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

Groups, Rings, and their Automorphisms, Lincoln
31.08-02.09, 2016
Cayley Graph Isomorphism Problem

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

- $\Gamma = \text{Cay}(G, X)$ and $\Gamma' = \text{Cay}(G, X')$
  \[ \text{Iso}(\Gamma, \Gamma') = \{f \in \text{Sym}(G) \mid s^f \in E(\Gamma') \text{ for } s \in E(\Gamma)\} \]
  \[ \text{Aut}(\Gamma) = \text{Iso}(\Gamma, \Gamma) \text{ and } G_{\text{right}} \leq \text{Aut}(\Gamma) \leq \text{Sym}(G) \]
  \[ \text{Iso}(\Gamma, \Gamma') \text{ is (if not empty) } \text{Aut}(\Gamma)\text{-coset in } \text{Sym}(G) \]

Cayley Graph Isomorphism Problem (CGIP)

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

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

Output $\text{Iso}(\Gamma, \Gamma')$ is either empty or given by a permutation from $\text{Iso}(\Gamma, \Gamma')$ and some generating set of $\text{Aut}(\Gamma)$
Babai’s algorithm solves CGIP in quasipolynomial time
CGIP ⇒ 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 poly(|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 ⇔ the automorphism group Aut(Γ) 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)
Recognition problem for Cayley graph over the cyclic groups is solved in polynomial time (Evdokimov-Ponomarenko, 2003)
Central Cayley Graphs

- $G$ is a group, $X \subseteq G$, and $\Gamma = \text{Cay}(G, X)$
- $\Gamma$ 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 $\Gamma$ is a Cayley graph then $G_{\text{right}} \leq \text{Aut}(\Gamma)$
- If $\Gamma$ is a central Cayley graph then $G_{\text{left}} G_{\text{right}} \leq \text{Aut}(\Gamma)$ because $h(g, xg) = (hg, x^{h^{-1}}hg) = (hg, x'(hg))$

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

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

Our Goal

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

Proposition

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

Indeed, if $G = \text{Sym}(n)$, 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 $\Gamma$ and $\Gamma'$ over an explicitly given almost simple group $G$ of order $n$, the set $\text{Iso}(\Gamma, \Gamma')$ can be found in time $\text{poly}(n)$.

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 $\text{poly}(n)$. 
Cayley Representations and Regular Subgroups

- $\Gamma = \text{Cay}(G, X)$ and $\Gamma' = \text{Cay}(G, X')$
- $\text{Iso}_{\text{Cay}}(\Gamma, \Gamma') = \text{Aut}(G) \cap \text{Iso}(\Gamma, \Gamma')$
- $\Gamma$ and $\Gamma'$ are called Cayley isomorphic if $\text{Iso}_{\text{Cay}}(\Gamma, \Gamma') \neq \emptyset$
- If $\Gamma$ and $\Gamma'$ are Cayley isomorphic, then their adjacency matrices are equal
- Cayley representation of a graph $\Gamma$ over a group $G$ is a Cayley graph $\text{Cay}(G, X)$ isomorphic to $\Gamma$
- Cayley representations of $\Gamma$ are equivalent if they are Cayley isomorphic
- 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, 1977)

There is a one-to-one correspondence between nonequivalent Cayley representations of a graph $\Gamma$ over a group $G$ and the conjugacy classes of $G$-regular subgroups of $\text{Aut}(\Gamma)$. 
**G-base of a Permutation Group**

**Definition**

Let \( G \) be a group and \( K \leq \text{Sym}(\Omega) \). 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 \( \Gamma = \text{Cay}(G, X) \) put \( b_G(\Gamma) = b_G(\text{Aut}(\Gamma)) \)
  - In this case \( b_G(\Gamma) \geq 1 \) due to \( G_{right} \leq \text{Aut}(\Gamma) \)
  - Babai’s argument yields that \( \Gamma \) 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 \( \Gamma \) over a group \( G \), find a \( G \)-base of \( \text{Aut}(\Gamma) \).
Main Results. Part 2

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

**Theorem 2**

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

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

### $G$-base of a Permutation Group. Remarks

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>For a group $G$ and $K \leq \text{Sym}(G)$, find a $G$-base of $K$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Evdokimov, Muzychuk, Ponomarenko, 2016:</th>
</tr>
</thead>
<tbody>
<tr>
<td>For every prime $p$ there is $K \leq \text{Sym}(p^3)$ such that $b_G(K) \geq p^{p-2}$, where $G$ is an elementary abelian group of order $p^3$</td>
</tr>
</tbody>
</table>

Note that $b_G(K)$ grows exponentially in the order of $G$ as $p$ grows, but the group $K$ cannot be the automorphism group of any graph.

<table>
<thead>
<tr>
<th>Problem (corrected version)</th>
</tr>
</thead>
<tbody>
<tr>
<td>For a group $G$ and a 2-closed permutation group $K \leq \text{Sym}(G)$, find a $G$-base of $K$</td>
</tr>
</tbody>
</table>

$H \leq \text{Sym}(\Omega)$ is 2-closed if $H = H^{(2)} = \text{Aut}(\text{Orb}(H, \Omega \times \Omega))$
Sketch of the Proof. Analysis

- $G$ is an almost simple group, $|G| = n$, $S = \text{Soc}(G)$, $X \subseteq G$
- $\Gamma = \text{Cay}(G, X)$ is a central Cayley graph, $K = \text{Aut}(\Gamma)$
- We have two cases:

1. $K$ is primitive, then $K = \text{Sym}(G)$ or $|K| = \text{poly}(n)$

2. $K$ is imprimitive, then $|K| = \text{poly}(n)$ or $K$ is a nontrivial generalized wreath product

- The generalized wreath product was introduced by D.K. Faddeev in 1950's in connection with the inverse Galois problem
Sketch of the Proof. Primitive case

Let $K = \text{Aut}(\Gamma)$ be primitive. Then the classification of regular almost simple subgroups of primitive permutation groups (Liebeck, Praeger, Saxl, 2010) $\Rightarrow$ $G = S$

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

Let \( K = \text{Aut}(\Gamma) \) be imprimitive.

- Set \( L \) to be the intersection of all non-singleton \( K \)-blocks containing the identity element of \( G \).
- Then \( S \leq L \unlhd G \) (because \( \Gamma \) is central).
- Moreover, if \( K_0 \) is the setwise stabilizer of the imprimitivity system \( \mathcal{L} \) containing \( L \), then
  \[
  K_0 = \prod_{Y \in G/U} (K_0)^Y
  \]
  for a uniquely determined \( K \)-block \( U \) containing \( L \).
- If \( U = G \), then \( K \leq N_{\text{Sym}(G)}(S_{\text{left}} \times S_{\text{right}}) \), so \( |K| = \text{poly}(n) \).
- If \( U < G \), then \( K \) is permutation isomorphic to the generalized wreath product of the groups \( K^U \) and \( K^{G/L} \).
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 the sections $U/L$ and $U'/L'$ by exhaustive search ($S \leq L \leq U \leq G$ and $|G/S| \leq \log n$)
2. Find $\text{Iso}(\Gamma_U, \Gamma'_U)$, where $\Gamma_U$ and $\Gamma'_U$ are the ‘restrictions’ of $\Gamma$ and $\Gamma'$ to $U$ and $U'$ ($|K^U| = \text{poly}(n)$ and $|(K')^U'| = \text{poly}(n)$)
3. Find $\text{Iso}(\Gamma_L, \Gamma'_L)$, where $\Gamma_L$ and $\Gamma'_L$ are the ‘quotients’ of $\Gamma$ and $\Gamma'$ modulo $L$ and $L'$ (the Babai algorithm for isomorphism testing)
4. Output $\text{Iso}(\Gamma, \Gamma')$ obtained by ‘gluing’ $\text{Iso}(\Gamma_U, \Gamma'_U)$ and $\text{Iso}(\Gamma_L, \Gamma'_L)$ (the Babai algorithm for coset intersection)
Cayley graphs and Schur rings

- A Cayley graph \( \Gamma = \text{Cay}(G, X) \) can be identified with the element \( \sum_{x \in X} x \) of a Schur ring over \( G \).
- In this language the analysis we made in the proof of our result gives the structure theorem for the central Schur rings over almost simple groups.