Separability of Schur rings and Cayley graph isomorphism problem

Grigory Ryabov

Novosibirsk State University

Symmetry vs Regularity,
Pilsen, July 1-7, 2018

S-rings

G is a finite group, e is the identity of G

A partition $\mathcal{S}$ of G is called a Schur partition if $\mathcal{S}$ satisfies the following properties:

- $\{e\} \in \mathcal{S}$,
- $X \in \mathcal{S} \;\Rightarrow\; X^{-1} \in \mathcal{S}$,
- for every $X, Y, Z \in \mathcal{S}$ the number $c_{X,Y}^{Z} = |Y \cap X^{-1}z|$ does not depend on $z \in Z$.

A subring $\mathcal{A} \subseteq \mathbb{Z}G$ is called an S-ring (Schur ring) over G if there exists a Schur partition $\mathcal{S} = \mathcal{S}(\mathcal{A})$ such that $\mathcal{A} = Span_{\mathbb{Z}}\{\underline{X} : \; X \in \mathcal{S}\}$, where $\underline{X} = \sum_{x \in X} x$.

S-rings

G is a finite group, e is the identity of G

A partition $\mathcal{S}$ of G is called a Schur partition if $\mathcal{S}$ satisfies the following properties:

- $\{e\} \in \mathcal{S}$,
- $X \in \mathcal{S} \Rightarrow X^{-1} \in \mathcal{S}$,
- for every $X, Y, Z \in \mathcal{S}$ the number $c_{X,Y}^{Z} = |Y \cap X^{-1}z|$ does not depend on $z \in Z$.

A subring $\mathcal{A} \subseteq \mathbb{Z}G$ is called an S-ring (Schur ring) over G if there exists a Schur partition $\mathcal{S} = \mathcal{S}(\mathcal{A})$ such that $\mathcal{A} = Span_{\mathbb{Z}}\{\underline{X} : X \in \mathcal{S}\}$, where $\underline{X} = \sum_{x \in X} x$.

- $\underline{X}\ \underline{Y} = \sum_{Z \in \mathcal{S}(\mathcal{A})} c_{X,Y}^{Z} \underline{Z}$
- The numbers $c_{X,Y}^{Z}$ are the structure constants of $\mathcal{A}$
- The elements of $\mathcal{S}$ are called the basic sets of $\mathcal{A}$
- $\mathrm{rk}(\mathcal{A}) = |\mathcal{S}|$ is called the rank of $\mathcal{A}$

Isomorphisms of S-rings

$\mathcal{A}$ and $\mathcal{A}^{'}$ are S-rings over groups G and $G^{'}$ respectively.

- An algebraic isomorphism from $\mathcal{A}$ to $\mathcal{A}^{'}$ is defined to be a bijection $\varphi : \mathcal{S}(\mathcal{A}) \to \mathcal{S}(\mathcal{A}^{'})$ such that $c_{X,Y}^{Z} = c_{X^{\varphi},Y^{\varphi}}^{Z^{\varphi}}$ for every $X, Y, Z \in \mathcal{S}(\mathcal{A})$.

- The mapping $\underline{X} \to \underline{X}^{\varphi}$ is extended by linearity to the ring isomorphism of $\mathcal{A}$ and $\mathcal{A}^{'}$.

Isomorphisms of S-rings

$\mathcal{A}$ and $\mathcal{A}'$ are S-rings over groups G and G' respectively.

- An algebraic isomorphism from $\mathcal{A}$ to $\mathcal{A}'$ is defined to be a bijection $\varphi : \mathcal{S}(\mathcal{A}) \to \mathcal{S}(\mathcal{A}')$ such that $c_{X,Y}^{Z} = c_{X^{\varphi},Y^{\varphi}}^{Z^{\varphi}}$ for every $X, Y, Z \in \mathcal{S}(\mathcal{A})$.

- The mapping $\underline{X} \to \underline{X}^{\varphi}$ is extended by linearity to the ring isomorphism of $\mathcal{A}$ and $\mathcal{A}'$.

- A (combinatorial) isomorphism from $\mathcal{A}$ to $\mathcal{A}'$ is defined to be a bijection $f : G \to G'$ such that for every basic set X of $\mathcal{A}$ the set $X' = X^f$ is a basic set of $\mathcal{A}'$ and f is an isomorphism of the Cayley graphs $\mathrm{Cay}(G, X)$ and $\mathrm{Cay}(G', X')$.

- Every combinatorial isomorphism of S-rings induces the algebraic one, however the converse statement is not true.

Separability

$\mathcal{K}$ is a class of groups

An S-ring is said to be separable with respect to $\mathcal{K}$ if every algebraic isomorphism from it to an S-ring over a group from $\mathcal{K}$ is induced by a combinatorial isomorphism (Evdokimov-Ponomarenko, 2009).

- A separable S-ring is determined up to isomorphism only by the tensor of its structure constants.
- For every group G the S-ring of rank 2 over G and $\mathbb{Z}G$ are separable with respect to the class of all groups.

Separability

$\mathcal{K}$ is a class of groups

An S-ring is said to be separable with respect to $\mathcal{K}$ if every algebraic isomorphism from it to an S-ring over a group from $\mathcal{K}$ is induced by a combinatorial isomorphism (Evdokimov-Ponomarenko, 2009).

- A separable S-ring is determined up to isomorphism only by the tensor of its structure constants.
- For every group G the S-ring of rank 2 over G and $\mathbb{Z}G$ are separable with respect to the class of all groups.

A finite group is said to be separable with respect to $\mathcal{K}$ if every S-ring over this group is separable with respect to $\mathcal{K}$.

Problem

Determine all (abelian) separable groups.

Separable groups

- C_n is the cyclic group of order n
- $\mathcal{K}_C$ is the class of cyclic groups
- $\mathcal{K}_A$ is the class of abelian groups
- $\mathcal{K}_G$ is the class of groups isomorphic to a group G

- Groups of order ≤ 15 are separable with respect to the class of all groups (follows from the computer calculations made by Hanaki and Miyamoto).
- For every group H with $|H| \geq 4$ the group $H \times H$ is not separable with respect to $\mathcal{K}_{H\times H}$ (follows from Golfand-Klin's result, 1985).
- Cyclic p-groups are separable with respect to $\mathcal{K}_C$ (Evdokimov-Ponomarenko, 2015).
- There exists n such that C_n is not separable with respect to $\mathcal{K}_{C_n}$ (Evdokimov-Ponomarenko, 2002).

Main results

Theorem 1

The group $C_p \times C_{p^k}$, where $p \in \{2, 3\}$ and $k \geq 0$, is separable with respect to $\mathcal{K}_A$.

Theorem 2

An abelian group of order $4p$ is separable with respect to $\mathcal{K}_A$ for every prime p.

Separability of p-S-rings

- p is a prime

An S-ring $\mathcal{A}$ is called a p-S-ring if for every $X \in \mathcal{S}(\mathcal{A})$ there exists $k \geq 0$ such that $|X| = p^k$.

Separability of p-S-rings

- p is a prime

An S-ring $\mathcal{A}$ is called a p-S-ring if for every $X \in \mathcal{S}(\mathcal{A})$ there exists $k \geq 0$ such that $|X| = p^k$.

Theorem 3

- If $n \leq 3$ then every p-S-ring over an abelian group of order p^n is separable with respect to $\mathcal{K}_A$.
- If $n \geq 4$ then there exists a p-S-ring over C_p^n which is not separable with respect to $\mathcal{K}_{C_p^n}$.

Separability and Cayley graph isomorphism problem

Proposition

Let $\mathcal{K}$ be a class of groups and G a group separable with respect to $\mathcal{K}$. Suppose that G is given explicitly and $|G| = n$. Then for every Cayley graph Γ over G and every Cayley graph $\Gamma^{'}$ over an arbitrary explicitly given group from $\mathcal{K}$ one can check in time poly(n) whether Γ and $\Gamma^{'}$ are isomorphic.

Separability and Cayley graph isomorphism problem

Proposition

Let $\mathcal{K}$ be a class of groups and G a group separable with respect to $\mathcal{K}$. Suppose that G is given explicitly and $|G| = n$. Then for every Cayley graph Γ over G and every Cayley graph $\Gamma^{'}$ over an arbitrary explicitly given group from $\mathcal{K}$ one can check in time poly(n) whether Γ and $\Gamma^{'}$ are isomorphic.

Corollary

Let $G \in \{C_2 \times C_{2^k}, C_3 \times C_{3^k}, C_{4p}, C_2 \times C_2 \times C_p\}$, where p is a prime and $k \geq 0$. Suppose that G is given explicitly and $|G| = n$. Then for every Cayley graph Γ over G and every Cayley graph $\Gamma^{'}$ over an arbitrary explicitly given abelian group one can check in time poly(n) whether Γ and $\Gamma^{'}$ are isomorphic.

Remark

It should be mentioned that the isomorphism problem for Cayley graphs over a group G was solved in the following cases:

- G is cyclic (Evdokimov-Ponomarenko, 2003; Muzychuk, 2004);
- $G = C_2 \times C_2 \times C_p$, where p is a prime (Nedela-Ponomarenko, 2017).

Proof of Proposition

- By using the Weisfeiler-Leman algorithm one can construct in time poly(n) the S-rings $\mathcal{A}$ and $\mathcal{A}^{'}$ corresponding to Γ and $\Gamma^{'}$ respectively and the bijection $\varphi : \mathcal{S}(\mathcal{A}) \to \mathcal{S}(\mathcal{A}^{'})$ such that:
    - if $\Gamma \cong \Gamma^{'}$ then φ is an algebraic isomorphism;
    - if φ is an algebraic isomorphism then the set $\mathrm{Iso}(\mathcal{A}, \mathcal{A}^{'}, \varphi)$ of all isomorphisms from $\mathcal{A}$ to $\mathcal{A}^{'}$ inducing φ coincides with the set $\mathrm{Iso}(\Gamma, \Gamma^{'})$ of all isomorphisms from Γ to $\Gamma^{'}$.
- One can test whether φ is an algebraic isomorphism in time poly(n) because $\mathcal{A}$ has at most n^3 structure constants.
- If φ is not an algebraic isomorphism then $\Gamma \ncong \Gamma^{'}$.
- If φ is an algebraic isomorphism then in view of separability of G with respect to $\mathcal{K}$, the set $\mathrm{Iso}(\mathcal{A}, \mathcal{A}^{'}, \varphi) = \mathrm{Iso}(\Gamma, \Gamma^{'})$ is not empty and hence $\Gamma \cong \Gamma^{'}$.

Schurity

- G is a finite group, e is the identity of G
- $G_{right} = \{x \mapsto xg,\, x \in G : \ g \in G\} \leq \mathrm{Sym}(G)$
- $\mathrm{Orb}(K, G)$ is the set of all orbits of $K \leq \mathrm{Sym}(G)$ on G

Proposition (Schur, 1933)

Let $K \leq \mathrm{Sym}(G)$ and $K \geq G_{right}$. Then $\mathrm{Orb}(K_e, G)$ is a Schur partition.

- An S-ring $\mathcal{A}$ over G is called schurian if $\mathcal{S}(\mathcal{A}) = \mathrm{Orb}(K_e, G)$ for some $K \leq \mathrm{Sym}(G)$ such that $K \geq G_{right}$.
- A finite group G is called a Schur group if every S-ring over G is schurian (Pöschel, 1974).

Separability and schurity

The following groups are Schur:

- groups of order ≤ 15 (follows from the computer calculations made by Fiedler, 1998);
- cyclic p-groups (Pöschel, 1974);
- $C_2 \times C_{2^k}$ (Muzychuk-Ponomarenko, 2015);
- $C_3 \times C_{3^k}$ (Ryabov, 2015);
- $C_2 \times C_2 \times C_p$, where p is a prime (Evdokimov-Kovács-Ponomarenko, 2013).

So all known separable groups are Schur.

Separability and schurity

The group $H \times H$ is non-Schur and non-separable whenever H is abelian, $|H| \geq 4$, and $H \neq C_2 \times C_2$.

- Non-schurity follows from the necessary conditions of schurity for abelian groups (Evdokimov-Kovács-Ponomarenko, 2013).
- Non-separability follows from Golfand-Klin's result (1985).

Separability and schurity

The group $H \times H$ is non-Schur and non-separable whenever H is abelian, $|H| \geq 4$, and $H \neq C_2 \times C_2$.

- Non-schurity follows from the necessary conditions of schurity for abelian groups (Evdokimov-Kovács-Ponomarenko, 2013).
- Non-separability follows from Golfand-Klin's result (1985).

The groups C_2^4, C_2^5 are Schur and non-separable.

- Schurity follows from the computer calculations made by Fiedler (1998) for C_2^4 and by Pech and Reichard (2009) for C_2^5.
- Non-separability follows from Golfand-Klin's result (1985).

Separability and schurity

The group $H \times H$ is non-Schur and non-separable whenever H is abelian, $|H| \geq 4$, and $H \neq C_2 \times C_2$.

- Non-schurity follows from the necessary conditions of schurity for abelian groups (Evdokimov-Kovács-Ponomarenko, 2013).
- Non-separability follows from Golfand-Klin's result (1985).

The groups C_2^4, C_2^5 are Schur and non-separable.

- Schurity follows from the computer calculations made by Fiedler (1998) for C_2^4 and by Pech and Reichard (2009) for C_2^5.
- Non-separability follows from Golfand-Klin's result (1985).

Question

Does a non-Schur separable group exist?

Separability and schurity

Let p be a prime.

- If $n \leq 3$ then every p-S-ring over an abelian group of order p^n is schurian (Kim, 2014).
- If p is odd and $n \geq 4$ then there exists a non-schurian p-S-ring over C_p^n.
- If $n \geq 6$ then there exists a non-schurian 2-S-ring over C_2^n (Evdokimov-Kovács-Ponomarenko, 2013).