Discrete Mathematics and Theoretical Computer Science DMTCS vol. **13:4**, 2011, 61–96

Polynomial-time normalizers

Eugene M. Luks[1†§] and Takunari Miyazaki[2‡§]

[1] *Department of Computer and Information Science, University of Oregon, Eugene, USA*
[2] *Computer Science Department, Trinity College, Hartford, Connecticut, USA*

received 27th March 2011, *revised 12th November 2011*, *accepted 17th November 2011*.

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, the problems of finding set stabilizers, intersections and centralizers have all been shown to be polynomial-time computable. A notable open issue for the class Γ_d has been the question of whether normalizers can be found in polynomial time. We resolve this question in the affirmative. We prove that, given permutation groups $G, H \le \mathrm{Sym}(\Omega)$ such that $G \in \Gamma_d$, the normalizer of H in G can be found in polynomial time. Among other new procedures, our method includes a key subroutine to solve the problem of finding stabilizers of subspaces in linear representations of permutation groups in Γ_d.

Keywords: permutation-group computation, solvable groups, Γ_d groups, subspace stabilizers

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 problem of testing graph isomorphism (ISO). Though rarely difficult in practice, ISO is not known to be solvable 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.

Problem 1
Given: *a permutation group* $G \le \mathrm{Sym}(\Omega)$ *and a subset* $\Delta \subseteq \Omega$.
Find: *the set stabilizer* $\mathrm{Stab}_G(\Delta) = \{g \in G \mid \Delta^g = \Delta\}$.

Problem 2
Given: *permutation groups* $G, H \le \mathrm{Sym}(\Omega)$.
Find: *the intersection* $G \cap H$.

[†] E-mail: luks@cs.uoregon.edu.
[‡] E-mail: takunari.miyazaki@trincoll.edu.
[§] Supported in part by NSF Grant CCR-9820945.

Problem 3
Given: *permutation groups* $G, H \leq \mathrm{Sym}(\Omega)$.
Find: *the centralizer* $\mathrm{C}_G(H) = \{g \in G \mid h^g = h \textit{ for all } h \in H\}$.

Problem 4
Given: *permutation groups* $G, H \leq \mathrm{Sym}(\Omega)$.
Find: *the normalizer* $\mathrm{N}_G(H) = \{g \in G \mid H^g = H\}$.

As customary, we assume that a permutation group is input or output via a generating set S of permutations on a set Ω. The input length is thus $|S||\Omega|$. In fact, Sims's classical method [50] can be used to reduce the sizes of generating sets to $O(|\Omega|)$ (see, e.g., Jerrum [23], Knuth [28]). Hence, polynomial time for permutation groups is generally phrased as time polynomial in $|\Omega|$.

Up to polynomial time, Problems 1–3 are equivalent, each is reducible to Problem 4, and ISO is reducible to any of the four problems. So, it is not surprising that, despite continued improvements in practical implementations (notably, in the computer algebra systems GAP [18] and MAGMA [9]), none of these problems is known to be solvable in polynomial time. On the other hand, the compelling evidence that ISO is unlikely to be NP-complete (see: Goldreich, Micali, and Wigderson [20, §2]; Schöning [48]) has been extended to decision versions of Problems 1-4 by Babai and Moran [8, §5]. This has motivated extensive investigation into polynomial-time computability for permutation-group problems in general but especially for Problems 1–4 (see [25], [35] for surveys).

Aside from the overall reducibility between these four problems, solutions geared to special classes of groups have facilitated polynomial-time algorithms for significant instances of ISO. For example, the solution to Problem 1 just for 2-groups yielded the first (and still the only known) polynomial-time approach to testing isomorphism of trivalent graphs (see [32, §2]). Subsequently, a polynomial-time set-stabilizer algorithm for the class of finite groups all of whose nonabelian composition factors are bounded (called the class Γ_d as defined below) yielded ISO in polynomial time for graphs of bounded valence (see Luks [32]) or bounded genus (see Miller [41]).

The polynomial-time solution to Problem 1 for $G \in \Gamma_d$ led immediately to similar success with Problems 2, 3 for $G \in \Gamma_d$. However, the normalizer question for $G \in \Gamma_d$ has remained open (see [35, Question 19]). The main result of this paper is its resolution.

The problem of finding normalizers is, of course, of both practical and theoretical interest. In practice, most implementations include backtrack search at some level and thereby have some potential to cause exponential worst-case running time (see [9], [18], [30], [53]). In fact, this exponential behavior has been observed even for instances of nilpotent groups (see [38], [39]).

Nevertheless, it was observed by Kantor and Luks [25, §10] that normalizers in nilpotent groups can be computed in polynomial time. Subsequently, a redesigned method of Luks, Rákóczi, and Wright [38] for nilpotent groups improved the polynomial timing to $O(|\Omega|^4)$.

In this paper, we consider the following class.

Definition For an integer $d > 0$, let Γ_d denote the class of finite groups all of whose nonabelian composition factors are isomorphic to subgroups of S_d.

Manifestly, Γ_d includes all solvable groups. As indicated, the class arises naturally in significant instances of ISO. It has also become an important subject of investigation in *asymptotic group theory* in its own right (see, e.g., [6], [45], [46]).

The key property that resolved Problems 1–3 for Γ_d groups was the following important result due to Babai, Cameron and Pálfy: there is a function $f(d)$ such that, if a subgroup G of S_n is primitive with $G \in \Gamma_d$, then $|G| = O(n^{f(d)})$ (see [6, Theorem 1.1]). (In fact, [6] deals with a more general class of groups; for more on this, see the remark following Theorem 3.8.) This enabled a polynomial-time divide-and-conquer method that exploits orbits and blocks. As it was the convention used in [32] and other previous studies on computation involving Γ_d groups [7], [25], [35], [43], throughout this paper, we regard d as a fixed constant and thus complexity of the form $O(|\Omega|^{g(d)})$, where $g(d)$ is a function depending only on d, as polynomial time.

The aforementioned results of [32] concerning Problems 2, 3 assert that, given $G, H \leq \mathrm{Sym}(\Omega)$ such that $G \in \Gamma_d$, *with no restriction on* H, one can find $G \cap H$ and $\mathrm{C}_G(H)$ in polynomial time. The gap in the theory has been the question of whether, given such $G, H \leq \mathrm{Sym}(\Omega)$ with $G \in \Gamma_d$, one can find $\mathrm{N}_G(H)$ in polynomial time. As a partial answer to this question, the authors announced in [36] that one can find $\mathrm{N}_G(H)$ in polynomial time if $H \leq G$. We now completely resolve this question to fill the gap. The principal result of this paper is

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

Given Theorem 1.1, via a standard reduction, we also derive a polynomial-time solution to the equivalent decision problem.

Theorem 1.2 *Given permutation groups $G, H_1, H_2 \leq \mathrm{Sym}(\Omega)$ such that $G \in \Gamma_d$, in polynomial time one can determine whether there is an element $g \in G$ such that $H_1^g = H_2$ and, if so, exhibit such g.*

In [25], Kantor and Luks hypothesized, in a *quotient-group thesis*, namely, that problems that are in polynomial time for permutation groups remain in polynomial time when applied to quotients of permutation groups.[(i)] In the spirit of this thesis, we extend these results to quotient groups via a method inspired by the *Frattini argument* (see [25, §7]).

Theorem 1.3 *Given permutation groups $G, K \leq \mathrm{Sym}(\Omega)$ such that K is a normal subgroup of G, and $G/K \in \Gamma_d$, in polynomial time one can solve the following problems.*

(i) *Given a permutation group $H \leq \mathrm{Sym}(\Omega)$ such that K is a normal subgroup of H, find the normalizer $\mathrm{N}_G(H)$.*

(ii) *Given permutation groups $H_1, H_2 \leq \mathrm{Sym}(\Omega)$ such that K is a normal subgroup of both H_1 and H_2, determine whether there is an element $g \in G$ such that $H_1^g = H_2$ and, if so, exhibit such g.*

The overall algorithm for Theorem 1.1 utilizes the G-chief series of $\langle H^G \rangle$ and, though reorganized here for clarity of our concerns, is thereby in the spirit of earlier normalizer computations (see, e.g., [14], [19], [39]). Thus, we reduce to the case where, for each chief factor L/K, H *covers* ($HL = HK$) or *avoids* ($H \cap L = H \cap K$) . We focus then on instances $M > L > K$ in the chief series such that 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 both these phases, we appeal, for polynomial time, to special properties of Γ_d. We utilize algorithms for each of Problems 1–3, but extensions of these are required as well.

(i) Assuming, of course, that the problem makes sense when stated for quotients, e.g., the problem of finding set stabilizers would not seem to have a meaningful extension.

We recall that the divide-and-conquer method that resolved Problems 1–3 exploits orbits and, in the transitive case, uses the primitive action on a block system to break the group into a 'small' number of cosets of the *intransitive* stabilizer of the blocks. This method is routinely used in our normalizer algorithm as well. But we further develop an analogue of this divide-and-conquer paradigm for matrix-group computation, since the normalizer problem even for permutation groups naturally leads to instances of finding stabilizers of subspaces in certain matrix groups. Whereas the permutation-group divide-and-conquer paradigm utilized orbits and imprimitivity blocks, the matrix-group analog, first introduced in [34, §6], makes use of invariant subspaces and systems of imprimitivity (cf. the *computational matrix group project* [29] that uses Aschbacher's classification [1]).

Using this matrix-group divide-and-conquer paradigm, we prove in particular the following result, which is required in our proof of Theorem 1.1 but may also be of independent interest (cf. [35, §10]).

Let V be an n-dimensional vector space over a finite field k of order q^e for some prime q.

Theorem 1.4 *Given a permutation group $G \leq \mathrm{Sym}(\Omega)$ such that $G \in \Gamma_d$ and a representation $\phi : G \to \mathrm{GL}(V)$, one can solve the following problems in time polynomial in $|\Omega|$, n, q and e.*

(i) *Given a vector $v \in V$, find the vector stabilizer $\mathrm{C}_G(v)$.*

(ii) *Given a subspace $W \leq V$, find the subspace stabilizer $\mathrm{N}_G(W)$.*

In this theorem, the characteristic q of the underlying field k is involved in the running time. This parametrization enables us to call Rónyai's deterministic algorithm for finding invariant subspaces from [47, §5] (while, if we appeal to his *Las Vegas* version instead, we can accomplish the same task in Las Vegas polynomial time in $|\Omega|$, n, $\log q$ and e, replacing q by $\log q$). For our applications to the problem of finding normalizers in permutation groups, all of the parameters n, q and e of V will be polynomially bounded in $|\Omega|$.

We remark that, more generally, Theorem 1.4 and its underlying divide-and-conquer machinery, which will be presented in §5, also apply to *manageable groups*, i.e., Γ_d groups with polynomial-time procedures for constructive membership-testing (see Luks [34] and Miyazaki [43]). Indeed, §5 fills necessary details on the divide-and-conquer machinery for solvable matrix groups that were only outlined in [34, §6] (in particular, §5.2 clarifies an important reduction in [34, §6.2] and [43, §IV.2]). While we will often reference and employ other basic results proven in [34] in the present paper, such references will be limited to those in the earlier sections, namely, [34, §§1–4].

In a future paper [37], the authors hope to elaborate on some analogues of the results herein for matrix groups in Γ_d.

Finally, we emphasize that our goal is a clear resolution of the polynomial-time issue. With this in mind, in several places, we have striven 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 (see [37], [43]).

We will appeal to the *Classification of the Finite Simple Groups* (CFSG) through several subroutines to prove Theorems 1.1–1.4. We will mark key results that depend on CFSG by "(CFSG)".

Organization of the paper In §2, we will review basic definitions and notation. In §3, we will recall elements of the known polynomial-time library for permutation groups, and we will further expand the library to include several subroutines needed for the normalizer algorithm. In §4, we will describe the overall architecture of the main algorithm and prove Theorems 1.1–1.3. Then, in §5, we will describe in detail the key subroutine for finding stabilizers of vectors and subspaces to prove Theorem 1.4.

The development requires statements of a large number of problems; with the exception of Problems 1–4 for general groups, all of these are shown to be in polynomial time. To facilitate searches for cited subroutines, we have numbered the problems and, where necessary, followed the problem statements with propositions (or lemmas or corollaries) that establish polynomial-time complexity.

2 Preliminaries

For the reader's convenience, we first review some basic definitions and notation of permutation and linear representations. We also summarize some standard conventions for computing with groups. Our general reference on finite group theory is [2].

2.1 Permutation representations

We denote by $\mathrm{Sym}(\Omega)$ the symmetric group of all permutations on an n-element set Ω or by S_n if the underlying set does not require explication. Throughout this subsection, let a group G act on such a set Ω via a homomorphism $\pi : G \to \mathrm{Sym}(\Omega)$. We call n the *degree* of π; if $G \leq \mathrm{Sym}(\Omega)$, where π is regarded as the natural injection, then we call n the *degree* of G.

For $g \in G$, we denote the images of $\alpha \in \Omega$ and $\Delta \subseteq \Omega$ under $\pi(g)$ by α^g and Δ^g, respectively. The *orbit* of $\alpha \in \Omega$ under G is $\alpha^G := \{\alpha^g \mid g \in G\}$. If Ω itself forms a single orbit, then we call G (as well as π) *transitive*.

For $\alpha \in \Omega$, the *point stabilizer* of α in G is the subgroup $G_\alpha := \{g \in G \mid \alpha^g = \alpha\}$. For $\Delta \subseteq \Omega$, the *pointwise stabilizer* of Δ in G is the subgroup $G_\Delta := \{g \in G \mid \delta^g = \delta \text{ for all } \delta \in \Delta\}$, whereas the *set stabilizer* of Δ in G is the subgroup $\mathrm{Stab}_G(\Delta) := \{g \in G \mid \Delta^g = \Delta\}$. If Ω possesses a group structure with G acting as automorphisms, then we often write $\mathrm{C}_G(\alpha)$, $\mathrm{C}_G(\Delta)$ and $\mathrm{N}_G(\Delta)$ to denote G_α, G_Δ and $\mathrm{Stab}_G(\Delta)$, respectively. For $x \in \mathrm{Sym}(\Omega)$, the *support* of x is $\mathrm{supp}(x) := \{\alpha \in \Omega \mid \alpha^x \neq \alpha\}$, whereas the *fixed points* of x is $\mathrm{fix}(x) := \{\alpha \in \Omega \mid \alpha^x = \alpha\}$. We also write $\mathrm{fix}(G) := \{\alpha \in \Omega \mid \alpha^g = \alpha \text{ for all } g \in G\}$; again, if Ω possesses a group structure with G acting as automorphisms, then we often write $\mathrm{C}_\Omega(G) := \mathrm{fix}(G)$.

For G-invariant $\Delta \subseteq \Omega$ (that is, $\Delta^g = \Delta$ for all $g \in G$), we call the restriction of π to Δ, denoted by $\pi|_\Delta : G \to \mathrm{Sym}(\Delta)$, the *constituent* of π on Δ and its image $G^\Delta := \pi|_\Delta(G)$ the *constituent* of G on Δ; if Δ is an orbit, then we call both $\pi|_\Delta$ and G^Δ *transitive constituents*.

Assume that G is transitive on Ω. A subset $\Delta \subseteq \Omega$ is a *block* if, for each $g \in G$, either $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$. We call the set of all images of a block, forming a G-invariant partition of Ω, a *system of blocks*. If G has no system of blocks other than the partition into singletons and the partition with Ω itself, then we call G (as well as π) *primitive*.

2.2 Linear representations

Let k be a field and V be an n-dimensional vector space over k. We denote by $\mathrm{End}_k(V)$ the algebra of k-linear endomorphisms of V and by $\mathrm{GL}(V) = \mathrm{GL}(V, k)$ the general linear group of all units of $\mathrm{End}_k(V)$. Throughout this subsection, let a group G act on V via a homomorphism $\phi : G \to \mathrm{GL}(V)$. We say V is a kG-module. We call n the *degree* of ϕ over k; if $G \leq \mathrm{GL}(V)$, where ϕ is regarded as the natural injection, then we call n the *degree* of G over k. Since $\mathrm{GL}(V) \leq \mathrm{Sym}(V)$, the notation of permutation representations applies to G.

A subspace W of V is a *kG-submodule* if $W^g = W$ for all $g \in G$. If the only kG-submodules are 0 and V, then we call V (as well as G and ϕ) *irreducible*. If V is a direct sum of irreducible kG-submodules, then we call V (as well as G and ϕ) *completely reducible*.

Suppose that V is completely reducible. For an irreducible kG-submodule W of V, the *kG-homogeneous component of V determined by W* is the kG-submodule generated by all irreducible kG-submodules of V that are kG-isomorphic to W (here, for kG-modules X, Y, a *kG-homomorphism* is a k-linear map $\psi : X \to Y$ commuting with the actions of G in the sense that $\psi(x^g) = \psi(x)^g$ for all $x \in X$ and $g \in G$). The (canonical) *isotypic decomposition* of V is the direct sum of its kG-homogeneous components. If V itself forms one kG-homogeneous component, then we call V (as well as G and ϕ) *kG-homogeneous*.

If $V = V_1 \oplus \cdots \oplus V_m$, $m \geq 2$, and G permutes $V_1, \ldots, V_m$ as a transitive permutation group of degree m under ϕ, then we call $\mathcal{V} := \{V_1, \ldots, V_m\}$ a *system of imprimitivity*. If the induced permutation representation of G on $\mathcal{V}$ is primitive, then we call $\mathcal{V}$ a *minimal system of imprimitivity*. If V is an irreducible kG-module but has no system of imprimitivity, then we call V (as well as G and ϕ) *primitive*.

Let $f : G \to V$ be a function. If $f(gh) = f(g)^h + f(h)$ for all $g, h \in G$, then we call f a *1-cocycle*. This also means that f is a 1-cocycle if and only if the extension of ϕ to $\phi_f : G \to \mathrm{GL}(V \oplus k)$ defined by

$$(v, a)^{\phi_f(g)} := (v^g + af(g), a)$$

for $v \in V$, $a \in k$ and $g \in G$ is a homomorphism. The set of all 1-cocycles from G to V, denoted by $\mathrm{Z}^1(G, V)$, forms a kG-module via $(f + f')(g) := f(g) + f'(g)$, $(af)(g) := a(f(g))$ and $f^h(g) := f(g^{h^{-1}})^h$ for $f, f' \in \mathrm{Z}^1(G, V)$, $g, h \in G$ and $a \in k$.

An element e of $\mathrm{End}_k(V)$ is *unipotent* if all characteristic values of e are equal to $1 \in k$. A subgroup G of $\mathrm{GL}(V)$ is *unipotent* if all elements of G are unipotent; if $\mathrm{char}\, k = p$, then G is unipotent if and only if G is a p-group.

2.3 Computational conventions

We summarize some standard computational conventions in the generality of abstract finite groups e-quipped with polynomial-time procedures to compute products and inverses of elements (for the related abstract notion of *black-box groups*, see, e.g., [49, Chapter 2]).

We again emphasize that, for both input and output, groups ares specified by generators, unless stated otherwise. In this subsection, assume that we are given a group $G = \langle S \rangle$.

All algorithms identifying group elements are constructive and computed via the following notion of a straight-line program: For $g \in G$, a *straight-line program to reach g from S* is a sequence $(g_1, \ldots, g_\ell)$ such that $g_\ell = g$ and, for $i = 1, \ldots, \ell - 1$, one of the following holds:

$g_i \in S$,
$g_i = g_j^{-1}$ for some $j < i$, or
$g_i = g_j g_k$ for some $j, k < i$.

Consider a homomorphism $\pi : G \to M$. In computational situations, π is specified by the image $\pi(s)$ of each $s \in S$, and the image $\pi(g)$ of $g \in G$ is computed via a straight-line program to reach g from S. For a representation $\phi : G \to \mathrm{GL}(V)$, where V is a finite dimensional vector space over a field k, a 1-cocycle $f : G \to V$ is specified by the image $f(s)$ of each $s \in S$. The image $f(g)$ of $g \in G$ is then computed via

$$(f(g), 0) := (0, 1)^{\phi_f(g)} - (0, 1),$$

where $(0,1)^{\phi_f(g)}$ is evaluated using a straight-line program to reach g from S.

Consider a coset Gx. In computational situations, Gx is specified by a pair consisting of generators for G and any coset representative. A *subcoset* of Gx is a subset of Gx that is either empty or a coset of a subgroup of G. Certain subcosets are defined by predicates that can be easily evaluated (for example, consider, for $G \leq \mathrm{Sym}(\Omega)$ and $\Delta_1, \Delta_2 \subseteq \Omega$, the *subset transporter* $\mathrm{Trans}_G(\Delta_1, \Delta_2) := \{g \in G \mid \Delta_1^g = \Delta_2\}$). In general, for a subcoset $Hy \subseteq Gx$ (using the notation Hy even if it may be empty), when generators for H and a coset representative are not necessarily available at hand, if we are given a polynomial-time procedure to determine, for any given $z \in Gx$, whether $z \in Hy$, then we say Hy is (*polynomial-time*) *recognizable*.

The length of a subgroup series is often essential to polynomial running time of algorithms. In S_n, by Lagrange's theorem, a series of subgroups has length at most $\log n! = O(n \log n)$, and this bound will be sufficient for our purposes (though, for optimum $O(n)$ bounds, see [5], [12]).

3 Polynomial-time library

In §§3.1–3.4, we will review relevant portions of the known polynomial-time library for permutation groups. In §§3.5–3.7, we will introduce some new additional tools. For further details on §§3.1–3.4, we refer to [25], [35].

3.1 Basic tools

We first summarize some of the most fundamental results (see [17], [24], [33], [35], [49], [50]).

Theorem 3.1 *Given $G = \langle S \rangle \leq \mathrm{Sym}(\Omega)$, in polynomial time one can solve the following problems.*

(i) *Given $\alpha \in \Omega$, list the orbit α^G and test the transitivity of G.*

(ii) *Test whether G is primitive and, if not, find a non-trivial block system.*

(iii) *Given a recognizable subgroup H of G such that $|G : H| = O(|\Omega|^c)$ for a constant $c > 0$ (specified by a polynomial-time procedure to test, for given $g \in G$, whether $g \in H$), find generators for H and a complete set of coset representatives for H in G.*

(iv) *Find $|G|$.*

(v) *Given $x \in \mathrm{Sym}(\Omega)$, test whether $x \in G$ and, if so, exhibit a straight-line program to reach x from S.*

(vi) *Given a homomorphism $\pi : G \to \mathrm{Sym}(\Omega')$ (defined on generators),*

  (a) *find $\mathrm{Ker}\,\pi$,*

  (b) *for given $M \leq \pi(G)$, find $\pi^{-1}(M) = \{g \in G \mid \pi(g) \in M\}$.*

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

(viii) *Given $N \leq \mathrm{Sym}(\Omega)$ such that N is normalized by G,*

  (a) *find $\mathrm{C}_G(N)$ (including, in particular, $\mathrm{Z}(G)$),*

(b) *find* $G \cap N$,

(c) *for given* $x \in GN$, *find* $g \in G$ *and* $n \in N$ *such that* $x = gn$.

(ix) *Find a composition series of* G.

(x) *Find a chief series of* G.

(xi) (CFSG) *Given a prime* p *dividing* $|G|$, *find a Sylow* p*-subgroup of* G*; furthermore, given such subgroups* P_1 *and* P_2 *of* G, *find* $g \in G$ *such that* $P_1^g = P_2$. □

It is well-known that Problems (i), (ii) can be solved easily by elementary combinatorial methods (see, e.g., [35, 3.1, 3.2]). Problems (iii)–(v) were first shown to be in polynomial time in [17] using a variant of Sims's method [50].

For Problem (vi)(a), under the induced action $\phi : G \to \mathrm{Sym}(\Omega \cup \Omega')$, it suffices to find the pointwise stabilizer of Ω' in $\phi(G)$ via Problem (iii) (see also [33, Lemma 1.1(8)]). For Problem (vi)(b), given $M = \langle X \rangle$, it is sufficient to find a small set $Y \subseteq G$ such that $\pi(Y) = X$ from straight-line programs to reach $x \in X$ from $\pi(S)$ via Problem (v), for $\pi^{-1}(M) = \langle Y \cup \mathrm{Ker}\,\pi \rangle$.

Problem (vii) is an easy extension of Problem (v) (see, e.g., [35, 3.12]), and Problem (viii)(b) is an extension of Problem (iii) (see, e.g., [35, Proposition 7.1]). To solve Problem (viii)(c), given $N = \langle T \rangle$, it suffices to form a straight-line program P to reach x from $S \cup T$, for a factor g of x may be obtained by substituting in P each occurrence of $t \in T$ by $1 \in \mathrm{Sym}(\Omega)$.

Problem (ix) was first shown in to be in polynomial time in [33]. A polynomial-time algorithm for Problem (viii)(a) was also given originally in [33, §3] as one of the key subroutines for Problem (ix) (cf. [35, Proposition 7.3]). It is an application of [33], [47] that Problem (x) is in polynomial time (see, e.g., [25, §4]).

Polynomial-time solutions to Problem (xi) are due to the seminal work of Kantor [24] and extensively use CFSG.

3.2 The quotient-group thesis

As suggested in the quotient-group thesis in [25], all known problems that are in polynomial time for permutation groups remain in polynomial time when applied to quotients of permutation groups. For our purposes, we essentially require the ability to solve in quotient groups only the most fundamental Problems (iv)–(viii) of Theorem 3.1.

Polynomial-time solutions to the quotient-group versions of Problems (iv)–(vii), (viii)(b), (c) are immediate from Theorem 3.1(iv)–(vii), (viii)(b), (c), respectively.(ii) However, for Problem (viii)(a), despite the elementary nature of the method for Theorem 3.1(viii)(a), as far as we know, the justification of the thesis is not routine. The next lemma from [25, §6] involves construction of Sylow subgroups via Theorem 3.1(xi) and thus must appeal to CFSG (cf. [35, §8]).

Throughout this paper, a quotient group $\mathbf{G} := G/K$, where $K \trianglelefteq G \leq \mathrm{Sym}(\Omega)$, is specified by a pair consisting of generating sets for G and K, and an element $\mathbf{g} \in \mathbf{G}$ is specified by a coset representative $g \in G$ such that $\mathbf{g} = Kg$.

Lemma 3.2 (Kantor–Luks)(CFSG) *For* $\mathbf{G} = G/K$, *where* $K \trianglelefteq G \leq \mathrm{Sym}(\Omega)$, *given* $\mathbf{H}, \mathbf{N} \leq \mathbf{G}$ *such that* $\mathbf{H}$ *normalizes* $\mathbf{N}$, *one can find* $\mathrm{C}_{\mathbf{H}}(\mathbf{N})$ *(including, in particular,* $\mathrm{Z}(\mathbf{H})$*) in polynomial time.* □

(ii) In the quotient-group version of Problem (v), we are given an element and a subgroup of a quotient group in $\mathrm{Sym}(\Omega)$. Likewise, in that of Problem (vi), we are given a homomorphism from a quotient group in $\mathrm{Sym}(\Omega)$ to a quotient group in $\mathrm{Sym}(\Omega')$.

3.3 Centralizers and normalizers in $\mathrm{Sym}(\Omega)$

In the following, we discuss some polynomial-time tools for finding centralizers and special instances of normalizers in $\mathrm{Sym}(\Omega)$.

We begin with

Problem 5
Given: $G \leq \mathrm{Sym}(\Omega)$.
Find: $\mathrm{C}_{\mathrm{Sym}(\Omega)}(G)$.

The following is a well-known fact (see, e.g., [49, §6.1.2]).

Lemma 3.3 *Problem* 5 *is in polynomial time.* □

Next, we consider

Problem 6
Given: $E \leq \mathrm{Sym}(\Omega)$ *such that* E *is elementary abelian and isomorphic to a direct product of its transitive constituents.*
Find: $\mathrm{N}_{\mathrm{Sym}(\Omega)}(E)$.

Lemma 3.4 *Problem* 6 *is in polynomial time.*

Proof: Let Δ_i, $i = 1, \ldots, \ell$, be the orbits of E so that $E \cong E^{\Delta_1} \times \cdots \times E^{\Delta_\ell}$ (i.e., for each i, the action of E^{Δ_i} on Δ_i is regular).

For $i = 1, \ldots, \ell$, let $N_i := \{x \in \mathrm{N}_{\mathrm{Sym}(\Omega)}(E) \mid \mathrm{supp}(x) \subseteq \Delta_i\}$ and $C_i := \mathrm{C}_{\mathrm{Sym}(\Omega)}(E) \cap N_i$. Notice now that, if we regard each E^{Δ_i} as a vector space, then each $N_i/C_i \cong \mathrm{GL}(E^{\Delta_i})$. With this correspondence in hand, we construct, for $i = 1, \ldots, \ell$, a small set (e.g., of size 2) T_i for which $N_i = \langle T_i, C_i \rangle$ (here, we construct T_i only, though C_i and thus N_i are computable in polynomial time).

It now remains to find, for each pair of orbits Δ_i and Δ_j of the same length, a transposition $x_{ij} \in \mathrm{N}_{\mathrm{Sym}(\Omega)}(E)$ that switches Δ_i and Δ_j, leaving the remaining points of Ω fixed. Indeed, $\mathrm{C}_{\mathrm{Sym}(\Omega)}(E)$ includes such transpositions since, for each such pair Δ_i and Δ_j, the regular E-action on Δ_i is equivalent to that on Δ_j. Thus, we return $\langle T_1, \ldots, T_\ell, \mathrm{C}_{\mathrm{Sym}(\Omega)}(E) \rangle = \mathrm{N}_{\mathrm{Sym}(\Omega)}(E)$. □

Remark Problem 6 is not known to be in polynomial time if we remove the assumption that G is isomorphic to a direct product of its transitive constituents. In fact, without such an assumption, ISO is reducible to this problem (see [35, §10]).

Via Problem 5, the following two additional problems are also in polynomial time.

Problem 7
Instance: $G, H \leq \mathrm{Sym}(\Omega)$ *and an isomorphism* $\pi : G \xrightarrow{\sim} H$ *(defined on generators of* G*).*
Question: *Is there* $x \in \mathrm{Sym}(\Omega)$ *such that* $\pi(g) = g^x$ *for all* $g \in G$*? If so, exhibit such* x*.*

Lemma 3.5 *Problem* 7 *is in polynomial time.*

Proof: Consider an action $\phi : G \to \mathrm{Sym}(\Omega \times \{1,2\})$ defined by $(\alpha, 1)^{\phi(g)} := (\alpha^g, 1)$ and $(\alpha, 2)^{\phi(g)} := (\alpha^{\pi(g)}, 2)$ for $\alpha \in \Omega$ and $g \in G$. Via Problem 5, we find $C := \mathrm{C}_{\mathrm{Sym}(\Omega \times \{1,2\})}(\phi(G))$; here, C acts on the set of the orbits of $\phi(G)$, say, $\mathcal{D} := \{\Delta_1, \ldots, \Delta_m\}$ via $\psi : C \to \mathrm{Sym}(\mathcal{D})$. Then there is an appropriate element $x \in \mathrm{Sym}(\Omega)$ if and only if, for each orbit Δ_i, exactly half of the sets in $\Delta_i^{\psi(C)}$ lie in $\Omega \times \{1\}$

(see, e.g., [49, §6.1.2]). If this holds, it is easy to find $y \in C$ such that $(\Omega \times \{1\})^y = \Omega \times \{2\}$ (in fact, for each orbit Δ_i, C induces the symmetric group on $\Delta_i^{\psi(C)}$). The desired element x is then defined by $(\alpha, 1)^y = (\alpha^x, 2)$. □

Remark In general, for $G = \langle S \rangle \leq \mathrm{Sym}(\Omega)$ and $M \leq \mathrm{Sym}(\Omega')$, it is easy to determine whether a given function $\pi : S \to M$ is extendible to a homomorphism (resp. isomorphism) $G \to M$ (cf. [25, §4]). To see this, let $D := \langle (s, \pi(s)) \mid s \in S \rangle \leq \mathrm{Sym}(\Omega) \times \mathrm{Sym}(\Omega')$. Then π extends to a homomorphism (resp. isomorphism) if and only if $|D| = |G|$ (resp. $|D| = |G| = |M|$).

Problem 8
Instance: $G \leq \mathrm{Sym}(\Omega)$ *and* $\sigma \in \mathrm{Aut}(G)$ (*defined on generators*).
Question: *Is* $\sigma \in \mathrm{Inn}(G)$*? If so, exhibit* $a \in G$ *such that* $g^a = g^\sigma$ *for all* $g \in G$.

Lemma 3.6 *Problem* 8 *is in polynomial time.*

Proof: We first find, via Problem 7, $x \in \mathrm{Sym}(\Omega)$ such that $g^x = g^\sigma$ for all $g \in G$. We then test whether $x \in G\mathrm{C}_{\mathrm{Sym}(\Omega)}(G)$, and if so, using Theorem 3.1(viii)(c), find $a \in G$ and $c \in \mathrm{C}_{\mathrm{Sym}(\Omega)}(G)$ such that $x = ac$. It suffices to return a. □

Remark Lemma 3.6 answers an open question of Kantor and Luks posed in [25, §13].

3.4 Tools for Γ_d

In the class Γ_d, there are polynomial-time solutions to a number of permutation-group problems that resemble ISO. The following results from [32] concerning Problems 1–3 are particularly well-known (cf. [35, Corollary 6.4]).

Theorem 3.7 (Luks) *Given* $G \leq \mathrm{Sym}(\Omega)$ *such that* $G \in \Gamma_d$*, in polynomial time one can solve the following problems.*

(i) *Given* $\Delta \subseteq \Omega$*, find* $\mathrm{Stab}_G(\Delta)$.

(ii) *Given* $H \leq \mathrm{Sym}(\Omega)$*, find* $G \cap H$.

(iii) *Given* $H \leq \mathrm{Sym}(\Omega)$*, find* $\mathrm{C}_G(H)$.

In fact, Theorem 3.7 was first proved in [32] under the stronger assumption that *all* composition factors, both abelian and nonabelian, were in S_d. With a view toward extending the applicability of the methods, Babai, Cameron and Pálfy subsequently derived the following important result in [6, Theorem 1.1].

Theorem 3.8 (Babai–Cameron–Pálfy) *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* $|G| = O(n^{f(d)})$. □

Remark (i) An earlier version of Theorem 3.8 was also proved in [32] under the assumption that all composition factors were in S_d, and this sufficed for the graph-isomorphism application. In fact, [6] weakened the restriction on composition factors even further than our assumption in Theorem 3.8; specifically, [6] deals with A_d*-free* groups, in which no section (i.e., quotient of any subgroup) is isomorphic to A_d (cf. [46]). However, we require the present definition of Γ_d to derive another crucial polynomial bound in linear groups in Proposition 5.7. Our definition of Γ_d is also the same as that of [35].

(ii) The function $f(d)$ has been investigated further (see [7]). By [45], it was improved from $O(d \log d)$ to $O(d)$ for A_d-free groups (cf. [31]). **Divide and conquer using orbits and blocks.** The divide-and-conquer paradigm that motivated Theorem 3.8 applies to problems that ask for construction of a recognizable subcoset of a given coset Gx in $X \leq \mathrm{Sym}(\Omega)$, where $G \in \Gamma_d$, equipped with a representation $X \to \mathrm{Sym}(\Sigma)$ and a G-invariant subset $\Phi \subseteq \Sigma$ such that the following hold:

(1) *Recursive property*. Given proper G-invariant subsets $\Phi_1, \Phi_2 \subset \Phi$ such that $\Phi = \Phi_1 \dot\cup \Phi_2$, the problem is recursively reducible to induced problems on Φ_1 and Φ_2 in time polynomial in $|\Omega|$ and $|\Sigma|$.

(2) *Base property*. If Φ is a singleton, then the problem is solvable in time polynomial in $|\Omega|$ and $|\Sigma|$.

We illustrate this paradigm by recalling the proof of Theorem 3.7. The essential steps are concentrated in the method for

Problem 9
Given: $G, H \leq \mathrm{Sym}(\Omega)$ *such that* $G \in \Gamma_d$ *and* $x \in \mathrm{Sym}(\Omega)$.
Find: $Gx \cap H$.

Proposition 3.9 *Problem* 9 *is in polynomial time.*

Proof: Consider the coordinatewise action of $Gx \times H$ on $\Omega \times \Omega$ and $\Delta := \mathrm{Diag}(\Omega \times \Omega)$. To solve Problem 9, it then suffices to find $\mathrm{Stab}_{Gx \times H}(\Delta) = \{(y, y) \mid y \in Gx \cap H\}$. To accommodate recursion, we consider, more generally, the following subcoset problem.

Let p_1 denote the first-coordinate projection map of $\mathrm{Sym}(\Omega) \times \mathrm{Sym}(\Omega)$. For $\Gamma \subseteq \Omega$, we write $\mathrm{Diag}(\Gamma, \Omega) := \{(\alpha, \alpha) \mid \alpha \in \Gamma\}$.

Given: $G \leq \mathrm{Sym}(\Omega) \times \mathrm{Sym}(\Omega)$ *such that* $p_1(G) \in \Gamma_d$, $x \in \mathrm{Sym}(\Omega) \times \mathrm{Sym}(\Omega)$ *and* $p_1(G)$*-invariant* $\Phi \subseteq \Omega$.
Find: $\mathcal{C}(Gx, \Phi) := \{y \in Gx \mid \mathrm{Diag}(\Phi, \Omega)^y = \mathrm{Diag}(\Phi^{p_1(x)}, \Omega)\}$.

If not empty, $\mathcal{C}(Gx, \Phi)$ is a coset of $\mathrm{Stab}_G(\mathrm{Diag}(\Phi, \Omega))$. We now solve this problem under the divide-and-conquer paradigm. We perform two levels of divide-and-conquer maneuvers under the G-action on Φ via p_1, involving the decomposition of Φ into orbits and, in the transitive case, the decompositions of Φ into blocks and G into cosets. In particular, we consider the following three (two recursive and one base) cases.

Intransitive case If G acts intransitively on Φ, then we first find proper G-invariant subsets $\Phi_1, \Phi_2 \subset \Phi$ such that $\Phi = \Phi_1 \dot\cup \Phi_2$. Since $\mathcal{C}(Gx, \Phi) = \mathcal{C}(\mathcal{C}(Gx, \Phi_1), \Phi_2)$, it is sufficient to solve recursively for, if not empty, $Hy := \mathcal{C}(Gx, \Phi_1)$ and then $\mathcal{C}(Hy, \Phi_2)$.

Transitive case If G acts transitively on Φ, where $|\Phi| > 1$, then we find a minimal block system $\boldsymbol{\Phi} := \{\Phi_1, \ldots, \Phi_m\}$ of Φ and decompose G into cosets of the kernel K of the G-action on $\boldsymbol{\Phi}$, say, $G = Ky_1 \dot\cup \cdots \dot\cup Ky_\ell$ for some $y_1, \ldots, y_\ell \in G$. Since K acts intransitively on Φ, the problem is reduced to ℓ instances of the intransitive case of finding $\mathcal{C}(Ky_1x, \Phi), \ldots, \mathcal{C}(Ky_\ell x, \Phi)$. Of ℓ solutions to these instances, nonempty ones are cosets $Lz_1, \ldots, Lz_k$ of the same subgroup $L := \mathrm{Stab}_K(\mathrm{Diag}(\Phi, \Omega))$. These cosets may easily be pasted together to form a single coset of $\mathrm{Stab}_G(\mathrm{Diag}(\Phi, \Omega))$, for $Lz_1 \dot\cup \cdots \dot\cup Lz_k = \langle L, \{z_i z_1^{-1}\}_{i=2,\ldots,k}\rangle z_1$.

Base case The above recursion bottoms out when G acts primitively on Φ (i.e., when $\Phi_1, \ldots, \Phi_m$ become singletons). If $\Phi = \{\alpha\}$ and $x = (x_1, x_2)$, we return either $\emptyset$ or $\{(g_1, g_2) \in G \mid \alpha^{g_2} = \alpha^{x_1 x_2^{-1}}\}x = \mathcal{C}(Gx, \Phi)$.

Timing analysis In the intransitive case, we solve sequentially on Φ_1 and Φ_2, where $|\Phi_1| + |\Phi_2| = |\Phi|$. In the transitive case, notice that, by Theorem 3.8, the kernel of the G-action on a minimal block system has polynomial index in G; that is, $\ell = O(m^c)$ for a constant $c > 0$. Therefore, the original problem on Φ is reduced to $O(m^{c+1})$ problems on subsets of size $|\Phi|/m$. By the results of §3.1, these reductions are in polynomial time. Hence, this algorithm runs in polynomial time. □

Via Problem 9, we can now solve Problem 1 in Γ_d. In fact, we can also solve

Problem 10
Given: $G \leq \mathrm{Sym}(\Omega)$ *such that* $G \in \Gamma_d$ *and* $\Delta_1, \Delta_2 \subseteq \Omega$.
Find: $\mathrm{Trans}_G(\Delta_1, \Delta_2) = \{g \in G \mid \Delta_1^g = \Delta_2\}$.

Corollary 3.10 *Problem* 10 *is in polynomial time.*

Proof: If $|\Delta_1| = |\Delta_2|$, then we find $x \in \mathrm{Sym}(\Omega)$ such that $\Delta_1^x = \Delta_2$ and, via Problem 9, $Gx^{-1} \cap \mathrm{Stab}_{\mathrm{Sym}(\Omega)}(\Delta_1)$. □

We now complete

Proof of Theorem 3.7: The assertions concerning Problems (i), (ii) are immediate from Proposition 3.9 and Corollary 3.10, so it remains to solve Problem (iii). For this, note that $\mathrm{C}_G(H) = G \cap \mathrm{C}_{\mathrm{Sym}(\Omega)}(H)$; that is, via Problems 5, 9, we have a polynomial-time solution to Problem (iii). □

Remark See [32, §3] for an illustration of the paradigm directly applied to Theorem 3.7(i).

Let $X = (\Omega, E)$ denote a *hypergraph* consisting of a set Ω and a collection $E \subseteq 2^{\Omega}$; here, we regard elements of Ω *vertices* and members of E *hyperedges*. For $G \leq \mathrm{Sym}(\Omega)$, under the induced action of G on 2^{Ω}, we consider the problem of finding the automorphism group of X in G.

Problem 11
Given: $G \leq \mathrm{Sym}(\Omega)$ *such that* $G \in \Gamma_d$ *and a hypergraph* $X = (\Omega, E)$.
Find: $\mathrm{Aut}_G(X) = \{g \in G \mid E^g = E\}$.

The following result is due to the work of Miller [42]. We include a proof in our notation as an additional illustration of the divide-and-conquer paradigm.

Lemma 3.11 (Miller) *Problem* 11 *is in polynomial time.*

Proof: For $\Phi \subseteq \Omega$, we define $E_\Phi := \{\Phi \cap \Delta \mid \Delta \in E\}$. To accommodate recursion, we consider the following generalization.

Given: $G \leq \mathrm{Sym}(\Omega)$ *such that* $G \in \Gamma_d$, $x \in \mathrm{Sym}(\Omega)$, G*-invariant* $\Phi \subseteq \Omega$ *and* $E \subseteq 2^{\Omega}$.
Find: $\mathcal{C}(Gx, \Phi, E) := \{y \in Gx \mid (E_\Phi)^y = E_{\Phi^x}\}$.

We note that, if not empty, $\mathcal{C}(Gx, \Phi, E)$ is a coset of $\mathrm{Stab}_G(E_\Phi)$.

To solve this problem, we apply the divide-and-conquer paradigm using the action of G on Φ, but the intransitive case requires some additional work: First, given proper G-invariant subsets $\Phi_1, \Phi_2 \subset \Phi$

such that $\Phi = \Phi_1 \dot{\cup} \Phi_2$, we find, via recursion, $\mathcal{C}(\mathcal{C}(Gx, \Phi_1, E), \Phi_2, E)$. If not empty, the result of this recursion is a coset Hy, where $H = \mathrm{Stab}_G(E_{\Phi_1}) \cap \mathrm{Stab}_G(E_{\Phi_2})$. Here, observe that, for each $\Delta \in E$, each element of Hy need not map $\Phi_1 \cap \Delta$ and $\Phi_2 \cap \Delta$ into the same member of E. Thus, we perform the following to find $\mathcal{C}(Gx, \Phi, E)$. We form $D := \{(\Phi_1 \cap \Delta, \Phi_2 \cap \Delta) \mid \Delta \in E\} \subseteq E_{\Phi_1} \times E_{\Phi_2}$ and $D' := \{(\Phi_1^x \cap \Delta, \Phi_2^x \cap \Delta) \mid \Delta \in E\} \subseteq E_{\Phi_1^x} \times E_{\Phi_2^x}$. Under the induced action of H on $E_{\Phi_1} \times E_{\Phi_2}$, we now find $\mathrm{Trans}_H(D, D'^{y^{-1}}) = \{h \in H \mid D^{hy} = D'\}$ via Problem 10.

In the base case in which Φ is a singleton, we simply compare E_Φ against E_{Φ^x} and return either Gx or $\emptyset$. □

We need the following extension of Problem 11.

Problem 12
Given: $G \leq \mathrm{Sym}(\Omega)$ *such that* $G \in \Gamma_d$ *and* $\mathcal{E} \subseteq 2^{2^\Omega}$.
Find: $\mathrm{Stab}_G(\mathcal{E})$.

Lemma 3.12 *Problem* 12 *is in polynomial time.*

Proof: To solve this problem, we first form $E' := \bigcup_{E \in \mathcal{E}} E \subseteq 2^\Omega$ and then, via Problem 11, find $H := \mathrm{Stab}_G(E')$. Here, notice that $\mathcal{E} \in 2^{E'}$. Under the induced action of H on E', we return, via Problem 11, $\mathrm{Stab}_H(\mathcal{E})$. □

3.5 Tools for linear representations

In this subsection, we consider several fundamental problems whose inputs are permutation groups equipped with linear representations. Throughout this subsection, we assume that V is an n-dimensional vector space over a finite field k of order q^e for some prime q.

We first begin with

Problem 13
Instance: $G \leq \mathrm{Sym}(\Omega)$ *and a representation* $\phi : G \to \mathrm{GL}(V)$.
Question: *Is* ϕ *irreducible? If not, exhibit a proper* kG*-submodule* $W < V$.

In [47], Rónyai considered problems in associative algebras and proved, as a byproduct of his main result,

Theorem 3.13 (Rónyai) *Problem* 13 *is solvable in time polynomial in* $|\Omega|$, n, q *and* e (*where* $V \cong \mathbb{F}_{q^e}^n$). □

Remark This theorem is used in finding a chief series of $G \leq \mathrm{Sym}(\Omega)$ in polynomial time (see, e.g., [25, §4]; see also Theorem 3.1(x)). As in the chief-series application, for any vector space V arising in the present work, all of the parameters n, q and e of V are polynomially bounded in $|\Omega|$. It is thus sufficient to achieve running time of linear-representation problems such as Problem 13 in time polynomial in $|\Omega|$, n, q and e (see also the remark following Theorem 5.1). Note, however, that $\log q$ suffices in the timings for Problems 14, 16, and we expect that these problems will have other applications.

Another fundamental problem is

Problem 14
Instance: $G \leq \mathrm{Sym}(\Omega)$, *a representation* $\phi : G \to \mathrm{GL}(V)$ *and* kG*-submodules* $W_1, W_2 \leq V$.
Question: *Is there a* kG*-isomorphism* $\psi : W_1 \xrightarrow{\sim} W_2$*? If so, exhibit such* ψ.

In general, Brooksbank and Luks [10] have shown that testing isomorphism of modules over an arbitrary field requires only a polynomial number of field operations (see also Chistov, Ivanyos and Karpinski [15], which suffices for our application over finite fields); in particular, we have

Lemma 3.14 *Problem* 14 *is solvable in time polynomial in* $|\Omega|$, n, $\log q$ *and* e (*where* $V \cong \mathbb{F}_{q^e}^n$). □

With Theorem 3.13 and Lemma 3.14 at hand, we next consider

Problem 15
Given: $G \leq \mathrm{Sym}(\Omega)$, *an irreducible representation* $\phi : G \to \mathrm{GL}(V)$ *and* $N \lhd G$.
Find: *a direct sum of the* kN*-homogeneous components* $V = V_1 \oplus \cdots \oplus V_m$ *whose summands form a system of imprimitivity for* G *or a report that* V *is* kN*-homogeneous.*

Lemma 3.15 *Problem* 15 *is solvable in time polynomial in* $|\Omega|$, n, q *and* e (*where* $V \cong \mathbb{F}_{q^e}^n$).

Proof: We apply the standard argument in the proof of Clifford's theorem (see, e.g., [2, 12.13]).

We first use Theorem 3.13 to find an irreducible kN-submodule $W \leq V$. Next, we find $1 = g_1, \ldots, g_r \in G$ such that $V = W^{g_1} \oplus \cdots \oplus W^{g_r}$ and form $\mathcal{V} := \{W^{g_1}, \ldots, W^{g_r}\}$.

We now appeal to Lemma 3.14 to partition $\mathcal{V}$ into isomorphism classes, say, $\mathcal{V}_1, \ldots, \mathcal{V}_m$; that is, we put W^{g_i} and W^{g_j} into the same class if they are kN-isomorphic. Unless $m = 1$, for each class $\mathcal{V}_i$, we add all its members to form a kN-homogeneous component V_i; hence, $V = V_1 \oplus \cdots \oplus V_m$, and G permutes the summands as a system of imprimitivity. If there is only one isomorphism class, then we report that V is kN-homogeneous. □

Now, we consider

Problem 16
Given: $G \leq \mathrm{Sym}(\Omega)$ *and a representation* $\phi : G \to \mathrm{GL}(V)$.
Find: $\mathrm{Ker}\, \phi$.

As far as we know, this problem cannot be solved efficiently via a sequential stabilization of a basis of V (for comparison, we note that Problem 18 hypothesizes that $G \in \Gamma_d$). Nevertheless, in [25, §4], with the help of Kantor's Sylow machinery and thus CFSG (Theorem 3.1(xi)), the problem was asserted to be in polynomial time; since the proof was omitted in [25] due to space limitations, we include it here.

Lemma 3.16 (CFSG) *Problem* 16 *is solvable in time polynomial in* $|\Omega|$, n, $\log q$ *and* e (*where* $V \cong \mathbb{F}_{q^e}^n$).

Proof: We reduce a given instance to a p-group case. For each prime p dividing $|G|$, we appeal to Theorem 3.1(xi) to find a single $P \in \mathrm{Syl}_p(G)$ and collect them in a common set $\mathcal{P}$. Since the kernel of ϕ is generated by the kernels of $\phi|_P$ for all $P \in \mathcal{P}$, it suffices to solve the problem for each $P \in \mathcal{P}$.

The remainder of the proof is in [34, §4.6], which in fact resolves, more generally, the problem for a solvable linear group G assuming the primes in $|G|$ are polynomially bounded. □

Remark (i) If we hypothesize that $G \in \Gamma_d$ in Problem 16, then the problem can be solved without invoking CFSG by using the method of Kantor and Taylor from [26], in place of Theorem 3.1(xi), to find Sylow subgroups.

(ii) We also note that, in general, if G and H are *manageable groups* (in the sense of [34]), i.e., groups with polynomial-time procedures for constructive membership-testing, for any homomorphism $\pi : G \to H$, finding $\mathrm{Ker}\, \pi$ and $\pi^{-1}(M)$ for given $M \leq \pi(G)$ is in polynomial time: To find $\mathrm{Ker}\, \pi$, we form a presentation $\langle X|R\rangle$ of $\pi(G)$ and pull back $\langle R^{F(X)}\rangle$. To find $\pi^{-1}(M)$ for given $M = \langle T\rangle$, it suffices to find $U \subseteq G$ such that $\pi(U) = T$ and return $\langle U \cup \operatorname{Ker}\pi\rangle = \pi^{-1}(M)$. For more on this, see [34, §4] (cf. Theorem 3.1(vi)).

Now, in general, for $N \trianglelefteq G \leq \mathrm{GL}(V)$, notice that $g \in G$ centralizes N if and only if g fixes all elements of the linear span $k[N]$ in $\mathrm{End}_k(V)$. So, Problem 16 is used to solve

Problem 17
Given: $G \leq \mathrm{Sym}(\Omega)$, $N \trianglelefteq G$ *and a representation* $\phi : G \to \mathrm{GL}(V)$.
Find: $C \trianglelefteq G$ *such that* $\phi(C) = \mathrm{C}_{\phi(G)}(\phi(N))$.

We next consider problems that resemble ISO in linear representations. As before, we restrict inputs to the class Γ_d to seek polynomial-time solutions. The following two problems are of our primary interest.

Problem 18
Given: $G \leq \mathrm{Sym}(\Omega)$ *such that* $G \in \Gamma_d$, *a representation* $\phi : G \to \mathrm{GL}(V)$ *and* $v \in V$.
Find: $\mathrm{C}_G(v) = \{g \in G \mid v^g = v\}$.

Problem 19
Given: $G \leq \mathrm{Sym}(\Omega)$ *such that* $G \in \Gamma_d$, *a representation* $\phi : G \to \mathrm{GL}(V)$ *and* $W \leq V$.
Find: $\mathrm{N}_G(W) = \{g \in G \mid W^g = W\}$.

To accommodate recursion, we first reformulate Problems 18, 19 to seek subcosets rather than subgroups. An equivalent subcoset-version of Problem 18 is naturally

Problem 20
Given: $G \leq \mathrm{Sym}(\Omega)$ *such that* $G \in \Gamma_d$, *a representation* $\phi : G \to \mathrm{GL}(V)$ *and* $v, w \in V$.
Find: $\mathrm{Trans}_G(v, w) = \{g \in G \mid v^g = w\}$.

In fact, Problem 20 is also equivalent to

Problem 21
Given: $G \leq \mathrm{Sym}(\Omega)$ *such that* $G \in \Gamma_d$, *a representation* $\phi : G \to \mathrm{GL}(V)$, $f \in \mathrm{Z}^1(G, V)$ *and* $v \in V$.
Find: $f^{-1}(v) = \{g \in G \mid f(g) = v\}$.

If not empty, $f^{-1}(v)$ is a coset of $\operatorname{Ker} f = f^{-1}(0)$. For given $v \in V$, let $f(x) := v^x - v$. Then $\operatorname{Ker} f = \mathrm{C}_G(v)$. Also, for another given $w \in V$, note that $f^{-1}(w - v)$ is the solution to Problem 20.

Conversely, to reduce Problem 21 to Problem 20, for given $f \in \mathrm{Z}^1(G, V)$, we consider the extension of ϕ to $\phi_f : G \to \mathrm{GL}(V \oplus k)$ defined by $(v, a)^g := (v^g + af(g), a)$ for $v \in V$, $a \in k$ and $g \in G$. With such ϕ_f, we have $f(g) = v$ if and only if $(v, 1)^g = (v^g + v, 1)$ for $v \in V$, $1 \in k$ and $g \in G$.

For Problem 19, we consider the following reformulation.

Problem 22
Given: $G \leq \mathrm{Sym}(\Omega)$ *such that* $G \in \Gamma_d$, *a representation* $\phi : G \to \mathrm{GL}(V)$ *and* $W_1, W_2 \leq V$.
Find: $\mathrm{Trans}_G(W_1, W_2) = \{g \in G \mid W_1^g = W_2\}$.

We will devote §5 to the proof of

Proposition 3.17 *Problems* 18–22 *are solvable in time polynomial in* $|\Omega|$, n, q *and* e (*where* $V \cong \mathbb{F}_{q^e}^n$).

To prove Proposition 3.17, we will first solve Problem 21 since it lends itself easily to a divide-and-conquer paradigm. As a corollary, we will immediately obtain solutions to Problems 18, 20. We will then solve Problems 19, 22 via Problem 20.

3.6 Automorphisms of characteristically simple groups

In this subsection, we will develop polynomial-time tools for constructing representations of the automorphism groups of direct products of isomorphic nonabelian simple groups.

We first recall some basic facts concerning permutation representations of group extensions. Suppose that a group H is an extension of a normal subgroup N by a group K. If N acts faithfully on a set Ω, then it induces a faithful action of H on $\Omega \times K$ in the following way: Consider the canonical homomorphism $* : H \to K$ whose kernel is N and fix a lifting of *, say, $\lambda : K \to H$ (i.e., $\lambda(k)^* = k$ for $k \in K$). For each $h \in H$, we define a function $f_h : K \to N$ by $f_h(k) := \lambda(k)h\lambda(kh^*)^{-1}$ for $k \in K$. Then, for $h \in H$ and $(\alpha, k) \in \Omega \times K$, we define $(\alpha, k)^h := (\alpha^{f_h(k)}, kh^*)$.

We now consider the following general problem.

Problem 23
Given: $G \leq \mathrm{Sym}(\Omega)$ *such that* $\mathrm{Z}(G) = 1$ *and* $\Sigma \subseteq \mathrm{Aut}(G)$ *such that* $\langle \mathrm{Inn}(G) \cup \Sigma \rangle = \mathrm{Aut}(G)$.
Find: *a faithful representation* $\pi : \mathrm{Aut}(G) \to \mathrm{Sym}(\Omega')$ (*where* $|\Omega'|$ *is polynomially bounded*).

More specifically, for $G = \langle S \rangle$, we assume that $\sigma \in \Sigma$ is defined on each $s \in S$ and that π performs the following: given $\sigma \in \mathrm{Aut}(G)$ defined on each $s \in S$, determine $\pi(\sigma)$ in $\mathrm{Sym}(\Omega')$.

Proposition 3.18 *Problem* 23 *is solvable in time polynomial in* $|\Omega|$, $|\Sigma|$ *and* $|\mathrm{Out}(G)|$.

Proof: We construct a faithful action of $\mathrm{Aut}(G)$ on $\Omega \times \mathrm{Out}(G)$ by applying the preceding method for general group extensions to 'H' $= \mathrm{Aut}(G)$, 'N' $= \mathrm{Inn}(G)$ and 'K' $= \mathrm{Out}(G)$. For this, it suffices to describe how to construct (i) a faithful action of $\mathrm{Inn}(G)$ on Ω and (ii) a multiplication table of $\mathrm{Out}(G)$, the canonical homomorphism $* : \mathrm{Aut}(G) \to \mathrm{Out}(G)$ and a lifting $\lambda : \mathrm{Out}(G) \to \mathrm{Aut}(G)$ in the desired time.

We recall that, for $G = \langle S \rangle$, given $\sigma, \tau \in \mathrm{Aut}(G)$ and $s \in S$, we can evaluate $s^{\sigma\tau} = (s^\sigma)^\tau$ by means of a straightline program from S to s^σ (cf. §2.3). We also recall that Problem 8, the problem of determining, for any given $\sigma \in \mathrm{Aut}(G)$, whether $\sigma \in \mathrm{Inn}(G)$, is in polynomial time.

For a faithful action of $\mathrm{Inn}(G)$ on Ω, since $\mathrm{Z}(G) = 1$, it suffices to construct an isomorphism $\phi : \mathrm{Inn}(G) \xrightarrow{\sim} G$. For this, given $\sigma \in \mathrm{Inn}(G)$, we use Problem 8 to determine $a \in G$ such that $g^a = g^\sigma$ for all $g \in G$ and set $\phi(\sigma) := a$.

For (ii), from Σ, again via Problem 8, we generate a complete set of coset representatives R for $\mathrm{Inn}(G)$ in $\mathrm{Aut}(G)$ and then construct a multiplication table for $\mathrm{Out}(G)$ indexed by elements a_ρ, $\rho \in R$. To construct $* : \mathrm{Aut}(G) \to \mathrm{Out}(G)$, for each $\sigma \in \Sigma$, we find $\rho \in R$ such that $\sigma\rho^{-1} \in \mathrm{Inn}(G)$ and define $\sigma^* := a_\rho$. To construct a lifting of *, we set $\lambda(a_\rho) := \rho$ for $a_\rho \in \mathrm{Out}(G)$. □

The preceding technique will be used when dealing with nonabelian simple groups. For this, we appeal to the following fact from CFSG: For every nonabelian simple group T, we have $|\mathrm{Out}(T)| = O(\log |T|)$ (see, e.g., [27]). Furthermore, if T is given as a permutation group, then, by [24], in polynomial time, one can find the "natural" representation of T, in which form the elements of $\mathrm{Out}(T)$ are easily listed: For the alternating groups A_n with $n \geq 5$, except for $n = 6$, it is an elementary fact that $\mathrm{Aut}(A_n) = S_n$ and thus $|\mathrm{Out}(A_n)| = 2$ (see, e.g., [52, I, 3.2.17]). For the simple groups of Lie type, the automorphisms adhere to a neatly-formulated pattern (more specifically, every automorphism is the product of an inner, a "diagonal", a "graph" and a "field" automorphism) (see, e.g., [13, Chapter 12], [21, §2.5]).

Consequently, for any nonabelian simple $T \leq \mathrm{Sym}(\Omega)$, $|\mathrm{Out}(T)|$ is polynomially bounded, and small $\Sigma \subseteq \mathrm{Aut}(T)$ such that $\langle \mathrm{Inn}(T) \cup \Sigma \rangle = \mathrm{Aut}(T)$ is computable in polynomial time. With this in mind, we consider

Problem 24
Given: $T \leq \mathrm{Sym}(\Omega)$ *such that* T *is nonabelian simple.*
Find: *a faithful representation* $\pi : \mathrm{Aut}(T) \to \mathrm{Sym}(\Omega')$ (*where* $|\Omega'|$ *is polynomially bounded*).

By Proposition 3.18, we have

Corollary 3.19 (CFSG) *Problem* 24 *is in polynomial time.* □

Remark It is also not difficult to directly solve Problem 24 using the well-known structures of the automorphisms of the simple groups. As indicated in Problem 23, the preceding approach offers a general method and applicable to any centerless groups whose outer automorphism groups are small.

Recall that, if $N \cong T^\ell$ for a nonabelian simple group T, then $\mathrm{Aut}(N) \cong \mathrm{Aut}(T) \wr S_\ell$. This isomorphism is used in the solution of

Problem 25
Given: $N \leq \mathrm{Sym}(\Omega)$, $T_1, \ldots, T_\ell \trianglelefteq N$ *such that* $N \cong T_1 \times \cdots \times T_\ell \cong T^\ell$ *for a nonabelian simple group* T*, and isomorphisms* $\tau_i : T_1 \xrightarrow{\sim} T_i$ (*defined on generators*) *for* $i = 2, \ldots, \ell$.
Find: *a faithful representation* $\pi : \mathrm{Aut}(N) \to \mathrm{Sym}(\Omega')$ (*where* $|\Omega'|$ *is polynomially bounded*).

Lemma 3.20 (CFSG) *Problem* 25 *is in polynomial time.*

Proof: We first construct an isomorphism $\phi : \mathrm{Aut}(N) \xrightarrow{\sim} \mathrm{Aut}(T) \wr S_\ell$. For this, given $\sigma \in \mathrm{Aut}(N)$, we perform the following: Let $a_\sigma \in S_\ell$ induced by the action of σ on $\{T_1, \ldots, T_\ell\}$ via the bijection $T_i \mapsto i$ for $i = 1, \ldots, \ell$. We now form $\alpha_\sigma \in \mathrm{Aut}(N)$ that permutes via a_σ the corresponding elements of $T_1, \ldots, T_\ell$ according to $\tau_2, \ldots, \tau_\ell$; that is, if $i^{a_\sigma} = j$, $1 \leq i \leq \ell$, $1 \leq j \leq \ell$, then $t_i^{\alpha_\sigma} := \tau_j(\tau_i^{-1}(t_i))$ for $t_i \in T_i$. Then $\sigma\alpha_\sigma^{-1}$ stabilizes each of $T_1, \ldots, T_\ell$; thus, $\sigma\alpha_\sigma^{-1} = \sigma_1 \cdots \sigma_\ell$ for some $\sigma_i \in \mathrm{Aut}(T_i)$ for $i = 1, \ldots, \ell$. Regarding $T = T_1 = \cdots = T_\ell$, we define $\phi(\sigma) := (\sigma_1, \ldots, \sigma_\ell)a_\sigma \in \mathrm{Aut}(T) \wr S_\ell$.
Via Problem 24, we next form a faithful representation $\psi : \mathrm{Aut}(T) \to \mathrm{Sym}(\Omega \times \mathrm{Out}(T))$. We paste together ϕ and ψ to form a faithful representation $\pi : \mathrm{Aut}(N) \to \mathrm{Sym}(\Omega \times \mathrm{Out}(T) \times \{1, \ldots, \ell\})$. □

We now apply the methods for Problems 24, 25 to solve

Problem 26
Given: $\mathbf{N} = N/K$ *for* $K \trianglelefteq N \leq \mathrm{Sym}(\Omega)$, $\mathbf{T}_1, \ldots, \mathbf{T}_\ell \trianglelefteq \mathbf{N}$ *such that* $\mathbf{N} \cong \mathbf{T}_1 \times \cdots \times \mathbf{T}_\ell \cong T^\ell$ *for a nonabelian simple group* T*, and isomorphisms* $\tau_i : \mathbf{T}_1 \xrightarrow{\sim} \mathbf{T}_i$ (*defined on generators*) *for* $i = 2, \ldots, \ell$.
Find: *a faithful representation* $\pi : \mathrm{Aut}(\mathbf{N}) \to \mathrm{Sym}(\Omega')$ (*where* $|\Omega'|$ *is polynomially bounded*).

Lemma 3.21 (CFSG) *Problem* 26 *is in polynomial time.*

Proof: As demonstrated above, since $\mathrm{Aut}(\mathbf{N}) \cong \mathrm{Aut}(T) \wr S_\ell$, we may assume that $\mathbf{N}$ is nonabelian simple. Here, we call a procedure from [33, §6] for constructing permutation representations of composition factors of permutation groups, to form, on a small set $\hat{\Omega}$, a faithful representation $\phi : \mathbf{N} \to \mathrm{Sym}(\hat{\Omega})$. Then, via ϕ, we apply the method for Problem 24. □

3.7 Normalizers of characteristically simple groups

In this subsection, we will develop polynomial-time tools for finding normalizers of direct products of isomorphic simple groups.

First, we consider normalizing elementary abelian groups.

Problem 27
Given: $G, E \leq \mathrm{Sym}(\Omega)$ *such that* $G \in \Gamma_d$, *and* E *is elementary abelian.*
Find: $\mathrm{N}_G(E)$.

Lemma 3.22 *Problem* 27 *is in polynomial time.*

Proof: First, we find the orbits of E, say Δ_i, $i = 1, \ldots, \ell$, and form $E_0 := E^{\Delta_1} \cdots E^{\Delta_\ell} \cong E^{\Delta_1} \times \cdots \times E^{\Delta_\ell}$. Here, we note that $\mathrm{N}_G(E) \leq \mathrm{N}_G(E_0)$. Next, via Problems 6, 9, we find $G_0 := \mathrm{N}_G(E_0) = G \cap \mathrm{N}_{\mathrm{Sym}(\Omega)}(E_0)$. Under the linear representation induced by the conjugation action of G_0 on E_0, we then find, via Problem 19, $\mathrm{N}_{G_0}(E) = \mathrm{N}_G(E)$. □

We next consider the following general problem (cf. Problem 23).

Problem 28
Given: $G \leq \mathrm{Sym}(\Omega)$ *and* $\Sigma \subseteq \mathrm{Aut}(G)$ (*defined on generators*) *such that* $\langle \mathrm{Inn}(G) \cup \Sigma \rangle = \mathrm{Aut}(G)$.
Find: $\mathrm{N}_{\mathrm{Sym}(\Omega)}(G)$.

Proposition 3.23 *Problem* 28 *is solvable in time polynomial in* $|\Omega|$, $|\Sigma|$ *and* $|\mathrm{Out}(G)|$.

Proof: We first form, via Problem 8, a complete set of right coset representatives $R := \{\rho_1, \ldots, \rho_\ell\}$ for $\mathrm{Inn}(G)$ in $\mathrm{Aut}(G)$. Then, for each $\rho_i \in R$, we test, via Problem 7, if there is $x_i \in \mathrm{Sym}(\Omega)$ such that $g^{x_i} = g^{\rho_i}$ for all $g \in G$, and if so, collect such x_i in a set X. Next, via Problem 5, we find $\mathrm{C}_{\mathrm{Sym}(\Omega)}(G)$ and then return $\langle X \rangle G \mathrm{C}_{\mathrm{Sym}(\Omega)}(G) = \mathrm{N}_{\mathrm{Sym}(\Omega)}(G)$. □

We will now consider several normalizer problems involving nonabelian simple groups. As in Problems 24–26, we will appeal to the aforementioned facts about the outer automorphism groups of nonabelian simple groups.

Problem 29
Given: $T \leq \mathrm{Sym}(\Omega)$ *such that* T *is nonabelian simple.*
Find: $\mathrm{N}_{\mathrm{Sym}(\Omega)}(T)$.

Since the structure of $\mathrm{Out}(T)$ is known, where $|\mathrm{Out}(T)|$ is polynomially bounded, we have, by Proposition 3.23,

Corollary 3.24 (CFSG) *Problem* 29 *is in polynomial time.* □

For $G, T \leq \mathrm{Sym}(\Omega)$, note that $\mathrm{N}_G(T) = G \cap \mathrm{N}_{\mathrm{Sym}(\Omega)}(T)$. Problems 9 and 29 now provide a solution to

Problem 30
Given: $G, T \leq \mathrm{Sym}(\Omega)$ *such that* $G \in \Gamma_d$, *and* T *is nonabelian simple.*
Find: $\mathrm{N}_G(T)$.

Corollary 3.25 (CFSG) *Problem* 30 *is in polynomial time.* □

We use a similar technique to solve

Problem 31
Given: $G, T_1, T_2 \leq \mathrm{Sym}(\Omega)$ *such that* $G \in \Gamma_d$*, and* T_1, T_2 *are nonabelian simple.*
Find: $\mathrm{Trans}_G(T_1, T_2) = \{g \in G \mid T_1^g = T_2\}$.

Lemma 3.26 (CFSG) *Problem* 31 *is in polynomial time.*

Proof: We consider, for the transposition t on $\{1, 2\}$, the natural action of $\hat{G} := G \wr \langle t \rangle$ on $\Omega \times \{1, 2\}$ via $(\alpha, i)^{(g_1, g_2)t} := (\alpha^{g_i}, i^t)$ for $(\alpha, i) \in \Omega \times \{1, 2\}$ and $g_i \in G$ for $i = 1, 2$. Also, consider $\hat{T} := T_1 \times T_2$ for which $(\alpha, i)^{(t_1, t_2)} := (\alpha^{t_i}, i)$ for $(\alpha, i) \in \Omega \times \{1, 2\}$ and $t_i \in T_i$ for $i = 1, 2$. Since the structure of $\mathrm{Out}(\hat{T})$ is known, where $|\mathrm{Out}(\hat{T})|$ is polynomially bounded, we proceed to find, via Problem 28, $\hat{N} := \mathrm{N}_{\hat{G}}(\hat{T})$ in polynomial time. If $\hat{N}$ stabilizes $\Omega \times \{1\}$, then we return $\mathrm{Trans}_G(T_1, T_2) = \emptyset$. Otherwise, we find a generator $\hat{n}$ of $\hat{N}$ such that $(\Omega \times \{1\})^{\hat{n}} = \Omega \times \{2\}$ and then determine $g \in G$ such that $(\alpha, 1)^{\hat{n}} = (\alpha^g, 2)$ for all $\alpha \in \Omega$. Now, via Problem 30, we find $\mathrm{N}_G(T_1)$ and return $\mathrm{N}_G(T_1)g = \mathrm{Trans}_G(T_1, T_2)$. □

For finding normalizers of direct products of isomorphic nonabelian simple groups, we first consider the following technical problem.

Problem 32
Given: $G, T_1, \ldots, T_\ell \leq \mathrm{Sym}(\Omega)$ *such that* $G \in \Gamma_d$*, and* $T_1, \ldots, T_\ell$ *are nonabelian simple, and an action of* G *on* $I = \{1, \ldots, \ell\}$.
Find: $\mathrm{Stab}_G(\{(t, i) \mid i \in I$ *and* $t \in T_i\})$ *in the action of* G *on* $\mathrm{Sym}(\Omega) \times I$.

Lemma 3.27 (CFSG) *Problem* 32 *is in polynomial time.*

Proof: To accommodate recursion, we write $\mathcal{T} := \{(t, i) \mid i \in I \text{ and } t \in T_i\}$ and consider the following generalization.

Given: $H \leq G$*,* $g \in G$ *and* H*-invariant* $J \subseteq I$.
Find: $\{x \in Hg \mid (\mathcal{T} \cap (\mathrm{Sym}(\Omega) \times J))^x = \mathcal{T} \cap (\mathrm{Sym}(\Omega) \times J^g)\}$.

For this, we apply the divide-and-conquer paradigm of §3.4 to the action of H on J (cf. Proposition 3.9). In the base case in which $J = \{j\}$, we return, via Problem 31, $\{x \in Hg \mid T_j^x = T_{j^g}\} = \mathrm{Trans}_H(T_j, T_{j^g}^{g^{-1}})g$. □

Problem 33
Given: $G, H \leq \mathrm{Sym}(\Omega)$ *such that* $G \in \Gamma_d$*, and* H *is a direct product of isomorphic nonabelian simple groups.*
Find: $\mathrm{N}_G(H)$.

Lemma 3.28 (CFSG) *Problem* 33 *is in polynomial time.*

Proof: Suppose that $H = T_1 \cdots T_\ell \cong T_1 \times \cdots \times T_\ell$ in which all T_i are isomorphic nonabelian simple groups. Since Problem 30 is in polynomial time, we may assume that $\ell \geq 2$. We will utilize the fact that $x \in \mathrm{Sym}(\Omega)$ normalizes H if and only if x stabilizes $\{T_1, \ldots, T_\ell\}$.

Suppose that two distinct T_i have a common nontrivial orbit. Then the orders of these two and therefore all T_i are equal to the size of such an orbit. For each T_i, we form $\mathcal{A}_i := \{(\alpha, \alpha^t) \mid \alpha \in \Omega \text{ and } t \in T_i\}$.

Now, notice that $x \in \mathrm{Sym}(\Omega)$ stabilizes $\{T_1, \ldots, T_\ell\}$ if and only if x stabilizes $\{\mathcal{A}_1, \ldots, \mathcal{A}_\ell\}$ under the natural action of $\mathrm{Sym}(\Omega)$ on $\Omega \times \Omega$. We thus find, via Problem 11, $\mathrm{Stab}_G(\{\mathcal{A}_1, \ldots, \mathcal{A}_\ell\})$.

Next, suppose instead that no two T_i have a common orbit. For this, for each T_i, we form the set $\mathcal{B}_i$ of all orbits of T_i. Under the natural action of G on 2^{2^Ω}, via Problem 12, we then find $G_0 := \mathrm{Stab}_G(\{\mathcal{B}_1, \ldots, \mathcal{B}_\ell\})$. Let G_0 act on $I := \{1, \ldots, \ell\}$ induced by the action of G_0 on $\{\mathcal{B}_1, \ldots, \mathcal{B}_\ell\}$ via the bijection $\mathcal{B}_i \mapsto i$ for $i = 1, \ldots, \ell$. It now suffices to find, via Problem 32, $\mathrm{Stab}_{G_0}(\{(t, i) \mid i \in I \text{ and } t \in T_i\})$. □

4 Main algorithm to find $\mathrm{N}_G(H)$

In this section, we will first describe the main steps of our normalizer algorithm and then prove Theorems 1.1, 1.2, 1.3.

For simplicity, it is convenient to focus on a procedure that is aimed only at getting a step closer to the normalizer; in particular, we consider

Problem 34
Given: $G, H \leq \mathrm{Sym}(\Omega)$ *such that* $G \in \Gamma_d$ *and* $\mathrm{N}_G(H) < G$.
Find: G_0 *such that* $\mathrm{N}_G(H) \leq G_0 < G$.

In the next two subsections, we will describe our procedure to prove

Proposition 4.1 (CFSG) *Problem* 34 *is in polynomial time.*

Here, we first recall the notions of covering and avoidance: Let G be a group, $A, B \leq G$, and $C \trianglelefteq B$. We say A *covers* B/C if $BA = CA$. We say A *avoids* B/C if $B \cap A = C \cap A$.

In §4.1, we will first reduce the given instance to the case in which H either covers or avoids each G-chief factor of $\langle H^G \rangle$. Then, in §4.2, we will focus on a segment $M > L > K$ in the chief series such that H covers M/L but avoids L/K.

4.1 Reducing to H that covers or avoids each factor

Using Theorem 3.1(x), we first construct a G-chief series for $X := \langle H^G \rangle$ as follows.

$$X = X_1 \vartriangleright X_2 \vartriangleright \cdots \vartriangleright X_r = 1.$$

If there is a chief factor L/K of X such that $L > (H \cap L)K > K$ (i.e., H neither covers nor avoids L/K), we then perform the following according to the structure of L/K. Here, we note that G does not normalize $(H \cap L)K$.

Case 1 *L/K is abelian.* Under the natural action of G on L/K, find $G_0 := \mathrm{N}_G((H \cap L)K/K)$ via Problem 19. Return G_0 and exit.

Case 2 *L/K is nonabelian.* On some set Ω', construct a faithful representation $\pi : \mathrm{Aut}_{GL/K}(L/K) \to \mathrm{Sym}(\Omega')$ via Problem 26. Now, use Lemma 3.2 to find a homogeneous component J/K in the socle of $(H \cap L)K/K$ (cf. [7, §5], [25, §9]). Here, $J/K \operatorname{char} (H \cap L)K/K$, so $\mathrm{N}_G((H \cap L)K/K) \leq \mathrm{N}_G(J/K)$; furthermore, since L/K is a chief factor, $\mathrm{N}_G(J/K) < G$. Now, working with the image of G in $\mathrm{Sym}(\Omega')$ via π, find $G_0 := \mathrm{N}_G(J/K)$ via Problem 33. Return G_0 and exit.

4.2 $M > L > K$ *where* H *covers* M/L *but avoids* L/K

We may assume now that H either covers or avoids each factor. For such a series, if applicable, we first move covered factors towards the tail of the series as follows: While there is a segment $M > L > K$ in the series, where H covers M/L but avoids L/K, and G normalizes $(H \cap M)K$, replace L by $(H \cap M)K$.

Since G does not normalize H, we then have a segment $M > L > K$ such that H covers M/L but avoids L/K, and G does not normalize $(H \cap M)K$. For such a segment, we perform the following according to the structure of L/K. Let $\mathbf{M} := M/K$, $\mathbf{L} := L/K$, and $\mathbf{H} := (H \cap M)K/K$ (here, $\mathbf{M} = \mathbf{HL}$, $\mathbf{H} \cap \mathbf{L} = \mathbf{1}$, and $\mathbf{H} \cong M/L$).

Case 1 $\mathbf{L}$ *is abelian*. Form the natural homomorphism $* : \mathbf{H} \to \mathbf{HL}/\mathbf{L}$ (actually, $*$ is an isomorphism since $\mathbf{H} \cap \mathbf{L} = \mathbf{1}$) and its inverse $\lambda : \mathbf{H}^* \to \mathbf{H}$ such that $\lambda(\mathbf{h}^*) = \mathbf{h}$ for all $\mathbf{h} \in \mathbf{H}$. Notice that, if $g \in G$, then

$$\begin{aligned} g \in \mathrm{N}_G(\mathbf{H}) \quad &\Leftrightarrow \quad \lambda(\mathbf{h}^{*g}) = \mathbf{h}^g \text{ for all } \mathbf{h} \in \mathbf{H} \\ &\Leftrightarrow \quad \lambda(\mathbf{h}^{*g^{-1}})^g = \lambda(\mathbf{h}^*) \text{ for all } \mathbf{h} \in \mathbf{H}. \end{aligned}$$

Form a 1-cocycle $f \in \mathrm{Z}^1(G, \mathrm{Z}^1(\mathbf{H}^*, \mathbf{L}))$ defined by

$$f(g)(\mathbf{h}^*) := \lambda(\mathbf{h}^*)^{-1} \lambda(\mathbf{h}^{*g^{-1}})^g$$

for $g \in G$ (here, $\mathbf{H}^*$ acts on $\mathbf{L}$ via $\mathbf{l}^{\mathbf{h}^*} := \mathbf{l}^{\mathbf{h}}$ for $\mathbf{l} \in \mathbf{L}$ and $\mathbf{h} \in \mathbf{H}$, and G acts on $\mathrm{Z}^1(\mathbf{H}^*, \mathbf{L})$ via $\alpha^g(\mathbf{h}^*) := \alpha(\mathbf{h}^{*g^{-1}})^g$ for $\alpha \in \mathrm{Z}^1(\mathbf{H}^*, \mathbf{L})$, $\mathbf{h} \in \mathbf{H}$ and $g \in G$). Working with the representation of G on $\mathrm{Z}^1(\mathbf{H}^*, \mathbf{L})$ (whose dimension is at most $\operatorname{rank} \mathbf{L} \cdot \log |\mathbf{H}|$), find $G_0 := \operatorname{Ker} f = \mathrm{N}_G(\mathbf{H})$ via Problem 21. Return G_0 and exit.

Case 2 $\mathbf{L}$ *is nonabelian*. For $\mathbf{G} := GK/K$, on some set Ω', construct a faithful representation $\pi : \mathrm{Aut}_{\mathbf{GM}}(\mathbf{L}) \to \mathrm{Sym}(\Omega')$ via Problem 26 (here, since $\mathbf{M}$ embeds in $\mathrm{Aut}_{\mathbf{GM}}(\mathbf{L})$, $\mathbf{H}$ embeds in $\mathrm{Sym}(\Omega')$ via π). Working with the image of G in $\mathrm{Sym}(\Omega')$ via π, find $G_0 := \mathrm{N}_G(\mathbf{H})$ via Problem 27 or 33. Return G_0 and exit. □

4.3 Proofs of Theorems 1.1–1.3

Proof of Theorem 1.1: With the help of the above procedure for Problem 34, we describe how to find $\mathrm{N}_G(H)$.

First, let $G_1 := G$. While G_1 does not normalize H, repeat the following: find G_0 such that $\mathrm{N}_{G_1}(H) \leq G_0 < G_1$ via Problem 34 and let $G_1 := G_0$. Finally, return $G_1 = \mathrm{N}_G(H)$. □

Proof of Theorem 1.2: We mimic a standard reduction from the problem of testing conjugacy of two elements to the problem of finding the centralizer of an element given in [25, §11] (cf. Lemma 3.26).

We consider, for the transposition t on $\{1, 2\}$, the natural action of $\hat{G} := G \wr \langle t \rangle$ on $\Omega \times \{1, 2\}$ such that $(\alpha, i)^{(g_1, g_2)t} := (\alpha^{g_i}, i^t)$ for $(\alpha, i) \in \Omega \times \{1, 2\}$ and $g_i \in G$ for $i = 1, 2$. We also form $\hat{H} := H_1 \times H_2$ for which $(\alpha, i)^{(h_1, h_2)} := (\alpha^{h_i}, i)$ for $(\alpha, i) \in \Omega \times \{1, 2\}$ and $h_i \in H_i$ for $i = 1, 2$. Using Theorem 1.1, we find $\hat{N} := \mathrm{N}_{\hat{G}}(\hat{H})$. Then there is $g \in G$ such that $H_1^g = H_2$ if and only if there is a generator $\hat{s}$ of $\hat{N}$ such that $(\Omega \times \{1\})^{\hat{s}} = \Omega \times \{2\}$. In particular, if such $\hat{s} = (s_1, s_2)t$ for $s_1, s_2 \in G$, then $H_1^{s_1} = H_2$ and $H_2^{s_2} = H_1$. □

Proof of Theorem 1.3: The following proof involves a computational use of the *Frattini method* with Kantor's Sylow machinery (Theorem 3.1(xi)) as in [25, §5].

We may assume that K is not nilpotent (because, if K is nilpotent, then $G \in \Gamma_d$). Suppose that $G = \langle S \rangle$ and $H = \langle T \rangle$. Since K is not nilpotent, for some prime p dividing $|K|$, there is $P \in \mathrm{Syl}_p(K)$ such that P is not normal in K. To begin, we appeal to Theorem 3.1(xi) to find such P. Now, we form $S_0 := \{s \in S \mid P^s = P\}$. Then, for each $s \in S$ such that $P \neq P^s$, with the help of Theorem 3.1(xi) again, we find $k \in K$ such that $P^k = P^s$ and add ks^{-1} to S_0. We repeat the same for T to form a set $T_0 \subseteq \mathrm{N}_H(P)$.

Next, form $X := \langle S, T \rangle$ and $Y := \langle S_0, T_0 \rangle$. We remark here that, by the *Frattini argument*, $X = \mathrm{N}_X(P)K = YK$. We then form an isomorphism $\phi : X/K \xrightarrow{\sim} Y/(Y \cap K)$. For this, we recall that, by Theorem 3.1(viii)(c), for any given $x \in X$, we can find $y_x \in Y$ and $k_x \in K$ such that $x = y_x k_x$; so, using any such y_x, we define $\phi(Kx) := (Y \cap K)y_x$. Under this isomorphism, we recursively find $\mathrm{N}_{\phi(G/K)}(\phi(H/K))$ in $Y/(Y \cap K)$ and then pull back the result in G/K; here, to find the pullback, we appeal to the quotient-group version of Theorem 3.1(vi)(b) (see §3.2). $\square$

5 Finding vector and subspace stabilizers

Throughout this section, we assume that V is an n-dimensional vector space over a finite field k of order q^e for some prime q.

The main purpose of this section is to prove Proposition 3.17 and thus Theorem 1.4. In particular, we will solve Problems 18–22 in time polynomial in $|\Omega|$, n, q and e. Our solutions are based on a divide-and-conquer paradigm resulting from the following.

Theorem 5.1 *Given $G \leq \mathrm{Sym}(\Omega)$ such that $G \in \Gamma_d$ and an irreducible representation $\bar{\ } : G \to \mathrm{GL}(V)$, one can find one of the following, in time polynomial in $|\Omega|$, n, q and e (where $V \cong \mathbb{F}_{q^e}^n$).*

(i) *$H \leq G$ and a direct sum $V = V_1 \oplus \cdots \oplus V_m$, where $m \geq 2$, such that*

   (a) *each $\dim_k V_i = n/m$, $|G : H| = O(m^c)$ for a constant $c > 0$, and*

   (b) *H acts on $\mathcal{V} = \{V_1, \ldots, V_m\}$ as a permutation group of degree m.*

(ii) *$A \trianglelefteq G$ such that $\bar{A}$ is abelian and $|G : A| = O(|\Omega| + n)$.*

Remark (i) As indicated in §1, in Theorem 5.1, the characteristic q of the field k is involved in the running time. Indeed, this parametrization enables us to call the deterministic version of Rónyai's method to test irreducibility (e.g., in Propositions 5.8, 5.11, where we have to make use of his method). (If, however, we appeal to his *Las Vegas* version instead, we can accomplish the same task in Las Vegas polynomial time in $|\Omega|$, n, $\log q$ and e, replacing q by $\log q$.) For our applications to the problem of finding normalizers in permutation groups, n, q and e are all polynomially bounded in $|\Omega|$.

(ii) We do not assert in Theorem 5.1(i) that $\mathcal{V}$ is a *system of imprimitivity for H* because the action of H on $\mathcal{V}$ will not necessarily be transitive. In fact, although the decomposition arises in various ways through the results leading up to the proof of Theorem 5.1, it will be seen that this action always turns out to be either transitive or trivial. However, the critical item for our divide-and-conquer paradigm is just that the summands in the decomposition of V have equal dimension n/m.

With the help of Rónyai's method to test irreducibility from [47, §5] (see also Theorem 3.13), Theorem 5.1 facilitates the extension to representations of Γ_d groups of the divide-and-conquer paradigm for solvable linear groups (see [34, §6]). As in §3.4, it is indeed Γ_d that enables us to find subgroups of polynomial index that preserve suitable direct-sum decompositions.

In §5.1, we will first present this divide-and-conquer paradigm resulting from Theorem 5.1. In §5.2, as promised in §3.5, we will prove that the paradigm is applicable to Problems 18–22 (cf. [34, §§6.2, 6.3]). The remainder of this section is devoted to proving Theorem 5.1. In §5.3, we will begin with some preliminaries on linear groups. In §§5.4, 5.5, we will next describe the two key subroutines that will be used in our main algorithm for Theorem 5.1. In §5.6, we will then present the main algorithm.

5.1 Divide and conquer using invariant subspaces and imprimitivity systems

In general, as in permutation groups, this divide-and-conquer paradigm for linear groups applies to problems (such as Problems 18–22) that ask for construction of a recognizable subcoset of a given coset Gx in $X \leq \mathrm{Sym}(\Omega)$, where $G \in \Gamma_d$, equipped with a representation $X \to \mathrm{GL}(V)$ such that the following hold:

(1) *Recursive property*. Given a proper kG-submodule $W < V$, the problem is recursively reducible to induced problems on W and V/W in time polynomial in $|\Omega|$, n, q and e.

(2) *Base property*. If the G-action on V is irreducible and cyclic, then the problem is solvable in time polynomial in $|\Omega|$, n, q and e.

The paradigm works in the following way. With the help of Theorems 3.13, 5.1, the paradigm performs two levels of divide-and-conquer maneuvers involving proper kG-submodules of V and, in the irreducible case, direct-sum decompositions of V on which subgroups of G of polynomial index act. In particular, we consider the following three cases (two recursive and one base).

Reducible case As required by (1) above, if there is a proper kG-submodule $W < V$, then we recursively solve the induced problems on W and V/W.

Irreducible case We first appeal to Theorem 5.1 and perform the following according to which of the outputs we obtain.

In case (i), we consider the output: $H \leq G$ and $V = V_1 \oplus \cdots \oplus V_m$, where $m \geq 2$. For this, we first decompose G into cosets of H, say, $G = Hy_1 \dot\cup \cdots \dot\cup Hy_\ell$ for some $y_1, \ldots, y_\ell \in G$, where $\ell = O(m^c)$. Thus, the problem for G on V reduces to ℓ problems for cosets of H on V. Each of these ℓ problems considers the orbit/imprimitivity structure of H in $\mathcal{V}$, following the standard permutation-group divide-and-conquer paradigm (illustrated previously for Theorem 3.7): in each orbit, consider the action on a minimal system of imprimitivity, and decompose the group into cosets of the kernel of that action. The process continues until we are faced with a single element of $\mathcal{V}$ and a group fixing that element.

(For simplicity of presentation and timing, the algorithm keeps to the submodules generated by elements of $\mathcal{V}$ until it is faced with a single V_i. In practice, finer decomposition may be observed and used, especially as the group at hand decreases.)

In case (ii), we consider the output: $A \trianglelefteq G$ such that the A-action on V is abelian. As before, we decompose G into cosets of A and reduce the problem to instances involving these cosets. The problem for A exploits the recursive property, ultimately reducing to $\leq n$ instances of the following base case

Base case The above recursion bottoms out when the abelian G-action on V becomes irreducible (and thus cyclic by Schur's lemma, see, e.g., [2, 12.4]). In this base case, the problem is solvable in the desired time as required by (2) above.

Timing analysis In the reducible case, we solve sequentially on W and V/W, where $\dim_k W + \dim_k V/W = n$.

In case (i), divide-and-conquer is applied to the action on $\mathcal{V}$ with respect to orbits and then minimal systems of imprimitivity using stabilizers of such systems (cf. §3.4). Having exhausted the action on $\mathcal{V}$, we end up with a problem on one of the V_i's. Using the bound on primitive Γ_d groups (from Theorem 3.8) for the index of the kernels of the minimal-system actions, we conclude that the problem for each coset of H is reduced to $O(m^{f(d)+1})$ instances on submodules of dimension n/m. Thus, since $|G:H| = O(m^c)$ for a constant $c > 0$, the original problem for G on V is reduced to $O(m^{c+f(d)+1})$ instances on submodules of dimension n/m.

In case (ii), where $A \trianglelefteq G$ such that the A-action on V is abelian, the original problem is reduced to $O(n(|\Omega| + n))$ instances of the base case.

5.2 Applying the divide-and-conquer paradigm

We will solve Problems 18–22 to prove Proposition 3.17 via the divide-and-conquer paradigm described above. (In the following solution to Problem 35, the proof of the base property (2) corrects a corresponding reduction in [34, §6.2] and the proof of Theorem 4.1.2(i), Case 1, in [43, §IV.2].)

Proof of Proposition 3.17: As indicated in §3.5, it suffices to solve Problems 21, 22 in the desired running time.

Solution to Problem 21: To accommodate the above paradigm, we consider the following generalization.

Problem 35
Given: $X \le \mathrm{Sym}(\Omega)$, *a representation* $^{-} : X \to \mathrm{GL}(V)$, $G \le X$ *such that* $G \in \Gamma_d$, $x \in X$,
$f \in \mathrm{Z}^1(X, V)$ *and* $v \in V$.
Find: $\mathcal{C}(Gx, V, f, v) := \{y \in Gx \mid f(y) = v\}$.

If not empty, $\mathcal{C}(Gx, V, f, v)$ is a coset of $\mathrm{Ker}\, f|_G = (f|_G)^{-1}(0)$.

As indicated in §5.1, to complete the proof, it suffices to prove that this problem has these properties: (1) given a proper kG-submodule $W < V$, the problem is recursively reducible to induced problems on W and V/W, and (2) if the G-action on V is irreducible and cyclic, then the problem is solvable in the desired time.

Proof of the recursive property (1) *for Problem* 35: To begin, we suppose that a proper kG-submodule $W < V$ is given. Let $u := (v - f(x))^{\bar{x}^{-1}}$. Since $\mathcal{C}(Gx, V, f, v) = \mathcal{C}(G, V, f, u)x$, it suffices to find $\mathcal{C}(G, V, f, u)$.

We first solve the problem on V/W. In particular, under the induced representation $G \to \mathrm{GL}(V/W)$, with $\hat{f} \in \mathrm{Z}^1(G, V/W)$ defined by $\hat{f}(g) := W + f(g)$ for $g \in G$, we solve recursively for $\mathcal{C}(G, V/W, \hat{f}, W + u)$, which is, if not empty, a coset $Ka \subseteq G$.

We next solve the problem on W. For this, we first note that $\hat{f}(g) = W$ if and only if $f(g) \in W$ for $g \in G$; so, $f(K) \subseteq W$. Under the restriction $K \to \mathrm{GL}(W)$, regarding $f \in \mathrm{Z}^1(K, W)$, we find $\mathcal{C}(K, W, f, (u - f(a))^{\bar{a}^{-1}})$ recursively. If not empty, the result is a coset $Hb \subseteq K$. So, $\mathcal{C}(G, V, f, u) = Hba$ and $\mathcal{C}(Gx, V, f, v) = Hbax$.

Proof of the base property (2) *for Problem* 35: We now suppose that the G-action on V is irreducible and cyclic. It is also convenient to assume that the ground field k is a prime field $\mathbb{F}_q$. (If k is of order q^e for $e > 1$, then we regard $V \cong \mathbb{F}_q^{en}$ and consider the induced $\mathbb{F}_q X$-representation of degree en.) As before, let $u := (v - f(x))^{x^{-1}}$. To solve for $\mathcal{C}(Gx, V, f, v)$, it suffices to find $\mathcal{C}(G, V, f, u)$. If $f(G) = 0$, we simply return $\emptyset$ if $u \neq 0$ or G if $u = 0$. So, we suppose that $f(G) \neq 0$.

To begin, via Problem 16, we find $N := \mathrm{C}_G(V)$, the kernel of the G-action on V. Clearly, $f|_N : N \to V$ is a homomorphism. By the cocycle property, $f(g^{-1}ng) = f(n)^g$ for $n \in N$ and $g \in G$. Thus, $f(N)$ is G-invariant as an abelian group and therefore a $\mathbb{Z}G$-module. That is, since k is a prime field, $f(N)$ is a kG-submodule of V. Since $\bar{G}$ is irreducible, $f(N) = 0$ or V.

We first assume that $f(N) = V$. We recall here that, for $f|_N : N \to V$ and any $w \in V$, finding the preimage $(f|_N)^{-1}(w) = \{n \in N \mid f(n) = w\}$ is in polynomial time (see Remark (ii) following Lemma 3.16). Suppose that $G = \langle S \rangle$. Now, for each $s \in S$, we find $n_s \in N$ such that $f(n_s) = -f(s)$ (and hence $f(sn_s) = 0$). Let $H := \langle sn_s \mid s \in S \rangle$. Then $G = HN$, where, for $h \in H$ and $n \in N$, we have $f(hn) = u$ if and only if $f(n) = u$. Thus, we return $H(f|_N)^{-1}(u) = \mathcal{C}(G, V, f, u)$.

Now, we assume that $f(N) = 0$. We first find $a \in G$ such that $G/N = \langle Na \rangle$ so that $G = \langle a \rangle N$ and $\mathcal{C}(G, V, f, u) = \mathcal{C}(\langle a \rangle, V, f, u)N$. Thus, it suffices to find the integers r such that $f(a^r) = u$. Let $t := f(a)$ and $\alpha := \bar{a}$. Clearly, $K := k[\alpha]$ is a field. Since $\bar{G}$ is irreducible, $V = Kt$; in particular, $u = \beta t$ for some $\beta \in K$. The cocycle property implies that $\alpha^r t = (\alpha - 1)f(a^r) + t$; hence, it suffices to solve for r in $\alpha^r = (\alpha - 1)\beta + 1$. This discrete-log problem in $\langle \alpha \rangle$ is in polynomial time since the primes in the order of α are polynomially bounded.

Solution to Problem 22: For this, we consider the following generalization.

Problem 36

Given: $X \leq \mathrm{Sym}(\Omega)$, *a representation* $\bar{\ } : X \to \mathrm{GL}(V)$, $G \leq X$ *such that* $G \in \Gamma_d$, $x \in X$ *and* $W_1, W_2 \leq V$.

Find: $\mathcal{C}(Gx, V, W_1, W_2) := \{y \in Gx \mid W_1^y = W_2\}$.

If not empty, $\mathcal{C}(Gx, V, W_1, W_2)$ is a coset of $\mathrm{N}_G(W_1)$.

As before, it suffices to prove that this problem has the aforementioned properties (1), (2). As indicated in §3.5, our methods eventually reduce the above problem to Problem 20, which is equivalent to Problem 21.

Proof of the recursive property (1) *for Problem* 36: As before, we suppose that a proper kG-submodule $W < V$ is given. Here, let $W_3 := W_2^{x^{-1}}$. Since $\mathcal{C}(Gx, V, W_1, W_2) = \mathcal{C}(G, V, W_1, W_3)x$, it suffices to find $\mathcal{C}(G, V, W_1, W_3)$.

We first solve an induced problem on W. In particular, under the restriction $G \to \mathrm{GL}(W)$, we solve recursively for $\mathcal{C}(G, W, W_1 \cap W, W_3 \cap W)$, which is, if not empty, a coset $Ka \subseteq G$.

We next solve a residual problem on V/W. For this, under the representation $K \to \mathrm{GL}(V/W)$, we find $\mathcal{C}(K, V/W, (W + W_1)/W, (W + W_3^{a^{-1}})/W)$ recursively. If not empty, the result is a coset $Nb \subseteq K$.

We still have some additional work to do to complete our solution. Let $W_4 := W_3^{a^{-1}b^{-1}}$. Since $\mathcal{C}(G, V, W_1, W_3) = \mathcal{C}(N, V, W_1, W_4)ba$, we now seek $\mathcal{C}(N, V, W_1, W_4)$. For this, form kN-submodules $A := W + W_1 = W + W_4$ and $B := W \cap W_1 = W \cap W_4$. As $A/B = W/B \oplus W_1/B = W/B \oplus W_4/B$, we next find $e, f \in \mathrm{End}_k(A/B)$ such that e and f are the projections onto W_1/B and W_4/B, respectively. Under the induced action of N on $\mathrm{End}_k(A/B)$, it now suffices to find $\mathrm{Trans}_N(e, f)$, which is computable via Problem 20.

Proof of the base property (2) *for Problem* 36: We suppose that the G-action on V is irreducible and abelian. We may also assume that $W_1 \neq 0$. Let $W_3 := W_2^{x^{-1}}$. Our goal is to find $\mathcal{C}(G, V, W_1, W_3)$. Here, we note that, since G is abelian, $\mathcal{C}(G, V, W, U) = \mathcal{C}(G, V, W^g, U^g)$ for all $W, U \leq V$ and $g \in G$.

Let $A := W_1$, $B := W_3$, $A' := 0$ and $B' := 0$. We perform the following:

while $A + A' \neq V$ **do**
  begin
    find $g \in G$ such that $A^g \not\leq A + A'$;
    (* Here, such $g \in G$ exists by the irreducibility of G. *)
    if $A^g \cap (A + A') \neq 0$ **then**
      begin
        $A := A \cap (A + A')^{g^{-1}}$;
        $B := B \cap (B + B')^{g^{-1}}$;
      end
    else
      begin
        $A' := (A + A')^{g^{-1}}$;
        $B' := (B + B')^{g^{-1}}$;
      end
  end

This loop maintains the following invariant:

$$A \neq 0, A \cap A' = 0 \text{ and } \mathcal{C}(G, V, W_1, W_3) \subseteq \mathcal{C}(G, V, A, B) \cap \mathcal{C}(G, V, A', B').$$

Once the loop terminates, we have $V = A \oplus A'$. Let $A'' = A' \cap W_1$ so that $W_1 = A \oplus A''$. Let $B'' = B' \cap W_3$. If either $V \neq B \oplus B'$ or $W_3 \neq B \oplus B''$, then we return $\emptyset$. Otherwise, by the above loop invariant and the fact that $W_1 = A \oplus A'$, we observe that

$$\begin{aligned}
\mathcal{C}(G, V, W_1, W_3) &\subseteq \mathcal{C}(G, V, A, B) \cap \mathcal{C}(G, V, A', B') \cap \mathcal{C}(G, V, W_1, W_3) \\
&\subseteq \mathcal{C}(G, V, A, B) \cap \mathcal{C}(G, V, A', B') \cap \mathcal{C}(G, V, A'', B'') \\
&\subseteq \mathcal{C}(G, V, W_1, W_3) \cap \mathcal{C}(G, V, A', B') \\
&\subseteq \mathcal{C}(G, V, W_1, W_3).
\end{aligned}$$

That is,

$$\mathcal{C}(G, V, W_1, W_3) = \mathcal{C}(G, V, A, B) \cap \mathcal{C}(G, V, A', B') \cap \mathcal{C}(G, V, A'', B'').$$

We first solve recursively for $\mathcal{C}(G, V, A'', B'')$, which is, if not empty, a coset $Ka \subseteq G$. It then remains to find $\mathcal{C}(K, V, A, B^{a^{-1}}) \cap \mathcal{C}(K, V, A', B'^{a^{-1}})$. For this, we form $e, f \in \mathrm{End}_k(V)$ such that e and f are projections from V onto A and $B^{a^{-1}}$ with respect to $V = A \oplus A'$ and $V = B^{a^{-1}} \oplus B'^{a^{-1}}$, respectively. It turns out that $\mathcal{C}(K, V, A, B^{a^{-1}}) \cap \mathcal{C}(K, V, A', B'^{a^{-1}}) = \{k \in K \mid e^k = f\}$, which is computable via Problem 20. $\square$

5.3 Preliminaries on linear groups

In this subsection, we will study some structural properties of linear groups. There are two key propositions. Lemma 5.2 is a general fact that will be used in the main result of §5.5. Proposition 5.7 is the most important result of this subsection. Along with Theorem 3.8, this result on irreducible Γ_d groups enables us to find subgroups of polynomial index that preserve direct-sum decompositions for Theorem 5.1(i) when V is homogeneous (see §5.4).

We begin with the following well-known fact. We include a proof for the reader's convenience. Recall that $n = \dim_k V$.

Lemma 5.2 *If G is an irreducible subgroup of $\mathrm{GL}(V)$, and A is a cyclic normal subgroup of G, then $|G : \mathrm{C}_G(A)| \leq n$.*

Proof: Suppose that $A = \langle a \rangle$. Let $\bar{k}$ be the algebraic closure of k and write $V^{\bar{k}} := \bar{k} \otimes_k V$. Regard $G \leq \mathrm{GL}(V^{\bar{k}}, \bar{k})$ so that a is diagonalizable.

Let U be an eigenspace for a and $G_1 := \mathrm{N}_G(U) = \{g \in G \mid U^g = U\}$. Since G normalizes A, it permutes the eigenspaces of a. Hence, $|G : G_1|$, which measures the number of images of U under G, is $\leq n$. Thus, it suffices to prove that $G_1 \leq \mathrm{C}_G(A)$.

Let $g \in G_1$. Since G normalizes A, it follows that $[g, a] = a^m \in A$ for some integer $m > 0$. Now, a acts on U as a scalar, so $[g, a]$ fixes every $u \in U$ and therefore has nonzero fixed points even over k. Since $\mathrm{C}_V(A^m)$ is a kG-submodule, the irreducibility of G implies that $[g, a] = 1$ and thus $g \in \mathrm{C}_G(A)$. □

To prepare for the proof of Proposition 5.7, we state four lemmas. The following lemma is borrowed from [6].

Lemma 5.3 *If G is an irreducible subgroup of $\mathrm{GL}(V)$ such that $G/\mathrm{Z}(G)$ is a direct product of ℓ non-abelian simple groups, then $n \geq 2^\ell$.*

Proof: Let $G_1/\mathrm{Z}(G)$ be a simple factor of $G/\mathrm{Z}(G)$. Then [6, Proposition 2.7] asserts that $n \geq 2^{\ell-1} n_1$, where n_1 is the dimension of an irreducible kG_1-submodule of V. □

Recall that, in general, an automorphism σ of a group G is *central* if σ is in the kernel of the induced action of $\mathrm{Aut}(G)$ on $G/\mathrm{Z}(G)$. Since the central automorphisms of G leave every element of G' fixed, we have

Lemma 5.4 *If G is a group such that $G = G'$, $\mathrm{Aut}(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(G/\mathrm{Z}(G))$.* □

A classical theorem of Wielandt [54, Theorem 8.7], Praeger and Saxl [44] asserts that, if a subgroup G of S_n is primitive with $A_n \not\leq G$, then $|G| \leq 4^n$ (in fact, via CFSG, $|G| \leq n^{\sqrt{n}}$ [11]; see also [3], [4], [40]). In turn, this leads to the following fact (see, e.g., [6, Lemma 2.2]).

Lemma 5.5 *Let $G \leq S_n$. If no composition factor of G is isomorphic to A_m for any $m > d \geq 6$, then $|G| < d^{n-1}$.* □

For the last of our lemmas, we prove

Lemma 5.6 *Let $N, M \leq \mathrm{GL}(V)$ with $[N, M] = 1$ and NM irreducible. If W is an irreducible kN-submodule of V, U is an irreducible kM-submodule of V, and $K := \mathrm{End}_{kN}(W)$, then $\dim_k V \geq \dim_K W \cdot \dim_k U$.*

Proof: The irreducibility of NM implies that V is homogeneous both as a kN-module and as a kM-module. Let $A := \mathrm{Hom}_{kG}(W, V)$. By [2, 27.14(5)], the k-space structures on V and A are extendible to K-space structures so that V is K-isomorphic to $A \otimes_K W$. Thus, $\dim_k V = \dim_k A \cdot \dim_K W$.

Now, fix $0 \neq w_0 \in W$. The kM-linear map $\phi : A \to V$ defined by $\phi(a) := w_0^a$ for $a \in A$ is nontrivial, else $\{w \in W \mid w^A = 0\}$ would be a proper kN-submodule of W. Hence, $\phi(A)$ is a nonzero kM-submodule of V and therefore contains an isomorphic copy of U. So, $\dim_k A \geq \dim_k \phi(A) \geq \dim_k U$. The result follows. □

We now come to the main result of this subsection.

Proposition 5.7 *Let G be an irreducible subgroup of $\mathrm{GL}(V)$ such that $G \in \Gamma_d$, and let $N, A \lhd G$ such that A is cyclic, and N/A is a nonabelian chief factor of G. Suppose that V is homogeneous both as a kN'-module and as a $k\mathrm{C}_G(N')$-module. If n_0 is the dimension of an irreducible $k\mathrm{C}_G(N')$-submodule of V, then $|G : \mathrm{C}_G(N')| \leq (n/n_0)^c$ for a constant $c > 0$.*

Proof: We first note that $A = \mathrm{Z}(N)$. To see this, notice that, since N/A is a minimal normal subgroup of G/A, either $A = \mathrm{C}_N(A)$ or $\mathrm{C}_N(A) = N$. However, if $A = \mathrm{C}_N(A)$, then N/A would embed in $\mathrm{Aut}(A)$, which is abelian, a contradiction. Hence, $\mathrm{C}_N(A) = N$ and thus $A = \mathrm{Z}(N)$.

Let $H := N'$ throughout. We next note that H is *semisimple*; that is, $H = H'$, and $H/\mathrm{Z}(H)$ is a direct product of nonabelian simple groups (see, e.g., [52, II, 6.6.5]). Further, $\mathrm{Z}(H) = H \cap \mathrm{Z}(N)$ so that $N/\mathrm{Z}(N) \cong H/\mathrm{Z}(H)$.

Let W be an irreducible kH-submodule of V and $K := \mathrm{End}_{kH}(W)$. Since V is a homogeneous kH-module, H acts faithfully on W. Consider the induced representation $\phi : H \to \mathrm{GL}(W, K)$ of degree t (where $t \geq 2$ since H is noncyclic). Now, let $Z := \mathrm{Z}(H)$, and write $H/Z \cong H_1/Z \times \cdots \times H_\ell/Z$, where each H_i/Z is isomorphic to a nonabelian simple group T. It follows from Lemma 5.3 that $2^\ell \leq t$.

Since H is semisimple, $\mathrm{Aut}(H)$ embeds in $\mathrm{Aut}(H/Z)$ by Lemma 5.4; therefore, $G/\mathrm{C}_G(H)$ embeds in $\mathrm{Aut}(H/Z) \cong \mathrm{Aut}(T) \wr S_\ell$. Let $\hat{G}$ denote the isomorphic image of $G/\mathrm{C}_G(H)$ in $\mathrm{Aut}(H/Z)$, and consider $\hat{L} \trianglelefteq \hat{G}$ that leaves each H_i/Z invariant. Clearly, $\hat{L}$ embeds in $\mathrm{Aut}(T)^\ell$ so that $|\hat{L}| \leq c_1^\ell$ for some constant $c_1 > 0$ (by the Γ_d hypothesis). Next, write $c_2 := \max(d, 6)$. Since $\hat{G}/\hat{L}$ lies in S_ℓ, where no composition factor of $\hat{G}/\hat{L}$ is isomorphic to A_m for any $m > c_2$, it follows from Lemma 5.5 that $|\hat{G}/\hat{L}| < c_2^{\ell-1}$. Hence, if $c_3 := c_1 c_2$, then $|G/\mathrm{C}_G(H)| = |\hat{L}||\hat{G}/\hat{L}| < c_3^\ell \leq c_3 t^{\log_2 c_3}$.

It suffices now to prove that $n/n_0 \geq t$. For this, let V_0 be an irreducible $kH\mathrm{C}_G(H)$-submodule such that $W \leq V_0 \leq V$ and U_0 be an irreducible $k\mathrm{C}_G(H)$-submodule of V_0. By Lemma 5.6, $\dim_k V_0 \geq \dim_K W \cdot \dim_k U_0$. Since V is a homogeneous $k\mathrm{C}_G(H)$-module, $n_0 = \dim_k U_0$. Consequently, $n \geq \dim_k V_0 \geq \dim_K W \cdot \dim_k U_0 = tn_0$. □

Remark It is in this proposition that the present definition of Γ_d (in which all nonabelian composition factors lie in S_d) is essential (in particular, to bound the orders of the automorphism groups of nonabelian simple groups).

5.4 Divide and conquer using nonabelian chief factors

As promised earlier, in this and the next subsections, we will describe the two key subroutines that will be used in the main procedure to prove Theorem 5.1. For given $G \leq \mathrm{Sym}(\Omega)$ such that $G \in \Gamma_d$, an irreducible representation $\bar{\ } : G \to \mathrm{GL}(V)$ and a chief factor N/A of G, both of these subroutines seek a decomposition of V into a system of imprimitivity or a direct sum of equal-dimensional kH-submodules for some $H < G$ of polynomial index, based on the structure of N/A (barring a few exceptional cases when N/A is abelian).

We first deal with nonabelian chief factors. In the following proposition, the key property of Γ_d linear groups we require is Proposition 5.7.

Proposition 5.8 *Given $G \le \mathrm{Sym}(\Omega)$ such that $G \in \Gamma_d$, an irreducible representation $\bar{}: G \to \mathrm{GL}(V)$ and $N, A \lhd G$ such that $\bar{N} > 1$, $\bar{A}$ is cyclic, and N/A is a nonabelian chief factor of G, one can find one of the following, in time polynomial in $|\Omega|$, n, q and e (where $V \cong \mathbb{F}_{q^e}^n$).*

(i) *A direct sum $V = V_1 \oplus \cdots \oplus V_m$, where $m \ge 2$, and the summands form a system of imprimitivity for G.*

(ii) *$H \lhd G$ and a direct sum of kG-isomorphic irreducible kH-submodules $V = V_1 \oplus \cdots \oplus V_m$, where $m \ge 2$, such that $|G : H| = O(m^c)$ for a constant $c > 0$.*

Proof: We will describe our algorithm in the following two steps. In Step 1, we first seek a system of imprimitivity for G induced by some accessible normal subgroup of G; if V has no such system, then, in Step 2, we appeal to Proposition 5.7 for a desirable pair $(H, \bigoplus_{i=1}^m V_i)$.

Step 1 *Reduction to Problem* 15. To begin, we solve Problem 15 to seek a system of imprimitivity $\mathcal{V} := \{V_1, \ldots, V_m\}$ for G induced by either N' or $C \lhd G$ such that $\bar{C} = \mathrm{C}_{\bar{G}}(\bar{N}')$ (here, C is computable in polynomial time via Problem 17). Unless V is homogeneous both as a kN'-module and as a kC-module, we return $\bigoplus_{i=1}^m V_i$ for (i) and halt.

Step 2 *V is homogeneous both as a kN'-module and as a kC-module*. Since $\bar{N}'$ centralizes $\bar{C}$ and is nonabelian, $\bar{C}$ is necessarily reducible. Via Problem 13, we find an irreducible kC-submodule $V_1 < V$, decompose $V = V_1 \oplus \cdots \oplus V_m$ such that each $V_i = V_1^{g_i}$ for some $g_i \in G$ and then return a pair $(H, \bigoplus_{i=1}^m V_i)$ with $H := C$.

We note here that, since V is a homogeneous kC-module, all irreducible kC-submodules of V share the same dimension; thus, *any* irreducible kC-submodule V_1 may be used to decompose $V = V_1 \oplus \cdots \oplus V_m$ for which Proposition 5.7 guarantees that $|G : C|$ is polynomially bounded in m. □

5.5 Divide and conquer using abelian chief factors

In this subsection, we will describe the second key subroutine for Theorem 5.1 that deals with abelian chief factors. We will give a top-level description of this subroutine in the proof of Proposition 5.11, which is the main result of this subsection. We will prove this proposition by way of three lemmas. Throughout this subsection, Q_8 denotes the quaternion group of order 8.

The following result is inspired by the well-known structure of *extraspecial* p-groups (see, e.g., [22, 13.7 Satz], [51, Theorem 19.2]).

Lemma 5.9 *Given $P \le \mathrm{Sym}(\Omega)$, a representation $\bar{}: P \to \mathrm{GL}(V)$ such that $\bar{P}$ is a p-group for some prime $p \ne q$, $\mathrm{C}_V(P') = 0$, $\mathrm{Z}(\bar{P})$ is cyclic, and $\bar{P}/\mathrm{Z}(\bar{P})$ is an elementary abelian group of rank $2\ell > 0$, one can find one of the following, in time polynomial in $|\Omega|$, n, q and e (where $V \cong \mathbb{F}_{q^e}^n$).*

(i) *$E \lhd P$ such that $P' < E$ and $\bar{E}$ is elementary abelian, with the isotypic decomposition with respect to E, $V = V_1 \oplus \cdots \oplus V_m$, where $m \ge p^{\ell/3}$, and the summands form a system of imprimitivity for P.*

(ii) $Q \lhd P$ *such that* $\bar{P} = \bar{Q}\mathrm{Z}(\bar{P})$ *and* $\bar{Q} \cong Q_8$. (*This option will only turn up when* $p = 2$ *and* $\ell = 1$.)

Proof: Let K be the kernel of $^{-} : P \to \mathrm{GL}(V)$. In this proof, for any $x \in P$ and $X \le P$, we write $\mathbf{x} := Kx$ and $\mathbf{X} := XK/K$.

We will describe our algorithm in the following two steps. In Step 1, we exploit the symplectic structure of $\mathbf{P}/\mathrm{Z}(\mathbf{P})$ and factor $\mathbf{P}$ into a product of $\mathrm{Z}(\mathbf{P})$ and 2ℓ cyclic groups. In Step 2, using this factorization, we construct $E \lhd P$ and a system of imprimitivity induced by E for P for (i) (except for one case in which we end up with (ii)).

Step 1 *Factoring* $\mathbf{P}$. Consider the natural homomorphism $* : \mathbf{P} \to \mathbf{P}/\mathrm{Z}(\mathbf{P})$. Since $\mathbf{P}/\mathrm{Z}(\mathbf{P})$ is elementary abelian, $|\mathbf{P}'| = p$, so that we may regard $\mathbf{P}'$ as a finite field of order p and $\mathbf{P}^*$ as a vector space over $\mathbf{P}'$. A function $f : \mathbf{P}^* \times \mathbf{P}^* \to \mathbf{P}'$ defined by $f(\mathbf{x}^*, \mathbf{y}^*) := [\mathbf{x}, \mathbf{y}]$ for $\mathbf{x}, \mathbf{y} \in \mathbf{P}$ is then a symplectic form, making $(\mathbf{P}^*, f)$ a symplectic space.

Our goal is to decompose $\mathbf{P}$ with respect to a hyperbolic basis of $(\mathbf{P}^*, f)$; that is, we seek $a_1, b_1, \ldots, a_\ell, b_\ell \in P$ such that $\mathbf{P} = \mathrm{Z}(\mathbf{P})\langle \mathbf{a}_\ell\rangle\langle \mathbf{b}_\ell\rangle \cdots \langle \mathbf{a}_1\rangle\langle \mathbf{b}_1\rangle$, where $|\mathbf{a}_i| \ge |\mathbf{b}_i|$ for $i = 1, \ldots, \ell$, $[\mathbf{a}_i, \mathbf{a}_j] = [\mathbf{a}_i, \mathbf{b}_j] = [\mathbf{b}_i, \mathbf{b}_j] = \mathbf{1}$ for all pairs $i \ne j$, and $\mathbf{1} \ne [\mathbf{a}_1, \mathbf{b}_1] = \cdots = [\mathbf{a}_\ell, \mathbf{b}_\ell] = \mathbf{z}_0$ where $\mathbf{P}' = \langle \mathbf{z}_0\rangle$. For this, we first fix $1 \ne z_0 \in P'$ and find $a_1, b_1 \in P$ such that $[\mathbf{a}_1, \mathbf{b}_1] = \mathbf{z}_0$ with $|\mathbf{a}_1| \ge |\mathbf{b}_1|$. We next find $P_1 \lhd P$ such that $\mathbf{P}_1 = \mathrm{C}_{\mathbf{P}}(\langle \mathbf{a}_1, \mathbf{b}_1\rangle)$. Then $\mathbf{P} = \mathbf{P}_1\langle \mathbf{a}_1\rangle\langle \mathbf{b}_1\rangle$. By repeating this procedure on $\mathbf{P}_1$ and so on, the desired factorization readily follows.

Step 2 *Seeking a suitable* E. There are three cases to consider.

Case (a) p *is odd*. For $i = 1, \ldots, \ell$, we first find an integer $\varepsilon_i \ge 0$ such that $\mathbf{a}_i^{p\varepsilon_i}\mathbf{b}_i^p = \mathbf{1}$ and let $e_i := a_i^{\varepsilon_i} b_i$. We then form $E := \langle e_1, \ldots, e_\ell, z_0\rangle$, where $\bar{E}$ is indeed elementary abelian of rank $\ell + 1$. For each ℓ-tuple $\lambda = (\lambda_1, \ldots, \lambda_\ell) \in \mathbb{Z}_p^\ell$, set

$$V_\lambda := \{v \in V \mid v^{e_1} = v^{z_0^{\lambda_1}}, \ldots, v^{e_\ell} = v^{z_0^{\lambda_\ell}}\}$$

and $\mathcal{V} := \{V_\lambda \mid \lambda \in \mathbb{Z}_p^\ell\}$. Then E acts as a cyclic group on each $V_\lambda \in \mathcal{V}$ and, since $\mathrm{C}_V(P') = 0$, each isotypic submodule for E is in $\mathcal{V}$. Furthermore, since, for $1 \le i \le \ell$,

$$V_{(\lambda_1, \ldots, \lambda_i, \ldots, \lambda_\ell)}^{a_i} = V_{(\lambda_1, \ldots, \lambda_i + 1, \ldots, \lambda_\ell)},$$

$\mathbf{P}$ acts transitively on $\mathcal{V}$, which is then the complete isotypic decomposition of V with respect to E. In this case, $m = p^\ell$.

Note that the system $\mathcal{V}$ is computable via Problem 15 or directly from the definition of V_λ.

Case (b) $p = 2$ *and* $\ell \ge 2$. For $i = 1, \ldots, \ell$, we find an integer $\varepsilon_i \ge 0$ such that $\mathbf{a}_i^{2\varepsilon_i}\mathbf{b}_i^2 = \mathbf{1}$ and let $d_i := a_i^{\varepsilon_i} b_i$. Next, let $e_1 := d_1 d_2, e_2 := d_3 d_4, \ldots$, and $e_{\lfloor \ell/2 \rfloor} := d_{\ell-2} d_{\ell-1}$ if ℓ is odd, or $e_{\lfloor \ell/2 \rfloor} := d_{\ell-1} d_\ell$ if ℓ is even. Now, we form $E := \langle e_1, \ldots, e_{\lfloor \ell/2 \rfloor}, z_0\rangle$. The rest is the same as Case (a)'s argument. In this case, $m = 2^{\lfloor l/2 \rfloor} \ge 2^{l/3}$.

Case (c) $p = 2$ *and* $\ell = 1$. Write $a := a_1$ and $b := b_1$. As before, we find an integer $\varepsilon \ge 0$ such that $\mathbf{a}^{2\varepsilon}\mathbf{b}^2 = \mathbf{1}$ and let $d := a^\varepsilon b$ (here, $|\mathbf{d}| = 2$ or 4).

Unless $|\mathbf{d}| = |\mathbf{a}| = 4$, we now perform one of the following: (1) if $|\mathbf{d}| = 2$, let $e_1 := d$; (2) if $|\mathbf{d}| = 4$ and $|\mathbf{a}| = 2$, let $e_1 := a$; (3) if $|\mathbf{d}| = 4$ and $|\mathbf{a}| \ge 8$, we find an integer $r \ge 3$ such that $|\mathbf{a}| = 2^r$ and let

$e_1 := a^{2^{r-2}}d$. Then, in any case, we form $E := \langle e_1, z_0 \rangle$. The rest is the same as Case (a)'s argument. In this case, $m = 2^\ell$.

Finally, if $|\mathbf{d}| = |\mathbf{a}| = 4$, we form $Q := \langle a, d \rangle$ for (ii). □

Before proving the main result, we present, with the help of Lemma 5.9, an intermediate lemma.

Lemma 5.10 *Given $G \leq \mathrm{Sym}(\Omega)$ such that $G \in \Gamma_d$, an irreducible representation $\bar{}: G \to \mathrm{GL}(V)$ and $N, A \trianglelefteq G$ such that $\bar{A}$ is cyclic and centralized by $\bar{N} > 1$, and N/A is an abelian chief factor of G, one can find one of the following, in time polynomial in $|\Omega|$, n, q and e (where $V \cong \mathbb{F}_{q^e}^n$).*

(i) *$H \leq G$ and a direct sum $V = V_1 \oplus \cdots \oplus V_m$, where $m \geq 2$, such that $|G : H| = O(m^c)$ for a constant $c > 0$, and the summands form a system of imprimitivity for H.*

(ii) *$Q \lhd G$ such that $N = QA$ and $\bar{Q} \cong Q_8$.*

(iii) *$B \trianglelefteq G$ such that $\bar{B}$ is abelian and $A < B$.*

Proof: We will describe our algorithm in the following two steps. In Step 1, unless $\bar{N}$ is abelian, to apply Lemma 5.9, we will first find $P \trianglelefteq N$ such that $\bar{P}$ is a p-group of class 2. In Step 2, we will then appeal to the lemma with respect to this P.

Step 1 *Finding a p-group of class* 2. If $\bar{N}$ is abelian, then we simply return $B := N$ for (iii). Otherwise, $\bar{N}$ is nilpotent of class 2, and we find $P \trianglelefteq N$ such that $\bar{P}$ is the unique Sylow p-subgroup of $\bar{N}$ for the prime p that divides $|N/A|$; here, as $\bar{G}$ is irreducible, $p \neq q$ and $\mathrm{C}_V(P') = 0$. We also find $Z \lhd G$ such that $\bar{Z} = \mathrm{Z}(\bar{P})$. Since N/A is a chief factor of G, $\bar{A} = \mathrm{Z}(\bar{N})$; therefore, $N = PA$ and thus $P/Z \cong N/A$. The rank of P/Z must then be even, say, $2\ell > 0$ (see, e.g., [22, 13.7 Satz]).

Step 2 *Applying Lemma* 5.9. We now appeal to Lemma 5.9 with respect to this P to either

(a) find $E \lhd P$ such that $P' < E$, and $\bar{E}$ is elementary abelian, with the isotypic decomposition with respect to E, $V = V_1 \oplus \cdots \oplus V_m$, where $m \geq p^{\ell/3}$, and the summands form a system of imprimitivity for P, or

(b) return $Q \lhd P$ such that $P = QZ$ (which implies $N = QA$) and $\bar{Q} \cong Q_8$ for (ii).

In case (a), we proceed to find the kernel H of the natural action of G on P/Z. Since H centralizes P/Z, it follows that $EZ \lhd H$ so that H acts on $\mathcal{V} := \{V_1, \ldots, V_m\}$ as well. We then return the pair $(H, \bigoplus_{i=1}^m V_i)$ for (i).

It now remains to prove that $|G : H|$ is polynomially bounded in m. Since G acts irreducibly on N/A, it also acts irreducibly on P/Z, whose rank is 2ℓ. By the result of Babai, Cameron and Pálfy on the orders of completely reducible linear groups in Γ_d [6, Corollary 3.3], there is a constant $c_2 > 0$ such that $|G : H| \leq p^{c_2(2\ell)}$. By Lemma 5.9, $m \geq p^{\ell/3}$; thus, if $c_1 := 6c_2$, then $|G : H| \leq m^{c_1}$. □

We are now ready to complete the proof of the main result of this subsection. In the following proposition, we refine Lemma 5.10 by amending (i) and removing (ii) with an additional assumption that $|G : A| > 24n$. Indeed, the proof of this proposition essentially consists of special routines to handle the quaternion case of Lemma 5.10(ii).

Proposition 5.11 *Given $G \leq \mathrm{Sym}(\Omega)$ such that $G \in \Gamma_d$, an irreducible representation $^- : G \to \mathrm{GL}(V)$ and $N, A \trianglelefteq G$ such that $\bar{A}$ is cyclic and centralized by $\bar{N} > 1$, N/A is an abelian chief factor of G, and $|G : A| > 24n$, one can find one of the following, in time polynomial in $|\Omega|$, n, q and e (where $V \cong \mathbb{F}_{q^e}^n$).*

(i) *$H \leq G$ and a direct sum $V = V_1 \oplus \cdots \oplus V_m$, where $m \geq 2$, such that $|G : H| = O(m^c)$ for a constant $c > 0$, and either*

(a) *$\{V_1, \ldots, V_m\}$ is a system of imprimitivity for H, or*

(b) *V is a homogeneous kH-module, where $V_1, \ldots, V_m$ are irreducible kH-submodules of V of dimension n/m.*

(ii) *$B \trianglelefteq G$ such that $\bar{B}$ is abelian and $A < B$.*

Proof: We will describe our algorithms in the following two steps. In Step 1, we reduce the given input to instances to which Proposition 5.8 and/or Lemma 5.10 are applicable. In Step 2, we handle a special case involving quaternion groups to which Proposition 5.8 and Lemma 5.10 do not apply, and we seek a system of imprimitivity induced by these groups.

Step 1 *Applying Proposition* 5.8 *and Lemma* 5.10. We first apply the algorithm for Lemma 5.10 to the given input. Unless it results in the quaternion type, we immediately return the result of applying this lemma, namely, the pair $(H, \bigoplus_{i=1}^m V_i)$ for (i)(a) or $B \trianglelefteq G$ such that $\bar{B}$ is abelian and $A < B$ for (ii), and halt.

We next consider the case in which the result of applying Lemma 5.10 is of the quaternion type (say, $Q \lhd G$). For this, via Problem 17, we first find $C \trianglelefteq G$ such that $\bar{C} = \mathrm{C}_{\bar{G}}(\bar{N})$. Here, we observe that $|G : C| \leq 24n$ (to see this, notice that $|\bar{G} : \mathrm{C}_{\bar{G}}(\bar{Q})| \leq |\mathrm{Aut}(Q_8)| = 24$ and, since $\mathrm{C}_{\bar{G}}(\bar{N}) = \mathrm{C}_{\bar{G}}(\bar{Q}) \cap \mathrm{C}_{\bar{G}}(\bar{A})$, $|\mathrm{C}_{\bar{G}}(\bar{Q}) : \mathrm{C}_{\bar{G}}(\bar{N})| \leq |\bar{G} : \mathrm{C}_{\bar{G}}(\bar{A})| \leq n$ by Lemma 5.2). Since $|G : A| > 24n$, this then implies that $A < C$. Now, we find $M \leq C$ such that M/A is a chief factor of G and consider the following two cases.

If M/A is nonabelian, then we appeal to Proposition 5.8 with respect to M/A and directly return its result for (i)(a) or (i)(b).

If M/A is abelian, then we appeal to Lemma 5.10 with respect to M/A. As before, unless it results in the quaternion type again (say, $R \lhd G$ this time), directly return the result of applying Lemma 5.10 for (i)(a) or (ii), and halt.

Step 2 *Finding a system of imprimitivity induced by quaternion groups*. We are now left with the case in which we have at hand both $Q, R \lhd G$ such that $N = QA = RA$ and $\bar{Q}, \bar{R} \cong Q_8$. Our goal here is to construct a system of imprimitivity induced by elements of Q, R and A.

First, we find $e_1 \in Q$ and $e_2 \in R$ such that $\bar{e}_1 \in \bar{Q} \setminus \bar{R}$ and $\bar{e}_2 \in \bar{R} \setminus \bar{Q}$. Then, with $a \in A$ such that $|\bar{a}| = 2$, we form $E := \langle e_1 e_2, a \rangle$. We also find the kernel H of the natural action of G on NM/A. As in the proof of Lemma 5.9, we find the set $\mathcal{V} := \{V_1, V_2\}$ of isotypic subspaces for E, which form a system of imprimitiviy for H. It suffices to return the pair $(H, V_1 \oplus V_2)$ for (i)(a), where $|G : H|$ is bounded by a constant. □

5.6 The main algorithm for Theorem 5.1

In this subsection, we will finally present our main algorithm to prove Theorem 5.1. We will prove the theorem by way of repeated applications of

Proposition 5.12 *Given $G \le \mathrm{Sym}(\Omega)$ such that $G \in \Gamma_d$, an irreducible representation $^{-} : G \to \mathrm{GL}(V)$ and $A \trianglelefteq G$ such that $\bar{A}$ is abelian, and $|G : A| > \max(|\Omega|, d!/2, 24n)$, one can find one of the following, in time polynomial in $|\Omega|$, n, q and e (where $V \cong \mathbb{F}_{q^e}^n$).*

- (i) *$H \le G$ and a direct sum $V = V_1 \oplus \cdots \oplus V_m$, where $m \ge 2$, such that $|G : H| = O(m^c)$ for a constant $c > 0$, and either*
  - (a) *$\{V_1, \dots, V_m\}$ is a system of imprimitivity for H, or*
  - (b) *V is a homogeneous kH-module, where $V_1, \dots, V_m$ are irreducible kH-submodules of V of dimension n/m.*
- (ii) *$B \trianglelefteq G$ such that $\bar{B}$ is abelian and $A < B$.*

Proof: We will describe our algorithm in the following two steps. In Step 1, we seek a system of imprimitivity induced by A; if V has no such system, then, in Step 2, we appeal to Propositions 5.8, 5.11.

We may assume that $\bar{G}$ is nonabelian and that G/A is nonsimple.

Step 1 *Reduction to Problem* 15. We solve Problem 15 to find, if it exists, a system of imprimitivity $\mathcal{V} = \{V_1, \dots, V_m\}$ for G induced by A. Unless V is a homogeneous kA-module, we return the result of solving Problem 15, namely, $\bigoplus_{i=1}^m V_i$, for (i)(a) and halt.

Step 2 *V is a homogeneous kA-module*. We note that, in this step, $\bar{A}$ must be cyclic. To begin, via Problem 17, we find $C \trianglelefteq G$ such that $\bar{C} = \mathrm{C}_{\bar{G}}(\bar{A})$. Notice here that $|G : C| \le n$ by Lemma 5.2. Since $|G : A| > n$, it then follows that $A < C$. We next find $N \le C$ such that N/A is a chief factor of G and consider two cases.

If N/A is nonabelian, then we apply the algorithm for Proposition 5.8 and directly return its result for (i)(a) or (i)(b).

If N/A is abelian, then we apply the algorithm for Proposition 5.11 and directly return its result; that is, the pair $(H, \bigoplus_{i=1}^m V_i)$ for (i)(a) or (i)(b), or $B \lhd G$ such that $\bar{B}$ is abelian and $A < B$ for (ii). □

Proof of Theorem 5.1: We now describe, with the help of Proposition 5.12, the top-level algorithm for Theorem 5.1. Recall that, for given $G \le \mathrm{Sym}(\Omega)$ such that $G \in \Gamma_d$ and an irreducible representation $^{-} : G \to \mathrm{GL}(V)$, our goal is to find one of the following.

- (i) $H \le G$ and a direct sum $V = V_1 \oplus \cdots \oplus V_m$, where $m \ge 2$, such that each $\dim_k V_i = n/m$, $|G : H| = O(m^c)$ for a constant $c > 0$, and H acts on $\mathcal{V} = \{V_1, \dots, V_m\}$ as a permutation group of degree m.
- (ii) $A \trianglelefteq G$ such that $\bar{A}$ is abelian and $|G : A| = O(|\Omega| + n)$.

Note that cases (i)(a) and (i)(b) of Proposition 5.12 both fall into case (i) above.

Algorithm We first initialize $A := 1$. While $|G : A| > \max(|\Omega|, d!/2, 24n)$, we repeat the following: (1) Apply the algorithm for Proposition 5.12; (2) if its result is $B \lhd G$ such that $\bar{B}$ is abelian and $A < B$, then we now let $A := B$; else, we return the result and halt. □

References

[1] M. Aschbacher, *On the maximal subgroups of the finite classical groups*, Invent. Math. **76** (1984), 469–514.

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

[3] L. Babai, *On the order of uniprimitive permutation groups*, Ann. of Math. (2) **113** (1981), 553–568.

[4] ______, *On the order of doubly transitive permutation groups*, Invent. Math. **65** (1982), 473–484.

[5] ______, *On the length of chains of subgroups in the symmetric group*, Comm. Algebra **14** (1986), 1729–1736.

[6] 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.

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

[8] 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.

[9] B. Bosma, J. Cannon and C. Playoust, *The* MAGMA *algebra system*. I. *The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[10] P. A. Brooksbank and E. M. Luks, *Testing isomorphism of modules*, J. Algebra **320** (2008), 4020–4029.

[11] P. J. Cameron, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc. **13** (1981), 1–22.

[12] P. J. Cameron, R. Solomon and A. Turull, *Chains of subgroups in symmetric groups*, J. Algebra **127** (1989), 340–352.

[13] R. W. Carter, *Simple groups of Lie type*, Pure Appl. Math., vol. 28, Wiley-Intersci., New York, 1972.

[14] F. Celler, J. Neubüser and C. R. B. Wright, *Some remarks on the computation of complements and normalizers in soluble groups*, Acta Appl. Math. **21** (1990), 57–76.

[15] A. Chistov, G. Ivanyos and M. Karpinski, *Polynomial-time algorithms for modules over finite dimensional algebras*, Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation, Kihei, Hawai'i, July 21–23, 1997, ACM, New York, 1997, pp. 68–74.

[16] J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Math., vol. 163, Springer, New York, 1996.

[17] 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.

[18] The GAP Group, GAP – *Groups, Algorithms, and Programming*, version 4.4.12, 2008 (`http://www.gap-system.org`).

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

[20] O. Goldreich, S. Micali and A. Wigderson, *Proofs that yield nothing but their validity or all languages in* NP *have zero-knowledge proofs*, J. ACM **38** (1991), 691–729.

[21] D. Gorenstein, R. Lyons and R. Solomon, *The classification of the finite simple groups*. *Number* 3. *Part* I. *Chapter* A. *Almost simple* $\mathcal{K}$*-groups*, Math. Surveys Monogr., vol. 40.3, Amer. Math. Soc., Providence, R.I., 1998.

[22] B. Huppert, *Endliche Gruppen*. I, Grundlehren Math. Wiss., Bd. 134, Springer, Berlin, 1967.

[23] M. Jerrum, *A compact representation for permutation groups*, J. Algorithms **7** (1986), 60–78.

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

[25] 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.

[26] W. M. Kantor and D. E. Taylor, *Polynomial-time versions of Sylow's theorem*, J. Algorithms **9** (1988), 1–17.

[27] S. Kohl, *A bound on the order of the outer automorphism group of a finite simple group of given order*, preprint, 2003 (`http://www.gap-system.org/DevelopersPages/StefanKohl/preprints/outbound.pdf`).

[28] D. E. Knuth, *Efficient representation of perm groups*, Combinatorica **11** (1991), 33–44.

[29] C. R. Leedham-Green, *The computational matrix group project*, Groups and Computation. III, Columbus, June 15–19, 1999 (W. M. Kantor and Á. Seress, eds.), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 229–247.

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

[31] M. W. Liebeck and A. Shalev, *Simple groups, permutation groups, and probability*, J. Amer. Math. Soc. **12** (1999), 497–520.

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

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

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

[35] ———, *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.

[36] E. M. Luks and T. Miyazaki, *Polynomial-time normalizers for permutation groups with restricted composition factors*, Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, Villeneuve d'Ascq, July 7–10, 2002, ACM, New York, 2002, pp. 176–183.

[37] ———, in preparation.

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

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

[40] A. Maróti, *On the orders of primitive groups*, J. Algebra **258** (2002), 631–640.

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

[42] ———, *Isomorphism of graphs which are pairwise k-separable*, Inform. and Control **56** (1983), 21–33.

[43] 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.

[44] C. E. Praeger and J. Saxl, *On the orders of primitive permutation groups*, Bull. London Math. Soc. **12** (1980), 303–307.

[45] L. Pyber, *Asymptotic 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.

[46] L. Pyber and A. Shalev, *Asymptotic results for primitive permutation groups*, J. Algebra **188** (1997), 103–124.

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

[48] U. Schöning, *Graph isomorphism is in the low hierarchy*, J. Comput. System Sci. **37** (1988), 312–323.

[49] Á. Seress, *Permutation group algorithms*, Cambridge Tracts in Math., vol. 152, Cambridge Univ. Press, Cambridge, 2003.

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

[51] D. A. Suprunenko, *Matrix groups*, "Nauka", Moscow, 1972 (Russian); English transl., Transl. Math. Monographs, vol. 45, Amer. Math. Soc., Providence, R.I., 1976.

[52] M. Suzuki, *Group theory.* I, II, Iwanami Shoten, Tôkyô, 1977, 1978 (Japanese); English transl., Grundlehren Math. Wiss., Bd. 247, 248, Springer, Berlin, 1982, 1986.

[53] H. Theißen, *Eine Methode zur Normalisatorberechnung in Permutationsgruppen mit Anwendungen in der Konstruktion primitiver Gruppen*, Dissertation, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, 1997.

[54] H. Wielandt, *Permutation groups through invariant relations and invariant functions*, Lecture Notes, Department of Mathematics, The Ohio State University, Columbus, 1969; Reprint, Mathematische Werke/Mathematical Works, vol. 1 (B. Huppert and H. Schneider, eds.), de Gruyter, Berlin, 1994, pp. 237–296.