Permutation groups and the graph isomorphism problem

Andrey Vasil'ev

Sobolev Institute of Mathematics

Omsk
26-30.09.2023

Graph isomorphism problem

$\Gamma = (\Omega, E)$ is a graph
Ω is the vertex set, $E \subseteq \Omega^2$ is the edge (arc) set

For graphs $\Gamma = (\Omega, E)$ and $\Gamma' = (\Omega', E')$,
$\mathrm{Iso}(\Gamma, \Gamma') = \{f : \Omega \to \Omega' \text{ a bijection } \mid E^f = E'\}$.

Graph ISO

Given two graphs Γ and Γ', test whether $\mathrm{Iso}(\Gamma, \Gamma') = \varnothing$.

Graph isomorphism problem

$\Gamma = (\Omega, E)$ is a graph
Ω is the vertex set, $E \subseteq \Omega^2$ is the edge (arc) set

For graphs $\Gamma = (\Omega, E)$ and $\Gamma' = (\Omega', E')$,
$\mathrm{Iso}(\Gamma, \Gamma') = \{f : \Omega \to \Omega' \text{ a bijection } \mid E^f = E'\}$.

Graph ISO

Given two graphs Γ and Γ', test whether $\mathrm{Iso}(\Gamma, \Gamma') = \varnothing$.

Graph ISO consists in finding an algorithm testing isomorphism of two graphs, and performing the minimal number of steps.

We may assume that $\Omega = \Omega'$, so $\mathrm{Iso}(\Gamma, \Gamma') \subseteq \mathrm{Sym}(\Omega)$.
If $f \in \mathrm{Iso}(\Gamma, \Gamma') \neq \varnothing$, then $\mathrm{Iso}(\Gamma, \Gamma') = \mathrm{Aut}(\Gamma) f$ is a coset.

Graph isomorphism problem

$\Gamma = (\Omega, E)$ is a graph
Ω is the vertex set, $E \subseteq \Omega^2$ is the edge (arc) set

For graphs $\Gamma = (\Omega, E)$ and $\Gamma' = (\Omega', E')$,
$\mathrm{Iso}(\Gamma, \Gamma') = \{f : \Omega \to \Omega' \text{ a bijection } \mid E^f = E'\}$.

Graph ISO

Given two graphs Γ and Γ', test whether $\mathrm{Iso}(\Gamma, \Gamma') = \varnothing$.

Graph ISO consists in finding an algorithm testing isomorphism of two graphs, and performing the minimal number of steps.

We may assume that $\Omega = \Omega'$, so $\mathrm{Iso}(\Gamma, \Gamma') \subseteq \mathrm{Sym}(\Omega)$.
If $f \in \mathrm{Iso}(\Gamma, \Gamma') \neq \varnothing$, then $\mathrm{Iso}(\Gamma, \Gamma') = \mathrm{Aut}(\Gamma) f$ is a coset.

Babai, 2015

There is a constant c such that for graphs Γ and Γ' of size n the set $\mathrm{Iso}(\Gamma, \Gamma')$ can be found in a quasipolynomial time $2^{O(\log^c n)}$.

Graph isomorphism problem: Naive algorithm

Γ is a (simple undirected) graph with vertex set Ω, $|\Omega| = n$.

Naive algorithm

1. Set initial coloring: $c(\alpha) = 0$ for all $\alpha \in \Omega$.
2. For all $\alpha \in \Omega$, find a multiset $s(\alpha) = \{c(\beta) \mid \beta \in \Omega : (\alpha, \beta) \in E(\Gamma)\}$.
3. Define a coloring c': $c'(\alpha) < c'(\beta) \Leftrightarrow s(\alpha) \prec s(\beta)$.
4. Go to Step 2 if $|c| \neq |c'|$; otherwise output c.

Graph isomorphism problem: Naive algorithm

Γ is a (simple undirected) graph with vertex set Ω, $|\Omega| = n$.

Naive algorithm

1. Set initial coloring: $c(\alpha) = 0$ for all $\alpha \in \Omega$.
2. For all $\alpha \in \Omega$, find a multiset
   $s(\alpha) = \{c(\beta) \mid \beta \in \Omega : (\alpha, \beta) \in E(\Gamma)\}$.
3. Define a coloring c': $c'(\alpha) < c'(\beta) \Leftrightarrow s(\alpha) \prec s(\beta)$.
4. Go to Step 2 if $|c| \neq |c'|$; otherwise output c.

Babai–Erdös–Selkow, 1979

Almost all graphs are completely individualized (into n different colors) after 2 rounds $\Longrightarrow$ for them the isomorphism problem can be solved in linear time in n.

Bottleneck: Regular graphs (all the vertices have the same valency).

Weisfeiler–Leman algorithm (1968)

Let Γ be a graph (directed or undirected) with vertex set Ω.

WL-algorithm

1. Set initial coloring: $c(\alpha, \beta) = 0$, 1, or 2 depending on (α, β) is loop, arc, or neither loop nor arc, for all $(\alpha, \beta) \in \Omega \times \Omega$.
2. For all $(\alpha, \beta) \in \Omega \times \Omega$, find a multiset $s(\alpha, \beta) = \{s_\gamma(\alpha, \beta) : \gamma \in \Omega\}$, $s_\gamma(\alpha, \beta) = (c(\alpha, \gamma), c(\gamma, \beta))$.
3. Define a coloring c': $c'(\alpha, \beta) < c'(\gamma, \delta) \Leftrightarrow s(\alpha, \beta) \prec s(\gamma, \delta)$.
4. Go to Step 2 if $|c| \neq |c'|$; otherwise output c.

Weisfeiler–Leman algorithm (1968)

Let Γ be a graph (directed or undirected) with vertex set Ω.

WL-algorithm

1. Set initial coloring: $c(\alpha,\beta) = 0$, 1, or 2 depending on (α,β) is loop, arc, or neither loop nor arc, for all $(\alpha,\beta) \in \Omega \times \Omega$.
2. For all $(\alpha,\beta) \in \Omega \times \Omega$, find a multiset $s(\alpha,\beta) = \{s_\gamma(\alpha,\beta) : \gamma \in \Omega\}$, $s_\gamma(\alpha,\beta) = (c(\alpha,\gamma), c(\gamma,\beta))$.
3. Define a coloring c': $c'(\alpha,\beta) < c'(\gamma,\delta) \Leftrightarrow s(\alpha,\beta) \prec s(\gamma,\delta)$.
4. Go to Step 2 if $|c| \neq |c'|$; otherwise output c.

- The pair $\mathcal{X} = (\Omega, S)$, where S is a partition of Ω^2 into the color classes obtained by WL-algorithm, is the WL-closure of Γ.
- $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\mathcal{X}) = \{f \in \mathrm{Sym}(\Omega) : s^f = s, s \in S\}$.

Weisfeiler–Leman algorithm (1968)

Let Γ be a graph (directed or undirected) with vertex set Ω.

WL-algorithm

1. Set initial coloring: $c(\alpha, \beta) = 0$, 1, or 2 depending on (α, β) is loop, arc, or neither loop nor arc, for all $(\alpha, \beta) \in \Omega \times \Omega$.
2. For all $(\alpha, \beta) \in \Omega \times \Omega$, find a multiset $s(\alpha, \beta) = \{s_\gamma(\alpha, \beta) : \gamma \in \Omega\}$, $s_\gamma(\alpha, \beta) = (c(\alpha, \gamma), c(\gamma, \beta))$.
3. Define a coloring c': $c'(\alpha, \beta) < c'(\gamma, \delta) \Leftrightarrow s(\alpha, \beta) \prec s(\gamma, \delta)$.
4. Go to Step 2 if $|c| \neq |c'|$; otherwise output c.

- The pair $\mathcal{X} = (\Omega, S)$, where S is a partition of Ω^2 into the color classes obtained by WL-algorithm, is the WL-closure of Γ.
- $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\mathcal{X}) = \{f \in \mathrm{Sym}(\Omega) : s^f = s, s \in S\}$.
- Conjecture: $\mathrm{Orb}(\mathrm{Aut}(\mathcal{X}))$ coincides with the color classes of the vertex set Ω, given by $c(\alpha, \alpha), \alpha \in \Omega$.

Weisfeiler–Leman algorithm (1968)

Let Γ be a graph (directed or undirected) with vertex set Ω.

WL-algorithm

1. Set initial coloring: $c(\alpha, \beta) = 0$, 1, or 2 depending on (α, β) is loop, arc, or neither loop nor arc, for all $(\alpha, \beta) \in \Omega \times \Omega$.
2. For all $(\alpha, \beta) \in \Omega \times \Omega$, find a multiset $s(\alpha, \beta) = \{s_\gamma(\alpha, \beta) : \gamma \in \Omega\}$, $s_\gamma(\alpha, \beta) = (c(\alpha, \gamma), c(\gamma, \beta))$.
3. Define a coloring c': $c'(\alpha, \beta) < c'(\gamma, \delta) \Leftrightarrow s(\alpha, \beta) \prec s(\gamma, \delta)$.
4. Go to Step 2 if $|c| \neq |c'|$; otherwise output c.

- The pair $\mathcal{X} = (\Omega, S)$, where S is a partition of Ω^2 into the color classes obtained by WL-algorithm, is the WL-closure of Γ.
- $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\mathcal{X}) = \{f \in \mathrm{Sym}(\Omega) : s^f = s, s \in S\}$.
- Conjecture: $\mathrm{Orb}(\mathrm{Aut}(\mathcal{X}))$ coincides with the color classes of the vertex set Ω, given by $c(\alpha, \alpha), \alpha \in \Omega$.
- Conjecture is wrong (Adel'son-Vel'ski–W–L–Faradzev, 1969).

m-dim WL-algorithm and WL-dimension

In fact, the WL-algorithm deals with any $\Gamma = (\Omega, P)$, where P is a (colored) partition of Ω^2.

If $\Gamma = (\Omega, P)$, where P is a partition of Ω^m, then one can define m-dim WL-closure $\mathrm{WL}_m(\Gamma)$ of Γ using an algorithm similar to the classical 2-dim WL-algorithm.

The WL-dimension $\mathrm{WL}(\Gamma)$ of Γ is the smallest positive integer m such that Γ can be uniquely identified by m-dim WL-algorithm.

Kiefer–Ponomarenko–Schweitzer, 2017

If Γ is a planar graph, then $\text{WL-dim}(\Gamma) \leq 3$.

m-dim WL-algorithm and WL-dimension

In fact, the WL-algorithm deals with any $\Gamma = (\Omega, P)$, where P is a (colored) partition of Ω^2.

If $\Gamma = (\Omega, P)$, where P is a partition of Ω^m, then one can define m-dim WL-closure $\mathrm{WL}_m(\Gamma)$ of Γ using an algorithm similar to the classical 2-dim WL-algorithm.

The WL-dimension $\mathrm{WL}(\Gamma)$ of Γ is the smallest positive integer m such that Γ can be uniquely identified by m-dim WL-algorithm.

Kiefer–Ponomarenko–Schweitzer, 2017

If Γ is a planar graph, then $\text{WL-dim}(\Gamma) \leq 3$.

If there is a constant $c > 0$ such that $\dim_{\mathrm{WL}}(\Gamma) \leq c$ for every finite graph Γ, then Graph ISO can be solved in time $\mathrm{poly}(n)$.

The notion of WL-dimension can be also formulated in the language of the counting first order logic.

Graphs and m-fragment of first-order logic

The language of the logic $\mathfrak{C}_m$, $m \in \mathbb{N}$ for graphs:

- m variables $x_1, x_2 \ldots, x_m$
- a binary predicate $e(\cdot, \cdot)$
- a symbol $=$; and logical connectives $\vee, \wedge, \rightarrow, \neg$
- counting quantifiers $\exists^i x$, $i \in \mathbb{N}$.

Interpretation of formulas of $\mathfrak{C}_m$ for a graph Γ:

- $x_1, x_2 \ldots, x_m$ are vertices of Γ
- $e(x_i, x_j)$ is true if there is an edge between x_i and x_j in Γ
- $\exists^i x \varphi(x)$ — the formula $\varphi(x)$ is true for at least i vertices of Γ
- $\Gamma \models \varphi$ means that φ holds true on Γ.

Example: $\Gamma \models (\forall x_1)(\exists^5 x_2) e(x_1, x_2)$ means $\deg(\Gamma) \geq 5$.

$\mathfrak{C}_m$-equivalency, WL-dimension, and Graph ISO

Graphs Γ and Δ are $\mathfrak{C}_m$-equivalent, if

$$\forall \varphi \in \mathfrak{C}_m : \quad \Gamma \models \varphi \Longleftrightarrow \Delta \models \varphi.$$

The WL-dimension $\dim_{\mathrm{WL}}(\Gamma)$ of a graph Γ is the least m such that every graph Δ which is $\mathfrak{C}_{m+1}$-equivalent to Γ is isomorphic to Γ.

Cai–Fürer–Immerman, 1992

There is a constant $c > 0$ and a family of graphs Γ_n of degree n, $n \in \mathbb{N}$, such that $\dim_{\mathrm{WL}}(\Gamma_n) \geq cn$.

$\mathfrak{C}_m$-equivalency, WL-dimension, and Graph ISO

Graphs Γ and Δ are $\mathfrak{C}_m$-equivalent, if

$$\forall \varphi \in \mathfrak{C}_m : \quad \Gamma \models \varphi \Longleftrightarrow \Delta \models \varphi.$$

The WL-dimension $\dim_{\mathrm{WL}}(\Gamma)$ of a graph Γ is the least m such that every graph Δ which is $\mathfrak{C}_{m+1}$-equivalent to Γ is isomorphic to Γ.

Cai–Fürer–Immerman, 1992

There is a constant $c > 0$ and a family of graphs Γ_n of degree n, $n \in \mathbb{N}$, such that $\dim_{\mathrm{WL}}(\Gamma_n) \geq cn$.

Nevertheless,

$\Gamma = (\Omega, R)$ and $\Gamma' = (\Omega, R')$ graphs

$\Downarrow$ Weisfeiler–Leman algorithm $\Downarrow$

$\mathcal{X} = (\Omega, S)$ and $\mathcal{X}' = (\Omega, S')$ WL-closures of Γ and Γ'

$\mathrm{Iso}(\Gamma, \Gamma') = \mathrm{Iso}(\mathcal{X}, \mathcal{X}')$.

WL-closures and m-closures of permutation groups

Ω is a finite set, $G \le \mathrm{Sym}(\Omega)$, and m is a positive integer

G acts componentwisely on Ω^m: $(\alpha_1, \ldots, \alpha_m)^g = (\alpha_1^g, \ldots, \alpha_m^g)$

$\mathrm{Orb}_m(G)$ is the set of orbits of this action (m-orbits).

WL-closures and m-closures of permutation groups

Ω is a finite set, $G \leq \mathrm{Sym}(\Omega)$, and m is a positive integer

G acts componentwisely on Ω^m: $(\alpha_1, \ldots, \alpha_m)^g = (\alpha_1^g, \ldots, \alpha_m^g)$

$\mathrm{Orb}_m(G)$ is the set of orbits of this action (m-orbits).

$\mathrm{Inv}_m(G) = (\Omega, \mathrm{Orb}_m(G))$ can be considered as a specific combinatorial structure on Ω consisting of (colored) m-ary relations.

m-dim WL-closure of $\mathrm{Inv}_m(G)$ is always $\mathrm{Inv}_m(G)$ itself.

WL-closures and m-closures of permutation groups

Ω is a finite set, $G \leq \mathrm{Sym}(\Omega)$, and m is a positive integer

G acts componentwisely on Ω^m: $(\alpha_1, \ldots, \alpha_m)^g = (\alpha_1^g, \ldots, \alpha_m^g)$

$\mathrm{Orb}_m(G)$ is the set of orbits of this action (m-orbits).

$\mathrm{Inv}_m(G) = (\Omega, \mathrm{Orb}_m(G))$ can be considered as a specific combinatorial structure on Ω consisting of (colored) m-ary relations.

m-dim WL-closure of $\mathrm{Inv}_m(G)$ is always $\mathrm{Inv}_m(G)$ itself.

Definition (H. Wielandt, 1969)

The *m-closure* $G^{(m)}$ of G is the largest subgroup of $\mathrm{Sym}(\Omega)$ with $\mathrm{Orb}_m(G^{(m)}) = \mathrm{Orb}_m(G)$.

Equivalently,

$$G^{(m)} = \{g \in \mathrm{Sym}(\Omega) : \Delta^g = \Delta, \Delta \in \mathrm{Orb}_m(G)\} = \mathrm{Aut}(\mathrm{Inv}_m(G)).$$

m-Closure problem for solvable groups

m-Closure problem

Given a permutation group G, find $G^{(m)}$.

Here groups are specified by list of generating permutations.

m-Closure problem for solvable groups

m-Closure problem

Given a permutation group G, find $G^{(m)}$.

Here groups are specified by list of generating permutations.

Ponomarenko-V., 2023

Given an integer $m \geq 3$, the m-closure of a solvable permutation group of degree n can be found in time $n^{O(m)}$.

Properties of m-closures

It follows from the definition that

$$G^{(1)} \geq G^{(2)} \geq \ldots \geq G^{(m)} \geq \ldots \geq G^{(|\Omega|-1)} = G.$$

Properties of m-closures

It follows from the definition that

$$G^{(1)} \geq G^{(2)} \geq \ldots \geq G^{(m)} \geq \ldots \geq G^{(|\Omega|-1)} = G.$$

How far can $G^{(m)}$ be from G?

The m-closure of m-transitive group $G \leq \mathrm{Sym}(\Omega)$ is $\mathrm{Sym}(\Omega)$, so if $\Omega = \underbrace{\Delta_1 \cup \ldots \cup \Delta_s}_{1-\text{orbits}}$, then $G^{(1)} = \mathrm{Sym}(\Delta_1) \times \ldots \times \mathrm{Sym}(\Delta_s)$.

Properties of m-closures

It follows from the definition that

$$G^{(1)} \geq G^{(2)} \geq \ldots \geq G^{(m)} \geq \ldots \geq G^{(|\Omega|-1)} = G.$$

How far can $G^{(m)}$ be from G?

The m-closure of m-transitive group $G \leq \mathrm{Sym}(\Omega)$ is $\mathrm{Sym}(\Omega)$, so if $\Omega = \underbrace{\Delta_1 \cup \ldots \cup \Delta_s}_{1-\text{orbits}}$, then $G^{(1)} = \mathrm{Sym}(\Delta_1) \times \ldots \times \mathrm{Sym}(\Delta_s)$.

Suppose $m \geq 2$. Then

1. G is abelian $\Rightarrow$ $G^{(m)}$ is abelian
2. G is of odd order $\Rightarrow$ $G^{(m)}$ is of odd order
3. G is a p-group $\Rightarrow$ $G^{(m)}$ is a p-group (Wielandt, 1969)

Properties of m-closures

It follows from the definition that

$$G^{(1)} \geq G^{(2)} \geq \ldots \geq G^{(m)} \geq \ldots \geq G^{(|\Omega|-1)} = G.$$

How far can $G^{(m)}$ be from G?

The m-closure of m-transitive group $G \leq \mathrm{Sym}(\Omega)$ is $\mathrm{Sym}(\Omega)$, so if $\Omega = \underbrace{\Delta_1 \cup \ldots \cup \Delta_s}_{1-\text{orbits}}$, then $G^{(1)} = \mathrm{Sym}(\Delta_1) \times \ldots \times \mathrm{Sym}(\Delta_s)$.

Suppose $m \geq 2$. Then

1. G is abelian $\Rightarrow G^{(m)}$ is abelian
2. G is of odd order $\Rightarrow G^{(m)}$ is of odd order
3. G is a p-group $\Rightarrow G^{(m)}$ is a p-group (Wielandt, 1969)
4. G is nilpotent $\Rightarrow G^{(m)}$ is nilpotent ($\sim$ 2020).

Solvable permutation groups

There are 2-transitive solvable groups, say, $\mathrm{AGL}(1,p)^{(2)} = \mathrm{Sym}(p)$ for a prime p, so assuming $p \geq 5$, we get

G is solvable $\not\Rightarrow G^{(2)}$ is solvable.

Solvable permutation groups

There are 2-transitive solvable groups, say, $\mathrm{AGL}(1,p)^{(2)} = \mathrm{Sym}(p)$ for a prime p, so assuming $p \geq 5$, we get

G is solvable $\not\Rightarrow$ $G^{(2)}$ is solvable.

A. Seress (1995):

If G is a solvable primitive group, then $G = G^{(5)}$.

Solvable permutation groups

There are 2-transitive solvable groups, say, $\mathrm{AGL}(1,p)^{(2)} = \mathrm{Sym}(p)$ for a prime p, so assuming $p \geq 5$, we get

G is solvable $\not\Rightarrow$ $G^{(2)}$ is solvable.

A. Seress (1995):

If G is a solvable primitive group, then $G = G^{(5)}$.

E. O'Brien, I. Ponomarenko, A. V., and E. Vdovin (2021):

If $m \geq 3$ and G is solvable, then $G^{(m)}$ is solvable.

Babai–Lucks argument

Babai–Lucks argument

The composition width $cw(H)$ of a group H is the least positive integer d such that every nonabelian composition factor of a group H can be embedded in $\mathrm{Sym}(d)$.

Babai–Lucks, 1983

Let $\Gamma = (\Omega, E)$ be a graph. Given $H \leq \mathrm{Sym}(\Omega)$ with $cw(H) \leq d$, the group $\mathrm{Aut}(\Gamma) \cap H$ can be constructed in time $n^{f(d)}$.

Corollary

Let $G \leq \mathrm{Sym}(\Omega)$ and $m \in \mathbb{N}$. Given $H \leq \mathrm{Sym}(\Omega)$ with $cw(H) \leq d$, the group $G^{(m)} \cap H$ can be constructed in time $n^{f(d)}$.

$G^{(m)} \cap H$ is called the relative m-closure of G with respect to H.

Inside the proof

A class $\mathfrak{K}$ of (abstract) groups is said to be complete if it is closed with respect to taking subgroups, quotients, and extensions.

The class of all permutation groups of degree at most n that belong to $\mathfrak{K}$ is denoted by $\mathfrak{K}_n$.
A permutation group is said to be non-basic if it is contained in a wreath product with the product action, and it is basic otherwise.

Let $m, n \in \mathbb{N}$, $m \geq 3$, and $\mathfrak{K}$ a complete class of groups. Then

1. $\mathfrak{K}_n$ is closed with respect to taking the m-closure if and only if $\mathfrak{K}_n$ contains the m-closure of every primitive basic group in $\mathfrak{K}_n$,
2. the m-closure of any group in $\mathfrak{K}_n$ can be found in time poly(n) by accessing oracles for finding the m-closure of every primitive basic group in $\mathfrak{K}_n$ and the relative m-closure of every group in $\mathfrak{K}_n$ with respect to any group in $\mathfrak{K}_n$.

2-Closures of supersolvable groups

A group G is called *supersolvable* if it has a finite normal series with cyclic factors, that is

$$G = G_0 \geq G_1 \geq \ldots \geq G_{n-1} \geq G_n = 1,$$

where $G_i \trianglelefteq G$ and G_i/G_{i-1} is cyclic for every $i = 1, \ldots, n$.

2-Closures of supersolvable groups

A group G is called *supersolvable* if it has a finite normal series with cyclic factors, that is

$$G = G_0 \geq G_1 \geq \ldots \geq G_{n-1} \geq G_n = 1,$$

where $G_i \trianglelefteq G$ and G_i/G_{i-1} is cyclic for every $i = 1, \ldots, n$.

The problem is that

Composition factors of the 2-closure of every supersolvable permutation group G are cyclic or alternating groups.

2-Closures of supersolvable groups

A group G is called *supersolvable* if it has a finite normal series with cyclic factors, that is

$$G = G_0 \geq G_1 \geq \ldots \geq G_{n-1} \geq G_n = 1,$$

where $G_i \trianglelefteq G$ and G_i/G_{i-1} is cyclic for every $i = 1, \ldots, n$.

The problem is that

Composition factors of the 2-closure of every supersolvable permutation group G are cyclic or alternating groups.

Ponomarenko–V., 2020

The 2-closure problem for a supersolvable permutation group G of degree n can be solved in time poly(n).

Key ingredients of the proof

1. Embedding of G in a large solvable group H
2. Constructing of the relative closure K of G inside H via the Babai–Lucks algorithm
3. Finding the certificates X_S (the sets of generators) of nonsolvable primitive sections S of the closure $K^{(2)}$ of K
4. Putting $X = \bigcup X_S$ and setting $G^{(2)} = \langle K, X \rangle$.

Key ingredients of the proof

1. Embedding of G in a large solvable group H
2. Constructing of the relative closure K of G inside H via the Babai–Lucks algorithm
3. Finding the certificates X_S (the sets of generators) of nonsolvable primitive sections S of the closure $K^{(2)}$ of K
4. Putting $X = \bigcup X_S$ and setting $G^{(2)} = \langle K, X \rangle$.

The same idea can be possibly applied to the general case of the m-closure problem.

Group isomorphism problem

Group ISO

For groups G and H given by their multiplicative tables, test whether $\mathrm{Iso}(G, H) = \varnothing$.

Group isomorphism problem

Group ISO

For groups G and H given by their multiplicative tables, test whether $\mathrm{Iso}(G, H) = \varnothing$.

Graph ISO $\Rightarrow$ Group ISO.

Group ISO can be solved in time $n^{O(\log n)}$.

Group isomorphism problem

Group ISO

For groups G and H given by their multiplicative tables, test whether $\mathrm{Iso}(G, H) = \varnothing$.

Graph ISO $\Rightarrow$ Group ISO.

Group ISO can be solved in time $n^{O(\log n)}$.

J. Brachter and P. Schweitzer (2020): WL-dimension for groups.

There is no an analog of Cai–Fürer–Immerman theorem for groups.

J. Brachter and P. Schweitzer (2022)

If G is indistinguishable from H by 5-dim WL-algorithm, then G and H have the same composition factors.