MSC 20E28, 20B40, 05E18

Subgroups of minimal index in polynomial time

S.V. Skresanov*

Abstract

Let G be a finite group and let H be a proper subgroup of G of minimal index. By applying an old result of Y. Berkovich, we provide a polynomial algorithm for computing $|G : H|$ for a permutation group G. Moreover, we find H explicitly if G is given by a Cayley table. As a corollary, we get an algorithm for testing whether a finite permutation group acts on a tree or not.

Keywords: subgroup of minimal index, minimal permutation representation, group representability problem, group representability on trees, permutation group algorithms.

1 Introduction

In [1] S. Dutta and P.P. Kurur introduced the following:

Group representability problem. *Given a group G and a graph Γ decide whether there exists a nontrivial homomorphism from G to the automorphism group of Γ.*

By [1, Theorem 3], the graph isomorphism problem reduces to the abelian group representability problem, so the latter inherits the notorious difficulty of the former.

As an attack from a different angle, one can consider the problem of group representability on trees. In [1] authors speculate that there might be no polynomial algorithm even for such a restriction. Nevertheless, in [1, Theorems 6 and 8] they provide a polynomial reduction of that problem to the

Permutation representability problem. *Given a group G and a positive integer n, decide whether there exists a nontrivial homomorphism from G into the symmetric group Sym_n.*

Denote by $\kappa(G)$ the degree of a minimal (not necessarily faithful) nontrivial permutation representation of G. Since such permutation representations are always transitive, we see that $\kappa(G) = \min\{|G : H| \mid H < G\}$. Notice that permutation representability problem reduces to the task of computing $\kappa(G)$,

*The work is supported by Russian Science Foundation (project 14-21-00065)

since for $n \geq \kappa(G)$ there always exists a nontrivial homomorphism from G into Sym_n.

Now, let $\mu(G)$ be the degree of a minimal faithful permutation representation of G. Obviously $\kappa(G) \leq \mu(G)$ and the equality should not hold in general. The following not widely known theorem of Berkovich tells us exactly when it holds.

***Theorem* 1** ([2, Theorem 1])**.** *Let G be a finite group. G is simple if and only if $\kappa(G) = \mu(G)$.*

As a consequence, if H is a proper subgroup of minimal index in G, then $G/core_G(H)$ is a simple group, where $core_G(H) = \bigcap_{g \in G} H^g$. This observation allows one to search for subgroups of minimal index only in simple quotients of G. We have the following result.

***Theorem* 2.** *Let G be a finite permutation group given by generators. Then $\kappa(G)$ can be computed in polynomial time in the degree of G.*

***Corollary*.** *The group representability on trees where the group is presented as a permutation group via a generating set can be solved in polynomial time.*

We note that in [1] authors are mainly focused on groups given by Cayley tables, so we in fact answered a more general question.

Notice that we do not claim to find the subgroup of minimal index itself (which is required to reconstruct the corresponding action of a group on a tree). Nevertheless, in the case when the group is given by its Cayley table, it is possible to enumerate all such subgroups.

***Theorem* 3.** *Let G be a finite group given by its Cayley table. Then the set $\{H < G \mid |G : H| = \kappa(G)\}$ can be computed in time polynomial in $|G|$.*

It might be very plausible that (at least one) subgroup of minimal index can be computed in polynomial time in the case of permutation groups, but it most certainly would need a more advanced machinery.

The author would like to express his gratitude to prof. Avinoam Mann, who pointed out that Theorem 1 was proved earlier and gave the reference to Berkovich's paper.

2 Proof of Theorem 1

The article [2] besides the original proof by Berkovich (originating in [3]) contains another very short and elegant proof attributed by the author to M.I. Isaacs. We reproduce it with almost no changes for the sake of completeness.

If G is simple, then clearly $\kappa(G) = \mu(G)$. Therefore it suffices to prove the converse statement.

Let H be a subgroup of index $\kappa(G)$ in G such that $core_G(H) = 1$. Suppose that N is a nontrivial proper normal subgroup of G. Since H is maximal, we have $G = NH$. Let U be a subgroup of H minimal with $G = NU$. Obviously

$U > 1$, and U does not lie in H^g for some $g \in G$. Set $V = U \cap H^g < U$. We have

$$|G : NV| = |NU : NV| = \frac{|N||U||N \cap V|}{|N||V||N \cap U|} \leq |U : V| < |G : H|,$$

since $|U : V| = |UH^g : H^g| = |UH^g|/|H|$ and $UH^g \subseteq HH^g \subset G$. By minimality of $|G : H|$ it follows that $G = NV$, contrary to the choice of U.

3 Proof of Theorem 2

In what follows, we assume the standard polynomial-time toolbox from [4].

Let S be a simple group. Denote by $O^S(G)$ the minimal normal subgroup of G such that each composition factor of $G/O^S(G)$ is isomorphic to S. It is noted in [4] that an algorithm for computing $O^S(G)$ in polynomial time is implicit in [5].

Now let G be a permutation group given by its generators. Compute the composition series of G, and let Σ be the collection of isomorphism types of composition factors. By Theorem 1, if H is a subgroup of minimal index, then it contains the maximal normal subgroup $N = core_G(H)$. The quotient G/N is simple, therefore its isomorphism type S lies in Σ and $O^S(G) \leq N < G$. Moreover, $\kappa(G) = \kappa(G/N) = \mu(S)$, so

$$\kappa(G) = \min\{\mu(S) \mid S \in \Sigma,\, O^S(G) < G\},$$

where $\mu(S)$ can be found by checking the description of minimal faithful permutation representations of finite simple groups, which is well-known (for example, see [6, Table 4] for groups of Lie type and [7, Table 4] for sporadic simple groups). Since all steps can be performed in polynomial time, we obtain the required algorithm.

4 Proof of Theorem 3

The key observation is the following.

***Lemma* 1.** *Let G be a finite simple group given by its Cayley table. Then the set of maximal subgroups of G can be computed in time polynomial in $|G|$.*

Proof. Try all possible 4-tuples of elements of G (there are $|G|^4$ of those) and generate corresponding subgroups. One can test in polynomial time if a given subgroup is maximal, so we obtain the list of all maximal subgroups of G generated by 4 elements. By [8, Theorem 1] every maximal subgroup of a finite simple group is 4-generated, so we in fact found all maximal subgroups of G. □

Set $\mathcal{M}(G) = \{N < G \mid N \textit{ is a normal subgroup of } G, \textit{ and } G/N \textit{ is simple}\}$, and recall that we can compute $\mathcal{M}(G)$ in polynomial time even for permutation groups (see the proof of [5, Lemma 7.4]). Notice that we can find the following set in polynomial time:

$$\mathcal{A}_N = \{H < G \mid N \leq H, \, |G : H| = \kappa(G)\}.$$

Indeed, $\kappa(G)$ can be computed in polynomial time by Theorem 2, and obviously the Cayley table for G/N can be found in polynomial time, thus by Lemma 1 we can find all maximal subgroups of G/N. By taking preimages and keeping only subgroups of index equal to $\kappa(G)$, we find the required set.

Now, by Theorem 1 every subgroup H with $|G : H| = \kappa(G)$ contains a maximal normal subgroup. Therefore $\{H < G \mid |G : H| = \kappa(G)\} = \bigcup_{N \in \mathcal{M}(G)} \mathcal{A}_N$, and this set can be computed in polynomial time.

References

[1] S. Dutta, P.P. Kurur, *Representing Groups on Graphs*, Mathematical Foundations of Computer Science (2009), 295-306.

[2] Y. Berkovich, *The Degree and Index of a Finite Group*, Journal of Algebra, **214** (1999), 740–761.

[3] Y. Berkovich, *A necessary and sufficient condition for the simplicity of a finite group*, Algebra and number theory, Nal'chik (1979), 17–21 (Russian).

[4] Á. Seress, *Permutation Group Algorithms*, Cambridge University Press (2003).

[5] L. Babai, E.M. Luks, Á. Seress, *Permutation groups in NC*, Proc. 19th ACM STOC (1987), 409–420.

[6] S. Guest, J. Morris, C.E. Praeger, P. Spiga, *On the maximum orders of elements of finite almost simple groups and primitive permutation groups*, Trans. Amer. Math. Soc., **367** (2015), 7665–7694.

[7] V.D. Mazurov, *Minimal permutation representations of Thompson's simple group*, Algebra and Logic, **27**, 5 (1988), 350–361.

[8] T.C. Burness, M.W. Liebeck, A. Shalev, *Generation and random generation: From simple groups to maximal subgroups*, Advances in Mathematics, **248** (2013), 59–95.

Saveliy V. Skresanov
Novosibirsk State University, 2 Pirogova Str.,
Novosibirsk, 630090, Russia
e-mail: s.skresanov@g.nsu.ru