On the isomorphism problem for Cayley graphs over abelian p-groups via S-rings

Grigory Ryabov

Novosibirsk State University

G2S2-2016

Part I: S-rings

S-rings

- G is a finite group with the identity element e, $X \subseteq G$
- $\mathbb{Z}G = \{\sum_{g \in G} a_g g : g \in G\}$ is the group ring
- $\underline{X} = \sum_{x \in X} x$ (an element of the group ring $\mathbb{Z}G$)

Definition

A ring $\mathcal{A} \subseteq \mathbb{Z}G$ is called an S-ring over G, if there exists a partition $\mathcal{S} = \mathcal{S}(\mathcal{A})$ of G such that:

- $\{e\} \in \mathcal{S}$,
- $X \in \mathcal{S} \;\Rightarrow\; X^{-1} \in \mathcal{S}$,
- $\mathcal{A} = \mathrm{Span}_{\mathbb{Z}}\{\underline{X} : \; X \in \mathcal{S}\}$.

The elements of $\mathcal{S}$ are the basic sets of $\mathcal{A}$.

Isomorphisms

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

Definitions

- A ring isomorphism $\varphi : \mathcal{A} \to \mathcal{A}'$ is called an algebraic isomorphism from $\mathcal{A}$ to $\mathcal{A}'$ if for every $X \in \mathcal{S}(\mathcal{A})$ there exists $X' \in \mathcal{S}(\mathcal{A}')$ such that $\varphi(\underline{X}) = \underline{X'}$. The mapping $X \to X' = X^{\varphi}$ is a bijection from $\mathcal{S}(\mathcal{A})$ to $\mathcal{S}(\mathcal{A}')$.
- A bijection $f : G \to G'$ is called a (combinatorial) isomorphism from $\mathcal{A}$ to $\mathcal{A}'$ if $\underline{X} \mapsto \underline{f(X)}$ induces an algebraic isomorphism.
- A group isomorphism $f : G \to G'$ is called a Cayley isomorphism from $\mathcal{A}$ to $\mathcal{A}'$ if for every $X \in \mathcal{S}(\mathcal{A})$ there exists $X' \in \mathcal{S}(\mathcal{A}')$ such that $f(X) = X'$.

Isomorphisms

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

Definitions

- A ring isomorphism $\varphi : \mathcal{A} \to \mathcal{A}^{'}$ is called an algebraic isomorphism from $\mathcal{A}$ to $\mathcal{A}^{'}$ if for every $X \in \mathcal{S}(\mathcal{A})$ there exists $X^{'} \in \mathcal{S}(\mathcal{A}^{'})$ such that $\varphi(\underline{X}) = \underline{X}^{'}$. The mapping $X \to X^{'} = X^{\varphi}$ is a bijection from $\mathcal{S}(\mathcal{A})$ to $\mathcal{S}(\mathcal{A}^{'})$.
- A bijection $f : G \to G^{'}$ is called a (combinatorial) isomorphism from $\mathcal{A}$ to $\mathcal{A}^{'}$ if $\underline{X} \mapsto \underline{f(X)}$ induces an algebraic isomorphism.
- A group isomorphism $f : G \to G^{'}$ is called a Cayley isomorphism from $\mathcal{A}$ to $\mathcal{A}^{'}$ if for every $X \in \mathcal{S}(\mathcal{A})$ there exists $X^{'} \in \mathcal{S}(\mathcal{A}^{'})$ such that $f(X) = X^{'}$.

Cayley isomorphism $\Rightarrow$ isomorphism $\Rightarrow$ algebraic isomorphism
Algebraic isomorphism $\not\Rightarrow$ isomorphism $\not\Rightarrow$ Cayley isomorphism

Schurity

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

Theorem (Schur, 1933)

$\mathbb{Z}$-module $\mathcal{A} = \mathcal{A}(K, G) = \mathrm{Span}_{\mathbb{Z}} \{\underline{X} : \; X \in \mathrm{Orb}\,(K_e, G)\}$ is an S-ring over G.

Schurity

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

Theorem (Schur, 1933)

$\mathbb{Z}$-module $\mathcal{A} = \mathcal{A}(K, G) = \mathrm{Span}_{\mathbb{Z}}\{\underline{X} :\ X \in \mathrm{Orb}(K_e, G)\}$ is an S-ring over G.

Definition (Pöschel, 1974)

An S-ring $\mathcal{A}$ over G is called schurian, if $\mathcal{A} = \mathcal{A}(K, G)$ for some permutation group K.

Schurity

Definition (Pöschel, 1974)

A finite group G is called a Schur group, if every S-ring over G is schurian.

Schurity

Definition (Pöschel, 1974)

A finite group G is called a Schur group, if every S-ring over G is schurian.

Problem

Determine all Schur groups.

Every S-ring over a Schur group is determined by a suitable permutation group.

Separability

$\mathrm{Iso}(\mathcal{A}, \mathcal{A}^{'}, \varphi)$ is the set of isomorphisms from $\mathcal{A}$ to $\mathcal{A}^{'}$ that induce given algebraic isomorphism φ.

Definition

Let $\mathcal{K}$ be a class of S-rings closed under Cayley isomorphisms. $\mathcal{A}$ is called separable with respect to $\mathcal{K}$ if $\mathrm{Iso}(\mathcal{A}, \mathcal{A}^{'}, \varphi) \neq \varnothing$ for all algebraic isomorphisms $\varphi : \mathcal{A} \to \mathcal{A}^{'}$, where $\mathcal{A}^{'} \in \mathcal{K}$.

Every separable S-ring is determined up to isomorphism only by its combinatorial parameters (so-called structure constants).

Separability

$\mathrm{Iso}(\mathcal{A}, \mathcal{A}^{'}, \varphi)$ is the set of isomorphisms from $\mathcal{A}$ to $\mathcal{A}^{'}$ that induce given algebraic isomorphism φ.

Definition

Let $\mathcal{K}$ be a class of S-rings closed under Cayley isomorphisms. $\mathcal{A}$ is called separable with respect to $\mathcal{K}$ if $\mathrm{Iso}(\mathcal{A}, \mathcal{A}^{'}, \varphi) \neq \varnothing$ for all algebraic isomorphisms $\varphi : \mathcal{A} \to \mathcal{A}^{'}$, where $\mathcal{A}^{'} \in \mathcal{K}$.

Every separable S-ring is determined up to isomorphism only by its combinatorial parameters (so-called structure constants).

Problem

Determine all groups G such that every S-ring over G is separable with respect to $\mathcal{K}$.

Cyclic p-groups

Theorem (Pöschel, 1974)

Cyclic p-groups are Schur. Moreover, if $p > 3$, then p-group G is Schur if and only if it is cyclic.

Theorem (Evdokimov-Ponomarenko, 2015)

Every S-ring over a cyclic p-group is separable with respect to the class of circulant S-rings.

Cyclic p-groups

Theorem (Pöschel, 1974)

Cyclic p-groups are Schur. Moreover, if $p > 3$, then p-group G is Schur if and only if it is cyclic.

Theorem (Evdokimov-Ponomarenko, 2015)

Every S-ring over a cyclic p-group is separable with respect to the class of circulant S-rings.

Theorem (Evdokimov-Ponomarenko, 2002)

There exists a cyclic group G and an S-ring $\mathcal{A}$ over G such that:

- G is not Schur;
- $\mathcal{A}$ is not separable with respect to the class of circulant S-rings.

Noncyclic p-groups

C_n is the cyclic group of order n.

Evdokimov, Kovács, Muzychuk, Pech, Ponomarenko, Reichard, R., Vasil'ev, ...-2015:

Let G be a noncyclic Schur p-group. Then $p \in \{2, 3\}$ and G is isomorphic to one of the following groups:

1. $C_2 \times C_{2^k},\ C_3 \times C_{3^k},\ k \geq 1$;
2. elementary abelian groups of order $4, 8, 9, 16, 27, 32$;
3. quaternion group Q_8;
4. $G_{16} = \langle a, b, c | a^4 = b^2 = c^2 = [a, b] = [a, c] = 1, [b, c] = a^2 \rangle$;
5. dihedral groups $D_{2^k},\ k \geq 1$.

Moreover, groups $(1) - (4)$ are Schur. Groups (5) are Schur whenever $1 \leq k \leq 5$.

Main results I

$G = C_p \times C_{p^k}$, $p \in \{2, 3\}$, $k \geq 1$.
All S-rings over G were classified by Muzychuk and Ponomarenko for $p = 2$ and by Ryabov for $p = 3$. By using this classification we prove the following theorem.

Theorem 1

Every S-ring over G is separable with respect to the class of S-rings over abelian groups.

Part II: Isomorphism problem for Cayley graphs

Isomorphism problem

Isomorphism problem

Given Cayley graphs Γ and $\Gamma^{'}$ over G check whether $\Gamma \cong \Gamma^{'}$.

Isomorphism problem

Isomorphism problem

Given Cayley graphs Γ and $\Gamma^{'}$ over G check whether $\Gamma \cong \Gamma^{'}$.

Theorem (Evdokimov-Ponomarenko,2003, Muzychuk, 2004)

Let Γ and $\Gamma^{'}$ be n-vertex circulant graphs. Then it can be tested in time $n^{O(1)}$ whether $\Gamma \cong \Gamma^{'}$.

Connection with S-rings

1. Let $\Gamma = \mathrm{Cay}(G, X)$ and $\Gamma^{'} = \mathrm{Cay}(G^{'}, X^{'})$ be Cayley graphs over the groups of the same order.
2. By using the Weisfeiler-Leman algorithm we can in time $|G|^{O(1)}$
   - construct the S-rings $\mathcal{A} = \mathcal{A}(\Gamma)$ and $\mathcal{A}^{'} = \mathcal{A}^{'}(\Gamma^{'})$ over G and $G^{'}$ respectively;
   - find an algebraic isomorphism $\varphi : \mathcal{A} \to \mathcal{A}^{'}$ such that $X^{\varphi} = X^{'}$ or establish that there are no such algebraic isomorphisms.
3. Every isomorphism $f : \Gamma \to \Gamma^{'}$ induces φ such that $X^{\varphi} = X^{'}$.
   φ does not depend on the choice of f.
   If there are no such φ then $\Gamma \ncong \Gamma^{'}$
4. If such algebraic isomorphism φ exists and $\mathcal{A}$ is separable then $\mathrm{Iso}(\mathcal{A}, \mathcal{A}^{'}, \varphi) \neq \varnothing$ and hence $\mathrm{Iso}(\Gamma, \Gamma^{'}) \neq \varnothing$.

Main results II

$G = C_p \times C_{p^k},\ p \in \{2,3\},\ k \geq 1,\ |G| = n$.
G is given explicitly.
$\mathcal{P}_n$ is the class of all graphs on n vertices that isomorphic to Cayley graphs over G.

Theorem 2

Given graphs $\Gamma, \Gamma^{'} \in \mathcal{P}_n$ it can be tested in time $n^{O(1)}$ whether $\Gamma \cong \Gamma^{'}$.

Theorem 2 immediately follows from Theorem 1.

Main results II

$G = C_p \times C_{p^k},\ p \in \{2,3\},\ k \geq 1,\ |G| = n.$
G is given explicitly.
$\mathcal{P}_n$ is the class of all graphs on n vertices that isomorphic to Cayley graphs over G.

Theorem 2

Given graphs $\Gamma, \Gamma' \in \mathcal{P}_n$ it can be tested in time $n^{O(1)}$ whether $\Gamma \cong \Gamma'$.

Theorem 2 immediately follows from Theorem 1.
In fact, Theorem 1 implies the next statement.

Theorem 2$'$

Given Cayley graph Γ over G and given Cayley graph Γ' over an arbitrary abelian group G' it can be tested in time $n^{O(1)}$ whether $\Gamma \cong \Gamma'$.