Polynomial-time normalizers for permutation groups with restricted composition factors

Eugene M. Luks*
Computer and Information Science
University of Oregon
Eugene, OR 97403-1202
luks@cs.uoregon.edu

Takunari Miyazaki*
Computer Science
Trinity College
Hartford, CT 06106-3100
miyazaki@starbase.cs.trincoll.edu

ABSTRACT

For an integer constant $d > 0$, let Γ_d denote the class of finite groups all of whose nonabelian composition factors lie in S_d; in particular, Γ_d includes all solvable groups. Motivated by applications to graph-isomorphism testing, there has been extensive study of the complexity of computation for permutation groups in this class. In particular, set-stabilizers, group intersections, and centralizers have all been shown to be in polynomial-time computable. The most notable gap in the theory has been the question of whether normalizers of subgroups can be found in polynomial time. We resolve this question in the affirmative. Among other new procedures, the algorithm requires instances of subspace-stabilizers for certain linear representations and therefore some polynomial-time computation in matrix groups.

1. INTRODUCTION

While algebraic methods are surely of core interest in computational complexity, a particular attraction of group-theoretic computation is its central role in the graph-isomorphism problem. Though rarely difficult in practice, the problem, ISO, of testing isomorphism of graphs is not known to be in polynomial time. Arguably, the most productive approaches to ISO have exploited its relation to a class of permutation-group problems usually represented by the following.

A. Finding subset-stabilizers.

B. Finding group intersections.

C. Finding centralizers of subgroups.

D. Finding normalizers of subgroups.

*This research was partially supported by NSF Grant CCR-9820945.

Up to polynomial time, **A**, **B**, **C** are equivalent problems, and each is reducible to **D**; ISO is reducible to any of them. So it is not surprising that, despite continued improvements in practical implementations, none of these problems is known to be solvable in polynomial time. Nevertheless, as with ISO [25], there is compelling evidence that the "decision" versions[1] of these problems are not NP-complete [4]. This has motivated extensive investigation into polynomial-time computability for permutation-group problems in general (see [12] and [17] for surveys) but especially for problems **A**–**D**.

Now, aside from the overall reducibility between the above problems, solutions geared to special group classes have facilitated polynomial-time algorithms for significant instances of ISO. For example, the solution to **A** just for 2-groups yielded the first (and still the only known) polynomial-time approach to testing isomorphism of trivalent graphs [14], and subsequently, a polynomial-time set-stabilizer algorithm for groups with bounded nonabelian composition factors (Γ_d groups, see below) yielded ISO in polynomial time for graphs of bounded valence or bounded genus [14], [21].

The polynomial time solution of **A** in Γ_d groups led immediately to similar success with **B** and **C**. However, the normalizer question for Γ_d has remained open (see [17, Question 16]). The main result of this paper is its resolution.

Specifically, problem **D** may be stated

Normalizer (NORM).
Given: *Permutation groups* $H \leq G \leq \mathrm{Sym}(\Omega)$.
Find: *The normalizer* $\mathrm{Norm}_G(H) = \{g \in G \mid H^g = H\}$.

As usual, we assume that permutation groups are input or output via a generating set S of permutations (so that the input length is considered to be $|S||\Omega|$).

Of course, NORM is of both practical and theoretical interest. In practice, most implementations include backtrack search at some level and thereby have exponential worst case running time (cf. [5], [7], and [13]). Although, "worst case" is not necessarily observed in groups of interest to the

[1]For each, there is a polynomial-time equivalent "Yes/No" version (see, e.g., [17]); for D, this could be the issue of conjugacy of two given subgroups.

users, it can be brought out even on input for which there are polynomial-time solutions to NORM, including nilpotent groups (see [19] and [20]).

It was pointed out first in [12] that normalizers of nilpotent groups could be computed in polynomial time. Subsequently, a redesigned method for nilpotent groups not only retained and improved (to $O(n^4)$) the polynomial timing but was implemented [20] and shown, in many cases, to improve substantially over the built-in library functions (at that time) of software systems GAP [7] and MAGMA [5]. For the solvable case, the first author described a critical step, namely, finding stabilizers of subspaces in linear representations [16] (but details for the application to normalizers were not included).

We consider the following class.

Definition. For an integer constant $d > 0$, let Γ_d denote the class of finite groups all of whose nonabelian composition factors lie in S_d.

Manifestly, Γ_d includes all solvable groups. As indicated, the class arises naturally in significant instances of ISO. It has also become a subject of investigation in its own right asymptotic group theory (cf. [2] and [23]).

The principle result of this paper is

Theorem 1.1. *Given permutation groups $H \leq G \leq \mathrm{Sym}(\Omega)$ such that $G \in \Gamma_d$, one can find the normalizer $\mathrm{Norm}_G(H)$ in polynomial time.*

By standard reductions, or by a careful review of the normalizer algorithm itself, one also derives a polynomial solution to the decision problem.

Theorem 1.2. *Given $G \leq \mathrm{Sym}(\Omega)$ such that $G \in \Gamma_d$ and subgroups H_1, H_2 of G, one can test in polynomial time whether H_1 and H_2 are conjugate in G.*

The overall algorithm for Theorem 1.1 utilizes the chief series of G and, though reorganized here for clarity of our concerns, is thereby in the spirit of methods in [20] and [8] for example. Thus, we reduce to the case that H *covers* ($HL = HK$) or *avoids* ($H \cap L = H \cap K$) each chief factor L/K. We focus then on instances $M \rhd L \rhd K$ in the chief series where H covers M/L but avoids L/K and seek the normalizer of $(H \cap M)K/K$ in the action of G on M/K. For the both these phases, we appeal, for polynomial time, to special properties of Γ_d groups. We utilize algorithms for each of the problems **A**, **B**, **C**, but extensions of these are required as well.

We recall that the key property that resolved problems **A**, **B**, **C** was the fact that if $G \leq S_n$ is primitive with $G \in \Gamma_d$ then $|G| = O(n^{f(d)})$. This enabled a divide-and-conquer method that easily exploited orbits and, in the transitive case, used the primitive action on a block system to break the group into a *'small'* number of cosets of the *intransitive* stabilizer of the blocks. (With care, and some additional tricks, the method can be shown to run in time $O(n^{cd/\log d})$ [3]). This method is routinely used in our normalizer algorithm as well. But we further develop an analog of this divide-and-conquer paradigm for matrix-group computation, since the normalizer problem even for permutation groups naturally leads to instances of finding subspace-stabilizers in certain matrix groups. Whereas the permutation-group divide-and-conquer utilized orbits and imprimitivity blocks, the matrix-group analog, introduced in [16], makes use of invariant subspaces and imprimitivity systems.

Finally, we emphasize that our goal is a clear resolution of the polynomial-time issue. With this in mind, in several places we have strived to simplify the exposition at the expense of both low-level complexity and practical efficiency. We specifically reserve the latter concern for future investigation wherein it will be coupled with more general techniques for implementing polynomial-time centralizers and normalizers in classes of matrix groups [18], [22].

This paper is organized as follows. In section 2, we summarize basic polynomial-time tools. The overall architecture of the main algorithm for computing normalizers in the class Γ_d is described in section 3. We leave for section 4, two lemmas that deal with critical base cases; these describe extensions of the techniques for problems **A** and **B**. A key subroutine of our normalizer algorithm involves a polynomial-time method for finding stabilizers of vectors and subspaces in linear representations of permutation groups in the class Γ_d; this method is described in Section 5.

2. PRELIMINARIES

We recall portions of the polynomial-time library for permutation groups. For more details, we refer to the survey article [17].

We begin with the following results (cf. [6], [10], [11], [15], and [27]).

Theorem 2.1. *Given $G \leq \mathrm{Sym}(\Omega)$, in polynomial time one can solve the following problems.*

(i) Given $\alpha \in \Omega$, find the orbit of α under G and test transitivity of G.

(ii) Test the primitivity of G and, if not, find a non-trivial block system.

(iii) Given $x \in \mathrm{Sym}(\Omega)$, test whether or not $x \in G$.

(iv) Find $|G|$.

(v) Find a Sylow p-subgroup of G and the normalizer in G of any such subgroup as well as the normalizer of any such subgroup.

(vi) Find the derived series of G and test the solvability of G.

(vii) Find a composition series of G.

(viii) Find a chief series of G. □

As indicated in the introduction, for groups in Γ_d, there are polynomial-time solutions for problems that resemble ISO in permutation groups. We use the following forms of these results.

Theorem 2.2 (Luks). *Given $G \leq \mathrm{Sym}(\Omega)$ such that $G \in \Gamma_d$, in polynomial time one can solve the following.*

(i) For given $\Delta \subset \Omega$, find $\mathrm{Stab}_G(\Delta) = \{g \in G \mid \Delta^g = \Delta\}$.

(ii) For given $H \leq \mathrm{Sym}(\Omega)$, find $H \cap G$. (Note that the Γ_d hypothesis is only needed on G.)

(iii) For given $x \in \mathrm{Sym}(\Omega)$, find $\mathrm{Cent}_G(x) = \{g \in G \mid gx = xg\}$. (By repeated application one finds centralizers of groups.) □

In [12], Kantor and Luks suggested, in a *quotient-group thesis*, that problems that are in polynomial time for permutation group remain in polynomial time when applied to quotients of permutation groups.[2] The "proof" of this thesis was its demonstration for the known polynomial-time library. We will freely make use of that thesis. In particular,

Theorem 2.3 (Kantor–Luks). *Problems (iv), (v), (vi), (vii), and (viii) of Theorem 2.1 and problems (ii) and (iii) of Theorem 2.2 remain in polynomial time if $G = L/K$ for $K \lhd L \leq \mathrm{Sym}(\Omega)$.* □

In the spirit of the quotient-group thesis, we observe that our Theorems 1.1 and 1.2 hold for quotient groups with no essential modification of the proofs.

Motivated by Theorem 2.2, Babai, Cameron, and Pálfy subsequently derived the following important related theorem [2].

Theorem 2.4 (Babai–Cameron–Pálfy). *For an integer $d > 0$, there is a function $f(d)$ satisfying the following: if G is a primitive permutation group of degree n such that $G \in \Gamma_d$, then $|G| \leq n^{f(d)}$.* □

In turn, Theorem 2.4 simplifies the divide-and-conquer techniques originally used for Theorem 2.2 and we employ that same simplication herein.

3. MAIN ALGORITHM

We outline the main steps of the normalizer algorithm for groups in Γ_d.

For simplicity, it is convenient to focus on a procedure that is aimed only at getting a step closer to the normalizer.

[2]Assuming, of course, the problem makes sense when stated for quotients, e.g. "subset-stabilizer" would have no such extension.

Proposition 3.1. *Given $H < G \leq \mathrm{Sym}(\Omega)$, where $G \in \Gamma_d$, such that G does not normalize H, in polynomial time one can find a subgroup J such that $\mathrm{Norm}_G(H) \leq J < G$.*

Proof. Our algorithm consists of four steps.

1. Construct a chief series for G:

$$G = G_1 \rhd G_2 \rhd \cdots \rhd G_q = 1$$

2. If there is a chief factor L/K not covered by H, then

- **a.** If L/K is abelian, then use Theorem 5.1 (subspace-stablizer) to find $J := \mathrm{Norm}_G((H \cap L)K/K)$. Return J and exit.
- **b.** If L/K is nonabelian, then use Lemma 4.1 to find suitable J. Return J and exit.

3. While there is a 3-term segment $M \rhd L \rhd K$ of the chief series, where H covers M/L but avoids L/K, and G normalizes $(H \cap M)K$, replace L by $(H \cap M)K$. (This moves covered factors toward the tail of the series when possible.)

4. Let now $M \rhd L \rhd K$ be a segment such that H covers M/L and avoids L/K. (By Step 3, G does not normalize $(H \cap M)K$.)

- **a.** If M/L is an abelian p-group, there are two cases to consider.
  - **i.** p does not divide $|L/K|$. Then $(H \cap M)K/K$ is a Sylow p-subgroup of M/K. Use the Sylow-normalizer result of [12, P13] to find $J := \mathrm{Norm}_G((H \cap M)K)$ in polynomial time. Return J and exit.
  - **ii.** p divides $|L/K|$. As $L/K \in \Gamma_d$, use the centralizer result of [12, P7] to construct $X = \mathrm{Cent}_{L/K}((H \cap M)K/K)$ in polynomial time. Then $X \neq 1$ since it intersects the center of a Sylow p-subgroup of M/K containing $(H \cap M)K$.
    If L/K is nonabelian, then we have $X < L/K$ (otherwise, $(H \cap M)K/K = \mathrm{Cent}_{M/K}(L/K)$ and would be normalized by G). Thus, use Lemma 4.1 to find $J := \mathrm{Norm}_G(X)$. Return J and exit.
    If L/K is abelian, then $X = \mathrm{Z}(M/K) \cap L/K$ and is normalized by G. Hence, we have $X = L/K$, and M/K is an elementary abelian p-group. Now use Theorem 5.1 (subspace stabilizer) to find $J := \mathrm{Norm}_G((H \cap M)K/K)$. Return J and exit.
- **b.** Otherwise, $M/L \simeq (H \cap M)K/K = T_1 \times \cdots \times T_\ell$, where the T_i are isomorphic nonabelian simple groups. Set $A = \bigcup_i T_i$. Then $\mathrm{Norm}_G((H \cap M)K/K) = \mathrm{Stab}_G(A)$. Now, consider a natural isomorphism of $M/L \simeq (H \cap M)K/K$ and the action of G on M/L, inducing a group R acting on A. Namely, $g \in G$ induces $r_g \in R$ if $(tL)^g = t^{r_g}L$ for $t \in A$. Furthermore, g stabilizes A if and only if $t^{r_g} = t^g$ for all $t \in A$. Thus, use Lemma 4.2 to find $J := \mathrm{Stab}_G(A)\big|_A \cap R = \mathrm{Norm}_G((H \cap M)K/K)$. Return J and exit. □

Using Proposition 3.1, we now present the algorithm to establish Theorem 1.1:

$M := G$

While M does not normalize H,
find J with $N_M(H) \leq J < M$ and reset $M := J$. □

Remark. This is a typical instance of our sacrifice of practical efficiency for succinct demonstration of polynomial time. We would certainly not advocate starting from scratch with each new M, e.g., in the construction of a chief series, etc.

4. TWO STABILIZER LEMMAS

Given an action of a Γ_d group on a nonabelian semisimple group with small factors, the next lemma guarantees that we can find the normalizer of a subgroup. This was required in steps **1** and **4** of our main procedure.

Lemma 4.1. *Given $G \leq \mathrm{Sym}(\Omega)$ such that $G \in \Gamma_d$, a minimal G-group $L = T_1 \times \cdots \times T_\ell$, where the T_i are isomorphic nonabelian simple groups of polynomially bounded size, and $H < L$, in polynomial time one can find a subgroup J such that $\mathrm{Norm}_G(H) \leq J < G$.*

Proof. Since the action of G on L permutes these factors, G acts naturally on the set $\Delta = \bigcup_{1 \leq i \leq \ell} T_i$. For $i = 1, \ldots, \ell$, let H_i denote the projection of H on T_i. We consider the following three cases.

Case 1. For some i, we have $H_i = 1$. Considering the permutation action of G on the ℓ simple factors of L, set $J = \mathrm{Stab}_G(\{i \mid H_i = 1\})$. Since G acts transitively on the factors, we have $J < G$.

Case 2. For some i, we have $1 < H_i < T_i$. Considering the induced action of G on Δ, set $J = \mathrm{Stab}_G(\bigcup_{1 \leq i \leq \ell} H_i)$. Since J stabilizes $H_1 \times \cdots \times H_\ell < L$, we have $J < G$.

Case 3. We may assume $H_i = T_i$ for all i. Then there is a partition of $\{T_1, \ldots, T_\ell\}$ into s blocks of isomorphic factors so that, after a suitable renumbering of the factors,

$$H = \mathrm{Diag}(T_1 \times \cdots \times T_{r_1}) \times \cdots \times \mathrm{Diag}(T_{r_{s-1}+1} \times \cdots \times T_{r_s}),$$

where the diagonals are formed with respect to suitable isomorphisms $\pi_{ij} : T_i \to T_j$ for T_i, T_j in the same block (see, e.g., [26]). Form a graph $\mathcal{X}$ with vertex set Δ and edge set E comprised of all $(t_i, t_i^{\pi_{ij}})$ for $t_i \in T_i$ and T_i, T_j in the same block. Since $G \in \Gamma_d$, one can compute the subgroup J inducing automorphisms of $\mathcal{X}$ (i.e., $J := \mathrm{Stab}_G(E)$) in polynomial time by Theorem 2.2 (i). Note that $J = \mathrm{Stab}_G(H) < G$. □

In step **4b** of our main algorithm, it was necessary to find the stabilizer in G of a subset A of G-group, which we will call M. The algorithm for Theorem 2.2(i) does not apply because the overall domain M (given only by group generators) is not of polynomial size. However, we also have a little more information about the way elements that do stabilize A have to act on A (in step **4b** this followed from the faithful representation of A in a G-homomorphic image of M where the image of A *is* G-stable). So, in effect, we are not looking merely for $\mathrm{Stab}_G(A)$ but for $\mathrm{Stab}_G(A)\big|_A \cap R$, where $R \leq \mathrm{Sym}(A)$ is a known Γ_d group. Thus, it is no surprise that the algorithm for this problem resembles the method for intersection with a Γ_d-group (see [14, §4]).

In the following lemma, we emphasize that A is just a *set* of cosets, and so we assume that it is enumerated in the input. Hence, by definition, it is of polynomial-size.

Lemma 4.2. *Given $K, G \leq \mathrm{Sym}(\Omega)$ such that G normalizes K, a set $A \subseteq \mathrm{Norm}_{\mathrm{Sym}(\Omega)}(K)/K$, and $R \leq \mathrm{Sym}(A)$, where both G and R are in Γ_d, in polynomial time one can compute $\mathrm{Stab}_G(A)\big|_A \cap R$.*

Proof. To accommodate a recursion, we consider the following more general problem.

Given: $x \in R \times G$, $X \leq R \times G$, $B \subseteq A$, *where X stabilizes B (here, $R \times G$ acts on B via its first coordinate).*

Find: $\mathcal{S}_{Xx}(B) = \{(r, g) \in Xx \mid \forall b \in B, b^r = b^g\}$

Observe that $\mathcal{S}_{Xx}(B)$ is either empty or a subcoset of xX. Also, note that $\mathcal{S}_{R \times G}(A) = \{(r, r) \mid r \in \mathrm{Stab}_G(A)\big|_A \cap R\}$.

We perform a divide-and-conquer procedure according to the following three cases.

Case 1. We divide the problem according to the orbits of X in B. Without loss of generality, suppose that $B = B_1 \dot\cup B_2$, where X stabilizes both B_1 and B_2. Then

$$\mathcal{S}_{Xx}(B) = \mathcal{S}_{\mathcal{S}_{Xx}(B_1)}(B_2).$$

Case 2. Suppose now that X acts transitively but not primitively on B, where $|B| > 1$. First, find a primitive action on a block system $B = B_1 \dot\cup \cdots \dot\cup B_m$. Then find the kernel H of the action of this system and decompose $X = \bigcup_{i=1}^{|G:H|} Y z_i$. Here, $\mathcal{S}_{Xx}(B) = \bigcup_{i=1}^{|G:H|} \mathcal{S}_{Yz_i x}(B)$. Since $G \in \Gamma_d$, it follows from Theorem 2.4 that $|G : H| = O(m^c)$ for some constant $c > 0$.

Case 3. Suppose finally that $B = \{b\}$. Suppose that $x = (r_0, g_0)$, and X projects onto $H \leq G$. Then $\mathcal{S}_{Xx}(B) = \{h \in H \mid (b^{g_0})^h = b^{r_0}\}$, which, since $H \in \Gamma_d$, is computable in polynomial time (see [12]). □

5. SUBSPACE STABILIZERS

Throughout this section, we assume that V is an n-dimensional vector space over a finite field k. We will outline the proof of the following fundamental result. We rely for some details on related results for the solvable case in [16, §10].

The main result of this section is

Theorem 5.1. *Given $G \leq \mathrm{Sym}(\Omega)$ such that $G \in \Gamma_d$, a linear representation $^- : G \to \mathrm{GL}(V)$, where $\mathrm{char}\, k$ is polynomially bounded in the input length, and a subspace $W \subseteq$*

V, in polynomial time one can find the subspace stabilizer $\mathrm{Stab}_G(W) = \{g \in G \mid W^{\bar{g}} = W\}$.

The method for Theorem 5.1 uses a divide-and-conquer paradigm resulting from the following.

Theorem 5.2. *Given $G \leq \mathrm{Sym}(\Omega)$ such that $G \in \Gamma_d$ and a linear representation $^- : G \to \mathrm{GL}(V)$, where $\mathrm{char}\, k$ is polynomially bounded in the input length, in polynomial time one can perform one of the following.*

(i) Prove that $\bar{G}$ is nonabelian simple.

(ii) Find a subgroup A of G, where $\bar{A}$ is abelian, such that $|G : A| \leq 24n$.

(iii) Find a proper subspace $W \subset V$.

(iv) Find a subgroup H of G and a set of $\bar{H}$-subspaces $\{V_1, \ldots, V_m\}$, $m \geq 2$, such that

(a) $V = V_1 \oplus \cdots \oplus V_m$,

(b) $\dim_k V_i = n/m$ for $i = 1, \ldots, m$, and

(c) $|G : H| = O(m^{c_1})$ for a constant $c_1 > 0$.

Remark. Note that Theorems 5.1 and 5.2 include an assumption on $\mathrm{char}\, k$. The polynomial bound on $\mathrm{char}\, k$ enables a call to Rónyai's algorithm [24] for finding invariant subspaces in deterministic polynomial time.

As indicated, Theorem 5.2 facilitates the extension to representations of Γ_d groups of a divide-and-conquer paradigm given in [16] for solvable matrix groups. The paradigm applies to problems that ask for construction of a recognizable[3] subcoset (the input is a coset of G) for which

- Given a G-invariant subpace $W \subset V$, the problem can be solved in polynomial time together with recursive calls to induced problems on W and V/W.
- The problem is in polynomial time for abelian $\bar{G}$.

We refer to [16] for the proof that the paradigm is applicable to finding subspace-stabilizers. We note in particular, that this is done in two stages. First the paradigm is applied to the problem of finding stabilizers of vectors. Then the paradigm is applied to subspace stabilizers assuming the polynomial-time solvability of finding vector stabilizers.

We proceed then to an outline the proof of Theorem 5.2. First, we begin with four fundamental lemmas essential to our algorithms.

By [12, P9], we can find kernels of linear representations of permutation groups in polynomial time.

Lemma 5.3 (Kantor–Luks). *Given $G \leq \mathrm{Sym}(\Omega)$ and a linear representation $\phi : G \to \mathrm{GL}(V)$, one can find the kernel of ϕ in polynomial time.* □

[3] One can easily test membership.

We say that an abelian subgroup of $\mathrm{GL}(V)$ is *uniform* if, for every integer $m \geq 1$, the subgroup A^m of A has no nonzero fixed vectors in V (i.e., $\mathrm{Cent}_V(A^m) = 0$) unless $A^m = 1$ (cf. [16, §2]).

The following result is given in [16, Lemma 4.6].

Lemma 5.4. *Let A be a uniform abelian subgroup of $\mathrm{GL}(V)$. If $V_1, \ldots, V_m$ are the distinct maximal A-subspaces of V such that the restrictions $A|V_i$ are cyclic, then V decomposes as a direct sum $V = V_1 \oplus \cdots \oplus V_m$.* □

The following result is implicit in [1, 27.14].

Lemma 5.5. *Let $G = NM$ be an irreducible subgroup of $\mathrm{GL}(V)$, where N and M are normal subgroups of G centralizing each other. Let W_1 be a minimal N-subspace of V and $U = \mathrm{Hom}_{kN}(W_1, V)$. Then there is a finite extension K of k, where $K \cong \mathrm{End}_{kN}(W_1)$, such that the following hold.*

(i) V is a KG-module, W_1 is a KN-module, and U is a KM-module.

(ii) $V \cong W_1 \otimes_K U$ as K-spaces. □

The next result is closely related to [2, Theorem 3.2] and [14, Proposition 3.9].

Lemma 5.6. *Let G be an irreducible subgroup of $\mathrm{GL}(V)$ such that $G \in \Gamma_d$. Suppose G has a cyclic normal subgroup $A \geq 1$, and G/A has a nonabelian minimal normal subgroup N/A. Then $\mathrm{Cent}_G(N')$ is reducible, and there are positive constants c_1 and c_2 such that at least one of the following holds.*

(i) $V = V_1 \oplus \cdots \oplus V_m$ such that $\mathcal{V} = \{V_1, \ldots, V_m\}$ forms a system of imprimitivity for G, where the transitive permutation representation of G on $\mathcal{V}$ is primitive and has the kernel L such that $N' \leq L$ and $|G : L| \leq m^{c_1}$.

(ii) $|G : \mathrm{Cent}_G(N')| = O(t^{c_2})$, where t is the dimension of a minimal N'-subspace W_1 of V over the finite extension $K_1 = \mathrm{End}_{kN'}(W_1)$ of k such that $t \geq 2$ and $t|n$. □

The algorithm for Theorem 5.2 involves a recursion that steps up a series of normal subgroups of $\bar{G}$. The following proposition, adapted from [16, Theorem 6.1], provides a subroutine to handle certain abelian chief factors of $\bar{G}$ during this recursion. Note that the algorithm establishing this proposition does not require any assumption on $\mathrm{char}\, k$ since it does not rely on Rónyai's result [24].

Proposition 5.7. *Given $G \leq \mathrm{Sym}(\Omega)$ such that $G \in \Gamma_d$, a linear representation $^- : G \to \mathrm{GL}(V)$, and normal subgroups N and A of G such that $\bar{A}$ is cyclic and uniform, $\bar{N}$ centralizes $\bar{A}$, and $\bar{N}/\bar{A}$ is elementary abelian, in polynomial time one can perform one of the following.*

(i) Prove that $|\bar{G} : \bar{A}| \leq 24n$.

(ii) Find a normal subgroup B *of* A*, where* $\bar{B}$ *is abelian, such that* $\bar{A} < \bar{B}$.

(iii) Find a normal subgroup M *of* G*, where* $\bar{A} < \bar{M}$*, such that* $\bar{M}/\bar{A}$ *is a nonabelian minimal normal subgroup of* $\bar{G}/\bar{A}$.

(iv) Find a normal subgroup H *of* G *and a decomposition* $V = V_1 \oplus \cdots \oplus V_m$*, forming a minimal system of imprimitivity* $\mathcal{V} = \{V_1, \ldots, V_m\}$ *for* $\bar{H}$ *such that* $|\bar{G} : \bar{H}| \leq m^{c_1}$ *for a constant* $c_1 > 0$*, and find the kernel* L *of the permutation representation of* H *on* $\mathcal{V}$ *such that* $|\bar{H} : \bar{L}| \leq m^{c_2}$ *for a constant* $c_2 > 0$.

Outline of proof. We describe a polynomial-time algorithm in three steps. Throughout, we write $\bar{Z} = \mathrm{Z}(\bar{N})$. First, use Lemma 5.3 to find $\bar{Z}$.

Step 1. Suppose that $\bar{N}/\bar{A}$ is an elementary abelian p-group. If $\bar{N}$ is abelian, return N as B for Case (ii). Suppose otherwise; that is, $\bar{N}$ is class-2 nilpotent. If $\bar{A} < \bar{Z}$, then return Z as B for Case (ii). Otherwise $\bar{A} = \bar{Z}$. Then, by [16, Lemma 4.7], we have $|\bar{N} : \bar{Z}| \leq n^2$. Here, the conjugation action of $\bar{G}$ on $\bar{N}/\bar{Z}$ induces a linear representation ϕ over a finite field of order p. In fact, since $|\bar{N} : \bar{Z}| \leq n^2$, we may assume that ϕ is irreducible. Suppose that the rank of $\bar{N}/\bar{Z}$ is 2ℓ for $\ell \geq 1$. Find $\bar{H} = \mathrm{Ker}\,\phi$. By [2, Corollary 3.3], there is a constant $c_3 > 0$ such that $|\bar{G} : \bar{H}| \leq p^{c_3(2\ell)}$. Then we obtain one of the following.

(1) A decomposition $V = V_1 \oplus \cdots \oplus V_m$ such that $\mathcal{V} = \{V_1, \ldots, V_m\}$ forms a minimal system of imprimitivity for $\bar{H}$, where $m = p^\ell$ if $p \neq 2$, $m = 2^{\lfloor \ell/2 \rfloor}$ if $p = 2$ and $\ell \geq 2$, or $m = 2$ if $p = 2$ and $\ell = 1$.

(2) A subgroup Q of N, where $\bar{Q}$ is a quaternion group of order 8, such that $\bar{N}' < \bar{Q} \leq \bar{N}$.

Step 2. Suppose that we obtain (1) in Step 1. Then there is a constant $c_1 > 0$ such that $|\bar{G} : \bar{H}| \leq m^{c_1}$; furthermore, the permutation representation of H on $\mathcal{V}$ is primitive. Find its kernel L. Then, by Theorem 2.4, there is a constant $c_2 > 0$ such that $|\bar{H} : \bar{L}| \leq m^{c_2}$. Therefore, we establish Case (iv).

Step 3. Suppose that we obtain (2) in Step 1. Let $Q_1 = Q$. Then $Q \trianglelefteq G$ and $|\bar{G} : \mathrm{Cent}_{\bar{G}}(\bar{N})| \leq 24n$. Use Lemma 5.3 to find $\mathrm{Cent}_{\bar{G}}(\bar{N})$. If $\bar{A} = \mathrm{Cent}_{\bar{G}}(\bar{N})$, then we have Case (i). Suppose that $\bar{A} < \mathrm{Cent}_{\bar{G}}(\bar{N})$. Find a normal subgroup M of G, where $\bar{A} < \bar{M} \leq \mathrm{Cent}_{\bar{G}}(\bar{N})$, such that $\bar{M}/\bar{A}$ is an elementary abelian group or a nonabelian minimal normal subgroup of $\bar{G}/\bar{A}$. If $\bar{M}/\bar{A}$ is nonabelian, then return M for Case (iii). Suppose that $\bar{M}/\bar{A}$ is elementary abelian. Here, $\bar{M}$ centralizes $\bar{A}$. Regarding M as N, recursively perform Step 1. If we obtain (1), then we have Case (iv).

Suppose now that we obtain (2), say, Q_2 such that $\bar{M}' < \bar{Q}_2 \leq \bar{M}$. Since $\bar{Q}_1$ and $\bar{Q}_2$ centralize each other, $\bar{Q}_1 \neq \bar{Q}_2$. Then we can find $\bar{d}_1 \in \bar{Q}_1 \setminus \bar{Q}_2$ and $\bar{d}_2 \in \bar{Q}_2 \setminus \bar{Q}_1$. Let $e = d_1 d_2$. Now, $\bar{N}' = \langle \bar{z}_0 \rangle$, where $\bar{z}_0$ is the unique element of order 2 in $\bar{Z}$ and centralized by $\bar{G}$. Let $\bar{E} = \langle \bar{e}, \bar{z}_0 \rangle$. Then $\bar{E}$ is an elementary abelian 2-group of rank 2 such that $\bar{E} < \bar{N}\bar{M}$ and $E \trianglelefteq H$. The maximal subspaces V_1 and V_2 such that the restrictions $\bar{E}|V_i$ are cyclic form a minimal system of imprimitivity $\mathcal{V} = \{V_1, V_2\}$ for $\bar{H}$. If L is the kernel of the H-action on $\mathcal{V}$, then $|\bar{H} : \bar{L}| = 2$. Thus, we have Case (iv). □

The next proposition provides a subroutine to handle certain nonabelian chief factors of $\bar{G}$ during the recursion.

Proposition 5.8. *Given* $G \leq \mathrm{Sym}(\Omega)$ *such that* $G \in \Gamma_d$*, a linear representation* $^- : G \to \mathrm{GL}(V)$*, where* $\mathrm{char}\, k$ *is polynomially bounded in the input length, and normal subgroups* N *and* A *of* G *such that* $\bar{A}$ *is cyclic,* $\bar{1} \leq \bar{A} < \bar{N}$*, and* $\bar{N}/\bar{A}$ *is a nonabelian minimal normal subgroup of* $\bar{G}/\bar{A}$*, in polynomial time one can perform one of the following.*

(i) Find a proper $\bar{G}$*-subspace* $W \subset V$.

(ii) Find a decomposition $V = V_1 \oplus \cdots \oplus V_m$*, forming a minimal system of imprimitivity* $\mathcal{V} = \{V_1, \ldots, V_m\}$ *for* $\bar{G}$*, and the kernel* L *of the permutation representation of* G *on* $\mathcal{V}$ *such that* $|\bar{G} : \bar{L}| \leq m^{c_1}$ *for a constant* $c_1 > 0$.

(iii) Find $\mathrm{Cent}_{\bar{G}}(\bar{N}')$ *such that* $|\bar{G} : \mathrm{Cent}_{\bar{G}}(\bar{N}')| = O(t^{c_2})$*, where* $t \geq 2$ *and* $t|n$*, and* c_2 *is a constant* > 0*, and minimal* $\mathrm{Cent}_{\bar{G}}(\bar{N}')$*-subspaces* $M_1, \ldots, M_e$ *of* V *of the same dimension such that* $V = M_1 \oplus \cdots \oplus M_e$*, where* $e \geq t$.

Outline of proof. By the result of Rónyai [24], we may assume that $\bar{G}$ is irreducible (otherwise, we find a proper $\bar{G}$-subspace for Case (i) using Rónyai's method).

Step 1. First, we find N' and a minimal $\bar{N}'$-subspace W_1 of V. Using Clifford's theorem (see, e.g., [1, 12.13]), we find either a system of imprimitivity for $\bar{G}$ or a direct sum of $\bar{N}'$-isomorphic minimal $\bar{N}'$-subspaces (cf. [9, §2]).

Step 2. If we find a system of imprimitivity, say $\mathcal{U}$, in Step 1, then we find a minimal system of imprimitivity $\mathcal{V}$ from $\mathcal{U}$ using a standard procedure to find a minimal block system in a permutation group. We also find the kernel L of the primitive permutation representation of G on $\mathcal{V}$. The polynomial bound on $|\bar{G} : \bar{L}|$ directly follows from the main result of [2]. This concludes Case (ii).

Step 3. It remains to consider Case (iii). Based on Lemmas 5.3, 5.5, and 5.6, we will find $\mathrm{Cent}_{\bar{G}}(\bar{N}')$ and decompose V into a direct sum of minimal $\mathrm{Cent}_{\bar{G}}(\bar{N}')$-subspaces to meet the condition of Case (iii).

Suppose that, in Step 1, we find a direct sum $V = W_1 \oplus \cdots \oplus W_r$, where the W_i are isomorphic minimal $\bar{N}'$-subspaces. By Clifford's theorem, the action of $\bar{N}'$ on each W_i is irreducible and faithful. Using Lemma 5.3, find $\mathrm{Cent}_{\bar{G}}(\bar{N}')$ and $\bar{D} = \mathrm{Cent}_{\bar{G}}(\bar{N}')\bar{N}'$. Then find a minimal $\bar{D}$-subspace V_0 of V such that $W_1 \subseteq V_0$. Let $\hat{} : D \to \mathrm{GL}(V_0)$ denote the restriction of $\bar{D}$ on V_0. Then $\hat{D}$ is an irreducible subgroup of $\mathrm{GL}(V_0)$.

Now, let $\bar{g}_1 = \bar{1}$, and find $\bar{g}_2, \ldots, \bar{g}_s \in \mathrm{Cent}_{\bar{G}}(\bar{N}')$ such that $V_0 = W_1 \oplus {W_1}^{\bar{g}_2} \oplus \cdots \oplus {W_1}^{\bar{g}_s}$. Form $k\bar{N}'$-isomorphisms $b_i : W_1 \to {W_1}^{\bar{g}_i}$ such that $b_i = \bar{g}_i | W_1$ for $i = 1, \ldots, s$.

Observe that $K_1 = \mathrm{End}_{k\bar{N}'}(W_1)$ is the centralizer of the linear span of the restriction $\bar{N}'|W_1$ over k in $\mathrm{End}_k(W_1)$. Thus, one can find a k-basis of K_1. Now, find a k-basis of an extension $K \subseteq \mathrm{End}_{k\bar{N}'}(V_0)$, $K \cong K_1$, consisting of all the elements of the form, with respect to $V_0 = W_1 \oplus {W_1}^{\bar{g}_2} \oplus \cdots \oplus {W_1}^{\bar{g}_s}$,

$$\begin{pmatrix} a_1 & & & 0 \\ & {\bar{g}_2}^{-1} a_1 \bar{g}_2 & & \\ & & \ddots & \\ 0 & & & {\bar{g}_s}^{-1} a_1 \bar{g}_s \end{pmatrix}$$

for $a_1 \in K_1$.

Here, by Lemma 5.5, we know that the set $\{b_1, \ldots, b_s\}$ forms a K-basis of $U_0 = \mathrm{Hom}_{k\bar{N}'}(W_1, V_0)$. Now, choose $0 \neq v_1 \in W_1$ and form a K-subspace M_0 spanned by $\{{v_1}^{b_1}, \ldots, {v_1}^{b_s}\}$. Next, find a minimal $\mathrm{Cent}_{\bar{G}}(\bar{N}')$-subspace M_1 in M_0. By Clifford's theorem, we can then find minimal $\mathrm{Cent}_{\bar{G}}(\bar{N}')$-subspaces $M_2, \ldots, M_e$ of the same dimension $\dim_k M_1$ such that $V = M_1 \oplus \cdots \oplus M_e$.

Let $t = \dim_{K_1} M_1$. By Lemma 5.6, we know that $|\bar{G} : \mathrm{Cent}_{\bar{G}}(\bar{N}')| = O(t^{c_2})$ for some constant $c_2 > 0$. By Lemma 5.5, we know that $V_0 \cong W_1 \otimes_K U_0$ as K-spaces; therefore, we have $e \geq t$. □

We are now ready to complete our outline of the proof of Theorem 5.2 using Propositions 5.7 and 5.8.

Outline of the proof of Theorem 5.2. We describe our algorithm in three steps.

Step 1. If $\bar{G}$ is nonabelian simple, then we have Case (i). If $\bar{G}$ is abelian, then we have Case (ii). Otherwise, find a normal subgroup N of G such that $\bar{N}$ is a nonabelian minimal normal subgroup of $\bar{G}$ or a normal subgroup A of G such that $\bar{A}$ is an abelian normal subgroup of $\bar{G}$. If we have N, then we appeal to Proposition 5.8 to establish Case (iii) or (iv).

Step 2. Suppose that Step 1 gives an abelian normal subgroup $\bar{A}$ of $\bar{G}$. If $\bar{A}$ is noncyclic or nonuniform, we establish Case (iii) or (iv) based on Lemma 5.4.

Step 3. Suppose that $\bar{A}$ is cyclic and uniform. Using Lemma 5.3, find $\mathrm{Cent}_{\bar{G}}(\bar{A})$. If $\bar{A} = \mathrm{Cent}_{\bar{G}}(\bar{A})$, then it follows that $|\bar{G} : \bar{A}| \leq n$; thus, we return A for Case (ii). If $\bar{A} < \mathrm{Cent}_{\bar{G}}(\bar{A})$, then find a normal subgroup N of G, where $\bar{A} < \bar{N} \leq \mathrm{Cent}_{\bar{G}}(\bar{A})$, such that $\bar{N}/\bar{A}$ is a nonabelian minimal normal subgroup of $\bar{G}/\bar{A}$ or an elementary abelian normal subgroup of $\bar{G}/\bar{A}$. If $\bar{N}/\bar{A}$ is nonabelian, then we again appeal to Proposition 5.8 to establish Case (iii) or (iv). If, on the other hand, $\bar{N}/\bar{A}$ is abelian, we use Proposition 5.7 to establish Case (ii) or (iv) or find one of the following.

(1) A normal subgroup B of G, where $\bar{B}$ is abelian, such that $\bar{A} < \bar{B}$.

(2) A nonabelian normal subgroup M of G such that $\bar{M}/\bar{A}$ is a nonabelian minimal normal subgroup of $\bar{G}/\bar{A}$.

If we have (1), then we regard B as A and recursively perform Step 2, and if necessary, Step 3. If we have (2), then we regard M as N and appeal to Proposition 5.8 to establish Case (iii) or (iv). □

6. REFERENCES

[1] M. Aschbacher, *Finite group theory*, 2nd ed., Cambridge Stud. Adv. Math., vol. 10, Cambridge Univ. Press, Cambridge, 2000.

[2] L. Babai, P. J. Cameron, and P. P. Pálfy, *On the orders of primitive groups with restricted nonabelian composition factors*, J. Algebra **79** (1982), 161–168.

[3] L. Babai, W. M. Kantor and E. M. Luks, *Computational complexity and the classification of finite simple groups*, 24th Symposium on Foundations of Computer Science, Tucson, Nov. 7–9, 1983, IEEE Comput. Soc. Press, Washington, D.C., 1983, pp. 162–171.

[4] L. Babai and S. Moran, *Arthur–Merlin games: a randomized proof system and a hierarchy of complexity classes*, J. Comput. System Sci. **36** (1988), 254–276.

[5] J. J. Cannon and C. Playoust, *An introduction to algebraic programming in* Magma, School of Mathematics and Statistics, The University of Sydney, Sydney, 1996.

[6] M. Furst, J. Hopcroft, and E. Luks, *Polynomial-time algorithms for permutation groups*, 21st Annual Symposium on Foundations of Computer Science, Syracuse, N.Y., Oct. 13–15, 1980, IEEE Comput. Soc. Press, Washington, D.C., 1980, pp. 36–41.

[7] The GAP Group, GAP–*Groups, Algorithms, and Programming*, version 4.2, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen; Centre for Interdisciplinary Research in Computational Algebra, University of St Andrews, St Andrews, 2000.

[8] S. P. Glasby and M. C. Slattery, *Computing intersections and normalizers in soluble groups*, J. Symbolic Comput. **9** (1990), 637–651.

[9] D. F. Holt, C. R. Leedham-Green, E. A. O'Brien, and S. Rees, *Testing matrix groups for primitivity*, J. Algebra **184** (1996), 795–817.

[10] W. M. Kantor, *Sylow's theorem in polynomial time*, J. Comput. System Sci. **30** (1985), 359–394.

[11] ———, *Finding Sylow normalizers in polynomial time*, J. Algorithms **11** (1990), 523–563.

[12] W. M. Kantor and E. M. Luks, *Computing in quotient groups*, Proceedings of the Twenty-Second Annual ACM Symposium on Theory of Computing, Baltimore, May 14–16, 1990, ACM, New York, 1990, pp. 524–534.

[13] J. S. Leon, *Partitions, refinements, and permutation group computation*, Groups and Computation. II, Piscataway, N.J., Jun. 7–10, 1995 (L. Finklelstein and W. M. Kantor, eds.), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 28, Amer. Math. Soc., Providence, R.I., 1997, pp. 123–158.

[14] E. M. Luks, *Isomorphism of graphs of bounded valence can be tested in polynomial time*, J. Comput. System Sci. **25** (1982), 42–65.

[15] ———, *Computing the composition factors of a permutation group in polynomial time*, Combinatorica **7** (1987), 87–99.

[16] ———, *Computing in solvable matrix groups*, 33rd Annual Symposium on Foundations of Computer Science, Pittsburgh, Oct. 24–27, 1992, IEEE Computer Soc., Los Alamitos, Calif., 1992, pp. 111–120.

[17] ———, *Permutation groups and polynomial-time computation*, Groups and Computation, Piscataway, N.J., Oct. 7–10, 1991 (L. Finkelstein and W. M. Kantor, eds.), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 11, Amer. Math. Soc., Providence, R.I., 1993, pp. 139–175.

[18] E.M. Luks and T. Miyazaki, In preparation.

[19] E. M. Luks, F. Rákóczi, and C. R. B. Wright, *Computing normalizers in permutation p-groups*, International Symposium on Symbolic and Algebraic Computation, Oxford, Jul. 20–22, 1994, ACM, New York, 1994, pp. 139–146.

[20] ———, *Some algorithms for nilpotent permutation groups*, J. Symbolic Comput. **23** (1997), 335–354.

[21] G. L. Miller, *Isomorphism of k-contractible graphs, a generalization of bounded valence and bounded genus*, Inform. and Control **56** (1983), 1–20.

[22] T. Miyazaki, *Polynomial-time computation in matrix groups*, Ph.D. dissertation, Tech. Rep. CIS-TR-99-11, Department of Computer and Information Science, University of Oregon, Eugene, 1999.

[23] L. Pyber, *Aymptotic results for permutation groups*, Groups and Computation, Piscataway, N.J., Oct. 7–10, 1991 (L. Finkelstein and W. M. Kantor, eds.), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 11, Amer. Math. Soc., Providence, R.I., 1993, pp. 197–219.

[24] L. Rónyai, *Computing the structure of finite algebras*, J. Symbolic Comput. **9** (1990), 355–373.

[25] U. Schöning, *Graph isomorphism is in the low hierachy*, STACS 87, 4th Annual Symposium on Theoretical Aspects of Computer Science, Passau, Feb. 19–21, 1987 (F.-J. Brandenburg, G. Vidal-Naquet, and M. Wirsing, eds.), Lecture Notes in Comput. Sci., vol. 247, Springer, 1987, pp. 114–124.

[26] L. L. Scott, *Representations in characteristic p*, The Santa Cruz Conference on Finite Groups, Santa Cruz, Calif., Jun. 25–Jul. 20, 1979 (B. Cooperstein and G. Mason, eds.), Proc. Sympos. Pure Math., vol. 37, Amer. Math. Soc., Providence, R.I., pp. 319–331.

[27] C. C. Sims, *Computational methods in the study of permutation groups*, Computational Problems in Abstract Algebra, Oxford, Aug. 29–Sep. 2, 1967 (J. Leech, ed.), Pergamon Press, Oxford, 1970, pp. 169–183.