Testing isomorphism of central Cayley graphs over an almost simple group in polynomial time

(based on the joint work with Ilia Ponomarenko)

Andrey Vasil'ev

Sobolev Institute of Mathematics, Novosibirsk, Russia

G2S2, Novosibirsk, August 15-28, 2016

Cayley Graph Isomorphism Problem

- G is a (finite) group, $X \subseteq G \Rightarrow \Gamma = \mathrm{Cay}(G, X)$:
  $V(\Gamma) = G$ and $E(\Gamma) = \{(g, xg) \mid g \in G, x \in X\}$

Cayley Graph Isomorphism Problem

- G is a (finite) group, $X \subseteq G \Rightarrow \Gamma = \mathrm{Cay}(G, X)$:
  $V(\Gamma) = G$ and $E(\Gamma) = \{(g, xg) \mid g \in G, x \in X\}$
- $\Gamma = \mathrm{Cay}(G, X)$ and $\Gamma' = \mathrm{Cay}(G, X')$
  $\mathrm{Iso}(\Gamma, \Gamma') = \{f \in \mathrm{Sym}(G) \mid s^f \in E(\Gamma') \text{ for } s \in E(\Gamma)\}$
  $\mathrm{Aut}(\Gamma) = \mathrm{Iso}(\Gamma, \Gamma)$ and $G_{right} \leq \mathrm{Aut}(\Gamma) \leq \mathrm{Sym}(G)$

Cayley Graph Isomorphism Problem

- G is a (finite) group, $X \subseteq G \Rightarrow \Gamma = \mathrm{Cay}(G, X)$:
  $V(\Gamma) = G$ and $E(\Gamma) = \{(g, xg) \mid g \in G, x \in X\}$
- $\Gamma = \mathrm{Cay}(G, X)$ and $\Gamma' = \mathrm{Cay}(G, X')$
  $\mathrm{Iso}(\Gamma, \Gamma') = \{f \in \mathrm{Sym}(G) \mid s^f \in E(\Gamma') \text{ for } s \in E(\Gamma)\}$
  $\mathrm{Aut}(\Gamma) = \mathrm{Iso}(\Gamma, \Gamma)$ and $G_{right} \leq \mathrm{Aut}(\Gamma) \leq \mathrm{Sym}(G)$

Cayley Graph Isomorphism Problem (CGIP)

For an explicitly given finite group G and $X, X' \subseteq G$, find the set $\mathrm{Iso}(\Gamma, \Gamma')$, where $\Gamma = \mathrm{Cay}(G, X)$ and $\Gamma' = \mathrm{Cay}(G, X')$

Cayley Graph Isomorphism Problem

- G is a (finite) group, $X \subseteq G \Rightarrow \Gamma = \mathrm{Cay}(G, X)$:
  $V(\Gamma) = G$ and $E(\Gamma) = \{(g, xg) \mid g \in G, x \in X\}$
- $\Gamma = \mathrm{Cay}(G, X)$ and $\Gamma' = \mathrm{Cay}(G, X')$
  $\mathrm{Iso}(\Gamma, \Gamma') = \{f \in \mathrm{Sym}(G) \mid s^f \in E(\Gamma') \text{ for } s \in E(\Gamma)\}$
  $\mathrm{Aut}(\Gamma) = \mathrm{Iso}(\Gamma, \Gamma)$ and $G_{right} \leq \mathrm{Aut}(\Gamma) \leq \mathrm{Sym}(G)$

Cayley Graph Isomorphism Problem (CGIP)

For an explicitly given finite group G and $X, X' \subseteq G$, find the set $\mathrm{Iso}(\Gamma, \Gamma')$, where $\Gamma = \mathrm{Cay}(G, X)$ and $\Gamma' = \mathrm{Cay}(G, X')$

Input consists of the multiplication table of G and the sets X, X'

Output $\mathrm{Iso}(\Gamma, \Gamma')$ is either empty or given by a permutation from $\mathrm{Iso}(\Gamma, \Gamma')$ and some generating set of $\mathrm{Aut}(\Gamma)$

Note that $\mathrm{Iso}(\Gamma, \Gamma')$ is $\mathrm{Aut}(\Gamma)$-coset in $\mathrm{Sym}(G)$.

- Babai's algorithm solves CGIP in quasipolynomial time
- CGIP $\Rightarrow$ Group Isomorphism Problem
- CGIP for the cyclic groups is solved in polynomial time (Evdokimov-Ponomarenko, 2003, and Muzychuk, 2004)
- CGIP for the CI-groups can be solved in time $\mathrm{poly}(|\operatorname{Aut}(G)|)$

- Babai's algorithm solves CGIP in quasipolynomial time
- CGIP $\Rightarrow$ Group Isomorphism Problem
- CGIP for the cyclic groups is solved in polynomial time (Evdokimov-Ponomarenko, 2003, and Muzychuk, 2004)
- CGIP for the CI-groups can be solved in time $\mathrm{poly}(|\operatorname{Aut}(G)|)$

- Recognition problem for Cayley graph: Whether a given graph is a Cayley graph over a given group?
- Sabidussi's criterion: For a group G, the graph Γ is a Cayley graph over $G \Leftrightarrow$ the automorphism group $\operatorname{Aut}(\Gamma)$ contains a regular subgroup isomorphic to G
- In general, the recognition problem for Cayley graphs is not easier than the problem of determining whether a graph admits a fixed-point-free automorphism, which is NP-complete (A. Lubiw, 1981)

Central Cayley Graphs

- G is a group, $X \subseteq G$, and $\Gamma = \mathrm{Cay}(G, X)$
- Γ is said to be central if X is a normal subset in G, i.e., $X^g = X$ for every $g \in G$.

Central Cayley Graphs

- G is a group, $X \subseteq G$, and $\Gamma = \mathrm{Cay}(G, X)$
- Γ is said to be central if X is a normal subset in G, i.e., $X^g = X$ for every $g \in G$.

Proposition

Any Cayley graph over an abelian group is central

Central Cayley Graphs

- G is a group, $X \subseteq G$, and $\Gamma = \mathrm{Cay}(G, X)$
- Γ is said to be central if X is a normal subset in G, i.e., $X^g = X$ for every $g \in G$.

Proposition

Any Cayley graph over an abelian group is central

- If Γ is a Cayley graph then $G_{right} \leq \mathrm{Aut}(\Gamma)$

Central Cayley Graphs

- G is a group, $X \subseteq G$, and $\Gamma = \mathrm{Cay}(G, X)$
- Γ is said to be central if X is a normal subset in G, i.e., $X^g = X$ for every $g \in G$.

Proposition

Any Cayley graph over an abelian group is central

- If Γ is a Cayley graph then $G_{right} \leq \mathrm{Aut}(\Gamma)$
- If Γ is a central Cayley graph then $G_{left} G_{right} \leq \mathrm{Aut}(\Gamma)$ because $h(g, xg) = (hg, x^{h^{-1}} hg) = (hg, x'(hg))$

Central Cayley Graphs

- G is a group, $X \subseteq G$, and $\Gamma = \mathrm{Cay}(G, X)$
- Γ is said to be central if X is a normal subset in G, i.e., $X^g = X$ for every $g \in G$.

Proposition

Any Cayley graph over an abelian group is central

- If Γ is a Cayley graph then $G_{right} \leq \mathrm{Aut}(\Gamma)$
- If Γ is a central Cayley graph then $G_{left} G_{right} \leq \mathrm{Aut}(\Gamma)$ because $h(g, xg) = (hg, x^{h^{-1}} hg) = (hg, x'(hg))$

Note that (a) G_{left} and G_{right} centralize each other, and (b) $G_{left} \cap G_{right} = \{h_{right} \mid h \in Z(G)\}$, so $Z(G) = 1 \Rightarrow G_{left} G_{right}$ is the direct product of two copies of G.

Central Cayley Graphs over Almost Simple Groups

- S is nonabelian simple group ($S \simeq \mathrm{Inn}(S)$)
- G is called an almost simple group, if $S \leq G \leq \mathrm{Aut}(S)$
- $S = \mathrm{Soc}(G)$ is the socle of G

Central Cayley Graphs over Almost Simple Groups

- S is nonabelian simple group ($S \simeq \mathrm{Inn}(S)$)
- G is called an almost simple group, if $S \leq G \leq \mathrm{Aut}(S)$
- $S = \mathrm{Soc}(G)$ is the socle of G

Proposition

The number of the central Cayley graphs over a symmetric group is exponential in the size of the group

Central Cayley Graphs over Almost Simple Groups

- S is nonabelian simple group ($S \simeq \mathrm{Inn}(S)$)
- G is called an almost simple group, if $S \leq G \leq \mathrm{Aut}(S)$
- $S = \mathrm{Soc}(G)$ is the socle of G

Proposition

The number of the central Cayley graphs over a symmetric group is exponential in the size of the group

Indeed, if $G = \mathrm{Sym}(n)$, then the number $N(n)$ of the central Cayley graphs over G is equal to $2^{p(n)}$, where $p(n)$ is the number of all partitions of n. Since $p(n)$ is approximately equal to $2^{\sqrt{n}}$, the number $N(n)$ is exponential in $|G| = n!$

Main Results. Part 1

Theorem 1

For any two central Cayley graphs Γ and Γ' over an explicitly given almost simple group G of order n, the set $\mathrm{Iso}(\Gamma, \Gamma')$ can be found in time $\mathrm{poly}(n)$.

Main Results. Part 1

Theorem 1

For any two central Cayley graphs Γ and Γ' over an explicitly given almost simple group G of order n, the set $\mathrm{Iso}(\Gamma, \Gamma')$ can be found in time $\mathrm{poly}(n)$.

Corollary

The automorphism group of a central Cayley graph over an explicitly given almost simple group G of order n can be found in time $\mathrm{poly}(n)$.

Cayley Representations and Regular Subgroups

- $\Gamma = \mathrm{Cay}(G, X)$ and $\Gamma' = \mathrm{Cay}(G, X')$
- $\mathrm{Iso}_{\mathrm{Cay}}(\Gamma, \Gamma') = \mathrm{Aut}(G) \cap \mathrm{Iso}(\Gamma, \Gamma')$
- Γ and Γ' are called Cayley isomorphic if $\mathrm{Iso}_{\mathrm{Cay}}(\Gamma, \Gamma') \neq \varnothing$
- Cayley representation of a graph Γ over a group G is a Cayley graph $\mathrm{Cay}(G, X)$ isomorphic to Γ
- Cayley representations of Γ are equivalent if they are Cayley isomorphic

Cayley Representations and Regular Subgroups

- $\Gamma = \mathrm{Cay}(G, X)$ and $\Gamma' = \mathrm{Cay}(G, X')$
- $\mathrm{Iso}_{\mathrm{Cay}}(\Gamma, \Gamma') = \mathrm{Aut}(G) \cap \mathrm{Iso}(\Gamma, \Gamma')$
- Γ and Γ' are called Cayley isomorphic if $\mathrm{Iso}_{\mathrm{Cay}}(\Gamma, \Gamma') \neq \varnothing$
- Cayley representation of a graph Γ over a group G is a Cayley graph $\mathrm{Cay}(G, X)$ isomorphic to Γ
- Cayley representations of Γ are equivalent if they are Cayley isomorphic

- A transitive permutation group is called regular if its point stabilizer is trivial
- Given a group G, a regular subgroup of a permutation group is said to be G-regular, if it is isomorphic to G.

Proposition (Babai, 1975)

There is a one-to-one correspondence between the non-equivalent Cayley representations of a graph Γ over a group G and the conjugacy classes of G-regular subgroups of $\mathrm{Aut}(\Gamma)$.

G-base of a Permutation Group

Definition

Let G be a group and $K \leq \mathrm{Sym}(\Omega)$. A set $\mathcal{B} = \{B_i, i \in I\}$ of G-regular subgroups of K is called a G-base of K iff every G-regular subgroup of K is conjugate in K to exactly one B_i. Set $b_G(K) = |\mathcal{B}|$.

G-base of a Permutation Group

Definition

Let G be a group and $K \leq \mathrm{Sym}(\Omega)$. A set $\mathcal{B} = \{B_i, i \in I\}$ of G-regular subgroups of K is called a G-base of K iff every G-regular subgroup of K is conjugate in K to exactly one B_i. Set $b_G(K) = |\mathcal{B}|$.

- For $\Gamma = \mathrm{Cay}(G, X)$ put $b_G(\Gamma) = b_G(\mathrm{Aut}(\Gamma))$
  In this case $b_G(\Gamma) \geq 1$ due to $G_{right} \leq \mathrm{Aut}(\Gamma)$

G-base of a Permutation Group

Definition

Let G be a group and $K \leq \mathrm{Sym}(\Omega)$. A set $\mathcal{B} = \{B_i, i \in I\}$ of G-regular subgroups of K is called a G-base of K iff every G-regular subgroup of K is conjugate in K to exactly one B_i. Set $b_G(K) = |\mathcal{B}|$.

- For $\Gamma = \mathrm{Cay}(G, X)$ put $b_G(\Gamma) = b_G(\mathrm{Aut}(\Gamma))$
  In this case $b_G(\Gamma) \geq 1$ due to $G_{right} \leq \mathrm{Aut}(\Gamma)$
- Babai's argument yields that Γ is CI-graph $\Leftrightarrow b_G(\Gamma) = 1$

G-base of a Permutation Group

Definition

Let G be a group and $K \leq \mathrm{Sym}(\Omega)$. A set $\mathcal{B} = \{B_i, i \in I\}$ of G-regular subgroups of K is called a G-base of K iff every G-regular subgroup of K is conjugate in K to exactly one B_i. Set $b_G(K) = |\mathcal{B}|$.

- For $\Gamma = \mathrm{Cay}(G, X)$ put $b_G(\Gamma) = b_G(\mathrm{Aut}(\Gamma))$
  In this case $b_G(\Gamma) \geq 1$ due to $G_{right} \leq \mathrm{Aut}(\Gamma)$
- Babai's argument yields that Γ is CI-graph $\Leftrightarrow$ $b_G(\Gamma) = 1$

CGIP is reducible in time polynomial in $b_G(\Gamma)$ to the problem:
Given a Cayley graph Γ over a group G, find a G-base of $\mathrm{Aut}(\Gamma)$

Main Results. Part 2

Let $\mathcal{G}_n$ stand for the set of central Cayley graphs Γ over an explicitly given group G of order n with a simple socle and a cyclic quotient $G/\operatorname{Soc}(G)$.

Theorem 2

For every $\Gamma \in \mathcal{G}_n$, one can find a G-base of $\operatorname{Aut}(\Gamma)$ in time $\operatorname{poly}(n)$. In particular, a full system of pairwise nonequivalent Cayley representations of Γ can be found within the same time.

Main Results. Part 2

Let $\mathcal{G}_n$ stand for the set of central Cayley graphs Γ over an explicitly given group G of order n with a simple socle and a cyclic quotient $G/\operatorname{Soc}(G)$.

Theorem 2

For every $\Gamma \in \mathcal{G}_n$, one can find a G-base of $\operatorname{Aut}(\Gamma)$ in time $\operatorname{poly}(n)$. In particular, a full system of pairwise nonequivalent Cayley representations of Γ can be found within the same time.

A canonical labelling of every graph in $\mathcal{G}_n$ can be constructed in time $\operatorname{poly}(n)$.

Sketch of the Proof. Analysis

- G is an almost simple group, $S = \mathrm{Soc}(G)$, $X \subseteq G$
- $\Gamma = \mathrm{Cay}(G, X)$ is a central Cayley graph, $K = \mathrm{Aut}(\Gamma)$

Sketch of the Proof. Analysis

- G is an almost simple group, $S = \mathrm{Soc}(G)$, $X \subseteq G$
- $\Gamma = \mathrm{Cay}(G, X)$ is a central Cayley graph, $K = \mathrm{Aut}(\Gamma)$
- L is the intersection of all non-singleton K-blocks containing e
- Then $S \leq L \trianglelefteq G$ (because Γ is central) and we have two cases:

Sketch of the Proof. Analysis

- G is an almost simple group, $S = \mathrm{Soc}(G)$, $X \subseteq G$
- $\Gamma = \mathrm{Cay}(G, X)$ is a central Cayley graph, $K = \mathrm{Aut}(\Gamma)$
- L is the intersection of all non-singleton K-blocks containing e
- Then $S \leq L \trianglelefteq G$ (because Γ is central) and we have two cases:

1. $L = G \Rightarrow K$ is primitive, then
    - $K = \mathrm{Sym}(G)$, or
    - The classification of regular subgroups of primitive permutation groups (Liebeck, Praeger, Saxl, 2010) $\Rightarrow G = S$

Sketch of the Proof. Analysis

- G is an almost simple group, $S = \mathrm{Soc}(G)$, $X \subseteq G$
- $\Gamma = \mathrm{Cay}(G, X)$ is a central Cayley graph, $K = \mathrm{Aut}(\Gamma)$
- L is the intersection of all non-singleton K-blocks containing e
- Then $S \leq L \trianglelefteq G$ (because Γ is central) and we have two cases:

1. $L = G \Rightarrow K$ is primitive, then
   - $K = \mathrm{Sym}(G)$, or
   - The classification of regular subgroups of primitive permutation groups (Liebeck, Praeger, Saxl, 2010) $\Rightarrow G = S$
2. $L < G \Rightarrow K$ is imprimitive, then
   - $\mathcal{L} = \{L^k \mid k \in K\}$ is the non-trivial system of imprimitivity
   - Based on some special equivalence relation on $\mathcal{L}$ we set U to be the union of blocks from $\mathcal{L}$ equivalent to L
   - Then $U \trianglelefteq G$ and K is the generalized wreath product w.r.t. the section U/L (in particular, if $U = L$, then $K \simeq K^L \wr K^{\mathcal{L}}$ is the ordinary wreath product)

Sketch of the Proof. Algorithm

As in many modern algorithm for testing isomorphism the main tool is the Weisfeiler–Leman algorithm.

Sketch of the Proof. Algorithm

As in many modern algorithm for testing isomorphism the main tool is the Weisfeiler–Leman algorithm.

Bird's-eye view of the algorithm

1. Find sections U/L and U'/L' of $K = \mathrm{Aut}(\Gamma)$ and $K' = \mathrm{Aut}(\Gamma')$ by exhaustive search ($S \leq L \leq U \leq G$ and $|G/S| \leq \log n$)
2. Find $\mathrm{Iso}(\Gamma_U, \Gamma'_{U'})$, where Γ_U and $\Gamma'_{U'}$ are the 'restrictions' of Γ and Γ' to U and U' (the special structure of U and U')
3. Find $\mathrm{Iso}(\Gamma_{\mathcal{L}}, \Gamma'_{\mathcal{L}'})$, where $\Gamma_{\mathcal{L}}$ and $\Gamma'_{\mathcal{L}'}$ are the 'quotients' of Γ and Γ' modulo $\mathcal{L}$ and $\mathcal{L}'$ (the Babai algorithm for isomorphism testing)
4. Output $\mathrm{Iso}(\Gamma, \Gamma')$ obtained by 'gluing' $\mathrm{Iso}(\Gamma_U, \Gamma'_{U'})$ and $\mathrm{Iso}(\Gamma_{\mathcal{L}}, \Gamma'_{\mathcal{L}'})$ (the Babai algorithm for coset intersection)

Sketch of the Proof. Case of Simple Groups

- G is nonabelian simple group, $\Gamma = \mathrm{Cay}(G, X)$, $K = \mathrm{Aut}(\Gamma)$
- $D(2, G) = \mathrm{Hol}(G).2 \leq \mathrm{Sym}(G)$, where $\mathrm{Hol}(G) = G\,\mathrm{Aut}(G)$ is extended by the involution $g \mapsto g^{-1}$, $g \in G$.
- $Z(G) = 1$ and Γ is central $\Rightarrow G_{left} \times G_{right} = G\,\mathrm{Inn}(G) \leq K$
- If $K \neq \mathrm{Sym}(G)$, then the O'Nan-Scott Theorem implies that $K \leq D(2, G)$
- It follows that $|K|$ is polynomial in $|G|$, in particular, a G-base of K can be found in polynomial time

Last Remarks

Evdokimov, Muzychuk, Ponomarenko, 2016:

For every prime p there is $K \leq \mathrm{Sym}(p^3)$ such that $b_G(K) \geq p^{p-2}$, where G is an elementary abelian group of order p^3

Last Remarks

Evdokimov, Muzychuk, Ponomarenko, 2016:

For every prime p there is $K \leq \mathrm{Sym}(p^3)$ such that $b_G(K) \geq p^{p-2}$, where G is an elementary abelian group of order p^3

Note that $b_G(K)$ grows exponentially in the order of G as p grows

Last Remarks

Evdokimov, Muzychuk, Ponomarenko, 2016:

For every prime p there is $K \leq \mathrm{Sym}(p^3)$ such that $b_G(K) \geq p^{p-2}$, where G is an elementary abelian group of order p^3

Note that $b_G(K)$ grows exponentially in the order of G as p grows

On the other hand, the group K cannot be the automorphism group of any graph.

Last Remarks

Evdokimov, Muzychuk, Ponomarenko, 2016:

For every prime p there is $K \leq \mathrm{Sym}(p^3)$ such that $b_G(K) \geq p^{p-2}$, where G is an elementary abelian group of order p^3

Note that $b_G(K)$ grows exponentially in the order of G as p grows

On the other hand, the group K cannot be the automorphism group of any graph.