Journal of Algorithms **31,** 132–195 (1999)
Article ID jagm.1999.0982, available online at http://www.idealibrary.com on IDEAL®

Sylow Subgroups in Parallel*

William M. Kantor†

Department of Mathematics, University of Oregon, Eugene, Oregon 97403

Eugene M. Luks†

Department of Computer and Information Sciences, University of Oregon, Eugene, Oregon 97403

and

Peter D. Mark†

Department of Computer Science, Seattle University, Seattle, Washington 98122

Received February 10, 1997; revised September 21, 1998

Sylow subgroups are fundamental in the design of asymptotically efficient group-theoretic algorithms, just as they have been in the study of the structure of finite groups. We present efficient parallel (NC) algorithms for finding and conjugating Sylow subgroups of permutation groups, as well as for related problems. Polynomial-time solutions to these problems were obtained more than a dozen years ago, exploiting a well-developed polynomial-time library. We replace some of those highly sequential procedures with ones that work through a polylog-length normal series that is a by-product of NC membership-testing. As in previous investigations, we reduce to the base case of simple groups, and handle this by a case-by-case analysis that depends heavily upon the classification of finite simple groups.

1. INTRODUCTION

In computational applications, groups are frequently specified and stored via generators in a permutation action. This tends to be a very terse description, since any permutation group on n letters can be generated by $O(n)$ elements while its order can be exponential in n. Thus, assuming the polynomial-time standard as a measure of efficiency, it is not trivial even

* This research was supported in part by the National Science Foundation.
† E-mail: kantor@math.uoregon.edu, luks@cs.uoregon.edu, peter@seattleu.edu.

0196-6774/99 $30.00

to show that one can efficiently test membership in a group given only by generators. Nevertheless, an ingenious method for this problem, first proposed by Sims in the 1960s [Si], was shown in [FHL] to be in polynomial time. This led to the more substantive issue of whether polynomial time suffices for computation of detailed information about the structure of the group. Considerable subsequent effort has resulted in extensive polynomial-time machinery for such investigations (cf. [KL1] and [Lu5] for surveys). Much of this machinery relies upon finding composition series [Lu4] and Sylow subgroups [Ka1, Ka2, Ka3]. The computational need for these ''building blocks'' is analogous to their critical role within group theory.

The attempt to parallelize the permutation-group machinery has introduced new and profound difficulties. Since the established polynomial-time machinery utilizes inherently sequential procedures (cf. [BL]), novel approaches are required. A start in this direction appears in a series of papers [MC, LM, Lu2, BLS1]. In particular, membership testing was finally shown to be in the class NC. Even for this rudimentary problem, the parallel method differs markedly from the traditional sequential procedures. While Sims's method does not require, or reveal, any of the group structure, the intricate divide-and-conquer of the NC approach makes the construction of a composition series a basic ingredient. The dependence on structural group theory includes essential citations of the monumental classification of all finite simple groups (surveyed, for example, in [Gor2]) for the timing analysis; by contrast, polynomial-time membership testing had been elementary.

Although the machinery of [BLS1] already provides knowledge of the group at hand, it does not include some of the most useful structural information. In particular, [BLS1] cited one of the leading open questions to be the parallelizability of the key problem of finding Sylow subgroups. The sequential solution to this problem was already unique in its heavy use of recent group-theoretic results: although the problem has an elementary formulation, the mathematical underpinnings of the polynomial-time solution include detailed use of the classification of all finite simple groups. In fact, the classification has, so far, been essential even for a polynomial-time solution to the problem of finding elements of order p for a prime $p \mid |G|$ [Ka1].

In this paper, we show that the Sylow problems have NC solutions as well. We prove:

THEOREM 1.1. *Given a permutation group G and a prime p, there are NC solutions to the following problems*:

(i) *Find a Sylow p-subgroup of G.*

(ii) *Given two Sylow p-subgroups* P_1, P_2 *of* G, *find* $g \in G$ *such that* $P_1^g = P_2$.

(iii) *Given any p-subgroup of* G, *find a Sylow p-subgroup of* G *containing it*.

(iv) *Given a Sylow p-subgroup* P *of* G, *find its normalizer* $\mathrm{N}_G(P)$.

The sequential solutions to these problems were developed in [Ka1, Ka2, Ka3]. However, there are very significant differences in the structure of parallel algorithms for permutation groups. Most sequential permutation-group algorithms exploit a sequence of subgroups, $G \geq G_0 \geq G_1 \geq \cdots \geq G_m = 1$. For example, membership testing uses pointwise stabilizers and reduces membership testing for G_i to that for G_{i+1} [Si]; the polynomial-time Sylow algorithms in [Ka1, Ka2, Ka3] used, in addition, a composition series for G. However, these series can have length $\Omega(n)$, and therefore can be too long for step-by-step NC computation. The parallelization of membership testing also uses a series, but of a different sort. In [Lu2] and [BLS1] it was shown that one could construct, and effectively use, a normal series whose length is polylogarithmic in n. The quotients of successive members of the series are *semisimple*: direct products of simple groups. In the base case of simple groups, the parallelization parallels the sequential procedures.

Most of our Sylow procedures work down a normal series, $G = G_0 \rhd G_1 \rhd G_2 \cdots$, as just indicated. The solution to the problem at hand for G/G_i utilizes a solution for G/G_{i-1}. Such recursive use of the normal series requires that we study not just permutation groups, but also quotient groups of permutation groups. This is analogous to the situation for sequential computation: it was demonstrated in [KL1] that one sometimes has to consider general quotients G/K of permutation groups even to resolve the case $K = 1$.

Another aspect of the procedure seems worth highlighting. As in [Ka2, Ka3] and [KL1], we are, in effect, manipulating induced permutation representations in which the new permutation domains are themselves too large to enumerate. One example occurs in the consideration of the transitive action of a permutation group G on its (possibly exponential-size) collection $\mathscr{P}$ of Sylow p-subgroups (where $g \in G$ maps $P \mapsto P^g = g^{-1}Pg$); given two "points" $P_1, P_2 \in \mathscr{P}$, we need to find some $g \in G$ such that $P_1^g = P_2$; parts (ii) and (iv) of the theorem allows us to find *all* such g. The results in [KL1] make it clear that, within algorithmic investigations, this ability to conjugate and find normalizers Sylow subgroups is as important as finding them.

We have not introduced any randomized methods into this paper (compare [Mo, KS]); nor have we dealt with further algorithmic consequences of the results obtained here. Some such consequences will be

dealt with in a later paper [KL2]. These include the ability to work with quotient groups of permutation groups, in the spirit of [KL1].

The basic outline of this work follows the polynomial-time version in [Ka1, Ka2, Ka3]. Some of our results were obtained in [Ma2] by following those references more closely than here: we diverge in various ways, making the overall algorithm shorter and, we hope, clearer. We emphasize that the issue herein is NC computation, so we freely trade efficiency for exposition. In particular, we make no attempt either to optimize worst-case time bounds or to describe efficient implementations. Nevertheless, we note that the need to parallelize has forced streamlining of previous Sylow algorithms [Ka2, Ka3], making the present work of more than theoretical interest. Versions of our algorithms have already been used in [Mo], suggesting that planned sequential implementations will be very efficient.

Overview of the Paper

Section 2 introduces group-theoretic and NC background. Section 3 provides some new or unpublished tools that are of use in contexts beyond the present needs. In Section 4 we present the solvable case of the theorem, generalized so as to include Hall subgroups in addition to Sylow subgroups. This is used in Section 5 to provide the critical reduction of the general case to that of simple groups. Up through this point the group theory can be considered elementary and the reader who accepts the results for simple groups can follow the main algorithms without recourse to the case-by-case details to follow. Only Sections 6 and 7 require detailed knowledge of the structure of finite simple groups. Section 6 constructs the ''natural actions'' of these groups and translates the classical group problems to linear algebra. Section 7 solves the Sylow problems for simple groups.

Table of Problem Names

Because of the large number of named problems and cross-references thereto, the reader may find it convenient to refer back to the following table for the location of problem specifications.

Section 2.2
- ORBIT
- BLOCKS
- MEMBERSHIP
- CONSTRUCTIVE_MEMBERSHIP
- ORDER
- NORMAL_CLOSURE
- DERIVED_SERIES
- POINT_STABILIZER

Section 4
- HALLFIND
- HALLEMBED
- HALLNORM
- HALLCONJ
- HALLFRATTINI

Section 3.1
PRESENTATION

Section 3.2
LIFT
INTERSECTION
FACTOR
SOLVE

Section 3.3
COMPLEMENT
EMBED
EXTRACT_NORMALIZER

Section 3.4
DECOMPOSITION
INVARIANT_COMPLEMENT

Section 3.5
TRANSVERSAL

Section 3.6
SERIES

Section 5.1
SYLFIND_SIMPLE
SYLNORM_SIMPLE
SYLCONJ_SIMPLE
SYLEMBED_SIMPLE
SYLNORMALIZED1_SIMPLE
SYLNORMALIZED2_SIMPLE

Section 5.2
SYLFIND_SS
SYLNORM_SS
SYLCONJ_SS
SYLEMBED_SIMPLE
SYLNORMALIZED1_SS
SYLNORMALIZED2_SS
FRATTINI_SS

Section 5.3
SYLFIND
SYLEMBED
SYLNORM
SYLCONJ
FRATTINI

2. BACKGROUND

This section briefly introduces background: some group-theoretic preliminaries and some of the many known group-theoretic problems for which NC solutions are known.

2.1. *Group-Theoretic Preliminaries*

We recall some standard group-theoretic notions. Others will be reviewed later when they are needed.

The center and derived subgroup of G are denoted $Z(G)$ and G', respectively. The *commutator* of elements $a, b \in G$ is $[a, b] = a^{-1}b^{-1}ab$. For any subsets $S, T \subseteq G$ and $g \in G$, write $S^g = g^{-1}Sg$ and $S^T = \{S^t | t \in T\}$. The subgroup generated by $S \subseteq G$ is denoted $\langle S \rangle$; the *normal closure* of S is then $\langle S^G \rangle$. If $A \leq G$ (denoting subgroup containment), then the *normalizer* of A is $N_G(A) = \{g \in G | A^g = A\}$ and the *centralizer* of A is $C_G(A) = \{g \in G | ag = ga, \forall a \in A\}$. More generally, if $K \trianglelefteq G$ and $A \leq G$, then $N_G(AK/K)$ and $C_G(AK/K)$ denote the subgroups of G contain-

ing K such that $N_G(AK/K)/K = N_{G/K}(AK/K)$ and $C_G(AK/K)/K = C_{G/K}(AK/K)$, respectively. If $A \leq G$, a (*right*) *transversal* for A in G is a complete set of right coset representatives.

We will be concerned with various types of strictly decreasing series $G = L_0 > L_1 > \cdots > L_s = 1$ of subgroups of G. Such a series is a *composition series* if each L_i is normal in the preceding and s is maximal subject to this condition; then each *composition factor* L_{i-1}/L_i of G is a simple group. We introduce another type of series in Section 3.6. This will be a normal series in which all the quotients L_{i-1}/L_i are semisimple, where a *semisimple* group is one that is the direct product of simple groups.

A permutation group is always assumed to be specified by a set of generating permutations: $G = \langle S \rangle$, where S is a subset of the symmetric group $\mathrm{Sym}_n = \mathrm{Sym}(\Omega)$ on an n-set Ω. The (*point*) *stabilizer* of $\omega \in \Omega$ is $G_\omega = \{g \in G | \omega^g = \omega\}$; the *orbit* of ω is $\omega^G = \{\omega^g | g \in G\}$, and G is *transitive* if $\omega^G = \Omega$. Let G_Δ denote the (*set*) *stabilizer* $\{g \in G | \Delta^g = \Delta\}$ of $\Delta \subseteq \Omega$ (this is standard geometric notation, more suitable to our needs than the notion in [Wi]); the permutation group it induces on Δ is G_Δ^Δ. A *block* for a transitive group G is a nonempty subset Δ of Ω such that $\Delta^g \cap \Delta = \varnothing$ or Δ for all $g \in G$. Then G induces a transitive permutation group G^Σ on the corresponding *block system* $\Sigma = \{\Delta^g | g \in G\}$. The trivial blocks are Ω and singletons; G is *primitive* on Ω if these are the only blocks. Standard methodology, both for algorithmic and mathematical purposes, is to reduce questions about general permutation groups first to transitive groups and then to primitive groups.

If G is a group and M is any subgroup, then G/M denotes the set of right cosets, equipped with the usual action of G.

2.2. *Permutation-Group Problems in NC*

We assume familiarity with the complexity class NC. The reader may view this as the class of problems solvable in polylog ($= \log^{\text{constant}} n$) time using a polynomial number of processors. For more formal characterizations as well as a survey of problems in the class, see, for example, [KR].

We list some of the NC permutation-group machinery that we use most frequently. Other problems in NC will be cited as they are needed. Groups are assumed to have been given via generators.

The following two problems were observed to be in NC in [Mc].

Problem. ORBIT
Input: $G \leq \mathrm{Sym}_n$.
Output: *The orbits of* G.

Problem. BLOCKS
Input: $G \leq \mathrm{Sym}_n$; *G transitive*.
Output: *A nontrivial block system for G, if one exists*; *otherwise, a report that G is primitive*.

ORBIT uses a parallel transitive-closure algorithm. BLOCKS uses orbits on pairs to find a block system, specifically: consider the orbits of the pair $\{\alpha, \beta\}$ as the edges in a graph, then the connected component containing α is the unique smallest block containing α and β.

We use two immediate extensions of the BLOCKS procedure. On occasion, we need to find a primitive action of G; for this we find blocks in any nontrivial orbit and repeat the process for the induced action on the blocks ($\log n$ times at most) until a primitive action is obtained. Note that this gives blocks that are each maximal with respect to inclusion. We also need to obtain nontrivial blocks that are minimal; for this, we need only consider in parallel all pairs α, β as above and select the smallest block so obtained.

Underlying most group-theoretic computation is the ability to test membership.

Problem. MEMBERSHIP
Input: $G \leq \mathrm{Sym}_n$; $g \in \mathrm{Sym}_n$.
Output: *Whether or not g is in G*.

MEMBERSHIP is often used implicitly. For example, we may assume that the list of generators for any constructed group is kept "small" by testing in parallel whether each element is in the group generated by its predecessors and, if so, removing it.

A principal announcement in [BLS1] is that MEMBERSHIP is in NC. Still, a simple guarantee that $g \in G$ does not suffice for many applications. We need a proof of membership in the form of a construction of g from the generators of G. If $g \in G = \langle S \rangle$, then g is, of course, a word in S. However, we cannot expect to exhibit such a word for it may require exponential length. For sequential computation, one can construct a polynomial-length *straight-line program from S to g* (see [FHL]), that is, a sequence of elements $h_1, h_2, \ldots, h_m = g$, such that, for all i, either $h_i \in S$ or $h_i = h_j h_k$ for some $j < i$, $k < i$, or $h_i = h_j^{-1}$ for some $j < i$. For parallel computation, we can allow simultaneous construction of a polynomial number of products or inverses in each round, but that alone does not guarantee a polylog bound on the number of rounds. Instead we observe that we have the additional capability of computing h^r for $h \in \mathrm{Sym}_n$ and $r = O(n!)$: in parallel in each cycle of h, this is carried out by reducing r modulo the cycle length (see [Mc]). Thus, for $S \subseteq \mathrm{Sym}_n$, $g \in \mathrm{Sym}_n$, we define an *NC program from S to g* to be a sequence $S = A_0, A_1, A_2, \ldots, A_m$

such that $m = O(\log^c n)$, each $A_i \subseteq \mathrm{Sym}_n$ is of polynomial size, $g \in A_m$, and for all i and all $h \in A_i$, either $h \in A_j A_k$ for some $j < i$, $k < i$, or $h \in A_j^{\pm r}$ for some $j < i$ and $r = O(n!)$. (One can also use a circuit model [KR] to describe NC programs but we find the preceding more convenient for our discussions.)

The results of [BLS1] are actually built around an NC procedure for

Problem. CONSTRUCTIVE_MEMBERSHIP
Input: $G = \langle S \rangle \leq \mathrm{Sym}_n$; $g \in \mathrm{Sym}_n$.
Output: *Whether or not g is in G and, if it is, an NC program from S to g.*

As in sequential methods, the membership test ultimately produces a chain of subgroups $G = G_1 \geq G_2 \geq \cdots \geq G_t = 1$ along with coset representatives for G_i mod G_{i+1} for each i (the indices $|G_i : G_{i+1}|$ are polynomially bounded but the chain is not the point-stabilizer chain utilized in [Si]). Thus, it is pointed out in [BLS1] that we can compute $|G|$, which is the product of the indices $|G_i : G_{i+1}|$.

Problem. ORDER
Input: $G \leq \mathrm{Sym}_n$; $g \in \mathrm{Sym}_n$.
Output: $|G|$.

Remark. We will need a still stronger by-product of the procedures of [BLS1]. The preceding chain $G = G_1 \geq G_2 \geq \cdots \geq G_t = 1$ is actually produced as a refinement of a polylog-length normal series $G = N_1 \trianglerighteq N_2 \trianglerighteq \cdots \trianglerighteq N_r = 1$ wherein N_i/N_{i+1} is semisimple for $1 \leq i < r$ (a careful reading of [BLS1] shows $r = O(\log^2 n)$). We will discuss this at greater length in Section 3.6.

The terms N_i of the normal series are constructed using a normal closure algorithm, which is generalized in [BLS1] to an NC procedure for

Problem. NORMAL_CLOSURE
Input: $H \leq G \leq \mathrm{Sym}_n$.
Output: $\langle H^G \rangle$, *the normal closure of H in G.*

This leads easily to an NC solution to the next problem.

Problem. DERIVED_SERIES
Input: $G \leq \mathrm{Sym}(\Omega)$.
Output: *The derived series* $G, G', G'', \ldots$.

One of the more difficult results in [BLS1] is the computation of arbitrary pointwise stabilizers of sets. However, in this paper, we need only an elementary special case, namely the stabilizer of a single point in the domain. This is obtained, as in sequential computation, via Schreier generators (see, for example, [Si, Lu5]).

Problem. POINT_STABILIZER
Input: $G \leq \mathrm{Sym}(\Omega)$; $\omega \in \Omega$.
Output: $G_\omega = \{g \in G | \omega^g = \omega\}$, *and a transversal for* G_ω *in* G.

3. TOOLS

We describe some consequences of the basic machinery quoted in the preceding section. Some of these use known techniques, though they may not have been observed in the context of NC computation.

3.1. *Presentations*

Presentations are fundamental in many algorithmic situations (see, for example, [BLS1, Lu4, CNW]). Here we recall the required algorithmic setting, and slightly extend a known observation. The resulting algorithm will be critical in the next two sections.

Let $\mathscr{F}(X)$ denote the free group on a set X. Given a map $\phi: X \to G$ into a group G, there is a unique extension of ϕ to a homomorphism $\phi: \mathscr{F}(X) \to G$.

Let $H \trianglelefteq G$. A *constructive presentation of* G *mod* H (or, if $H = 1$, a *constructive presentation of* G) is a 4-tuple $\Pi = (X, \phi, \psi, \mathscr{R})$ in which

$$X \text{ is a set}; \qquad \phi: X \to G; \qquad \psi: G \to \mathscr{F}(X); \qquad \mathscr{R} \subset \mathscr{F}(X)$$

such that

$$g\left(\hat{\phi}\psi(g)\right)^{-1} \in H, \forall g \in G \quad \text{and} \quad \hat{\phi}^{-1}(H) = \langle \mathscr{R}^{\mathscr{F}(X)} \rangle.$$

For computational purposes, it is assumed that Π is input or output by

(i) Specifying $\phi(X)$ and $\mathscr{R}$, and

(ii) Giving a procedure for determining $\psi(g)$ for any $g \in G$.

The following is observed in [Lu4, Sect. 4.2]:

LEMMA 3.1. *Let* $(X, \phi, \psi, \mathscr{R})$ *be a constructive presentation for* G *mod* H. *Then*

(i) $\langle X | \mathscr{R} \rangle$ *is a generator–relator presentation of the group* G/H, *with mutually inverse isomorphisms* $F(X)/\langle \mathscr{R}^{F(X)} \rangle \leftrightarrow G/H$ *naturally induced by* $\hat{\phi}$ *and* ψ.

(ii) *If* $G = \langle \phi(X) \rangle$ *then* $H = \langle \hat{\phi}(\mathscr{R})^G \rangle$. *More generally, if* $G = \langle S \rangle$ *then* $H = \langle (\hat{\phi}(\mathscr{R}) \cup \{s(\hat{\phi}\psi(s))^{-1} | s \in S\})^G \rangle$.

Problem. PRESENTATION
Input: $N \trianglerighteq G \leq \mathrm{Sym}_n$.
Output: *A constructive presentation for G mod N.*

PROPOSITION 3.2. *PRESENTATION is in NC.*

Proof. The case $N = 1$ is proved in [BLS2] (the idea was already implicit in [BLS1]). We review just the construction. As noted in [BLS1], one can construct a chain of subgroups $G = G_1 \geq \cdots \geq G_{m+1} = 1$ along with transversals C_i for G_i mod G_{i+1}, $1 \leq i \leq m$, such that, for any $g \in G$, the factorization $g = c_m \cdots c_1$ with $c_i \in C_i$ is obtainable in NC. (As noted in Section 1, in general, this subgroup chain is *not* Sims's traditional point-stabilizer chain [Si].) We may assume $1 \in C_i$, for all i. Let $S = \bigcup_{i=1}^{m}(C_i \backslash \{1\})$. Let X be a set of cardinality $|S|$ and fix an injection ϕ: $X \to G$ with $\phi(X) = S$. Let ψ: $G \to \mathscr{F}(X)$ satisfy $\psi(g) = \phi^{-1}(c_m) \cdots \phi^{-1}(c_1)$ for any given $g = c_m \cdots c_1$ with $c_i \in C_i$ for $1 \leq i \leq m$ (we take $\phi^{-1}(1)$ to be 1). Finally, set $\mathscr{R} = \{y^{-1}x^{-1}\psi(\phi(x)\phi(y)) | x, y \in X\}$.

For general $N = \langle T \rangle$, start with a constructive presentation $(X, \phi, \psi, \mathscr{R})$ of G. Then $(X, \phi, \psi, \mathscr{R} \cup \{\psi(t) | t \in T\})$ is a constructive presentation for G mod N. ∎

Remark. For many applications, including those herein, it is not necessary to have the words in $\mathscr{R}$ or $\psi(G)$ expressible as polynomial-length strings in X; NC programs (Section 2.2) from X would suffice. However, the presentations resulting from [BLS2] produce words of length $O(n)$.

3.2. *Inverse Images, Solving Equations*

In this section we consider groups that are permutation groups, not necessarily all with the same permutation domain (though it would not be difficult to translate to that case). Of course, when quotient groups appear they are specified as quotients of two permutation groups on the same domain.

Problem. LIFT
Input: *Groups* G, H, K *with* $K \trianglelefteq H$; *a homomorphism* $\rho: G \to H/K$; $h \in H$.
Output: $\{g \in G | \rho(g) \in Kh\}$.

We assume that ρ is specified via a map ρ_0: $S \to H$, where S is a generating set of G, so $\rho(s) = K\rho_0(s)$ for $s \in S$. From this, $\rho(g)$, for any given $g \in G$, may be determined in NC, by copying an NC program (Section 2.2) from S through g to an NC program from $\rho(S)$ through $\rho(g)$.

LEMMA 3.3. *LIFT is in NC.*

Proof. Given any $t \in H$, we can find one $g \in G$ such that $\rho(g) = Kt$, if such a g exists, as follows: CONSTRUCTIVE_MEMBERSHIP yields an NC program from $\rho_0(S) \cup K$ to t (if the membership test fails then $Kt \notin \rho(G)$). The same program, substituting $s \in S$ for $\rho_0(s)$ and 1 for $k \in K$, leads to a suitable g.

Consider the special case $h = 1$: the case of finding the kernel $\{g \in G | \rho(g) \in K\}$. Let $L = \langle \rho_0(S), K \rangle$ (note that $G/\ker(\rho) \cong L/K$). Using PRESENTATION, find a constructive presentation $(\{x_1, \ldots, x_m\}, \phi, \psi, \mathscr{R})$ of L mod K. In parallel, for $1 \le i \le m$, find $g_i \in G$ such that $\rho(g_i) = K\phi(x_i)$ (using the preceding paragraph). Define $\phi'\colon X \to G$ by $\phi'(x_i) = g_i$, and specify a map $\psi'\colon G \to \mathscr{F}(X)$ as follows: given any $g \in G$, determine some $t \in H$ such that $\rho(g) = Kt$ and set $\psi'(g) = \psi(t)$ (it is immaterial which coset representative t is chosen by this procedure). Then $(\{x_1, \ldots, x_m\}, \phi', \psi', \mathscr{R})$ is a constructive presentation for G mod $\ker(\rho)$. By Lemma 3.1(ii), $\ker(\rho)$ is computable via NORMAL_CLOSURE.

To find $\rho^{-1}(Kh)$ for general h, find one $g \in G$ satisfying $\rho(g) = Kh$. Then $\rho^{-1}(Kh) = \ker(\rho)g$. ∎

Remarks. (i) LIFT is applied in this paper in several ways. The first usage is implicit in much of the polynomial-time and NC literature. It is often the case that we deal with some induced representation of $G \le \mathrm{Sym}_n$ on some other domain Δ. Elements constructed in the latter need to be pulled back to Sym_n. In practical computations, even if the element or subgroup is to be constructed in a straight-line or NC program from the images of elements of G, it may have been convenient to restrict attention to Δ without keeping track of discardable intermediate operations in Sym_n. Also, many constructions made with Δ may be the result of the structure of Δ itself (e.g., if G acts on Δ as a classical group in a "natural action"; see Section 6), in which case lifting as before is the only option.

The second important usage occurs in the course of solving systems of equations as will be indicated below. Yet another easy application appears in INTERSECTION.

(ii) The specific problem of finding kernels of induced permutation actions (i.e., of homomorphisms into some Sym_m) was already addressed in [Lu2] and [BLS1]. What has been added here is the observation that the method extends to homomorphisms into quotient groups. For some of our needs, the quotients H/K are abelian; in that special case, it is also possible, even in NC, to represent H/K as a permutation group.

In [BLS1] it was pointed out that NC contains the problem of intersecting groups when one normalizes the other. The following is a slight

generalization and could also be obtained by an extension of the method of [BLS1].

Problem. INTERSECTION
Input: *Groups* H, N *such that* H *normalizes* N; *a permutation* x.
Output: $N \cap Hx$.

LEMMA 3.4. *INTERSECTION is in NC.*

Proof. Note that $N \cap Hx$ is either empty or a coset of $N \cap H$. First test nonemptiness by verifying whether or not $x \in HN$. If it is then $N \cap Hx = \{h \in H \mid \rho(h) = Nx^{-1}\}x$ is computable by LIFT, where $\rho: H \to HN/N$ is induced by the natural homomorphism. ∎

This version of INTERSECTION has an important application:

Problem. FACTOR
Input: *Subgroups* H *and* K *of* G *such that* $G = HK \trianglerighteq K$; $g \in G$.
Output: $k \in K$, $h \in H$ *with* $g = hk$.

COROLLARY 3.5. *FACTOR is in NC.*

Proof. Find $k \in K \cap Hg$ and let $h = k^{-1}g$. ∎

We now turn to another application of LIFT. Fix $\mathbf{g} = (g_1, \ldots, g_r) \in G^r$. For any word $w = w(\mathbf{x}, \mathbf{y}) = w(x_1, \ldots, x_r, y_1, \ldots, y_s)$ in the free group $\mathcal{F}(x_1, \ldots, x_r, y_1, \ldots, y_s)$ on an $(r + s)$-set $\{x_1, \ldots, x_r, y_1, \ldots, y_s\}$, define Φ_w: $G^s \to G$ by

$$\Phi_w(\mathbf{h}) = w(\mathbf{g}, \mathbf{1})^{-1} w(\mathbf{g}, \mathbf{h}) \qquad \text{for } \mathbf{h} \in G^s,$$

where $\mathbf{1} = (1, \ldots, 1) \in G^s$.

LEMMA 3.6. *Let* $K \leq M$ *be normal subgroups of* G *with* M/K *abelian and let* $\bar{g}$ *denote the image of* $g \in G$ *in* G/K. *Then, for any* $w \in \mathcal{F}(x_1, \ldots, x_r, y_1, \ldots, y_s)$, *the map given by*

$$\mathbf{m} \mapsto \overline{\Phi_w(\mathbf{m})} = \Phi_w(\mathbf{m})K$$

is a homomorphism from M^s *into* M/K.

Proof. That $\Phi_w|_{M^s}$ maps into M follows from the congruence $w(\mathbf{g}, \mathbf{1}) \equiv w(\mathbf{g}, \mathbf{m}) \pmod{M}$ for $\mathbf{m} \in M^s$. We show that $\Phi_w|_{M^s}$ induces a homomorphism into M/K by induction on the length $|w|$ of w. For $|w| = 1$: if $w = x_i^{\pm 1}$ then Φ_w is the trivial map, while if $w = y_i^{\pm 1}$ then $\Phi_w(m_1, \ldots, m_s) = m_i^{\pm 1}$. For the inductive step, we observe that $w = uv$ implies $\overline{\Phi_w(\mathbf{m})} = \overline{\Phi_u(\mathbf{m})}^{v(\mathbf{g}, \mathbf{1})} \overline{\Phi_v(\mathbf{m})}$ whenever $\mathbf{m} \in M^s$. ∎

The lemma is the key to an algorithm for

Problem. SOLVE

Input: $G \leq \mathrm{Sym}_n$; *normal subgroups* $K \leq M$ *of* G *with* M/K *abelian*; $\mathbf{g} \in G^r$; *words* $w_1, \ldots, w_q \in \mathscr{F}(x_1, \ldots, x_r, y_1, \ldots, y_s)$.

Output: $\{\mathbf{m} \in M^s | w_i(\mathbf{g}, \mathbf{m}) \in K, 1 \leq i \leq q\}$.

Equivalently, we seek to "solve" the system of congruences

$$w_i(\mathbf{g}, \mathbf{m}) \equiv 1 \pmod{K}, \qquad 1 \leq i \leq q.$$

PROPOSITION 3.7. *SOLVE is in NC.*

Proof. If, for any i, $w_i(\mathbf{g}, \mathbf{1}) \notin M$, then the required set is empty. Otherwise, note that $w_i(\mathbf{g}, \mathbf{m}) \in K$ iff $\Phi_{w_i}(\mathbf{m}) \equiv w_i(\mathbf{g}, \mathbf{1})^{-1} \pmod{K}$. Thus, we seek the inverse image of $(\overline{w_1(\mathbf{g}, \mathbf{1})}, \ldots, \overline{w_q(\mathbf{g}, \mathbf{1})})$ under the homomorphism from M^s to $(M/K)^q$ given by

$$\mathbf{m} \mapsto \left(\overline{\Phi_{w_1}(\mathbf{m})}, \ldots, \overline{\Phi_{w_q}(\mathbf{m})}\right).$$

To interpret this problem as an instance of LIFT, we may consider M^s in its natural action on the disjoint union of s copies of the permutation domain for M; similarly, M^q acts on q copies. ∎

Remarks. (i) As indicated in the proof, the desired output is the inverse image of an element under a homomorphism and is, therefore, a coset of the kernel. In describing the output, the kernel is, of course, specified by generators which, in this case, are s-tuples of permutations.

(ii) In our applications in Section 3.3 the words w_i will be explicitly available. However, it would suffice to specify them via NC programs from the free generators $x_1, \ldots, y_s$, since it is essential only that $\Phi_{w_i}(\mathbf{m})$ be NC-computable for any given $\mathbf{m}$.

(iii) When M/K is semisimple (in particular, when it is elementary abelian), SOLVE has a natural interpretation in terms of linear algebra.

3.3. *Complements*

In this section we deal with three problems that are encountered enroute, respectively, to SYLFIND, SYLEMBED, and SYLNORM. They seem of independent interest. Once again, we will be dealing with subgroups of Sym_n.

For $M \trianglelefteq G$, a *complement of* M *in* G is a subgroup $H \leq G$ such that $G = HM$ and $H \cap M = 1$.

Problem. COMPLEMENT
Input: *Normal subgroups* $K \leq M$ *of* G *with* M/K *abelian.*
Output: *A complement* H/K *to* M/K *in* G/K, *or the assertion that no such complement exists.*

PROPOSITION 3.8. *COMPLEMENT is in NC.*

Proof. Use PRESENTATION to find a constructive presentation $\langle X = \{x_1, \ldots, x_s\}, \phi, \psi, \mathscr{R}\rangle$ for G mod M (recall that ϕ is a map $X \to G$). If a complement H/K exists then it is generated mod K by $\langle \phi(x_1)m_1, \ldots, \phi(x_s)m_s\rangle$ for some $(m_1, \ldots, m_s) \in M^s$, and the s-tuple $(\phi(x_1)m_1, \ldots, \phi(x_s)m_s)$ must satisfy the relations in $\mathscr{R}$. Thus, use SOLVE to determine whether any $(m_1, \ldots, m_s) \in M^s$ satisfies

$$w(\phi(x_1)m_1, \ldots, \phi(x_s)m_s) \equiv 1 \pmod{K}, \qquad \forall w(x_1, \ldots, x_s) \in \mathscr{R}$$

(where SOLVE is called with $\mathbf{g} = (\varphi(x_1), \ldots, \varphi(x_s)) \in G^s$ and the words $w(x_1y_1, \ldots, x_sy_s)$ for $w(x_1, \ldots, x_s) \in \mathscr{R}$); and, if so, find one and set $H := \langle \phi(x_1)m_1, \ldots, \phi(x_s)m_s, K\rangle$. ∎

The preceding should be compared with [CNW, pp. 60–61].

Problem. EMBED
Input: *Normal subgroups* $K \leq M$ *of* G *with* M/K *abelian*; $K \leq H \leq G$ *such that* $H^M = H^G$; $K \leq L \leq G$.
Output: $\{u \in M | L \leq H^u\}$.

Note that, if $L \leq H^u$ for some $u \in G$, then M contains such an element u. As the following proof indicates, the desired output set is either empty or is a coset of a subgroup of M.

PROPOSITION 3.9. *EMBED is in NC.*

Proof. Note that the statement $H^M = H^G$ means that $G = M\mathrm{N}_G(H)$. Then $G \trianglerighteq HM$ and $G \trianglerighteq H \cap M$ (since M/K is abelian, it normalizes $(H \cap M)/K$).

If $L \not\leq HM$ then we output "$\emptyset$."

We suppose $L = \langle T\rangle \leq HM$. Use FACTOR in parallel for each $t \in T$ to express $t = h(t)m(t)$, with $h(t) \in H$, $m(t) \in M$. If $u \in M$ then $h(t)^{-1}t^{u^{-1}} = u^{h(t)}u^{-1}m(t) \in M$, and hence

$$t \in H^u \quad \Leftrightarrow \quad h(t)^{-1}t^{u^{-1}} \in H \cap M.$$

Since M/K is abelian, $M/H \cap M$ is abelian. Hence, we can use SOLVE to find all $u \in M$ satisfying the system

$$h(t)^{-1}utu^{-1} \equiv 1 \pmod{H \cap M}, \qquad \forall t \in T,$$

if any such u exist (the value of the parameter "K" in SOLVE is the present $H \cap M$; with $T = \{t_1, \ldots, t_q\}$, the other parameters in the call to SOLVE can be specified as follows: $r = 2q$, $s = 1$, $w_i(x_1, \ldots, x_r, y) = x_{i+q}^{-1} y x_i y^{-1}$ for $1 \le i \le q$, $\mathbf{g} = (t_1, \ldots, t_q, h(t_1), \ldots, h(t_q))$). ▮

Remark. As the proof indicates, one can weaken the input hypothesis "M/K is abelian" to "$H \cap M \trianglelefteq G$ with $M/H \cap M$ abelian."

Problem. EXTRACT_NORMALIZER
Input: *Normal subgroups $K \le M$ of G with M/K abelian; $K \le H \le G$ such that $H^M = H^G$.*
Output: $\mathrm{N}_G(H)$.

PROPOSITION 3.10. *EXTRACT_NORMALIZER is in NC.*

Proof. For any $s \in G$, $C_s = \{u \in M | su \in \mathrm{N}_G(H)\}$ is nonempty (because $G = M\mathrm{N}_G(H)$) and is, therefore, a left coset of $\mathrm{N}_M(H)$. For the same reason, $\mathrm{N}_G(H)/\mathrm{N}_M(H) \cong G/M$, so if $G = \langle S \rangle$ then $\mathrm{N}_G(H)$ is generated by $\mathrm{N}_M(H)$ and the elements sc_s with one $c_s \in C_s$ for each $s \in S$. Thus, $\mathrm{N}_G(H) = \langle sC_s | s \in S \rangle$.

Since $C_s = \{u \in M | H^s \le H^u\}^{-1}$, these sets may be found in parallel for all $s \in S$ by applying EMBED with $L = H^s$. ▮

Remark. Once again, one can replace the hypothesis "M/K abelian" by the weaker "$H \cap M \trianglelefteq G$ with $M/H \cap M$ abelian."

3.4. *G-Invariant Decompositions*

Let V be a vector space over a field K, and assume that V is equipped with a "form" $(\ ,\ ): V \times V \to K$ such that $(au + bv, w) = a(u, w) + b(v, w)$ and $(u, v) = 0 \Rightarrow (v, u) = 0$ for all $a, b \in K$, $u, v \in V$. The examples we have in mind are symmetric, skew-symmetric, hermitian, and identically zero forms. We call $v, w \in V$ *orthogonal* if $(v, w) = 0$; this is a symmetric relation on V. For any nonempty subset A of V, $A^\perp = \{v \in V | (v, w) = 0, \forall w \in A\}$ is a subspace.

Let $G \le \mathrm{GL}(V)$. A collection $\mathscr{V}$ of nonzero subspaces of V will be called a (G)-*respectful decomposition* if

$$V = \bigoplus_{W \in \mathscr{V}} W, \tag{1}$$

$$\mathscr{V} \text{ is } G\text{-stable}, \tag{2}$$

$$\forall W_1, W_2, W_3 \in \mathscr{V}: (W_1, W_2) \ne 0 \text{ and } (W_1, W_3) \ne 0 \quad \Rightarrow \quad W_2 = W_3. \tag{3}$$

Thus, each member of $\mathscr{V}$ is not orthogonal to at most one other member of $\mathscr{V}$. If $\mathscr{U}$ and $\mathscr{V}$ are respectful decompositions of V, we write $\mathscr{V} \prec \mathscr{U}$ if,

for all $W \in \mathscr{U}$, there is some $W' \in \mathscr{V}$ such that $W \leq W'$. A respectful decomposition $\mathscr{V}$ is called *maximal* if there is no respectful decomposition $\mathscr{U} \neq \mathscr{V}$ such that $\mathscr{V} \prec \mathscr{U}$.

A linear transformation $g: V \to V$ is said to be *orthogonality preserving* if $\forall v, w \in V$, $(w, v) = 0 \Leftrightarrow (v^g, w^g) = 0$. If a subspace A is invariant under a group of orthogonality-preserving transformations, then so is $A^\perp$.

In applications of the results of this section we can treat V as a vector space over the prime field, and let "G" include the multiplicative group of the current field as well as the group we really have in mind. This observation means that we can replace considerations of groups of semilinear transformations by considerations of groups of linear transformations, merely by slight extensions of the acting groups.

Problem. DECOMPOSITION

Input: *V, a polynomial-size vector space with a "form" (,); $G <$ GL(V), a completely reducible group of orthogonality-preserving transformations of V.*

Output: *A maximal G-respectful decomposition $\mathscr{V}$ of V.*

Our algorithm for DECOMPOSITION requires a procedure for finding invariant subspaces complementary to invariant subspaces. Since this subproblem does not require the assumption of a polynomial-size vector space, we extract this subresult and deal with it in a more general setting. We use the fact that solving a system of linear equations is in NC by [Mu].

Problem. INVARIANT_COMPLEMENT

Input: *A set S of linear transformations of a vector space V; an S-invariant subspace $W \leq V$.*

Output: *An S-invariant subspace $U \leq V$ such that $V = U \oplus W$, or the fact that there is no such subspace.*

LEMMA 3.11. *INVARIANT_COMPLEMENT is in NC.*

Proof. We may assume that W is a proper subspace of V. Find any complementary subspace $\hat{U}$ to W, i.e., $V = \hat{U} \oplus W$. For example, follow the standard procedure of adjoining a basis of V to the end of a basis of W and then discarding any vector that is in the span of its predecessors, these tests being performed *in parallel* for all vectors in the sequence; take $\hat{U}$ to be the span of the remaining vectors that are not in W.

The transformations in S act on the vector space $\mathrm{Hom}(\hat{U}, W)$ via $f^s(y) = f(u)^s - f(u^s)$ for $s \in S$, $u \in \hat{U}$. Find $F = \{f \in \mathrm{Hom}(\hat{U}, W) | f^s = 0, \forall s \in S\}$ (this involves solving a homogeneous system of linear equations). If $F = 0$ then no invariant complement to W exists. Otherwise, take $0 \neq f \in F$ and then $U = \{u + f(u) | u \in \hat{U}\}$ is an invariant complement to W. ∎

Remark. In the setting appearing later in Sections 6 and 7, V has polynomial size. In that case, a simple brute-force strategy can be used: for each $v \in V - W$ test whether $W \cap \langle v^G \rangle = 0$, and if so replace W by $W \oplus \langle v^G \rangle$ and iterate.

PROPOSITION 3.12. *DECOMPOSITION is in NC.*

Proof. Test in NC whether G acts irreducibly on V by checking, in parallel for all $0 \neq u \in V$, that $\langle u^G \rangle = V$.

1. *We assume first that G acts irreducibly on V.* In this case, if $0 \neq v \in V$ and T is a right transversal for G_v in G (found using POINT_STABILIZER) then $\langle v^T \rangle = V$ (for $v^T = v^G$ spans a G-invariant subspace); in particular, if $\mathscr{W}$ is a respectful decomposition of V and $v \in W \in \mathscr{W}$, then $\mathscr{W} = W^T$, otherwise the proper subset W^T would span V, contradicting irreducibility and the directness in (1).

For any $0 \neq v \in V$ we can find (in NC) the unique maximal respectful decomposition $\mathscr{W}(v)$ such that $v \in W$ for some $W \in \mathscr{W}(v)$ as follows:

Initially, set $W := \langle v \rangle$. We describe tests for each of the conditions (1), (2), and (3) on $W^T = \{W^{t_1}, \ldots, W^{t_m}\}$ ($t_i \in T$, $1 \leq i \leq m$). In each test, failure leads to a proper increase of W that maintains the invariant: *for any respectful decomposition $\mathscr{U}$ of V with some member containing v, $W \leq U$ for some $U \in \mathscr{U}$*. If that happens, we restart the testing with the increased W. Since each such increase at least doubles $|W|$, the procedure is in NC.

Testing (1). The sum $\sum_{i=1}^{m} W^{t_i}$ is direct iff $|W|^m = |V|$. If this condition fails, we find the minimum k such that $|W|^k \neq |\langle W^{t_i} | 1 \leq i \leq k \rangle|$, i.e., the minimum k such that $\sum_{i=1}^{k} W^{t_i}$ is not direct. Since $|W|^{k-1} \leq |V|$, $k = O(\log|V|)$ and so we can enumerate all k-tuples $(w_1, \ldots, w_k)$, with $w_i \in W^{t_i}$, $1 \leq i \leq k$. Fix one such k-tuple for $w_1 + \cdots + w_k = 0$ with $w_k \neq 0$, the existence of which is guaranteed by the choice of k. If $U \in \mathscr{U}$, where $\mathscr{U}$ is a respectful decomposition, and U contains any one of the subspaces W^{t_i}, for which $w_i \neq 0$, then it must contain them all: by the directness of $\oplus_{U \in \mathscr{U}} U$, the sum of those w_i contained in any one U must be 0 but, by the choice of k, any collection of nonzero terms whose sum is 0 must include w_k. It follows that $W' = \langle (W^{t_i})^{t_k^{-1}} | w_i \neq 0 \rangle$ is contained in any element of any respectful decomposition that contains W. Thus, we set $W := W'$.

Testing (2). Suppose $G = \langle S \rangle$. In parallel for all $s \in S$, $1 \leq k \leq m$, we test whether $W^{t_k s} \in W^T$, since W^T is G-stable iff all these membership tests succeed. If any fails, fix one pair k, s for which $W^{t_k s} \notin W^T$. Since the sum $W^{t_1} + \cdots + W^{t_m} + W^{t_k s}$ is not direct, by enumerating all sums, we find $w_1 + \cdots + w_m + w_{t_k s} = 0$, with $w_i \in W^{t_i}$, $1 \leq i \leq m$ and $0 \neq w_{t_k s} \in$

$W^{t_k s}$. With the same reasoning as in the directness test in (1), we set $W := \langle W, \{W^{t_i (t_k s)^{-1}} | w_i \neq 0\} \rangle$.

Testing (3). Suppose $\exists i, j, k$: $j \neq k$, $(W^{t_i}, W^{t_j}) \neq 0$, $(W^{t_i}, W^{t_k}) \neq 0$ (these tests having been performed in parallel for all i, j, k). If $W \leq U \in \mathscr{U}$, for any respectful decomposition $\mathscr{U}$, then $(U^{t_i}, U^{t_j}) \neq 0$ and $(U^{t_i}, U^{t_k}) \neq 0$ and so $U^{t_j} = U^{t_k}$. This means W^{t_j} and W^{t_k} are in the same element of $\mathscr{U}$ (for any such $\mathscr{U}$) and therefore the same is true for W and $W^{t_k t_j^{-1}}$. Thus, we set $W := W + W^{t_k t_j^{-1}}$.

Once W has passed these three tests, we set $\mathscr{W}(v) := W^T$.

Having computed $\mathscr{W}(v)$ in parallel for all $0 \neq v \in V$, we output a collection of maximum size from $\{\mathscr{W}(v) | 0 \neq v \in V\}$.

II. *Assume now that G does not act irreducibly.* We make the following general observation.

(#) Suppose we have found (in some NC computation) a proper decomposition $V = V_1 \oplus V_2$ wherein each V_i is G-invariant and $(V_1, V_2) = 0$. In such case, we can recursively, and in parallel, compute maximal respectful decompositions for V_1 and V_2, the union of these being a maximal respectful decomposition for V. For the timing, we observe that $|V_i| \leq |V|/2$ so that the depth of such a recursion does not exceed $\log|V|$.

Note that, for any subspace $W \leq V$, $\dim(W) + \dim(W^\perp) \geq \dim(V)$. Hence, if W is a proper G-invariant subspace for which $W \cap W^\perp = 0$, we may apply the above to the decomposition $V = W \oplus W^\perp$.

Find a G-irreducible subspace $W \leq V$ by taking any minimal element in $\{\langle u^G \rangle | 0 \neq u \in V\}$. Find $W^\perp$ (for example, by testing, in parallel, all elements $v \in V$ for orthogonality to all elements of W). Since W is irreducible, $W \cap W^\perp$ is 0 or W.

If $W \cap W^\perp = 0$, use (#).

We may assume $W \leq W^\perp$. If $W^\perp = V$, use INVARIANT_COMPLEMENT to express $V = W \oplus Z$ and apply (#) to this decomposition. (The existence of the complement Z is guaranteed by the complete reducibility of G.)

We may assume $W \leq W^\perp < V$. Use INVARIANT_COMPLEMENT to express $V = W^\perp \oplus U$. It follows that $\dim(U) = \dim(V) - \dim(W^\perp) \leq \dim(W)$. Also $W \cap U^\perp = 0$, otherwise $W \cap U^\perp = W$ since W is irreducible, contradicting $U \cap W^\perp = 0$.

We claim that *U is G-irreducible and* $\dim(U) = \dim(W)$. For, suppose, to the contrary, that $0 \neq U_0 \leq U$ where U_0 is G-invariant and $\dim(U_0) < \dim(W)$. Then $W \cap U_0^\perp \neq 0$ (for $W \cap U_0^\perp = 0$ would imply $\dim(V) \geq \dim(W) + \dim(U_0^\perp) \geq \dim(W) + \dim(V) - \dim(U_0) > \dim(V)$). Since W is irreducible, $W \cap U_0^\perp = W$, contradicting $U \cap W^\perp = 0$.

If $U \cap U^{\perp} = 0$, use (#). Hence, we may assume $U \leq U^{\perp}$.

We now have $U \cap W^{\perp} = 0$, $W \cap U^{\perp} = 0$, $W \leq W^{\perp}$, and $U \leq U^{\perp}$. It follows that $(W \oplus U) \cap (W \oplus U)^{\perp} = 0$. If $W \oplus U < V$ use (#). Hence, we may now assume that $W \oplus U = V$.

Find (by case I) a maximal respectful decomposition $\mathscr{W} = \{W_i\}_{i \in I}$ of W. For $i \in I$, let $U_i := U \cap \langle W_j | j \neq i \rangle^{\perp}$.

We claim that $\mathscr{U} = \{U_i\}_{i \in I}$ *is a maximal respectful decomposition of* U. It is clear that (2) and (3) hold. That $U = \oplus_{i \in I} U_i$ follows from the identification ϕ: $U \cong W^*$, where W^* is the dual space of W, given by $\phi(u)(w) = (u, w)$, for $u \in U$, $v \in W$ (that ϕ is injective follows from $U \cap W^{\perp} = 0$). Namely, $W = \oplus_{i \in I} W_i$ implies $W^* = \oplus_{i \in I} F_i$, where $F_i = \{f \in W^* | f(w_i) = 0\}$, and clearly $F_i = \phi(U_i)$. To see that $\mathscr{U}$ is maximal, we use similar arguments: if $\mathscr{U} \prec \mathscr{U}' = \{U_j'\}_{j \in J}$ then, letting $W_j' = W \cap \langle U_i' | k \neq j \rangle^{\perp}$, we would have $\mathscr{W} \prec \{W_j'\}_{j \in J}$.

Finally, since $(W_j, U_i) \neq 0$ only if $i = j$, $\mathscr{W} \cup \mathscr{U}$ is a maximal respectful decomposition of $V = W \oplus U$. ∎

3.5. *Small-Index Subgroups*

It is often necessary to be able to pass from one permutation representation to a new one. Standard occurrences of this arise from the action on the k-sets of the permutation domain or on a block system. We also need to be able to construct the representation on the cosets of a subgroup of small index that is given only by generators. For this purpose, it suffices to have a right transversal. The following problem was cited in [BLS1] as an open question for NC computation.

Problem. TRANSVERSAL
Input: $H < G \leq \mathrm{Sym}_n$ *with* $|G : H| = O(n^c)$ *for some constant* c.
Output: *A right transversal for* H *in* G.

Remark. A complete NC solution to TRANSVERSAL will appear in [KL2]. In the present paper, we will cite only the special case in which $\log|G|$ is of polylog size (see Section 6.2).

PROPOSITION 3.13. *TRANSVERSAL is in NC if* $|G| = O(n^{c' \log n})$ *for some constant* c'.

Proof. Let ω be any point not fixed by G. Find G_ω and H_ω. Use POINT_STABILIZER to find a transversal C for G_ω in G. Recursively, find a transversal C' for H_ω in G_ω. In parallel, consider all pairs of elements in $C'C$, and use MEMBERSHIP to discard all but one element in each coset of H. The remaining elements form a transversal for H in G.

Clearly, $G = HC'C$, so that $C'C$ contains a transversal of H in G. For the timing, since $|G_\omega| \leq |G|/2$ the depth of the recursion is at most $\log |G|$. ∎

3.6. *Good Series*

A central component of the methods in [BLS1] is the construction of a polylog-length normal series in a given group G, along with "manageable" representations of the successive quotients. For example, CONSTRUCTIVE_MEMBERSHIP "sifts" through these representations. Our algorithms rely on a modification of the series in [BLS1].

Let $K \leq N$ be normal subgroups of $G \leq \mathrm{Sym}_n$ and let p be prime. A *good p-G-series from N to K* is a series of G-normal subgroups

$$\mathscr{G}: N = L_0 \trianglerighteq L_1 \trianglerighteq \cdots \trianglerighteq L_r = K$$

of polylog-length $l(\mathscr{G}) = r$ such that, for each i, L_{i-1}/L_i is either abelian or a direct product of nonabelian simple groups, and, in the latter case, the orders of the simple groups are either all divisible by p or all prime to p. For our applications, we need not only the subgroups L_i in such a series, but also a faithful permutation representation of each nonabelian simple factor T/L_i of L_{i-1}/L_i, i.e., a homomorphism $\pi: T \to \mathrm{Sym}_q$, for some q, with $\ker(\pi) = L_i$. In referring to constructions of good p-G-series, we *always assume these ingredients to be included.*

With this understanding, we require an NC procedure for

Problem. SERIES
Input: *Normal subgroups $K \leq N$ of G; prime p.*
Output: *A good p-G-series from N to K.*

LEMMA 3.14. *SERIES is in NC.*

Proof. We first consider the case $K = 1$, $N = G$. The main construction of [BLS1] produces a series

$$G = M_0 \trianglerighteq M_1 \trianglerighteq \cdots \trianglerighteq M_r = 1,$$

with $r = O(\log^2 n)$ and semisimple quotients M_{i-1}/M_i, each either abelian or a direct product of nonabelian simple groups. Furthermore, in the nonabelian case, the construction includes a permutation representation of the simple factors. Thus, it fails to be a good p-G-series from G to 1 only in the lack of separation of levels according to p-divisibility of simple group orders. Modification to satisfy this requirement involves the possible insertion of an intermediate group for each nonabelian M_{i-1}/M_i: insert between M_{i-1} and M_i the group $\breve{M}_i = \langle T | T/M_i$ is a simple p'-factor of $M_{i-1}/M_i \rangle$. The augmented series is p-G-good. Thus, the simple factors of $\breve{M}_i/M_i$ are a subset of those of M_{i-1}/M_i and we retain their permutation representations. The simple factors of $M_{i-1}/\breve{M}_i$ are of the form $T\breve{M}_i/\breve{M}_i$ where T/M_i is a factor of M_{i-1}/M_i. To obtain a permutation representa-

tion of $T\breve{M}_i/\breve{M}_i$, we determine the image of $x \in T\breve{M}_i$ as follows: use FACTOR to find $t \in T$ such that $xt^{-1} \in \breve{M}_i$, and then take the image of t under the given homomorphism $T \to \mathrm{Sym}_q$.

To construct a good p-G-series from N to K for general K and N, we start with a good p-G-series from G to 1, $G = M_0 \trianglerighteq M_1 \trianglerighteq \cdots \trianglerighteq M_r = 1$. For $0 \le i \le r$, find $L_i := (M_i \cap N)K$ (using INTERSECTION). Then $N = L_0 \trianglerighteq L_1 \trianglerighteq \cdots \trianglerighteq L_r = K$ is a good p-G-series from N to K. For, the natural map $L_{i-1}/L_i \to M_{i-1}/M_i$ is an isomorphism with a normal subgroup of M_{i-1}/M_i. Thus, if L_{i-1}/L_i is nonabelian then it is the direct product of simple groups, all or none of which have order divisible by p; hence, it is the direct product of the nontrivial groups in $\{(T \cap N)K/L_i | T/M_i$ is a simple factor of $M_{i-1}/M_i\}$. A permutation representation of $(T \cap N)K/L_i$ is obtained as before by using FACTOR and (the restriction to $T \cap N$ of) a known homomorphism $T \to \mathrm{Sym}_q$. ∎

Remark. When no confusion can occur we just use the expressions *good G-series* or *good series*. This is the case, for example, when N/K is solvable and hence the prime p is irrelevant. Note that, in this situation, one can employ the derived series (constructible in NC by NORMAL_CLOSURE; see [BLS1]) $N \trianglerighteq N' \trianglerighteq N'' \trianglerighteq \cdots$ to construct a good G-series $N \trianglerighteq N'K \trianglerighteq N''K \trianglerighteq \cdots \trianglerighteq K$ from N to K.

Remark. On occasion, we will construct new good series from old ones.

1. If M is the next-to-last term in a good series $\mathscr{G}$ from N to K, then $\mathscr{G} - \{K\}$ is a good series from N to M.

2. If $\mathscr{G}$ is a good p-G-series from N to L and $\mathscr{G}'$ is a good p-G-series from L to K, then $\mathscr{G} \cup \mathscr{G}'$ is a good p-G-series from N to K.

3. If D normalizes M and $\mathscr{G}$ is a good DM-series from DM to M, use INTERSECTION to construct the good D-series $\{D \cap H | H \in \mathscr{G}\}$ from D to $D \cap M$. The permutation representations of the nonabelian quotients are then obtained as in the proof of Lemma 3.14.

Since we view a good series as a set of groups, these produce good series.

4. SOLVABLE GROUPS

This section includes the NC algorithms for Sylow subgroups of solvable groups. We will need these algorithms not only for permutation groups, but also for solvable quotients of permutation groups. Since the algorithms for handling Hall subgroups [Gor1, p. 231] are not significantly more complicated than those for Sylow subgroups, we will only present the more

general algorithms. However, a reader might wish to replace "Hall" by "Sylow" and π by $\{p\}$ when reading this section, keeping in mind that we are focusing here on the solvable case.

Throughout this section, fix a set π of primes. As usual, π' denotes the complement of π in the set of all primes. Let $G \leq \mathrm{Sym}_n$. We will show that the following problems are in NC.

Problem. HALLFIND
Input: $K \trianglelefteq G \leq \mathrm{Sym}_n$ *with* G/K *solvable*.
Output: *A subgroup* $P \geq K$ *of* G *such that* P/K *is a Hall* π*-subgroup of* G/K.

Problem. HALLEMBED
Input: $K \trianglelefteq G \leq \mathrm{Sym}_n$ *with* G/K *solvable*; *a* π*-subgroup* R/K *and a Hall* π*-subgroup* P/K *of* G/K.
Output: $g \in G$ *with* $R \leq P^g$.

Problem. HALLNORM
Input: $K \trianglelefteq G \leq \mathrm{Sym}_n$ *with* G/K *solvable*; *a Hall* π*-subgroup* P/K *of* G/K.
Output: *A subgroup* $N \geq K$ *of* G *such that* $N/K = \mathrm{N}_{G}(P/K)$.

Direct applications of HALLEMBED will put the following two problems in NC.

Problem. HALLCONJ
Input: $K \trianglelefteq G \leq \mathrm{Sym}_n$ *with* G/K *solvable*; *Hall* π*-subgroups* R/K *and* P/K *of* G/K.
Output: $g \in G$ *with* $R = P^g$.

Problem. HALLFRATTINI
Input: $G \leq \mathrm{Sym}_n$; *normal subgroups* $K \leq M$ *of* G *with* M/K *solvable*; *a Hall* π*-subgroup* P/K *of* M/K.
Output: *A subgroup* $D \trianglerighteq P$ *of* G *such that* $G = DM$.

For the main procedures, it is convenient to assume that *the input already includes a good series* $\mathscr{G}$ *from* G *to* K (the construction of good series is in NC by SERIES).

The following procedure solves HALLFIND. Notation: $\mu(n, \pi) = \prod_{p \in \pi} p^{\lfloor n/p \rfloor}$ (thus, for $x \in \mathrm{Sym}_n$, $\langle x^{\mu(n,\pi)} \rangle$ is the Hall π'-subgroup of $\langle x \rangle$, where $x^{\mu(n,\pi)}$ can be found in NC, as noted in Section 2.2).

procedure hallfind($\mathscr{G}$) ($*$ $\mathscr{G}$ is a good series from G to K $*$)
begin
if $l(\mathscr{G}) = 0$ **then output** G
else ($*$ $l(\mathscr{G}) \geq 1$ $*$)

$M = \langle T \rangle \leftarrow$ the next-to-last term of $\mathscr{G}$;
$H \leftarrow$ hallfind($\mathscr{G} - \{K\}$);
($*$ H/M is a Sylow π-subgroup of G/M $*$)
in parallel for all $t \in T$
$r_t \leftarrow t^{\mu(n,\pi)}$;
$L \leftarrow \langle \{r_t | t \in T\}, K \rangle$;
($*$ $L \trianglelefteq G$ $*$)
use COMPLEMENT to find a complement P/K to L/K in H/K;
output P
end.

PROPOSITION 4.1. *HALLFIND is in NC.*

Proof. Since M/K is abelian, L/K is its Hall π'-subgroup. Hence, any Hall π-subgroup of H/K is a complement to L/K in H/K. Thus, COMPLEMENT is applicable.

The timing is clear since the recursive call involves a shorter good series. ∎

The following procedure solves HALLEMBED.

procedure hallembed($\mathscr{G}$; R; P) ($*$ $\mathscr{G}$ is a good series from G to K $*$)
begin
if $l(\mathscr{G}) = 0$ **then output** 1
else ($*$ $l(\mathscr{G}) \geq 1$ $*$)
$M \leftarrow$ the next-to-last term of $\mathscr{G}$;
$g \leftarrow$ hallembed($\mathscr{G} - \{K\}$; RM; PM);
($*$ $R \leq P^g M$ $*$)
use EMBED to find $x \in M$ such that $R \leq (P^g)^x$;
output gx
end.

PROPOSITION 4.2. *HALLEMBED is in NC.*

Proof. To see that EMBED is applicable, note that P^g/K is a Hall π-subgroup of $P^g M/K$. Hence, $R \leq (P^g)^x$ for some $x \in P^g M$ and clearly such an x exists in M.

The timing is clear since the recursive call involves a shorter good series. ∎

COROLLARY 4.3. *HALLCONJ is in NC.*

Proof. This is a special case of HALLEMBED. ∎

COROLLARY 4.4. *HALLFRATTINI is in NC.*

Proof. Let $G = \langle S \rangle$. In parallel, for each $s \in S$ use HALLCONJ to find $m_s \in M$ such that $(P^s)^{m_s} = P$. Set $D = \langle \{sm_s | s \in S\}, P \rangle$. ∎

The following procedure solves HALLNORM.

procedure hallnorm($\mathscr{G}$; P) (* $\mathscr{G}$ is a good series from G to K *)
begin
  if $l(\mathscr{G}) = 0$ **then output** $\mathscr{G}$;
  else (* $l(\mathscr{G}) \geq 1$ *)
    $M \leftarrow$ the next-to-last term of $\mathscr{G}$;
    $L \leftarrow$ hallnorm($\mathscr{G} - \{K\}$; PM);
      (* $L = \mathrm{N}_G(PM/M) \geq \mathrm{N}_G(P/K)$ *)
    use EXTRACT_NORMALIZER to find $R = \mathrm{N}_L(P/K)$;
      (* $P^L = P^{PM} = P^M$ *)
    output R
end.

PROPOSITION 4.5. *HALLNORM is in NC.*

Proof. We have $\mathrm{N}_G(P/K) = \mathrm{N}_L(P/K)$. EXTRACT_NORMALIZER applies since $P^L = P^M$ by the conjugacy of Hall π-subgroups of PM and of L.

The timing is clear since the recursive call involves a shorter series. ∎

5. REDUCTIONS TO SIMPLE GROUPS

In this section we present NC algorithms for the Sylow problems stated in Section 1, assuming that related problems for simple groups have NC solutions. Section 5.1 states these simple group problems; Section 5.2 extends these to problems for nonabelian semisimple groups, which, in turn, are key ingredients in the solutions in Section 5.3 to the general Sylow problems.

Throughout this section we fix a prime p. Unless otherwise indicated, groups are contained in Sym_n.

5.1. *Simple Group Problems*

NC algorithms for the following problems will be given later, in Section 7. The order of the problems in the following list is the same as that of their solutions in that section.

Problem. SYLFIND_SIMPLE
  Input: *A nonabelian simple group G such that $p \mid |G|$.*
  Output: *A Sylow p-subgroup of G.*

Problem. SYLNORM_SIMPLE
Input: *A nonabelian simple group* G *such that* $p \mid |G|$; *a Sylow* p*-subgroup* P *of* G.
Output: $N_G(P)$.

Problem. SYLCONJ_SIMPLE
Input: *A nonabelian simple group* G *such that* $p \mid |G|$; *Sylow* p*-subgroups* P_1, P_2 *of* G.
Output: $g \in G$ *such that* $P_1^g = P_2$.

Remark. Note that we did not explicitly include the simple group case of SYLEMBED (see Section 5.3), which is incorporated into SYLNORMALIZED2_SIMPLE below.

The following two problems hypothesize a set of automorphisms of a group $G = \langle S \rangle$. We may assume that $u \in \mathrm{Aut}(G)$ is specified by indicating $u(s)$ for $s \in S$; an NC program (Section 2.2) from S to g can be used to determine $u(g)$ for any $g \in G$. In our application of the result, the action of u on G will arise naturally, e.g., by conjugation within a supergroup.

Problem. SYLNORMALIZED1_SIMPLE
Input: *A nonabelian simple group* G *such that* $p \nmid |G|$; $U \subseteq \mathrm{Aut}(G)$ *with* $\langle U \rangle$ *a* p*-group.*
Output: *A Sylow* 2*-subgroup of* G *normalized by* U.

Problem. SYLNORMALIZED2_SIMPLE
Input: *A nonabelian simple group* G *such that* $p \mid |G|$; $U \subseteq \mathrm{Aut}(G)$ *with* $\langle U \rangle$ *a* p*-group.*
Output: *A Sylow* p*-subgroup of* G *normalized by* U.

5.2. *Extensions to Semisimple Group Problems*

Our objective in this section is essentially to replace by ''semisimple'' the ''simple'' assumption in the problems of Section 5.1 (for SYLNORMALIZED1 and SYLNORMALIZED2, we give a more precise formulation of the setting where they are needed). In the application to our main results, the semisimple groups arise as quotients of successive terms in a good series; thus, we assume that we have available the factorization of a semisimple quotient G/K into a product of simple groups and a faithful permutation representation of each simple factor. In any case, the methods of [BLS1] would provide these pieces in NC for any semisimple quotient of permutation groups.

We deal with the following problems.

Problem. SYLFIND_SS
Input: $K \trianglelefteq G$ with G/K nonabelian semisimple such that $p \mid |G/K|$.
Output: *A Sylow p-subgroup of* G/K.

Problem. SYLNORM_SS
Input: $K \trianglelefteq G$ with G/K nonabelian semisimple such that $p \mid |G/K|$; *a Sylow p-subgroup* P/K *of* G/K.
Output: $\mathrm{N}_G(P/K)$.

Problem. SYLCONJ_SS
Input: $K \trianglelefteq G$ with G/K nonabelian semisimple such that $p \mid |G/K|$; *Sylow p-subgroups* P_1/K, P_2/K *of* G/K.
Output: $g \in G$ *such that* $P_1^g = P_2$.

Problem. SYLNORMALIZED1_SS
Input: $K \trianglelefteq G$ *and* $K \trianglelefteq R$, *with* G/K *nonabelian semisimple and normalized by* R, R/K *a p-group and* $p \nmid |G/K|$.
Output: *A Sylow* 2*-subgroup of* G/K *normalized by* R.

Problem. SYLNORMALIZED2_SS
Input: $K \trianglelefteq G$ *and* $K \trianglelefteq R$, *with* G/K *nonabelian semisimple and normalized by* R, R/K *a p-group and* $p \mid |G/K|$.
Output: *A Sylow p-subgroup of* G/K *normalized by* R.

PROPOSITION 5.1. *The above five problems are in NC.*

Proof. We may assume we have $G/K = T_1/K \times \cdots \times T_m/K$ and we have faithful permutation representations π_i: $T_i/K \to \mathrm{Sym}(\Delta_i)$.

For SYLFIND_SS, we apply SYLFIND_SIMPLE in parallel to find Sylow p-subgroups $P_i = \langle S_i \rangle$ of $\pi(T_i/K)$. We may take $P := \langle \pi_i^{-1}(S_i) | 1 \le i \le m \rangle$, computing the inverse images via LIFT.

For SYLNORM_SS, $\mathrm{N}_G(P/K) = \langle \pi_i^{-1}(\mathrm{N}_{\pi_i(G)}(\pi_i(P))) | 1 \le i \le m \rangle$, using SYLNORM_SIMPLE to compute $\mathrm{N}_{\pi_i(G)}(\pi_i(P))$ and then using LIFT.

For SYLCONJ_SS, use SYLCONJ_SIMPLE in parallel for all i to find $h_i \in \pi_i(T_i/K)$ such that $\pi_i(P_1)^{h_i} = \pi_i(P_2)$ and then, by use of LIFT, $t_i \in T_i$ such that $\pi_i(t_i K) = h_i$. Take $g := t_1 t_2 \cdots t_m$. Then $P_1^g = P_2$.

We describe an NC procedure for SYLNORMALIZED2_SS. SYLNORMALIZED1_SS is solved similarly (replacing p by 2). The elements of R permute the factors $\{T_i/K | 1 \le i \le m\}$ of G/K inducing a permutation representation of R on $\{1, 2, \ldots, m\}$. Let $\{i_1, \ldots, i_s\}$ be a set of representatives of the orbits of R in this action. Denoting by R_i the stabilizer in R of i, $1 \le i \le m$, in parallel for each i_k, $1 \le k \le s$:

Use POINT_STABILIZER to find $R_{i_k} = \langle U_{i_k} \rangle$;
find a Sylow p-subgroup P_{i_k} of T_{i_k}/K normalized by R_{i_k}
by applying SYLNORMALIZED1_SIMPLE to the action of U_{i_k} on T_{i_k}/K;
in parallel for each $j \in i_k^R$:
find $r_j \in R$ such that $i_k^{r_j} = j$;
($*$ so P_j is a Sylow p-subgroup of T_j/K normalized by R_j $*$).

Then $\langle P_i | 1 \le i \le m \rangle$ is a Sylow p-subgroup of G/K normalized by R. ∎

That the following is in NC follows from SYLCONJ_SS as in the solution of HALLFRATTINI using HALLCONJ.

Problem. FRATTINI_SS
Input: *Normal subgroups $K < M$ of G with M/K semisimple*; *a Sylow p-subgroup Q/K of M/K.*
Output: *$D \le G$ with $D \trianglerighteq Q$ and $G = DM$.*

5.3. *Solutions to the Main Problems*

We can reduce the main problems to the simple case. To be precise, given NC procedures for the problems in Section 5.2, we show that the following are also in NC.

Problem. SYLFIND
Input: *$K \trianglelefteq G$.*
Output: *A subgroup $P \ge K$ such that P/K is a Sylow p-subgroup of G/K.*

Problem. SYLEMBED
Input: *$K \trianglelefteq G$; subgroups $P \ge K$, $R \ge K$ such that R/K is a p-subgroup and P/K is a Sylow p-subgroup of G/K.*
Output: *$g \in G$ such that $R \le P^g$.*

Problem. SYLNORM
Input: *$K \trianglelefteq G$; a subgroup $P \ge K$ such that P/K is a Sylow p-subgroup of G/K.*
Output: $N_G(P)$.

The next two procedures follow, in sequence, from SYLEMBED exactly as for the HALL analogues in Section 4.

Problem. SYLCONJ
Input: *$K \trianglelefteq G$; subgroups $P \ge K$, $R \ge K$ such that R/K and P/K are Sylow p-subgroups of G/K.*
Output: *$g \in G$ such that $R = P^g$.*

Problem. FRATTINI
Input: *Normal subgroups* $K < M$ *of* G; *a Sylow p-subgroup* Q/K *of* M/K.
Output: $D \leq G$ *with* $D \trianglerighteq Q$ *and* $G = DM$.

As in Section 4, we start the main procedures with the assumption that *the input already includes a good series* $\mathscr{G}$ *from* G *to* K (the construction of $\mathscr{G}$ is in NC by SERIES). In particular, this simplifies the timing arguments. Associated with a good series $\mathscr{G}$ is a triple $\hat{l}(\mathscr{G})$ of nonnegative integers $(l_p(\mathscr{G}), l_{\mathrm{NA}}(\mathscr{G}), l(\mathscr{G}))$, representing, respectively, the number of nonabelian levels with factors divisible by p, the number of nonabelian levels, and the number of levels. The collection of such triples is totally ordered by left-to-right lexicographic ordering. A key to critical timings is the fact that recursive calls involve series with decreased $\hat{l}$, where the number of triples preceding $\hat{l}(\mathscr{G})$ is $O(\log^6 n)$.

The following procedure solves SYLFIND.

procedure sylfind($\mathscr{G}$) (* $\mathscr{G}$ is a good series from $G = \langle S \rangle$ to K *)
begin
  if $l(\mathscr{G}) = 0$ **then output** K
  else (* $l(\mathscr{G}) \geq 1$ *)
    $M \leftarrow$ the next-to-last term of $\mathscr{G}$;
    if M/K is abelian **then**
      $H \leftarrow$ sylfind($\mathscr{G} - \{K\}$);
        (* H/M is a Sylow p-subgroup of G/M *)
      use HALLFIND to find a Sylow p-subgroup P of H/K;
      output P
    else (* M/K is nonabelian semisimple *)
      if M/K is a p'-group **then**
        use SYLFIND_SS to find a Sylow 2-subgroup Q/K of M/K
        use FRATTINI_SS to find $D \leq \mathrm{N}_G(Q)$ such that $G = DM$
      else
        use SYLFIND_SS to find a Sylow p-subgroup Q/K of M/K;
        use FRATTINI_SS to find $D \trianglerighteq Q$ such that $G = DM$;
      use INTERSECTION to construct $D \cap J$ for $J \in \mathscr{G} - \{K\}$
        thereby forming a good series $\mathscr{G}'$ from D to $D \cap M$;
      use SERIES to find a D-invariant good series $\mathscr{G}''$ from $D \cap M$ to K;
      output sylfind($\mathscr{G}' \cup \mathscr{G}''$)
end.

PROPOSITION 5.2. *SYLFIND is in NC.*

Proof. We deal first with the correctness of sylfind.

For M/K abelian, we find a subgroup H that contains a Sylow p-subgroup of G. HALLFIND applies since H/M is a p-group and so H/K is solvable.

For M/K nonabelian semisimple, we need to observe that the group D passed in the recursive calls still contains a Sylow p-subgroup of G. If M/K is a p'-group, we express $G = DM$ and so DK/K contains a Sylow p-subgroup of G/K. If $p \mid\mid M/K\mid$, then D/K contains a Sylow p-subgroup of G/K since $D/D \cap M$ and the isomorphic group $DM/M = G/M$ have the same size Sylow p-subgroups, as do $D \cap M$, Q, and M.

For the timing, we need only check that the recursive call involves good series with lesser $\hat{l}$.

If M/K is abelian then $l_p(\mathscr{G} - \{K\}) = l_p(\mathscr{G})$, $l_{\mathrm{NA}}(\mathscr{G} - \{K\}) = l_{\mathrm{NA}}(\mathscr{G})$, and $l(\mathscr{G} - \{K\}) < l(\mathscr{G})$.

If M/K is nonabelian then the factors in the series $\mathscr{G}'$ are isomorphic to those of $\mathscr{G} - \{K\}$, so we need only compare the levels of $\mathscr{G}''$ with one level M/K of the series $\{M, K\}$. If M/K is a p'-group, then $l_p(\mathscr{G}'') = l_p(\{M, K\}) = 0$. However, $l_{\mathrm{NA}}(\{M, K\}) = 1$, while $l_{\mathrm{NA}}(\mathscr{G}'') = 0$ since $(DK \cap M)/K$ normalizes a Sylow 2-subgroup in M/K and is therefore solvable. If $p \mid\mid M/K\mid$ then $l_p(\{M, K\}) = 1$ but $l_p(\mathscr{G}'') = 0$ since the Sylow p-subgroup, Q/K, of $(D \cap M)/K$ is normal. ∎

The following procedure solves SYLEMBED.

```
procedure sylembed(𝒢; R; P)
  (* 𝒢 is a good series from G = ⟨S⟩ to K *)
begin
  if l(𝒢) = 0 then output 1
  else (* l(𝒢) ≥ 1 *)
    M ← the next-to-last term of 𝒢;
    if M/K is abelian then
      g ← sylembed(𝒢 − {K}; RM; PM);
      use HALLEMBED to find h ∈ P^g M such that R ≤ P^gh;
      output gh
    else (* M/K is nonabelian semisimple *)
      if M/K is a p'-group then
        use SYLNORMALIZED1_SS to find
          a Sylow 2-subgroup Q/K of M/K normalized by R/K;
        use SYLNORMALIZED1_SS to find
          a Sylow 2-subgroup Q_1/K of M/K normalized by P/K;
```

else
use SYLNORMALIZED2_SS to find
a Sylow p-subgroup Q/K of M/K normalized by R/K;
use SYLNORMALIZED2_SS to find
a Sylow p-subgroup Q_1/K of M/K normalized by P/K;
use SYLCONJ_SS to find $m \in M$ so that $Q_1^m = Q$;
use FRATTINI_SS to find $D \trianglerighteq Q$ such that $G = DM$;
$D \leftarrow \langle D, R, P^m \rangle$;
use INTERSECTION to construct $D \cap H$ for $H \in \mathscr{G} - \{K\}$,
thereby forming a good series $\mathscr{G}'$ from D to $D \cap M$;
use SERIES to find a D-invariant good series $\mathscr{G}''$ from $D \cap M$ to K;
$h \leftarrow$ sylembed($\mathscr{G}' \cup \mathscr{G}''$; R; P^m);
output mh
end.

PROPOSITION 5.3. *SYLEMBED is in NC.*

Proof. We deal first with the correctness of sylembed.

If M/K is abelian then $P^g M$ is solvable so that HALLEMBED can be used to find h.

In the nonabelian M/K case, the group D contains R and P^m and therefore will contain some h for which $R \leq P^{mh}$.

For the timing, we check that the recursive calls involve series with lesser $\hat{l}$.

If M/K is abelian, then $l_p(\mathscr{G} - \{K\}) \leq l_p(\mathscr{G})$, $l_{\mathrm{NA}}(\mathscr{G} - \{K\}) = l_{\mathrm{NA}}(\mathscr{G})$, and $l(\mathscr{G} - \{K\}) < l(\mathscr{G})$.

If M/K is nonabelian, note first that $D/(D \cap M) \cong DM/M = G/M$, so the levels for $\mathscr{G}'$ coincide with those for $\mathscr{G}$ from G to M. If $\mathscr{G}_M$ denotes the part of $\mathscr{G}$ from M to K, we need to show that $\hat{l}(\mathscr{G}'') < \hat{l}(\mathscr{G}_M)$. If M/K is a p'-group, $(D \cap M)/K$ normalizes its Sylow 2-subgroup Q/K and hence is solvable; in this case $l_p(\mathscr{G}'') = 0 \leq l_p(\mathscr{G}_M)$ while $l_{\mathrm{NA}}(\mathscr{G}'') = 0 < l_{\mathrm{NA}}(\mathscr{G}_M)$. If $p \,||M/K|$, $(D \cap M)/K$ normalizes its Sylow p-subgroup Q/K, so the nonabelian levels of $(D \cap M)/K$ are p'-groups; in this case $l_p(\mathscr{G}'') = 0 < l_p(\mathscr{G}_M)$. ∎

This yields the following consequences exactly as Corollaries 4.3 and 4.4 follow from Proposition 4.2.

COROLLARY 5.4. *SYLCONJ is in NC.*

COROLLARY 5.5. *FRATTINI is in NC.*

We now turn to SYLNORM, starting with the following special situation we find to be independently interesting: in [KL2] we generalize this to the case $(|P/K|, |M/K|) = 1$.

Problem. SYLNORM1
Input: $K \lhd M$ *and* $K \lhd P$, M *normalized by* P, P/K *a* p*-group and* M/K *a* p'*-group.*
Output: *Find* $\mathrm{N}_M(P)$.

Remark. Note that $\mathrm{N}_M(P) = \mathrm{C}_M(P/K)$. Namely, since $\mathrm{N}_M(P)/K$ and P/K normalize one another and have trivial intersection (since their orders are relatively prime), they centralize one another.

The following procedure solves SYLNORM1.

procedure sylnorm1 (K; M; P)
begin
in parallel for all primes $q \,||M/K|$
use SYLFIND to find a Sylow q-subgroup $\breve{Q}_q/K$ of M/K;
use FRATTINI to express $PM = D_q M$ where $D_q \trianglerighteq \breve{Q}_q$;
use SYLFIND to find a Sylow p-subgroup $\breve{P}/K$ of D_q/K;
use SYLCONJ to find $g \in PM$ such that $\breve{P}^g = P$;
$Q_j \leftarrow \breve{Q}_q^g$;
(* Q_q/K is a Sylow q-subgroup of M/K normalized by P/K *)
use HALLNORM to find $\mathrm{N}_{PQ_q}(P)$;
(* PQ_q/K is solvable *)
use INTERSECTION to find $C_q = Q_q \cap \mathrm{N}_{PQ_q}(P)$;
output $\langle C_q | q$ prime dividing $|M/K| \rangle$
end.

PROPOSITION 5.6. *SYLNORM*1 *is in NC.*

Proof. By [Gor1, p. 224], any P-invariant q-subgroup of M/K is contained in a P-invariant Sylow q-subgroup of M/K and any two P-invariant Sylow q-subgroups of M/K are conjugate by an element of $C_{M/K}(P/K)$. It follows that Q_q/K contains a Sylow q-subgroup of $C_{M/K}(P/K) = \mathrm{N}_{M/K}(P/K)$; hence, C_q/K is that Sylow q-subgroup. The correctness of the procedure follows immediately.
The timing is clear since the cited problems are all in NC. ∎

The following procedure follows SYLNORM.

procedure sylnorm($\mathscr{G}$; P) (* $\mathscr{G}$ is a good series from G to K *)
begin
if $l(\mathscr{G}) = 0$ **then output** K
else (* $l(\mathscr{G}) > 1$ *)
$M \leftarrow$ the next-to-last term of $\mathscr{G}$;
if M/K is abelian **then**
$L \leftarrow$ sylnorm($\mathscr{G} - \{K\}$; PM);
(* $L = \mathrm{N}_G(PM) \geq \mathrm{N}_G(P)$ *)

use EXTRACT_NORMALIZER to find $R = \mathrm{N}_L(P/K)$;
($*$ $P^L = P^{PM} = P^M$ $*$)
output R
else if M/K is nonabelian **and** $p \,||M/K|$ **then**
use INTERSECTION to find $Q = P \cap M$;
($*$ P/K is a Sylow p-subgroup of M/K $*$)
use FRATTINI to express $G = \breve{D}M$ where $\breve{D}$ normalizes Q;
use SYLNORM_SS to find $\mathrm{N}_M(Q)$;
$D \leftarrow \breve{D}\mathrm{N}_M(Q)$;
($*$ so $D = \mathrm{N}_G(Q) \geq \mathrm{N}_G(P)$ $*$);
use INTERSECTION to construct $D \cap H$ for $H \in \mathscr{G} - \{K\}$,
thereby forming a good series $\mathscr{G}'$ from D to $D \cap M$;
use SERIES to find a D-invariant good series $\mathscr{G}''$ from $D \cap M$ to K;
output sylnorm($\mathscr{G}' \cup \mathscr{G}''$; P)
else ($*$ M/K is a p'-group $*$)
$L \leftarrow$ sylnorm($\mathscr{G} - \{K\}$, PM);
use FRATTINI to express $L = D(PM)$, where $D \trianglerighteq P$;
use SYLNORM1 to find $\mathrm{N}_M(P)$;
output $D\mathrm{N}_M(P)$
end.

PROPOSITION 5.7. *SYLNORM is in NC.*

Proof. We deal first with the correctness of sylnorm.

In the case where M/K is abelian, we find $L = \mathrm{N}_G(PM/M) \geq \mathrm{N}_G(P/K)$. Since $PM \trianglelefteq L$, $P^L = P^{PM} = P^M$ by the conjugacy of Sylow subgroups. Hence EXTRACT_NORMALIZER is applicable.

In the case where M/K is nonabelian and $p \,||M/K|$, since $G = DM$, we have $\mathrm{N}_G(P) \leq \mathrm{N}_G(Q) = D$. Hence, $\mathrm{N}_G(P) = \mathrm{N}_D(P)$.

In the case where M/K is a p'-group, FRATTINI applies to find D since $PM \trianglelefteq L$. Then $\mathrm{N}_G(P) = \mathrm{N}_L(P) = D\mathrm{N}_M(P)$.

For the timing, observe that the recursive calls when M/K is abelian or a p'-group simply involve truncated series.

If M/K is nonabelian with $p \,||M/K|$ then we observe that the levels in the series $\mathscr{G}'$ are isomorphic to those of $\mathscr{G} - \{K\}$ (since $G = DM$), so we need only compare the levels of $\mathscr{G}''$ with the one level M/K of the series $\{M, K\}$. We have $l_p(\{M, K\}) = 1$, but $l_p(\mathscr{G}'') = 0$ since the Sylow p-subgroup, Q/K, of $(D \cap M)/K$ is normal. ∎

The following is a simple extension of SYLNORM; stronger results of this sort are in [KL2].

COROLLARY 5.8. *There is an NC solution to the following problem*: *given proper normal subgroups* $K \leq L$ *of the permutation group* G *and a Sylow* p*-subgroup* P/K *of* L/K, *find* $N_G(P)$.

Proof. Use FRATTINI to find $D \trianglerighteq P$ such that $G = DL$. Use SYLNORM to find $N_L(P)$. Output $DN_L(P)$. ∎

6. NATURAL ACTIONS OF SIMPLE GROUPS

In this section and the next we will describe algorithms for simple groups that are required in the previous section.

6.1. *Simple Groups*

According to the classification of finite simple groups, any nonabelian simple group G is one of the following: an alternating group, a classical group, an exceptional group of Lie type, or one of 26 sporadic groups. We can ignore the latter small number of examples. As we will see in Theorem 6.1, exceptional groups of Lie type are too small to create any difficulties (cf. Section 7.2). Alternating groups are, of course, familiar (cf. Section 7.3.2). Therefore, we will spend most of the remainder of this paper studying classical groups.

We will freely use properties of classical groups that can be found in [Di, Ta, As]. We will not, however, provide complete details concerning these groups: that would require a book-length exposition.

A classical group is defined on a finite vector space V over a field K. The most familiar example is $\mathrm{PSL}(V)$, the group of all linear transformations of V of determinant 1, modulo scalar transformations. We have separated this case in Section 6.4, since it is simpler and easier to understand. The reader may wish to first read the remainder of this section, as well as Section 7, when $G = \mathrm{PSL}(V)$.

The remaining classical groups are defined using a quadratic, bilinear, or hermitian form on V: if $\mathrm{Isom}(V)$ denotes the group of all isometries of the form, then, in general, the relevant group is $\mathrm{PIsom}(V)'$, its commutator subgroup modulo scalars. We will introduce further notation when needed. For now, we recall that a *quadratic form* on V is a map $f: V \to K$ such that $f(\alpha v) = \alpha^2 f(v)$ for all $\alpha \in K$, $v \in V$, and such that $(u, v) := f(u + v) - f(u) - f(v)$, $u, v \in V$, defines a nonsingular bilinear form $(\ ,\ )$ on V [Di, Ta, As]. If the characteristic is odd, then $(\ ,\ )$ can be recovered from f, but this is not the case in characteristic 2. For the definitions of alternating and hermitian forms, see [Di, Ta, As].

For a quadratic, alternating, or hermitian form, if we ignore small-dimensional anomalies then $\mathrm{Isom}(V)'$ is $\Omega(V)$ (an orthogonal group), $\mathrm{Sp}(V)$

(a symplectic group), or SU(V) (a unitary group), respectively. Here and elsewhere we will omit the form from the (admittedly ambiguous) notation Isom(V). In the case $G \cong \mathrm{PSL}(V)$ we will occasionally view V as equipped with the 0 form, in which case $\mathrm{Isom}(V) = \mathrm{GL}(V)$. The group PSL($V$), and its *projective* subgroups $G = \mathrm{PIsom}(V)' = \mathrm{PSL}(V)$, P$\Omega(V)$, PSp($V$), or PSU($V$), do not act on V itself: they act on the set of all subspaces of V, and, in particular, on the set $\overline{V}$ of all *points* (1-spaces) of V, and we will focus on this action. If some small-dimensional cases are again ignored, then G is a simple group acting primitively on the point orbit of size relatively prime to the characteristic of V.

Consider any simple group G. Whereas we will start with one permutation action of G, we will need another one: a more ''natural'' action on another set. When G is isomorphic to an alternating group A_r, this ''natural permutation representation'' is that of G on an r-set; when G is isomorphic to a classical group, this permutation representation is on $\overline{V}$. Section 6.2 discusses the reconstruction of this better permutation representation. Sections 6.3–6.5 continue with algorithms concerning classical groups; alternating groups are, as one would expect, much easier to deal with.

The following is crucial for the present paper, as well as for [Ka1, Ka2, Ka3, Ma2, Mo]:

THEOREM 6.1. *If G is a simple primitive subgroup of* Sym(Ω) *with* $|G| \geq |\Omega|^8$, *then G and Ω are as follows* (*up to a permutation isomorphism*):

(I) $G \cong \mathrm{Alt}_r$ *for some r, and Ω is the set of all k-sets of the underlying r-set for some k*;

(II) $G \cong \mathrm{Alt}_r$ *for some r, and Ω is the set of partitions of the underlying r-set into blocks of size k for some k*; *or*

(III) *G is a classical group, and Ω is an orbit of subspaces of an underlying vector space*.

This is proved in [Ka1, (6.1)]. A stronger result of the same sort, assuming $|G| \geq |\Omega|^5$, is proved in [KP, (2.2)]. We have retained the weaker condition $|G| \geq |\Omega|^8$ in order to more easily match up with [Ka1, Ka2, Ka3], as well as to ensure that $\dim(V)$ is large enough to avoid some tedious cases that would require separate treatment.

The proofs depend on the fact that all sufficiently large subgroups of simple groups have been determined, which, in turn, rests heavily on the classification and properties of finite simple groups. Some care must be taken in (III): a symplectic group $\mathrm{Sp}(2m, q)$ and q even should be viewed as an orthogonal group $\Omega(2m + 1, q) \cong \mathrm{Sp}(2m, q)$ in order to obtain all orbits referred to in the result; however, we will not have to deal explicitly with this situation. Also note that, when the group is $G \cong \mathrm{PSL}(d, q)$, there

are again two "underlying" vector spaces, dual to one another but equally good from the standpoint of (III).

6.2. *Finding a Vector Space*

From an algorithmic perspective, it is necessary to pass from the permutation representations in Theorem 6.1(I)–(III) to even better ones:

THEOREM 6.2. *There is an NC algorithm which, when given a simple primitive subgroup G of* $\mathrm{Sym}(\Omega)$ *with* $|G| \geq |\Omega|^8$, *finds one of the following*:

(i) *A set* Ξ *and an action of* G *on* Ξ *as* $\mathrm{Alt}(\Xi)$; *or*

(ii) *A vector space* V *over a field* K, *and an action of* G *on the set* $\Xi = \overline{V}$ *of all* 1*-spaces of* V, *such that one of the following holds*:

(a) $G \cong \mathrm{PSL}(V)$, *or*

(b) *There is a nonsingular quadratic, alternating, or hermitian form on* V *such that* $G \cong \mathrm{PIsom}(V)'$, *in which case such a form is found.*

For the forms implicit in (ii)(b), see Lemma 6.11(i). While we will not need information concerning the procedures used in the proof of this theorem, we present an overview of that proof.

NC algorithms for Theorem 6.2 proceed in three stages:

(α) Construct a set Ξ_0 on which G acts either as $\mathrm{Alt}(\Xi_0)$ or, when G is a classical group, such that Ξ_0 can be identified with a suitable orbit of 1-spaces of an underlying vector space.

(β) When G is classical, reconstruct the set Ξ consisting of *all* 1-spaces of the aforementioned vector space, together with the action of G on Ξ.

(γ) Reconstruct the vector space V from its set Ξ of 1-spaces, as well as the form in (ii)(b).

The following NC algorithm for (α) is essentially the one given in [Ka1, p. 493]; its correctness is proved for the alternating groups, $\mathrm{PSL}(V)$, and the remaining classical groups, respectively, in [Ka2, pp. 494–496, 496–497, 504–505].

procedure natural(G)
($*$ $G \leq \mathrm{Sym}(\Omega)$ is simple, primitive, and $|G| \geq |\Omega|^8$ $*$)
begin
let $\omega = \Omega$;
in parallel for all $\psi \in \Omega$
find $G_{\{\omega, \psi\}}$;
find all proper subgroups N of G of which $G_{\{\omega, \psi\}}$ is a maximal subgroup;
($*$ These are the minimal elements in $\{\langle G_{\{\omega, \psi\}}, t\rangle | t \in T\}$, where T is a TRANSVERSAL for $G_{\{\omega, \psi\}}$ in G. $*$)

$\mathscr{A}_\Omega(\psi) \leftarrow \{G_{\{\omega,\psi\}}\} \cup \{\text{all such } N\}$;
in parallel for all $N \in \mathscr{A}_\Omega(\psi)$
find all I such that $N < I < G$;
(* Each member of $\mathscr{A}_\Omega(\psi)$ is contained in $O(1)$ subgroups of G, so we can find the minimal such I as above, and recursively find all J such that $I < J < G$. *)
$\mathscr{A}_\Omega(\psi)^* \leftarrow \{\mathscr{A}_\Omega(\psi)\} \cup \{\text{all such } I\}$;
$\mathscr{B}(G,\Omega) \leftarrow \{\text{all maximal subgroups of } G \text{ in } \bigcup_\psi \mathscr{A}_\Omega(\psi)^*\}$;
in parallel for for all $M \in \mathscr{B}(G,\Omega)$
find $\mathscr{B}(G, G/M)$;
(* As above. A TRANSVERSAL for M in G can be found and therefore an action of G on G/M. *)
$\mathscr{B} \leftarrow \bigcup\{\mathscr{B}(G,G/M) | M \in \mathscr{B}(G,\Omega)\}$;
in parallel for all $M \in \mathscr{B}$
find $|G: M|$;
find the three smallest such indices $b_0 < b_1 < b_2$, and $L_i \in \mathscr{B}$ with $|G: L_i| = b_i$;
if $b_1 > 4b_0/3$ **then**
$L \leftarrow L_0$
else if $\delta((b_1/b_0)^\delta - 1)^{-1}$ is a power of 3 for $\delta = \pm 1$ **then**
$L \leftarrow L_{\max\{0,\delta\}}$
else if b_i is odd and b_{1-i} is even for $i \in \{0,1\}$ **then**
$L \leftarrow L_i$
else
$L \leftarrow L_2$;
output a TRANSVERSAL for L in G and thereby the action of G on G/L
end.

Remarks. The transversals in the preceding procedure do not actually require the method given in Proposition 3.13, since one is finding transversals for intermediate groups B in C, given $A \le B \le C \le D$, wherein a transversal for A in D is known or easily knowable.

The indices b_0, b_1, b_2 are handled here in a manner designed to correct an arithmetic error in [Ka2, 10.1]; cf. [KL1, p. 175]. It is clear that the preceding algorithm is in NC. While it dealt with cases (I)–(III) simultaneously, there are other ways to handle individual cases. This is especially true for the alternating groups, since this is the most concrete of the cases. From a ''practical'' point of view, the previous algorithm is too space consuming, and this provided motivation for alternative approaches in [KP, Ka4, KS, Mo].

The following is a direct parallelization of the procedure for (β) in [Ka1, pp. 505–506].

procedure allpoints(G)
  (* $G \leq \mathrm{Sym}(\Xi_0)$ with G and Ξ_0 as in natural (G) *)
begin
  if G is 2-transitive on Ξ_0 **then**
    $\Xi \leftarrow \Xi_0$
    output Ξ
  else let $\xi \in \Xi_0$;
  find G_ξ using POINT_STABILIZER;
  use ORBIT to find the G_ξ-orbit on $\Xi_0 - \{\xi\}$ of length a power of a prime p;
  let q be the largest power of p dividing $|\Xi_0| - 1$;
  find G'_ξ using DERIVED_SERIES;
  find $\Delta := G/G'_\xi$ using TRANSVERSAL;
    (* $|G_\xi/G'_\xi| < q < |\Xi_0|$ *)
  let $\alpha \in \Delta$;
  in parallel for all $\beta, \gamma, \delta \in \Delta$
    find $G_{\alpha\beta}$ and $G_{\gamma\delta}$ using POINT_STABILIZER;
    test whether $G_\alpha \neq G_{\alpha\beta}$, $G_\gamma \neq G_{\gamma\delta}$, and $G_{\alpha\beta} < \langle G_{\alpha\beta}, G_{\gamma\delta} \rangle < G$ using ORDER;
    if so **then**
      $M \leftarrow \langle G_{\alpha\beta}, G_{\gamma\beta} \rangle$;
      find a TRANSVERSAL T for H in G;
      while $\exists t \in T$: $M < \langle M, t \rangle < G$
        (* tests are carried out in parallel *)
        replace M by such a $\langle M, t \rangle$;
          (* M is now the unique maximal subgroup of G containing $\langle G_{\alpha\beta}, G_{\gamma\delta} \rangle$ *)
  $\Xi \leftarrow$ {all such M with $|G: M| < q^3|\Xi_0|$};
  output Ξ
end.

The set Ξ "is" the set of all 1-spaces of "the" vector space. If G is $\mathrm{PSL}(d, q)$ then we may have to relabel V^* as V. If G is symplectic then Ξ is just Ξ_0, while for orthogonal and unitary groups Ξ is Ξ_0 together with one or two additional conjugacy classes of subgroups. We note that all of this presumes the input requirement $|G| \geq |\Omega|^8$ of natural(G).

Remark. The procedure for allpoints(G) in [KP] is much more efficient than the preceding one: it only deals with sets of size $O(n)$. However, it is also quite a big longer and makes much more significant use of TRANSVERSAL.

Stage (γ) can be viewed as classical projective geometry: starting with the "geometry" of Ξ, it is required to "coordinatize" Ξ using a vector

space V: construct an explicit G-invariant bijection $\overline{V} \to \Xi$. Once again, NC algorithms are presented in the previous references. The one in [Ka2, Ma2, pp. 371–373] is classical projective geometry based on [VY] (cf. [KP]). Forms are found in [Ka2, p. 375].

Other NC algorithms for all parts of Theorem 6.2 are given in [Ka1, Ka2, KP, Ma2, Mo], as well as in [BLS1] for (i). While some of these papers do not refer to NC at all, the algorithms given in Theorem 6.2 are readily seen to be in NC. Namely, these algorithms use tools available in NC, in view of our Section 3, making it easy for a polynomial-time reader to change perspective minutely in order to become an NC reader. Note that classical groups have order $O(n^{\log^2 n})$, so all subgroup chains involved in the procedures have polylog length and hence recursive calls involving proper subgroups have polylog depth (cf. Lemma 6.3).

Much more than Theorem 6.2 is obtained in [Ka1, KP, Ma2]; this is summarized in the next sections. More recently, other approaches to parts of Theorem 6.2 have been given in [Ka4] and [KS].

6.3. *Classical Groups*: *Preliminaries*

The results stated in Sections 6.3–6.5 *all refer to problems for which NC solutions exist and, in general, are presented.* In this section we merely describe problems for which NC solutions are given in [Ka1, KP, Ma2]. These all deal with "elementary" aspects of managing vectors and forms. The hypotheses of Theorem 6.2 are always presupposed, so that $|G| \geq |\Omega|^8$. Since Ξ will be identified with the set $\overline{V}$ of all 1-spaces of V, we do not merely have a basis available: we can compute and use a list of *all* vectors of V. For (randomized) versions of parts of Sections 6 and 7 in which not all vectors can be listed, see [Mo, KS].

Since $|G| \geq |\Omega|^8$, it is not hard to check the following (compare [Ka1, (6.1iii)]):

LEMMA 6.3. $\dim(V) = O(\log n)$ *and* $\dim(V) > 8$.

This will allow recursion to depth $\dim(V)$ when needed in Sections 6 and 7. Now we turn to *problems already known to be in NC*. In this section we will only mention procedures for elementary linear algebra. These are especially easy in the present context: in effect, we have a list of all vectors of our (small) vector space V (compare Section 3.4). Perpendicularity of sets of vectors is defined in the obvious manner.

LEMMA 6.4. *Given any subset S of Ξ or V, there is an NC algorithm for finding the subspace $\langle S \rangle$ it spans, as well as the subspace $S^\perp$ of all vectors perpendicular to S if $G \not\cong \mathrm{PSL}(V)$.*

LEMMA 6.5. *The following are in NC.*

(i) *Given a subspace W of V and linearly independent vectors $e_1, \ldots, e_i$ in W, find a basis $e_1, \ldots, e_k$ of W containing them.*

(ii) *Given another basis $f_1, \ldots, f_k$ of W, find the linear transformation of W, i.e., the permutation of W it induces, such that $e_i \mapsto f_i$ for $i = 1, \ldots, k$.*

(iii) *For any basis $e_1, \ldots, e_d$ of V and for any $g \in \mathrm{P\Gamma L}(V)$, find $(\alpha_{ij}) \in \mathrm{GL}(V)$ and $\sigma \in \mathrm{Aut}(K)$ such that the semilinear transformation $\sum_i c_i e_i \mapsto \sum_{ij} c_i^{\sigma} a_{ij} e_j$ acts on Ξ as g does.*

(iv) *Find the group $\mathrm{GL}(V)$ of all nonsingular linear transformations of V.*

Of course, (i) is an easy application of Lemma 6.4; special bases will be found later in Lemma 6.11. Note that it is straightforward to find $\mathrm{Aut}(K)$ in NC. Namely, we know the characteristic p, and the map $\alpha \mapsto \alpha^p$ generates $\mathrm{Aut}(K)$.

LEMMA 6.6. *There is an NC algorithm for finding a group G^* of linear transformations of V such that $G^{*\prime} = G^*$ and such that the actions on Ξ of G^* and G coincide.*

Whereas G did not actually act on V, G^* does. The latter group is $\mathrm{SL}(V)$ if G is $\mathrm{PSL}(V)$, $\mathrm{Sp}(V)$ if G is a symplectic group $\mathrm{PSp}(V)$, $\mathrm{SU}(V)$ if G is a unitary group $\mathrm{PSU}(V)$, or $\Omega(V)$ if G is an orthogonal group $P\Omega(V)$. Thus, Lemma 6.6 will allow us to focus on a group that is "almost" the same as G but easier to compute using linear algebra.

6.4. *Classical Groups*: $PSL(V)$

We now turn to NC algorithms going more deeply into the structure of subgroups and subspaces [Ka1, Ma2]. Subspaces will always be nonzero unless the context suggests otherwise. We start with the simplest case: $G = \mathrm{PSL}(V)$. Recall that q is the size of the field K in Theorem 6.2(ii).

LEMMA 6.7. *Given a basis $e_1, \ldots, e_k$ of a subspace W of V, there is an NC algorithm for finding the stabilizer in G of the sequence of subspaces $\langle e_1, \ldots, e_i \rangle$, $i = 1, \ldots, k$.*

Proof. For $0 \le j \le k$, let G_j denote the stabilizer of the sequence $\langle e_1, \ldots, e_i \rangle$, $i = 1, \ldots, j$. By Lemma 6.3, $k = O(\log n)$, so it suffices to show how to compute G_{j+1} given G_j. For this, using Lemma 6.4, we first determine $\langle e_1, \ldots, e_j, e_{j+1} \rangle^{G_j}$, by determining the subspaces $\langle e_1, \ldots, e_j, e \rangle$ in parallel for all $e \in e_{j+1}^{G_j}$ (using ORBIT) and discarding duplicates. In the action of G_j on the (small) resulting collection, G_{j+1} is the POINT_STABILIZER of $\langle e_1, \ldots, e_j, e_{j+1} \rangle$. ∎

Remark. Lemma 6.7 strongly depends upon our ability to list the full orbit of a vector. Given an action of a permutation group G on an arbitrary vector space, the problem of determining the indicated stabilizer is not known even to be in polynomial time. A polynomial-time algorithm for *solvable* G follows from results of [Lu4].

LEMMA 6.8. *Let W be a subspace of V. The following are in NC.*

(i) *Given elements $t, t' \in \mathrm{GL}(W)$ that are irreducible on W and have the same order, find $g \in \mathrm{GL}(W)$ with $\langle t \rangle^g = \langle t' \rangle$.*

(ii) *Find $t \in \mathrm{GL}(W)$ of order $|W| - 1$.*

(iii) *If $t \in \mathrm{GL}(W)$ is irreducible, find the field $K(t)$ of size $|W|$ it spans as a K-algebra of linear transformations, and find the (solvable) groups $\mathrm{C}_{\mathrm{GL}(W)}(t)$, $\mathrm{N}_{\mathrm{GL}(W)}(\langle t \rangle)$, and $\mathrm{N}_{\mathrm{SL}(W)}(\langle t \rangle)$ of order $< |W|\dim(W)$.*

Proof. For (i), find $k := \dim(W)$ using Lemma 6.5(i), fix $u \in W - \{0\}$, and use Lemma 6.5(ii) to test in parallel, for all $v \in W$ and all distinct powers t'^j, whether the linear transformation defined by $u^{t^i} \mapsto v^{(t^j)^i}$, $i = 0, \ldots, k-1$, conjugates t to t'^j.

For (ii), fix a basis of W, form all companion matrices, use Lemma 6.5(ii) to view the corresponding linear transformations in $\mathrm{GL}(W)$ as permutations, and find one of the desired order.

In (iii), by Schur's Lemma [Gor1, p. 76] both $\mathrm{C}_{\mathrm{GL}(W)}(t) \cup \{0\}$ and the desired span $K(t)$ are fields, and $\mathrm{C}_{\mathrm{GL}(W)}(t) \cup \{0\} \supseteq K(t)$. Since $K(t)$ is irreducible, $|K(t)| = |W|$, and hence $\mathrm{C}_{\mathrm{GL}(W)}(t) \cup \{0\} = K(t)$. Finding the span $K(t)$ is straightforward. For the last part of (iii), note that $\mathrm{N}_{\mathrm{GL}(W)}(\langle t \rangle)$ is generated by the multiplicative group of $K(t)$ together with the linear transformation defined by $u^{t^i} \mapsto u^{t^{iq}}$, $i = 0, \ldots, k-1$, obtained using Lemma 6.5(ii); then $|\mathrm{N}_{\mathrm{GL}(W)}(\langle t \rangle)| = (|W| - 1)\dim(W)$, also proving the order assertion. Finally, $\mathrm{N}_{\mathrm{SL}(W)}(\langle t \rangle) = \mathrm{N}_{\mathrm{GL}(W)}(\langle t \rangle) \cap \mathrm{SL}(W)$ can be found using INTERSECTION. ∎

LEMMA 6.9. *The following are in NC.*

(i) *Given a subspace W, find its set stabilizers G'_W and $\mathrm{GL}(V)_W$.*

(ii) *Given subspaces W_1, W_2 of the same dimension, find $g \in G^*$ such that $W_1^g = W_2$.*

Proof. (i) Use Lemma 6.5(i) to find a basis $e_1, \ldots, e_d$ of V such that $e_1, \ldots, e_k$ is a basis of W. Use Lemma 6.7 to find the stabilizer J in G^* of the sequence of subspaces $\langle e_1, \ldots, e_i \rangle$, $i = 1, \ldots, k$. Use Lemma 6.5(ii) to find the linear transformation g of V defined by $e_i \mapsto e_{k+1-i}$, $i = 1, \ldots, k$, fixing all other basis vectors. Then it is easy to check that $\langle J, g \rangle = \mathrm{GL}(V)_W$, and $G^*_W = G^* \cap \mathrm{GL}(V)_W$ is obtained using INTERSECTION.

(ii) Use Lemma 6.5 to find an ordered basis B_i of V starting with a basis of W_i, as well as the linear transformation defined by sending B_1 to B_2. ∎

Note that we could not use POINT_STABILIZER or ORBIT here: in general, W^{G^*} does not have polynomial size.

LEMMA 6.10. *The following are in NC.*

(i) *Given a decomposition* $V = V_1 \oplus \cdots \oplus V_s$, *find its set stabilizers* $G_{\{V_1,\ldots,V_s\}}$ *and* $\mathrm{GL}(V)_{\{V_1,\ldots,V_s\}}$.

(ii) *Given two decompositions in* (i) *for which some element of* G *sends the first to the second, find such an element.*

(iii) *Given a subspace* V_1, *find a maximal-size family* $\{V_1,\ldots,V_m\} \subseteq V_1^G$ *such that* $\langle V_1,\ldots,V_m\rangle = V_1 \oplus \cdots \oplus V_m$.

All parts again use bases in a straightforward manner (cf. Lemma 6.14).

6.5. *Classical Groups*: *Isom*(V)

We now turn to groups preserving forms, as in Theorem 6.2(ii)(b). Thus, throughout the remainder of this section, we assume that V *is equipped with a nonsingular quadratic form* f *having associated bilinear form* $(\ ,\ )$, *or a nonsingular alternating or hermitian form* $(\ ,\ )$. A vector v is called *isotropic* if $(v,v) = 0$; if V is an orthogonal space then v is called *singular* if $f(v) = 0$; the two notions coincide for orthogonal spaces of odd characteristic, but not for ones of characteristic 2. In the orthogonal case we will only consider singular vectors, never isotropic ones when the characteristic is 2, even though this leads to an overuse of phrases such as "isotropic or singular." A subspace is called *totally isotropic* or *totally singular* if all of its vectors are. A subspace W is called *nonsingular* if either $W \cap W^{\perp} = 0$ or V is an orthogonal space of characteristic 2 and W is a 1-space such that $f(W) \neq 0$. Totally isotropic, totally singular, and nonsingular subspaces are the main ones we will need to deal with: *every subspace* W *whose set stabilizer* $\mathrm{Isom}(V)_W$ *acts irreducibly on* W *is one of these*. A subspace W is *anisotropic* if it contains no nonzero isotropic or singular vectors; then $\dim(W) \leq 1$ except when V is orthogonal, in which case $\dim(W)$ can be 2.

If $V_1,\ldots,V_i$ are pairwise perpendicular nonsingular subspaces such that $\langle V_1,\ldots,V_i\rangle = V_1 \oplus \cdots \oplus V_i$, then we write $\langle V_1,\ldots,V_i\rangle = V_1 \perp \cdots \perp V_i$. In particular, if W is a nonsingular subspace and $(W,W) \neq 0$ (where the latter automatically holds except when V is an orthogonal space of characteristic 2 and $\dim(W) = 1$), then $V = W \perp W^{\perp}$.

We now continue with problems having NC solutions.

LEMMA 6.11. *The following are in NC.*

(i) *Find a basis* $e_1, \dots, e_m, f_1, \dots, f_m, u_1, \dots, u_s$ *of* V *such that each* e_i *and* f_i *is isotropic or singular,* $(e_i, f_j) = \delta_{ij}$ *for all* i, j, $(e_i, u_l) = (f_i, u_l) = 0$ *for all* i, l, *and* $\langle u_1, \dots, u_s \rangle$ *is anisotropic* (*so* $s \leq 2$).

(ii) *Find* Isom(V).

(iii) *Find the stabilizers in* G, G^* *and* Isom(V) *of the sequence of subspaces* $\langle e_1, \dots, e_i \rangle$, $i = 1, \dots, m$.

Terminology. We will call a basis in Lemma 6.11(i) a *standard* basis (there is no standard terminology for this purpose); the integer m is uniquely determined by V, and is called the *Witt index* of V.

Proof. To find a standard basis, pick any nonzero isotropic or singular vector e_1 in V, use Lemma 6.4 to pick an isotropic or singular vector $f_1 \notin e_1^{\perp}$ with $(e_1, f_1) = 1$ and to find $\langle e_1, f_1 \rangle^{\perp}$, and iterate. Eventually, an anisotropic subspace remains, of dimension ≤ 2, and a basis is easily found (e.g., by brute force). For (ii), use brute force to find Isom($\langle e_1, f_1 \rangle$), and extend it to a subgroup of Isom(V) inducing 1 on $\langle e_1, f_1 \rangle^{\perp}$; then Isom($V$) = $\langle G^*, \text{Isom}(\langle e_1, f_1 \rangle) \rangle$. Part (iii) is handled exactly as in Lemma 6.7. These procedures are in NC, in view of Lemma 6.3. ∎

More generally, but exactly as in Lemma 6.11:

LEMMA 6.11′. *The following are in NC.*

(i) *Given a nonsingular subspace* W *of* V *and given a sequence* $e_1, \dots, e_k$ *of linearly independent vectors spanning a totally isotropic or totally singular subspace of* W, *find a standard basis for* W *that starts with* $e_1, \dots, e_k$.

(ii) *Find the stabilizers in* G, G^* *and* Isom(V) *of the sequence of subspaces* $\langle e_1, \dots, e_i \rangle$, $i = 1, \dots, k$.

LEMMA 6.12. *Given two standard bases* $e_1, \dots, e_m, f_1, \dots, f_m, u_1, \dots, u_s$ *and* $e'_1, \dots, e'_m, f'_1, \dots, f'_m, u'_1, \dots, u'_s$, *there are NC algorithms for finding an element of* Isom(V) *sending* e_i *to* e'_i *and* f_i *to* f'_i *for each* i *and for finding such an element in* G^* *if one exists* (*there is one except possibly when* V *is an orthogonal space of dimension* $2m$).

Proof. Test in parallel all sequences $u''_1, \dots, u''_s \in \langle u'_1, \dots, u'_s \rangle$ in order to decide whether the linear transformation $e_i \mapsto e'_i$, $f_i \mapsto f'_i$, $u_j \mapsto u''_j$, for all i, j, is in Isom(V) (cf. Lemma 6.5(ii)); there are at most $|K|^2$ sequences, and they are tested using the form. At least one of the resulting transformations lies in G^*, except when $G^* = \Omega^+(2m, q)$ (see [Di, Ta, As] for discussions of this exceptional behavior of these particular orthogonal groups; also see Proposition 7.6(ii)). ∎

Note that, in general, there is no isometry sending $u_j \mapsto u'_j$ for the original vectors u'_j.

LEMMA 6.13. *Given a subspace W that is either totally isotropic, totally singular, or nonsingular, the following are in NC.*

(i) *Find the set stabilizers* $\mathrm{Isom}(V)_W$ *and* G^*_W (*in particular, find* $\mathrm{Isom}(V)$); *and*

(ii) *Given a subspace W', decide whether or not $W' \in W'^{G^*}$, and, if it is, then find $g \in G^*$ such that $W^g = W'$.*

Remark. We cannot use POINT_STABILIZER or ORBIT here: in general W^{G^*} does not have polynomial size.

Proof. (i) If W is totally isotropic or totally singular, use Lemma 6.11′ to find a standard basis $e_1, \ldots, e_m, f_1, \ldots, f_m, u_1, \ldots, u_s$ of V starting with a basis $e_1, \ldots, e_k$ of W, and to find the stabilizer J in $\mathrm{Isom}(V)$ of the sequence of subspaces $\langle e_1, \ldots, e_i \rangle$, $i = 1, \ldots, k$. Let g be the linear transformation defined by $e_i \mapsto e_{k+1-i}$, $f_i \mapsto f_{k+1-i}$, for $i = 1, \ldots, k$, and fixing all other basis vectors (cf. Lemma 6.5(ii)). Then it is easy to check that $\langle J, g \rangle = \mathrm{Isom}(V)_W$, so $G^*_W = G^* \cap \mathrm{Isom}(V)_W$ can be obtained using INTERSECTION.

If W is a nonsingular 1-space in an orthogonal vector space V of characteristic 2, then $\mathrm{Isom}(V)_W$ and G^*_W are obtained as point stabilizers in the actions on $\Xi = \overline{V}$.

If W is nonsingular and $(W, W) \neq 0$, use Lemma 6.4 to find $W^\perp$; here, $V = W \perp W^\perp$. Use Lemma 6.11′ to find a standard basis $e_1, \ldots, e_k, f_1, \ldots, f_k, u_1, \ldots, u_s$ of W. As in Lemma 6.11′(ii), find the stabilizer J in $\mathrm{Isom}(V)$ of the sequence of subspaces $\langle e_1, \ldots, e_i \rangle$ for $i = 1, \ldots, k$, $\langle e_1, \ldots, e_k, u_1, \ldots, u_s \rangle$ (recall that $s \leq 2$), $\langle e_1, \ldots, e_k, u_1, \ldots, u_s, f_j, \ldots, f_k \rangle$ for $j = k, \ldots, 2$, $\langle e_1, \ldots, e_k, u_1, \ldots, u_s, f_1, \ldots, f_k \rangle = W$. Let g be the linear transformation defined by $e_i \mapsto f_i \mapsto \pm e_i$ for all i and fixing all u_j, where the sign is chosen so that $g \in \mathrm{Isom}(W)$; extend g to all of V by requiring that it induces the identity on $W^\perp$. Then it is easy to check that $\langle J, g \rangle = \mathrm{Isom}(V)_W$. Once again, $G^*_W = G^* \cap \mathrm{Isom}(V)_W$ can be obtained using INTERSECTION.

(ii) If W is totally isotropic or totally singular, we may assume that W' is totally isotropic or totally singular of the same dimension as W. Find standard bases for V starting with bases for W and W', using Lemma 6.11′. Now use Lemma 6.12 to obtain the desired element of G^* if there is one.

Next assume that W is nonsingular. If $\dim(W) = 1$ we can use ORBIT for the action of G on Ξ, so suppose that $\dim(W) > 1$ and hence $V = W \perp V^\perp$. Use the approach in Lemmas 6.11′ and 6.12 to try to find

ordered standard bases B and B' of W and W' such that the order-preserving map $B \to B'$ arises from an isometry $W \to W'$; if the approach in those lemma fails then W and W' are not isometric and hence certainly $W' \notin W^{G^*}$. By Witt's Lemma [Di, Ta, As], if W and W' are isometric then so are $W^\perp$ and $W'^\perp$. Again using standard bases as in Lemmas 6.11′ and 6.12, find an isometry $W^\perp \to W'^\perp$ (cf. Lemma 6.4). Together these isometries yield an isometry h of V sending W to W'.

Use INTERSECTION to find $G^* \cap \mathrm{Isom}(V)_W h$. If this is empty then $W' \notin W^{G^*}$; if it contains an element g then output g. ∎

LEMMA 6.14. *The following are in NC.*

(i) *Find a representative of each G^*-orbit of totally isotropic or totally singular subspaces of V.*

(ii) *Find a representative of each G^*-orbit of nonsingular subspaces of V.*

(iii) *For a given W in* (ii) *such that $(W, W) \neq 0$, find a maximal-size family $\{W_1, \ldots, W_k\}$ of members of W^{G^*} such that $\langle W_1, \ldots, W_k \rangle = W_1 \perp \cdots \perp W_k$, and find its set stabilizers $\mathrm{Isom}(V)_{\{W_1, \ldots, W_k\}}$ and $G^*_{\{W_1, \ldots, W_k\}}$.*

(iv) *Given two families in* (iii) *arising from the same orbit W^{G^*}, find an element of G^* sending one to the other if there is one.*

Proof. (i) and (ii) Representatives of all G^*-orbits of totally isotropic or totally singular subspaces appear in Lemma 6.11(iii), except when $G^* = \Omega^+(2m, q)$, in which case there is a unique further orbit, represented by $\langle e_1, \ldots, e_{m-1}, f_m \rangle$ [Ta, As] (cf. Proposition 7.6(ii)).

ORBIT, applied to the action of G on Ξ, produces representatives in the case of 1-spaces.

This leaves the case of nonsingular subspaces W of dimension $l > 1$. For each l there are at most two orbits of such subspaces of V [Di, Ta, As]. If $l = 2k$ is even, then one orbit contains $\langle e_1, \ldots, e_k, f_1, \ldots, f_k \rangle$ (in the notation of Lemma 6.11(i)). If $l = 2k + 1$ is odd and V is unitary, then there is just one orbit, and a representative is $\langle e_1, \ldots, e_k, f_1, \ldots, f_k, u_1 \rangle$ for a nonsingular $u_1 \in \langle e_1, \ldots, e_k, f_1, \ldots, f_k \rangle^\perp$. If V is an orthogonal space, then one of the following occurs.

- $l = 2k$ is even, and every nonsingular l-space of V is in the G^*-orbit containing $\langle e_1, \ldots, e_k, f_1, \ldots, f_k \rangle$ or $\langle e_1, \ldots, e_{k-1}, f_1, \ldots, f_{k-1}, u_1, u_2 \rangle$, where $\langle u_1, u_2 \rangle$ is an anisotropic 2-space lying in $\langle e_1, \ldots, e_{k-1}, f_1, \ldots, f_{k-1} \rangle^\perp$; such a 2-space can be found using Lemma 6.4 and brute force;

• $l = 2k + 1$ and q are both odd, and $W = \langle e_1, \ldots, e_k, f_1, \ldots, f_k, u_1 \rangle$ for a nonsingular $u_1 \in \langle e_1, \ldots, e_k, f_1, \ldots, f_k \rangle^\perp$; the isometry type of W is determined by the element $(u_1, u_1)K^{*2}$ of the group $K^*/K^{*2} \cong \mathbb{Z}_2$; u_1 can be found using Lemma 6.4 and brute force.

(iii) Let $W_1 = W$. Use Lemma 6.4 to find $W_1^\perp$. As in Lemma 6.13(ii) test whether $W_1^\perp$ contains some $W_2 \in W_1^G$. Iterate in order to find a family of the desired sort (compare DECOMPOSITION).

Let $\{W_1, \ldots, W_k\}$ be such a family. Then $V = W_1 \perp \cdots \perp W_{k+1}$, where $W_{k+1} = \langle W_1, \ldots, W_k \rangle^\perp$. Find $\mathrm{Isom}(V)_{W_i}$ for $1 \le i \le k + 1$, using Lemma 6.13(i).

For $i = 2, \ldots, k$ in parallel, we have $W_i = W_1^{g_i}$ with $g_i \in \mathrm{Isom}(V)$; use g_i to define an isometry g_i' of V that agrees with g_i on W_1, with g_i^{-1} on W_i, and induces the identity on all other W_j. Then $\mathrm{Isom}(V)_{\{W_1, \ldots, W_k\}}$ is generated by these transformations g_i' together with all of the groups $\mathrm{Isom}(V)_{W_i}$, $1 \le i \le k + 1$. As usual, $G^*_{\{W_1, \ldots, W_k\}}$ is determined as $G^* \cap \mathrm{Isom}(V)_{\{W_1, \ldots, W_k\}}$.

(iv) Let $\{W_1, \ldots, W_k\}$ and $\{W_1', \ldots, W_k'\}$ be two such families. Let $V = W_1 \perp \cdots \perp W_{k+1}$ and $V = W_1' \perp \cdots \perp W_{k+1}'$, as above. By Witt's Lemma [Di, Ta, As], W_{k+1} and W_{k+1}' are isometric. Exactly as in Lemma 6.13(ii), find an isometry h of V taking W_i to W_i' for all i, and find and output an element g of $G^* \cap \mathrm{Isom}(V)_{\{W_1, \ldots, W_k\}} h$ if one exists. ∎

LEMMA 6.15. *Given a nonsingular subspace W of Witt index $\frac{1}{2}\dim(W)$, there are NC algorithms for finding totally isotropic or totally singular subspaces E, F, such that $W = E \oplus F$, and for finding the set stabilizers $\mathrm{Isom}(V)_{\{E,F\}}$ and $G^*_{\{E,F\}}$ of any such pair $\{E, F\}$.*

Proof. For the first part, use Lemma 6.11′(i) to find a standard basis $e_1, \ldots, e_k, f_1, \ldots, f_k$ of W, and let $E = \langle e_1, \ldots, e_k \rangle$ and $F = \langle f_1, \ldots, f_k \rangle$. In the second part, for each nonsingular $k \times k$ matrix A, form its inverse transpose A^{-t}—except that $\bar{A}^{-t}$ is used in the unitary case (where the "overbar" denotes the involutory automorphism of K and is applied to each entry of A). With respect to our basis of W, the isometry of W produced by the matrix $\left(\begin{smallmatrix} A & O \\ O & A^{-t} \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} A & O \\ O & \bar{A}^{-t} \end{smallmatrix}\right)$ is an isometry. Let h be the isometry of W defined by the matrix $\left(\begin{smallmatrix} O & I \\ \delta I & O \end{smallmatrix}\right)$, where δ is -1 if V is symplectic and 1 otherwise. As usual, we obtain isometries of V by inducing 1 on $W^\perp$. Also, use Lemma 6.13 to find $\mathrm{Isom}(W^\perp)$, and extend this to a subgroup of $\mathrm{Isom}(V)$ by inducing 1 on W. It is easy to check that the isometries of V just constructed generate $\mathrm{Isom}(V)_{\{E,F\}}$. Finally, find $G^*_{\{E,F\}} = G^* \cap \mathrm{Isom}(V)_{\{E,F\}}$ using INTERSECTION. (N.B.—We could also have used stabilizers of sequences of subspaces as in Lemma 6.13(i)),

but we will need the matrix point of view in the algorithm for Lemma 6.17(i).) ∎

Notation 6.16. Let $q = |K|$ if G is symplectic or orthogonal, and let $q^2 = |K|$ if G is unitary.

LEMMA 6.17. *Suppose that a nonsingular subspace W of V is given. Then the following are in NC.*

(i) *Given totally isotropic or totally singular spaces E and F such that $W = E \oplus F$, find $t \in \mathrm{Isom}(W)$ of order $|E| - 1$ fixing E and F, and find the solvable groups $\mathrm{C}_{\mathrm{Isom}(W)}(t)$ and $\mathrm{N}_{\mathrm{Isom}(W)}(\langle t \rangle)$.*

(ii) *Given E, F as in* (i) *and given $t, t' \in \mathrm{Isom}(W)$ irreducible on E, fixing F, and having the same order, find $g \in \mathrm{Isom}(W)$ such that $\langle t \rangle^g = \langle t' \rangle$.*

(iii) *Given $t, t' \in \mathrm{Isom}(W)$ irreducible on W and having the same order, find $g \in \mathrm{Isom}(W)$ such that $\langle t \rangle^g = \langle t' \rangle$, and find the solvable groups $\mathrm{C}_{\mathrm{Isom}(W)}(t)$ and $\mathrm{N}_{\mathrm{Isom}(W)}(\langle t \rangle)$.*

(iv) *Given that $\mathrm{Isom}(W)$ contains an element of order $\sqrt{|W|} + 1$, find one.*

Proof. (i) As in Lemma 6.15, find a basis of W consisting of a basis of E and the dual basis of F with respect to $(\ ,\ )$. Let g act on E as in Lemma 6.8(ii), find its matrix A with respect to the basis of E, and extend g to act on W by using $\left(\begin{smallmatrix} A & O \\ O & A^{-t} \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} A & O \\ O & \bar{A}^{-t} \end{smallmatrix}\right)$ as in the proof of Lemma 6.15.

The matrices A and A^t both generate fields of $|E|$ matrices. Find an integer j such that A and A^{-tj} have the same minimal polynomial (testing all $1 \le j < |E|$ in parallel). Find $M \in \mathrm{GL}(E)$ such that $M^{-1}AM = A^{-tj}$. Then $\mathrm{N}_{\mathrm{Isom}(W)}(\langle t \rangle$ is generated by $\mathrm{N}_{\mathrm{Isom}(W)}(\langle t \rangle)_{E,F}$ and $\left(\begin{smallmatrix} O & M \\ \delta M^{-t} & O \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} O & M \\ \bar{M}^{-t} & O \end{smallmatrix}\right)$ for δ in the preceding lemma, where generating matrices $\left(\begin{smallmatrix} B & O \\ O & B^{-t} \end{smallmatrix}\right)$ (or $\left(\begin{smallmatrix} B & O \\ O & \bar{B}^{-t} \end{smallmatrix}\right)$) in $\mathrm{N}_{\mathrm{Isom}(W)}(\langle t \rangle)_{E,F}$ are obtained from the generators B of $\mathrm{N}_{\mathrm{GL}(E)}(\langle A \rangle)$ found in Lemma 6.8(iii).

(ii) This is an immediate consequence of Lemma 6.8(i): if A is the conjugating matrix obtained there then use $g = \left(\begin{smallmatrix} A & O \\ O & A^{-t} \end{smallmatrix}\right)$ (or $\left(\begin{smallmatrix} A & O \\ O & \bar{A}^{-t} \end{smallmatrix}\right)$ in the unitary case) with respect to our dual bases of E and F.

(iii) The first part is handled exactly as in the proof of Lemma 6.8(i), but including a check of whether each of the linear transformations tested there is an isometry of our form. For the second part, find $\mathrm{N}_{\mathrm{GL}(W)}(\langle t \rangle)$ as in Lemma 6.8(iii), enumerate its elements, and check in parallel to find those that are isometries of W.

(iv) This is harder. First we need a list of the groups in question: the only groups $\mathrm{Isom}(W)$ containing an element irreducible on W are $\mathrm{Sp}(2l, q)$ or $\Omega^-(2l, q)$, or $\mathrm{SU}(l, q)$ with l odd. (This can be checked using, for example, the order formulas in [Gor1]; cf. [Ka1, Ka2, Ka3].)

Consider any one of these cases. Find *any* element t of $\mathrm{GL}(W)$ as in Lemma 6.8(ii). Then $L = \langle t \rangle \cup \{0\}$ is a field of size $|W| = q^{2l}$; as usual, let "overbar" denote its involutory automorphism. Find $\lambda \in L$ with $\bar{\lambda} = -\lambda \neq 0$. Let $\mathrm{Tr}_{e,f}$ denote the trace map $\mathrm{GF}(q^e) \to \mathrm{GF}(q^f)$ between subfields of L. Identify K with the subfield of L of order $|K|$. Define forms on the K-space L as follows, for all $a, b \in L$:

$(a, b)' = \mathrm{Tr}_{2l,1}(\lambda a\bar{b})$ if V is symplectic.

$(a, b)' = \mathrm{Tr}_{2l,2}(a\bar{b})$ if V is unitary, and

$f'(a) = \mathrm{Tr}_{l,1}(a\bar{a})$ if V is orthogonal; the associated bilinear form is $(a, b)' = \mathrm{Tr}_{l,1}(a\bar{b} + \bar{a}b) = \mathrm{Tr}_{2l,1}(a\bar{b})$.

(Of course, it is only necessary to define any of these forms using a basis of L.) Then L, equipped with this form, is isometric to the subspace W in (iv). The transformation $r\colon x \mapsto ax$ is an isometry whenever $a \in L$ and $a\bar{a} = 1$. Choose a of order $q^l + 1$.

As in Lemma 6.11′(i), find a standard basis of L with respect to the preceding form. Use it to find an isometry $g\colon L \to W$ exactly as was done in the proof of Lemma 6.12. Then $g^{-1}rg$ is an isometry of W behaving as required in (iv). ∎

7. SIMPLE GROUP ALGORITHMS

We continue the discussion in Section 6 by presenting algorithms for the problems in Section 5.1. Throughout this section, let G denote an alternating group or a simple classical group. We always assume that G arose from an "original" set Ω. If $|G| < |\Omega|^8$ then brute force will be used. If $|G| \geq |\Omega|^8$, we assume that the set Ξ in Theorem 6.2 has already been found, as has the underlying vector space V and form in the cases of classical groups.

Each algorithm will be split into three pieces: the brute-force case (Section 7.2), the alternating group case (Section 7.3), and the classical group case (Sections 7.4–7.6). Of course, the latter is the only one requiring effort. Moreover, if G is a classical group, our task is significantly easier when its characteristic is p (cf. Propositions 7.6 and 7.9).

7.1. *Statement of Results*

We begin by stating the results to be proved later in the section. The following Propositions 7.x are handled for alternating groups in Section 7.3 and for classical groups in Sections 7.4–7.6. In Section 7.6 the first three of them are renamed Propositions 7.x′ within the vector space setting.

PROPOSITION 7.1. *SYLFIND_SIMPLE is in NC.*

Proof. Use ORBIT and BLOCKS to reduce to the case in which G is primitive. If $|G| < |\Omega|^8$ use brute force (Section 7.2). Use Theorem 6.2 together with Section 7.3.2 and Propositions 7.9 and 7.1′. ▮

PROPOSITION 7.2. *SYLNORM_SIMPLE is in NC.*

Proof. Use ORBIT and BLOCKS to reduce to the case in which G is primitive. If $|G| < |\Omega|^8$ use brute force (Section 7.2). Use Theorem 6.2 together with Section 7.3.2 and Propositions 7.9 and 7.2′. ▮

PROPOSITION 7.3. *SYLCONJ_SIMPLE is in NC.*

Proof. Use ORBIT and BLOCKS to reduce to the case in which G is primitive. If $|G| < |\Omega|^8$ use brute force (Section 7.2). Use Theorem 6.2 together with Section 7.3.2 and Propositions 7.9 and 7.3′. ▮

PROPOSITION 7.4. *SYLNORMALIZED*1*_SIMPLE is in NC.*

Proof. Use ORBIT and BLOCKS to reduce to the case in which G is primitive. If $|G| < |\Omega|^8$ use brute force (Section 7.2). Use Theorem 6.2 together with Section 7.3.2 and Propositions 7.9 and 7.4′. ▮

PROPOSITION 7.5. *SYLNORMALIZED*2*_SIMPLE is in NC.*

Proof. Use ORBIT and BLOCKS to reduce to the case in which G is primitive. If $|G| < |\Omega|^8$ use brute force (Section 7.2). Next use Theorem 6.2 together with Section 7.3.2 and Proposition 7.9. The proof is completed at the end of Section 7.6 ▮

7.2. *Tiny Groups*

In this section we deal with *tiny* groups, i.e., groups of order $O(n^c)$ with c fixed. We show that the basic problems of Section 5.1 are then amenable to straightforward ''brute-force'' solutions in NC.

We note first that, given generators S for a tiny group G, the elements of G can be listed in NC. For this, we start with the collection $A = S$ and repeat until stable: $A \leftarrow A \cup \{ab | a, b \in A\}$. After m iterations, A contains the elements in G that are expressible as words in S of length $\leq 2^m$. Hence, at most $\log_2|G|$ iterations are required.

Remark. Note that the preceding is just a special case of the "transitive-closure" method used for ORBITS.

SYLNORM and SYLCONJ for tiny groups. Normalizers and conjugating elements, if any exist, can be found for any subgroups. Namely, for $H \leq G$, $N_H(G)$ is found by testing in parallel for all $g \in G$ whether $H^g = H$, the test being performed by conjugating all $h \in H$ by g in parallel. For $H_1, H_2 \leq G$, test in parallel for all $g \in G$ whether $H_1^g = H_2$.

SYLFIND for tiny groups. Initialize $P \leftarrow 1$. While there is some $g \in N_G(P) - P$ of p-power order, $P \leftarrow \langle P, g \rangle$ for one such g. As each iteration of the loop at least doubles $|P|$, at most $\log_2|G|$ iterations are required.

*SYLNORMALIZED*1 *AND SYLNORMALIZED*2 *for tiny groups*. For these problems $U \subseteq \mathrm{Aut}(G)$, and we seek a Sylow q-subgroup normalized by U. Since G is tiny, we can list *all* Sylow q-subgroups of G: conjugate one such group by all $g \in G$ in parallel. We then test in parallel all these groups for normalization by R: apply, in parallel, all $u \in U$.

7.3. *Alternating Groups*

In this section we deal with an alternating group Alt_r, and we assume that we have constructed its natural action (Theorem 6.2) on r points.

We will focus first on NC procedures for the full symmetric group Sym_r; NC procedures for Alt_r follow easily (in Section 7.3.2).

7.3.1. *Sym$_r$*

Within the natural representation of Sym_r, we begin by providing explicit descriptions of Sylow subgroups and their normalizers. Parallel Sylow procedures for these groups are then straightforward.

Case 1: $r = p^m$. We are guided by a standard, elegant recursive description of a Sylow p-subgroup $P(m)$ of Sym_{p^m} in terms of wreath products [Hup]: $P(1)$ is generated by a p-cycle; for $m \geq 2$, $P(m) = P(1) \wr P(m-1)$. However, with the goal of explicit procedures for the Sylow problems, we give an explicit description of $P(m)$.

SYLFIND. For $m \geq 0$, let $\Delta_m = \mathrm{GF}(p)^m$ so that $\mathrm{Sym}(\Delta_m) \cong \mathrm{Sym}_{p^m}$. Given $P(m-1) \leq \mathrm{Sym}(\Delta_{m-1})$, we employ the natural identification $\Delta_m \approx \Delta_{m-1} \times \mathrm{GF}(p)$ to construct $P(m)$. There is a monomorphism $\mu: P(m-1) \hookrightarrow \mathrm{Sym}(\Delta_m)$ sending $g \mapsto (g, 1)$ for $g \in P(m-1)$. Also,

$\mathrm{Sym}(\Delta_m)$ contains an elementary abelian p-group $H_{m-1} = \langle h_\delta | \delta \in \Delta_{m-1} \rangle$ of order $p^{p^{m-1}}$, where, for all $(\delta', s) \in \Delta_{m-1} \times \mathrm{GF}(p)$,

$$(\delta', s)^{h_\delta} = \begin{cases} (\delta', s+1) & \text{if } \delta' = \delta, \\ (\delta', s) & \text{otherwise} \end{cases}$$

(H_{m-1} is the "base" of the wreath product). Then $P(m) := \langle P(m-1)^\mu, H_{m-1} \rangle = H_{m-1} \rtimes P(m-1)^\mu)$ is a Sylow p-subgroup as required.

Of course, in practice one can easily write generators for this group in a direct, nonrecursive manner. We have chosen the preceding description in order to more succinctly deal with the normalizer of $P(m)$:

SYLNORM. The multiplicative action of $\mathrm{GF}(p)^*$ on $\mathrm{GF}(p)$ naturally induces a faithful, coordinatewise action of $\mathrm{GF}(p)^{*m}$ on $\mathrm{GF}(p)^m = \Delta_m$. The induced subgroup of $\mathrm{Sym}(\Delta_m)$ normalizes $P(m)$, and, together with $P(m)$ itself, generates $\mathrm{N}_{\mathrm{Sym}(\Delta_m)}(P(m))$. (Different descriptions of this normalizer are given in [CL, Ka1, DS]. It is easy to check that the descriptions produce groups of the same order.)

SYLEMBED, SYLCONJ. Suppose we are given a p-group $Q \le \mathrm{Sym}(\Psi)$ where $|\Psi| = p^m \ge p$. We use the orbit/imprimitivity structure of Q to recursively construct a bijection $f: \Psi \to \Delta_m$ such that $Q \le fP(m)f^{-1}$, as follows. In parallel, in each nontrivial orbit of Q find a block system whose blocks have size p; also break the set of fixed points of Q into subsets of size p. Denote the collection of all these p-sets by $\overline{\Psi}$. Let $\overline{Q} := Q^{\overline{\Psi}}$ be the induced permutation group on $\overline{\Psi}$. Recursively, construct a bijection $\bar{f}: \overline{\Psi} \to \Delta_{m-1}$ such that $\overline{Q} \le \bar{f}P(m-1)\bar{f}^{-1}$. In parallel, for each p-set $\psi \in \overline{\Psi}$ define a bijection $k_\psi: \psi \to \mathrm{GF}(p)$ as follows: if the group Q_ψ^ψ induced on ψ is 1, then k_ψ is any bijection; if $|Q_\psi^\psi| = p$, choose any $\alpha \in \psi$ and $g \in Q_\psi$ such that $\alpha^g \ne \alpha$, and define k_ψ by $(\alpha^{g^s})^{k_\psi} = s$ for $0 \le s < p$. Then $Q \le fP(m)f^{-1}$ if $f: \Psi \to \Delta_m$ is defined by $\beta^f = (\omega^{\bar{f}}, \beta^{k_\psi})$ for $\beta \in \psi \in \Psi$.

Case 2. Arbitrary r.

SYLFIND. Write $|\Omega| = r = (d_m \cdots d_1 d_0)_p$ in the base p, where $0 \le d_i < p$ for all i. Take any disjoint decomposition $\Omega = \bigcup_{0 \le i \le m} \bigcup_{1 \le j \le d_i} \Psi_{ij}$ where $|\Psi_{ij}| = p^i$. For each i, j, let Q_{ij} be a Sylow p-subgroup of $\mathrm{Sym}(\Psi_{ij})$. Then the direct product $P = \prod_{0 \le i \le m} \prod_{1 \le j \le d_i} Q_{ij}$ acts naturally on Ω as a Sylow p-subgroup of $\mathrm{Sym}(\Omega)$.

SYLEMBED, SYLCONJ. Now suppose that we are given a p-subgroup $R \le \mathrm{Sym}(\Omega)$. We will carry out the preceding construction in order to obtain $R \le P$, by choosing the Ψ_{ij} to be R-invariant and then constructing Q_{ij} containing $R^{\Psi_{ij}}$ using Case 1. Namely, we find the orbits of R and sort

them by size in nondecreasing order, say $\Phi_1, \Phi_2, \ldots, \Phi_t$. For $0 \le k \le t$, compute $r_k = \sum_{j=1}^{k} |\Psi_j|$ in parallel, set

$$\Psi_{ij} := \bigcup \left\{ \Phi_k \mid (j-1)p^i + (d_{i-1} \cdots d_0)_p \le r_k < jp^i + (d_{i-1} \cdots d_0)_p \right\}$$

(which is, indeed, R-invariant) and obtain the desired P as before.

If R is itself a Sylow p-subgroup of $\mathrm{Sym}(\Omega)$, then the Ψ_{ij} are the orbits of R, and $R^{\Psi_{ij}} = Q_{ij}$ is a Sylow p-subgroup of $\mathrm{Sym}(\Psi_{ij})$. Use SYLCONJ in Case 1 to construct bijections $f_{ij}: \Psi_{ij} \to \Delta_i = \mathrm{GF}(p^i)$ inducing isomorphisms $Q_{ij} \cong P(i)$. Given a second Sylow p-subgroup, $\breve{R}$, of $\mathrm{Sym}(\Omega)$, similarly construct its orbits $\breve{\Psi}_{ij}$ and additional bijections $\breve{f}_{ij}: \breve{\Psi}_{ij} \to \Delta_i$. Then $R^g = \breve{R}$, where $g \in \mathrm{Sym}(\Omega)$ is defined to be $f_{ij}\breve{f}_{ij}^{-1}$ on Ψ_{ij}.

SYLNORM. Again suppose that R is a Sylow p-subgroup of $\mathrm{Sym}(\Omega)$, and obtain $\{Q_{ij}\}, \{\Psi_{ij}\}, \{f_{ij}\}$ as before. We construct $\mathrm{N}_{\mathrm{Sym}(\Omega)}(R)$ as follows. For each i, j in parallel, construct $N_{ij} = \mathrm{N}_{\mathrm{Sym}(\Psi_{ij})}(Q_{ij})$ using Case 1. The direct product $N := \prod_{0 \le i \le m} \prod_{1 \le j \le d_i} N_{ij}$ acts naturally on Ω, normalizing R. For each i and each j, k with $0 \le j < k \le d_i$, define $g_{ijk} \in \mathrm{Sym}(\Omega)$ to be $f_{ij}f_{ik}^{-1}$ on Ψ_{ij}, $f_{ik}f_{ij}^{-1}$ on Ψ_{ik}, and 1 on the remainder of Ω. Then $\mathrm{N}_{\mathrm{Sym}(\Omega)}(R) = \langle N, \{g_{ijk} \mid 0 \le i \le m, 0 \le j < k \le d_i\} \rangle$.

Remark. A useful visualization of $P(m)$ is obtained by lifting the action on Δ_m to automorphisms of a complete p-ary tree T_m of height m with leaves Δ_m. Note first, by the preceding construction, $P(m)$ acts naturally on Δ_i, for $0 < i < m$, via projection on the first i coordinates. The nodes of T_m are $\bigcup_{i=0}^{m} \Delta_i$. The root of T_m is (the singleton set) Δ_0. For any internal node $\delta \in \Delta_i$, $0 \le i < m$, the set of children of δ is $\{\delta\} \times \mathrm{GF}(p)$ $(\subseteq \Delta_{i+1})$. Thus, the set of leaves, B_δ, descendent from $\delta \in \Delta_i$ is $\{\delta\} \times \mathrm{GF}(p)^{m-i}$. For any i, $0 \le i \le m$, $\{B_\delta \mid \delta \in \Delta_i\}$ is a block system for the action of $P(m)$ on Δ_m (these are the only blocks systems for this action). In fact, these are block systems even for the action of $\mathrm{N}_{\mathrm{Sym}_{p^m}}(P(m))$. That is, $N_{\mathrm{Sym}_{p^m}}(P(m))$ acts on T_m via automorphisms. One can characterize $P(m) \le \mathrm{Aut}(T_m)$ as the subgroup of elements that induce and preserve cyclic orderings of the children at any node. That is, for $g \in \mathrm{Aut}(T_m)$, $g \in P(m)$ iff for any $\delta \in \Delta_i$, $i < m$, and $s \in \mathrm{GF}(p)$, $(\delta, s)^g = (\delta', t)$ implies $(\delta, s+1)^g = (\delta', t+1)$.

7.3.2. Alt_r

We will need some elementary facts concerning alternating groups. Consider a prime $p \le r$ and a Sylow p-subgroup Q of Sym_r. If p is odd then Q is also a Sylow subgroup of Alt_r, and $\mathrm{N}_{\mathrm{Alt}_r}(Q) = \mathrm{N}_{\mathrm{Sym}_r}(Q) \cap \mathrm{Alt}_r$. If r is a power of 2 and $r \ne 4$, then Q is the *unique* Sylow p-subgroup of Sym_r containing the Sylow p-subgroup $Q \cap \mathrm{Alt}_r$ of Alt_r.

Write $r = \sum_i a_i p^i$ in the base p; let $r_i = a_i p^i$. Then $N_{\mathrm{Sym}_r}(Q) = \Pi_i N_{\mathrm{Sym}_{r_i}}(Q \cap \mathrm{Sym}_{r_i})$, where $N_{\mathrm{Sym}_{r_i}}(Q \cap \mathrm{Sym}_{r_i})$ is the wreath product of $N_{\mathrm{Sym}_{p^i}}(Q \cap \mathrm{Sym}_{p^i})$ with Sym_{a_i}. Moreover, $N_{\mathrm{Sym}_r}(Q \cap \mathrm{Alt}_r) = N_{\mathrm{Sym}_r}(Q) \cap \mathrm{Alt}_r$ except when $p = 2$ and $r = 4$ or 5 (in the latter cases $N_{\mathrm{Sym}_r}(Q \cap \mathrm{Alt}_r)$ is Sym_4 while $N_{\mathrm{Sym}_r}(Q) = Q$). Note that $\mathrm{Sym}_r = \mathrm{Alt}_r \cdot N_{\mathrm{Sym}_r}(Q \cap \mathrm{Alt}_r)$ by the Frattini argument, so that $N_{\mathrm{Sym}_r}(Q \cap \mathrm{Alt}_r)$ contains elements outside of Alt_r.

SYLFIND and SYLEMBED. In order to embed a p-subgroup P of Alt_r into a Sylow p-subgroup of Alt_r, embed P in a Sylow p-subgroup of Sym_r and use INTERSECTION.

SYLNORM. As indicated previously, if $r > 5$ the normalizer in Alt_r of a Sylow p-subgroup of Alt_r is obtained via INTERSECTION from the normalizer in Sym_r of a Sylow p-subgroup of Sym_r.

SYLCONJ. If P_1, P_2 are Sylow p-subgroups of Alt_r, embed P_i in a Sylow p-subgroup Q_i of Sym_r, find $h \in \mathrm{Sym}_r$ conjugating Q_1 to Q_2, find $N_{\mathrm{Sym}_r}(Q_2)$, and output either $g = h$ or $g = hk$ with $k \in N_{\mathrm{Sym}_r}(Q_2) - N_{\mathrm{Alt}_r}(Q_2)$, depending on which of these elements is in Alt_r. (Note that at least one of the generators of $N_{\mathrm{Sym}_r}(Q_2)$ is found in the preceding section is not in Alt_r.)

*SYLNORMALIZED*1 *and SYLNORMALIZED*2. These require information concerning $\mathrm{Aut}(\mathrm{Alt}_r)$ for $r \geq 5$. If $r \neq 6$ then Alt_r has a unique conjugacy class of proper subgroups of index $\leq r$ [Wi, p. 42], and hence $\mathrm{Aut}(\mathrm{Alt}_r)$ is just Sym_r. (In the exceptional case, $\mathrm{Alt}_6 \cong \mathrm{PSL}(2,9)$ and $\mathrm{Aut}(\mathrm{Alt}_6) \cong \mathrm{P\Gamma L}(2,9)$.) We are given $U \subseteq \mathrm{Aut}(G)$, and we seek a Sylow subgroup normalized by U; we may assume that $r \neq 6$. In SYLNORMALIZED1 U is 1 and hence normalizes every Sylow p-subgroup of G. In SYLNORMALIZED2, if $|G| < |\Omega|^8$ use Section 7.2. Otherwise use Theorem 6.2 to find the r-set Ξ on which $\langle U \rangle G$ induces Alt_r or Sym_r, embed $\langle U \rangle$ in a Sylow p-subgroup of that group and intersect with Alt_r.

7.4. *Descriptions of Sylow Subgroups of Classical Groups*

Before proving the propositions in Section 7.1, we will describe the behavior of Sylow subgroups of classical groups. In every instance it suffices to replace all considerations of G by the corresponding ones for the group G^* of linear transformations found in Lemma 6.6 such that $G^*/Z(G^*) = G$. See [We, CF, Ka2, Ka3] for the descriptions in Proposition 7.6 and Theorem 7.7. Recall that q was defined in (6.16). Let q_0 denote the characteristic of K.

PROPOSITION 7.6. *Each Sylow q_0-subgroup P of G^* fixes a sequence of subspaces appearing in Lemma* 6.7 *or Lemma* 6.11(iii):

(i) $\langle e_1, \ldots, e_i \rangle$, $i = 1, \ldots, d-1$, *for a basis* $e_1, \ldots, e_d$, *when* G *is* $\mathrm{PSL}(V)$; *or* $\langle e_1, \ldots, e_k \rangle$, $k = 1, \ldots, m$, *where* m *is the Witt index of* V *and* $e_1, \ldots, e_m, f_1, \ldots, f_m, u_1, \ldots, u_s$ *is a standard basis.*

(ii) *Such a sequence is uniquely determined by* P *unless* V *is an orthogonal space of dimension* $2m$, *in which case there is exactly one other such sequence, which then has the form*

$$\langle e_1, \ldots, e_i \rangle, \qquad i = 1, \ldots, m-1, \qquad \langle e_1, \ldots, e_{m-1}, f_m \rangle;$$

these two sequences are in different G^**-orbits but in the same* $\mathrm{Isom}(V)$*-orbit. In this case,* P *fixes a unique fixed sequence* $\langle e_1, \ldots, e_k \rangle$, $k = 1, \ldots, m-1$, *consisting of totally singular subspaces.*

(iii) *The stabilizer in* G^* *of a sequence in* (i) *is a solvable group having a unique Sylow* q_0*-subgroup.*

(iv) *There are NC-algorithms for finding a sequence in* (i) *and* (ii), *as well as its stabilizers in* $\mathrm{Isom}(V)$ *and* G^*.

Proof. (i)–(ii) are easy to check, and (iv) follows from Lemmas 6.7 and 6.11(iii). ∎

THEOREM 7.7. *Let* $p \neq q_0$ *be a prime dividing* $|G|$. *Let* P *be a Sylow* p*-subgroup of either* G^* *or* $\mathrm{Isom}(V)$. *Then there is a decomposition* $V = V_1 \perp \cdots \perp V_s$ (*read "$\oplus$" for "$\perp$" if* $G^* = \mathrm{SL}(V)$) *such that the following all hold.*

(a) P *acts on* $\Delta := \{V_1, \ldots, V_s\}$.

(b) *If the space* $\mathrm{C}_V(P)$ *of fixed vectors* P *is nonzero, then* $\mathrm{C}_V(P)$ *is one of the* V_i, *say* V_c; *if* $\mathrm{C}_V(P) = 0$ *write* $V_c = 0$.

(c) *One of the following holds*:

(c1) *If* $p \neq 2$ *then, for each* $V_i \neq V_c$, *the set stabilizer* P_{V_i} *induces a cyclic group on* V_i, *and either*

(c1.1) P_{V_i} *is irreducible on* V_i, *or*

(c1.2) $G^* \neq \mathrm{SL}(V)$ *and* P *splits* V_i *into the direct sum of two totally isotropic or totally singular* P_{V_i}*-irreducible subspaces of dimension* $\frac{1}{2}\dim(V_i)$.

(c2) *If* $p = 2$ *then* $\dim(V_i) \leq 2$ *for each* i.

(d) Δ *can* (*and always will*) *be ordered so that each* $V_i \neq V_c$ *lies in* $V_1^{G^*} = V_1^{\mathrm{Isom}(V)}$, *except perhaps when* $p = 2$ *and* G *is orthogonal or unitary, in which case* $V_c = 0$ *and* $\Delta - V_1^{G^*}$ *can consist of one or two* 1*-spaces.*

(e) *The set stabilizers* $\mathrm{Isom}(V)_\Delta$ *and* G^*_Δ *induce the symmetric group on the set of members of* $V_1^{G^*}$ *lying in* Δ, *while fixing all remaining members of* Δ.

(f) *The orbit* $V_1^{\mathrm{Isom}(V)}$ *of subspaces is characterized by the following conditions*:

V_1 *is nonsingular if* G *is not* $\mathrm{PSL}(V)$;

if $p = 2$ *then* $\dim(V_1) = 2$ *and* $8 \mid |\mathrm{Isom}(V_1)|$; *and*

if $p \neq 2$ *then* $\dim(V_1)$ *is minimal for* $V_1 \subseteq V$ *subject to* $p \mid |\mathrm{Isom}(V_1)|$.

There are remarks in [Ka2, Ma2] providing a number-theoretic method for determining the isometry type of V_1. However we will sidestep that, opting instead for the cruder approach indicated in (*f*): *use* Lemmas 6.9(i), 6.13(i), and 6.14(ii) *to find representatives of all* G^**-orbits of nonsingular subspaces of* V, *find the set stabilizer in* G^* *of each such subspace, and then test their orders for divisibility by* p.

The set Δ is uniquely determined by P. This is a consequence of the characterization of Δ we are about to give in Proposition 7.8. First we need some notation. If G^* and P are as in Theorem 7.7, and if W is any minimal P-invariant subspace of V, write

$$\Pi(W) := \{C_V(P_v) \mid |P_v| \text{ is maximal for } v \in W - \{0\}\},$$

$$\Pi^2(W) := \{\langle X, Y\rangle \mid X, Y \in \Pi(W) \text{ and } \langle X, Y\rangle \text{ contains more than two members of } \Pi(W)\},$$

$$\Pi^1(W) := \{C_V(P_v) \mid |P_v| \text{ is maximal or next-to-maximal for } v \in W - \{0\}\},$$

$$\Pi^{12}(W) := \{\langle X, Y\rangle \mid X, Y \in \Pi^1(W) \text{ and } \langle X, Y\rangle \text{ contains more than two members of } \Pi^1(W)\}.$$

PROPOSITION 7.8 [Ka3]. *Assume that* $\dim(V) > 8$. *Then one of the following holds*:

(i) $p \neq 2$ *or* G *is symplectic, and* $\Delta - \{C_V(P)\}$ *consists of all of the sets* $\Pi(W)$ *as* W *ranges over all minimal nonsingular* P*-invariant subspaces of* V *not contained in* $C_V(P)$; *or*

(ii) $p = 2$, G *is not symplectic, and* Δ *consists of all of the* 1*-spaces fixed by* P *together with all of the following sets as* W *ranges over all minimal nonsingular* P*-invariant subspaces* V *of dimension* > 1:

(iia) $\Pi^{12}(W)$ *if* G *is either* $\mathrm{PSL}(d, q)$, $q \equiv 1 \pmod 4$, *or* $\mathrm{PSU}(d, q)$, $q \equiv 3 \pmod 4$,

(iib) $\Pi^2(W)$ *otherwise*.

Remark. Evidently, Proposition 7.8 provides a simple way to find Δ, given P. However, DECOMPOSITION will do that in some sense "better"; it can also be used for *any* p-subgroup of G, whereas the description in Proposition 7.8 is very specifically aimed at Sylow subgroups. [Ka1, Ka2, Ka3] contain other complicated and unpleasant approaches that deal with this general case. Note that, in view of the uniqueness of Δ implied by Proposition 7.8, Δ *is invariant under the normalizer of* P.

7.5. *The case* $p = q_0$

We can now continue with the proof of Theorem 1.1 for the classical groups. At this point we have constructed the underlying vector space V and its set Ξ of 1-spaces, together with an action of G on Ξ and a preimage G^* of G inside $\mathrm{SL}(V)$. All results in Sections 6.3–6.5 can be used.

In this section we handle the easy case: when p is the characteristic q_0 of the underlying field K, all required algorithms are straightforward using the fixed sequences in Proposition 7.6(i) and (ii).

PROPOSITION 7.9. *There are NC algorithms for SYLFIND_SIMPLE, SYLNORM_SIMPLE, SYLCONJ_SIMPLE, SYLNORMALIZED*1*_SIMPLE, and SYLNORMALIZED*2*_SIMPLE if* G *is a simple primitive subgroup of* $\mathrm{Sym}(\Omega)$ *such that* $|G| \geq |\Omega|^8$, G *is isomorphic to a classical group, and* p *is the characteristic of* G.

Proof. SYLFIND, *SYLNORM*. Use Proposition 7.6(iv) to find a sequence behaving as in Proposition 7.6(i), together with its stabilizer B in G. Then B is solvable and has a unique Sylow p-subgroup P. Use HALLFIND_SOLVABLE to find P. Moreover, $B = \mathrm{N}_G(P)$.

SYLCONJ_SIMPLE. Use Proposition 7.6(iv) to find sequences of subspaces fixed by P_1 and P_2, and use Lemma 6.9(ii) or 6.13(ii) to find $g \in G$ sending a sequence for P_1 to one for P_2 (in the special case indicated in Proposition 7.6(ii) ignore the last terms of the two sequences). Then $P_1^g = P_2$.

*SYLNORMALIZED*1*_SIMPLE*. Since the characteristic of G divides $|G|$ we have $U = 1$, so U normalizes every Sylow subgroup of G.

*SYLNORMALIZED*2*_SIMPLE*. If $R = \langle U \rangle$ acts on Ξ, find a sequence of R-invariant subspaces as in Proposition 7.6(iv), and the stabilizer B of this sequence in $\mathrm{P\Gamma L}(V)$. Then B is solvable, and R normalizes the Sylow p-subgroup of B.

Suppose that R does not arise from a subgroup of $\Gamma\mathrm{L}(V)$. The only classical group G for which this can occur is $\mathrm{PSL}(V)$, and then $p = 2$. (N.B.—Recall that $\dim(V) > 8$ by Lemma 6.3, thereby avoiding some

small-dimensional classical groups having outer automorphisms that do not act on Ξ.) Here, R acts on $\Xi \cup \Xi^*$, where Ξ^* "is" the set of hyperplanes of V; the action of G on Ξ^* can be found using elementary linear algebra. Since R normalizes a Sylow p-subgroup of G it fixes a sequence of subspaces behaving as in Proposition 7.6(i). In particular, R fixes some pair (x, H) consisting of a point x and a hyperplane H containing x. Use ORBIT to find such a pair (x, H). Then R acts on the set of subspaces of H/x, and we can iterate in order to find a sequence in Proposition 7.6(i) fixed by R. Then R normalizes the Sylow p-subgroup of the stabilizer in PSL(V) of that sequence. ∎

7.6. *The Case $p \neq q_0$*

Throughout the remainder of this section we assume that p is not the characteristic of K. It is convenient to modify parts of Section 7.1 so as to deal with *linear* groups, as follows.

PROPOSITION 7.1′. *There is an NC algorithm for finding Sylow p-subgroups of* Isom(V) *and* G^*.

PROPOSITION 7.2′. *There is an NC algorithm which, when given a Sylow p-subgroup P of* G^*, *finds* $N_{\mathrm{Isom}(V)}(P)$ *and* $N_{G^*}(P)$.

PROPOSITION 7.3′. *There is an NC algorithm which, when given Sylow p-subgroups* P_1, P_2 *of* G^*, *finds* $g \in G^*$ *such that* $P_1^g = P_2$.

We will continually use the decomposition in Theorem 7.7. Recall that, if G is PSL(V), "$\oplus$" should be read in place of "$\perp$" and "GL(V)" in place of "Isom(V)."

Each time we will find the following:

(#)
- a decomposition $\Delta = \{V_1, \ldots, V_s\}$, using Theorem 7.7(f) or Proposition 7.8 (depending on whether we are finding a Sylow subgroup P or already have one) together with Lemma 6.10(iii) or 6.14(iii),
- its set stabilizer $H = \mathrm{Isom}(V)_\Delta$, using Lemma 6.10(i) or 6.14(iii), and
- its pointwise stabilizer $L = \Pi_i L_i$ in Isom(V), with $L_i = \mathrm{Isom}(V_i)$ trivial on each $V_j \neq V_i$, using Lemma 6.9(i) or 6.13(i).

Additional aspects of Δ, H, and L will be needed from Theorem 7.7: $H/L \cong \mathrm{Sym}(V_1^H)$; the subspace $V_c = C_V(P)$, which is appended to Δ even if it is 0; and the fact that all $\dim V_i \leq 2$ if $p = 2$, in which case all L_i are

tiny. We will use the following straightforward algorithmic properties of L:

LEMMA 7.10. *For all L and p, the following problems are in NC*:

(i) (SYLFIND) *Find a Sylow p-subgroup Q of L;*

(ii) (SYLCONJ) *Given two Sylow p-subgroups Q and Q^* of L, find $l \in L$ with $Q^l = Q^*$;*

(iii) (FRATTINI) *Given $L \leq S \leq H$, find $D \trianglerighteq Q$ with $S = DL$; and*

(iv) (SYLNORM) *Find* $N_L(Q)$.

Proof. If $p \geq 2$, then each L_i has a cyclic Sylow p-subgroup Q_i, which is found using either Lemma 6.8(ii) or 6.17(i) and (iv), and then let $Q = \Pi_i Q_i$. Moreover, $N_L(Q) = \Pi_i N_{L_i}(Q_i)$, where $N_{L_i}(Q_i)$ is found in either Lemma 6.8(iii) or 6.17(i) and (iii); and Sylow subgroups of L_i are conjugated in either Lemma 6.8(i) or 6.17(ii) and (iii). If $p = 2$, each L_i is tiny, so Section 7.2 can be used.

This proves (i), (ii), and (iv), while (iii) is deduced precisely as in the proof of Corollary 4.4. ▮

Proof of Proposition 7.1′. Start with (#). Use Lemma 7.10(i) to find a Sylow p-subgroup Q of L. Use Section 7.3.1 to find a Sylow p-subgroup T/L of H/L, where $H/L \cong \mathrm{Sym}(V_1^H)$ by Theorem 7.7(e).

Use Lemma 7.10(iii) to find $D \trianglerighteq Q$ such that $T = DL$. We focus on D, which contains a Sylow p-subgroup of $\mathrm{Isom}(V)$.

If $p = 2$ let $D_0 = D$. If $p > 2$ let D_0 denote the subgroup of $\mathrm{Isom}(V)$ that agrees with D on $V_0 = \langle V_1^H \rangle$ and induces 1 on $V_0^\perp$. Then D_0 contains a Sylow p-subgroup of $\mathrm{Isom}(V)$, $D_0 \cap L \trianglerighteq Q$ and $D_0/(D_0 \cap L)$ is a p-group. By Theorem 7.7(c) and either Lemma 6.8(iii) or 6.17(i) and (iii), if $p > 2$ then $D_0 \cap L$ is solvable; the same is true if $p = 2$ since Q is a normal Sylow 2-subgroup of $D_0 \cap L$. Use HALLFIND to find a Sylow p-subgroup P of D_0, and hence of $\mathrm{Isom}(V)$. Output P and the Sylow p-subgroup $G^* \cap P$ of G^* (obtained using INTERSECTION). ▮

Proof of Proposition 7.2′. Start with (#). Use INTERSECTION to find $Q = P \cap L$ and, for each $V_i \in \Delta$, the group $Q_i \leq L_i$ agreeing with Q on V_i while inducing the identity on all other V_j. Find $N_L(Q)$ using Lemma 7.10(iv).

We construct $T = N_H(Q)$ using a Frattini argument, as follows. For each $V_i \in V_1^H$ let $g_i \in H$ send V_1 to V_i. Find $h_i \in L_i$ with $(Q_1^{g_i})^{h_i} = Q_i$: if $p > 2$ use either Lemma 6.8(i) or 6.17(i) and (iii), and if $p = 2$ use brute force (Section 7.2). Let g_i' be the isometry of V that acts as $g_i h_i$ on V_1, as $(g_i h_i)^{-1}$ on V_i, and induces the identity on every other member of Δ. Let T be the group generated by $N_L(Q)$ and all of these elements g_i'. Then $T \trianglerighteq Q$, $T \cap L = N_L(Q)$, and $T^\Delta = H^\Delta$ is $\mathrm{Sym}(V_1^H)$, so that $T = N_H(Q)$.

Since $N_{\mathrm{Isom}(V)}(P)$ acts on Δ by Proposition 7.8, it lies in H, normalizes Q, and hence lies in T.

Since $T/(T \cap L) \cong TL/L = H/L \cong \mathrm{Sym}(V_1^H)$, we can use Section 7.3.1 to find $M/(T \cap L) = N_{T/(T \cap L)}(P(T \cap L)/(T \cap L))$. Then $N_{\mathrm{Isom}(V)}(P) \leq M$. View the respective restrictions P_0, M_0, and T_0 of P, M, and $N_L(Q) = T \cap L$ to $V_0 = \langle V_1^H \rangle$ as isometry groups of V inducing 1 on $V_0^\perp$. Then $N_{\mathrm{Isom}(V)}(P) = N_{M_0}(P_0) \times N_{\mathrm{Isom}(V_0^\perp)}(P)$, where $N_{\mathrm{Isom}(V_0^\perp)}(P) = \mathrm{Isom}(V_0^\perp)$ if $p > 2$ while $\mathrm{Isom}(V_0^\perp)$ is tiny if $p = 2$, in which case $N_{\mathrm{Isom}(V_0^\perp)}(P)$ can be found by brute force.

Since $M \trianglerighteq P(T \cap L)$ we have $M_0 \trianglerighteq P_0T_0$. By Theorem 7.7(c) and either Lemma 6.8(iii) or 6.17(i) and (iii), T_0 is solvable if $p > 2$; the same is true if $p = 2$. Thus, P_0T_0 is solvable. Apply HALLFRATTINI to $1 \leq P_0T_0 \trianglelefteq M_0$ in order to find $D \trianglerighteq P_0$ such that $M_0 = D \cdot P_0T_0$; then $N_{M_0}(P_0) = DN_{P_0T_0}(P_0)$. Use HALLNORM to find $N_{P_0T_0}(P_0)$, let $N = DN_{P_0T_0}(P_0)$ $N_{\mathrm{Isom}(V_0^\perp)}(P)$, and output $N = N_{\mathrm{Isom}(V)}(P)$ and $G^* \cap N = N_{G^*}(P)$. ∎

Proof of Proposition 7.3′. Use Proposition 7.8 or DECOMPOSITION to find the decomposition Δ_j of V in Theorem 7.7 arising from P_j. Use Lemma 6.10(ii) or 6.14(iv) to find an element of $f \in G^*$ with $\Delta_1^f = \Delta_2$. Let $\Delta = \Delta_2$ and $P = P_2$, and proceed with (#).

Since $H/L \cong \mathrm{Sym}(V_1^H)$, we can use Section 7.3.1 to find $h \in H$ such that $(P_1^f)^h$ and P_2 induce the same Sylow p-subgroup of $\mathrm{Sym}(V_1^H)$. Let $P_3 = P_1^{fh}$, so $P_3L = P_2L$.

Find $P_j \cap L$ for $j = 2, 3$; let P_{ji} be the subgroup of L_i it induces on V_i. Then $R_j = (\Pi_i P_{ji})P_j$ is a Sylow p-subgroup of $\mathrm{Isom}(V)$. Use Lemma 7.10(ii) to find $l \in L$ such that $(R_3 \cap L)^l = R_2 \cap L$.

Now R_2 and R_3^l agree on Δ and contain $R_2 \cap L$ as a normal subgroup. Then $T = \langle R_3^l, R_2 \rangle$ is a p-group on Δ and $T \trianglerighteq R_2 \cap L$, while T is 1 on V_c. By Theorem 7.7(c) and either Lemma 6.8(iii) or 6.17(i) and (iii), $N_L(\Pi_i P_{ji}) \cap C_L(V_c)$ is solvable if $p \neq 2$; solvability is clear if $p = 2$. Consequently, $T \trianglerighteq T \cap L$ with $T/(T \cap L)$ a p-group and $T \cap L$ solvable. Use HALLCONJ to find $t \in T$ with $(R_3)^t = R_2$. Then $(P_1^{fhl})^t = (G^* \cap R_3)^t = G^* \cap R_2 = P_2$.

By Sylow's Theorem, $P_1^g = P_2$ for some $g \in G^*$, so $fhltg^{-1} \in N_{\mathrm{Isom}(V)}(P_1)$. Use Proposition 7.2′ and INTERSECTION to find such an element g in $G^* \cap N_{\mathrm{Isom}(V)}(P_1)fhlt$. Output g. ∎

Proof of Proposition 7.4. This result is a special case of the following slightly more general one, which has essentially the same proof but will be needed in [KL2].

PROPOSITION 7.4′. *The following problem is in NC*: *given a nonabelian simple group* $G \leq \mathrm{Sym}(\Delta)$ *and a subset* U *of* $\mathrm{Aut}(G)$ *generating a group*

$R \neq 1$ such that $(|R|, |G|) = 1$, find a Sylow 2-subgroup of G normalized by U.

Proof. As in Section 7.1, reduce to the case in which G is a classical group; note that G is not isomorphic to any alternating group A_k since $|\mathrm{Aut}(A_k): A_k| \mid |A_k|$ (cf. Section 7.3.1). Use Theorem 6.2 to find a vector space V underlying G.

We have $(|R|, |\mathrm{Isom}(V)|) = 1$. Then R is an odd order group of outer automorphisms of G obtained by extending a group of automorphisms of the field K to V. (If $|R|$ is a prime power, just apply Sylow's Theorem to GR; in the general case apply the Schur–Zassenhaus Theorem [Gor1, p. 221] to GR; or see [BGL, 1.3].)

In particular, R acts on the set of 1-spaces of V. As usual, it now suffices to change perspective and consider G^* instead of G, together with a subgroup R^* of $\Gamma\mathrm{L}(V)$ inducing R and satisfying the condition $(|R^*|, |G^*|) = 1$.

First we consider the case where G has characteristic 2. There is a unique odd-size G-orbit of pairs (x, W) consisting of a 1-space x and a hyperplane W of V containing it (here $W = x^\perp$ if G is not $\mathrm{PSL}(V)$). There is such a pair (x, W) fixed by R^* (this is clear if $|R^*|$ is a prime power; the general case follows easily from the Schur–Zassenhaus theorem since $(|R^*|, |G^*|) = 1$). Use elementary linear algebra to find the set of hyperplanes of V, and then use ORBIT to find such a fixed pair (x, W). Iterate this for W/x in order to obtain an R^*-invariant sequence as in Proposition 7.6(i); find its stabilizer using Proposition 7.6(iv). Then R^* normalizes the Sylow 2-subgroup of that stabilizer (cf. Proposition 7.6(iii)).

From now on we may assume that G does not have characteristic 2. Then a Sylow 2-subgroup of G^* is described in Theorem 7.7. When R^* acts on the $\mathrm{Isom}(V)$-orbit of 2-spaces behaving as in Theorem 7.7(f), it fixes some V_1 in this orbit (once again by the Schur–Zassenhaus theorem); find such a fixed V_1 using ORBIT. If G^* is not $\mathrm{SL}(V)$, iterate for $V_1^\perp$ (cf. Lemma 6.3) in order to obtain a decomposition $V = V_1 \perp \cdots \perp V_s$ as in Theorem 7.7 each of whose members is R^*-invariant. If $G^* = \mathrm{SL}(V)$ use DECOMPOSITION to find an R^*-invariant complement to V_1 in V, and once again iterate.

Proceed with (#). Since $\dim(V_i) \leq 2$, by brute force (Section 7.2) for each $V_i \in \Delta$ we can find a Sylow 2-subgroup Q_i of L_i normalized by R^*. Then $Q = \Pi_i Q_i$ is an R^*-invariant Sylow 2-subgroup of L.

Since R^* acts on the symmetric group H/L it centralizes it. Use Section 7.3.1 to find a Sylow 2-subgroup E/L of H/L. Then R^* normalizes E and E contains a Sylow 2-subgroup of G^*. Since $R^*E \trianglerighteq L$, by Lemma 7.10(iii) we can find $D \trianglerighteq Q$ such that $R^*E = DL$. Then D contains a Sylow

2-subgroup of G^*. Replace D by the group $\langle D, R^* \rangle$ that also normalizes Q.

Now note that D is solvable: $D = R^*(D \cap H)$ where R^* has odd order (and is, in fact, cyclic), $(D \cap H)/(D \cap L) \cong (D \cap H)L/L$ is the normalizer of a Sylow 2-subgroup of a symmetric group and hence is a 2-group (cf. Section 7.3.1), and the subgroup $D \cap L$ of the normalizer in L of a Sylow 2-subgroup T of L also is solvable. Use HALLFIND, HALLNORM, and HALLCONJ to find a Sylow 2-subgroup S of D, then $N_D(S)$, then a Hall subgroup of $N_D(S)$ conjugate in D to the Hall subgroup R^* of D, and finally $d \in D$ such that $R^{*d} \leq N_D(S)$. Use INTERSECTION to find $G^* \cap S^{d^{-1}}$, and output this group. ∎

Remark. SYLNORMALIZED1_SIMPLE is used in SYLEMBED1, where we needed to know that $N_G(T)$ is solvable when T is a suitable Sylow subgroup of the simple group G. That is true for a Sylow 2-subgroup T by [FT]. An alternative, and perhaps slightly simpler approach when G is a simple classical group, would have been to find and use a Sylow q_0-subgroup Q_0 of G, since once again $N_G(Q_0)$ is solvable by Proposition 7.6.

Remark. An alternative approach to Proposition 7.4 imitates Case 1 of the proof of Lemma 7.11. Namely, since R^* can be identified with a group of field automorphisms, $V' = C_V(R^*)$ is a $\dim V$-dimensional vector space over the fixed field K' of R^*, naturally equipped with a K'-form. Moreover, R^* centralizes $\mathrm{Isom}(V')$, and hence centralizes a Sylow 2-subgroup of $\mathrm{Isom}(V')$. This determines a decomposition of V' behaving as in Theorem 7.7. Each member of the decomposition spans a subspace of V, and these latter subspaces yield a decomposition Δ of V also behaving as in Theorem 7.7. Now proceed as in the proof of SYLCONJ_SS in Section 5.2 in order to obtain an R-invariant Sylow 2-subgroup of G_Δ.

We now turn to Proposition 7.5, the hardest result in Section 7.

LEMMA 7.11. *Proposition* 7.5 *holds if* R *arises from a subgroup of* $\Gamma L(V)$.

Proof. As before, by INTERSECTION this reduces to the following problem: *find a Sylow p-subgroup of* $\mathrm{Isom}(V)R$ *containing a given p-subgroup* R *of* $N_{\Gamma L(V)}(\mathrm{Isom}(V))$.

Let $W = \langle C_V(R) \rangle$. Then W is a nonsingular subspace of V if the form on V is nonzero, in which case R also acts on $W^\perp$; in the case of $\mathrm{SL}(V)$ let $W^\perp$ denote any R-invariant complement to W (found using COMPLEMENT).

Case 1: $p > 2$ *and* $p \mid |\mathrm{Isom}(W)|$. By [BGL, Lemma 1.3] R induces a group of field automorphisms of $\mathrm{Isom}(W)$, so $W' = C_V(R)$ is a $\dim W$-dimensional vector space over a subfield K' of K (where $[K: K'] = |R|$),

and some nonzero scalar multiple of the form on W can be written as a K'-valued form on W' of the same type and Witt index as the original one on W. Test all scalar multiples of the form on W for this property.

This embeds $\mathrm{Isom}(W')$ as a subgroup of $\mathrm{Isom}(W)$ centralizing R; we extend $\mathrm{Isom}(W')$ to a subgroup of $\mathrm{Isom}(V)$ inducing 1 on $W^{\perp}$. Note that $p \mid |\mathrm{Isom}(W')|$ since $p \mid |\mathrm{Isom}(W)|$. (Namely, $|\mathrm{Isom}(W)|$ is the product of a power of the characteristic with integers of the form $q^k \pm 1$, possibly together with a factor 2. The same statement is true for $|\mathrm{Isom}(W')|$, using integers $(q^{1/|R|})^k \pm 1$ for the same signs and same k since p is odd. If $p \mid q^k \pm 1$ with $q^k \pm 1 \mid |\mathrm{Isom}(W)|$, then $p \mid (q^{1/|R|})^k \pm 1$ since $|R|$ is odd, where $(q^{1/|R|})^k \pm 1 \mid |\mathrm{Isom}(W')|$.)

Use Proposition 7.1′ to find a Sylow p-subgroup P of $\mathrm{Isom}(W')$, and replace R by the p-group $\langle R, P \rangle$.

Thus, we may now assume that, *if p is odd, then $p \nmid |\mathrm{Isom}(W)|$*.

Before continuing we need some additional notation. Use DECOMPOSITION to find a $\mathrm{GF}(q)^*R$-invariant decomposition $V = W_1 \perp \cdots \perp W_s$ with the following properties: if $W \neq 0$ then $W_1 \neq W \in \Delta = \{W_1, \ldots, W_s\}$; and each R-orbit Θ on $\Delta - \{W\}$ comprises a minimal $\mathrm{GF}(q)^*R$-respectful decomposition of $\langle \Theta \rangle$ (since R is a p-group this means that $|\Theta|$ is 1 or p). Use POINT_STABILIZER to find, for each i, the stabilizer R_i of W_i in the action of R on Δ. Eventually we will enlarge R and deduce that Δ behaves as in Theorem 7.7. We will only need to consider those $W_i \in \Delta - \{W\}$.

Case 2: $p > 2$. Suppose first that there is just one orbit Θ. If $p \nmid |\mathrm{Isom}(W_1)|$ then R_1 induces on W_1 a group of field automorphisms as in Case 1, while $|R/R_1| = p$ and $[R_1, R \cap \mathrm{Isom}(W_1)] = 1$, so that R is abelian. Here we proceed as in Case 1 in order to obtain a Sylow p-subgroup P_1 of a smaller classical group centralized by R_1 and containing $R \cap \mathrm{Isom}(V)$. Replace R by the p-group $\langle R, P_1 \rangle$. Thus, we may assume that $p \mid |\mathrm{Isom}(W_1)|$. Recursively find a Sylow p-subgroup P_1 of $\mathrm{Isom}(W_1)$ normalized by R_1, and again replace R by $\langle R, P_1 \rangle$.

If there is more than one orbit Θ, then for each Θ use the preceding paragraph to obtain a Sylow p-subgroup P_Θ of $\mathrm{Isom}(\langle \Theta \rangle)$ normalized by R. Replace R by the group generated by R and all of these groups P_Θ. Now each Θ behaves as in Theorem 7.7, and hence so does Δ (cf. Theorem 7.7(f)).

Thus, we may now assume that Δ behaves exactly as in Theorem 7.7. Proceed with (#) for Δ. Clearly, HR contains a Sylow p-subgroup of $\mathrm{Isom}(V)R$, and we must embed R into such a Sylow subgroup. We already know that $Q = R \cap L$ is a Sylow p-subgroup of L.

We found a Sylow p-subgroup P of H in Proposition 7.1′. Find $g \in H$ such that $\langle R^\Delta, P^{g\Delta} \rangle$ is a p-group (using Theorem 7.7(e) and Section 7.3.1). Use Lemma 7.10(ii) to find $l \in L$ with $(P^g \cap L)^l = Q$. Then $\langle R, P^{gl} \rangle \trianglerighteq Q$.

Let T_0 denote the subgroup of H coinciding with $\langle R, P^{gl}\rangle \cap \mathrm{Isom}(V)$ on $V_0 = \langle W_1^H\rangle$ and inducing 1 on $V_0^\perp$. Let $T = T_0 R$.

Here $T \trianglerighteq T \cap L \trianglerighteq Q$, where $T/(T \cap L)$ is a p-group and $T \cap L \leq \mathrm{N}_L(P \cap L)$. By Lemma 6.8(iii) or 6.17(iii), $\mathrm{N}_T(P \cap L)$ is solvable, and hence so is T. Use HALLEMBED to find $t \in T$ such that $\langle R, P^{glt}\rangle$ is a p-group, and output this subgroup.

Case 3: $p = 2$. Find the $\mathrm{Isom}(V)$-orbit $\Theta = V_1^G$ of 2-spaces behaving as described in Theorem 7.7(d) and (f). Test all $V_1 \in \Theta$ in parallel in order to find one such that $\langle V_1^R\rangle$ has the form $V_1 \perp \cdots \perp V_k$. Find $(V_1 \perp \cdots \perp V_k)^\perp$, or an R-invariant complement to $V_1 \perp \cdots \perp V_k$ if G is $\mathrm{PSL}(V)$ (using COMPLEMENT). This produces a decomposition $V = V_1 \perp \cdots \perp V_s$ behaving as in Theorem 7.7. Proceed with (#), and conclude as in the last three paragraphs of Case 2. ∎

Proof of Proposition 7.5. It remains only to consider the case in which R does not arise from a subgroup of $\Gamma\mathrm{L}(V)$. The only group G for which this can occur is $\mathrm{PSL}(V)$, and then $p = 2$. (N.B.—Recall that $\dim(V) > 8$ by Lemma 6.3, thereby avoiding some small-dimensional classical groups also having outer automorphisms that do not act on Ξ.)

Equip $W = V \oplus V^*$ with the nonsingular symmetric bilinear form defined by $(v_1 + f_1, v_2 + f_2) = v_1 f_2 + v_2 f_1$ for $v_1, v_2 \in V$, $f_1, f_2 \in V^*$. Then $\mathrm{Aut}(\Gamma\mathrm{L}(V))$ acts on W and preserves this form. Use Lemma 6.5(ii) to find a 2-group R^* of semilinear transformations of W that induces the subgroup R of $\mathrm{P}\Gamma\mathrm{L}(W)$ and preserves this form.

Use DECOMPOSITION to find an R^*-invariant decomposition $V \oplus V^* = U_1 \oplus \cdots \oplus U_s \oplus W_1^* \oplus \cdots \oplus W_s^*$ with each $\dim(U_i) = \dim(W_i^*) \leq 2$, $U_i \subseteq V$, $W_i^* \subseteq V^*$, and $(U_k, W_j^*) \neq 0$ if and only if $i \neq j$; by the uniqueness implied by Proposition 7.8, such a decomposition exists since R lies in a Sylow 2-subgroup of $\mathrm{Aut}(G)$.

Let $V_i = U_i \oplus W_i^*$, $1 \leq i \leq s$. Then R^* acts on $\Delta = \{V_1, \ldots, V_s\}$.

We wish to alter the subspaces V_i so that at most one of them has dimension 2. If there are two R^*-invariant subspaces in Δ of dimension 2, replace them by their sum. Consider a nontrivial R^*-orbit Θ of subspaces in Δ of dimension 2. Let $r \in R^*$ be such that r^Θ is an involution in $Z(R^{*\Theta})$, and replace each $V_i \in \Theta$ by $V_i + V_i^r$. These modifications of Δ leave us with an R^*-invariant decomposition Δ of $V \oplus V^*$ whose intersections with V behave as in Theorem 7.7.

Now proceed as in (#), with $L_i < \mathrm{GL}(V)$ inducing $\mathrm{GL}(U_i) \cong \mathrm{GL}(W_i^*)$ on V_i. Then R^*H acts on Δ, and $(R^*H)^\Delta = \mathrm{Sym}(V_1^H)$ (by Theorem 7.7(e)). For all i, use POINT_STABILIZER to find the stabilizer R_i^* of L_i in R^*, and use brute force to find a Sylow 2-subgroup of L_i normalized by R_i^*. Now proceed exactly as in the SYLNORMALIZER2_SS part of the proof of Proposition 5.1 in order to obtain a Sylow 2-subgroup Q of L normal-

ized by R^*. Replace R^* by QR^*, and conclude as in the last three paragraphs of Case 2 of Lemma 7.11. ∎

The algorithm for Proposition 7.5 should be compared to the one presented in [Ka3, pp. 558–561].

REFERENCES

[As] M. Aschbacher, "Finite Group Theory," Cambridge Univ. Press, Cambridge, 1986.

[BLS1] L. Babai, E. M. Luks, and A. Seress, Permutation groups in NC, *in* "Proceedings of the ACM Symposium on Theory of Computing, 1987," pp. 409–420.

[BLS2] L. Babai, E. M. Luks, and A. Seress, Parallel computation in permutation groups I, in preparation.

[BL] K. Blaha and E. M. Luks, *P*-complete problems for groups, in preparation.

[BGL] N. Burgoyne, R. Griess, and R. Lyons, Maximal subgroups and automorphisms of Chevalley groups, *Pacific J. Math.* **71** (1977), 365–403.

[CL] H. Cárdenas and E. Lluis, The normalizer of the Sylow *p*-subgroup of the symmetric group, *Bol. Soc. Mat. Mexicana* **2** (1964), 1–6.

[Car] R. Carter, "Simple Groups of Lie Type," Wiley, London/New York/ Sydney/ Toronto, 1972.

[CF] R. Carter and P. Fong, The Sylow 2-subgroups of the finite classical groups, *J. Algebra* **1** (1964), 139–151.

[CNW] 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.

[Di] J. Dieudonné, "La géométrie des groupes classiques," Springer-Verlag, Berlin/ Göttingen/ Heidelberg, 1963.

[DS] Yu. V. Dmitruk and V. I. Sushchanskii, Structure of Sylow 2-subgroups of the alternating groups and normalizers of Sylow subgroups in the symmetric and alternating groups, *Ukraïn. Mat. Zh.* **33** (1981), 304–312. [English translation: New York, Plenum, 1982.]

[FT] W. Feit and J. G. Thompson, The solvability of groups of odd order, *Pacific J. Math.* **13** (1963), 775–1029.

[FHL] M. Furst, J. Hopcroft, and E. Luks, Polynomial-time algorithms for permutation groups, *in* "Proceedings of the 21st IEEE Symposium on the Foundations of Computer Science, 1980," pp. 36–41.

[Gor1] D. Gorenstein, "Finite Groups," Harper & Row, New York, 1968.

[Gor2] D. Gorenstein, "Finite Simple Groups. An introduction to Their Classification," Plenum, New York, 1982.

[Hup] B. Huppert, "Endliche Gruppen," Springer-Verlag, Berlin/Göttingen/Heidelberg, 1967.

[Kal] L. Kaloujnine, La structure des *p*-groupes de Sylow des groupes symmétriques finis, *Ann. Sci. École Norm. Sup.* **3** (1948), 239–276.

[Ka1] W. M. Kantor, Polynomial-time algorithms for finding elements of prime order and Sylow subgroups, *J. Algorithms* **6** (1985), 478–514.

[Ka2] W. M. Kantor, Sylow's theorem in polynomial time, *J. Comput. System Sci.* **30** (1985), 359–394.

[Ka3] W. M. Kantor, Finding Sylow normalizers in polynomial time, *J. Algorithms* **11** (1990), 523–563.

[Ka4] W. M. Kantor, Geometry in computer algebra systems, unpublished manuscript for Magma Conf. 1993. [http://www.uoregon.edu/~kantor/PAPERS/magmapaper.ps.]

[KL1] W. M. Kantor and E. M. Luks, Computing in quotient groups *in* "Proceedings of the 22nd ACM Symposium on Theory of Computing, 1990," pp. 524–534.
[KL2] W. M. Kantor and E. M. Luks, in preparation.
[KP] W. M. Kantor and T. Penttila, Reconstructing simple group actions, to appear.
[KS] W. M. Kantor and Á. Seress, Black box classical groups, submitted.
[KT] W. M. Kantor and D. E. Taylor, Polynomial-time versions of Sylow's theorem, *J. Algorithms* **9** (1988), 1–17.
[KR] R. M. Karp and V. Ramachandran, Parallel algorithms for shared-memory machines, *in* "Handbook of Theoretical Computer Science, A" (J. Van Leeuwan, Ed.), pp. 869–941, MIT Press/Elsevier, 1990.
[KlLi] P. B. Kleidman and M. W. Liebeck, The subgroup structure of the finite classical groups, London Mathematical Society Lecture Note Series, Vol. 129, Cambridge Univ. Press, Cambridge, 1990.
[Lu1] E. M. Luks, Isomorphism of graphs of bounded valence can be tested in polynomial time, *J. Comput. System Sci.* **25** (1982), 42–65.
[Lu2] E. M. Luks, Parallel algorithms for permutation groups and graph isomorphism, *in* "Proceedings of the 27th IEEE Symposium on the Foundations of Computer Science, 1986," pp. 292–302.
[Lu3] E. M. Luks, Computing the composition factors of a permutation group in polynomial time, *Combinatorica* **7** (1987), 87–99.
[Lu4] E. M. Luks, Computing in solvable matrix groups, *in* "Proceedings of the 33rd IEEE Symposium on the Foundations of Computer Science, 1992," pp. 111–120.
[Lu5] E. M. Luks, Permutation groups and polynomial-time computation, "Groups and Computation" (L. Finkelstein and W. M. Kantor, Eds.), pp. 139–175, Amer. Math. Soc., Providence, 1993.
[LM] E. M. Luks and P. McKenzie, Parallel computation in solvable permutation groups, *J. Comput. System Sci.* **37** (1988), 39–62.
[Ma1] P. D. Mark, Parallel computation of Sylow subgroups of solvable groups, *in* "Groups and Computation" (L. Finkelstein and W. M. Kantor, Eds.), pp. 177–187, Amer. Math. Soc., Providence, 1993.
[Ma2] P. D. Mark, "Sylow's Theorem and Parallel Computation," Ph.D. thesis, University of Oregon, 1993. [Tech. Rep. 93-19, Department of Computer and Information Science, Univ. of Oregon.]
[Mc] P. McKenzie, "Parallel Complexity and Permutation Groups," Ph.D. thesis, University of Toronto, 1984. [Tech. Rep. 173/84, Department of Computer Science, Univ. of Toronto.]
[MC] P. McKenzie and S. A. Cook, The parallel complexity of abelian permutation group problems, *SIAM J. Comput.* **16** (1987), 880–909.
[Mo] P. Morje, "A Nearly Linear Algorithm for Sylow Subgroups of Permutation Groups," Ph.D. thesis, Department of Mathematics, Ohio State University, 1996.
[Mu] K. Mulmuley, A fast parallel algorithm to compute the rank of a matrix over an arbitrary field, *Combinatorica* **7** (1987), 101–104.
[Si] C. C. Sims, Computational methods in the study of permutation groups, *in* "Computational Problems in Abstract Algebra" (J. Leech, Ed.), pp. 169–183, Pergamon, Elmsford, NY, 1970.
[Ta] D. E. Taylor, "The Geometry of the Classical Groups," Heldermann, Berlin, 1992.
[VY] O. Veblen and J. W. Young, "Projective Geometry," Ginn, Boston, 1916.
[We] A. Weir, A Sylow p-subgroup of the classical groups over finite fields with characteristic prime to p, *Proc. Amer. Math. Soc.* **6** (1955), 529–533.
[Wi] H. Wielandt, "Finite Permutation Groups," Academic Press, New York, 1964.