Closures of finite permutation groups (Lectures 7,8)

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

The plan of the lecture

At present the k-closure problem in the class of all solvable groups is open. We will talk about polynomial-time algorithms for

1. reduction to basic primitive groups,
2. odd order groups and all k,
3. all solvable groups and $k \geq 3$,
4. all supersolvable groups and $k = 2$ (briefly).

Recall that a permutation group is *nonbasic* if it is contained in a wreath product with the product action; it is *basic* otherwise.

The embedding problem: statement

The signs $\times, \wr$, and $\uparrow$ denote the operations of direct and wreath product in imprimitive action and primitive action, respectively.

$\star$-**embedding problem**: given $G \leq \mathrm{Sym}(\Omega)$ and $\star \in \{\times, \wr, \uparrow\}$ test whether there exists an embedding of $G \to K \star L$ for some sections $K \leq \mathrm{Sym}(\Delta)$ and $L \leq \mathrm{Sym}(\Gamma)$ of G, such that $|\Delta| < |\Omega|$ and $|\Gamma| < |\Omega|$, and if so, then to find the embedding explicitly.

Under the embedding $G \to K \star L$, a bijection f from Ω to the underlying set of the permutation group $K \star L$, such that

$$f^{-1}Gf \leq K \star L.$$

Exercise 1. Solve the $\star$-embedding problem for intransitive G and $\star = \times$, and for imprimitive G and $\star = \wr$, see also [Seress, 2002].

The embedding problem: theorem

Theorem [Pon–Vasil'ev, 2024] Let $G \leq \mathrm{Sym}(n)$, $\star \in \{\times, \wr, \uparrow\}$. Assume that G is imprimitive if $\star = \wr$, and primitive if $\star = \uparrow$. Then the $\star$-embedding problem for G can be solved in time $\mathrm{poly}(n)$.

Sketch of the proof (for $\star = \uparrow$).

1. Find $S = \mathrm{Soc}(G)$ of G and test whether or not S is abelian.
2. If S is abelian, then $S = C_p \times \cdots \times C_p$ (d times) and can be identified with a d-dim linear space over $\mathbb{F}_p$ ($n = p^d$).
3. Find a minimal subspace $\Delta \subseteq \Omega$ so that Ω is the direct sum of the subspaces belonging to the set $\Gamma = \{\Delta^g : \; g \in G\}$.
4. Set $L = G^\Gamma$ and K to be the restriction of the setwise stabilizer of Δ in G to Δ.
5. Now G embeds to $K \uparrow L$ or $\Delta = \Omega$.
6. If S is not abelian, then the proof is more complicated.

Primitive odd order groups

Let G be a primitive odd order group. By the Suprunenko theory, we may assume that $G \leq \mathrm{AGL}_d(p)$ for some $d \geq 1$ and prime p.

Theorem [Evdok-Pon, 2001] Suppose that the group G is basic. Then $G = G^{(2)}$ or $G \leq \mathrm{A\Gamma L}_1(p^d) \leq \mathrm{AGL}_d(p)$.

Proof. Let $\alpha \in \Omega$ and $\bar{G} = G^{(2)}$.

1. Assume that G is not embedded to $\mathrm{A\Gamma L}_1(p^d)$.
2. By [Seress, 1996], G_α and $\bar{G}_\alpha$ have a faithful regular orbit Δ.
3. Hence $|G_\alpha| = |\Delta| = |\bar{G}_\alpha|$, and so $|G| = |\bar{G}|$.
4. Since $G \leq \bar{G}$, we conclude that $G = \bar{G} = G^{(2)}$.

Corollary. Given G as in the theorem, one can efficiently find an odd order group H such that $G^{(2)} \leq H$.

Proof. If $G \leq \mathrm{A\Gamma L}_1(p^d)$, then H is the Hall $2'$-subgroup of $\mathrm{A\Gamma L}_1(p^d)$; otherwise, $H := G = G^{(2)}$.

The k-closure problem for odd order groups

Theorem [Evdok-Pon, 2001]. Let $k \geq 1$. Then given an odd order group $G \leq \mathrm{Sym}(n)$, one can find $\bar{G} = G^{(k)}$ in time $\mathrm{poly}(n)$.

Let $k \geq 2$. By the Babai-Luks theorem, it suffices to find an odd order group $\bar{G} \leq H \leq \mathrm{Sym}(n)$, and output $\bar{G} := \bar{G} \cap H$.

Algorithm (finding the group H).

1. If G is basic primitive, then output H as in the corollary.
2. By the $\star$-embedding theorem, find groups K and L, and an embedding $G \leq K * L$, where $* \in \{\times, \wr, \uparrow\}$.
3. Recursively find $\bar{K} = K^{(k)}$ and $\bar{L} = L^{(k)}$.
4. Output $H = \bar{K} * \bar{L}$.

Correctness: $G^{(k)} \leq (K * L)^{(k)} \leq K^{(k)} * L^{(k)}$.

Exercise 2. Verify the time bound.

General reduction: statement

Given a class $\mathfrak{K}$ of (abstract) groups, denote by $\mathfrak{K}_n$ the class of all permutation groups of degree at most n that belong to $\mathfrak{K}$.

Theorem [Pon–Vasil'ev, 2024] Let $k, n \in \mathbb{N}$, $k \geq 3$, and $\mathfrak{K}$ a complete class of groups. Then

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

Remark. If $\mathfrak{K}$ is the class of solvable groups, then statement (1) does not true for $k < 3$ (hint: the 2-closure of a 2-transitive solvable group of degree ≥ 5 is not solvable).

General reduction: algorithm (1)

Step 1. If $G \leq \mathrm{Sym}(\Omega)$ is intransitive, imprimitive, or primitive, we set $\star = \times$, $\wr$, or $\uparrow$, respectively. Test in time poly(n) whether there exists an embedding of G to $K \star L$ for some sections

$$K \leq \mathrm{Sym}(\Delta) \quad \text{and } L \leq \mathrm{Sym}(\Gamma)$$

of G, such that the numbers $n_K = |\Delta|$ and $n_L = |\Gamma|$ are less than $n = |\Omega|$, and if so, then find the embedding explicitly.

Step 2. If there is no such embedding, then G is primitive basic, belongs to $\mathfrak{K}_n$, and the k-closure of G can be found for the cost of one call of the corresponding oracle.

Now G is not primitive basic and we have a bijection f from Ω to the underlying set of $K \star L$, such $f^{-1}Gf \leq K \star L$. Since $f^{-1}G^{(k)}f = (f^{-1}Gf)^{(k)}$, we may assume that

$$G \leq K \star L.$$

General reduction: algorithm (2)

Step 3. Since $K \in \mathfrak{K}_{n_K}$ and $L \in \mathfrak{K}_{n_L}$ (the class $\mathfrak{K}$ is complete), we apply the algorithm recursively to K and L to find the groups $K^{(k)}$ and $L^{(k)}$ in time poly(n_K) and poly(n_L), respectively, and then the group $K^{(k)} \star L^{(k)}$ in time poly(n).

Step 4. By induction, $K^{(k)} \in \mathfrak{K}_{n_K}$ and $L^{(k)} \in \mathfrak{K}_{n_L}$, whence $K^{(k)} \star L^{(k)} \in \mathfrak{K}_n$. By theorems about the closures, we have

$$G^{(k)} \leq (K \star L)^{(k)} \leq K^{(k)} \star L^{(k)}.$$

Accessing (one time) the oracle for finding the relative k-closure of G with respect to $K^{(k)} \star L^{(k)}$, we find the group $G^{(k)}$.

General reduction: running time

Let us estimate the number of the oracles calls. Each recursive call divides the problem for a group of degree n to the same problem for a group K of degree n_K and for a group L of degree n_L. Moreover,

$$n = \begin{cases} n_K + n_L & \text{if } \star = \times, \\ n_K \cdot n_L & \text{if } \star = \wr, \\ {n_K}^{n_L} & \text{if } \star = \uparrow. \end{cases}$$

Thus the total number of recursive calls and hence the number of accessing oracles is at most n.

Exercise 3. Prove that if statement (1) of the theorem holds also for the class $\mathfrak{K}$ and $k = 2$, then statement (2) holds for $k = 2$ too.

The k-closure problem for solvable groups ($k \geq 3$)

Theorem [Pon–Vasil'ev, 2024] Given an integer $k \geq 3$, the k-closure of a solvable permutation group of degree n can be found in time $n^{O(k)}$.

Proof

1. The class $\mathfrak{K}$ of all solvable groups is complete.
2. The relative k-closure of any $G \in \mathfrak{K}_n$ wrt any $H \in \mathfrak{K}_n$ can be found in time poly(n) by the Babai-Luks algorithm.
3. By the reduction theorem, it suffices to find $G^{(3)}$ in time poly(n) for any primitive basic group $G \in \mathfrak{K}_n$.
4. If $b(G) = 2$, then $G = G^{(3)}$ by the Wielandt theorem.
5. If $b(G) \geq 3$ and $n > n_0$ for some large enough $n_0 \in \mathbb{N}$, then $G \leq \mathrm{A\Gamma L}_1(q)$ and $G = G^{(3)}$ by [Yang et al, 2020].
6. Find $G^{(3)}$ by inspecting all permutations of Sym(n_0).

The 2-closure of supersolvable groups (1)

Recall that a finite group is *supersolvable* if it contains a normal series with cyclic factors. [Example: the group $\mathrm{AGL}_1(q)$ is supersolvable iff q is a prime.]

The class of supersolvable groups is not invariant with respect to taking the 2-closure: if p is a prime, then $\mathrm{AGL}_1(p)^{(2)} = \mathrm{Sym}(p)$.

Theorem [Ponom–Vasil'ev, 2020] Given a supersolvable group $G \leq \mathrm{Sym}(n)$, the group $G^{(2)}$ can be found in time $\mathrm{poly}(n)$.

The main idea of the algorithm is a consequence of the following fact also proved in [Ponom–Vasil'ev, 2020]: *every composition factor of the* 2*-closure of a supersolvable group is either a cyclic group or an alternating group of prime degree*.

The 2-closure of supersolvable groups (2)

A sketch of the algorithm finding the 2-closure of a (transitive) supersolvable group $G \leq \mathrm{Sym}(n)$.

1. Find an embedding of G into the iterated wreath product of $s \geq 1$ groups $G_i \leq \mathrm{AGL}_1(p_i)$ with prime p_i:

$$\mathrm{Wr}(G_1, \ldots, G_s) = G_1 \wr G_2 \wr \ldots \wr G_s \leq \mathrm{Sym}(n),$$

2. The group $\bar{G} = G^{(2)}$ has sections $G_i \leq \bar{G}_i \leq \mathrm{Sym}(p_i)$ such that $\mathrm{Wr}(G_1, \ldots, G_s) \leq \bar{G} \leq \mathrm{Wr}(\bar{G}_1, \ldots, \bar{G}_s)$.
3. For each $i = 1, \ldots, s$, put

$$(H_i, \bar{H}_i) = \begin{cases} (C_{p_i}, \mathrm{Wr}(\ldots, 1, \bar{G}_i, 1, \ldots)) & \text{if } \bar{G}_i = \mathrm{Sym}(p_i), \\ (G_i, 1) & \text{otherwise.} \end{cases}$$

4. Construct the relative 2-closure $\bar{H}$ of the group G with respect to $\mathrm{Wr}(H_1, \ldots, H_s)$ and output $\bar{G} = \langle \bar{H}, \bar{H}_1, \ldots, \bar{H}_s \rangle$.

What's next?

Recall that the class $\mathfrak{K}$ of the $\mathrm{Alt}(d)$-free groups with $d \geq 25$ is closed with respect to the k-closure for $k \geq 4$, see [Ponom et al, 2025]. *Whether the k-closure problem can be solved for a group in $\mathfrak{K}$ in polynomial time?* [an ongoing project with A. V. Vasil'ev].

Ambitious problem: find a polynomial-time algorithm that constructs the 100-closure of an arbitrary permutation group.

The 2-closure problem for solvable group. As an example in [Skresanov, 2019] shows there are solvable permutation groups G such that $G^{(2)}$ has a nonabelian composition factor which is isomorphic to no alterntaing group. This is an obstacle for the 2-closure problem.

Question. Let $G \leq \mathrm{Sym}(n)$ be a solvable primitive basic group. Is it true that if n is large enough, then any nonabelian composition factor of $G^{(2)}$ is an alternating group?

Schurian color graphs: definition and problems

For every undirected graph $\mathfrak{X}$, the group $\mathrm{Aut}(\mathfrak{X})$ is 2-closed. The converse is not true: $C_2 \times C_2 \leq \mathrm{Sym}(4)$ equals $\mathrm{Aut}(\mathfrak{X})$ for no $\mathfrak{X}$. However, every 2-closed group is $\mathrm{Aut}(\mathfrak{X})$ for some arc colored $\mathfrak{X}$.

An arc colored graph $\mathfrak{X}$ can be thought as a partition $\mathcal{X}$ of $\Omega \times \Omega$: each color class of arcs of $\mathfrak{X}$ is a class of $\mathcal{X}$. The colored graph $\mathcal{X}$ is *schurian* if $\mathcal{X} = \mathrm{Orb}_2(G)$ for some $G \leq \mathrm{Sym}(\Omega)$.

Main open problems

1. *Recognition*: whether a given arc colored graph is schurian?
2. *Isomorphism*: whether two schurian graphs are isomorphic?
3. *Automorphism*: given a schurian graph $\mathfrak{X}$, find $\mathrm{Aut}(\mathfrak{X})$.

The recognition problem (with a certain certificate at output) is polynomially equivalent to the graph isomorphism problem; the automorphism problem is the 2-closure problem.

Schurian color graphs: some results

For many "natural combinatorial" classes of graphs, solving the isomorphism problem implies solving the *recognition, isomorphism, automorphism* problems for the corresponding class of schurian color graphs. Examples: graphs with bounded Hadwiger number (max degree, max multiplicity of spectra, etc.)

All the problems (*recognition, isomorphism, automorphism*) are solved in polynomial time for schurian color graphs coming from:

1. the odd order groups [Ponom, 2012],
2. the groups having regular cyclic subgroup [Evdok-Ponom, 2004], [Ponom, 2006].

The *isomorphism* and *automorphism* problems are solved in polynomial time for 3/2-transitive groups in [Vasil'ev–Churikov, 2019]; the *recognition* problem is still open.

Schurian color graphs: the rank 3 case

The *rank* of a schurian color graph is the number of color classes. When it equals 3 (the first interesting case), we come to the rank 3 graphs. Example: the Paley graphs and tournaments.

By [Skresanov, 2021], the automorphism groups of the rank 3 schurian color graphs are known. It seems that the *isomorphism* and *automorphism* problems inside this class can be solved.

By the Skresanov result *isomorphism* problem in the class of rank 3 schurian color graphs reduces to the *recognition* problem for this class, that is still open.

It seems that the *recognition* problem in the class of rank 3 schurian color graphs can be solved by the k-dim Weisfeiler-Leman algorithm for k bounded from above by an absolute constant.

Some problems relating with the k-closure problem

Problem 1. Given group $G, H \leq \mathrm{Sym}(n)$ and $k \geq 1$, test whether G and H are k-equivalent.

Problem 2. Given a group $G \leq \mathrm{Sym}(n)$ and $k \geq 1$, test whether G is k-closed.

The obvious algorithm solves Problems 1 and 2 in time $n^{O(k)}$ and the real problem is to find an algorithm running in time $\mathrm{poly}(n, k)$.

Problem 3. Given a group $G \leq \mathrm{Sym}(n)$, find the smallest $k \geq 1$ such that G is k-closed.

It is not quit clear how to approach Problem 3 even if the group G is abelian (and hence each transitive constituent of G is regular).

Exercise 4. Prove that all problems 1–3 can be solved in time $\mathrm{poly}(n)$ in the class of all abelian groups G with $b(G) \leq \mathit{const}$.

Linear codes and closures of abelian groups

A linear code of length n is a linear subspace C of an n-dim space Ω over $\mathbb{F}_q$. The elements $\alpha \in C$ correspond to the permutations

$$f_v : (x_1, \ldots, x_n) \mapsto (x_1 + \alpha_1, \ldots, x_n + \alpha_n),\ (x_1, \ldots, x_n) \in V.$$

C becomes a group $G_C \leq \mathrm{Sym}(\Omega)$ with n orbits each of size q.

Question 1. What does it mean in code theoretical terms that the group G_C associate with a code C is k-closed for some k?

Question 2. Is there any relationship between the equivalence of codes C and D of the same length and the k-equivalence of the permutation groups G_C and G_D associated with C and D?

Even the case of prime $q = p$ is interesting (in this case G_C is an elementary abelian p-group with n orbits of length p).

Bibliography (1)

S. Evdokimov and I. Ponomarenko, *Two-closure of odd permutation group in polynomial time*, Discrete Math. **235** (2001), no. 1-3, 221–232.

S. Evdokimov and I. Ponomarenko, *Recognizing and isomorphism testing circulant graphs in polynomial time*, St. Petersburg Math. J. **15** (2004), no. 6, 813–835.

I.Ponomarenko, *Determination of the automorphism group of a circulant association scheme in polynomial time*, J. Math. Sci., New York **136** (2006), no. 3, 3972–3979.

I. Ponomarenko, S. V. Skresanov, and A. V. Vasil'ev, *Closures of permutation groups with restricted nonabelian composition factors*, Bulletin of Mathematical Sciences (2025), 2550012.

I. Ponomarenko and A. Vasil'ev, *Two-closure of supersolvable permutation group in polynomial time*, Computational Complexity **29** (2020), no. 5.

I. Ponomarenko and A. V. Vasil'ev, *On computing the closures of solvable permutation groups*, Internat. J. Algebra Comput. **34** (2024), no. 1, 137–145.

I. N. Ponomarenko, *Bases of Schurian antisymmetric coherent configurations and isomorphism test for Schurian tournaments*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **402** (2012), no. Kombinatorika i Teoriya Grafov. IV, 108–147.

Á. Seress, *The minimal base size of primitive solvable permutation groups*, J. London Math. Soc. **53** (1996), 243–255.

Á. Seress,*Permutation group algorithms*, Cambridge Univ. Press, 2002.

Bibliography (2)

S. V. Skresanov, *Counterexample to two conjectures in the Kourovka notebook*, Algebra Logika **58** (2019), no. 3, 370–375.

S. V. Skresanov, *On 2-closures of rank 3 groups*, Ars Math. Contemp. **21** (2021), no. 1, Paper No. 8, 20.

A. V. Vasil'ev and D. V. Churikov, *2-closures of $\frac{3}{2}$-transitive groups in polynomial time*, Sibirsk. Mat. Zh. **60** (2019), no. 2, 360–375.

Y. Yang, Al. Vasil'ev, and E. Vdovin, *Regular orbits of finite primitive solvable groups, III*, J. Algebra, **590** (2020) 1–13.