

Closures of finite permutation groups (Lectures 1,2)

Ilia Ponomarenko^a and Andrey Vasil'ev^b

^a St.Petersburg Department Steklov Mathematical Institute, St.Petersburg, Russia

^b Sobolev Institute of Mathematics, Novosibirsk, Russia

The G2A2-Summer School, Novosibirsk
03.08-16.08.2025

Graph Isomorphism Problem: statement

The graphs \mathfrak{X} on Ω and \mathfrak{X}' on Ω' are said to be *isomorphic* if there is a bijection $f : \Omega \rightarrow \Omega'$, the *isomorphism* from \mathfrak{X} to \mathfrak{X}' , such that

$$(*) \quad \alpha \sim \beta \text{ if and only if } \alpha^f \sim \beta^f.$$

The set of all such f is denoted by $\text{Iso}(\mathfrak{X}, \mathfrak{X}')$. When $\mathfrak{X} = \mathfrak{X}'$, the group $\text{Aut}(\mathfrak{X}) = \text{Iso}(\mathfrak{X}, \mathfrak{X})$ is called the *automorphism group* of \mathfrak{X} .

The Graph Isomorphism Problem (ISO): given two graphs \mathfrak{X} and \mathfrak{X}' , test whether $\text{Iso}(\mathfrak{X}, \mathfrak{X}') \neq \emptyset$.

To check whether a bijection $f : \Omega \rightarrow \Omega'$ belongs to the set $\text{Iso}(\mathfrak{X}, \mathfrak{X}')$, one needs to verify $|\Omega|^2$ conditions (*). Thus, ISO belongs to the class **NP**.

It is still unknown whether the isomorphism of any two graphs of order n can be tested in a polynomial-time in n .

Graph Isomorphism Problem: results

- ① The exhaustive search algorithm runs in time $2^{cn \log n}$.
- ② A "naive classification" algorithm tests isomorphism of a random graphs in time cn^2 [Babai et al, 1980].
- ③ The best (at the moment) algorithm tests isomorphism of arbitrary graphs in time $n^{(\log n)^c}$ [Babai, 2019].
- ④ Natural combinatorial algorithms tests graph isomorphism not faster than $2^{cn \log n}$ [Cai et al, 1992].
- ⑤ Isomorphism of graphs of Hadwiger number (max degree, ...) d can be tested in time $n^{(\log d)^c}$ [Grohe et al, 2020].
- ⑥ There are algorithms (Nauty and Traces among the others) that work efficient in practice [McKay–Piperno, 2014].

Graph Isomorphism Problem and permutation groups

A (computational) problem \mathfrak{P}_1 is *polynomial-time reduced* to a problem \mathfrak{P}_2 , if \mathfrak{P}_1 can be solved by a polynomial-time algorithm using as an elementary step an “oracle” giving a solution of \mathfrak{P}_2 for a given input. We say that \mathfrak{P}_1 and \mathfrak{P}_2 are *polynomially equivalent* if each of them is polynomial-time reduced to the other.

Exercise 1. The Graph Isomorphism Problem for graphs, connected graphs, regular graphs, bipartite graphs, graphs without triangles, colored graphs are pairwise polynomially equivalent.

Theorem [Mathon, 1979]. The following problems for graphs \mathfrak{X} and \mathfrak{X}' are polynomially equivalent:

- ① find a bijection in $\text{Iso}(\mathfrak{X}, \mathfrak{X}')$ or a certificate of $\text{Iso}(\mathfrak{X}, \mathfrak{X}') = \emptyset$,
- ② find a generator set of $\text{Aut}(\mathfrak{X})$,
- ③ find the orbits of $\text{Aut}(\mathfrak{X})$.

The Weisfeiler-Leman algorithm: general

A main goal is given a graph \mathfrak{X} , construct the orbits of $\text{Aut}(\mathfrak{X})$.

The idea is: for $k \in \mathbb{N}$, construct a partition of the Cartesian power Ω^k , and project it to one coordinate. This is done by the k -dim Weisfeiler-Leman algorithm (k -dim WL); see [Cai et al, 1992].

Remarks

- 1-dim WL is known as the “naive classification” of vertices;
- 2-dim WL is the classical Weisfeiler-Leman algorithm;
- the k -dim WL for large k is used in the Babai quasipolynomial algorithm [Babai, 2015].

Notation. For any point $\alpha \in \Omega$, any tuple $x = (x_1, \dots, x_k) \in \Omega^k$, and an index $i \in \{1, \dots, k\}$, we define an k -tuple

$$x_{i \leftarrow \alpha} = (x_1, \dots, x_{i-1}, \alpha, x_{i+1}, \dots, x_k),$$

The algorithm below consistently refines a coloring c_0 of Ω^k to obtain a “stable” coloring, which is no longer refined.

The Weisfeiler-Leman algorithm: description

The k -dim WL color refinement ($k \geq 2$)

Input: a coloring c_0 of Ω^k .

Output: a “stable” coloring c of Ω^k .

Step 1. Set $m = 0$.

Step 2. For each $x \in \Omega^k$, find a multiset $s(x) = \{s_\alpha(x) : \alpha \in \Omega\}$ with

$$s_\alpha(x) = (c_m(x_{1 \leftarrow \alpha}), \dots, c_m(x_{k \leftarrow \alpha})).$$

Step 3. Find a new coloring c_{m+1} of Ω^k such that

$$c_{m+1}(x) < c_{m+1}(x') \iff c_m(x) < c_m(x') \text{ or } s(x) < s(x').$$

Step 4. If $|c_m| \neq |c_{m+1}|$, then $m := m + 1$ and go to Step 2, else output $c = c_m$.

The algorithm runs in time $O(k^2 n^{2k+1} \log n)$, where $n = |\Omega|$.

The k -dim WL and graph isomorphism: graph colorings

Let $k \geq 2$, \mathfrak{X} be a graph on Ω , and $c_0 = c_0(\mathfrak{X})$ be the *initial coloring* of the k -tuples $x \in \Omega^k$: $c_0(x) = c_0(y)$ if and only if

$$x_i \sim x_j \text{ (resp., } x_i = x_j) \Leftrightarrow y_i \sim y_j \text{ (resp., } y_i = y_j), \quad 1 \leq i, j \leq k,$$

where \sim is the adjacency relation of \mathfrak{X} .

The initial coloring is *invariant*:

$$f \in \text{Iso}(\mathfrak{X}, \mathfrak{X}') \Rightarrow c_0(x) = c'_0(x') \text{ for all } x,$$

where $c'_0 = c_0(\mathfrak{X}')$ and $x' = (x_1^f, \dots, x_k^f)$.

Let $c = c(\mathfrak{X})$ be the (invariant!) coloring constructed by the k -dim WL applied to $c_0 = c_0(\mathfrak{X})$. If $\text{Iso}(\mathfrak{X}, \mathfrak{X}') \neq \emptyset$ and $c' = c(\mathfrak{X}')$, then

$$\text{Im}(c) = \text{Im}(c') \text{ and } |c^{-1}(i)| = |c'^{-1}(i)| \text{ for any color } i \in \text{Im}(c).$$

The k -dim WL and graph isomorphism: algorithm

Testing isomorphism of \mathfrak{X} and \mathfrak{X}' by the k -dim WL

Step 1. Construct $c_0 = c_0(\mathfrak{X})$ and $c'_0 = c_0(\mathfrak{X}')$.

Step 2. Construct $c = c(\mathfrak{X})$ and $c' = c(\mathfrak{X}')$ by the k -dim WL.

Step 3. Declare $\text{Iso}(\mathfrak{X}, \mathfrak{X}') \neq \emptyset$ iff conditions (7) are satisfied.

In many cases, the above procedure correctly tests the isomorphism of \mathfrak{X} and \mathfrak{X}' ; for example, if the graph \mathfrak{X} is planar and $k = 3$ (see, [Kiefer et al, 2017]), or $k \geq n$.

However, there is a constant $\varepsilon > 0$ and infinitely many pairs of graphs \mathfrak{X} and \mathfrak{X}' such that the above procedure is not correct for all $k \leq \varepsilon n$ [Cai et al, 1992].

The k -closure problem: preparation

Let $k \geq 1$ be an integer and $G \leq \text{Sym}(\Omega)$. It has a natural action on the set Ω^k of all k -tuples of Ω , namely:

$$(x_1, \dots, x_k)^g = (x_1^g, \dots, x_k^g), \quad g \in G.$$

We extend the action of G to all k -ary relations $X \subseteq \Omega^k$ by setting $X^g = \{x^g : x \in X\}$ for all $g \in G$. The relation X is *invariant* with respect to G , or *G -invariant*, if $X^g = X$ for all $g \in G$.

The set of all G -invariant k -ary relations is denoted by $\text{Rel}_k(G)$. Clearly, it is closed with respect to the union, intersection, etc.

Exercise 2. Let \mathfrak{X} be a graph and $\text{WL}_k(\mathfrak{X})$ the partition of Ω^k into the color classes of the coloring $c(\mathfrak{X})$. Then

- ① every class of $\text{WL}_k(\mathfrak{X})$ is an $\text{Aut}(\mathfrak{X})$ -invariant relation;
- ② the group $\text{Aut}(\text{WL}_k(\mathfrak{X}))$ of all $g \in \text{Sym}(\Omega)$ such that $X^g = X$ for all $X \in \text{WL}_k(\mathfrak{X})$ coincides with the group $\text{Aut}(\mathfrak{X})$.

The k -closure problem: statement

A set $x^G = \{x^g : g \in G\}$ with $x \in \Omega^k$ is called a k -orbit of G , the set of all of them denote by $\text{Orb}_k(G)$.

Clearly, $\text{Orb}_k(G) \subseteq \text{Rel}_k(G)$, each G -invariant relation is a union of k -orbits, and the k -orbits form a partition of Ω^k .

The partitions $\text{WL}_k(\mathfrak{X})$ and $\text{Orb}_k(G)$ are examples of k -ary coherent configurations in the sense of [Babai, 2015].

The k -closure $G^{(k)} = \text{Aut}(\text{Orb}_k(G))$ of the group G is the group of all $g \in \text{Sym}(\Omega)$ such that $X^g = X$ for all $X \in \text{Orb}_k(G)$.

If $k = 2$ and $\text{WL}_2(\mathfrak{X}) = \text{Orb}_2(G)$ for some $G \leq \text{Sym}(\Omega)$, then $\text{Aut}(\mathfrak{X}) = G^{(k)}$. This motivates the computation problem.

The k -closure problem: given a permutation group G , find the k -closure $G^{(k)}$ of G .

The Babai–Luks algorithm: the relative k -closure

The problem below was implicit in solving isomorphism problems for vertex-colored graphs with small color classes [Babai, 1979], graphs of bounded degree [Luks, 1982], tournaments [Baba–Luks, 1983], arbitrary graphs in quasipolynomial time [Babai, 2019].

The relative k -closure problem: given groups $H, G \leq \text{Sym}(\Omega)$, find the intersection $G^{(k)} \cap H$.

For $H = \text{Sym}(\Omega)$, it is just the k -closure problem.

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

Theorem [Babai–Luks, 1983]

For a fixed k , there exists a function $f = f_k(x)$ such that the relative closure of G with respect to H can be found in time $n^{f(d)}$, where $n = |\Omega|$ and $d = \text{cw}(H)$.

The Babai–Luks algorithm: reductions

1. We may assume that $k = 1$: indeed, replace Ω by Ω^k , and G and H by the permutation groups induced by the componentwise actions of them on Ω^k . Thus we need to find the subgroup

$$G^{(1)} \cap H = \{h \in H : X^h = X \text{ for all } X \in \text{Orb}_1(G)\}$$

of the group H that leaves any orbit of G fixed.

2. To use recursion, given a set $\Delta \subseteq \Omega$ and a coset $Ug \leq \text{Sym}(\Delta)$ such that $\Delta^U = \Delta$, put

$$C_\Delta(Ug) = \{h \in Ug : (X \cap \Delta)^h = X \cap \Delta \text{ for all } X \in \text{Orb}(G)\},$$

where $\text{Orb}(G) = \text{Orb}_1(G)$. It is assumed that Δ is U -invariant.

3. Our goal is to present algorithm constructing the coset $C_\Delta(Ug)$ for any given Δ , U , and g . This would solve our problem, because

$$G^{(1)} \cap H = C_\Omega(H).$$

The Babai–Luks algorithm: description

Step 1. If U is primitive, then find $C_{\Delta}(Ug)$ by the exhaustive search in the coset Ug .

Step 2. If U is intransitive and $\Gamma \in \text{Orb}(U)$, then recursively find $C := C_{\Gamma}(Ug)$ and output $C_{\Delta \setminus \Gamma}(C)$.

Step 3. Find an imprimitivity system e for U , such that $\bar{U} := U^{\bar{\Delta}}$ is primitive, where $\bar{\Delta} = \Delta/e$. Put $\bar{g} := g^{\bar{\Delta}}$.

Step 3.1. For each $\bar{h} \in \bar{U}\bar{g}$, choose $h \in Ug$ such that $h^{\bar{\Delta}} = \bar{h}$.

Step 3.2. Let $U_0 = \{u_0 \in U : \Gamma^{u_0} = \Gamma \text{ for all } \Gamma \in \bar{\Delta}\}$.

Step 3.3. For each $\bar{h} \in \bar{U}$, find recursively $C_{\bar{h}} = C_{\Delta}(U_0h)$.

Step 3.4. Output the union of $C_{\bar{h}}$, $\bar{h} \in \bar{U}$.

The Babai–Luks algorithm: analysis

Correctness. Induction on the number of recursive calls. Take into account that at Step 3, the group U is a disjoint union of the cosets $U_0 h$, where \bar{h} runs over \bar{U} .

Running time. The proof is based on the following statement.

Theorem [Babai–Cameron–Palfy, 1982]

The order of a primitive group of degree n and composition width d is at most $n^{f_0(d)}$ for some function $f_0 = f_0(x)$.

It follows that Step 1 runs in time $m^{f_0(d)}$, whereas at Step 3, we have $|\bar{U}| \leq m^{f_0(d)}$, where $m = |\Delta|$ and $\bar{m} = |\bar{\Delta}|$.

The recursion divides the problem into

- two subproblems of sizes $|\Gamma|$ and $|\Delta \setminus \Gamma|$ (Step 2).
- $\bar{m}^{f_0(d)} \cdot |e|$ subproblems of size $\frac{m}{|e|}$ (Step 3.3).

Thus, by induction, the running time is $m^{f(d)}$ for a suitable f .

A method of invariant relations

In 1969, Helmut Wielandt wrote in [Wielandt, 1969b]:

There are three major tools that have been developed for the purpose of studying the actions of a group G on a set Ω . The first of these is the well known theory of linear representations over a field... The second method is due to Schur, and dates from 1933: this is the method of Schur rings... There is one more method, of rather recent origin. This is the study of those relations between points of Ω that remain invariant under the action of G . By studying these invariant relations, we hope to get information on the action of G .

In other words, what can be said about the group G from studying the sets $\text{Rel}_k(G)$ and $\text{Orb}_k(G)$ for small (or specific, or all k)?

k -equivalence of permutation groups

Two permutation groups $G, H \leq \text{Sym}(\Omega)$ are called k -equivalent, $G \approx_k H$, if they have the same k -orbits, i.e. $\text{Orb}_k(G) = \text{Orb}_k(H)$.

Obviously,

$$G \approx_k H \iff \text{Rel}_k(G) = \text{Rel}_k(H). \quad (1)$$

One can see that if $G \approx_k H$ and $k \geq n = |\Omega|$, then $G = H$. On the other hand, all k -transitive groups on Ω are k -equivalent (in particular, any two transitive groups are 1-equivalent). Moreover, there is a number of 2-equivalent groups which are not equal.

Lemma

Let $k \geq 2$ and $G \approx_k H$. Then

- i $G \approx_{k-1} H$,
- ii G and H have the same orbits and systems of imprimitivity,
- iii $G_\alpha \approx_{k-1} H_\alpha$ for all $\alpha \in \Omega$.

The k -closure

Let $k \geq 1$ and $G \leq \text{Sym}(\Omega)$. The class of all groups k -equivalent to G contains the largest element, namely, $G^{(k)} := \text{Aut}(\text{Orb}_k(G))$; it is called the k -closure of G .

We have

$$G \approx_k G^{(k)} \text{ and } G \approx_k H \Rightarrow G^{(k)} = H^{(k)}. \quad (2)$$

Note that taking the k -closure is indeed a closure operator, namely,

$$G \leq G^{(k)}, \quad G^{(k)} = (G^{(k)})^{(k)}, \quad G \leq H \Rightarrow G^{(k)} \leq H^{(k)}, \quad (3)$$

Using these statements, one can easily verify that

$$G^{(1)} \geq G^{(2)} \geq \dots \geq G^{(k)} = G^{(k+1)} = \dots = G \quad (4)$$

for some $k < |\Omega|$. In this sense, the k -closure can be considered as a natural approximation of G .

Exercise 3. For any G : $G^{(1)} = \text{Sym}(\Omega_1) \times \dots \times \text{Sym}(\Omega_m)$, where $\Omega_1, \dots, \Omega_m$ are the orbits of G .

Closure argument and closed groups

Lemma (The closure argument, [Wielandt, 1969a])

Let $G \leq \text{Sym}(\Omega)$, $f \in \text{Sym}(\Omega)$, and $k \in \mathbb{N}$. Then $f \in G^{(k)}$ if and only if for every $x \in \Omega^k$ there is $g \in G$ such that $x^f = x^g$.

Proof. Set $\bar{G} = G^{(k)}$. If $f \in \bar{G}$ and $x \in \Omega^k$, then $x^{\bar{G}} = x^G$. Hence, $x^f \in x^G$. Conversely, assume that for every $x \in \Omega^k$ there is $g \in G$ such that $x^f = x^g$. Then $X^f = X$ for all $X \in \text{Orb}_k(G)$. Therefore, $f \in \text{Aut}(\text{Orb}_k(G)) = \bar{G}$.

A permutation group G is said to be *k-closed* if $G = G^{(k)}$. Clearly, the 1-closed groups are exactly the direct products of symmetric groups and the 2-closed groups are the automorphism groups of arc-colored graphs. In general, G is *k-closed* iff $G = \text{Aut}(\text{Rel}_k(G))$.

Base of permutation group

A set $\Delta \subseteq \Omega$ is called the *base* of a permutation group $G \leq \text{Sym}(\Omega)$ if the pointwise stabilizer of Δ in G is trivial.

Any subset of Ω that contains a base of G , is also the base of G .

The minimum cardinality of a base is called the *base number* of G and is denoted by $b(G)$.

Clearly, $0 \leq b(G) \leq n - 1$ and the bounds attain for the identity and symmetric group, respectively.

Let $X \in \text{Orb}_k(G)$, $x = (x_1, \dots, x_k) \in X$, and $\Delta = \{x_1, \dots, x_k\}$ is a base of G . Then the action of G on X is regular and faithful: if $x^g = x$ for some $g \in G$, then $g \in G_{x_1, \dots, x_k} = 1$. Thus,

$$|G| = |X| \leq n^{b(G)},$$

and the equality attains for any regular group.

The Wielandt criterion for the k -closedness

Theorem [Wielandt, 1969a] A permutation group G is $(b+1)$ -closed for any $b \geq b(G)$.

Proof. Let $k = b + 1$. To verify that $G^{(k)} \leq G$, take $h \in G^{(k)}$. Let $\{x_1, \dots, x_b\}$ be a base of G . By the closure argument,

$$(x_1, \dots, x_b)^h = (x_1, \dots, x_b)^g. \quad (5)$$

for some $g \in G$, and given $\alpha \in \Omega$,

$$(x_1, \dots, x_b, \alpha)^h = (x_1, \dots, x_b, \alpha)^{g_\alpha} \quad (6)$$

for some $g_\alpha \in G$. From (5) and (6) it follows that

$$(x_1, \dots, x_b)^g = (x_1, \dots, x_b)^h = (x_1, \dots, x_b)^{g_\alpha}.$$

So $gg_\alpha^{-1} \in G_{x_1, \dots, x_b} = 1$ (since $\{x_1, \dots, x_b\}$ is a base of G). Hence $g = g_\alpha$, and by (6), $\alpha^h = \alpha^g$ for all $\alpha \in \Omega$. Thus, $h = g \in G$.

Some corollaries of the Wielandt criterion

Corollary 1. Any regular group is 2-closed.

Proof. If G is a regular group of degree > 1 , then $b(G) = 1$ and we are done by the Wielandt criterion.


Corollary 2. Let G and H be permutation groups of the same degree n and $G^{(n)} = H^{(n)}$. Then $G = H$.

Proof. Clearly, $b(G) \leq n - 1$ and $b(H) \leq n - 1$. From the Wielandt criterion, it follows that G and H are n -closed. Thus $G = G^{(n)} = H^{(n)} = H$.


Exercise 4. Prove that

- ① the automorphism group of any (finite) group is 3-closed,
- ② if G is abelian, then $b(G) \leq |\text{Orb}(G)|$ and the bound is sharp.


Bibliography (1)




L. Babai, *Monte-Carlo algorithms in graph isomorphism testing*, Tech. Report Tech. Rep. 79–10, Université de Montréal, 1979, [Lhttp://people.cs.uchicago.edu/~laci/lasvegas79.pdf](http://people.cs.uchicago.edu/~laci/lasvegas79.pdf).




L. Babai, P. Erdős, and S. Selkow, *Random graph isomorphism*, SIAM J. Comput., **9** (1980), no. 3, 628–635.




L. Babai, *Graph isomorphism in quasipolynomial time*, 2016, arXiv:1512.03547 [cs.DS], pp. 1–89.




L. Babai, *Group, Graphs, Algorithms: the Graph Isomorphism Problem*, Proceedings of the International Congress of Mathematicians (ICM 2018), vol. 3, WORLD SCIENTIFIC, 2019, pp. 3319–3336.




L. Babai, P. J. Cameron, and P. P. Pálffy, *On the orders of primitive groups with restricted nonabelian composition factors*, J. Algebra **79** (1982), no. 1, 161–168.




László Babai and Eugene M. Luks, *Canonical labeling of graphs*, Proc. 15th ACM STOC, 1983, pp. 171–183.




J. Y. Cai, M. Fürer, and N. Immerman, *An optimal lower bound on the number of variables for graph identification*, Combinatorica **12** (1992), 389–410.



M. Grohe, D. Neuen, and D. Wiebking, *Isomorphism testing for graphs excluding small minors* FOCS, 625–637 (2920); doi:10.1109/FOCS46700.2020.00064.



E.M.Luks, *Isomorphism of graphs of bounded valence can be tested in polynomial time*, J. Comp. Sys. Sci. **25** (1982), 42–65.



S. Kiefer, I. Ponomarenko, and P. Schweitzer, *The Weisfeiler–Leman Dimension of Planar Graphs Is at Most 3*, Journal of the ACM **66** (2019), no. 6, 1–31.

Bibliography (2)



R. Mathon, *A note on the graph isomorphism counting problem*, Inform. Process. Lett. **8** (1979), 131–132.



B. D. McKay and A. Piperno, *Practical graph isomorphism, II*, J. Symbolic Comput. **60** (2014), 94–112.



H. Wielandt, *Permutation groups through invariant relations and invariant functions*, The Ohio State University (1969).



H. Wielandt, *Permutation representations*, Illinois J. Math. **13** (1969), 91–94.