

The group isomorphism problem in computational complexity theory

Saveliy Skresanov

Sobolev Institute of Mathematics, Novosibirsk, Russia

Computational complexity

A Turing machine has 3 tapes: input, a working tape, output.

An algorithm works in **polynomial time** if the corresponding Turing machine halts in the number of steps, polynomially bounded in terms of input length.

Examples

Input: An integer $n > 1$ in unary (input length is n)
Output: Smallest prime divisor of n } poly-time

Input: An integer $n > 1$ in binary (input length is $\log_2 n$)
Output: Smallest prime divisor of n } ?

Graph isomorphism problem

Graph isomorphism problem (ISO)

Input: graphs Γ_1, Γ_2 given by adjacency matrices (input length is $O(n^2)$, where n is the number of vertices)

Output: 1, if $\Gamma_1 \simeq \Gamma_2$, 0 otherwise.

Bruteforce algorithm of complexity $n! = O(n^n)$.

Conjectured to be a problem of intermediate complexity, i.e. not in P, but not NP-complete either.

Best algorithm is due to Babai, 2015: $n^{O((\log n)^c)}$, $c > 1$.

Group isomorphism problem

Group isomorphism problem (GrpISO)

Input: groups G, H given by Cayley tables (input length is $O(n^2 \log n)$, where $n = |G| = |H|$)

Output: 1, if $G \simeq H$, 0 otherwise.

Trivial algorithm of complexity $n^{\log n + O(1)}$: choose $\log n$ generators in G and bruteforce their images in H .

Nothing much better is known.

GrpISO is poly-time reducible to ISO, i.e. the group isomorphism problem is a “lower bound” for graph isomorphism.

What is known

GrpISO in time $n^{\frac{1}{4} \log n + O(1)}$ (Rosenbaum et al., 2016)

Essentially a technical improvement to the $n^{\log n + O(1)}$ algorithm.

Isomorphism of k -generated groups in time $n^{k+O(1)}$.

E.g. cyclic groups, simple groups in poly-time.

Abelian groups in linear time (Kavitha, 2007)

Groups of cube-free order in poly-time (Dietrich, Wilson, 2020)

Theorem (Babai, Codenotti, Qiao, 2012)

GrpISO for groups with trivial solvable radical in poly-time.

p -Groups

Let G be a p -group of class 2 and exponent $p > 2$.

Set $W = [G, G]$, $V = G/W$.

We need to determine isomorphism of bilinear maps

$$[\cdot, \cdot] : V \times V \rightarrow W.$$

Theorem (Sun et al., 2025)

GrpISO in time $n^{O((\log n)^{8/9})}$ for odd order nilpotent groups of class 2.

There are generalizations for p -groups of class c and exponent p , where $c < p$. For $p = 2$ and exponent 4 nothing is known.

Extensions of abelian groups

What about extending an abelian group by a “well-understood” group?

GrpISO in poly-time for coprime extensions of abelian groups by cyclic groups (LeGall, 2009).

Theorem (Qiao, Sarma, Tang, 2011)

GrpISO in time $n^{O(k)}$ for coprime extensions of abelian groups by k -generated groups.

By Schur–Zassenhaus theorem, a coprime extension splits $G = A \rtimes H$, and isomorphism is determined by the action of $G/A \simeq H$ on A .

In the general case one needs additional info about the extension.

Theorem (S., 2026+)

G, G_0 — groups given by Cayley tables, $n = |G|$,
 $A \trianglelefteq G$, $A_0 \trianglelefteq G_0$ are normal abelian subgroups, and G/A is
 k -generated. If an isomorphism $\psi : G/A \rightarrow G_0/A_0$ is given, then
one can check in time $n^{O(k)}$ whether it can be extended to an
isomorphism $\Psi : G \rightarrow G_0$.

If A, A_0 are given as a part of input, then this generalizes the result
of Qiao–Sarma–Tang to non-coprime extensions.

Corollary

GrpISO in time $n^{O(k)}$ for extensions of abelian groups by
 k -generated abelian groups.

In particular, this resolves the isomorphism problem for
abelian-by-cyclic groups.

Proof idea

Set $H \simeq G/A \simeq G_0/A_0$. Then A and A_0 are H -modules.

Checking that A and A_0 are isomorphic H -modules isn't enough.

We need to find an H -module isomorphism $\phi : A \rightarrow A_0$ such that $\phi(a_i) = a_i^0$ for some carefully chosen $a_1, \dots, a_m \in A$ and $a_1^0, \dots, a_m^0 \in A_0$.

These elements are chosen by writing down a presentation of H and evaluating relators in G and G_0 .

ϕ is found by linearization and computing units of a finite ring.

Units of a finite ring

Theorem (S., 2026+)

Let R be a finite unitary ring given by its additive generators. If p is the largest prime divisor of $|R|$, then multiplicative generators of $R^\times$ can be computed in time polynomial in p and $\log |R|$.

One cannot remove the condition on p , because of the factorization and discrete logarithm problems (Hofmann, 2026).

Proof idea: find Jacobson radical and reduce everything to matrix algebras.

Cohomological methods

Let $A \trianglelefteq G$ and assume A is abelian. G is determined up to isomorphism by:

- ▶ the action of G/A on A (module isomorphism problem).
- ▶ cohomology class in $H^2(G/A, A)$.

Finite module isomorphism problem is solvable in poly-time (Ciocănea–Teodorescu, 2015).

Grochow, Qiao, 2017, suggested an approach towards the cohomological problem when $\text{Aut}(G/A)$ can be enumerated effectively and A is central (+ sometimes also elementary abelian).

Theorem (Grochow, Qiao, 2017)

GrpISO is poly-time for groups G such that the solvable radical A is central and elementary abelian, while G/A is isomorphic to a direct product of simple groups.

One can assume only that A is abelian, if G/A is generated by a bounded number of elements:

Theorem (S., 2026+)

GrpISO in time $n^{O(k)}$ for groups G with the abelian solvable radical A such that G/A is k -generated.

Corollary

GrpISO in time $n^{O(k)}$ for groups G with the abelian solvable radical A such that G/A is isomorphic to a direct product of k simple groups.

Theorem (S., 2026+)

GrpISO in time $n^{O(k)}$ for groups G with a normal abelian subgroup A such that G/A has a subnormal series of length k with cyclic and simple factors.

Proof idea: to find A explicitly, bruteforce through all subnormal series of length k starting from G . For each suitable A apply the algorithm for abelian by $O(k)$ -generated extensions.

Groups with abelian Sylow towers

Since p -groups are most problematic, it is natural to restrict the structure of Sylow subgroups.

Theorem (Babai, Qiao, 2012)

GrpISO in poly-time for G with abelian Sylow towers, i.e.

$G = N_1 \supseteq N_2 \supseteq \cdots \supseteq N_k = 1$, $N_i \trianglelefteq G$, and N_i/N_{i+1} is abelian and isomorphic to a Sylow subgroup of G .

The main idea is that G is built out of abelian p -groups by coprime extensions, so the cohomological part of the problem vanishes.

Solvable A-groups

G is an **A-group**, if all its Sylow subgroups are abelian.

Babai–Qiao groups are A-groups, but there exist nonsolvable A-groups (e.g. $\text{Alt}(5)$), and solvable A-groups without a Sylow tower (e.g. $\text{Sym}(3) \times \text{Alt}(4)$).

Theorem (S., 2026+)

GrpISO in poly-time for solvable A-groups.

The class of A-groups is better from the group-theoretic point of view than the class of groups with abelian Sylow towers, since it's closed with respect to taking subgroups, quotients and direct products.

Proof idea

$G = A \rtimes H$, where A is an abelian p -group. All p -elements of H act trivially on A , since Sylow p -subgroups of G are abelian.

Everything reduces to the action of a p' -group H/K on A , where $K \leq H$ is generated by all p -elements of H , and also to the following two problems:

Intertwining automorphisms problem:

$\alpha, \beta : H \rightarrow \text{Aut}(A)$, find $\{\psi \in \text{Aut}(A) \mid \alpha^\psi = \beta\}$.

Representation-transporting automorphisms problem:

$\alpha, \beta : H \rightarrow \text{Aut}(A)$, $P \leq \text{Aut}(H)$, find $\{\phi \in P \mid \alpha^\phi = \beta\}$.

Wild problems vs. computation

“Wild” problems are often computationally easy:

- ▶ Given matrices $A_1, \dots, A_n, B_1, \dots, B_n$ find a matrix T s.t.

$$T^{-1}A_iT = B_i, \quad i = 1, \dots, n.$$

- ▶ Given matrices $A_1, \dots, A_n$ find generators of the centralizer:

$$\{T \in \mathrm{GL}_m \mid TA_i = A_iT, \quad i = 1, \dots, n\}.$$

Not all problems are easy though:

- ▶ Given a permutation group $G \leq \mathrm{Sym}(\Omega)$ and $\Delta \subset \Omega$ find

$$\{g \in G \mid \Delta^g = \Delta\}.$$

- ▶ Computations with $H^2(G/A, A)$.

Reductions

Graph problems:

ISO(Γ_1, Γ_2):	decide if $\Gamma_1 \simeq \Gamma_2$ or not
IMAP(Γ_1, Γ_2):	find an isomorphism $\Gamma_1 \rightarrow \Gamma_2$
ICOUNT(Γ_1, Γ_2):	find $ \text{Iso}(\Gamma_1, \Gamma_2) $
ACOUNT(Γ):	find $ \text{Aut}(\Gamma) $
AGEN(Γ):	find generators of $\text{Aut}(\Gamma) \leq \text{Sym}(\Gamma)$
APART(Γ):	find orbits of $\text{Aut}(\Gamma)$ on Γ

A problem P_1 is **polynomial-time reducible** to P_2 , if P_1 can be solved in poly-time with oracle P_2 (notation: $P_1 \propto P_2$).

P_1 and P_2 are poly-time equivalent, if $P_1 \propto P_2$ and $P_2 \propto P_1$.

Theorem (Mathon, 1979)

Above problems on graphs are poly-time equivalent to each other.

Group problems:

$\text{GrpISO}(G, H)$:	decide if $G \simeq H$ or not
$\text{GrpIMAP}(G, H)$:	find an isomorphism $G \rightarrow H$
$\text{GrpICOUNT}(G, H)$:	find $ \text{Iso}(G, H) $
$\text{GrpACOUNT}(G)$:	find $ \text{Aut}(G) $
$\text{GrpAGEN}(G)$:	find generators of $\text{Aut}(G) \leq \text{Sym}(G)$
$\text{GrpAPART}(G)$:	find orbits $\text{Aut}(G)$ on G

Theorem (S., 2026+)

- (i) $\text{GrpISO} \propto \text{GrpACOUNT} \propto \text{GrpAGEN}$,
- (ii) $\text{GrpISO} \propto \text{GrpAPART} \propto \text{GrpAGEN}$,
- (iii) $\text{GrpIMAP} \propto \text{GrpAGEN}$,
- (iv) GrpICOUNT and GrpACOUNT are poly-time equivalent.

This theorem holds for any class of groups which is closed with respect to taking direct products and direct factors.

Left offscreen

- ▶ Many results solve GrpIMAP and GrpAGEN.
- ▶ Connection with algebraic problems such as tensor isomorphism, matrix tuple conjugacy etc.
- ▶ Permutation groups and black-box groups.
- ▶ Counting logics and Weisfeiler–Leman algorithm.

Open problems

- ▶ GrpISO in time $n^{o(\log n)}$?
- ▶ GrpISO for groups with abelian solvable radical?
- ▶ $\text{GrpAGEN} \propto \text{GrpISO}$?
- ▶ Reduce GrpISO to the case of p -groups?

The research was carried out within the framework of the Sobolev Institute of Mathematics state contract (project FWNF-2026-0017).