mathcal{X}$ is a scheme and $\mathrm{Inv}(\mathrm{Aut}(\mathcal{X})) \sqsubseteq \mathrm{Inv}(H_R)$.
- Thus $\mathcal{X} \sqsubseteq \mathrm{Inv}(\mathrm{Aut}(\mathcal{X})) \sqsubseteq \mathrm{Inv}(H_R)$.

Exercise: the coherent configuration $\mathrm{Inv}(H_R)$ is homogeneous, and any basic relation of it is of the form $h_L \in \mathrm{Sym}(H)$ for some $h \in H$.

Association schemes

Proposition
A pair (Ω, S) where $\mathcal{S} \vdash \Omega^2$ is an association scheme (=homogeneous coherent configuration) if and only if the following statements hold:

- $1_\Omega \in \mathcal{S}$;
- $\mathcal{S}^* = \mathcal{S}$;
- $\text{Ы}(\mathcal{S}) = \mathcal{S}$.

Recall that the intersection numbers c_{RS}^T of the scheme (Ω, S) are defined so that

$$\forall S, R, T \in \mathcal{S} \quad \forall (\alpha, \beta) \in T : \quad |\alpha S \cap R\beta| = c_{RS}^T.$$

The number $n_S := c_{S\bar{S}}^{1_\Omega} = |\omega S|$ is called the valency of S.

Elementary properties of association schemes

Proposition
Let $(\Omega, \mathcal{S})$ be an association scheme. Then

- each relation $R \in \mathcal{S}^\cup$ is regular;
- the set $\mathcal{S}^\cup$ is closed under intersections, unions and complements;
- $1_\Omega, \Omega^2 \in \mathcal{S}^\cup$;
- $(\mathcal{S}^\cup)^* = \mathcal{S}^\cup$;
- $\mathcal{S}$ is closed under relational product;
- for any $S \in \mathcal{S}$ there exists m such that $1_\Omega \in S^m$;
- if $S \in \mathcal{S}^\cup$ and $S^+ = \cup_{i=0}^\infty S^i$, then $S^+ \in \mathcal{S}^\cup$;
- if $S \in \mathcal{S}^\cup$, then S^+ is an equivalence relation on Ω.

Lecture 5.

Main classes of association schemes

Definition
A scheme is $\mathcal{X} = (\Omega, \mathcal{S})$ is called

- symmetric if every $S \in \mathcal{S}$ is symmetric,
- antisymmetric if every $S \in \mathcal{S}$, $S \neq 1_\Omega$, is anti-symmetric,
- commutative if the algebra $\mathbb{F}\mathcal{X}$ is commutative.

Exercise: a symmetric scheme is always commutative.

Proposition
Let $(\Omega, \mathcal{S})$ be a scheme. Then

- $\sum_{S \in \mathcal{S}} n_S = |\Omega|$;
- $1 \leq |\mathcal{S}| \leq |\Omega|$;
- $|\mathcal{S}| = 2$ if and only if $\mathcal{S} = \{1_\Omega, \Omega^2 \setminus 1_\Omega\}$;
- $|\mathcal{S}| = |\Omega|$ if and only if $n_S = 1$ for all $S \in \mathcal{S}$.

Primitive and imprimitive schemes

Definition
A scheme $\mathcal{X} = (\Omega, \mathcal{S})$ is called imprimitive if $\mathcal{S}^\cup$ contains an equivalence relation E other than 1_Ω and Ω^2; the sets in Ω/E form a partition of Ω called the imprimitivity system of $\mathcal{S}$.

Proposition
Given an equivalence relation $E \in \mathcal{S}^\cup$ we have $|\Omega/E| \cdot n_E = |\Omega|$.

Proposition
The following statements are equivalent:

- $\mathcal{X}$ is imprimitive;
- there exists $S \in \mathcal{S}$ such that $1_\Omega \neq S^+ \neq \Omega^2$;
- there exists $\mathcal{T} \subset \mathcal{S}$ with $1 < |\mathcal{T}| < |\mathcal{S}|$ such that $\langle A(T) \rangle_{T \in \mathcal{T}}$ is a subalgebra of $\mathbb{F}\mathcal{X}$.

Schurian schemes

Recall that a scheme $\mathcal{X} = (\Omega, \mathcal{S})$ is schurian if there exists a group $G \leq \mathrm{Sym}(\Omega)$ such that $\mathcal{X} = \mathrm{Inv}(G)$. In this case

- G is transitive on Ω;
- $\omega S \in \mathrm{Orb}(G_\omega, \Omega)$ for all $\omega \in \Omega$ and $S \in \mathcal{S}$;
- the mapping $S \mapsto \{g \in G : \ \omega^g \in \omega S\}$ is a bijection from $\mathcal{S}$ onto the set of double cosets of G_ω in G;
- a rescaling of the above mapping is an isomorphism from $\mathbb{F}\mathcal{X}$ onto the Hecke algebra $\mathbb{F}(G_\omega \backslash G / G_\omega)$;
- G is primitive if and only if $\mathrm{Inv}(G)$ is primitive.

Thin 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 if and only if $\mathcal{S}$ is a regular subgroup of $\mathrm{Sym}(\Omega)$.

Example:

- (H, H_R) and (H, H_L) are thin schemes;
- the bijection $h \mapsto h^{-1}$ is an isomorphism from (H, H_R) onto (H, H_L);
- $\mathrm{Inv}(H_R) = H_L$ and $\mathrm{Inv}(H_L) = H_R$;
- $\mathrm{Aut}(H_L) = H_R$ and $\mathrm{Aut}(H_R) = H_L$.

Cayley schemes

Definition
An association scheme $\mathcal{X}$ which is a fusion of (H, H_L) is called a Cayley scheme over H, or equivalently, $\mathrm{Aut}(\mathcal{X}) \geq H_R$.

A basic relation S of such a scheme is a Cayley graph $\mathsf{Cay}(H, Se)$.

Proposition
Let $(H, \mathcal{R})$ be a Cayley scheme.Then the set $\mathcal{S} := \{Re : \ R \in \mathcal{R}\}$ is a partition of H, and

- $\{e\} \in \mathcal{S}$;
- $X^{(-1)} \in \mathcal{S}$ for all $X \in \mathcal{S}$;
- for any triple $X, Y, Z \in \mathcal{S}$ the number $c_{XY}^Z := |Y \cap X^{(-1)}z|$ does not depend on $z \in Z$.

Cayley schemes and Schur partitions

Definition
A partition $\mathcal{S}$ of a group H is called a Schur partition if it satisfies the above conditions, that is

- $\{e\} \in \mathcal{S}$;
- $X^{(-1)} \in \mathcal{S}$ for all $X \in \mathcal{S}$;
- for any triple $X, Y, Z \in \mathcal{S}$ the number $c_{XY}^Z := |Y \cap X^{(-1)}z|$ does not depend on $z \in Z$.

Notice that $|Y \cap X^{(-1)}z| = \{(y, x) \in Y \times X : \ yx = z\}$.

Proposition
Let $\mathcal{S}$ be a partition of H. Then the partition $\mathsf{Cay}(H, \mathcal{S}) := \{\mathsf{Cay}(H, X) : \ X \in \mathcal{S}\}$ of the set $H \times H$ is a scheme if and only if $\mathcal{S}$ is a Schur partition.

Group rings

Notation

- RH is the group algebra of H over a unitary ring R;
- if $x = \sum_h x_h h$ and $y = \sum_h y_h h$ belong to RH, then
$$xy := \sum_{h,f\in H} x_h y_f (hf) \quad \text{and} \quad x \circ y = \sum_{h\in H} (x_h y_h) h$$
are the convolution and the Schur-Hadamard product of x and y;
- any $\circ$-idempotent is of the form $\underline{X} := \sum_{h\in X} h$ where $X \subseteq H$;
- $\underline{\{h\}}$ is abbreviated as h;
- if $\mathcal{S} \vdash H$, then $\underline{\mathcal{S}} := \{\underline{X} : \ X \in \mathcal{S}\}$;
- for each $m \in \mathbb{Z}$ and $x \in RH$ we set $x^{(m)} := \sum_{h\in H} x_h h^m$.

Schur partitions and Schur rings

Proposition
Let $\mathcal{S} \vdash H$ be such that $\{e\} \in \mathcal{S}$ and $\mathcal{S}^{(-1)} = \mathcal{S}$. Then $\mathcal{S}$ is a Schur partition if and only if 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 over H if there exists a Schur partition $\mathcal{S} \vdash H$ such that $\mathcal{A} = \langle \underline{\mathcal{S}} \rangle$. The elements of $\mathcal{S}$ and $\mathcal{S}^{\cup}$ are called basic sets and $\mathcal{A}$-sets respectively.

Theorem
A vector space $\mathcal{A} \leq \mathbb{Q}H$ is a Schur ring if and only if $e, \underline{H} \in \mathcal{A}$ and $\mathcal{A}$ closed with respect to the 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

- $\mathcal{A} \subseteq \mathcal{B}$ if and only if $\mathcal{S} \sqsubseteq \mathcal{T}$;
- $\mathcal{A} \cap \mathcal{B} = \langle \underline{\mathcal{S} \wedge \mathcal{T}} \rangle$.

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

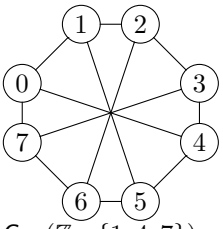
Theorem
Let $X \subseteq H$, $\mathcal{A} = \langle\langle \underline{X} \rangle\rangle$ a Schur ring generated by $\underline{X}$ and $\mathcal{S}$ the corresponding S-partition. Then $\langle\langle \mathrm{Cay}(H, X) \rangle\rangle = \mathrm{Cay}(H, \mathcal{S})$ and $S \in \mathcal{S}^{\cup}$.

Schur-Wielandt principle
For a function $f : \mathbb{Q} \to \mathbb{Q}$ and $x = \sum_{h\in H} x_h h$ set
$$f[x] := \sum_{h\in H} f(x_h) h.$$

Proposition
Let $f : \mathbb{Q} \to \mathbb{Q}$ be a function, $\mathcal{A}$ is an S-ring over H and $x \in \mathcal{A}$. Then $f[x] \in \mathcal{A}$.

Corollary
Let $\mathcal{A}$ be an S-ring over H, $x \in \mathcal{A}$ and $r \in Q$. Then the element $\underline{X}$ where $X = \{h \in H : \ x_h = r\}$, belongs to $\mathcal{A}$. In particular, X is an $\mathcal{A}$-set.

Proof. Follows from the Proposition because $X = f[x]$ where $f = \delta_r$ is the Kronecker delta-function.



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

Computation of $\langle\langle \underline{S} \rangle\rangle$ where $S = \{1,4,7\} \subseteq \mathbb{Z}_8$

Write $\underline{S} = \underline{\{1,4,7\}}$ as $c + c^4 + c^7$ where $c^8 = 1$. Then

- $\langle\langle \underline{S} \rangle\rangle$ contains $\underline{S}^2 = 3c^0 + c^2 + c^6 + 2c^5 + 2c^3$.
- Therefore $c^5 + c^3$, $c^2 + c^6 \in \langle\langle \underline{S} \rangle\rangle$.
- So $\langle\langle \underline{S} \rangle\rangle$ contains $(c^2 + c^6)^2 = 2c^0 + 2c^4$.
- Thus $\langle\langle \underline{S} \rangle\rangle = \langle c^0, c^4, c + c^7, c^2 + c^6, c^3 + c^5 \rangle$, and
- $\langle\langle \mathsf{Cay}(\mathbb{Z}_8, \{1,4,7\}) \rangle\rangle = \mathsf{Cay}(\mathbb{Z}_8, \{\{0\}, \{4\}, \{1,7\}, \{2,6\}, \{3,5\}\})$.

In other words, we found the coherent closure of the graph:

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

- $F = \mathsf{Inn}(H) \implies \mathbf{Z}(\mathbb{Q}[H])$ 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 e.

Properties of S-rings

Proposition
Let $\mathcal{S}$ be a Schur partition of H and $\mathsf{Cay}(H,\mathcal{S})$ the corresponding Cayley scheme. Then $\mathsf{Cay}(H,\mathcal{S})^\cup = \mathsf{Cay}(H,\mathcal{S}^\cup)$ 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 $E = \mathsf{Cay}(H,S), S \in \mathcal{S}^\cup$ is an equivalence iff S is a subgroup of H.

Definition
A subgroup $F \le H$ 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 $H_R \le G \le \mathrm{Sym}(H)$. Then the orbits of G_e form an S-partition.

Proof. Set $\mathcal{S} := \mathrm{Inv}(G)$. Then $H_R \le G \implies \mathcal{S} \sqsubseteq \mathrm{Inv}(H_R) = H_L$. 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, $e\mathcal{S} = \mathrm{Orb}(G_e, H)$. □

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

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

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

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 $\mathsf{Cay}(H,\mathcal{S})$ and $\mathsf{Cay}(K,\mathcal{T})$ are isomorphic (as schemes);
- algebraically isomorphic if the schemes $\mathsf{Cay}(H,\mathcal{S})$ and $\mathsf{Cay}(K,\mathcal{T})$ are algebraically isomorphic.

In what follows we abbreviate

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

Isomorphisms between S-rings

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

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 $f : \mathsf{Cay}(H, S) \to \mathsf{Cay}(H, T)$ 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 ISO 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 $\mathsf{Cay}(H, S)$ and $\mathsf{Cay}(H, T)$ are isomorphic iff there exists $f \in P$ s.t. $\mathsf{Cay}(H, S)^f = \mathsf{Cay}(H, T)$.

Example

N	S-partition $\mathcal{S}$	$\lvert\mathsf{Alg}(\mathcal{S})\rvert$	$\mathrm{Iso}(\mathcal{S})/\mathrm{Aut}(\mathcal{S})$ 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 soving set for $\mathbb{Z}_n$ of at most n^3 permutations in time $n^{O(1)}$.

Lecture 6.

Cyclotomic S-rings

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 $(\mathbb{Q}H)^F$.

Special cases

- If $F = \mathsf{Inn}(H)$, then $(\mathbb{Q}H)^F = \mathbf{Z}(\mathbb{Q}H)$ and the basic sets are the conjugacy classes of H. Fusion S-rings of $\mathbf{Z}(\mathbb{Q}H)$ are in one-to-one correspondence with supercharacters.
- If R is a finite ring, $H = (R, +)$ and $K \leq R^\times$, then $\mathsf{Cyc}(K, H) := (\mathbb{Q}H)^K$ is called a cyclotomic S-ring; its basic sets are rK, $r \in R$.
- When $R = \mathbb{Z}_n$, then H is a cyclic group and K isomorphic to a subgroup of $\mathrm{Aut}(H)$; the S-ring $\mathsf{Cyc}(K, H)$ is called circulant.

Properties of $\mathcal{A}$-subsets

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

- $\mathcal{S}^\cup$ is closed with respect to boolean operations;
- $\{e\}, H \in \mathcal{S}^\cup$;
- $(\mathcal{S}^\cup)^{-1} = \mathcal{S}^\cup$;
- $\mathcal{S}^\cup$ is closed with respect to the group product;
- $\langle X\rangle \in \mathcal{S}^\cup$ for all $X \in \mathcal{S}^\cup$;
- if $X \in \mathcal{S}^\cup$, then $E = \mathsf{Cay}(H,X)$ is an equivalence relation if and only if $X \le H$.

Definition
A subgroup $F \le H$ is called an $\mathcal{A}$-group if $\underline{F} \in \mathcal{A}$; $\mathcal{A}$ is called primitive if $\{e\}, H$ are the only $\mathcal{A}$-subgroups.

Schurian S-rings

Theorem (Schur, 1933)
Let H be a group and $H_R \le G \le \mathrm{Sym}(H)$. Then $\mathrm{Orb}(G_e, H)$ is an S-partition.

Proof.

- Set $\mathcal{X} := \mathrm{Inv}(G)$.
- Since $H_R \le G$, we have $\mathcal{X} \sqsubseteq \mathrm{Inv}(H_R) = H_L$.
- Thus $\mathcal{X} = (H,\mathcal{R})$ is a Cayley scheme over H,
- and $e\mathcal{R} = \{eS :\ S \in \mathcal{R}\}$ is a Schur partition of H.
- Since $\mathcal{X}$ is schurian, $e\mathcal{R} = \mathrm{Orb}(G_e, H)$.

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

Isomorphisms between S-rings: definitions
Let $\mathcal{S} \vdash H$ and $\mathcal{T} \vdash K$ be S-partitions of groups H and K.

Definition
The S-rings $\mathcal{A} := \langle\underline{\mathcal{S}}\rangle$ and $\mathcal{B} := \langle\underline{\mathcal{T}}\rangle$ are called

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

In what follows we abbreviate

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

Isomorphisms between S-rings: characterization

Proposition
Let $\mathcal{A} := \langle\underline{\mathcal{S}}\rangle$ and $\mathcal{B} := \langle\underline{\mathcal{T}}\rangle$ be S-rings. Then

- $\mathcal{A} \cong_{alg} \mathcal{B}$ if and only if there exists a bijection $f : \mathcal{S} \to \mathcal{T}$ such that $c^R_{PQ} = c^{R^f}_{P^f Q^f}$ for all $P, Q, R \in \mathcal{S}$.
- $\mathcal{A} \cong_{com} \mathcal{B}$ if and only if there exists a bijection $f : H \to K$ such that $(e_H)^f = e_K$, $f|_{\mathcal{S}}$ is an algebraic isomorphism from $\mathcal{A}$ onto $\mathcal{B}$ and $(hS)^f = h^f S^f$ for all $h \in H$ and $S \in \mathcal{S}$.

Remark:

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

Klin-Pöschel approach

A "solution" to the ISO 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 $\mathcal{A}_j$ such that $f^* = \phi$ (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 is a solving set for the Cayley graphs over H: two Cayley graphs $\mathsf{Cay}(H, S)$ and $\mathsf{Cay}(H, T)$ are isomorphic if and only if there exists $f \in P$ such that $\mathsf{Cay}(H, S)^f = \mathsf{Cay}(H, T)$.

Example

N	S-partition $\mathcal{S}$	$\lvert\mathsf{Alg}(\mathcal{S})\rvert$	$\mathrm{Iso}(\mathcal{S})/\mathrm{Aut}(\mathcal{S})$ 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 (Muzychuk, 1994)

Two S-rings over cyclic groups are algebraically isomorphic if and only if they coincide.

This gives 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 $\mathrm{Iso}(\mathcal{A}_i)/\mathrm{Aut}(\mathcal{A}_i)$;
- now the union of T_i's produces a solving set for $\mathbb{Z}_n$.

Theorem (Muzychuk, 2004)

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

B-groups

Definition (Wielandt, 1964)

A finite group H is called a B-group if every primitive permutation group G satisfying $H_R \leq G \leq \mathrm{Sym}(H)$ is 2-transitive.

Theorem

A group H is a B-group if and only if every primitive Schurian S-ring over H has rank 2.

To prove this theorem, it suffices to verify the following statement.

Proposition

Let $H_R \leq G \leq \mathrm{Sym}(H)$, $\mathcal{A} := \langle \underline{\mathrm{Orb}(G_e, H)} \rangle$ the corresponding S-ring and $B \subseteq H$ with $e \in B$. Then B is a block of G if and only if B is an $\mathcal{A}$-group.

Proof of the theorem on B-groups

Proof.

- Assume first that B is a block of G.
- Then B is a block of H_R.
- So for any $h \in H$: $Bh = B$ or $Bh \cap B = \emptyset$.
- It follows that B is a coset.
- Since $e \in B$, this implies that $B \leq H$.
- Besides, since B is a block, $B^{G_e} = B$.
- Thus B is a union of G_e-orbits, and hence is an $\mathcal{A}$-group.
- Conversely, let now B be an $\mathcal{A}$-group.
- Then $\mathsf{Cay}(H, B)$ is a G-invariant equivalence relation.
- Therefore the classes of $\mathsf{Cay}(H, B)$ are blocks of G,
- and B is a block of G.

Exercise:
prove that a simple group of order > 2 is not a B-group.

Strong B-groups

Definition
A finite group H is strong B-group if the trivial S-ring is the only primitive S-ring over H.

Known strong B-groups:

- a cyclic group of composite order (Schur, 1933);
- an abelian group with a cyclic Sylow subgroup (Wielandt, 1935);
- an abelian group with a Sylow p-subgroup of type (p^a, p^b), $a < b$ (Bercov, 1962);
- a dihedral group (Wielandt, 1949).

Exercise:
prove that any group of order 6 or 8 is a strong B-group.

Lecture 7.

$\mathcal{A}$-groups

Let $\mathcal{A} \leq \mathbb{Q}H$ be an S-ring over H and $\mathcal{S}$ the corresponding S-partition of H.

Proposition
Given $\mathcal{A}$-groups A and B, $A \cap B$ and $\langle A, B\rangle$ are $\mathcal{A}$-groups.

Proposition.
Given $S \in \mathcal{S}^{\cup}$, the groups $\langle S\rangle$ and

$$\begin{array}{rcl} \mathsf{Rad}_\ell(S) & := & \{h \in H \mid hS = S\}, \\ \mathsf{Rad}_r(S) & := & \{h \in H \mid Sh = S\}, \\ \mathsf{Rad}(S) & := & \mathsf{Rad}_\ell(S) \cap \mathsf{Rad}_r(S) \end{array}$$

$\mathcal{A}$-groups.

Indeed, $h \in \mathsf{Rad}_\ell(S)$ if and only if $Sh = S$ if and only if h appears $|S|$ times in the product $\underline{S} \cdot \underline{S}^{(-1)}$. Thus $\underline{\mathsf{Rad}_\ell(S)} = \delta_{|S|}[\underline{S} \cdot \underline{S}^{(-1)}]$ and by Schur-Wielandt principle $\underline{\mathsf{Rad}_\ell(S)} \in \mathcal{A}$.

Subring of an S-ring

In what follows $K \leq H$ is an $\mathcal{A}$-group.

Proposition
The vector space $\mathcal{A}_K := \mathcal{A} \cap \mathbb{Q}K$ is an S-ring over K the basic sets of which are $\mathcal{S}_K := \{S \in \mathcal{S} : \ S \subseteq K\}$.

The quotient S-ring: auxiliary lemma

Proposition
For basic sets $S, T \in \mathcal{S}$ the following conditions hold:

(a) $SK \neq TK \implies SK \cap TK = \emptyset$;

(b) $KSK \neq KTK \implies KSK \cap KTK = \emptyset$;

(c) $\underline{K} \cdot \underline{S} = c\underline{KS}$ where $c = |Ks \cap S|, s \in S$

(d) $\underline{K} \cdot \underline{S} \cdot \underline{K} = c\underline{KSK}$ where $c = |KS \cap sK|, s \in S$.

Proof: (a) if $SK \cap TK \neq \emptyset$, then $sk_1 = tk_2$ for some $s \in S, t \in T$ and $k_1, k_2 \in K$. Then $S \cap TK \neq \emptyset$, and $S \subseteq TK \implies SK \subseteq TK$. By symmetry $TK \subseteq SK$.

(c) The coefficient of h in the product $\underline{K} \cdot \underline{S}$ is equal to the intersection number $|K^{(-1)}h \cap S| = |Kh \cap S|$. Since S is a basic set, the number $c := |K^{(-1)}s \cap S|$ doesn't depend on a choice $s \in S$. Thus if $h \in KS$, then $h = ks$ for some $k \in K$ and $s \in S$, and $|Kh \cap S| = |Ks \cap S| = c$.

The quotient S-ring: definition

Denote by $K\backslash\mathcal{S}/K$ the partition of H into classes KSK, $S \in \mathcal{S}$.

Proposition
The linear span $\langle \underline{X} : \ X \in K\backslash\mathcal{S}/K \rangle$ is closed under $\circ$, $\cdot$ and $^{(-1)}$ and contains $\underline{H}$. It coincides with $e_K\mathcal{A}e_K$ where $e_K = \frac{1}{|K|}\underline{K}$.

If K is normal in H then the algebra $e_K\mathcal{A}e_K$ may be identified with an S-ring over H/K. The mapping $\pi : x \mapsto e_K x, x \in \mathbb{Q}H$ is an epimorphism from $\mathbb{Q}H$ onto $e_K\mathbb{Q}H$. Identifying the elements he_K with the cosets hK we obtain the following statement.

Proposition
The image $\pi(\mathcal{A})$ is an S-ring over H/K the basic sets of which are $\pi(T), T \in \mathcal{S}$. This S-ring is called a quotient of $\mathcal{A}$ and is denoted as $\mathcal{A}/K$ or $\mathcal{A}_{H/K}$.

Exercises

Exercise 1:
let $C = \langle c \rangle$ be a cyclic group of order 8. Then the subspace $\mathcal{A} = \langle c^0, c^2, c^4, c^6, c + c^5, c^3 + c^7 \rangle$ is an S-ring over C. Check that

- every subgroup of C is an $\mathcal{A}$-group;
- $\mathcal{A}_{\langle c^2 \rangle} = \mathbb{Q}[c^2]$;
- $\mathcal{A}/\langle c^4 \rangle = \mathbb{Q}[C/\langle c^4 \rangle]$;
- find $\mathrm{Aut}(\mathcal{A}), \mathrm{Iso}(\mathcal{A})$ and $\mathsf{Alg}(\mathcal{A})$.

Exercise 2:
let $\mathcal{A} \leq \mathbb{Q}H$ be an S-ring and $K \trianglelefteq H$ an $\mathcal{A}$-subgroup. Then $\mathcal{A}_K$ and $\mathcal{A}_{H/K}$ are schurian, whenever so is $\mathcal{A}$.

Wreath product of S-rings

Proposition

$$\dim(\mathcal{A}) \geq \dim(\mathcal{A}_K) + \dim(\mathcal{A}_{H/K}) - 1.$$

Proof. $\mathcal{A}_K$ and $e_K\mathcal{A}$ are subspaces of $\mathcal{A}$. Since $\dim(\mathcal{A}_{H/K}) = \dim(e_K\mathcal{A})$ and $\mathcal{A}_K \cap e_K\mathcal{A} = \langle \underline{K} \rangle$, we are done.

Proposition
The following conditions are equivalent:

(a) $\dim(\mathcal{A}) = \dim(\mathcal{A}_K) + \dim(\mathcal{A}_{H/K}) - 1$;

(b) $\mathcal{A} = \mathcal{A}_K + e_K\mathcal{A}$;

(c) $K \leq \mathsf{Rad}(T)$ for each basic set of $\mathcal{A}$ with $T \cap K = \emptyset$.

If any of the above conditions hold, the S-ring $\mathcal{A}$ is called the wreath product of $\mathcal{A}_K$ by $\mathcal{A}_{H/K}$, notation $\mathcal{A}_K \wr \mathcal{A}_{H/K}$.

Generalized wreath product

Definition
Let $1 \le L \le U \le H$ and $L \trianglelefteq H$ be $\mathcal{A}$-groups. The S-ring $\mathcal{A}$ is called a generalized wreath product or U/L-wreath product of $\mathcal{A}_U$ and $\mathcal{A}_{U/L}$ if every basic set $S \in \mathcal{S}$ outside of U is a union of L-cosets. The product is called nontrivial or proper if $L \neq 1, U \neq H$.

Remark: under above conditions $(\mathcal{A}_U)_{U/L} = \mathcal{A}_{U/L} = (\mathcal{A}/L)_{U/L}$.

Theorem
Let $S = U/L$ be a section of a group H, and let $\mathcal{A}_1$ and $\mathcal{A}_2$ be S-rings over the groups U and H/L respectively such that S is both an $\mathcal{A}_1$- and an $\mathcal{A}_2$-section with

$$(\mathcal{A}_1)_S = (\mathcal{A}_2)_S.$$

Then the set of all $\mathcal{A}$ such that $\mathcal{A}_U = \mathcal{A}_1$ and $\mathcal{A}_{H/L} = \mathcal{A}_2$ has the smallest element, and it is a unique S-wreath product in this set.

Tensor (direct) product of S-rings

Let $\mathcal{S}$ and $\mathcal{T}$ be partitions of the groups H and K, and $\mathcal{S} \times \mathcal{T}$ the partition of $H \times K$ the classes of which are $S \times T$ where $S \in \mathcal{S}$, $T \in \mathcal{T}$.

Proposition
Let $\mathcal{A} = \langle \underline{\mathcal{S}} \rangle$ and $\mathcal{B} = \langle \underline{\mathcal{T}} \rangle$ be S-rings over H and K. Then $\mathcal{S} \times \mathcal{T}$ is an S-partition of $H \times K$; the S-ring of it is $\mathcal{A} \otimes \mathcal{B}$.

Exercise:
prove that $(\mathcal{A} \otimes \mathcal{B})_{(1,K)} \cong_{Cay} \mathcal{B}$ and $(\mathcal{A} \otimes \mathcal{B})/(1, K) \cong_{Cay} \mathcal{A}$.

Leung-Man and Schur-Wielandt theorem

Theorem (Leung-Man, 1994)
Let $\mathcal{A}$ be a circulant S-ring. Suppose that $\mathcal{A}$ is not a generalized wreath product. Then

$$\mathcal{A} = \mathcal{A}_0 \otimes \mathcal{A}_1 \otimes \cdots \otimes \mathcal{A}_k,$$

where $\mathcal{A}_0$ is cyclotomic and $\mathrm{rk}(\mathcal{A}_i) = 2$ for all $i = 1, \ldots, k$.

Remark: the factors $\mathcal{A}_i$ are circulant S-rings of pairwise coprime degrees.

Theorem (Schur-Wielandt, 1964)
Let H be an abelian group of composite order with cyclic Sylow p-subgroup for some prime divisor p of $|H|$.Then any S-ring over H is imprimitive.

Schur theorem

Theorem
Let $\mathcal{A}$ be an arbitrary S-ring over an abelian group H. Then $x^{(m)} \in \mathcal{A}$ for each $m \in \mathbb{Z}$ coprime to $|H|$ and all $x \in \mathcal{A}$.

Proof

- We may assume that $x = \underline{S}$ where $S \in \mathcal{S}$, and m is a prime;
- then $\underline{S}^m \equiv \underline{S^{(m)}} (\mathrm{mod}\, m)$;
- since $\gcd(m, |H|) = 1$, this implies that $|S^{(m)}| = |S|$.
- Thus $S^{(m)} \in \mathcal{S}$.

Consequences of Schur's Theorem

Corollary 1
X is a basic set of $\mathcal{A}$ if and only if $X^{(m)}$ is a basic set of $\mathcal{A}$.

Corollary 2
If $\mathcal{A}$ is circulant S-ring over a group H, then $\mathrm{Iso}_{cay}(\mathcal{A}) = \mathrm{Aut}(H)$.

In particular, if $\mathcal{A}$ is circulant, then the group $\mathsf{Rad}(\mathcal{A}) := \mathsf{Rad}(X)$ does not depend on $X \in \mathcal{S}$ containing a generator of H; it is called the radical of $\mathcal{A}$.

Corollary 3
Any S-ring $\mathcal{A}$ over a cyclic group C of prime order p is cyclotomic, that is $\mathcal{S} = \mathrm{Orb}(K, C)$ for some $K \le \mathrm{Aut}(C)$.