SYLOW'S THEOREM AND PARALLEL COMPUTATION

by

PETER D. MARK

A DISSERTATION

Presented to the Department of Computer and Information Science
and the Graduate School of the University of Oregon
in partial fulfillment of the requirements
for the degree of
Doctor of Philosophy

August 1993

APPROVED: Eugene M. Luks

Dr. Eugene M. Luks

An Abstract of the Dissertation of

Peter D. Mark for the degree of Doctor of Philosophy

in the Department of Computer and Information Science

to be taken August 1993

Title: SYLOW'S THEOREM AND PARALLEL COMPUTATION

Approved: Eugene M. Luks

Dr. Eugene M. Luks

Given a finite group G and a prime p, a Sylow p-subgroup of G is a subgroup whose order is the largest power of p dividing $|G|$. Sylow's theorem asserts that such subgroups exist and that any two such are conjugate. This theorem is a fundamental tool in group-theoretic investigations. Similarly, in computational group theory there is an important role for efficient constructive analogues of Sylow's theorem. For computational purposes, it is typical to deal with large groups by specifying a permutation action, storing only a small set of generating permutations. This leads naturally to the following computational problems.

SYLFIND(p, G)

Given: a prime p and generators for a group G,

Find: generators for a Sylow p-subgroup $P \leq G$.

SYLCONJ(P_1, P_2, G)

Given: generators for G and for two of its Sylow p-subgroups P_1 and P_2,

Find: an element $g \in G$ for which $P_1^g = P_2$.

In a recent series of papers, Kantor has shown that these problems have polynomial-time solutions. His methods exploit both a well-developed library of polynomial-time procedures for permutation groups and consequences of the classification of finite simple groups. The impressive nature of the machinery used for sequential solutions left open the question of whether there are methods that can take advantage of parallel machines. Following the prevalent paradigm, the question arises whether such problems are in the complexity class NC; i.e., are they solvable in polylogarithmic time ($O(\log^c n)$ steps) using a polynomial number of processors working in parallel? This dissertation establishes an affirmative answer, placing SYLFIND and SYLCONJ into NC.

VITA

NAME OF THE AUTHOR: Peter D. Mark

PLACE OF BIRTH: Philadelphia, Pennsylvania

DATE OF BIRTH: July 20 1957

GRADUATE AND UNDERGRADUATE SCHOOLS ATTENDED:

University of Oregon
Cornell University
Harvard College

DEGREES AWARDED:

Ph. D. Computer Science 1993, University of Oregon
M. S. Computer Science 1986, Cornell University
A. B. Mathematics 1979, Harvard College

AREAS OF SPECIAL INTEREST:

Parallel Computation, Algebraic Algorithms

PROFESSIONAL EXPERIENCE:

Visiting Faculty, Department of Mathematics and Computer Science
Colby College, Waterville, Maine 1992-1993

Graduate Research Assistant, Department of Computer Science
University of Oregon, Eugene, Oregon 1987-1992

Graduate Teaching Fellow, Department of Computer Science
University of Oregon, Eugene, Oregon 1987-1992

Software Engineer, SofTech, Inc.
Waltham, Massachusetts 1981-1983

Computer Programmer-Operator, Negev Airbase Constructors
Tel Aviv, Israel 1979-1981

AWARDS AND HONORS:

McMullen Fellowship, Cornell University, 1984
Harvard College Scholarship, 1979
Valedictorian, Nether Providence High School, 1975
Wallingford, Pennsylvania

PUBLICATIONS:

Parallel Computation of Sylow Subgroups in Solvable Groups,
in *Groups and Computation*, to appear in the DIMACS Series
in Discrete Mathematics and Theoretical Computer Science

ACKNOWLEDGEMENTS

It is a pleasure to acknowledge my indebtedness to my advisor, Eugene Luks, whose help and guidance are reflected throughout this dissertation. His sharp mathematical insight and sense of mathematical style led to many improvements to its the organization and exposition. This applies equally to William Kantor, who carefully read and meticulously critiqued numerous preliminary drafts of this dissertation, particularly the final chapter. His helpful explanations of the subtleties of finite simple groups were invaluable.

I am also grateful to Charley Wright, whose course on classical groups was as interesting as it was useful, and to Chris Wilson and Andrzej Proskurowski, who served on my dissertation committee.

Larry Finkelstein, Gene Cooperman, and Namita Sarawagi provided a welcoming and supportive environment at Northeastern University, where I spent the spring term of 1990.

Ken Blaha shared his office, his interest in permutation group problems, and his good cheer. Many other students, faculty, and staff of the Department of Computer and Information Science made my years at the University of Oregon pleasant and enjoyable. I am also deeply thankful to Mark Freeland, Phil Moore, Eugene Pinsky, Eric Taswell, and Steve Taswell for their close friendship of many years.

Most of all, I would like to acknowledge my parents, sister, and grandmother, whose faith in my abilities never waned, and whose love and encouragement inspired me to persevere.

The research for this dissertation was partially funded by National Science Foundation Grant CCR-9013410.

DEDICATION

To My Parents

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

Historical Background

Interest in computational group theory initially arose in the 1960s when group theorists began to find the computer a useful tool in their investigations, especially in the construction of large simple groups. By the 1970s and 1980s whole software systems had been designed to aid in group-theoretic computation, notably CAYLEY and GAP. The group theoretic algorithms themselves became a fertile field of investigation in the early 1980s when Luks employed group theoretic techniques to develop efficient algorithms for restricted versions of the problem of graph isomorphism, a problem whose complexity is one of the central open questions in theoretical computer science [21]. This sparked extensive research into group theoretic algorithms within the computer science community.

Over the last two decades, sequential, polynomial-time algorithms were found for a variety of basic permutation group problems, including determining the order of a such a group, testing membership, and finding some of the important subgroups such as the center and commutator subgroup. The study of group theoretic algorithms has continued to influence theoretical computer science. For example, Babai's study of matrix group problems led to the development of "Arthur-Merlin" games and a new complexity hierarchy that collapses above NP; this work also contributed to the development of interactive proof systems [5].

There has also been an interplay between pure and computational group theory. Algorithms have become progressively more complex, employing recent group theoretic results that give, for example, bounds on the length of subgroup towers in permutation groups (Babai [3]), bounds on the order of primitive solvable groups (Pálfy [28]), and bounds on the order of primitive groups with bounded nonabelian composition factors (Babai, Cameron, and Pálfy [4]). These purely mathematical investigations were actually inspired by the computational complexity arguments that require them. Perhaps the most striking use of deep mathematical results in group-theoretic algorithms is the use of consequences of the classification of finite simple groups in two fundamentally important algorithms: Luks's algorithms for finding composition factors of permutation groups [22], and Kantor's sequential, polynomial time algorithms for SYLFIND, SYLCONJ, and related problems [16, 17, 18].

Just as Sylow subgroups play a fundamental role in group theory, efficient algorithms for Sylow subgroup computations have played, and can be expected to play, an analogous role in computational group theory. Sylow subgroups have already been used by Kantor and Luks in [19] for finding centers in quotient groups and for a variety of other problems (see also [25]). A restricted version of SYLFIND also played a role in Luks's development of a polynomial time algorithm for bounded valence graph isomorphism testing [24].

Parallel Algorithms for Permutation Group Problems

Inspired by new generations of machines, new theoretical models were developed to describe and analyze parallel computation. In particular, the class NC consists of those problems with algorithms that employ $O(n^c)$ processors that communicate via shared memory and require $O(\log^k n)$ time steps, where n is the input

size and c and k are constants. This class was first described by Pippinger in [29], and gives a useful framework in which to study the inherent parallelizability and logical structure of computations independent of any interprocessor connection network. In the case of permutation group algorithms, many of the known techniques appeared to depend on inherently sequential methods. In a series of papers by McKenzie and Cook [26], Luks and McKenzie [23], Luks [24], and Babai, Luks, and Seress [6], entirely new machinery was developed for parallel permutation group computation. It ultimately brought a sizable portion of the collection of polynomial-time algorithms, including finding composition factors, into NC. However, a number of critical questions remained open. As pointed out by Babai, Luks, and Seress in [6], a leading one of these problems was the parallelization of the problem of finding Sylow subgroups. This dissertation gives an NC algorithm for this problem, as well as the problem of computing an element that conjugates one given Sylow subgroup to another.

Most of the sequential permutation group algorithms exploit a tower of subgroups, $G = G_0 \geq G_1 \geq \cdots \geq G_n = 1$, that is either a series of pointwise stabilizers or a composition series for G [13, 16, 17, 31]. Membership testing, for example, uses a series of point stabilizers and reduces membership testing for G_i to membership testing for G_{i+1} [31]. Kantor's polynomial-time sequential Sylow algorithms used a composition series for G.

Both of these towers can have length linear in the degree n of G, and hence may be too long for computation in NC. The parallelization of order and membership testing as well as the new NC Sylow algorithms utilize a different (normal) series $G = K_0 \rhd K_1 \rhd \cdots \rhd K_r = 1$ for G whose length r is polylogarithmic in n. The quotients K_i/K_{i+1} of successive groups in the series are *semisimple*, i.e. direct

products of simple groups. The existence and NC-constructability of such a normal semisimple series are demonstrated by Luks in [24], and by Babai, Luks, and Seress in [6].

Groups in this tower arise from two different divide and conquer strategies. The first involves only a naive construction of a *structure forest* described by Luks and McKenzie in [23], a data structure based on the orbits and imprimitivity blocks of the group. This reduces to the primitive group case, which requires a second divide and conquer approach based on the internal structure of primitive groups, Luks's composition factors algorithm, and consequences of the classification of finite simple groups. The tower can be refined so that successive quotients K_i/K_{i+1} are direct products of simple groups that are either all abelian or all nonabelian.

One can then describe the algorithm for SYLFIND, for example, as the computation of a series of subgroups $G = P_0 \geq P_1 \geq \cdots \geq P_r$ where P_i/K_i is a Sylow p-subgroup of G/K_i and $G = K_0 \rhd K_1 \rhd \cdots \rhd K_r = 1$ is a tower of polylogarithmic length as described above. As noted above, such a semisimple tower is available; indeed it is intrinsic to the basic machinery for NC computation, including membership testing [24, 6]. However, it simplifies the exposition to avoid repeated and explicit reference to a precomputed tower. Thus, we compute suitable K_i as they are needed. Given a group $K \trianglelefteq G$ that appears as one of the groups in the (implicit) tower, we compute a subgroup $L \trianglelefteq K$ (where also $L \trianglelefteq G$) such that K/L is either abelian semisimple, or nonabelian semisimple. In fact, L is the successor of K in some polylogarithmic semisimple tower for G. In addition, in the case where K/L is nonabelian semisimple, we require that either all the simple factors are divisible by p, or none are.

An important ingredient is the ability to find an NC-efficient representation

domain for K/L. If K/L is abelian, we represent it as a product of vector spaces, otherwise we build a faithful permutation representation for K/L. NC-representation domains, and procedures for their construction, are discussed in Chapter II.

In solvable groups, all the quotients are abelian semisimple, and SYLFIND reduces to the following two problems, which are described in Chapter III: 1. given $L \trianglelefteq K \trianglelefteq H$ where H/K is an elementary abelian p-group and K/L is an elementary abelian p'-group, find a group $P \leq H$ for which P/L is a Sylow p-subgroup of H/L; and 2. given $L \trianglelefteq K \trianglelefteq H \trianglelefteq G$ and $P \leq H$ where L, K, H, P are as in 1., find a subgroup $G^* \leq G$ that normalizes P and contains a Sylow p-subgroup of G. The latter problem is an algorithmic form of the Frattini argument. These permutation group problems reduce to the problem of solving systems of linear equations over finite fields. This problem was shown to be in NC by work culminating with Mulmuley [27]; significant contributions toward this result were made by Berkowitz [7], Csanky [11], Chistov [10], and Borodin, von zur Gathen, and Hopcroft [8].

The technique of translating group theoretic conditions in abelian semisimple quotients into systems of linear equations appeared first in [23], and was later exploited by Luks to give an NC algorithm for SYLFIND in solvable groups.

The Reduction to the Simple Case

Chapter IV gives reductions of SYLFIND and SYLCONJ to the case where G is simple. The reduction involves computing in nonabelian semisimple groups, where parallelism arises in a natural way by working within all simple factors independently. As an intermediate step, Chapter IV introduces two problems, SYLFIND-$\mathcal{L}_{p'}$ and SYLCONJ-$\mathcal{L}_{p'}$, which, respectively, solve the problems of finding and conjugating Sylow p-subgroups for the class $\mathcal{L}_{p'}$ of groups whose nonabelian composition

factors have orders relatively prime to p. Introducing the class $\mathcal{L}_{p'}$ allows algorithms for finding and conjugating Sylow p-subgroups for solvable groups, $\mathcal{L}_{p'}$-groups, and general permutation groups to share a common logical structure, and permits the timing arguments for each of these algorithms to be handled in a uniform manner that exploits the polylogarithmic length of a normal series for G as described above. Here, as in the solvable case, an algorithmic form of the Frattini argument plays an important role.

Handling Simple Groups

The NC Sylow algorithms for handling simple groups follow Kantor in using a case analysis based upon the classification of finite simple groups. Kantor's concern was establishing polynomial-time Sylow algorithms; in fact his overall approach leads to natural parallelizations. To describe these parallelizations, we first give an overview of the techniques involved.

If G is an alternating group, we construct a *natural action* for G, i.e., an action of G on a set Δ upon which G acts as $\mathrm{Alt}(\Delta)$. Then, Sylow p-subgroup computations use a wreath product construction (in effect, building complete p-ary forests on Ω).

If G is a classical simple group, we also construct a *natural action* for G, i.e., an action of G on a permutation domain Y that corresponds to the set of 1-spaces of a vector space involved in the abstract definition of G. For example, if $G \cong PSp(V)$, then there is a bijection from Y to the set of 1-spaces of V, where the action of G on Y is permutation-isomorphic to the action of $PSp(V)$ on the 1-spaces of V. Once we construct this natural action, we identify G (i.e., determine the name and associated parameters of the simple group to which G is isomorphic), and translate questions about the original permutation action for G to questions about this natural action.

This new domain is coordinatized by exploiting geometric properties of finite projective spaces. The actions of the original generators of G on this domain are determined using elements of $GL(V)$, and a form involved in the definition of G is constructed. Finally, the algorithms exploit the structure of a Sylow p-subgroup P of G and the decomposition of V into P-invariant subspaces, then translate this information to the original permutation action of G on Ω.

The parallelizations of these techniques critically depend on the relatively small size of the natural actions constructed. If G is given by generating permutations on a set Ω, then the vector space V has size polynomial in $|\Omega|$, and hence $\dim(V)$ is logarithmic in $|\Omega|$. These two facts permit all vectors in V to be examined in parallel in constant time, and allow algorithms to proceed sequentially over sequences of subspaces of length $\dim(V)$. Despite the straightforwardness of the parallelizations, many of the procedures given by Kantor in [16, 17, 18] have undergone significant revision in Chapter V of this dissertation, and the structure of their logical dependence has been substantially reoganized.

CHAPTER II

DEFINITIONS AND BASIC TECHNIQUES

This chapter describes tools for NC computation in permutation groups. We describe semisimple quotient groups and show how to find a subgroup H of a given group $G \leq \mathrm{Sym}(\Omega)$ for which G/H is semisimple. We also describe how to construct NC-effective representation domains for such a quotient group. A basic tool used in Chapters III and IV is a semisimple tower for G modulo a normal subgroup N, i.e., a tower $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = N$ in which quotients G_i/G_{i+1} of successive subgroups are semisimple and have NC-effective representation domains.

Primitive NC Operations for Permutation Groups

Permutation-group problems require three basic permutation operations: computing the product of two permutations, computing inverses of permutations, and computing large powers of permutations. The first two are straightforward. To form a power α^b of a permutation α, where b is represented in binary (in practice, b may be $O(n!)$ where n is the degree of α), form α^b independently on each cycle of α by reducing b modulo the cycle length (see [26]). Note that, for sequential computation, one does not need to emphasize such powering as a "primitive" operation, for it is accomplished by repeated-squaring, therefore by a polynomial number of multiplications. However, the number of successive squarings would be prohibitive for an NC result.

Basic NC Permutation Group Algorithms

An *action* of G on a set Ω is a homomorphism $G \rightarrow \mathrm{Sym}(\Omega)$. If this homomorphism is injective, the action of G on Ω is *faithful*. If $M \leq G$, then G/M denotes the set of right cosets of M in G. The action of G on G/M is given by $g \mapsto \phi_g \in \mathrm{Sym}(G/M)$ where $(Ma)^{\phi_g} = Mag$ for each $Ma \in G/M$. If $G \leq \mathrm{Sym}(\Omega)$, then $|\Omega|$ is the *degree* of G. If $\alpha \in \Omega$, then the *orbit* of α is the set $\{\beta \in \Omega \mid \alpha^g = \beta \text{ for some } g \in G\}$. This orbit is denoted α^G. The set of orbits of G partition Ω. If $O \subseteq \Omega$ is an orbit for G, then the group G induces on O is denoted G^O, and is called a *constituent* of G. If G is has only one orbit, then the action of G on Ω is said to be *transitive*. The subgroup of G that stabilizes a point $\alpha \in \Omega$ is denoted G_α; the subgroup of G that stabilizes a subset Δ (the set stabilizer of Δ) is denoted $G_{\{\Delta\}}$. If G acts transitively on Ω, and it is possible to partition Ω into disjoint subsets $\Omega = \Delta_1 \cup \cdots \cup \Delta_m$ where $1 < |\Delta_i| < |\Omega|$ and for each $g \in G$ and each Δ_i, $\Delta_i^g \cap \Delta_i = \emptyset$ or Δ_i, then the action of G on Ω is said to be *imprimitive*. In that case, each set Δ_i is called a *block of imprimitivity* and the collection $\mathcal{C} = \{\Delta_1, \ldots, \Delta_m\}$ is called a *block system* for G. A block $\Delta \subseteq \Omega$ is a *minimal block* for G if $G_{\{\Delta\}}$ acts primitively on Δ. A block system $\mathcal{C}$ for G is called *minimal* if G acts on $\mathcal{C}$ primitively. See, [14], [30], or [33] for additional discussion of primitivity.

An NC algorithm for the following problem is given in [6]. It uses the classification of finite simple groups.

Problem II.1 MEMBER(G, x)

GIVEN: a permutation group $G = \langle S \rangle \leq \mathrm{Sym}(\Omega)$ and an element $x \in \mathrm{Sym}(\Omega)$,

DETERMINE: whether $x \in G$.

Remark II.2 The membership test given in [6] sequentially computes sets of permutations $\mathcal{S} = \mathcal{S}_0, \mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_r$ where r is polylogarithmic in $|\Omega|$, and for each $i = 1, \ldots, r$, $|\mathcal{S}_i|$ is polynomial in $|\Omega|$, and each permutation in $\mathcal{S}_i$ is an inverse or a power of a permutation in $\cup_{l=0}^{i-1}\mathcal{S}_l$, or the product of two permutations in $\cup_{l=0}^{i-1}\mathcal{S}_l$. and where $x \in \mathcal{S}_r$ if and only if $x \in G$. Hence the membership test is *constructive,* i.e., it gives an NC procedure to compute x from $\mathcal{S}$, for any $x \in G$.

Remark II.3 Some applications require the ability to form *liftings* of elements and subgroups. Specifically, suppose we are given a permutation group $G = \langle \mathcal{S} \rangle \leq \mathrm{Sym}(\Omega)$ and an additional action of G on another set Δ, i.e., a homomorphism $\delta : G \rightarrow \mathrm{Sym}(\Delta)$. The image of G under δ is denoted G^Δ, and the image of any element $g \in G$ is denoted g^Δ. The homomorphism δ may be specified by the set $\mathcal{S}^\Delta = \{g^\Delta \mid g \in \mathcal{S}\}$, i.e., the set of images of the generators of G under the homomorphism δ. The set $\mathcal{S}^\Delta$ is sufficient to determine the map δ: given any $g \in G$, compute g^Δ by applying the same operations to S^Δ that yields $g \in G$ in an NC constructive membership test (see Remark II.2).

Moreover, the process may be reversed: given any element $g^* \in G^\Delta \leq \mathrm{Sym}(\Delta)$, we can find an element $g \in G$ for which $g^\Delta = g^*$ (i.e., a *lifting* of g^*). The action on Δ of set of generators suffices to compute a lifting of any $g^* \in G^\Delta$: apply the same operations to $\mathcal{S}$ in $\mathrm{Sym}(\Omega)$ that yields $g^* \in G^\Delta$ from $\mathcal{S}^\Delta$ in an NC constructive membership test (see Remark II.2).

Furthermore, if $H^* = \langle \mathcal{T}^* \rangle \leq G^\Delta$, we can find generators for $H \leq G \leq \mathrm{Sym}(\Omega)$ for which $H^\delta = H^*$ (i.e., a *lifting* of H^*). If $\mathcal{T}$ is comprised of generators for the kernel of the action of G on Δ (found using Problem II.18) together with liftings of each of the generators in $\mathcal{T}^*$ for H^*, then $\mathcal{T}$ will generate H. Hence we can find liftings of both elements and subgroups given in terms of auxiliary actions. We will

write LIFT(g^*) or LIFT(H^*) when the action δ is clear from the context.

Remark II.3 permits the following:

Remark II.4 Let $G = \langle \mathcal{S} \rangle \in \mathrm{Sym}(\Omega)$ and suppose G also acts on a set Δ. The phrase "find the action of G on Δ" means: *find the image in this action of a generating set for G, i.e., find $\mathcal{S}^\Delta = \{g^\Delta \mid g \in \mathcal{S}\}$.*

In problems II.5 - II.12, we assume G is given by a set of generating permutations: $G = \langle \mathcal{S} \rangle \leq \mathrm{Sym}(\Omega)$.

Problem II.5 ORBITS(G)

GIVEN: a group $G \leq \mathrm{Sym}(\Omega)$,

FIND: the orbits of G on Ω.

Lemma II.6 *ORBITS is in NC.*

Let Γ be the graph with vertex set Ω and edge set $\{(\alpha, \beta) \mid \alpha^g = \beta$ for some $g \in \mathcal{S}\}$. The orbits of G are the connected components of Γ, found by computing the transitive closure of Γ. □

Definition II.7 *Let H be a subgroup of G. A* transversal *for H in G is a complete set of coset representatives for H in G.*

Problem II.8 FIND-TRANSVERSAL1(G, L)

GIVEN: a point stabilizer L of $G = \langle S \rangle \leq \mathrm{Sym}(\Omega)$,

FIND: a transveral for L in G.

Lemma II.9 *FIND-TRANSVERSAL1 is in NC.*

Proof: Let $\Omega = \{1, \ldots, n\}$ and let Γ be the graph with vertex set Ω and edge set $\{(\alpha, \beta) \mid \alpha^g = \beta \text{ for some } g \in \mathcal{S}\}$. Add the identity to the set of generators $\mathcal{S}$, and maintain a table $T[i,j]$, $1 \leq i,j \leq n$ of entries in G, where initially $T[i,j] = g$ if there is some $g \in \mathcal{S}$ such that $i^g = j$, otherwise, $T[i,j]$ is empty. Proceed in a succession of rounds; in each round, do the following. For each empty entry $T[i,j]$ in parallel, for each $k = 1, \ldots, n$ in parallel, if $T[i,k]$ and $T[k,j]$ are both nonempty, then set $T[i,j]$ to $T[i,k]T[k,j]$. After l rounds, $T[i,j]$ is nonempty if there is a path in Γ from i to j of length less than or equal to 2^l. Since the diameter of Γ is less than $|\Omega|$, after $\log|\Omega|$ rounds, the first row of T contains a desired transversal. □

Problem II.10 MINIMAL-BLOCKS(G)

GIVEN: a transitive group $G \leq \mathrm{Sym}(\Omega,$

FIND: a block system $\mathcal{C}$ for G where, for any block $\Delta \in \mathcal{C}$, $G_{\{\Delta\}}$ acts primitively on Δ.

Lemma II.11 *MINIMAL-BLOCKS is in NC.*

Proof: Fix $\alpha \in \Omega$. For each $\beta \in \Omega$ in parallel, find a block system in which the blocks have size as small as possible and α and β are contained in the same block as follows. Form the graph Γ with vertices Ω and edges $\{(\alpha^g, \beta^g) \mid g \in G\}$ (by computing the orbit of (α, β) in the action of G on $\Omega \times \Omega$ using Problem II.5). Let $\mathcal{C}_\beta$ be the set of connected components of Γ (found using transitive closure on graphs). Then $\mathcal{C}_\beta$ is a block system for which α and β are contained in the same block. Let $\mathcal{C}$ be such a block system for which the blocks are of minimal size. The blocks in $\mathcal{C}$ cannot be unions of smaller blocks of another block system, hence for each block $\Delta \in \mathcal{C}$, $G^{\Delta}_{\{\Delta\}}$ is primitive. □

Problem II.12 MINIMAL-BLOCK-SYSTEM(G)

GIVEN: a transitive group $G \leq \mathrm{Sym}(\Omega)$,

FIND: a block system $\mathcal{C}$ for G where the induced action of G on $\mathcal{C}$ is primitive.

Lemma II.13 *MINIMAL-BLOCK-SYSTEM is in NC.*

Proof: Use Problem II.10 to find a block system $\mathcal{C}$ in which the blocks have minimal size. If G acts primitively on $\mathcal{C}$, then return $\mathcal{C}$. Otherwise, replace Ω with $\mathcal{C}$, and recurse. In a given recursive call, the size of the block system is at most half the size of the block system in the previous call, so no more than $\log |\Omega|$ recursive calls are possible. □

Remark II.14 *If at each stage in the algorithm, we view each block Δ of $\mathcal{C}$ as a vertex v_Δ in a tree, and we view the points of Ω contained in Δ as children of v_Δ, then we obtain a tree with leaves consisting of the points of Ω. In an intransitive group, one obtains a forest, with one tree per orbit. Such a forest is called* a structure forest *for G (see [23]). Problems II.5, II.10 and II.12 show that a structure forest for G may be found in NC.*

NC algorithms for the following permutation group problems II.15 - II.21 are given in [6]. These algorithms use the classification of finite simple groups. As above, we assume $G = \langle S \rangle \leq \mathrm{Sym}(\Omega)$.

Problem II.15 ORDER(G)

GIVEN: a group $G \leq \mathrm{Sym}(\Omega)$,

FIND: $|G|$.

Problem II.16 COMMUTATOR(G)

GIVEN: a permutation group $G = \langle \mathcal{S} \rangle \leq \mathrm{Sym}(\Omega)$,

FIND: the commutator subgroup G' of G.

Problem II.17 FACTOR(x, H, N)

GIVEN: $H, N \leq \mathrm{Sym}(\Omega)$ where $N = \langle Y \rangle$ is normalized by $H = \langle X \rangle$ and $x \in HN$,

FIND: $h \in H, n \in N$ such that $x = hn$.

Problem II.18 KERNEL(G, Δ)

GIVEN: a group $G \leq \mathrm{Sym}(\Omega)$ and an action of G on an additional set Δ,

FIND: the kernel of the action of G on Δ.

Problem II.19 POINTWISE-STABILIZER(G, A)

GIVEN: a group $G \leq \mathrm{Sym}(\Omega)$ and a subset $A \subseteq \Omega$,

FIND: the pointwise stabilizer of A in G.

Remark II.20 In particular, POINTWISE-STABILIZER includes the problem of finding kernels of actions (Problem II.18) as a special case. For, if $G \leq \mathrm{Sym}(\Omega)$ also acts on a set Δ, we can view G as a subgroup of $\mathrm{Sym}(\Omega \cup \Delta)$. Then the kernel of the action of G on Δ is the pointwise stabilizer of Δ. In fact, the NC permutation group machinery developed in [6] gives a simpler algorithm for finding kernels independent of POINTWISE-STABILIZER.

Problem II.21 INTERSECTION(H, N)

GIVEN: permutation groups $H, N \leq \mathrm{Sym}(\Omega)$, where H normalizes N,

FIND: $H \cap N$.

An important application of FACTOR (Problem II.17) that is used later in Chapter V is:

Problem II.22 COSET-INTERSECTION(H, c, N)

GIVEN: $H, N \leq \mathrm{Sym}(\Omega)$, $c \in \mathrm{Sym}(\Omega)$, and H normalizes N,

FIND: $Hc \cap N$.

Lemma II.23 *COSET-INTERSECTION is in NC.*

Proof: $Hc \cap N$ is either empty or a coset of $H \cap N$. $Hc \cap N \neq \emptyset$ if and only if $hc = n$ for some $h \in H, n \in N$, i.e., if and only if $c \in HN$, which can be tested using Problem II.1. If $c \in HN$, then use FACTOR (Problem II.17) to find $h \in H, n \in N$ such that $c = hn$. Note that $Hc = Hn$, so $Hc \cap N = (H \cap N)n$. Return $(H \cap N)n$. □

Problem II.24 FIND-TRANSVERSAL2(G, M, H, R_H)

GIVEN: $H \leq M \leq G \leq \mathrm{Sym}(\Omega)$ and a transversal R_H for H in G,

FIND: a transversal R_M for M in G.

Lemma II.25 *FIND-TRANSVERSAL2 is in NC.*

Proof: To find a transversal R_M for M in G, define an equivalence relation on R_H by $a \sim b \Leftrightarrow a^{-1}b \in M$ (using Problem II.1 in parallel) and return a collection R_M that contains one representative from each equivalence class. □

Problem II.26 MINIMAL-SUBGROUPS(G, H, R_H)

GIVEN: $H < G \leq \mathrm{Sym}(\Omega)$ with $[G : H]$ polynomially bounded, and a transversal R_H for H in G,

FIND: the set of all pairs of the form (M, R_M) where M is a minimal subgroup of G that properly contains H (i.e., $M \leq G$ and H is maximal in M), and R_M is a transversal for M in G.

Lemma II.27 *MINIMAL-SUBGROUPS is in NC.*

Proof: For each pair $g_1, g_2 \in R_H \setminus H$ in parallel, if $\langle g_1, H\rangle < \langle g_2, H\rangle$ (tested using Problem II.1), then discard g_2. For each nondiscarded g, H is maximal in $M = \langle g, H\rangle$. Let $R_M =$ FIND-TRANSVERSAL2(G, M, H, R_H) (Problem II.24). Return the set of pairs of such groups and their transversals. □

Problem II.28 MAXIMAL-SUBGROUP(G, H, R)

GIVEN: $H < G \leq \mathrm{Sym}(\Omega)$ with $[G : H]$ polynomially bounded, and a transversal R_H for H in G,

FIND: a maximal subgroup $M < G$ containing H, and a transversal R_M for M in G.

Lemma II.29 *MAXIMAL-SUBGROUP is in NC.*

Proof: If $A = \langle g, H\rangle \neq G$ for some $g \in R_H$ (all $|R_H|$ such tests can be performed in parallel using Problem II.15) then let $R_A =$ FIND-TRANSVERSAL2(G, A, H, R_H) be a transversal for A in G (Problem II.24), and recursively return $(M, R_M) =$ MAXIMAL-SUBGROUP(G, A, R_A); otherwise (i.e., $\langle g, H\rangle = G$ for each $g \in R_H$), return (H, R_H).

Each recursive call at least doubles the size of the subgroup of G containing H being considered. Since $[G : H]$ is polynomially bounded, the number of recursive calls is logarithmic, hence the algorithm is in NC. □

Alternatively, we may also find a maximal subgroup as follows. Find the action of G on the right cosets of H (Problem II.30), and find a block system for this action upon which G acts primitively (Problem II.12), obtain a point stabilizer in this action, and lift this stabilizer to the given action of G on Ω.

Problem II.30 BUILD-ACTION(G, L, R_L)

GIVEN: a subgroup L of a group $G = \langle S \rangle \leq \mathrm{Sym}(\Omega)$ of index polynomial in $|\Omega|$, and a transversal R_L for L in G,

FIND: the action of G on G/L (see Remark II.4).

Lemma II.31 *BUILD-ACTION is in NC.*

Proof: For each $s \in S$ in parallel, for each pair $h, k \in R_L$ in parallel, use Problem II.1 to test if $hsk^{-1} \in L$. If so, then s maps Lh to Lk (since $Lhs = Lk$). Hence the action of G on Δ is computable in NC, where Δ is the set of cosets G/L. Return the set Δ, together with this action (see Remark II.4). □

Problem II.32 PRIMITIVE-ACTION(G, Ω)

GIVEN: $G \leq \mathrm{Sym}(\Omega)$

FIND: a primitive action of G on a set Δ (see Remark II.4).

Lemma II.33 *PRIMITIVE-ACTION is in NC.*

Proof: Let H be a point stabilizer of G (Problem II.19) and let R_H be a transversal for H in G (Problem II.8). Let (M, R_M) = MAXIMAL-SUBGROUP(G, H, R_H)

(Problem II.28) and let $\Delta = G/M$. Then the map $G \to \mathrm{Sym}(\Delta)$ given by $g \mapsto \phi_g$, where $\phi_g : Mx \mapsto Mxg$ gives a primitive action of G on Δ. This action is returned by BUILD-ACTION(G, M, R_M) (Problem II.30; see also Remark II.4). □

Alternatively, a primitive action of G may also be found by finding a minimal block system $\mathcal{C}$ (Problem II.12), determining the induced action of G on $\mathcal{C}$, and lifting the result back to the given action on Ω (Remark II.3). The method given in the proof utilizes available machinery already developed for other other purposes (see, for example, Problem V.27).

Note that if G is simple, PRIMITIVE-ACTION produces a faithful action of G.

Problem II.34 FIND-TRANSVERSAL3(G, L)

GIVEN: $L < G \leq \mathrm{Sym}(\Omega)$ where $|G|$ is quasipolynomial in $|\Omega|$ (i.e., $|G| = O(\exp(\log^c |\Omega|))$ for some constant c), and $[G : L]$ is polynomial in $|\Omega|$,

FIND: a transversal for L in G.

Lemma II.35 *FIND-TRANSVERSAL3 is in NC.*

Proof: Let H be a point stabilizer in G for which $H < G$ (Problem II.19) and let R_H be a transversal for H in G (Problem II.8). Obtain the action of G on G/H using BUILD-ACTION(G, H, R_H) (Problem II.30). Find $L_1 = L \cap H$ as the stabilizer in L of H in the action of L on the cosets of H in G. Recursively find a transversal R_{L_1} of L_1 in H. The recursion has polylogarithmic depth, because the length of any point stabilizer tower for G is polylogarithmic in $|\Omega|$ since $|G|$ is quasipolynomial in $|\Omega|$ by hypothesis. Since we can find a transversal R_H of H in G (using Problem II.8), we obtain a transversal of L_1 in G by forming the set $\{ab \mid a \in R_{L_1}, b \in R_H\}$. Since $L_1 \leq L \leq G$, we may obtain a transversal for L in G using Problem II.24. □

Semisimple Quotient Groups and Their Representations

Semisimple groups (groups that are direct products of simple groups) play a major role in the NC algorithms for SYLFIND and SYLCONJ, as they do in many of the fundamental algorithms given in [6]. If we know H/K is semisimple, we define an NC-effective representation domain for H/K and indicate how to construct one. Later, in chapters III and IV, we will use these domains in the Sylow algorithms. Since the methods for working with abelian semisimple groups differ from those for handling nonabelian semisimple groups, we treat them separately in the two following subsections.

Abelian Semisimple Quotient Groups

Let p' denote the set of primes other than p.

Definition II.36 *An* abelian semisimple group *is a direct product of elementary abelian groups for various primes. If π is a set of primes, an* abelian semisimple π-group *is an abelian semisimple group whose order is a product of powers of primes in π. We view an abelian semisimple group G as a direct product of vector spaces over different prime fields. For convenience, we refer to such a group as a* generalized vector space.

Definition II.37 *A* generalized basis *for a generalized vector space $H = P_1 \times \cdots \times P_l$ (where P_i is an elementary abelian p_i-group and $p_i \neq p_j$ for $i \neq j$) is the union $\cup_i \mathcal{B}_i$ where $\mathcal{B}_i$ is a basis for P_i. Similarly, if the quotient H/K is abelian semisimple, a subset $\mathcal{B} \subset H$ is called a* generalized basis for H modulo K *if $\{Kb \mid b \in \mathcal{B}\}$ is a generalized basis for H/K.*

Lemma II.38 *Given groups $K \lhd H = \langle T \rangle$ with H/K abelian semisimple, a generalized basis $\mathcal{B}$ for H modulo K can be found in NC.*

Proof: Let $p_1, \ldots, p_l$ be the prime factors of $|H/K|$ (Problem II.15). Let $\pi = \prod_{i=1}^{l} p_i$, let $\pi_i = \pi/p_i$, and let $C_i = \{t^{\pi_i} \mid t \in T\}$ for each $i = 1, \ldots, l$. Let $P_i = \langle C_i, K \rangle$. Then $H/K = P_1/K \times \cdots \times P_l/K$ where each P_i/K is an elementary abelian p_i-group for $i = 1, \ldots, l$. To obtain a basis $\mathcal{B}_i$ of P_i modulo K for all $i = 1, \ldots, l$ in parallel, suppose $C_i = \{t_1, \ldots, t_m\}$, and let $\mathcal{B}_i = \{t_j \in C_i \mid t_j \notin \langle t_1, \ldots, t_{j-1}, K \rangle\}$. These membership tests are each in NC (Problem II.1) and may be performed in parallel. $\mathcal{B} = \cup_{i=1}^{l} \mathcal{B}_i$ is a generalized basis for H modulo K. □

Definition II.39 *If H/K is an abelian semisimple group, a* generalized vector space representation *for H/K is a pair (V, ϕ) consisting of a generalized vector space V together with an epimorphism $\phi : H \to V$ with kernel K. A generalized vector space representation (V, ϕ) for H/K is* NC-effective *if ϕ is an* NC-computable function, *i.e., there is an NC procedure that can compute $\phi(h)$ for any given $h \in H$.*

We use F_q^d to denote the d-dimensional vector space over F_q, a field of q elements, and $\{e_1, \ldots, e_d\}$ to denote the standard basis.

Lemma II.40 *Given groups $K \lhd H$ where H/K is abelian semisimple, an NC-effective generalized vector space representation (V, ϕ) for H/K can be found in NC. Moreover, for any $v \in V$, a preimage of v in H, i.e., an element $h \in H$ for which $\phi(h) = v$, can be found in NC.*

Proof: Let $\mathcal{B} = \cup_{i=1}^{l} \mathcal{B}_i$ be a generalized basis for H modulo K (Lemma II.38), where $\mathcal{B}_i = \{b_{i1}, \ldots, b_{id_i}\}$. Let $P_i = \langle \mathcal{B}_i, K \rangle$, so $\{Kb \mid b \in \mathcal{B}_i\}$ is a basis for the vector space P_i/K; let p_i and d_i be the characteristic and dimension, respectively, of

this vector space. Then $H/K = P_1/K \times \cdots \times P_l/K$ and $P_i/K \cong V_i$, where $V_i = F_{p_i}^{d_i}$, for $i = 1, \ldots, l$. Let $V = V_1 \times \cdots \times V_l$. Let $\{e_{i1}, \ldots, e_{id_i}\}$ be the standard basis of V_i. We specify an NC-computable function $\phi : H \to V$ with kernel K as follows. Let h be an element of H. For all b_{ij}, $1 \leq i \leq l$, $1 \leq j \leq d_i$, in parallel: test, for all a, $0 \leq a \leq p_i - 1$, in parallel, whether $h^{-1} \cdot b_{ij}^a \in \langle \mathcal{B} \setminus \{b_{ij}\}, K \rangle$ (tested using Problem II.1) and let a_{ij} be the unique a satisfying this condition. Then $h \equiv \prod_{i,j} b_{ij}^{a_{ij}} \pmod{K}$. Define $\phi(h) = \sum_{ij} a_{ij} e_{ij}$. Hence the map $\phi : H \to V$ is an NC-computable function with kernel K. The pair (V, ϕ) is an NC-effective representation for H/K.

Furthermore, let v be any element of V. If we express v as $v = \sum_{ij} a_{ij} e_{ij} \in V$, then the element $h = \prod_{i,j} b_{ij}^{a_{ij}} \in H$ satisfies $\phi(h) = v$. Hence we may compute preimages in H of elements of V in NC. □

We also require the ability to perform basic operations of linear algebra within generalized vector spaces in NC.

Definition II.41 *A* generalized linear transformation *of a generalized vector space $V = V_1 \times \cdots \times V_d$ is a direct product of linear transformations $L = L_1 \times \cdots \times L_d$, where each L_i is a linear transformation of V_i. Hence $Lv = (L_1 v_1, \cdots, L_d v_d)$, where $v = (v_1, \cdots, v_d) \in V$.*

Lemma II.42 *Given a generalized linear transformation $L = L_1 \times \cdots \times L_d$ of a generalized vector space $V = V_1 \times \cdots \times V_d$ and an element $b = (b_1, \ldots, b_d) \in V$, a solution of $Lx = b$ can be found in NC, if one exists.*

Proof: A solution X_i to the equation $L_i x_i = b_i$ may be found in NC using [27], if one exists. Then the element $(X_1, \cdots, X_d) \in V$ is a solution we seek. □

Definition II.43 *A set of equations of the form described in Lemma II.42 is called a system of* generalized linear equations.

Nonabelian Semisimple Quotient Groups

Definition II.44 *A* nonabelian semisimple group *is the direct product of nonabelian simple groups. A* nonabelian p-semisimple group *is the direct product of nonabelian simple groups each of which has order divisible by p. A* nonabelian p'-semisimple group *is the direct product of nonabelian simple groups each simple factor of which has order relatively prime to p.*

Note that the simple factors of a nonabelian semisimple group are uniquely determined.

Definition II.45 *Suppose $K \lhd H \leq Sym(\Omega)$. If H/K is an nonabelian semisimple group, a* semisimple permutation representation *for H/K is a pair (S, ϕ) consisting of a semisimple permutation group $S = S_1 \times \cdots \times S_d \leq Sym(\Delta_1) \times \cdots \times Sym(\Delta_d)$ where each S_i is simple, together with an epimorphism $\phi : H \rightarrow S$ with kernel K. A semisimple permutation representation (S, ϕ) for H/K is* NC-effective *if ϕ is an* NC-computable function, *i.e., there is an NC procedure that can compute $\phi(h)$ for any given $h \in H$.*

Lemma II.46 *Given groups $K \lhd H$ where H/K is nonabelian semisimple, an NC-effective semisimple permutation representation (S, ϕ) for H/K can be found in NC. Moreover, for any $s \in S$, a preimage of s in H, i.e., an element $s \in H$ for which $\phi(h) = s$, can be found in NC.*

Proof: Let $\mathcal{M} = \{M_1, \ldots, M_r\}$ be the set of maximal normal subgroups of H that contain K. By Lemma 7.4 and Theorem 8.3 of [6], one can find $\mathcal{M}$. For each such $M_i \in \mathcal{M}$ in parallel, find a permutation representation $\phi_i : H \rightarrow \mathrm{Sym}(\Delta_i)$ with kernel M_i Then $K = \cap M_i$ and H/K has a faithful permutation representation $H \rightarrow \Delta_1 \cup \cdots \cup \Delta_r$ given by $h \mapsto (\phi_1(h), \ldots, \phi_r(h))$. □

Constructing Semisimple Quotients

We give techniques for computing a subgroup K of a group H (Definition II.49) for which H/K is abelian semisimple or nonabelian semisimple (see Definitions II.36 and II.44). Lemmas II.40 and II.46 then apply to construct a representation domain for H/K.

Definition II.47 *Let $\mathcal{L}_{p'}$ denote the class of groups each of whose nonabelian composition factors has order relatively prime to p.*

Definition II.48 *Fix a prime p. We adopt the following designations for classes of simple groups closed under isomorphism:*

$$\begin{aligned} \mathcal{T}_1 &= \textit{simple } p\textit{-groups,} \\ \mathcal{T}_2 &= \textit{simple abelian groups,} \\ \mathcal{T}_3 &= \textit{simple } \mathcal{L}_{p'}\textit{-groups, and} \\ \mathcal{T}_4 &= \textit{all simple groups.} \end{aligned}$$

We adopt the following designations for later convience:

$$\begin{aligned} \mathcal{A} &= \mathcal{T}_2 \\ \mathcal{N} &= \textit{nonabelian simple groups.} \end{aligned}$$

If $\mathcal{T}$ is one of the above classes of simple groups, a group G is a $\mathcal{T}$-semisimple *if it is semisimple and all of its simple factors are in the class $\mathcal{T}$; G is a* $\mathcal{T}$-group *if all its composition factors are in the class $\mathcal{T}$.*

Definition II.49 *For a class of simple groups $\mathcal{T}$ given in Definition II.48, $R_{\mathcal{T}}(G)$ denotes the smallest normal subgroup $H \trianglelefteq G$ for which G/H is $\mathcal{T}$-semisimple. In*

addition, we use the following designations as useful aliases:

$$\begin{aligned} R_p(G) &= R_{\mathcal{T}_1}(G) \\ R_{\mathcal{A}}(G) &= R_{\mathcal{T}_2}(G) \\ R_{\mathcal{C}_{p'}}(G) &= R_{\mathcal{T}_3}(G) \\ R(G) &= R_{\mathcal{T}_4}(G). \end{aligned}$$

For a class of simple groups $\mathcal{T}$ as given in Definition II.48, $R_{\mathcal{T}}(G)$ is well defined since if G/H and G/K are both $\mathcal{T}$-semisimple groups, then so is $G/(H \cap K)$, since $g \mapsto (gH, gK)$ gives an injective map from $G/(H \cap K)$ into $G/H \times G/K$ that is onto each factor.

Note that $R(G) < G$ for any $G \neq 1$.

Definition II.50 *For $\mathcal{T}$ as in Definition II.48, let $O^{\mathcal{T}}(G)$ be the smallest normal subgroup $H \trianglelefteq G$ such that all the composition factors of G/H are in $\mathcal{T}$. Note that $O^{\mathcal{T}_4}(G) = 1$ and $O^{\mathcal{T}_2}(G) = O^{\mathcal{A}}(G)$ is the last term in the derived series of G.*

For $\mathcal{T}$ as in Definition II.48, $O^{\mathcal{T}}(G)$ is well defined since if H and K are normal in G and G/H and G/K are both $\mathcal{T}$-groups, then $G/(H \cap K)$ is also a $\mathcal{T}$-group.

Definition II.51 *For any class $\mathcal{T}$ in Definition II.48, let $R_{\mathcal{T}}^0(G) = G$ and $R_{\mathcal{T}}^{j+1}(G) = R_{\mathcal{T}}(R_{\mathcal{T}}^j(G))$. Let $d_{\mathcal{T}}(G)$ denote the smallest integer r for which $R_{\mathcal{T}}^r(G) = R_{\mathcal{T}}^{r+1}(G)$. For a fixed $j \in \{2,3,4\}$ let $d_{\mathcal{T}_j,\mathcal{T}_{j-1}}(G)$ denote the smallest integer s for which $(R_{\mathcal{T}_j}O^{\mathcal{T}_{j-1}})^s(G) = (R_{\mathcal{T}_j}O^{\mathcal{T}_{j-1}})^{s+1}(G)$. Where convenient, we will use the aliases given in Definition II.49, for example, we write $d_p(G)$ in place of $d_{\mathcal{T}_1}(G)$, $d_{\mathcal{A},p}(G)$ in place of $d_{\mathcal{T}_2,\mathcal{T}_1}(G)$, and so forth.*

Lemma II.52 *Let $r = d_{\mathcal{T}}(G)$. Then $O^{\mathcal{T}}(G) = R_{\mathcal{T}}^r(G)$.*

Proof: Let $R = R_{\mathcal{T}}^{r}(G)$. Then $O^{\mathcal{T}}(G) \leq R$ since all the composition factors of G/R are in $\mathcal{T}$. But if $O^{\mathcal{T}}(G) < R$, then $R_{\mathcal{T}}(R) < R$, contrary to the choice of R. The lemma follows. □

Before describing algorithms for computing $R_{\mathcal{T}}(G)$ and $O^{\mathcal{T}}(G)$ for each class $\mathcal{T}$ of simple groups described in Definition II.48, we turn our attention to semisimple towers. Our purpose in doing so is two-fold:

1. to show the $d_{\mathcal{T}}(G)$ is polylogarithmic in the degree of G (see Lemma II.59), so that $O^{\mathcal{T}}(G)$ can be computed in NC (see Lemma II.62), and

2. to show that the towers

$$G \rhd R_{\mathcal{T}_i}O^{\mathcal{T}_{i-1}}(G) \rhd (R_{\mathcal{T}_i}O^{\mathcal{T}_{i-1}})^2(G) \rhd \cdots \rhd (R_{\mathcal{T}_i}O^{\mathcal{T}_{i-1}})^r(G) = O^{\mathcal{T}_i}(G)$$

(for $i = 2, 3, 4$), have length polylogarithmic in the degree of G, i.e., that $d_{\mathcal{T}_j,\mathcal{T}_{j-1}}(G)$ (Definition II.51) is polylogarithmic in the degree of G (Lemma II.61), a fact which will be used to prove the polylogarithmic time complexity of the Sylow algorithms in Chapters III and IV.

Semisimple Towers and Their Lengths

Definition II.53 *Let $N \trianglelefteq G \leq Sym(\Omega)$. A* semisimple tower for G modulo N *is a tower of subgroups $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_r = N$ where G_i/G_{i+1} is semisimple and $G_i \trianglelefteq G$ for $i = 0, \ldots, r-1$. The* length *of this tower is r. If $N = 1$, this tower is called a* semisimple tower for G.

Note that if $O^{\mathcal{T}}(G) = 1$, each quotient G_i/G_{i+1} of successive groups in a semisimple tower for G is a $\mathcal{T}$-semisimple group.

Fact II.54 *If $G \leq Sym(\Omega)$, then there exists a semisimple tower for G whose length is polylogarithmic in $|\Omega|$ [24, 6].*

Lemma II.55 *$R_{\mathcal{T}}(G)$ is a characteristic subgroup of G where $\mathcal{T}$ is any class of semisimple groups listed in Definition II.48. Moreover, $R^i_{\mathcal{T}}(G)$ is a characteristic subgroup of G for each $i = 2, \ldots, d_{\mathcal{T}}(G)$.*

Proof: Let $\mathcal{M}_{\mathcal{T}}$ be the set of all normal subgroups N of G for which G/N is a $\mathcal{T}$-semisimple group. Any automorphism of G acts on $\mathcal{M}_{\mathcal{T}}$, and so preserves the intersection of the subgroups in $\mathcal{M}_{\mathcal{T}}$, which is equal to $R_{\mathcal{T}}(G)$. Hence $R_{\mathcal{T}}(G)$ char G.

The second assertion of the Lemma follows from the fact that a characteristic subgroup of a characteristic subgroup of G is characteristic in G. □

Lemma II.56 *If $H \trianglelefteq G$, then $R_{\mathcal{T}}(H) \trianglelefteq R_{\mathcal{T}}(G)$ where $\mathcal{T}$ is any class of simple groups defined in Definition II.48.*

Proof: Let $R = R_{\mathcal{T}}(G)$. R is the smallest normal subgroup of G for which G/R is $\mathcal{T}$-semisimple. Since a normal subgroup of a $\mathcal{T}$-semisimple group is also $\mathcal{T}$-semisimple, we conclude that $HR/R \cong H/(H \cap R)$ is $\mathcal{T}$-semisimple. This implies $R_{\mathcal{T}}(H) \leq H \cap R \leq R = R_{\mathcal{T}}(G)$. Since $R_{\mathcal{T}}(H)$ char $H \trianglelefteq G$, it follows that $R_{\mathcal{T}}(H) \trianglelefteq G$, and so $R_{\mathcal{T}}(H) \trianglelefteq R_{\mathcal{T}}(G)$. □

Lemma II.57 *The tower $G \rhd R(G) \rhd R^2(G) \rhd \cdots \rhd R^r(G) = 1$ of a group G has length r less than or equal to the length of any semisimple tower of G. In particular, if $G \leq Sym(\Omega)$, then the residual tower has length polylogarithmic in $|\Omega|$.*

Proof: Let $G = G_0 \rhd G_1 \rhd \cdots \rhd G_s = 1$ be a semisimple tower of G. It suffices to show $R^i(G) \trianglelefteq G_i$ for all i. Since G/G_1 is semisimple, $R(G) \trianglelefteq G_1$ by the definition of $R(G)$. Inductively assuming $R^i(G) \trianglelefteq G_i$, we have

$$\begin{aligned} R^{i+1}(G) &= R(R^i(G)) \\ &\trianglelefteq R(G_i) && \text{by inductive hypothesis and Lemma II.56} \\ &\leq G_{i+1} && \text{since } G_i/G_{i+1} \text{ is semisimple.} \end{aligned}$$

Also $R^{i+1}(G)$ is characteristic in G (by Lemma II.55), so in particular $R^{i+1}(G) \trianglelefteq G_{i+1}$. If $G \leq \mathrm{Sym}(\Omega)$, then the length r is polylogarithmic in $|\Omega|$ by Fact II.54. □

The following lemmas permit us to prove Proposition II.61, which plays an essential role in the time complexity analyses of algorithms presented in Chapters III and IV.

Lemma II.58 *Let $N \lhd G \leq Sym(\Omega)$. There exists a semisimple tower for G modulo N (Definition II.53) of length polylogarithmic in $|\Omega|$.*

Proof: Let $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = 1$ be a polylogarithmic length semisimple tower (see Fact II.54). Note that

$$\frac{G_iN}{G_{i+1}N} = \frac{G_i(G_{i+1}N)}{G_{i+1}N} \cong \frac{G_i}{G_i \cap (G_{i+1}N)} \cong \frac{G_i/G_{i+1}}{(G_i \cap (G_{i+1}N))/G_{i+1}}$$

is a quotient of the semisimple group G_i/G_{i+1}, so is semisimple. Hence the tower $G = G_0 \trianglerighteq G_1N \trianglerighteq G_2N \trianglerighteq \cdots \trianglerighteq G_rN = N$ is a polylogarithmic length semisimple tower for G modulo N. □

An immediate consequence of this lemma is the following:

Corollary II.59 *Let $G \leq Sym(\Omega)$ and let $\mathcal{T}$ be any of the classes of simple groups given in Definition II.48. There is a semisimple tower for G modulo $O^{\mathcal{T}}(G)$ of length polylogarithmic in $|\Omega|$ in which the quotients G_i/G_{i+1} of successive groups in the tower are $\mathcal{T}$-semisimple groups. Namely, the tower $G \rhd R_T(G) \rhd R_T^2(G) \rhd \cdots \rhd R_T^r(G) = O^{\mathcal{T}}(G)$ is such a tower.*

We next note the following

Lemma II.60 *If $H \trianglelefteq G$, then $R_{\mathcal{T}_i}O^{\mathcal{T}_{i-1}}(H) \trianglelefteq R_{\mathcal{T}_i}(G)$, for $i = 2, 3, 4$.*

Proof: $O^{\mathcal{T}_{i-1}}(H) \trianglelefteq G$, since $O^{\mathcal{T}_{i-1}}(H) \operatorname{char} H \trianglelefteq G$ by Lemma II.55. The result follows from Lemma II.56. □

Proposition II.61 *If $G \leq Sym(\Omega)$, the tower*

$$G > (R_{\mathcal{T}_i}O^{\mathcal{T}_{i-1}})(G) > (R_{\mathcal{T}_i}O^{\mathcal{T}_{i-1}})^2(G) > \cdots > (R_{\mathcal{T}_i}O^{\mathcal{T}_{i-1}})^{r_i}(G) = O^{\mathcal{T}_i}(G)$$

has polylogarithmic length, for $i = 2, 3, 4$.

Proof: Inductively, assume $H = (R_{\mathcal{T}_i}O^{\mathcal{T}_{i-1}})^j(G) \trianglelefteq R_{\mathcal{T}_i}^j(G)$. Then by Lemma II.60,

$$R_{\mathcal{T}_i}O^{\mathcal{T}_{i-1}}(H) = (R_{\mathcal{T}_i}O^{\mathcal{T}_{i-1}})^{j+1}(G) \trianglelefteq R_{\mathcal{T}_i}^{j+1}(G).$$

The result now follows, since the length of the tower $G \rhd R_T(G) \rhd R_T^2(G) \rhd \cdots \rhd R_T^r(G) = O^{\mathcal{T}}(G)$ is polylogarithmic in $|\Omega|$ (Lemma II.59). □

Computing $R_{\mathcal{T}}(G)$ and $O^{\mathcal{T}}(G)$

Lemma II.62 *Given a permutation group $G = \langle S \rangle \leq Sym(\Omega)$ and a prime p, the subgroups groups $R_{\mathcal{T}_1} = R_p(G)$, $O^{\mathcal{T}_1}(G) = O^p(G)$, $R_{\mathcal{T}_2}(G) = R_A(G)$, $O^{\mathcal{T}_2}(G) =$*

$O^{\mathcal{A}}(G)$, $R_{\mathcal{N}}(G)$, $R_{\mathcal{T}_3}(G) = R_{\mathcal{L}_{p'}}(G)$, and $O^{\mathcal{T}_3}(G) = O^{\mathcal{L}_{p'}}(G)$ can each be computed in NC.

Proof: $R_p(G) = \langle G', \{s^p \mid s \in \mathcal{S}\}\rangle$ and $R_{\mathcal{A}}(G) = \langle G', \{s^q \mid s \in \mathcal{S}\}\rangle$ where q is the product of the primes that divide $|G|$, so each of these groups may be found in NC (see Problem II.16). Computing $R_{\mathcal{N}}(G)$ is shown to be in NC in [6], Lemma 7.4 and Theorem 8.3. To find $R_{\mathcal{L}_{p'}}(G)$, first compute $N = R_{\mathcal{N}}(G)$ and construct a representation (S, ϕ) for G/N (see Lemma II.46). Suppose $\phi(G) = S_1 \times \cdots \times S_d$. Use Problem II.15 to determine the order of each S_i and let $\mathcal{U} = \{S_i \mid p \text{ divides } |S_i|\}$. $R_{\mathcal{L}_{p'}}(G) = \text{LIFT}(U)$ where $U = \prod_{S \in \mathcal{U}} S$. (See Remark II.3.)

Since $O^{\mathcal{T}}(G) = R^r_{\mathcal{T}}(G)$ where $r = d_{\mathcal{T}}(G)$, $O^{\mathcal{T}}(G)$ may be found by computing $R^i_{\mathcal{T}}(G)$ for $i = 1, \ldots, r$ sequentially, where $\mathcal{T}$ is any of $\mathcal{T}_1, \mathcal{T}_2$, or $\mathcal{T}_3$. This is an NC computation since r is polylogarithmic in $|\Omega|$ by Corollary II.59. □

CHAPTER III

THE SYLOW ALGORITHMS FOR SOLVABLE GROUPS

A Base Case and the Frattini Argument

Finding and conjugating Sylow subgroups of solvable groups give rise to two particular subproblems: (1) finding a subgroup P of a group H where $L \lhd K \lhd H \lhd G$ such that P/L is a Sylow p-subgroup of H/L, where K/L is an elementary abelian p'-group and H/K is an elementary abelian p-group, and (2) finding a subgroup $G^* \leq G$ that normalizes such a group P and contains a Sylow p-subgroup of G. The latter problem is an algorithmic form of the "Frattini argument" ([30, p. 61]). This section describes procedures BASECASE1-SOLVABLE and FRATTINI-SOLVABLE for these problems.

The essential technique in both these procedures is to transform a group theoretic condition into the problem of solving systems of generalized linear equations, for which there exist NC algorithms (Lemma II.42). Linear transformations arise since L and K are both normal subgroups of G, K/L is abelian semisimple, and an NC-effective generalized vector space representation (V, ϕ) for K/L is constructible. Then each element $g \in G$ induces a generalized linear transformation T_g on V, given by $\phi(x) \mapsto \phi(g^{-1}xg)$.

For later use in Chapter IV, the algorithms given here handle solvable quotients of a permutation group. For example, if we are given a permutation group G and a normal subgroup N for which G/N is solvable, then SYLFIND-SOLVABLE finds a

subgroup P of G for which PN/N is a Sylow p-subgroup of G/N.

Problem III.1 BASECASE1-SOLVABLE(H, K, L)

GIVEN: $L \trianglelefteq K \trianglelefteq H \leq \mathrm{Sym}(\Omega)$, $L \trianglelefteq H$, H/K is an elementary abelian p-group, and K/L is an abelian semisimple p'-group,

FIND: a group P for which $L \leq P \leq H$ and P/L is a Sylow p-subgroup of H/L.

Proposition III.2 *BASECASE1-SOLVABLE is in NC.*

Proof: If P is such a group then $H = PK$ and, since $P \cap K = L$, $H/K \cong P/L$. In particular, P/L is elementary abelian. Suppose $H = \langle \mathcal{S} \rangle$. Then for each $s \in \mathcal{S}$, there exists $x_s \in K$ such that $sx_s \in P$. Hence,

1. for all $s \in \mathcal{S}$, $(sx_s)^p \in L$
2. for all $s, t \in \mathcal{S}$, $[sx_s, tx_t] \in L$.

Conversely, if $\{x_s \mid s \in \mathcal{S}\} \subseteq K$ satisfies (i) and (ii), then we can take $P = \langle \{sx_s \mid s \in \mathcal{S}\} \rangle$.

Let $\phi : K \to V$ induce a generalized vector space representation of K/L (see Lemma II.40) and for $g \in G$, let T_g be defined as above. Since $[sx_s, tx_t] = x_s^{-1}(x_t^{-1})^s[s,t]x_s^t x_t$,

$$\phi([sx_s, tx_t]) = -\phi(x_s) - T_s\phi(x_t) + \phi([s,t]) + T_t\phi(x_s) + \phi(x_t).$$

Thus $[sx_s, tx_t] \in L$ if and only if each pair of elements in $\{\phi(x_s) \mid s \in \mathcal{S}\}$ satisfies the following system of $|\mathcal{S}|^2$ generalized linear equations:

$$\forall\, s, t \in \mathcal{S},\ (T_t - I)X_s - (T_s - I)X_t = -\phi([s,t]).$$

Hence, a set $\{x_s \mid s \in \mathcal{S}\}$ satisfying (ii) is obtained by solving this system for $\{X_s\} \subseteq V$ (see Lemma II.42) and letting x_s be a preimage of X_s in K (see Lemma II.40).

We can modify this set to satisfy (i), while maintaining (ii), by replacing each x_s by $s^{-1}(sx_s)^m$ where m is chosen so that $|K/L|$ divides m and $m \equiv 1 \pmod{p}$. □

Recall the *Frattini argument* (see [30, p. 61]): if $P \leq K \trianglelefteq G$ with P a Sylow p-subgroup of K then $G = N_G(P)K$, where $N_G(P)$ is the normalizer of P in G.

Problem III.3 FRATTINI-SOLVABLE(G, H, K, L, P)

GIVEN: $L \lhd K \lhd H \trianglelefteq G \leq \mathrm{Sym}(\Omega)$, each of L, K is also normal in G, K/L is an abelian semisimple p'-group, H/K is a p-group, and P/L is a Sylow p-subgroup of H/L,

FIND: a subgroup $G^* \leq G$ that normalizes P and contains P for which G^*/L contains a Sylow p-subgroup of G/L.

Proposition III.4 *FRATTINI-SOLVABLE is in NC.*

Proof: We are given $G = \langle \mathcal{S} \rangle$, $P = \langle \mathcal{T} \rangle$. By the Frattini argument, for any $s \in \mathcal{S}$ there exists $x_s \in K$ such that $sx_s \in N_G(P)$. For any such collection, $\{x_s \mid s \in \mathcal{S}\}$, we can take $G^* = \langle P, \{sx_s \mid s \in \mathcal{S}\} \rangle$; to see that G^*/L contains a Sylow p-subgroup of G/L, we observe that $|G^*K/L| = |G/L|$, but the p-part of $|G^*K/L|$ equals the p-part of $|G^*/L|$ since $(|K/L|, p) = 1$.

To find such x_s (in parallel for each $s \in \mathcal{S}$) it suffices to ensure that $t^{sx_s} \in P$ for each $t \in \mathcal{T}$. For each $t \in \mathcal{T}$, write $t^s = a_t k_t$, with $a_t \in P, k_t \in K$ (see Problem II.17). The required x_s must therefore satisfy $a_t^{x_s} k_t \in P$. But, $a_t^{x_s} k_t = a_t [a_t, x_s] k_t$ and

$[a_t, x_s]k_t \in K$. Since $P \cap K \leq L$, the condition on x_s is equivalent to $[a_t, x_s]k_t \in L$, or, if $\phi : K \to V$ induces a vector-space representation of K/L, to

$$\phi(x_s) - \phi(x_s^{a_t}) + \phi(k_t) = 0.$$

Therefore, $\phi(x_s)$ is a solution to the system of $|\mathcal{T}|$ generalized linear equations

$$\forall t \in \mathcal{T},\ (I - T_{a_t})X + \phi(k_t) = 0,$$

where T_{a_t} is defined just before Problem III.1. Hence, x_s is obtained by solving this system for $X \in V$ (see Lemma II.42) and letting x_s be a preimage of X in K (see Lemma II.40). □

SYLFIND-SOLVABLE

Before giving a procedure for SYLFIND-SOLVABLE, we describe another special case.

Problem III.5 BASECASE2-SOLVABLE(G, K, L, p)

GIVEN: $L \trianglelefteq K \trianglelefteq G \leq \mathrm{Sym}(\Omega)$, where $L \lhd G$, G/K is a p-group, and K/L is an abelian semisimple p'-group,

FIND: a subgroup $P \leq G$ containing L for which P/L is a Sylow p-subgroup of G/L.

Proposition III.6 *BASECASE2-SOLVABLE is in NC.*

Proof: Let $G_1 = R_p(G)L$ (see Lemma II.62). Note that $K \leq G_1$. If $G_1 = G$, then $G = K$, and $|G/L| = |K/L|$ is relatively prime to p so G/L has no nontrivial Sylow p-subgroup. In this case, return $P = L$.

Otherwise, recursively find P_1 = BASECASE2-SOLVABLE(G_1, K, L). The group G^* = FRATTINI-SOLVABLE(G, G_1, K, L, P_1) normalizes P_1 and contains a Sylow p-subgroup of G. We seek a group P for which P/P_1 is a Sylow p-subgroup of G^*/P_1. Find the group $U = R_p(G^*)L$ (see Lemma II.62) . By definition, G^*/U is an elementary abelian p-group. Also note that U/P_1 is an elementary abelian p'-group since, letting $W = U \cap K$, we have $U/P_1 = P_1W/P_1 \cong W/(P_1 \cap W) = W/L \leq K/L$, which is an elementary abelian p'-group. Hence BASECASE1-SOLVABLE (see Problem III.1) applies, and P = BASECASE1-SOLVABLE(G^*, U, P_1) is the group we seek.

In each recursive call, $L \leq G_1 < G$, so the number of recursive calls is bounded by $d_p(G/L)$. Since $d_p(G/L) \leq d_p(G)$ (see Definition II.51), which is polylogarithmic in $|\Omega|$ by Corollary II.59, the algorithm for BASECASE2 is in NC. □

Problem III.7 SYLFIND-SOLVABLE(G, p)

GIVEN: a group $G \leq \mathrm{Sym}(\Omega)$ and a prime p that divides $|G|$,

FIND: a subgroup P of G for which $P \geq R$ and P/R is a Sylow p-subgroup of G/R, where $R = O^{\mathcal{A}}(G)$.

Theorem III.8 *SYLFIND-SOLVABLE is in NC.*

Proof: Let $K = O^p(G)$ and $L = R_{\mathcal{A}}(K)$ (see Lemma II.62). If $L = K$ (tested using Problem II.1) then $R_p(K) = R_{\mathcal{A}}(K)$, which implies $K = R$, so return G. Otherwise let P = BASECASE2-SOLVABLE(G, K, L, p) and recurse by returning SYLFIND-SOLVABLE(P, p).

To analyze the running time of SYLFIND-SOLVABLE, note that $L = R_{\mathcal{A}}O^p(G)$ so the group P that is passed in the recursive call satisfies $R_{\mathcal{A}}O^p(P) = R_{\mathcal{A}}O^p(L) = (R_{\mathcal{A}}O^p)^2(G)$. Hence the depth of the recursion is logarithmic by Proposition II.61.

Moreover, the procedures BASECASE1-SOLVABLE and FRATTINI-SOLVABLE are in NC. Hence SYLFIND-SOLVABLE is in NC. □

SYLCONJ-SOLVABLE and SYLEMBED-SOLVABLE

We now describe a procedure SYLCONJ-EMBED-SOLVABLE which can be used for conjugating Sylow p-subgroups and embedding a p-subgroup into a Sylow p-subgroup. Specifically, we obtain SYLCONJ-SOLVABLE as a special case of SYLCONJ-EMBED-SOLVABLE by letting P_1 and P_2 be Sylow p-subgroups of G. Similarly, SYLEMBED-SOLVABLE can be implemented by first letting $P_2 =$ SYLFIND-SOLVABLE(G, p), then setting

$$g = \text{SYLCONJ-EMBED-SOLVABLE}(G, P_1, P_2)$$

and returning $P_2^{g^{-1}}$, a Sylow p-subgroup of G containing P_1.

Problem III.9 SYLCONJ-EMBED-SOLVABLE(G, P_1, P_2)

GIVEN: a group $G \leq \text{Sym}(\Omega)$, a p-subgroup P_1 of G, and a Sylow p-subgroup P_2 of G,

FIND: an element $x \in G$ for which $P_1^x R/R \leq P_2 R/R$ where $R = O^{\mathcal{A}}(G)$.

Theorem III.10 *SYLCONJ-EMBED-SOLVABLE is in NC.*

Proof: Find $H = O^p(G)$ (see Lemma II.62), so that $P_1 H/H \leq G/H = P_2 H/H$. Find $K = R_{\mathcal{A}}(H)$ (see Lemma II.62). If $K = H$, then $H = R$ and $P_1 \leq P_2 = G$. In this case, return $x = 1$.

We may assume $K < H$. We first show that we can find $x \in H$ such that $P_1^x \leq P_2 K$. Suppose $P_1 = \langle S \rangle$. Since $G = P_2 H$, for each $s \in S$, we can factor

$s = bh$ with $b \in P_2, h \in H$ (see Problem II.17). For $x \in H$, $s^x \in P_2K$ if and only if $b^{-1}s^x = (x^{-1})^b x h^x \in P_2K$; since $h^x = h[h,x] \in hK$, this happens if and only if $(x^{-1})^b x h \in P_2K \cap H \leq K$. Thus, if $\phi : H \to V$ induces a generalized vector space representation of H/K (see Lemma II.40), then $s^x \in P_2K$ if and only if $\phi(x)$ is a solution to the system of $|\mathcal{S}|$ linear equations

$$\forall s \in \mathcal{S},\ (I - T_{b_s})X + \phi(h_s) = 0,$$

where $s = b_s h_s$ with $b_s \in P_2, h_s \in H$, and where T_{b_s} is defined just before Problem III.1.

Hence, x is obtained by solving this system for $X \in V$ and taking a preimage of X in H (see Lemma II.40).

Let $G^* = \langle P_1^x, P_2 \rangle$ and recursively solve SYLCONJ-EMBED(G^*, P_1^x, P_2) for $y \in G^*$ such that $(P_1^x)^y \leq P_2$. Return the element xy.

To analyze the running time of SYLCONJ-EMBED-SOLVABLE, note that the group K computed in SYLCONJ-EMBED-SOLVABLE is equal to $R_A O^p(G)$. Hence the group G^* that is passed in the recursive call satifies $R_A O^p(G^*) = R_A O^p(K) = (R_A O^p)^2(G)$. Thus, the depth of the recursion is logarithmic by Proposition II.61. Therefore, SYLCONJ-EMBED-SOLVABLE is in NC. □

CHAPTER IV

REDUCTION TO THE SIMPLE GROUP CASE

A Frattini Argument

Problem IV.1 FRATTINI(G, K, L, q)

GIVEN: $L \lhd K \lhd G = \langle S \rangle \leq \mathrm{Sym}(\Omega)$, G/K a p-group, K/L a nonabelian semisimple group such that either p divides the order of each simple factor of K/L and $q = p$, or p does not divide $|K/L|$ and $q = 2$,

FIND: a group $G^* \leq G$ for which G^* contains a Sylow p-subgroup of G and G^*/L normalizes a Sylow q-subgroup of K/L.

Theorem IV.2 *FRATTINI is in NC.*

Proof: Use Lemma II.46 to construct an NC-effective semisimple permutation representation (S, ϕ) for K/L where $\phi : K \to S = S_1 \times \cdots \times S_r$ with kernel L. Each element $g \in G$ induces an automorphism T_g of S via conjugation. For each $i = 1, \ldots, r$ in parallel, let $Q_i = \text{SYLFIND-SIMPLE}(S_i, q)$, $Q = Q_1 \times \cdots \times Q_r$, and $\hat{Q} = \text{LIFT}(Q)$ (Remark II.3). By the Frattini argument, for any $s \in \mathcal{S}$ there exists $x_s \in K$ such that $sx_s \in N_G(\hat{Q})$. To find such x_s (in parallel for each $s \in \mathcal{S}$), for each $i = 1, \ldots, r$ in parallel, let $s_j = \text{SYLCONJ-SIMPLE}(S_j, Q_i^s, Q_j)$, where j is such that $T_s(S_i) = S_j$, and let x_s be a preimage in $\hat{Q}$ of $s_1 \cdots s_r \in Q$ (Remark II.3).

For any such collection $\{x_s \mid s \in \mathcal{S}\}$, we can take $G^* = \langle \hat{Q}, \{sx_s \mid s \in \mathcal{S}\} \rangle$; to see that G^* contains a Sylow p-subgroup of G, note that $\hat{Q} \trianglelefteq G^*$ and observe that

$[G^*K : \hat{Q}] = [G : \hat{Q}]$, so the p-part of $[G^*K : \hat{Q}]$ equals the p-part of $[G^* : \hat{Q}]$ since $(p, [K : \hat{Q}]) = 1$. Return G^*. □

SYLFIND

Problem IV.3 SYLFIND-$\mathcal{L}_{p'}(G, p)$

GIVEN: a group $G \leq \mathrm{Sym}(\Omega)$ and a prime p that divides $|G|$,

FIND: a subgroup P of G for which $P \geq R$ and P/R is a Sylow p-subgroup of G/R, where $R = O^{\mathcal{L}'_p}(G)$.

Theorem IV.4 *SYLFIND-$\mathcal{L}_{p'}$ is in NC.*

Proof: Let $K = O^A(G)$ (Lemma II.62) and $P = \mathrm{SYLFIND\text{-}SOLVABLE}(G, p)$ (Problem III.7), so P/K is a Sylow p-subgroup of G/K. Let $L = R_{\mathcal{L}_{p'}}(K)$ (Lemma II.62). If $L = K$ (tested using Problem II.1) then $R_A(K) = R_{\mathcal{L}_{p'}}(K)$, which implies $K = R$, so return P. Otherwise, note that $p \neq 2$ since p does not divide $|K/L|$ (since K/L is nonabelian semisimple, it has even order; see [12]), so the group $G^* = \mathrm{FRATTINI}(P, K, L, 2)$ contains a Sylow p-subgroup of P (Problem IV.1). Also, G^*/L normalizes a Sylow 2-subgroup Q/L of K/L. Q/L is in fact a Sylow 2-subgroup of P/L, since $|P/K|$ is a p-power and $p \neq 2$. Hence G^*/L is contained in the normalizer of a Sylow 2-subgroup of P/L, and is therefore solvable. Hence $O^A(G^*) \leq L$, so P^*L/L is a Sylow p-subgroup of G^*/L where $P^* = \mathrm{SYLFIND\text{-}SOLVABLE}(G^*, p)$. Hence we may recurse by returning SYLFIND-$\mathcal{L}_{p'}(P^*L, p)$.

To analyze the running time of SYLFIND-$\mathcal{L}_{p'}$, note that $L = R_{\mathcal{L}_{p'}}O^{\mathcal{A}}(G)$ so the group P^* that is passed in the recursive call satisfies

$$R_{\mathcal{L}_{p'}}O^{\mathcal{A}}(P^*) = R_{\mathcal{L}_{p'}}O^{\mathcal{A}}(L) = (R_{\mathcal{L}_{p'}}O^{\mathcal{A}})^2(G).$$

Hence the depth of the recursion is logarithmic in $|\Omega|$ by Proposition II.61. Moreover, the procedures SYLFIND-SOLVABLE and FRATTINI are in NC. Hence SYLFIND-$\mathcal{L}_{p'}$ is in NC. □

Problem IV.5 SYLFIND(G, p)

GIVEN: a group $G \leq \mathrm{Sym}(\Omega)$ and a prime p that divides $|G|$,

FIND: a Sylow p-subgroup P of G.

Theorem IV.6 *SYLFIND is in NC.*

Proof: Let $K = O^{\mathcal{L}_{p'}}(G)$ (Lemma II.62) and $P = \text{SYLFIND-}\mathcal{L}_{p'}(G, p)$ (Problem IV.3), so P/K is a Sylow p-subgroup of G/K. Let $L = R_{\mathcal{N}}(K)$ (Lemma II.62). If $L = K$ (tested using Problem II.1) then $R_{\mathcal{L}_{p'}}(K) = R_{\mathcal{N}}(K)$, which implies $K = 1$, so return P. Otherwise, p divides the order of each simple factor of K/L (by choice of K and L), so we may let $G^* = \text{FRATTINI}(P, K, L, p)$ (Problem IV.1). G^* contains a Sylow p-subgroup of P; let $P^* = \text{SYLFIND-}\mathcal{L}_{p'}(G^*, p)$. P^* contains a Sylow p-subgroup of G^*, and hence of G. G^*/L is an $\mathcal{L}_{p'}$-group since it normalizes a Sylow p-subgroup of K/L. Then $O^{\mathcal{L}_{p'}}(G^*) \leq L$, so P^*/L is a Sylow p-subgroup of G^*/L. Hence we may recurse by returning SYLFIND(P^*, p).

To analyze the running time of SYLFIND, note that $L = R_{T_4}O^{T_5}(G)$ so the group P^* that is passed in the recursive call satisfies

$$R_{T_4}O^{T_5}(P^*L) = R_{T_4}O^{T_5}(L) = (R_{T_4}O^{T_5})^2(G).$$

Hence the depth of the recursion is logarithmic in $|\Omega|$ by Proposition II.61. Moreover, the procedures SYLFIND-$\mathcal{L}_{p'}$ and FRATTINI are in NC. Hence SYLFIND is in NC. □

SYLCONJ

We now turn to the reduction of SYLCONJ to the case where G is simple. As in the reduction for SYLFIND, there is a subproblem, SYLCONJ-$\mathcal{L}_{p'}$. We first describe algorithms for two problems used by SYLCONJ-$\mathcal{L}_{p'}$.

Problem IV.7 FIND-NORMALIZED-SYLOW-SEMISIMPLE(G, K, L, S, P)

GIVEN: groups $L \trianglelefteq K \trianglelefteq G \leq \mathrm{Sym}(\Omega)$ where $L \trianglelefteq G$ and K/L is a nonabelian semisimple $\mathcal{L}_{p'}$-group; a Sylow p-subgroup P of G; and an NC-effective semisimple permutation representation (S, ϕ) for K/L where $S = S_1 \times \cdots \times S_d$ and each S_i is simple,

FIND: a direct product $Q = Q_1 \times \cdots \times Q_d$ where $Q_i \leq S_i$ is a Sylow q_i-subgroup of S_i for some q_i that divides $|S_i|$, Q is normalized by P, and $N_S(Q)$ is solvable.

Lemma IV.8 *FIND-NORMALIZED-SYLOW-SEMISIMPLE is in NC.*

Proof: P acts on the set $\Delta = \{S_1, \ldots, S_d\}$ by conjugation. Let $\mathcal{O}$ be the set of orbits of this action. For each P-orbit $O \in \mathcal{O}$, pick some element $S_t \in O$. Find

$P^* = N_P(S_t)$, the stabilizer in P of S_t in the action of P on Δ, find $G^* = N_G(S_t)$, the stabilizer in G of S_t in the action of G on Δ (Problem II.19), and find $K^* = LIFT(S_t)$, the lifting in K of S_t (Remark II.3). Let Q_t = FIND-NORMALIZED-SYLOW-SIMPLE(G^*, K^*, L, S_t, P^*) (Problem IV.9). Find a transversal $\mathcal{C}$ for P^* in P (Problem II.8) and let $Q_O = \langle Q_t^c \mid c \in \mathcal{C} \rangle$. Note that for any two distinct elements $c, d \in \mathcal{C}$, S_t^c and S_t^d are distinct simple factors of S in the P-orbit O. Since $Q_t < S_t$, it follows that $Q_t^c < S_t^c$ and $Q_t^d < S_t^d$. Hence Q_O is in fact the direct product $\prod_{c \in \mathcal{C}} Q_t^c$. Return $Q = \prod_{O \in \mathcal{O}} Q_O$. □

Problem IV.9 FIND-NORMALIZED-SYLOW-SIMPLE(G, K, L, S, P)

GIVEN: groups $L \trianglelefteq K \trianglelefteq G \leq \mathrm{Sym}(\Omega)$ where $L \trianglelefteq G$ and K/L is a nonabelian simple $\mathcal{L}_{p'}$-group; a Sylow p-subgroup P of G; and an NC-effective semisimple permutation representation (S, ϕ) for K/L,

FIND: a Sylow q-subgroup Q of S normalized by P such that $N_S(Q)$ is solvable, for some prime q that divides $|S|$.

The proof that Problem IV.9 is in NC is postponed until Chapter V (Lemma V.112).

Problem IV.10 SYLCONJ-$\mathcal{L}_{p'}(G, P_1, P_2)$

GIVEN: a group $G \leq Sym(\Omega)$ and two Sylow p-subgroups P_1, P_2 of G,

FIND: an element $g \in G$ for which $P_1^g R/R = P_2 R/R$, where $R = O^{\mathcal{L}_{p'}}(G)$.

Theorem IV.11 *SYLCONJ-$\mathcal{L}_{p'}$ is in NC.*

Proof: Let $K = O^{\mathcal{A}}(G)$ (Lemma II.62) and let $x =$ SYLCONJ-EMBED-SOLVABLE (G, P_1, P_2) (Problem III.9), so $P_1^x K/K = P_2 K/K$. We seek an element that con-

jugates P_1^x to P_2 within $G^\# = \langle P_1^x, P_2, K\rangle$; note that $G^\#/K$ is a p-group. Let $L = R_{\mathcal{L}_{p'}}(K)$ (Lemma II.62). If $L = K$ (tested using Problem II.1) then $R_A(K) = R_{\mathcal{L}_{p'}}(K)$, which implies $K = R$, so return the element x.

Otherwise, compute an NC-effective semisimple permutation representation (S, ϕ) for K/L (Lemma II.46), such that $S = S_1 \times \cdots \times S_d$ where each S_i is nonabelian simple and $(|S_i|, p) = 1$. $G^\#$, and hence P_1^x and P_2, all act on S via conjugation. Let $Q' =$ FIND-NORMALIZED-SYLOW-SEMISIMPLE(G, K, L, S, P_1^x) and let $Q'' =$ FIND-NORMALIZED-SYLOW-SEMISIMPLE(G, K, L, S, P_2) (Problem IV.7; n.b. here Q' does not indicate the derived group), so $Q' = Q'_1 \times \cdots \times Q'_d$ is normalized by P_1^x, and $Q'' = Q''_1 \times \cdots \times Q''_d$ is normalized by P_2, where for each $i = 1, \ldots, d$, Q'_i and Q''_i are Sylow q_i-subgroups of S_i, and $N_S(Q')$ (and hence $N_S(Q'')$) are both solvable. For each $i = 1, \ldots, d$ in parallel, let $s_i =$ SYLCONJ-SIMPLE(S_i, Q'_i, Q''_i), and let y be a preimage in K of $s_1 \cdots s_d \in S$ (Remark II.3) so that P_1^{xy}/L normalizes Q''. Let $G^* = \langle P_1^{xy}, P_2, L\rangle$. Since P_1^{xy}/L and P_2/L both normalize Q'', it follows that $(G^* \cap K)/L = (\langle P_1^{xy}, P_2\rangle \cap K)/L \leq N_{K/L}(Q'') \cong N_S(Q'')$, which is solvable; hence $(G^* \cap K)/L$ is solvable. Moreover, $G^*/(G^* \cap K) \cong G^*K/K \leq G/K = G/O^A(G)$, so $G^*/(G^* \cap K)$ is also solvable. Hence G^*/L is solvable. Recursively find $z =$ SYLCONJ-$\mathcal{L}_{p'}(G^*, P_1^{xy}, P_2)$ and return $g = xyz$.

To analyze the running time of SYLCONJ-$\mathcal{L}_{p'}$, note that $L = R_{\mathcal{L}_{p'}}O^A(G)$ so the group G^* that is passed in the recursive call satisfies

$$R_{\mathcal{L}_{p'}}O^A(G^*) = R_{\mathcal{L}_{p'}}O^A(L) = (R_{\mathcal{L}_{p'}}O^A)^2(G).$$

Hence the depth of the recursion is logarithmic by Proposition II.61. □

Problem IV.12 SYLCONJ(G, P_1, P_2)

GIVEN: a group $G \leq Sym(\Omega)$ and two Sylow p-subgroups P_1, P_2 of G,

FIND: an element $g \in G$ for which $P_1^g \leq P_2$.

Theorem IV.13 *SYLCONJ is in NC.*

Proof: Let $K = O^{\mathcal{L}_{p'}}(G)$ (Lemma II.62). and let $x = \text{SYLCONJ-}\mathcal{L}_{p'}(G, P_1, P_2)$ (Problem IV.10), so $P_1^x K/K = P_2 K/K$. Let $L = R_{\mathcal{N}}(K)$ (Lemma II.62). If $L = K$, then $R_{\mathcal{L}_{p'}}(K) = R_{\mathcal{N}}(K)$, which implies $K = 1$, so return the element x.

Otherwise, compute a semisimple permutation representation (S, ϕ) for K/L (Lemma II.46), and $S = S_1 \times \cdots \times S_d$ where S_i is nonabelian simple and p divides $|S_i|$ for each $i = 1, \ldots, d$. For $i = 1, \ldots, d$ we find Sylow p-subgroups P_i' and P_i'' of S_i as follows: $P_i' = \phi(P_1^x \cap K) \cap S_i$ and $P_i'' = \phi(P_2 \cap K) \cap S_i$ (Problem II.21). For each $i = 1, \ldots, r$ in parallel, let $s_i = \text{SYLCONJ-SIMPLE}(S_i, P_i', P_i'')$, and let y be a preimage in K, of $s_1 \cdots s_r \in S$ (Remark II.3). Then $P_1^{xy} \cap K = P_2 \cap K$. Let $G^* = \langle P_1^{xy}, P_2, L \rangle$. Note that $G^*/(G^* \cap K) \cong G^* K/K \leq G/K$ is an $\mathcal{L}_{p'}$-group, and $(G^* \cap K)/L = (\langle P_1^{xy}, P_2 \rangle \cap K)/L = (P_2 \cap L)/L$, which is a p-group, and so also an $\mathcal{L}_{p'}$-group. Hence G^*/L is is an $\mathcal{L}_{p'}$-group. Recursively find $z = \text{SYLCONJ}(G^*, P_1^{xy}, P_2)$, and return $g = xyz$.

To analyze the running time of SYLCONJ, note that $L = R_{\mathcal{T}_4} O^{\mathcal{T}_3}(G)$ so the group G^* that is passed in the recursive call satisfies

$$R_{\mathcal{T}_4} O^{\mathcal{T}_3}(G^*) = R_{\mathcal{T}_4} O^{\mathcal{T}_3}(L) = (R_{\mathcal{T}_4} O^{\mathcal{T}_3})^2(G).$$

Hence the depth of the recursion is logarithmic in $|\Omega|$ by Proposition II.61. □

CHAPTER V

SYLFIND AND SYLCONJ FOR NONABELIAN SIMPLE GROUPS

Overview of the Algorithms

This chapter presents algorithms for finding and conjugating Sylow subgroups in nonabelian simple groups. Before delving into the technicalities, we give a brief overview of the algorithm for SYLFIND-SIMPLE, Problem V.135 (the algorithm for SYLCONJ-SIMPLE, Problem V.148, has a similar overall structure). The reader unfamiliar with the classical simple groups may consult the next section, where their definitions are recalled.

Given a nonabelian simple group $G \leq \mathrm{Sym}(\Omega)$ and a prime p, we first construct a set X upon which G acts primitively (using procedure PRIMITIVE-ACTION, Problem II.32). If $|G| \leq |X|^8$—a condition that holds if G is sporadic or exceptional ([16] Lemma 6.1)—we find a Sylow p-subgroup P of G by brute force (using procedure SYLFIND-SMALL) and lift P to a Sylow p-subgroup of G in the original action on Ω.

Otherwise ($|G| > |X|^8$), G must be either an alternating group or a classical simple group ([16] Lemma 6.1). We construct an action of G on a set Y (using procedure NATURAL-ACTION; see Definition V.26) that is permutation-isomorphic to a natural action of G. If G is an alternating group, we find a Sylow p-subgroup P^Y of G^Y using procedure SYLFIND-ALT, lift P^Y to a group P^X acting on X, and finally lift P^X to a Sylow p-subgroup P of G in the original action on Ω (see Remark

II.3).

If G is a classical group defined over a vector space V, we coordinatize the set Y, i.e., we identify with each point in Y the coordinates, relative to a fixed basis, of some nonzero vector in a 1-space of V (or possibly of V^*, the dual space of V). If for example, $G \cong PSp(V)$, then the action of $PSp(V)$ on the 1-spaces of V induces the action of G on Y via this identification (and similarly for the other classical groups).

Next, we find a group G^* that acts linearly on V and induces G on $\overline{V}$, the set of 1-spaces of V (or if $G = PSL(V)$, possibly $\overline{V^*}$, the set of 1-spaces of V^*), for which $G^* = G^{*\prime}$ (using procedure TRANSLATE-GROUP), and use procedures SYFIND-GL or SYLFIND-CLASSICAL to find a Sylow p-subgroup P^* of G^*. We lift the group P^* to a group P^Y acting on Y, then lift P^Y to a group P^X acting on X, and finally lift P^X to a Sylow p-subgroup in the original given action on Ω.

Preliminaries Concerning Classical Groups

Much of this chapter assumes some familiarity with classical groups. For convenience, the essential definitions are included here. For more information about the material given in this section, consult [9], Chapter 1, and [32], Chapters 8, 10, and 11.

In the following, let F_q denote a field of q elements.

Definition V.1 *The group of all linear transformations of a vector space V to itself with nonzero determinant is the* general linear group *on V and is denoted $GL(V)$. If $V \cong F_q^n$, this group is also denoted $GL(n,q)$.*

Definition V.2 *The group $\{T \in GL(V) \mid det(T) = 1\}$ is the* special linear group *and is denoted $SL(V)$. If $V \cong F_q^n$, this group may also be denoted $SL(n,q)$.*

Note that $SL(V) \trianglelefteq GL(V)$, and $SL(V)$ is the kernel of the map $GL(V) \to F_q^*$ given by $T \mapsto det(T)$.

Fact V.3 *The center of* $GL(V)$ *is* $Z = \{\alpha I \mid \alpha \in F_q^*\}$.

The set of 1-spaces of a vector space V is denoted $\overline{V}$. The action of $GL(V) = GL(n,q)$ on $\overline{V}$ via $\langle v \rangle \mapsto \langle Tv \rangle$, for $T \in GL(V)$ and $v \in V$, gives a homomorphism $GL(V) \to Sym(\overline{V})$ with kernel Z.

Definition V.4 *The group* $GL(V)/Z$ *is the* projective general linear group *and is denoted* $PGL(V)$ *or* $PGL(n,q)$. *The group* $SL(V)/(SL(V) \cap Z)$ *is the* projective special linear group *and denoted* $PSL(V)$ *or* $PSL(n,q)$.

Fact V.5 $|GL(n,q)| = q^{n(n-1)/2}(q^n - 1)(q^{n-1} - 1)\cdots(q-1)$.

Fact V.6 $|SL(n,q)| = |PGL(V)| = \frac{1}{q-1}|GL(V)|$.

Fact V.7 $|PSL(n,q)| = \frac{1}{(n,q-1)}|SL(V)|$.

Definition V.8 *Let* θ *be an automorphism of a field* F. *A* sesquilinear form *on* V *with respect to* θ *is a function* $f : V \times V \to F$ *which satisfies:* $\forall\, u, v \in V$, $\forall\, a \in F$,

1. $f(u_1 + u_2, v) = f(u_1, v) + f(u_2, v)$ *and* $f(u, v_1 + v_2) = f(u, v_1) + f(u, v_2)$
2. $f(au, v) = af(u, v)$ *and* $f(u, av) = a^\theta f(u, v)$

Definition V.9 *A function* f *is a* bilinear form *if* f *is sesquilinear and* $\theta = 1$.

Definition V.10 *Two forms* f *and* g *on* V *are* equivalent *if there is some nonzero* $c \in F$ *and some nonsingular linear transformation* $T : V \to V$, *for which* $g(u,v) = cf(Tu, Tv)$ *for all* $u, v \in V$.

For conciseness, we will sometimes use the notation $(\ ,\ )$ instead of $f(\ ,\ )$ to denote a bilinear or sesquilinear form, when the meaning is clear. We restrict ourselves to *reflexive* forms, i.e., we require $(u,v) = 0 \Rightarrow (v,u) = 0$.

Definition V.11 *A bilinear form on V is*

1. symmetric *if* $(u,v) = (v,u)$ *for all* $u, v \in V$,

2. alternating *(or* skew-symmetric*) if* $(u,v) = -(v,u)$ *for all* $u, v \in V$.

A sesquilinear form on V with respect to θ is

3. Hermitian *if* $(u,v) = (v,u)^\theta$ *for all* $u, v \in V$ *and* $|\theta| = 2$*; in this case,* α^θ *is denoted* $\overline{\alpha}$*, for* $\alpha \in F$.

Definition V.12 *Fix a bilinear (or sesquilinear) form* $(\ ,\ )$. *If* $S \subseteq V$, *let* $S^\perp = \{v \in V \mid (v,s) = 0 \forall s \in S\}$. $V^\perp$ *is called the* radical *of* V. *If* $V^\perp = 0$, *then* V *and the form* $(\ ,\ )$ *are called* nonsingular.

Definition V.13 *Let* $(\ ,\ )$ *be a nonsingular form on* V. *A linear transformation* $T \in GL(V)$ *is an* isometry *of* V *if* $(u,v) = (Tu, Tv)$ *for all* $u, v \in V$.

If a form $(\ ,\ )$ on V is identically zero (i.e., $(u,v) = 0$ for all $u, v \in V$), then the group of isometries of V is $GL(V)$. Including this form will permit us to handle $PSL(V)$ and the other classical groups more uniformly.

Definition V.14 *Let* V *a vector space over a field* F.

1. *If* $(\ ,\ )$ *is a nonsingular alternating form on* V, *then the group of isometries of* V *is called a* symplectic group, *and is denoted* $Sp(V)$. *If* $|F| = q$ *and* $V \cong F^n$, *this symplectic group is also denoted* $Sp(n,q)$. V *is referred to as a* symplectic space *with respect to the form. The dimension of a symplectic space is always even.*

2. *If* $(\ ,\ )$ *is a nonsingular hermitian form on* V*, then the group of isometries of* V *is called a* unitary group*, and is denoted* $U(V)$*.* V *is called a* unitary space *with respect to the form. The field size of a unitary space is always a square. If* $|F| = q^2$ *and* $V \cong F^n$*, the unitary group is also denoted* $U(n,q)$*. The isometries of determinant 1 form a normal subgroup* $SU(n,q)$ *of* $U(n,q)$*, called the* special unitary group.

3. *A function* $Q : V \to F$ *is a* quadratic form *on* V *if, for all* $u, v \in V$*,* $Q(au + bv) = a^2Q(u) + b^2Q(v) + ab(u,v)$ *where* $(\ ,\ )$ *is a symmetric bilinear form on* V *and* $a, b \in F$*. A bilinear form* $(\ ,\ )$ *determines a unique quadratic form* $Q(u) = \frac{1}{2}(u,u)$ *unless char(*F*) = 2. A quadratic form is* nonsingular *if the associated bilinear form is nonsingular. If* Q *is a nonsingular quadratic form, an* isometry *of* V *(with respect to* Q*), is a nonsingular linear transformation* T *for which* $Q(Tv) = Q(v)$ *for all* $v \in V$*. The group of isometries of* V *is called an* orthogonal group*, and is denoted* $O(V)$*.* V *is called an* orthogonal space *with respect to the form* Q*.*

Definition V.15 *A subspace* U *of* V *is called* totally isotropic *(resp.* totally singular *if* V *is an orthogonal space) if* $(u,w) = 0$ *for all* $u, w \in U$ *(resp.* $Q(u) = 0$ *for all* $u \in U$ *if* V *is orthogonal). If* $\langle u \rangle$ *is a totally isotropic (resp. totally singular) space, then* u *is called an* isotropic vector *(resp.* singular vector*). All maximal totally isotropic or totally singular subspaces of a space* V *have the same dimension, which is called the* Witt index *of* V*.*

Remark V.16 Let $V \cong F_q^n$ be an orthogonal space. If n is odd, then the Witt index is $\frac{1}{2}(n-1)$ and all quadratic forms are equivalent, i.e., they induce equivalent bilinear forms (Definition V.10). In this case, $O(V)$ is also denoted $O(n,q)$. If n is

even, there are two inequivalent quadratic forms depending on the Witt index of V, which may be either $\frac{n}{2}$ or $\frac{n}{2}-1$. These two forms give rise to two nonisomorphic orthogonal groups which are denoted $O^+(n,q)$ and $O^-(n,q)$, respectively.

Orders of the Classical Simple Groups

The center of $Sp(2m,q)$ consists of the transformations $v \mapsto \alpha v$, where $\alpha = \pm 1$. The groups $PSp(2m,q) = Sp(2m,q)/Z(Sp(2m,q))$ are simple except for $PSp(2,2)$, $PSp(2,3)$, and $PSp(4,2)$.

Fact V.17 *The sizes of the symplectic groups are given by the following formulas:*

1. $|Sp(2m,q)| = q^{m^2}(q^{2m}-1)(q^{2m-2}-1)\cdots(q^2-1)$ *and*
2. $|PSp(2m,q)| = \frac{1}{(2,q-1)}|Sp(2m,q)|$ *([32], p.70).*

The center of $U(n,q)$ consists of the transformations $v \mapsto \alpha v$, where $\alpha\overline{\alpha} = 1$. The group $PSU(n,q) = SU(n,q)/Z(SU(n,q))$ is simple except for $PSU(2,2)$, $PSU(2,3)$, and $PSU(3,2)$.

Fact V.18 *The sizes of the unitary groups are given by the following formulas:*

1. $|U(n,q)| = q^{n(n-1)/2}(q^n-(-1)^n)\cdots(q^3+1)(q^2-1)(q+1)$.
2. $|SU(n,q)| = \frac{1}{q+1}|U(n,q)|$.
3. $|PSU(n,q)| = \frac{1}{(n,q+1)}|SU(n,q)|$ *([32], p. 118).*

The determinant of an orthogonal transformation in $O(V) = O(2m+1,q)$ or $O^{\pm}(2m,q)$ is ± 1, and the orthogonal transformations of determinant 1 form a subgroup $SO(2m+1,q)$ or $SO^{\pm}(2m,q)$. The center of $O(V)$ consists of the isometries

$v \mapsto \alpha v$ where $\alpha = \pm 1$, provided $n > 2$. The corresponding projective groups are defined as

$$PSO(2m+1,q) = SO(2m+1,q)/Z(SO(2m+1,q)),$$
$$PO^{\pm}(2m,q) = O^{\pm}(2m,q)/Z(O^{\pm}(2m,q)), \text{ and}$$
$$PSO^{\pm}(2m,q) = SO^{\pm}(2m,q)/Z(SO^{\pm}(2m,q)) \ ([32], p.140).$$

Unlike the symplectic and unitary cases, the groups $PSO(2m+1,q)$ and $PSO^{\pm}(2m,q)$ are not always simple. However, if we let $\Omega(2m+1,q)$ be the commutator subgroup of $O(2m+1,q)$ and let $\Omega^{\pm}(2m,q)$ be the commutator subgroup of $O^{\pm}(2m,q)$, then the projective groups

$$P\Omega(2m+1,q) = \Omega(2m+1,q)/Z(\Omega(2m+1,q)),$$
$$P\Omega^{\pm}(2m,q) = \Omega^{\pm}(2m,q)/Z(\Omega^{\pm}(2m,q))$$

are simple if $2m \geq 6$. For brevity, we sometimes use $P\Omega(V)$ to refer to any of $P\Omega(2m+1,q)$, $P\Omega^{+}(2m,q)$ or $P\Omega^{-}(2m,q)$, where the isometry group of V is $O(2m+1,q)$, $O^{+}(2m,q)$ or $O^{-}(2m,q)$, respectively.

Fact V.19 *The sizes of the orthogonal groups are given by the following formulas: If n is odd, let $n = 2m+1$. There is only one orthogonal group, whose order is*

1. $|P\Omega(2m+1,q)| = \frac{1}{(2,q-1)} q^{m^2}(q^{2m}-1)\cdots(q^4-1)(q^2-1)$.

If n is even, let $n = 2m$. There are two inequivalent quadratic forms that give rise to the nonisomorphic orthogonal groups $P\Omega^{+}(2m,q)$ and $P\Omega^{-}(2m,q)$ whose orders are

1. $|P\Omega^{+}(2m,q)| = \frac{1}{(4,q^m-1)} q^{m(m-1)}(q^m-1)(q^{2m-2}-1)\cdots(q^4-1)(q^2-1)$,
2. $|P\Omega^{-}(2m,q)| = \frac{1}{(4,q^m+1)} q^{m(m-1)}(q^m+1)(q^{2m-2}-1)\cdots(q^4-1)(q^2-1)$.

For later reference, we note the following:

Lemma V.20 *Let G be a classical simple group defined abstractly in terms of a vector space V. Then $|G|$ is quasipolynomial in $|V|$ (i.e., $\log|G| = O(\log^c|V|)$ for some constant c),*

Proof: $|G| \leq |SL(V)| = q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\cdots(q^2-1) < (q^n)^{\frac{3}{2}n} = |V|^{\frac{3}{2}\log(|V|)}$ (recall $q^n = |V|$ so $n = \log_q|V|$). □

Let V be a vector space with a nonsingular form ϕ over a field F of size q. Let G^* be a classical group defined in terms of V and ϕ. Let G be the group induced by G^* on $\overline{V}$.

Fact V.21 *If $\dim(V) > 2$, then V is spanned by its isotropic or singular points.*

Proof: [32] 11.21. □

Fact V.22 *If y is isotropic or singular, G_y induces a classical group on $y^\perp/y$. If y is nonisotropic or nonsingular, G_y on $y^\perp$ is a classical group.*

Proof: [32], Ex. 8.11, 10.13. □

Fact V.23 *The set of isotropic points is the unique G-orbit on $\overline{V}$ of q'-size.*

Proof: By [32], Lemma 10.4 and Theorem 11.5, the set of isotropic points has q' size in the unitary or orthogonal case. In the symplectic case, all points in $\overline{V}$ are isotropic, and $|\overline{V}|$ is q'. Witt's Theorem ([32], Theorem 7.4), implies the set of isotropic or singular points is an orbit. If G is unitary, the nonisotropic points comprise a single orbit. In the orthogonal case, the set of nonsingular 1-spaces form either one or two orbits. In either case, the sizes of these orbits are multiples of q. □

Fact V.24 *Let V be a vector space where* $\dim(V) > 3$. *If $y \in \overline{V}$ is nonisotropic or nonsingular, there is a unique G_y-orbit on the set of isotropic or singular points of q' size, and this orbit spans $y^\perp$. If $y \in \overline{V}$ is isotropic or singular, then the unique smallest orbit of G_y on the set of isotropic or singular points spans $y^\perp$.*

Proof: If y is nonisotropic or nonsingular, $y^\perp$ is a nonsingular space by Fact V.22. The isotropic vectors span this space and form a q'-orbit by Facts V.21 and V.23. If y is isotropic or singular, $y^\perp/y$ is a nonsingular space by Fact V.22. The isotropic points span this space; the number i of such points is given by [32], Lemma 10.4 and Theorem 11.5. Preimages in $\overline{V}$ are isotropic points in G_y, and the number of preimages is qi. From the values of i given in [32], it follows that $y^\perp$ is the smallest orbit of G_y on the set of isotropic points. □

Obtaining Natural Actions

Definition V.25 *Throughout the remainder of this chapter, if V is a vector space, $\overline{V}$ will denote the set of 1-spaces of V.*

Definition V.26 *If $G \cong A_n$ $(n > 6)$, the* natural action *of G is a faithful permutation representation as $Alt(\Delta)$ on a set Δ. If $G \cong PSp(V), PSU(V)$ or $P\Omega(V)$ where* $\dim(V) > 8$, *the* natural action *of G is its action on $\overline{V}$. If $G \cong PSL(V)$, there are two natural actions, on $\overline{V}$ and $\overline{V^*}$.*

Excluding alternating groups A_n for $n \leq 6$ and classical groups where $\dim(V) \leq 8$ from consideration eliminates ambiguities that would otherwise arise from the nonuniqueness of some standard natural actions for certain groups (e.g., due to $PSp(4,q) \cong P\Omega(5,q)$ reflecting two different but equally "natural" actions).

If $G \cong PSL(n,q)$, we cannot distinguish the two natural actions based on the abstract group G or based on any properties of the available permutation representation. The procedure NATURAL-ACTION (Problem V.35) finds one of these two actions, and the procedure COORDINATIZE (Problem V.69) constructs a coordinatization of it. Either action suffices for our purposes; the one we find arises from a vector space which we rename V.

Furthermore, since $PSp(2m,q) \cong P\Omega(2m+1,q)$ if q is even, an ambiguity arises when we refer to a "natural action" of one of these groups. Our algorithms resolve this ambiguity: the procedure DOUBLE-PAIRING will always construct $PSp(2m,q)$ rather than $P\Omega(2m+1,q)$.

The requirement that $|G| > |X|^8$ not only ensures that G is not exceptional or sporadic, as noted above, but also guarantees that if G is a classical group defined on a vector space V, then $\dim(V) > 8$ ([16], Lemma 6.1 (iii)).

The following two procedures, PAIRING and DOUBLE-PAIRING, are given in [16], p. 493, and shown to be in polynomial time. These procedures are reproduced here; some details left implicit in [16] are included to make clear that the procedures are in fact also in NC.

Procedure V.27 PAIRING(G, X)

{ G is a simple group acting faithfully and primitively on X, and $|G| > |X|^8$ }
choose $x \in X$
for each $y \in X$ **in parallel**
  $K \leftarrow G_{\{x,y\}}$ (Problem II.19) { K is a point stabilizer of the action of G on the set of unordered pairs of elements of X }
  let R_K be a transversal for K in G (Problem II.8)
  $\mathcal{Y}_K \leftarrow$ MINIMAL-SUBGROUPS(G, K, R_K) (Problem II.26)
  { each element of $\mathcal{Y}_K$ is a pair consisting of a subgroup H and a transversal R_H for H in G }
  if $\mathcal{Y}_K$ is empty **then** $\mathcal{Y}_K \leftarrow \{(K, R_K)\}$
  for each $(H, R_H) \in \mathcal{Y}_K$ **in parallel**
    $\mathcal{Z}_H \leftarrow$ MINIMAL-SUBGROUPS(G, H, R_H)
    { each element of $\mathcal{Z}_H$ is a pair consisting of a subgroup H^* and a transversal R_{H^*} for H^* in G }
    if $\mathcal{Z}_H$ is empty **then** $\mathcal{Z}_H \leftarrow \{(H, R_H)\}$
    for each $(H^*, R_{H^*}) \in \mathcal{Z}_H$ **in parallel**
      $(M_{H^*}, R_{M_{H^*}}) \leftarrow$ MAXIMAL-SUBGROUP(G, H^*, R_{H^*}) (Problem II.28)
    $\mathcal{M}_H \leftarrow \{(M_{H^*}, R_{M_{H^*}}) \mid H^* \in \mathcal{Z}_H\}$
  $\mathcal{N}_K \leftarrow \cup_{H \in \mathcal{Y}_K} \mathcal{M}_H$

return $\mathcal{M}(G_x) = \{(N, R_N) \in \cup_K \mathcal{N}_K \mid [G : N] < 2|X|\}$ $\diamond$[1]

Procedure V.28 DOUBLE-PAIRING(G, X)

{ G is a simple group acting faithfully and primitively on X, and $|G| > |X|^8$ }
$\mathcal{C} \leftarrow$ PAIRING(G, X) (Procedure V.27)
return $\mathcal{M}' = \cup_{(M,R_M) \in \mathcal{C}}$ PAIRING(BUILD-ACTION(G, M, R_M)) (Problem II.30)
$\diamond$

Lemmas 6.1, 10.1, and Theorem 6.2, in [16] combine to give

Theorem V.29 *Let $G \leq Sym(X)$ be a simple, faithful, primitive group with $|G| >$*

[1] Throughout this chapter, this symbol denotes the end of a procedure.

$|X|^8$, and let $\mathcal{M}'$ =DOUBLE-PAIRING(G, X). Let (M_1, R_{M_1}) be a pair in $\mathcal{M}'$ for which $|M_1|$ is maximal. If there exists $(M_2, R_{M_2}) \in \mathcal{M}'$ with $|G : M_1| < |G : M_2| < 2|G : M_1|$, then let $M = M_2$ and $R_M = R_{M_2}$; otherwise let $M = M_1$ and $R_M = R_{M_1}$. Let the set of cosets of M in G be denoted Y'. Then exactly one of the following holds:

1. *G is an alternating group, and G acts on Y' as $Alt(Y')$;*
2. *$G \cong PSL(V)$ (resp. $PSp(V)$) for some vector space V, and G acts on Y' as $PSL(V)$ (resp. $PSp(V)$) acts on $\overline{V}$ (see Definition V.25) (or possibly $\overline{V^*}$ in the case $G \cong PSL(V)$).*
3. *$G \cong PSU(V)$ or $P\Omega(V)$ for some vector space V, and G acts on Y' respectively as $PSU(V)$ or $P\Omega(V)$ acts on the orbit of isotropic or singular 1-spaces of V.*

With M as in Theorem V.29, BUILD-ACTION(G, M, R_M) yields the action of G on Y'. This call to BUILD-ACTION, and the calls within PAIRING to MINIMAL-SUBGROUPS and MAXIMAL-SUBGROUP, are valid because in each case the second argument is a subgroup of G whose index is polynomial in the degree of G.

Corollary V.30 *PAIRING and DOUBLE-PAIRING are in NC.*

Proof: The procedures they invoke are in NC. □

The following definition provides a succinct notation for a class of permutation groups that arise frequently in the remainder of this chapter.

Definition V.31 *Let $\mathcal{G}$ denote the set of pairs (G, X) where G is a classical simple group, G acts on X, $|G| > |X|^8$, and G^X is permutation-isomorphic to a natural*

action of G (Definition V.26). Similarly, let $\mathcal{G}^*$ denote the set of pairs (G^*, V) where $G^* = G^{*\prime} \leq SL(V)$ and $(G^{*\overline{V}}, \overline{V}) \in \mathcal{G}$.

In fact, it is desirable to include forms in the definition of $\mathcal{G}^*$. However, forms are not yet available, so they are absent in Definition V.31. Nevertheless, until forms become available, Definition V.31 will be of much use. Following the construction of forms in CONSTRUCT-FORM (Problem V.87) and CONSTRUCT-QUAD-FORM (Problem V.89), the symbol "$\mathcal{G}^*$" will refer to the following *modified definition:*

Definition V.31* *Let $\mathcal{G}^*$ be the set of triples (G^*, V, ϕ), where $G^* = G^{*\prime} \leq SL(V)$, $(G^{*\overline{V}}, \overline{V}) \in \mathcal{G}$ (Definition V.31), and ϕ is the form on V involved in the definition of the classical group G^*; hence, ϕ is nonsingular unless $G^* \cong SL(V)$, in which case ϕ is the zero-form.*

Remark V.32 We restate a point made prior to Problem V.27 in terms of the notation just defined: If $(G^*, V) \in \mathcal{G}^*$ then $\dim(V) > 8$.

Problem V.33 MAKE-POINTS(G, Y')

GIVEN: a classical (non-PSL) simple group $G \leq \mathrm{Sym}(Y')$ where the action of G on Y' is the restriction of the natural action of G to the orbit of isotropic or singular points of the natural action, and $|G| > |Y'|^8$,

FIND: an action of G on a set Y such that $(G, Y) \in \mathcal{G}$.

The following procedure for MAKE-POINTS is given in [16], p. 505-506, and shown to be in polynomial time. It is reproduced here with some details left implicit in [16] included to make clear that the procedure is in fact also in NC.

Procedure for Problem V.33:
choose $y \in Y'$
let O_1 and O_2 be the two orbits of G_y (other than $\{y\}$) with $|O_1| < |O_2|$
let q be the size of a minimal block in the action of G on O_1
choose $z \in O_2$ { so $z \notin y^\perp$ }
if G_{yz} has an orbit on $Y' - \{y, z\}$ of size $\sqrt{q} - 1$ **then** $q \leftarrow \sqrt{q}$
{ $z \notin y^\perp$, G_{yz} fixes the 2-space $\langle y, z \rangle$; an orbit has size $\sqrt{q} - 1$ only if G is unitary }
$L \leftarrow (G_{yz} \cap (G_y)') \cap (G_z)'$ { Problem II.21; note $L = (G_y)' \cap (G_z)'$ }
{ $[G : L]$ is polynomial in $|Y'|$ since
$[G : (G_y)'] = [G : (G_z)'] = [G : G_y][G_y : (G_y)'] \leq |Y'|^2$ ([16], p. 497) }
let R_L be a transversal for L in G (Problem II.34) { valid by Fact V.20 }
$\mathcal{L} \leftarrow \{L^r \mid r \in R_L\}$ { the set of G-conjugates of L, since $L \leq N_G(L)$ }
{ this requires removing duplicates; $L^r = L^s$ can be tested using Problem II.1 }
{ $|\mathcal{L}|$ has size polynomial in $|Y'|$ since $|\mathcal{L}| = [G : N_G(L)] \leq [G : L]$ }
$\mathcal{L}^* \leftarrow \{\langle L, L^* \rangle \mid L^* \in \mathcal{L}, \langle L, L^* \rangle \neq G\}$
$\mathcal{M} \leftarrow \{M \leq G \mid (M, R_M) =$ MAXIMAL-SUBGROUP(G, L^*, R_{L^*}), where $L^* \in \mathcal{L}^*$,
$R_{L^*} =$ FIND-TRANSVERSAL1(G, L^*, L, R_L), and $[G : M] < q^3|Y'|\}$
(Problems II.28, II.24)
return the action of G by conjugation on $Y = \cup_{M \in \mathcal{M}} \{M^r \mid r \in R_M\}$ (Remark II.4)
{ this requires removing duplicates; $M^r = M^s$ can be tested using Problem II.1 }
{ Y is the set of conjugates of all $M \in \mathcal{M}$ since $M \leq N_G(M)$ for each $M \in \mathcal{M}$ }
$\diamond$

Lemma V.34 *MAKE-POINTS is correct and in NC.*

Proof: The correctness is proved in [16] Theorem 10.5. MAKE-POINTS is in NC since the procedures it invokes are in NC. □

As noted above, if G is an alternating, projective special linear, or a symplectic group, the action of G on the set Y' found by DOUBLE-PAIRING is the sought-after natural action. If G is a symplectic, unitary or orthogonal group, the natural action is not transitive and DOUBLE-PAIRING finds only the orbit of of G on the isotropic or singular points. Invoking the procedure MAKE-POINTS constructs the

the additional orbit(s) of nonsingular points of G in a natural action, if any exist. (If G is symplectic, G acts transitively on Y', each $y \in Y'$ is isotropic, and $Y' = Y$ [16], 6.1, 6.2.)

The preceding discussion of finding natural actions for simple groups can be summarized by the following:

Problem V.35 NATURAL-ACTION(G, X)

GIVEN: a simple group G acting faithfully and primitively on X and $|G| > |X|^8$

FIND: the action of G on a set Y which is a natural action of G.

Procedure for Problem V.35:
$\mathcal{M}' \leftarrow$ DOUBLE-PAIRING(G, X) (Procedure V.28)
choose $(M_1, R_{M_1}) \in \mathcal{M}'$ such that $|M_1|$ is maximal
if there exists $(M_2, R_{M_2}) \in \mathcal{M}'$ for which $|G : M_1| < |G : M_2| < 2|G : M_1|$
  then $(M, R_M) \leftarrow (M_2, R_{M_2})$ **else** $(M, R_M) \leftarrow (M_1, R_{M_1})$ { cf. Theorem V.29 }
let $Y' = G/M$ and find the action of G on Y' via BUILD-ACTION(G, M, R_M)
choose $y \in Y'$
if $G^{Y'}$ is 2-transitive
  then return the action of G on Y' (Remark II.4)
  { no need to call MAKE-POINTS if G is alternating or a PSL }
else return the action of G on a set Y found by MAKE-POINTS(G, Y')
    (Problem V.33) $\diamond$

Remark V.36 We have just shown how to find a set Y upon which a group G acts in its natural action if G is known to be a classical group. This set can be identified with the set $\overline{V}$ of 1-spaces of a vector space V over a field F; subsequently, this identification of Y with $\overline{V}$ will be assumed. Even before constructing V explicitly, we show how to find the span of a given subset of Y; more precisely, given a subset $A \subseteq Y$, we show how to find a subset $[A] \subseteq Y$ such that under the identification of Y with $\overline{V}$, $[A]$ is identified with the span of the set with which A is identified. We will then be able to speak, for example, of the line containing two points $a, b \in Y$, without

explicitly remarking that Y is identified with $\overline{V}$ (see, for example, the statement of LINE, Problem V.41). We also show how to compute the characteristic and size of F, the the dimension n of V, an independent set of points, and the set $A^{\perp}$ for any set $A \subseteq Y$. For these computations, we do not require an explicit identification of Y with $\overline{V}$ i.e., a coordinatization. (In COORDINATIZE, Problem V.69, we give an NC algorithm for making this identification explicit.) The following observations will be used to prove that these computations are in NC.

Remark V.37 Let $G \leq \mathrm{Sym}(\Omega)$ be a simple classical group, let X be the set found by PRIMITIVE-ACTION(G, Ω) (Problem II.32), and let Y be the set found by NATURAL-ACTION(G, X) (Problem V.35). Then $|X| = O(|\Omega|)$, by construction. Also, by the constructions in DOUBLE-PAIRING and MAKE-POINTS, the size of the set Y produced by MAKE-POINTS (and hence by NATURAL-ACTION) is polynomial in $|X|$. Hence we have:

Lemma V.38 *Let $G \leq Sym(\Omega)$ be a simple classical group, let X be the set found by PRIMITIVE-ACTION(G, Ω), and let Y be the set found by NATURAL-ACTION(G, X), so Y is identifiable with $\overline{V}$ for a vector space V. Then* $\dim(V) = O(\log |\Omega|)$.

Proof: We have $\dim(V) = O(\log |V|) = O(\log |Y|) = O(\log |X^c|) = O(\log |X|) = O(\log |\Omega|)$ by Remark V.37. □

To prove that the running time of a procedure is in NC with respect to the size of the original given input set Ω, it suffices, by Lemma V.38, to show the time required by the procedure is polylogarithmic in the size of V, or in particular, is polynomial in $\dim(V)$.

Definition V.39 *Suppose $(G, Y) \in \mathcal{G}$.*

1. *If a, b are two distinct points $\in Y$, let* $[a,b] = \{c \in Y \mid G_c \geq G_a' \cap G_b'\}$.

2. *If $A \subseteq Y$, let $[A]$ be the smallest subset of Y containing A such that for any pair of distinct points $a, b \in [A]$, $[a,b] \subseteq [A]$.*

Fact V.40 *$[A]$ is the set of 1-spaces of $\langle A \rangle$ (see Remark V.36).*

Proof: [16] Lemmas 8.3 and 10.6. □

Fact V.40 implicitly assumes an identification of Y with the 1-spaces of a vector space. This identification is also assumed in the following Problems V.41–V.53. In particular, $[a,b]$ is the set of 1-spaces of $\langle a,b \rangle$, which we refer to as the *line* containing the points a and b. This definition and fact suggest the following:

Problem V.41 LINE(G, Y, a, b)

GIVEN: $(G,Y) \in \mathcal{G}$ and two distinct points $a, b \in Y$,

FIND: $[a,b] \subseteq Y$, the line containing a and b.

Procedure for Problem V.41:
$L \leftarrow (G_{ab} \cap (G_a)') \cap (G_b)'$ { Problems II.19 and II.21; note $L = (G_a)' \cap (G_b)'$ }
return the set of fixed points of L on Y (Problem II.5) ◇

Lemma V.42 *LINE is correct and in NC.*

Proof: Correctness follows at once from Fact V.40 and Definition V.39; LINE is in NC since Problems II.5, II.19, and II.21 are in NC. □

The following two procedures, FIND-FIELD-SIZE and SPAN-POINTS are immediate applications of the procedure LINE.

Problem V.43 FIND-FIELDSIZE(G, Y)

GIVEN: $(G, Y) \in \mathcal{G}$,

FIND: the size of the field over which G is defined.

Procedure for Problem V.43:
return $|\text{LINE}(G, Y, y, z)| - 1$ (Problem V.41) $\diamond$

Lemma V.44 *FIND-FIELDSIZE is correct and in NC.*

Proof: Correctness follows from the observation that the number of points on a line is one greater than the size of the field; FIND-FIELDSIZE is in NC since LINE (Problem V.41) is in NC. □

Problem V.45 SPAN-POINTS(G, Y, A)

GIVEN: $(G, Y) \in \mathcal{G}$ and $A \subseteq Y$,

FIND: $[A]$, the set of points in $\langle A \rangle$.

Procedure for Problem V.45:
$i \leftarrow 0$
$B_i \leftarrow \emptyset$
while $A \setminus B_i$ is not empty
  choose $a_{i+1} \in A \setminus B_i$
  $B_{i+1} \leftarrow \cup_{b \in B_i} \text{LINE}(G, Y, a_{i+1}, b)$ (Problem V.41)
  $i \leftarrow i + 1$
return B_i $\diamond$

Lemma V.46 *SPAN-POINTS is correct and in NC.*

Proof: Correctness follows from Definition V.39 and Fact V.40. To show polylogarithmic running time, note that "$B_i = [a_1, \ldots, a_i]$" is a loop invariant, so the number of iterations is bounded by $\dim(V)$, and hence is logarithmic in $|Y|$ by Lemma V.38.

Moreover, in each iteration there are a polynomial number of calls to LINE which may all be performed in parallel. □

Problem V.47 FIND-INDEPENDENT-SET(G, Y)

GIVEN: $(G, Y) \in \mathcal{G}$,

FIND: a maximal set of independent points in $\overline{V} = Y$.

Procedure for Problem V.47:
$A \leftarrow \{a\}$ for some $a \in Y$
while SPAN-POINTS$(G, Y, A) \neq Y$ (see Problem V.45)
  choose $a \in Y \setminus$ SPAN-POINTS(G, Y, A)
  $A \leftarrow A \cup a$
return A ◇

Lemma V.48 *FIND-INDEPENDENT-SET is correct and in NC.*

Proof: Correctness is clear. Since $\dim(V)$ is logarithmic in $|\overline{V}| = |Y|$ (see Lemma V.38), FIND-INDEPENDENT-SET is in NC. □

Problem V.49 FIND-DIMENSION(G, Y)

GIVEN: $(G, Y) \in \mathcal{G}$,

FIND: $\dim(V)$ where $Y = \overline{V}$.

Procedure for Problem V.49:
$\mathcal{B} \leftarrow$ FIND-INDEPENDENT-SET(G, Y) (Problem V.47)
return $|\mathcal{B}|$ ◇

Lemma V.50 *FIND-DIMENSION is correct and in NC.*

Proof: Clear. □

As noted prior to Problem V.41, Y is implicitly identified with the set of 1-spaces of a vector space V. G can be defined abstractly in terms of V and a form

ϕ on V. For $y \in Y$, let $\langle v_y \rangle \in \overline{V}$ be the 1-space identified with y. Define $y^\perp$ to be the subset of Y that is identified with the set $\langle v_y \rangle^\perp \subseteq \overline{V}$. Although V and ϕ have not yet been constructed, the set $y^\perp \subseteq Y$ can nevertheless be found from the orbit structure of G and G_y, as described in the procedure for the following:

Problem V.51 PERP-POINT(G, Y, y)

GIVEN: $y \in Y$, $(G, Y) \in \mathcal{G}$ and $G \ncong PSL(V)$,

FIND: the set of points in $y^\perp$.

Procedure for Problem V.51:
$q \leftarrow$ FIND-FIELDSIZE(G, Y) (Problem V.43)
$\mathcal{I} \leftarrow$ the unique orbit of G on Y of size relatively prime to q
if $y \in Y \setminus \mathcal{I}$ **then**
  $\mathcal{O} \leftarrow$ the unique G_y-orbit on $\mathcal{I}$ of size relatively prime to q
else $\mathcal{O} \leftarrow$ smallest orbit of G_y on $\mathcal{I} \setminus \{y\}$
return SPAN-POINTS$(G, Y, \mathcal{O})$ (Problem V.45) $\diamond$

Lemma V.52 *PERP-POINT is correct and in NC.*

Proof: The space $y^\perp$ is spanned by its isotropic or singular points (Fact V.21). One of the orbits of G_y on $\mathcal{I}$ consists of the set of isotropic or singular points in $y^\perp$. The set $O = \{w \in \mathcal{I} \mid (w, y) = 0, w \neq y\}$ is an orbit of G_y since for any $w, v \in O$, there is an isometry from $\langle y, w \rangle$ to $\langle y, v \rangle$, which extends to an element of G by Witt's Theorem. The set O is equal to the set $\mathcal{O}$ found in the procedure by Fact V.24. The procedure is in NC since the problems it invokes are in NC. □

Problem V.53 PERP-POINTS(G, Y, A)

GIVEN: $(G, Y) \in \mathcal{G}$, $G \ncong PSL(V)$, and a set $A \subseteq Y$,

FIND: the set of points in $A^\perp$.

Procedure for Problem V.53:
$B \leftarrow$ FIND-INDEPENDENT-SET(SPAN-POINTS(G, Y, A)) (Problem V.47)
for each $b \in B$ **in parallel**
  $S_b \leftarrow$ PERP-POINT(G, Y, b) (Problem V.51)
return $\cap_{b \in B} S_b$ $\diamond$

Lemma V.54 *PERP-POINTS is correct and in NC.*

Proof: Let V be a vector space for which G acts on $\overline{V}$ as it does on Y. Let $\dim(V) = n$, and let $(\ ,\ )$ be the form on V. Let U be the subspace of V spanned by the points of A and let $B = \{b_1, \ldots, b_k\}$ be as in the procedure. Let $\mathcal{B} = \{\beta_1, \ldots, \beta_k\}$ be a set of vectors in V such $b_i = \langle \beta_i \rangle$ for each $i = 1, \ldots, k$ (hence $\mathcal{B}$ is a basis for U). Note that $U^\perp = \langle \mathcal{B} \rangle^\perp = \cap_i \{v \mid (\beta_i, v) = 0\} = \cap_i \beta_i^\perp$. Hence $A^\perp = \cap_i b_i^\perp$. These $k-1$ intersections may be performed in $O(\log k)$ rounds, but to show this procedure is in NC, it suffices to perform them sequentially by Lemma V.38. □

Identifying Nonabelian Simple Groups

If $G = \mathrm{Alt}(Y)$ or $(G, Y) \in \mathcal{G}$ (i.e., $G \leq \mathrm{Sym}(Y)$ and $|G| > |Y|^8$), then G is isomorphic to one of the following groups:

A_n

$PSL(n, q)$

$PSp(n, q)$ (n even)

$PSU(n, q)$

$P\Omega(n, q)$ (n odd, q even)

$P\Omega^+(n, q)$ (n even)

$P\Omega^-(n, q)$ (n even)

Given such a group $G \leq \mathrm{Sym}(Y)$ acting in its natural action on Y, the following procedure determines which of the groups listed above is isomorphic to G, together with the relevant *parameters* indicated in the list above: n, q (if G is not an alternating group), and a sign ($+$ or $-$) if G is isomorphic to an orthogonal group on an even dimensional space.

Problem V.55 IDENTIFY(G, Y)

GIVEN: $G \leq \mathrm{Sym}(Y)$, where G is $\mathrm{Alt}(Y)$ and $|G| > |Y|^8$, or $(G, Y) \in \mathcal{G}$

FIND: the name and appropriate parameters (n, also q if $(G, Y) \in \mathcal{G}$), of the group in the preceding list to which G is isomorphic.

Procedure for Problem V.55:

if G acts 3-transitively on Y **then**
  return ("G is the alternating group $Alt(|Y|)$")
else
  $n \leftarrow$ FIND-DIMENSION(G, Y) (Problem V.49)
  $q \leftarrow$ FIND-FIELDSIZE(G, Y) (Problem V.43; cf. line (*) below)
  let Y' be the unique orbit of q'-size
  if G_y is transitive on $Y - \{y\}$ **then**
    return ("$G = PSL(n, q)$ ")
  else if G is transitive on Y **then**
    return ("G is the symplectic group $PSp(n, q)$")
  { G must now be either orthogonal or unitary; hence G may be determined
    by the size of the orbit of isotropic or singular points }
  else if $n = 2m + 1$ is odd, and $|Y'| = (q^{2m} - 1)/(q - 1)$ **then**
    return ("$G = P\Omega(n, q)$")
  else if $n = 2m$ is even, and $|Y'| = (q^m \mp 1)(q^{m-1} \pm 1)/(q - 1)$ **then**
    return ("$G = P\Omega^{\pm}(n, q)$")

else { here G must be unitary }
  $q \leftarrow \sqrt{q}$ (*)
  if $n = 2m+1$ is odd, and $|Y'| = (q^{2m+1}+1)(q^{2m}-1)/(q^2-1)$ **then**
    return ("$G = PSU(2m+1, q)$")
  else if $n = 2m$ is even, and $|Y'| = (q^{2m}-1)(q^{2m-1}+1)/(q^2-1)$ **then**
    return("$G = PSU(2m, q)$") $\diamond$

Lemma V.56 *IDENTIFY is correct and in NC.*

Proof: See [16] B1-B4 (p. 486), Lemma 10.1. The values of $|Y'|$ in the unitary and orthogonal groups are always distinct. (Note the values of "n" for $PSU(2m+1, q)$ and $PSU(2m, q)$ are reversed in the table above Lemma 10.1 in [16].) □

Sylow Subgroups of the Symmetric and Alternating Groups

Before describing algorithms for Sylow subgroups of the classical simple groups, we first give algorithms for the symmetric and alternating groups. The procedures for the symmetric and alternating groups are closely related. These algorithms are used not only to solve SYLFIND-SIMPLE (Problem V.135) and SYLCONJ-SIMPLE (Problem V.148) when the given group is an alternating group, but also in the algorithms for SYLFIND-CLASSICAL (Problem V.133) and SYLCONJ-CLASSICAL (Problem V.146).

To describe a Sylow p-subgroup P of the symmetric group $\mathrm{Sym}(\Omega)$, we make the following definitions.

Definition V.57 *([14], p. 81) Let $H \leq Sym(\Delta)$ and let $K \leq Sym(\Gamma)$. The* wreath product *of H and K, written $H \wr K$, is a subgroup of $Sym(\Delta \times \Gamma)$ consisting of elements of the form*

$$(\delta, \gamma) \mapsto (\delta^{h_\gamma}, \gamma^k), \text{ for } (\delta, \gamma) \in \Delta \times \Gamma,$$

where $h_\gamma \in H$ (the permutations h_γ may be different for different choices of γ) and $k \in K$.

Remark V.58 In the context of the above definition, let $\Delta_\gamma = \Delta \times \{\gamma\}$ for each $\gamma \in \Gamma$, and view $\Delta \times \Gamma$ as the disjoint union $C = \cup_{\gamma \in \Gamma} \Delta_\gamma$. Then $H \wr K \leq \mathrm{Sym}(C)$ and

1. $H \wr K$ contains a normal subgroup $\prod_{\gamma \in \Gamma} H_\gamma$, where H_γ induces H on Δ_γ and induces the identity on each Δ_β, for $\beta \neq \gamma$. (This is the subgroup of $H \wr K$ of all permutations with $k = 1$ in Definition V.57.)

2. For each $k \in K \leq \mathrm{Sym}(\Gamma)$ define an action of k on C that maps

$$\Delta_\gamma \rightarrow \Delta_{\gamma^k}, \text{ for each } \gamma \in \Gamma$$

via

$$(\delta, \gamma) \mapsto (\delta, \gamma^k), \text{ for each } \delta \in \Delta.$$

(This is the subgroup of $\mathrm{Sym}(\Delta \times \Gamma)$ where each $h_\gamma = 1$ in Definition V.57.)

3. If H and K are transitive, then so is $H \wr K$; moreover, $H \wr K$ acts imprimitively on C since $\{\Delta_\gamma \mid \gamma \in \Gamma\}$ is a system of blocks for this action. $H \wr K$ is generated by the actions of H_γ and K given above in 1. and 2. where γ is any element of Γ.

4. $|H \wr K| = |H|^{|\Gamma|}|K|$.

5. If $H \leq \mathrm{Sym}(\Delta)$, $K \leq \mathrm{Sym}(\Gamma)$, and $L \leq \mathrm{Sym}(\Lambda)$, then $(H \wr K) \wr L = H \wr (K \wr L)$, where we identify $(\Delta \times \Gamma) \times \Lambda$ and $\Delta \times (\Gamma \times \Lambda)$.

The following is a classical construction given in [14], Sect.5.9, p. 82, and [15], Lemma 2.12.2. First, we make the following notational conventions, which will be in effect throughout this section. Let $P^* = \langle \rho \rangle$ be a Sylow p-subgroup of $\mathrm{Sym}(Y)$, where $Y = \{1, \ldots, p\}$, and for $n > 1$, inductively define $Wr(P, n) = Wr(P, n-1) \wr P^*$. By Remark V.58, for each $n > 0$, $Wr(P, n)$ acts on the set $Y^n = Y \times \cdots \times Y$ (n factors).

Fix $n > 0$. We find a convenient set of generators of $Wr(P, n)$ as follows. For notational convenience, identify Y^k with $Y^i \times Y^{k-i}$ for each $k = 2, \ldots, n$ and $i = 1, \ldots, k-1$. For $i = 1, \ldots, n$, define $r_i \in \mathrm{Sym}(Y^i)$ by $(\delta, j) \mapsto (\delta, j^\rho)$ for each $\delta \in Y^{i-1}$ and each $j \in Y$, and define $\rho_i \in \mathrm{Sym}(Y^n)$ by

$$(\delta, \lambda)^{\rho_i} = \begin{cases} (\delta^{r_i}, \lambda) & \text{where } \delta \in Y^i \text{ and } \lambda = (1, \ldots, 1) \in Y^{n-i} \\ (\delta, \lambda) & \text{where } \delta \in Y^i \text{ and } \lambda \neq (1, \ldots, 1) \in Y^{n-i} \end{cases}$$

The set $\Phi_n(\rho) = \{\rho_1, \ldots, \rho_n\}$ generates $Wr(P, n)$, by Remark V.58.3. We refer to $\Phi_n(\rho)$ as a set of *standard generators* for $Wr(P, n)$. Note that given Y^n, each permutation in $\Phi_n(\rho)$ may be found independently, so $\Phi_n(\rho)$ may be found in NC.

By Remark V.58.4, $|Wr(P, n)| = p^{p^{n-1} + \cdots + p + 1}$, which is the p-part of $(p^n)!$. Hence $Wr(P, n)$ is a Sylow p-subgroup of $\mathrm{Sym}(Y^n)$. To construct a Sylow p-subgroup of $\mathrm{Sym}(\Omega)$, write $|\Omega| = a_0 + a_1 p + \cdots + a_\nu p^\nu$ with $0 \leq a_i < p$ for each $i = 1, \ldots, \nu$. Let $\mathcal{C}$ be a collection of $a_0 + \cdots + a_\nu$ disjoint subsets of Ω such that a_l subsets have size p^l for $l = 0, \ldots, \nu$. Proceed as follows for each Λ in $\mathcal{C}$ in parallel. Suppose $|\Lambda| = p^l$. Let $\varphi : Y^l \to \Lambda$ be an arbitrary bijection, and identify Λ with Y^l via φ. Hence, for any $\sigma \in \mathrm{Sym}(Y^l)$, we obtain a permutation σ^φ of Λ given by

$$\delta \mapsto \delta^{\varphi^{-1} \sigma \varphi} \text{ for each } \delta \in \Lambda.$$

Then $Wr(P,l)^\varphi$ is a Sylow p-subgroup P_Λ of $\mathrm{Sym}(\Lambda)$. Moreover, if $\{\rho_1,\ldots,\rho_l\}$ is a set of standard generators for $Wr(P,l)$, then $\{\rho_1^\varphi,\ldots,\rho_l^\varphi\}$ is a set of generators of P_Λ. Given φ, this set may be found in NC.

Let $\hat{P}$ be the direct product of the groups P_Λ for each $\Lambda \in \mathcal{C}$. Note that $|\hat{P}|$ equals the p-part of $|\Omega|!$, so $\hat{P}$ is a Sylow p-subgroup of $\mathrm{Sym}(\Omega)$ (see [14], p. 82). Hence, the following is in NC:

Problem V.59 SYLFIND-SYM(Ω,p)

GIVEN: a set Ω and a prime p,

FIND: a Sylow p-subgroup of $\mathrm{Sym}(\Omega)$.

Suppose P is a Sylow p-subgroup of $\mathrm{Sym}(\Omega)$. If $p>2$, P is also a Sylow p-subgroup of $\mathrm{Alt}(\Omega)$, and if $p=2$, then $P\cap\mathrm{Alt}(\Omega)$ is a Sylow p-subgroup of $\mathrm{Alt}(\Omega)$. This intersection may be formed in NC since P normalizes $\mathrm{Alt}(\Omega)$ (Problem II.21). Hence the following problem is in NC:

Problem V.60 SYLFIND-ALT(Ω,p)

GIVEN: a set Ω and a prime p,

FIND: a Sylow p-subgroup of $\mathrm{Alt}(\Omega)$.

We now consider the problem of SYLCONJ for symmetric groups. We exploit our knowledge that a Sylow p-subgroup P of $\mathrm{Sym}(\Omega)$ is the direct product $\prod_{O\in\mathcal{O}} P^O$, where $\mathcal{O}$ is the set of orbits of P, and each P^O is isomorphic to a wreath product $Wr(P,i) = P^* \wr \cdots \wr P^*$ (i terms), for some $i \le \log_p|\Omega|$.

In the algorithm given above for finding a Sylow p-subgroup of $\mathrm{Sym}(\Omega)$, we identified subsets of Ω that are orbits of some Sylow p-subgroup, thereby reducing to the case where $|\Omega|$ is a p-power, say p^n. In that case, we noted that a Sylow p-subgroup is isomorphic to $Wr(P,n) = P^* \wr \cdots \wr P^*$ (n terms), which acts on the set

Y^n (see Remark V.58.5). Hence *any* bijection $\varphi : Y^n \to \Omega$ yields a Sylow p-subgroup $Wr(P,n)^\varphi$ of $\mathrm{Sym}(\Omega)$.

Now consider the following:

Problem V.61 SYLCONJ-SYM(Ω, P_1, P_2)

GIVEN: Sylow p-subgroups $P_1, P_2 \leq \mathrm{Sym}(\Omega)$,

FIND: an element g of $\mathrm{Sym}(\Omega)$ for which $P_1^g = P_2$.

The algorithm for Problem V.61 has an overall structure similar to the algorithm for Problem V.59. First, we reduce to the transitive case by finding $h \in \mathrm{Sym}(\Omega)$ that maps the set of orbits of P_1 to the set of orbits of P_2, replacing P_1 by P_1^h, and handling each orbit independently in parallel.

So we may assume P_1 and P_2 are transitive on Ω, where $|\Omega| = p^n$; we seek $g \in \mathrm{Sym}(\Omega)$ such that $P_1^g = P_2$. Our approach is to find two bijections $\varphi_j : Y^n \to \Omega$ with the property that $Wr(P,n)^{\varphi_j} = P_j$, for $j = 1, 2$. Finding such bijections suffices, since the permutation $g = \varphi_1^{-1}\varphi_2 \in \mathrm{Sym}(\Omega)$ satisfies $P_1^g = P_2$. Hence Problem V.61 is in NC by the following:

Lemma V.62 *Let $|\Omega| = p^n$, Let $Y = \{1, \ldots, p\}$, let ρ be a p-cycle in $Sym(Y)$, and let $Wr(P,n) \leq Sym(Y^n)$ be defined as above. Then given a Sylow p-subgroup P of $Sym(\Omega)$, a bijection $\varphi : Y^n \to \Omega$ for which $Wr(P,n)^\varphi = P$ can be found in NC.*

Proof: Let $\Phi_n(\rho) = \{\rho_1, \ldots, \rho_n\}$ be a set of standard generators for $Wr(P,n) \leq \mathrm{Sym}(Y^n)$. Find a system $\mathcal{D} = \{\Delta_1, \ldots, \Delta_p\}$ of blocks for P (Problem II.12; each block of size p^{n-1}), and find an element σ_n of P that induces a p-cycle in $\mathrm{Sym}(\mathcal{D})$. Relabel the elements of $\mathcal{D}$, if necessary, so that σ_n induces the permutation given by $\Delta_i \mapsto \Delta_{i\rho}$. $P_{\{\Delta_1\}}^{\Delta_1}$ is isomorphic to $Wr(P, n-1)$. Recursively, label each point $v \in \Delta_1$ with an $(n-1)$-tuple in Y^{n-1} so that $Wr(P, n-1)$ induces $P_{\{\Delta_1\}}^{\Delta_1}$ via

the identification of each point in Δ_1 with its label; furthermore, this identification associates the set of standard generators $\Phi_{n-1}(\rho) = \{\rho_1, \ldots, \rho_{n-1}\}$ of $Wr(P, n-1)$ with a set of generators $\{\sigma_1, \ldots, \sigma_{n-1}\}$ of $P^{\Delta_1}_{\{\Delta_1\}}$. For each point $v \in \Delta_1$, suppose the label of v is $\delta \in Y^{n-1}$; relabel v as as $(\delta, 1)$. For each $j = 1 \ldots, p-1$ in parallel, and for each $(\delta, 1) \leq \Delta_1$ in parallel, label $(\delta, 1)^{\rho^j} \in \Delta_{1\rho^j}$ as $(\delta, 1^{\rho^j})$. Note that ρ_n induces σ_n on $\mathcal{D}$, but not on Ω. Let τ be the permutation in $\mathrm{Sym}(\Omega)$ that fixes pointwise $\Omega \setminus \Delta_1$ and $\tau^{\Delta_1} = (\sigma_n^p)^{\Delta_1}$. Note that $\sigma_n^p \in P_{\Delta_1} \times \cdots \times P_{\Delta_p}$, the subgroup of P that stabilizes each block in $\mathcal{D}$. Hence $(\sigma_n^p)^{\Delta_1} = \tau^{\Delta_1} \in P_{\Delta_1}$. Replace σ_n by $\sigma_n\tau^{-1}$. Now σ_n^p is the identity on Ω. Hence $Wr(P, n)^\varphi = \langle Wr(P, n-1)^\varphi, \rho_n^\varphi \rangle = \langle P_{\{\Delta_1\}}, \sigma_n \rangle = P$, so this labelling of Ω provides a desired bijection.

This procedure is in NC because the depth of the recursion is $n = O(\log |\Omega|)$. □

Let p be an odd prime. Suppose P_1 and P_2 are two Sylow p-subgroups of $\mathrm{Alt}(\Omega)$, and hence of $\mathrm{Sym}(\Omega)$. The above algorithm for SYLCONJ-SYM is inadequate for finding an element in $\mathrm{Alt}(\Omega)$ that conjugates P_1 to P_2, since the permutation g returned by SYLCONJ-SYM may be odd. We therefore show how to construct an odd permutation h that normalizes P_2, so that the product gh is odd and satisfies $P_1^{gh} = P_2$. Our approach will be to find an odd permutation that normalizes the group generated by a single p-cycle in P_2, and to use the wreath product structure of P_2 to obtain a permutation that normalizes P_2.

Let P be a Sylow p-subgroup of $\mathrm{Sym}(\Omega)$ (p odd), $|\Omega| = p^n$. To find an odd permutation that normalizes P, it suffices to find an odd permutation h that normalizes $Wr(P, n)$ on Y^n by Lemma V.62, since if φ be a bijection from $Y^n \to \Omega$ for which $Wr(P, n)^\varphi = P$, then h^φ is an odd permutation of Ω that normalizes P. Let $Y = \{1, \ldots, p\}$, and let ρ be a p-cycle in $\mathrm{Sym}(Y)$. Recall that $r_i \in \mathrm{Sym}(Y^i)$ is

defined by $(\delta, j) \mapsto (\delta, j^{\rho})$ for each $\delta \in Y^{i-1}$ and each $j \in Y$, and that ρ_i is defined to act on Y^n by

$$(\delta, \lambda)^{\rho_i} = \begin{cases} (\delta^{\tau_i}, \lambda) & \text{where } \delta \in Y^i \text{ and } \lambda = (1, \ldots, 1) \in Y^{n-i} \\ (\delta, \lambda) & \text{where } \delta \in Y^i \text{ and } \lambda \neq (1, \ldots, 1) \in Y^{n-i} \end{cases}$$

For each $\delta = (\delta_2, \ldots, \delta_n) \in Y^{n-1}$, let s_δ be the p-cycle $\rho_1^{\rho_2^{\delta_2} \cdots \rho_n^{\delta_n}}$, and let $N = \langle s_\delta \mid \delta \in Y^{n-1} \rangle$. Note that ρ_δ is a p-cycle on the set $C_\delta = \{(i, \delta) \mid i \in Y\}$, for each $\delta \in Y^{n-1}$. The sets C_δ, for $\delta \in Y^{n-1}$, comprise a collection of p^{n-1} pairwise disjoint subsets of Y^n, each of size p. Hence N is an elementary abelian p-subgroup of $Wr(P, n)$ of order $p^{p^{n-1}}$. Each of $\rho_2, \ldots, \rho_n$ acts on the set $\{s_\delta \mid \delta \in Y^{n-1}\}$, so $N \lhd Wr(P, n)$.

Let h be a permutation in $\mathrm{Sym}(Y)$ that normalizes $\langle \rho \rangle$ so that $\rho^h = \rho^j$ for some $j = 1, \ldots, p-1$. Define h_δ analogously, i.e., let $h_\delta = h^{\rho_2^{\delta_2} \cdots \rho_n^{\delta_n}}$; note that h_δ induces h on C_δ, and the identity on C_β for $\beta \neq \delta$. Let $\hat{h}$ be the product of such h_δ, i.e., $\hat{h} = \prod_{\delta \in Y^{n-1}} h_\delta$. Then $\hat{h}$ normalizes N because it normalizes each $\langle s_\delta \rangle$; furthermore, $\hat{h}$ normalizes $Wr(P, n)$ because it normalizes $\langle \rho_1 \rangle$ and it centralizes each $\rho_2, \ldots, \rho_n$. If h is an odd permutation, then so is $\hat{h}$. Hence it suffices to find an such an h that is odd.

Suppose two permutations α, β each consist of a single n-cycle, i.e., $\alpha = (a_1, \ldots, a_n)$ and $\beta = (b_1, \ldots, b_n)$. A permutation h for which $\alpha^h = \beta$ can be found easily: let h be a permutation that maps a_i to b_i for each $i = 1, \ldots, n$. Then $h^{-1} \alpha h = \beta$. Thus, to determine an odd permutation $h \in \mathrm{Sym}(Y)$, that normalizes $P^* = \langle \rho \rangle$, for each $l = 2, \ldots, p-1$ in parallel, let $h_l \in \mathrm{Sym}(Y)$ satisfy $\rho^{h_l} = \rho^l$. One such h_l is an odd permutation (in fact, half are), since $\mathrm{Sym}(Y) = \mathrm{Alt}(Y) N_{Sym(Y)}(P^*)$, by the Frattini argument.

We have proved

Lemma V.63 *Given an odd prime p and a Sylow p-subgroup P of $Sym(\Omega)$, an odd permutation $\sigma \in Sym(\Omega)$ that normalizes P can be found in NC.*

We now have the tools to describe an NC algorithm for the following:

Problem V.64 SYLCONJ-ALT(Ω, P_1, P_2)

GIVEN: Sylow p-subgroups $P_1, P_2 \leq \mathrm{Alt}(\Omega)$,

FIND: an element g of $\mathrm{Alt}(\Omega)$ for which $P_1^g = P_2$.

If $p = 2$, and P_1, P_2 are Sylow p-subgroups of $\mathrm{Alt}(\Omega)$, then, for $j = 1, 2$, find Sylow p-subgroups P_j^* of $\mathrm{Sym}(\Omega)$ with $P_j < P_j^*$ as follows. For $j = 1, 2$, find a minimal block Δ_j for P_j, let s_j be the permutation that transposes the two points of Δ_j and fixes all other points in Ω, and set $P_j^* = \langle P_j, s_j \rangle$.

Let $g = \text{SYLCONJ-SYM}(\Omega, P_1^*, P_2^*)$ (Problem V.61). If g is an odd permutation, then let h be a generator of P_2^* that is an odd permutation, and replace g by gh. Note that both P_1^g and P_2 are Sylow p-subgroups of $\mathrm{Alt}(\Omega)$ that are contained in $\mathrm{Alt}(\Omega) \cap P_2^*$, but $\mathrm{Alt}(\Omega) \cap P_2^* = P_2$, so $P_1^g = P_2$, hence we may return g.

If $p > 2$, P_1 and P_2 are Sylow p-subgroups of $\mathrm{Sym}(\Omega)$, so we can find $g = \text{SYLCONJ-SYM}(\Omega, P_1, P_2)$. If g is odd, let k be an odd permutation that normalizes P_2 (Lemma V.63), and replace g by gk. Return g.

Sylow Subgroups of Small Groups

For a group $G = \langle \mathcal{S} \rangle \leq \mathrm{Sym}(\Omega)$ where $|G| < |\Omega|^c$ for some constant c, there are brute force algorithms for finding and conjugating Sylow subgroups of G. The elements of such a group G can be enumerated in NC: Let $\mathcal{S}_1 = \mathcal{S} \cup \{1\}$, and proceed in a succession of rounds; in the i-th round, let $\mathcal{S}_i$ be the set obtained by forming the set of products $\{gh \mid g, h \in \mathcal{S}_{i-1}\}$ (the set of products of elements of $\mathcal{S}$ of length

less than or equal 2^i), and removing duplicate permutations. This process ends after $\log_2 |G|$ rounds, since every element in G can be expressed by a word in S of length no greater than $|G|$ (an upper bound on the diameter of the Cayley graph of G formed with S).

The following two procedures exploit the NC enumerability of polynomially sized groups. Each procedure is correct by construction and in NC because $|G|$ is polynomial in $|\Omega|$.

Problem V.65 SYLFIND-SMALL(G, Ω, p)

GIVEN: $G = \langle S \rangle \leq \mathrm{Sym}(\Omega)$ where $|G| < |\Omega|^c$ for some constant c, and a prime p,

FIND: a Sylow p-subgroup of G.

Procedure for Problem V.65:
enumerate G
let $P = \{1\}$
while possible (sequentially)
  choose $g \in G \setminus P$ of p-power order that normalizes P
  {test all such elements in parallel }
  $P \leftarrow \langle P, g \rangle$
return P $\diamond$

Problem V.66 SYLCONJ-SMALL(G, Ω, P_1, P_2)

GIVEN: Sylow p-subgroups P_1, P_2 of $G \leq \mathrm{Sym}(\Omega)$, where $|G| < |\Omega|^c$ for some constant c,

FIND: an element g of $\mathrm{Sym}(\Omega)$ for which $P_1^g = P_2$.

Procedure for Problem V.66:
enumerate G
for each $g \in G$ **in parallel**
  test if $P_1^g = P_2$ (Problem II.1)
return one such successfully tested g $\diamond$

Coordinatization

Earlier in this chapter, we obtained an action of classical simple group G on a set Y that is permutation-isomorphic to a natural action of G on a projective $(n-1)$-space over a finite field F. The set of points of this projective space is the set $\overline{V}$ of 1-spaces of an associated n-dimensional vector space V. We now make this permutation-isomorphism explicit by assigning to each point in Y the coordinates of a vector in V (relative to some basis), so that the action of G on $\overline{V}$ induces the given action of G on Y. For example, if $G \cong PSL(n,q)$, then Y is identified with $\overline{V}$ where $V \cong F_q^n$, such that the action of $PSL(n,q)$ on $\overline{V}$ induces the action of G on Y. Such coordinates are "homogeneous coordinates"; for each point, we choose an appropriate scalar multiple so that the last nonzero coordinate of is 1.

Definition V.67 *Let $(G,Y) \in \mathcal{G}$. A* coordinatization *of Y is a function $f : Y \rightarrow F^n$ that associates to each point $y \in Y$ a vector $f(y) \in F^n$, such that the induced map $y \mapsto \langle f(y) \rangle$ is an isomorphism of the projective spaces Y and $\overline{F^n}$, i.e., it preserves collinearity (collinearity in Y is via Problem V.41).*

Remark V.68 In subsequent problems, $\overline{V}$ or V appear as parameters. The reader should bear in mind that $\overline{V}$ and V arose from a coordinatization of some $(G,Y) \in \mathcal{G}$ (Problem V.69). The action of G on Y remains available, if implicit, since Y and $\overline{V}$ are identified. Hence, an element (resp. subgroup) of $G^{\overline{V}}$, in effect, *is* an element (resp. subgroup) of G^Y. Moreover, an element (resp. subgroup) of G^V induces an element (resp. subgroup) of $G^{\overline{V}}$, and hence of G^Y. (See SYLFIND-SIMPLE Problem V.135, and SYLCONJ-SIMPLE Problem V.148).

Problem V.69 COORDINATIZE(Y, G)

GIVEN: $(G, Y) \in \mathcal{G}$

FIND: a vector space V and a coordinatization $f : Y \to V$.

Procedure for Problem V.69:

let $\{x_1, \ldots, x_n\}$ = FIND-INDEPENDENT-SET(G, Y) (Problem V.47)

{ $\{x_1, \ldots, x_n\}$ is maximal such that $x_{i+1} \notin W_i = [x_1, \ldots, x_i]$, for $i = 1, \ldots, n-1$ }

let u be a point of W_3 not on any of the lines $[x_1, x_2]$, $[x_1, x_3]$, or $[x_2, x_3]$
(Definition V.39 and Problem V.41)

let F be a set of size $|[x_3, u]| - 1$

let t be an arbitrary bijection from $[x_3, u] - (W_2 \cap [x_1, x_2])$ to F

for each point p of $[x_3, u] - (W_2 \cap [x_1, x_2])$ **in parallel**

label p as $(t(p), t(p), 1)$

define $0 = \alpha \in F$ where x_3 has been labeled above as $(\alpha, \alpha, 1)$

define $1 = \beta \in F$ where u has been labeled above as $(\beta, \beta, 1)$

label x_1 as $(1, 0, 0)$ and x_2 as $(0, 1, 0)$

{ we may view $[x_1, x_2]$ as the line at infinity of the projective plane W_3, x_3 as the "origin," $[x_1, x_3]$ as the "x-axis", $[x_2, x_3]$ as the "y-axis," and $[x_3, u]$ as the line "$x = y$;" we have labeled the (finite) points of the line $x = y$ and points at infinity of the $x-$ and $y-$axes }

{ label the $x-$ and y-axes }

for each point $p_a = (a, a, 1) \in [x_3, u]$ **in parallel**

label the point $[x_1, x_3] \cap [p_a, x_2]$ as $(a, 0, 1)$

label the point $[x_2, x_3] \cap [p_a, x_1]$ as $(0, a, 1)$

{ label the remaining "finite" points of W_3 }

for each point $p \in W_3 \setminus [x_1, x_2]$ **in parallel**

label p as $(a, b, 1)$

where $[p, x_2] \cap [x_1, x_3] = (a, 0, 1)$ and $[p, x_1] \cap [x_2, x_3] = (0, b, 1)$

{ now label the points on the "line at infinity" }

for each point $p = (a, 1, 1) \in [x_1, u] - \{x_1\}$ **in parallel**

label $[x_3, p] \cap W_2$ as $(a, 1, 0)$

{ now define field operations on F consistent with the geometry of W_3 }
for each pair $a, b \in F$ **in parallel**
  define $a + b = c_2$ where $(c_1, c_2, 1) = [(0, b, 1), (1, 1, 0)] \cap [(a, a, 1), x_2]$
for each pair $a, b \in F$ **in parallel**
  define $a * b = 0$ if a or b is 0, otherwise
  define $a * b = c_2$ where $(c_1, c_2, 1) = [x_3, (1, a, 1)] \cap [x_2, (b, 0, 1)]$
{ coordinatize W_i, $i = 4, \ldots, n-1$, sequentially }
for $i = 4, \ldots, n-1$ **(sequentially)** (*)
{assume points of W_i are labeled with i-tuples with last nonzero coordinate 1}
  relabel each point $y = (a_1, \ldots, a_i) \in W_i$) as the $i+1$-tuple $(a_1, \ldots, a_i, 0)$
  label x_{i+1} as $(0, \ldots, 0, 1)$
  { it is helpful to consider W_i as the "hyperplane at infinity" of W_{i+1},
    and x_{i+1} as the "origin" of W_{i+1}. }
  let u be any point on $[x_{i+1}, (1, \ldots, 1, 0)]$ other than x_{i+1} or $(1, \ldots, 1, 0)$
  label u as $(1, \ldots, 1)$
  for each unlabeled point $x \in W_{i+1} \setminus [x_{i+1}, u]$ **in parallel**
      label it as follows:
    find $y = (a_1, \ldots, a_i, 0) = [x, x_{i+1}] \cap W_i$
    find $z = (b_1, \ldots, b_i, 0) = [x, u] \cap W_i$
    find $c_1, c_2 \in F$ such that $z = c_1 y + c_2 u_i$ (where $u_i = (1, \ldots, 1, 0)$)
      (by brute force, since $|F|$ is small)
    $h \leftarrow -c_1/c_2$ ($c_2 \neq 0$ since $x \notin [x_{i+1}, u]$)
    label x as $(ha_1, \ldots, ha_i, 1)$
    { $z = (ha_1 - 1, \ldots, ha_i - 1, 0)$, so $(ha_1, \ldots, ha_i, 1)$ is on *both* $[u, z]$ *and*
    $[x_{i+1}, y]$, so it must be the unique point of intersection of these two
    lines, namely, x }
  for each unlabeled point $x \in [x_{i+1}, u]$ **in parallel**
    find $y = (a+1, a, \ldots, a, 1) = [x_1, x] \cap [(1, 0, \ldots, 0, 1), u_i]$
    label x as $(a, \ldots, a, 1)$
let $f : Y \to F^n$ be the function that maps each $y \in Y$ to the n-tuple with which it has been labelled
return $V = F^n$ and f $\diamond$

Lemma V.70 *COORDINATIZE is correct and in NC.*

Proof: COORDINATIZE is correct by construction. See [17], Proposition 11.1 and also [14], Sect.20.3, p.353.

By Lemma V.38, $\dim(V)$ is logarithmic in $|Y|$. Hence, the one sequential loop (line (*) in the procedure above) has a logarithmic number of iterations. □

COORDINATIZATE (Problem V.69), leads to the following:

Remark V.71 In subsequent problem statements, the phrases "given a vector space V" and "given $(G^*, V) \in \mathcal{G}^*$" (Definition V.31) mean that we are given all of the following:

1. the characteristic and size of a field F over which V is constructed,
2. the set of elements of F, together with addition and multiplication tables for F,
3. the dimension n of V over F,
4. the set of vectors in V, together with scalar multiplication and vector addition tables for V.

Also, the phrases "given a form ϕ on V" or "given $(G^*, V, \phi) \in \mathcal{G}^*$" (Definition V.31*) mean, in addition to the above,

5. a complete table of values $\phi(u, v)$ for all $u, v \in V$ (or $\phi(v)$ for all $v \in V$ if ϕ is a quadratic form).

Finding $G^* \leq SL(V)$ that Induces G on $\overline{V}$

Recall from Definition V.31 that $\mathcal{G}$ denotes the set of pairs (G, X) where G is a classical simple group acting on X in its natural action, and $\mathcal{G}^*$ denotes the set of

pairs (G^*, V) where $G^* = G^{*\prime} \leq SL(V)$ and $(G^{*\overline{V}}, \overline{V}) \in \mathcal{G}$, where $G^{*\overline{V}}$ is the group G^* induces on $\overline{V}$.

If $(G, \overline{V}) \in \mathcal{G}$, there exists a unique group $G^* \leq SL(V)$ such that $(G^*, V) \in \mathcal{G}^*$ and G^* induces G on $\overline{V}$. In particular, if $G = PSL(V)$, $PSp(V)$, $PSU(V)$, or $P\Omega(V)$, then $G^* = SL(V)$, $Sp(V)$, $SU(V)$, or $\Omega(V)$, respectively. (Recall that $\dim(V) > 8$ by Remark V.32, so we never consider nonsimple groups such as $Sp(4,2)$ and $SU(3,2)$.)

Since the elements of the group G^* are linear transformations which act on a vector space V, while G is isomorphic to the quotient group $G^*/Z(G^*)$, it is more natural to work with the group G^*. We will compute a Sylow subgroup P^* of G^* in the action of G^* on V, then obtain the group P^* that induces a Sylow p-subgroup P of G in the action of G on $\overline{V}$ (and hence on Y, since Y and $\overline{V}$ are identified by COORDINATIZE). This induced group $(P^*)^{\overline{V}}$ is a Sylow subgroup of G.

Given generators for $G \leq \mathrm{Sym}(\overline{V})$, we show in this section how to find generators for $G^* \leq SL(V)$ and find, for each element $g \in G$, an element $g^* \in G^*$ that induces g on $\overline{V}$.

Lemma V.72 *Given a vector space V and $(G, \overline{V}) \in \mathcal{G}$, we can find a basis for V in NC.*

Proof: Selecting one nonzero vector from each of the 1-spaces found by FIND-INDEPENDENT-SET$(G, \overline{V})$ (Problem V.47) yields a basis of V. □

The following two lemmas describe how we can translate between linear transformations on V and the permutations of $\overline{V}$ they induce.

Lemma V.73 *Let $T \in GL(V)$. If we are given the matrix $[T]_{\mathcal{B}}$ of T with respect to a basis $\mathcal{B}$, then we can compute in NC the action of T on V and the action induced*

by T on $\overline{V}$.

Proof: For each $v \in V$ in parallel, compute $[Tv]_{\mathcal{B}} = [T]_{\mathcal{B}}[v]_{\mathcal{B}}$, where $[v]_{\mathcal{B}}$ denotes the coordinate (column) vector of v with respect to $\mathcal{B}$. This suffices for the actions of T on both V and $\overline{V}$—knowing Tv implies knowing $\langle Tv \rangle$. This is in NC by Remark V.37. □

Lemma V.74 *Suppose $g \in Sym(\overline{V})$ and there exists some linear transformation $T \in GL(V)$ that induces g on $\overline{V}$. A matrix $[T]_{\mathcal{B}}$ for T with respect to a given basis $\mathcal{B} = \{v_1, \ldots, v_n\}$ can be computed in NC.*

Proof: Suppose $T \in GL(V)$ induces the same permutation in $\mathrm{Sym}(\overline{V})$ as g. For each $v_j \in \mathcal{B}$, choose a vector in the 1-space $\langle v_j \rangle^g$ and write it as a linear combination $\sum_i a_{ij} v_i$ of the basis vectors in $\mathcal{B}$. T must map v_j to some nonzero scalar multiple, say $c_j(\sum_i a_{ij} v_i)$, of this linear combination. There are only $(|F| - 1)^n = |V|$ choices for $c_1, \ldots, c_n$. For each such choice in parallel, test if the matrix $(c_j a_{ij})$ induces the permutation g on $\overline{V}$. The element g is induced by *some* linear transformation, hence for *some* choice of scalars, so one of these tests must succeed, say for scalars $c'_1, \ldots, c'_n$. Then the matrix $(c'_j a_{ij})$ induces g. □

The following problem, TRANSLATE-ELT is in NC by Lemma V.74. It is used by TRANSLATE-GROUP.

Problem V.75 TRANSLATE-ELT$(g, \overline{V}, V, \mathcal{B})$

GIVEN: an element $g \in \mathrm{Sym}(\overline{V})$ induced by a linear transformation in $GL(V)$; a basis $\mathcal{B} = \{v_1, \ldots, v_n\}$ for V,

FIND: the matrix with respect to $\mathcal{B}$ of a linear transformation that induces g on $\overline{V}$ (such a linear transformation is unique up to a scalar).

An analogous lemma for Sym(V) is even more straightforward.

Lemma V.76 *Suppose $g^* \in Sym(V)$ and there exists some linear transformation $T \in GL(V)$ that induces g^* on V. The matrix $[T]_{\mathcal{B}}$ for T with respect to a given basis $\mathcal{B} = \{v_1, \ldots, v_n\}$ can be computed in NC.*

Proof: Express each $v_i^{g^*}$ as a linear combination $\sum_j a_{ij} v_j$ (an NC computation). Then $T = (a_{ij})$. □

Lemma V.77 *Let $T \in GL(V)$. We can determine in NC whether or not T induces the same permutation on $\overline{V}$ as some element of a given group $G \leq GL(V)$.*

Proof: Determine the permutation in Sym($\overline{V}$) induced by T. Apply MEMBER (Problem II.1). □

Problem V.78 TRANSLATE-GROUP($G, \overline{V}, V, \mathcal{B}$)

GIVEN: a basis $\mathcal{B}$ of a vector space V, $(G, \overline{V}) \in \mathcal{G}$, and $G = \langle A \rangle$,

FIND: matrices, relative to $\mathcal{B}$, of generators for the group G^* for which $(G^*, V) \in \mathcal{G}^*$ and G^* induces G on $\overline{V}$.

Procedure for Problem V.78:
for each generator g of G **in parallel**
  $T_g \leftarrow$ TRANSLATE-ELT($g, \overline{V}, V, \mathcal{B}$) (Problem V.75)
  $t_g \leftarrow (T_g)^V$ { the permutation in Sym(V) induced by the matrix T_g }
    (Lemma V.73)
$G^* \leftarrow$ COMMUTATOR($\langle t_g \mid g \in A \rangle$) (Problem II.16)
{ use permutation action on V (Lemma V.73) }
for each generator g of G^* **in parallel**
  let M_g be the matrix with respect to $\mathcal{B}$ that induces g on V (Lemma V.76)
return $\{M_g \mid g$ a generator of $G^*\}$ ◇

Lemma V.79 *TRANSLATE-GROUP is correct and in NC.*

Proof: Let Q be the kernel of the action of G^* on $\overline{V}$. If $G^{*\prime} \leq Q$, then $G^{*\prime}$ acts trivially on $\overline{V}$. This is impossible, however, since G^*/Q is simple and acts faithfully on $\overline{V}$. Hence $1 < G^{*\prime}Q/Q \trianglelefteq G^*/Q \cong G$, so $G^* = G^{*\prime}$. This procedure is in NC since the procedures it invokes are in NC. □

Problem V.80 TRANSLATE-p-GROUP$(P, G, \overline{V}, V, \mathcal{B})$

GIVEN: a vector space $V = F^n$, and a Sylow p-subgroup $P = \langle S \rangle$ of G where $(G, \overline{V}) \in \mathcal{G}$, and a basis $\mathcal{B}$ of V,

FIND: matrices, relative to $\mathcal{B}$, of generators for the Sylow p-subgroup P^* of G^* that induces P on $\overline{V}$, where $(G^*, V) \in \mathcal{G}^*$ and G^* induces G on $\overline{V}$.

Procedure for Problem V.80:
let $|F| - 1 = ap^r$, where $(a, p) = 1$
let $t \in F$ have order p^r (Problem II.15; test all t in parallel)
$\Psi \leftarrow \{\text{TRANSLATE-ELEMENT } (s^{\overline{V}}, \overline{V}, V, \mathcal{B})^a \mid s \in S\}$
return $P^* = \langle \Psi, tI \rangle$ ◇

Lemma V.81 *TRANSLATE-p-GROUP is correct and in NC.*

Proof: Let $G^* = \text{TRANSLATE-GROUP}(G, \overline{V}, V, \mathcal{B})$. P^* is the largest p-subgroup of G^* that induces P on $\overline{V}$. The element $r = \text{TRANSLATE-ELEMENT}(s^{\overline{V}}, \overline{V}, V, \mathcal{B})$ $\in G^*$ induces an element of P for each $s \in S$; hence $\Psi \subseteq P^*Z$. But P^*Z is nilpotent, so $P^*Z = P^* \times Q$ for some $Q \leq Z$ where $|Q|$ divides a. Hence $r^a \leq P^*$, and so $\Psi \subseteq P^*$. If p divides $|Z|$, $P^* \cap Z$ is a nontrivial Sylow p-subgroup of Z. Z is abelian (in fact, cyclic), so it has a unique cyclic Sylow p-subgroup, generated by tI. Hence, $P^* = \langle \Psi, tI \rangle$. TRANSLATE-$p$-GROUP is in NC since the procedures it invokes are in NC. □

Having shown how to construct $(G^*, V) \in \mathcal{G}^*$, given $(G, \overline{V}) \in \mathcal{G}$, for which G^* induces G on $\overline{V}$ and $G^{*\prime} = G^*$ (Problem V.78), we will have occasion to find $\langle S \rangle$ and

$S^\perp$, given any $S \subseteq V$. We have already given algorithms for analogous problems stated in terms of points in $\overline{V}$ (Problems V.45 and V.53); we recast these problems here in terms of vectors in V.

Problem V.82 SPAN-VECTORS$(G^*, V, \mathcal{A})$

GIVEN: $(G^*, V) \in \mathcal{G}$ and $\mathcal{A} \subseteq V$,

FIND: the set of vectors in $\langle \mathcal{A} \rangle$.

Lemma V.83 *SPAN-VECTORS is in NC.*

Proof: Let $A = \{\langle a \rangle \mid a \in \mathcal{A}\}$, let A^* = SPAN-POINTS$(G^{*\overline{V}}, \overline{V}, A)$ (Problem V.45; in NC by Lemma V.46), and return the set of vectors in the collection of 1-spaces A^*. □

Problem V.84 PERP-VECTORS$(G^*, V, \mathcal{A})$

GIVEN: $(G^*, V) \in \mathcal{G}^*$, $G^* \ncong SL(V)$, and a set $\mathcal{A} \subseteq V$,

FIND: $\mathcal{A}^\perp$.

Lemma V.85 *PERP-VECTORS is in NC.*

Proof: Let $A = \{\langle a \rangle \mid a \in \mathcal{A}\}$, let A^* = PERP-POINTS$(G^{*\overline{V}}, \overline{V}, A)$ (Problem V.53; in NC by Lemma V.54), and return the set of vectors in the collection of 1-spaces A^*. □

Constructing Bilinear and Quadratic Forms

The SYLFIND-CLASSICAL and SYLCONJ-CLASSICAL procedures invoke the procedure CONSTRUCT-FORM to obtain a bilinear or hermitian form on V. If V is an orthogonal space over a field of characteristic 2, CONSTRUCT-FORM returns a pair of forms, one bilinear and one quadratic. In that case, recall (Definition

V.14) that the bilinear form ϕ is determined by the quadratic form Q via

$$\phi(u,v) = Q(u+v) - Q(u) - Q(v). \qquad (*)$$

In the remainder of this chapter, the phrases "given a form ϕ" and "given $(G^*, V, \phi) \in \mathcal{G}^*$ mean a complete table of values $\phi(u,v)$ (or $\phi(v)$ if ϕ is quadratic) for all $u, v \in V$ (Remark V.71). Furthermore, all forms considered are nonsingular or 0.

If G is a classical group, there is a form used in the definition of G. Forms are used chiefly to construct isometries (e.g., in MATCH-BASES, Problem V.100) and to test whether a given linear transformation is an isometry (e.g., in procedure SYLCONJ-IRRED-CYCLIC, Problem V.136). As we have seen in Problem V.84, given any vector v or subspace U, we can form $v^\perp$ and $U^\perp$ without the aid of forms. Similarly, we may test whether a vector v is isotropic or singular without the use of forms by testing if $v \in v^\perp$. Also, we may test whether a subspace U is totally isotropic by testing if $U \leq U^\perp$. If G is orthogonal and the characteristic is 2, we may use the quadratic form to test if a vector v is singular ($Q(v) = 0$), since possibly $Q(v) = 0$ while $\phi(v,v) \neq 0$ where ϕ is defined from Q as in (*) above. Note, however, that we have already obtained the the orbit of isotropic or singular vectors, since v is isotropic or singular if $\langle v \rangle$ is in the unique G-orbit on $\overline{V}$ of size relatively prime to the characteristic of V, which is the set Y' constructed in the procedure NATURAL-ACTION (Problem V.35).

Remark V.86 In the problem statements of several of the following procedures, the phrase "a form ϕ" will indicate either a bilinear (or Hermitian) form defined on $V \times V$, or a quadratic form, in the case that the group is orthogonal and the characteristic of the underlying field is 2. In the latter case, the associated bilinear

form (needed, for example, by MATCH-BASES) may be obtained directly from the quadratic form via (*). Granting this minor ambiguity permits a considerable simplification of notation and obviates the need to explicitly repeat this remark in each relevant problem statement.

Problem V.87 CONSTRUCT-FORM(G^*, V)

GIVEN: $(G^*, V) \in \mathcal{G}^*$ (Definition V.31), where V is a vector space over a field F,

FIND: a bilinear or Hermitian form on V preserved by G^* (nonsingular, unless $G^* \cong SL(V)$), and in addition, a quadratic form preserved by G^* if G^* is orthogonal and $char(V) = 2$; i.e., a form ϕ such that $(G^*, V, \phi) \in \mathcal{G}^*$) as in Definition V.31*.

Procedure for Problem V.87:
if $G^* \cong SL(V)$ **then return** the 0-form
else
  if G^* is orthogonal **and** $char(V) = 2$ **then**
    return CONSTRUCT-QUAD-FORM(G^*, V) and
      the induced bilinear form (Problem V.89)
  else
    $\mathcal{O} \leftarrow$ the unique G^*-orbit on $\overline{V}$ of size relatively prime to $char(V)$
    { $\mathcal{O}$ is the set of isotropic or singular points of $\overline{V}$ }
    choose $u_1, v_1 \in \mathcal{O}$ where $u_1 \notin v_1^{\perp}$ (Problem V.51)
    choose a vector e_1 in the 1-space u_1 and a vector f_1 in the 1-space v_1
    $H_1 \leftarrow \langle e_1, f_1 \rangle$ (Problem V.82)
    { define ϕ on $H_1 = \langle e_1, f_1 \rangle$ }
    let $\phi(e_1, e_1) = \phi(f_1, f_1) = 0,\ \phi(e_1, f_1) = 1$
    if G is symplectic **then**
      let $\phi(f_1, e_1) = -1$ **else let** $\phi(f_1, e_1) = 1$

choose $(e_2, f_2) \in (e_1, f_1)^{G^*} \cap (H_1^\perp \times H_1^\perp)$ (Problems II.5, V.84)
$H_2 \leftarrow \langle e_1, f_1, e_2, f_2 \rangle$ (Problem V.82)
{ extend by bilinearity (or sesquilinearity if G unitary) to H_2 }
for each pair $u = a_1e_1 + b_1f_1 + a_2e_2 + b_2f_2$ **and**
$v = c_1e_1 + d_1f_1 + c_2e_2 + d_2f_2$ $(a_i, b_i, c_i, d_i \in F)$ **in parallel**
if G^* is orthogonal **then let** $\phi(u, v) = a_1d_1 + b_1c_1 + a_2d_2 + b_2c_2$
if G^* is symplectic **then let** $\phi(u, v) = a_1d_1 - b_1c_1 + a_2d_2 - b_2c_2$
if G^* is unitary **then let** $\phi(u, v) = a_1d_1 + b_1\bar{c}_1 + a_2d_2 + b_2\bar{c}_2$
{ in particular, $\phi(e_2, f_2) = \phi(e_1, f_1)$ and $\phi(f_2, e_2) = \phi(f_1, e_1)$,
and $\phi(e_2, e_2) = \phi(f_2, f_2) = \phi(e_1, f_2) = \phi(e_2, f_1) = 0$ }
for each $(u, v) \in V \times V$ **in parallel**
$\Delta \leftarrow (u, v)^{G^*} \cap (H_2 \times H_2)$ (Problem II.5; G^* acts on $V \times V$)
let $\phi(u, v) = \phi(e, f)$ for any $(e, f) \in \Delta$
return ϕ $\diamond$

Lemma V.88 *CONSTRUCT-FORM is correct and in NC.*

Proof: Every G^*-orbit of pairs of $(u, v) \in V \times V$ meets $H_2 \times H_2$ ([32] pp. 138-139), so this procedure computes $\phi(u, v)$ for each $(u, v) \in V \times V$. Moreover, G^* preserves the form ϕ by construction (cf. [17], Lemma 13.1). The algorithm is in NC since PERP-VECTORS (Problem V.84) is in NC, and since we may consider all $|V|^2$ pairs $(u, v) \in V \times V$ in parallel. □

Problem V.89 CONSTRUCT-QUAD-FORM(G^*, V)

GIVEN: $(G^*, V) \in \mathcal{G}^*$ with G^* orthogonal, $char(V) = 2$, and $\dim(V)$ even,

FIND: a quadratic form on V preserved by G^*.

Procedure for Problem V.89:
$\mathcal{O} \leftarrow$ the unique G^*-orbit on $\overline{V}$ of odd size $\{\mathcal{O}$ is the set of singular 1-spaces of $V\}$
choose $u_1, v_1 \in \mathcal{O}$ where $u_1 \notin v_1^\perp$ (Problem V.51)
choose $e_1, f_1 \in V$ where $e_1 \in u_1$ and $f_1 \in v_1$
$H_1 \leftarrow \langle e_1, f_1 \rangle$ (Problem V.82)
{ define ϕ on H_1 }
for each $u = a_1 e_1 + b_1 f_1 \in H_1$
  let $\phi(u) = a_1 b_1$ { in particular, this implies $\phi(e_1) = \phi(f_1) = 0$ }
{ extend to all of V }
for each $v \in V$ **in parallel**
  $\Delta \leftarrow v^{G^*} \cap H_1$
  let $\phi(v) = \phi(u)$ for any $u \in \Delta$
return ϕ $\diamond$

Lemma V.90 *CONSTRUCT-QUAD-FORM is correct and in NC.*

Proof: Every G^*-orbit of vectors meets H_1 ([32] p. 138-139), so this procedure computes $\phi(v)$ for each $v \in V$. Moreover, G^* preserves the form ϕ by construction (cf. [17], Lemma 13.2). The algorithm is in NC since PERP-VECTORS (Problem V.84) is in NC, and since we may consider all $|V|$ vectors in V in parallel. □

Remark V.91 Note that the form ϕ returned by CONSTRUCT-QUAD-FORM is a complete table of values $\phi(v)$ for each $v \in V$.

Operations with Standard Bases

Procedures in later sections require the ability to manipulate standard bases for symplectic, unitary, and orthogonal spaces.

Definition V.92 *An ordered basis* $\mathcal{B} = \{e_1, \ldots, e_t; f_1, \ldots, f_t; u_1, \ldots, u_s\}$ *for a vector space* V *with a nonsingular bilinear (or Hermitian if* V *is unitary) form* ϕ *is*

called a standard basis *if* $\phi(e_i, e_j) = \phi(f_i, f_j) = 0$ *and* $\phi(e_i, f_j) = \delta_{ij}$ *for* $1 \leq i, j \leq t$, *and* $s \leq 2$ *with* $\langle u_1, \ldots, u_s \rangle$ *anisotropic (0 if* $s = 0$*). For an orthogonal space* V *of characteristic 2 with nonsingular quadratic form* Q*, define a standard basis for* V *using the bilinear form induced by* Q*, with the additional requirement that each* e_i *and* f_i *must be singular, i.e.,* $Q(e_i) = Q(f_i) = 0$ *for* $i = 1, \ldots, t$.

Note that t and s are invariants of V, independent of the choice of standard basis (see [16], 9.1); in fact t, is the Witt index of V.

Remark V.93 The input to the following problem, STANDARD-BASIS1 (Problem V.94), does not include a triple $(G^*, V, \phi) \in \mathcal{G}^*$, but only a vector space V and a form ϕ. This is a concession to FIND-IRREDUCIBLE (Problem V.123), which calls STANDARD-BASIS1 when no such group G^* is available (in all other invocations of STANDARD-BASIS1, a suitable G^* is, in fact, available). Hence, within the procedure for STANDARD-BASIS1, calls to SPAN-VECTORS (Problem V.82) and PERP-VECTORS (Problem V.84) are not valid, since part of the input to those problems is such a group G^*. To handle this anomaly, the procedure for STANDARD-BASIS1 computes spans and perps directly as needed. The properties of the vector space listed in Remark V.71, which apply in this case as well, since the procedure for FIND-IRREDUCIBLE explicitly constructs all the elements of the vector space.

Problem V.94 STANDARD-BASIS1(V, ϕ)

GIVEN: the set of vectors of a vector space V over a field F as in Remark V.71, a zero or nonsingular alternating or symmetric bilinear or Hermitian form ϕ on V; and a quadratic form Q that induces ϕ if V is an orthogonal space of characteristic 2,

FIND: a standard basis $\mathcal{B}$ for V.

Procedure for Problem V.94:
if ϕ is the zero-form, **then return** any basis of V
else if $V = 0$ **then return** $\emptyset$
else
  $W \leftarrow 0$
  while possible
    { find $W^\perp$; see Remark V.93 }
    let $W^\perp = \{v \in V \mid \phi(v, w) = 0 \text{ for all } w \in W\}$
      { for each v in parallel, test all w in parallel }
    $e_i \leftarrow$ a nonzero isotropic or singular vector in $W^\perp$
    { e_i is a vector for which $\phi(e_i, e_i) = 0$ or $Q(e_i) = 0$ }
    $f_i \leftarrow$ an isotropic or singular vector in $\langle W, e_i\rangle^\perp \setminus \langle e_i\rangle$ with $\phi(e_i, f_i) = 1$
    let $\langle W, e_i, f_i\rangle = \{w + \alpha e_i + \beta f_i \mid w \in W, \alpha,\ \beta \in F\}$
    $W \leftarrow \langle W, e_i, f_i\rangle$ { now $\dim(V) - \dim(W) \leq 2$ }
  $m \leftarrow i$ { i.e., $m = \dim(W)/2$ }
  if $W = V$ **then**
    return $\mathcal{B} = \{e_1, \ldots, e_m; f_1, \ldots, f_m;\}$
  else { $\dim(W) < \dim(V)$ }
    choose any vector $u_1 \in W^\perp$
    if $\langle W, u_1\rangle = V$ **then**
      return $\mathcal{B} = \{e_1, \ldots, e_m; f_1, \ldots, f_m; u_1\}$
    else { must have $\dim(V) = \dim(W) + 2$ }
      choose $u_2 \in W^\perp \setminus \langle u_1\rangle$
      return $\mathcal{B} = \{e_1, \ldots, e_m; f_1, \ldots, f_m; u_1, u_2\}$ $\diamond$

In this procedure m is the Witt index (Definition V.15), and $\langle e_1, \ldots, e_m\rangle$ is a maximally totally isotropic or totally singular subspace of V.

Lemma V.95 *STANDARD-BASIS1 is correct and in NC.*

Proof: The correctness of the construction follows from the definition of standard bases (Definition V.92). It is in NC by Remark V.37 and Lemma V.38. □

The following procedure is used in procedure SYLCONJ-CYCLIC, Problem V.138.

Problem V.96 STANDARD-BASIS2(G^*, V, ϕ, U_1, U_2)

GIVEN: $(G^*, V, \phi) \in \mathcal{G}^*$, where $G^* \ncong SL(V)$ (Definition V.31*; Remark V.71), and two maximally totally isotropic or totally singular subspaces U_1, U_2 such that $V = U_1 \oplus U_2$,

FIND: a standard basis $\mathcal{B} = \{e_1, \ldots, e_m; f_1, \ldots, f_m\}$ for V where $U_1 = \langle e_1, \ldots, e_m \rangle$ and $U_2 = \langle f_1, \ldots, f_m \rangle$.

Procedure for Problem V.96:
choose $e_1 \in U_1$ and $f_1 \in U_2$ with $\phi(e_1, f_1) = 1$
{ if ϕ is quadratic and $char(V) = 2$, then $\phi(e_1) = \phi(f_1) = 0$, since U_1 and U_2 are totally singular in that case}
let $W = \langle e_1, f_1 \rangle$ (Problem V.82)
for $i = 2, \ldots, m$ (sequentially)
$W^\perp \leftarrow$ PERP-VECTORS(G^*, V, W) (Problem V.84)
  choose $e_i \in W^\perp \cap U_1$ and $f_i \in W^\perp \cap U_2$ with $\phi(e_i, f_i) = 1$
  $W \leftarrow \langle W, e_i, f_i \rangle$ (Problem V.82)
return $\mathcal{B} = \{e_1, \ldots, e_m; f_1, \ldots, f_m;\}$ $\diamond$

Lemma V.97 *STANDARD-BASIS2 is correct and in NC.*

Proof: The correctness of the construction follows at once from the definition of standard bases (Definition V.92). It is in NC by Remark V.37 and Lemma V.38. □

Definition V.98 *Two vector spaces U_1, U_2, with forms ϕ_1, ϕ_2, respectively, of the same type, are* isometric *if there is an isometry σ (with respect to ϕ_1, ϕ_2 for which $U_1^\sigma = U_2$. Two bases $\mathcal{B}_1, \mathcal{B}_2$ for U_1, U_2 respectively, are isometric of there is an isometry σ for which $\mathcal{B}_1^\sigma = \mathcal{B}_2$.*

Remark V.99 Let ϕ be the zero-form on a vector space V. We make the following conventions:

1. "isometric" and "isometry" mean "isomorphic" and "isomorphism";

2. all subspaces are regarded simultaneously as nonsingular, totally isotropic, and totally singular;

3. "$V = V_1 \perp V_2$" means $V = V_1 \oplus V_2$;

4. "a standard basis" (as in Definition V.92) means "any basis" (see Problem V.94);

5. if E is a subspace of V, $E^{\perp} = V$.

These conventions permit SYLCONJ-CLASSICAL (Problem V.133), and the other problems it invokes, to be applicable when $G^* \cong SL(V)$, in addition to other classical group cases.

Problem V.100 MATCH-BASES$(V, \phi, \mathcal{B}_1, \ldots, \mathcal{B}_a)$

GIVEN: a vector space V with a form ϕ (see Remark V.71), and standard bases $\mathcal{B}_j = \{e_1^j, \ldots, e_t^j; f_1^j, \ldots, f_t^j; u_1^j, \ldots, u_s^j\}$ for isometric subspaces U_j, $j = 1, \ldots, a$ (t and $s \leq 2$ are fixed parts of the input; see the remark following Definition V.92),

FIND: standard bases $\mathcal{C}_1, \ldots, \mathcal{C}_a$ for $U_1, \ldots, U_a$, respectively, which are pairwise isometric.

Procedure for Problem V.100:
if $s = 0$ or ϕ is the zero-form **return** $\mathcal{B}_1, \ldots, \mathcal{B}_a$
else if $s = 1$ **then**
  for each $\mathcal{B}_j$, $j = 2, \ldots, a$ **in parallel**
    if V is not an orthogonal space **or** $char(V) \neq 2$ **then**
      choose $v \in \langle u_1^j \rangle$ such that $\phi(v, v) = \phi(u_1^1, u_1^1)$ (test each in parallel)
    else { V is an orthogonal space **and** $char(V) = 2$ (ϕ is quadratic) }
      choose $v \in \langle u_1^j \rangle$ such that $\phi(v) = \phi(u_1^1)$ (test each in parallel)
    $\mathcal{C}_j \leftarrow \{e_1^j, \ldots, e_t^j; f_1^j, \ldots, f_t^j; v\}$
else if $s = 2$ **then**
  for each $\mathcal{B}_j$ $j = 2, \ldots, a$ **in parallel**
    if V is not an orthogonal space **or** $char(V) \neq 2$ **then**
      choose $v, w \in \langle u_1^j, u_2^j \rangle$ such that
        $\phi(v, v) = \phi(u_1^1, u_1^1)$, $\phi(w, w) = \phi(u_2^1, u_2^1)$, and $\phi(v, w) = \phi(u_1^1, u_2^1)$
        (found by testing all such pairs in parallel)
    else { V is an orthogonal space **and** $char(V) \neq 2$ (ϕ is quadratic) }
      choose $v, w \in \langle u_1^j, u_2^j \rangle$ such that
        $\phi(v) = \phi(u_1^1)$, $\phi(w) = \phi(u_2^1)$, and $\phi(v + w) = \phi(u_1^1 + u_2^1)$ (*)
        (found by testing all such pairs in parallel)
        { line (*) ensures the associated bilinear form satisfies
          $(v, w) = (u_1^1, u_2^1)$, since $(u, v) = \phi(u + v) - \phi(u) - \phi(v)$ }
    $\mathcal{C}_j \leftarrow \{e_1^j, \ldots, e_t^j; f_1^j, \ldots, f_t^j; v, w\}$
return $\mathcal{C}_1, \ldots, \mathcal{C}_a$ $\diamond$

Lemma V.101 *MATCH-BASES is correct and in NC.*

Proof: The procedure is correct, since for any $1 \leq i < j \leq a$, the map from $\mathcal{C}_i = \{e_1^i, \ldots, e_t^i; f_1^i, \ldots, f_t^i; u_1^i, \ldots, u_s^i\}$ to $\mathcal{C}_j = \{e_1^j, \ldots, e_t^j; f_1^j, \ldots, f_t^j; u_1^j, \ldots, u_s^j\}$ given by $e_l^i \mapsto e_l^j; f_l^i \mapsto f_l^j; u_k^i \mapsto u_k^j$ for all $l = 1, \ldots, t; k = 1, \ldots, s$ is an isometry, by construction. MATCH-BASES is in NC by Remark V.37 and Lemma V.38. □

Basic Operations with Flags

Definition V.102 *A* maximal flag *of a vector space V is an ordered set $\{E_1, \ldots, E_m\}$ of subspaces of V where $E_1 < \cdots < E_m$, $\dim(E_i) = i$, and $E_m = V$. If V is a space with a form, then a* maximal totally isotropic or totally singular flag *of V is an ordered set $\{E_1, \ldots, E_m\}$ of totally isotropic or totally singular subspaces of V where $E_1 < \cdots < E_m$, where $\dim(E_i) = i$ and m is the Witt index of the form on V.*

Remark V.103 Let ϕ be the zero-form on a vector space V. We make the following conventions, in addition to those already stated in Remark V.99:

1. "maximal totally isotropic or totally singular flag" means "maximal flag";
2. "Witt index" means "$\dim(V)$".

This convention allows Problems V.106, V.108, and V.110 to be applicable in the case $G^* \cong SL(V)$.

Lemma V.104 *Let E be a subspace of V. Given the set of vectors of V, the set $\mathcal{E}$ of $\dim(E)+1$-dimensional subspaces of V containing E can be enumerated in NC. Moreover, if $G \leq GL(V)$ the action of $G_{\{E\}}$ on $\mathcal{E}$ can be found in NC.*

Proof: Any subspace $U \in \mathcal{E}$ is equal to $\langle E, v\rangle$ for some $v \in V \setminus E$. Moreover, one can test in NC if $\langle E, v_1\rangle = \langle E, v_2\rangle$. So if V is the ordered set $\{v_1, \ldots, v_l\}$, one can form all subspaces $U_i = \langle E, v_i\rangle$ for $v_i \notin E$. For any pair of such subspaces U_i, U_j, if $U_i = U_j$ and $i < j$, then discard U_j.

To obtain the action of G on $\mathcal{E}$, for each generator g of G in parallel, for each $U_i \in \mathcal{E}$ in parallel, determine $U_j \in \mathcal{E}$ such that $U_i^g = U_j$ by testing all elements of $\mathcal{E}$ in parallel. □

Remark V.105 *Let E be a totally isotropic or totally singular subspace of V. Each $g \in G_{\{E\}}$ acts on the quotient space $E^{\perp}/E$ via $E + v \mapsto (E+v)^g = E + v^g$.*

Given $(G^*, V, \phi) \in \mathcal{G}^*$, the SYLFIND-CLASSICAL procedure requires the ability to find suitable (maximal totally isotropic or totally singular) flags in V that are stabilized by some Sylow p-subgroup, where p is the characteristic of of V.

Problem V.106 STABILIZE-FLAG$(G^*, V, \phi, \mathcal{F})$

GIVEN: $(G^*, V, \phi) \in \mathcal{G}^*$,

FIND: the stabilizer in G^* of a maximal flag $\mathcal{F} = \{E_1, \ldots, E_m\}$ of totally isotropic or totally singular subspaces ($G \cong SL(V)$ permitted; see Remarks V.99, V.103).

Procedure for Problem V.106:
let $E_0 = 0$; $L_0 = G^*$;
for $i = 1, \ldots, m$ (sequentially)
  let $L_i \leq L_{i-1}$ be the stabilizer of $E_{i-1} + \langle e_i \rangle$ in the action of L_{i-1} on $E_{i-1}^{\perp}/E_{i-1}$
  { construct this action by using Lemma V.104, then use Problem II.19 }
return L_m $\diamond$

Lemma V.107 *STABILIZE-FLAG is correct and in NC.*

Proof: For $i = 1, \ldots, m$, let $\mathcal{F}_i$ denote the flag $\{E_1, \ldots, E_i\}$. Assume inductively that L_{i-1} is the stabilizer of $\mathcal{F}_{i-1}$. Note that $L_i \leq L_{i-1}$ and that L_i is the stabilizer of E_i by construction. Hence L_i is the stabilizer of $\mathcal{F}_i$. It follows that L_m is the stabilizer of $\mathcal{F}_m = \mathcal{F}$. STABILIZE-FLAG is in NC by Remark V.37 and Lemma V.38. □

Problem V.108 FIND-FLAG(G^*, P^*, V, ϕ)

GIVEN: $(G^*, V, \phi) \in \mathcal{G}^*$, a group P^* acting on V that stabilizes a maximal totally isotropic or totally singular flag of V ($G \cong SL(V)$ permitted; see Remarks V.99, V.103),

FIND: a maximal flag $\mathcal{F}$ of totally isotropic or singular subspaces of V stabilized by P^*.

Procedure for Problem V.108:
let m be the dimension of a maximal totally isotropic or totally singular subspace
{ see Problem V.94, Remark V.103, and the remark following Problem V.94 }
let $E_0 = 0$
for $i = 1, \ldots, m$ (sequentially)
  choose e_i such that $E_{i-1} + \langle e_i \rangle$ is fixed by the action of P^* on $E_{i-1}^{\perp}/E_{i-1}$
  { use G^* to construct this action using Lemma V.104 }
  let $E_i = \langle e_1, \ldots, e_i \rangle$
return $\mathcal{F} = \{E_1, \ldots, E_m\}$ $\diamond$

Lemma V.109 *FIND-FLAG is correct and in NC.*

Proof: By the choice of $E_1, \ldots, E_m$, the flag $\mathcal{F}$ is stabilized by P^*. FIND-FLAG is correct by construction. FIND-FLAG is in NC by Remark V.37 and Lemma V.38.

□

Problem V.110 MAP-FLAG($G^*, V, \mathcal{F}, \mathcal{F}', \phi$)

GIVEN: $(G^*, V, \phi) \in \mathcal{G}^*$ and two maximal totally isotropic or totally singular flags $\mathcal{F}, \mathcal{F}'$ of V ($G \cong SL(V)$ permitted; see Remarks V.99, V.103),

FIND: an element $g \in G^*$ that maps $\mathcal{F}$ to $\mathcal{F}'$.

Procedure for Problem V.110:
let $\mathcal{F} = \{E_1, E_2, \ldots, E_m\}$
let $\mathcal{F}' = \{E'_1, E'_2, \ldots, E'_m\}$
let $E_0 = E'_0 = 0$; $L_0 = G^*$;
for $i = 1, \ldots, m$ (sequentially)
  let $L_i \leq G^*$ be the stabilizer of E'_i in the action of L_{i-1} on $E'^{\perp}_{i-1}/E'_{i-1}$
  { construct this action by using Lemma V.104, then use Problem II.19 }
  let g_i be an element of L_i that maps $E_i^{g_1 \cdots g_{i-1}}$ to E'_i
  { $g_i \in L_i$, hence stabilizes $E'_1, \ldots, E'_{i-1}$ }
return $g_1 \cdots g_m$ $\quad \diamond$

Lemma V.111 *MAP-FLAG is correct and in NC.*

Proof: For $i = 1, \ldots, m$, let $\mathcal{F}_i$ denote the flag $\{E_1, \ldots, E_i\}$ and let $\mathcal{F}'_i$ denote the flag $\{E'_1, \ldots, E'_i\}$. Assume inductively that $g_1 \cdots g_{i-1}$ maps $\mathcal{F}_{i-1}$ to $\mathcal{F}'_{i-1}$; in particular, $E_{i-1}^{g_1 \cdots g_{i-1}} = E'_{i-1}$. Hence $E_i^{g_1 \cdots g_{i-1}}$ is a 1-space of $E'^{\perp}_{i-1}/E'_{i-1}$. Inductively, each L_i induces a classical group on $E'^{\perp}_{i-1}/E'_{i-1}$ (by Fact V.22), and is therefore transitive on the isotropic or singular 1-spaces of $E'^{\perp}_{i-1}/E'_{i-1}$.

Hence there exists an element $g_i \in L_i$ that fixes $\mathcal{F}'_{i-1}$ and maps $E_i^{g_1 \cdots g_{i-1}}$ to E'_i. Since g_i stabilizes $\mathcal{F}'_{i-1}$, the product $g_1 \cdots g_i$ also maps $\mathcal{F}_{i-1}$ to $\mathcal{F}'_{i-1}$. Moreover, $E_i^{g_1 \cdots g_i} = E'_i$, by the choice of g_i, so $g_1 \cdots g_i$ maps $\mathcal{F}_i$ to $\mathcal{F}'_i$. Hence, by induction, the element $g_1 \cdots g_m$ found by MAP-FLAG maps $\mathcal{F}$ to $\mathcal{F}'$. MAP-FLAG is in NC by Remark V.37 and Lemma V.38. □

We digress from the main development to prove that Problem IV.9 is in NC.

Lemma V.112 *FIND-NORMALIZED-SYLOW-SIMPLE is in NC.*

Proof: Construct a set X on which S acts primitively (using Problems II.28 and II.32). In each of the following cases below, compute a Sylow subgroup $Q \leq S$ using

the action of S on X, but return the lifting of Q to a subgroup of K in the original action on Ω (Remark II.3).

Case 1: $|S| \leq |X|^8$ (this includes the cases where S is exceptional or sporadic; see [16], Lemma 6.1). Compute a Sylow 2-subgroup Q of S using SYLFIND-SMALL (Problem V.65).

Form the set $\mathcal{Q}$ of all Sylow 2-subgroups of S by conjugation by forming Q^s for each $s \in S$ in parallel and discarding any duplicates obtained (one can test if $Q^{s_1} = Q^{s_2}$ for any $s_1, s_2 \in S$ using Problem II.1). Since P acts on $\mathcal{Q}$, and since p is relatively prime to $|S|$, it is also relatively prime to $|\mathcal{Q}|$, a set upon which S acts transitively. At least one element of $\mathcal{Q}$ is stabilized by P. Let $Q_0 \in \mathcal{Q}$ be such an element (Problem II.19). Hence $Q_0 \in \mathcal{Q}$ is normalized by P. $N_S(Q_0)/Q_0$ is solvable because it has odd order (see [12]). Then $N_S(Q_0)$ is solvable, since Q_0 and $N_S(Q_0)/Q_0$ are solvable. Return LIFT$(Q_0) \leq K \leq$ Sym(Ω). This concludes Case 1.

If $|S| > |X|^8$, then S is either alternating or classical. Construct a set Y on which the action of S is a natural action (Problem V.35, Definition V.26). If S is alternating, $|Y| > 6$; if S is classical, it is defined in terms of a vector space V with $dim(V) > 8$ (cf. Definition V.26 and the comments following it).

Case 2: If S is 6-transitive on Y, then S is alternating. Since p does not divide $|S|$, it cannot divide $|Aut(S)|$ (see [17], p. 366). Hence P induces by conjugation only trivial automorphisms of S, so P normalizes all Sylow subgroups of S. Let $Q =$ SYLFIND-ALT$(S, 2)$, a Sylow 2-subgroup of S. As in Case 1, $N_S(Q)$ is solvable. Return LIFT$(Q) \leq K \leq$ Sym(Ω) (Remark II.3).

Case 3: Neither Case 1 nor Case 2 applies, so S must be a classical group. If q is a prime and q^k is the largest prime power that divides $|S|$, then q is the

characteristic of the field over which S is defined (see [1]). Coordinatize Y as the 1-spaces of a vector space V using Problem V.69 (Definition V.67) and construct a form ϕ on V using Problem V.87. P normalizes some Sylow q-subgroup Q, hence it stabilizes a maximal flag of totally isotropic or totally singular subspaces (the same flag stabilized by Q).

Let $\mathcal{F}$ = FIND-FLAG(S, P, V, ϕ) (Problem V.108), so $\mathcal{F}$ is a maximal totally isotropic or totally singular flag in V. Let B = STABILIZE-FLAG$(S, V, \phi, \mathcal{F})$ (Problem V.106) be the stabilizer of the flag $\mathcal{F}$. Then B is a Borel subgroup ([16], p. 499; [9], p. 104). Let Q = SYLFIND-SOLVABLE(B, q) (Problem III.7). Then Q is a Sylow q-subgroup of S. B is solvable and $B = N_S(Q)$ ([9], pp. 172, 262). Return LIFT$(Q) \leq K \leq \mathrm{Sym}(\Omega)$ (Remark II.3). □

Decompositions Induced by Sylow Subgroups

Theorem V.113 *Let P be a Sylow p-subgroup of G where $(G, \overline{V}, \phi) \in \mathcal{G}$ (Definition V.31). Let $(G^*, V, \phi) \in \mathcal{G}^*$ (Definition V.31*) where G^* induces G on $\overline{V}$. Let P^* be the largest p-subgroup of G^* that projects onto P. Then there is a decomposition $V = V_1 \perp \cdots \perp V_a \perp V_c$, with the following properties:*

1. *P^* acts on $\Omega = \{V_1, \ldots, V_a; V_c\}$.*
2. *($p \neq 2$) For each $j = 1, \ldots, a$, $(P^*)^{V_j}_{\{V_j\}}$ is cyclic and acts fixed-point freely on V_j. Also, either:*
   (a) *$P^*_{\{V_i\}}$ acts irreducibly on V_i, or*
   (b) *Each V_i splits into the direct sum of two $P^*_{\{V_i\}}$-irreducible totally isotropic or totally singular subspaces of dimension $\frac{1}{2}\dim(V_i)$.*

3. *($p = 2$) Each V_i has dimension ≤ 2, and $P_{\{V_i\}}$ acts irreducibly on each $V_i \neq V_c$.*

4. *Any $V_i \neq V_c$ lies in V_1^G except possibly if $p = 2$ and G is orthogonal, in which case $V_c = 0$ and there can be one or two subspaces $V_i \notin V_1^G$, each of dimension 1.*

5. *P^* induces a Sylow p-subgroup of $Sym(\{V_1, \ldots, V_a\})$.*

6. *The set stabilizer G_Ω induces the symmetric group on $V_1^G \cap \Omega$ and fixes each member of Ω not in $V_1^G \cap \Omega$.*

7. *$V_c = C_V(P^*)$, i.e., $V_c = \{v \in V \mid P^* \text{ fixes } v\}$. Note that V_c may be 0.*

Furthermore, if $V_i \neq V_c$ and $p > 2$, then V_i is a nonsingular subspace of minimal dimension subject to the condition that p divides $|(G^*)^{V_i}_{\{V_i\}}|$. Also, in case 2.b. above, if G is symplectic or orthogonal, then $\frac{1}{2}\dim(V_i)$ is odd, and if G is unitary then $\frac{1}{2}\dim(V_i)$ is even.

If $p = 2$ and $V_i \in V_1^G$, then V_i is a nonsingular 2-space subject to the requirement that 8 divides $|(G^*)^{V_i}_{\{V_i\}}|$. If G is not orthogonal or has odd dimension, then $|(V_1)^{G_\Omega}| = [\frac{1}{2}\dim V]$. In the case where G is orthogonal and even dimensional, if V is the orthogonal sum of subspaces isometric to V_1 then $|(V_1)^{G_\Omega}| = \frac{1}{2}\dim V$; otherwise $|(V_1)^{G_\Omega}| = \frac{1}{2}\dim V - 1$.

Proof: [18] Theorem 5.7. □

Two important steps in the process of constructing a Sylow p-subgroup of G^*, where $(G^*, V, \phi) \in \mathcal{G}^*$, is to construct a decomposition of V described in Theorem V.113, and to construct a Sylow p-subgroup $P^*_{V_i}$ of $(G^*)^{V_i}_{\{V_i\}}$ ($p \neq 2$), where V_i is one of the subspaces in the decomposition of V. We describe algorithms for these problems

in the next two sections, respectively. (If $p = 2$, then this Sylow p-subgroup $P^*_{V_i}$ is small, and may be found by brute force using Problem V.65.)

Making a Decomposition

Let $(G^*, V, \phi) \in \mathcal{G}^*$ and let p be a prime. Suppose $V \cong F_q^n$, or $V \cong F_{q^2}^n$ if G^* is unitary. This section describes how to construct a decomposition for V induced by some Sylow p-subgroup of G^* as in Theorem V.113. Let U be a nonsingular subspace of V in the standard decomposition (Theorem V.113) for a Sylow p-subgroup P^* of G^* where $U \neq C_V(P^*)$. If $p \neq 2$, and e is the order of q modulo p, then $\dim(U)$ is given by the following table. The values in this table are obtained by determining the dimension of the smallest vector space V for which the orders of the symplectic group, orthogonal, or unitary groups, respectively, are divisible by p (using Facts V.17, V.18, and V.19). If $p = 2$ then $\dim(U)$ is defined to be 2.

	Dimension of U		
	symplectic	*orthogonal*	*unitary*
e odd	$2e$	$2e$	$2e$
e even	e	e	
$\frac{e}{2}$ odd			$\frac{e}{2}$
$\frac{e}{2}$ even			e

This table, and the fact that $\dim(U) = 2$ when $p = 2$, justify the following procedure COMPUTE-DIM-NONSINGULAR-SUBSPACE (Problem V.115). This procedure is in constant time by inspection. The following lemma explains the comments within the procedure for Problem V.115.

Lemma V.114 *Let $(G^*, V, \phi) \in \mathcal{G}^*$ and let U be a nonsingular subspace of V in the*

standard decomposition for a Sylow p-subgroup P^* of G^* where $p \neq 2$, and let e be the order of q modulo p. If e is odd, or if G^* is unitary and $\frac{\epsilon}{2}$ is even, then P^* acts reducibly on U (as in Theorem V.113.2.b); otherwise (i.e., if e is even and G^* is symplectic or orthogonal, or if G^* is unitary and $\frac{\epsilon}{2}$ is odd), then P_U^* acts irreducibly on U (as in Theorem V.113.2.a).

Proof: If e is odd, then by the above table, $\dim(U) = 2e$. In this case, Facts V.17, V.18, and V.19 imply that $|GL(e,q)|$ divides each of $|Sp(2e,q)|, |U(2e,q)|$, and $|O^+(2e,q)|$. U has Witt index e in these cases, and has a standard basis $\{\epsilon_1, \ldots, \epsilon_e; \delta_1, \ldots, \delta_e\}$. Relative to this basis, the form has the matrix $\begin{bmatrix} 0 & I \\ \pm I & 0 \end{bmatrix}$ and $GL(e,q)$ can be embedded into $Sp(2e,q), U(2e,q)$, or $O^+(2e,q)$ via

$$X \mapsto \begin{bmatrix} X & 0 \\ 0 & X^{-t} \end{bmatrix} \text{ or } \begin{bmatrix} X & 0 \\ 0 & \overline{X}^{-t} \end{bmatrix} \text{if unitary.}$$

The image of a Sylow p-subgroup of $GL(e,q)$ is a Sylow p-subgroup of $Sp(2e,q)$, $U(2e,q)$, or $O^+(2e,q)$, and this Sylow p-subgroup acts irreducibly on $U_1 = \langle \epsilon_1, \ldots, \epsilon_e \rangle$ and on $U_2 = \langle \delta, \ldots, \delta_e \rangle$. Similarly, if $\frac{\epsilon}{2}$ is even, then $|GL(\frac{\epsilon}{2}, q^2)|$ divides $|U(e,q)|$, and U has Witt index $\frac{\epsilon}{2}$ and a standard basis $\{\epsilon_1, \ldots, \epsilon_{\frac{\epsilon}{2}}; \delta_1, \ldots, \delta_{\frac{\epsilon}{2}}\}$, and a Sylow p-subgroup acts reducibly on U.

Otherwise, $|GL(e,q)|$ does not divide $|Sp(e,q)|$ or $|O^{\pm}(e,q)|$, and $|GL(\frac{\epsilon}{2}, q^2)|$ does not divide $|U(\frac{\epsilon}{2}, q)|$. Hence, an embedding as above is impossible, and P_U^* acts irreducibly on U. □

Problem V.115 COMPUTE-DIM-NONSINGULAR-SUBSPACE(G^*, V, p)

GIVEN: $(G^*, V, \phi) \in \mathcal{G}^*$, $G^* \neq SL(V)$, where $V \cong F_q^n$ (or $F_{q^2}^n$ if G is unitary), and a prime p dividing $|G|$ but not dividing q,

FIND: the dimension of a nonsingular subspace $U \leq V$ such that either $p \neq 2$ and $\dim(U)$ is minimal such that p divides $|(G^*)^U_{\{U\}}|$, or $p = 2$ and 8 divides $|(G^*)^U_{\{U\}}|$.

Procedure for Problem V.115:

if $p = 2$ { so q must be odd } **then return** 2

else { $p \neq 2$ }

  $e \leftarrow$order of q mod p { e smallest positive integer for which $p|(q^e - 1)$ }

  if G^* is symplectic **then**

    if e is odd **then return** $2e$

      { there exists a nonsingular subspace U of dimension $2e$ such that some Sylow p-subgroup splits U as $U = U_1 \oplus U_2$ with U_1, U_2 totally isotropic of dimension e }

    else { e is even } **return** e

      { some Sylow p-subgroup acts irreducibly on a nonsingular subspace U of dimension e }

  if G^* is orthogonal **then**

    if e is odd **then return** $2e$

      { there exists a nonsingular subspace U of dimension $2e$ such that some Sylow p-subgroup splits U as $U = U_1 \oplus U_2$ where U_1, U_2 are totally singular of dimension e }

    else { e is even } **return** e

      { some Sylow p-subgroup acts irreducibly on a nonsingular subspace U of dimension e }

if G^* is unitary **then**
  if e is odd **then return** $2e$
    { there exists a nonsingular subspace U of dimension $2e$ such that some Sylow p-subgroup splits U as $U = U_1 \oplus U_2$ where U_1, U_2 are totally isotropic of dimension e }
  else { e is even }
    if $\frac{e}{2}$ is even **then return** e
    { there exists a nonsingular subspace U of dimension e on which some Sylow p-subgroup splits U as $U_1 \oplus U_2$ with U_1, U_2 totally isotropic of dimension $\frac{e}{2}$ }
    else { $\frac{e}{2}$ is odd } **return** $\frac{e}{2}$
    { there exists a nonsingular subspace U of dimension $\frac{e}{2}$ on which some Sylow p-subgroup acts irreducibly } $\diamond$

Problem V.116 MAKE-NONSINGULAR-SUBSPACE(G^*, V, ϕ, d, sgn)

GIVEN: $(G^*, V, \phi) \in \mathcal{G}^*$, $G^* \ncong PSL(V)$, with $\dim(V) > d$ where d is the dimension of a nonsingular subspace in the decomposition of some Sylow subgroup P^* of a classical group defined on V (except for $C_V(P^*)$ if $p > 2$, and except for 1-spaces if $p = 2$), and a sign $sgn = \pm$ if V is orthogonal and d is even,

FIND: a nonsingular subspace $W < V$ of dimension d, and a standard basis for this subspace (see Definition V.92); moreover if V is orthogonal and d is even, then the subspace W found has the isometry type sgn, i.e., the Witt index of W is $\frac{d}{2}$ if sgn is "+" or $\frac{d}{2} - 1$ if sgn is "−".

Procedure for Problem V.116:

$\mathcal{C} = \{e_1, \ldots, e_m; f_1, \ldots, f_m; u_1, \ldots, u_s\} \leftarrow$ STANDARD-BASIS1(V, ϕ)
(Problem V.94)

if d is even **then** $l \leftarrow \frac{d}{2}$ **else** $l \leftarrow \frac{1}{2}(d-1)$

if d is even **and**

(V is symplectic **or** V is unitary **or** (V is orthogonal **and** $sgn =$"+")) **then**

{ here $s = 0$, so $2l = d < \dim(V) = 2m$, hence $l < m$
so the following line is valid }

return $(\langle e_1, \ldots, e_l; f_1, \ldots, f_l\rangle,\ \{e_1, \ldots, e_l; f_1, \ldots, f_l\})$

else if d is odd **then**

{ d is odd, so V is unitary (see table preceding Problem V.115); hence $0 \leq s \leq 1$, so $2l+1 = d < 2m \leq \dim(V) \leq 2m+1$, hence $l < m$ so the following line is valid }

return $(\langle e_1, \ldots, e_l; f_1, \ldots, f_l; u_1\rangle,\ \{e_1, \ldots, e_l; f_1, \ldots, f_l; u_1\})$

else { V is orthogonal, $sgn =$"$-$" (and hence d is even) }

{ here $s \leq 2$, so $2(l-1)+2 = d < 2m \leq \dim(V) \leq 2m+2$,
hence $l - 1 < m$, so the following line is valid }

return $(\langle e_1, \ldots, e_{l-1}; f_1, \ldots, f_{l-1}; u_1, u_2\rangle,\ \{e_1, \ldots, e_{l-1}; f_1, \ldots, f_{l-1}; u_1, u_2\})$ ◇

Lemma V.117 *MAKE-NONSINGULAR-SUBSPACE is correct and in NC.*

Proof: By construction, the space returned has dimension d, and has the correct isometry type if V is an orthogonal space and d is even. The procedure is in NC since STANDARD-BASIS1 (Problem V.94) is in NC. □

Problem V.118 MAKE-DECOMP(G^*, V, ϕ, p)

GIVEN: $(G^*, V, \phi) \in \mathcal{G}^*$, $G^* \ncong PSL(V)$, and a prime $p \neq char(V)$ that divides $|G^*|$,

FIND: a collection of pairs $\mathcal{U} = \{(U_1, \mathcal{B}_1), \ldots, (U_a, \mathcal{B}_a); (U_c, \mathcal{B}_c)\}$, where $\{U_1, \ldots, U_a; U_c\}$ is the standard decomposition of V (Theorem V.113) for some Sylow p-subgroup of G^*, and $\mathcal{B}_i$ is a standard basis (Definition V.92) for U_i for each $i = 1, \ldots, a; c$ (possibly $U_c = 0$ and $\mathcal{B}_c = \emptyset$).

Procedure for Problem V.118:

$d \leftarrow$ COMPUTE-DIM-NONSINGULAR-SUBSPACE(G^*, V, p) (Problem V.115)
{ (*) if $p \neq 2$, then d is the dimension of a minimal nonsingular subspace $U \leq V$ for which $p \| |(G^*)^U_{\{U\}}|$; if $p = 2$, then $d = 2$ and there exists a nonsingular 2-space U such that $8 \| |(G^*)^U_{\{U\}}|$ }
if G^* is orthogonal and $p = 2$ **then**
  if $q \equiv 1 \bmod 4$ **then** $sgn \leftarrow$ "+" { so U will satisfy $(G^*)^U_{\{U\}} = O^+(2,q)$ }
  else { $q \equiv -1 \bmod 4$ } $sgn \leftarrow$ "−" { so U will satisfy $(G^*)^U_{\{U\}} = O^-(2,q)$, cf. (*)}
if G^* orthogonal and $p \neq 2$ { so d is even (see table preceding Problem V.115) }
  if $\{p | (q^{\frac{d}{2}} \pm 1)\}$ **then** $sgn \leftarrow$ "$\mp$" { so U will satisfy $(G^*)^U_{\{U\}} = O^{\mp}(d,q)$, cf. (*) }
$U_0 \leftarrow 0$; $W \leftarrow V$; $\mathcal{U} \leftarrow \emptyset$; $i \leftarrow 1$ { loop initialization }
while $\dim(W) > d$ **do** (sequentially)
  $i \leftarrow i + 1$; $W \leftarrow \langle U_1, \ldots, U_{i-1} \rangle^{\perp}$ (Problems V.82, V.84)
  if $\dim(W) > d$ { get another subspace }
    $H^* \leftarrow (G^*)^W_{\{W\}}$ { pointwise stabilize a basis for a complementary subspace of W in V (Problem II.19); H^* is a classical group by Fact V.22 }
    if $|H^*| > |W|^8$ **then**
      $(U_i, \mathcal{B}_i) \leftarrow$ MAKE-NONSINGULAR-SUBSPACE$(H^*, W, \phi|_W, d, sgn)$ (Problem V.116)
    else form a standard basis for W (Problem V.94) and find $(U_i, \mathcal{B}_i)$ as in Problem V.116
    $\mathcal{U} \leftarrow \{(U_1, \mathcal{B}_1), \ldots, (U_i, \mathcal{B}_i)\}$
  if $\dim(W) = d$
    $\mathcal{B}_i \leftarrow$ STANDARD-BASIS1$(W, \phi|_W)$
    let m and m' be the Witt indices of U_1 and W, respectively
      { standard bases for each are available }
    if $m = m'$ (i.e., W and U_1 have same the isometry type) **then**
      $U_i \leftarrow W$; $\mathcal{U} \leftarrow \{(U_1, \mathcal{B}_1), \ldots, (U_{i-1}, \mathcal{B}_{i-1}), (U_i, \mathcal{B}_i); (0, \emptyset)\}$
    else { W and U_1 have different isometry types }
      if $p = d = 2$ and G^* orthogonal **then** { see Theorem V.113.4 }
        let $\{w_1, w_2\}$ be a basis for W with $\phi(w_1, w_2) = 0$
        $\mathcal{U} \leftarrow \{(U_1, \mathcal{B}_1), \ldots, (U_{i-1}, \mathcal{B}_{i-1}), (\langle w_1 \rangle, \{w_1\}), (\langle w_2 \rangle, \{w_2\}); (0, \emptyset)\}$
      else $U_c \leftarrow W$; $\mathcal{B}_c \leftarrow \mathcal{B}_i$; $\mathcal{U} \leftarrow \{(U_1, \mathcal{B}_1), \ldots, (U_{i-1}, \mathcal{B}_{i-1}); (U_c, \mathcal{B}_c)\}$

if $\dim(W) < d$ { this occurs in the last iteration, if at all }
  if $p = d = 2$ (and hence $\dim(W) = 1$) **then**
    let $\{w_1\}$ be a basis for W
    $\mathcal{U} \leftarrow \{(U_1, \mathcal{B}_1), \ldots, (U_{i-1}, \mathcal{B}_{i-1}),\ (\langle w_1 \rangle, \{w_1\})\}$
  else
    $U_c \leftarrow \langle U \mid (U, B) \in \mathcal{U} \rangle^{\perp}$
    $\mathcal{B}_c \leftarrow$ STANDARD-BASIS1$(U_c, \phi|_{U_c})$
    $\mathcal{U} \leftarrow \{(U_1, \mathcal{B}_1), \ldots, (U_{i-1}, \mathcal{B}_{i-1}); (U_c, \mathcal{B}_c)\}$
return $\mathcal{U}$ $\diamond$

Lemma V.119 *MAKE-DECOMP is correct and in NC.*

Proof: The correctness follows from the construction and Theorem V.113. Note that the only time we encounter spaces of the same dimension with different isometry types is in the even dimensional orthogonal case. (Two odd-dimensional orthogonal spaces might not be isometric, but this case does not arise, since if d is odd, V must be a unitary space, by the table preceding Problem V.115.) Two even dimensional orthogonal spaces U_1, U_2, have different isometry type if they have different Witt indices (this can be determined by inspecting standard bases for U_1 and U_2). The procedure is in NC by Remark V.37 and Lemma V.38. □

Finding Cyclic Sylow Subgroups

Given $(G^*, V, \phi) \in \mathcal{G}^*$, this section shows how to construct a Sylow p-subgroup P_i^* of $(G^*)^{V_i}_{\{V_i\}}$ $(p \neq 2)$, where V_i is one of the subspaces in the decomposition of V described in Theorem V.113.

Let e be the order of q modulo p. Let r be the highest power of p dividing $q^e - 1$ (so $q^e \equiv 1 \bmod p^r$). Let $V = F_q^e$, and embed $GL(1, q^e) \hookrightarrow GL(e, q)$ as follows. Since $F_{q^e} \cong V$ as F_q-spaces, we may identify F_{q^e} with V. Each element of $GL(1, q^e)$ is F_{q^e}-linear, hence F_q-linear on V, hence induces an element of $GL(e, q)$. Also, since

$|GL(1,q^e)| = |F_{q^e}^*| = q^e - 1$ and $|GL(e,q)| = q^{e(e-1)/2}(q^e-1)\cdots(q^2-1)(q-1)$, p^r is the highest power of p that divides $|GL(1,q^e)|$ and also $|GL(e,q)|$. Hence, the embedding carries Sylow p-subgroups of $GL(1,q^e)$ to Sylow p-subgroups of $GL(e,q)$. Since $GL(1,q^e) \cong F_{q^e}^*$ and $F_{q^e}^*$ is cyclic, a Sylow p-subgroup of of $GL(e,q)$ is cyclic of order p^r.

Lemma V.120 *Let $P = \langle T \rangle$ be a Sylow p-subgroup of $GL(e,q)$. There exists a basis for V relative to which the matrix of T is a companion matrix*

$$M(\alpha_0,\ldots,\alpha_{e-1}) = \begin{pmatrix} 0 & 0 & \ldots & 0 & \alpha_0 \\ 1 & 0 & \ldots & 0 & \alpha_1 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & \alpha_{e-2} \\ 0 & 0 & \ldots & 1 & \alpha_{e-1} \end{pmatrix}$$

of a polynomial $x^e - \alpha_{e-1}x^{e-1} - \cdots - \alpha_0$ of degree e.

Proof: P must act irreducibly on V, otherwise there would be an invariant subspace of dimension $f < e$, which would imply, by Fact V.5, that $p \mid q^f - 1$, a contradiction. Choose any nonzero vector $v \in V$. If $T^j v \in U = \langle T^i v \mid 0 \le i < j \rangle$ for some $j < e$, then U is a proper T-invariant subspace of V, contradicting the irreducibility of V. Hence $T^j \notin \langle T^i v \mid 0 \le i < j \rangle$ for any $j < e$, so $\{v, Tv, T^2v, \ldots, T^{e-1}v\}$ is a basis for V. Relative to this basis, the matrix of T is the companion matrix for the polynomial $x^e - \alpha_{e-1}x^{e-1} - \cdots - \alpha_0$, where $T^e v = \alpha_0 v + \alpha_1 Tv + \cdots + \alpha_{e-1}T^{e-1}v$. □

Problem V.121 COMPANION(e, p, q)

GIVEN: a prime p, a prime power q where p does not divide q, and the order e of q mod p,

FIND: an $e \times e$ companion matrix over the field F_q with order p^r, the largest power of p that divides $q^e - 1$.

Procedure for Problem V.121:
let r be the largest power of p that divides $q^e - 1$
{ by Lemma V.120, there exists some companion matrix of order p^r }
for each companion matrix $T = M(\alpha_0, \ldots, \alpha_{e-1})$ (not all $\alpha_i = 0$) **in parallel**
  let $\sigma_T = \text{ORDER}(\langle T \rangle)$ (Problem II.15) }
return any T for which $\sigma_T = p^r$ $\diamond$

Lemma V.122 *COMPANION is correct and in NC.*

Proof: Correctness follows from Lemma V.120. COMPANION is in NC because all $q^e - 1$ companion matrices are tested in parallel, and Problem II.15 is in NC. □

Problem V.123 FIND-IRREDUCIBLE$(U, \phi, \mathcal{B}, p)$

GIVEN: a vector space U of dimension d over $F = F_q$ (or $F = F_{q^2}$ if U is unitary); a nonsingular alternating, Hermitian, or quadratic form ϕ on U (both U and ϕ as in Remark V.71); a standard basis $\mathcal{B}$ (see Definition V.113) with respect to ϕ, and an odd prime p such that Isom(U) has an irreducible cyclic Sylow p-subgroup,

FIND: a generator for some Sylow p-subgroup of Isom(U).

Procedure for Problem V.123:
if U symplectic or orthogonal **then** {d is even by the table preceding Problem V.115}
  $k \leftarrow \frac{d}{2}$
else { U is unitary; hence d odd by the table preceding Problem V.115 }
  $k \leftarrow d$ { note that in either case, $|U| = q^{2k}$ }
$A \leftarrow$ a $d \times d$ companion matrix of order $|U| - 1$ (test all, as in Problem V.121)
$E \leftarrow \langle A \rangle \cup \{0\}$ { E is an NC-enumerable subring of $GL(U)$ isomorphic to $F_{q^{2k}}$ }
let $\overline{e} = e^{q^k}$ $\forall e \in E$ { so the map $e \mapsto \overline{e}$ is the involutory automorphism of E }
let $Tr(e) = \sum_{i=0}^{d-1} e^{|F|^i}$ for all $e \in E$ (Tr is the trace map $E \rightarrow F$)
if (U, ϕ) is symplectic **then** { construct an alternating form B' over F_q }
    let λ be an element of F which satisfies $\overline{\lambda} = -\lambda \neq 0$
    let B' be the map given by $(u, v) \mapsto Tr(\lambda u \overline{v})$
else if (U, ϕ) is unitary **then** { construct a Hermitian form H' over F_{q^2} }
    let H' be the map given by $(u, v) \mapsto Tr(u\overline{v})$ when $|F| = q^2$
else if (U, ϕ) is orthogonal **then** { construct a quadratic form Q' over F_q }
    let Q' be the map given by $u \mapsto Tr(u\overline{u})$
let ϕ' denote B', H', or Q', if U is a symplectic, unitary, or orthogonal space, respectively
$\mathcal{B}' \leftarrow$ STANDARD-BASIS1(E, ϕ') (Problem V.94; see Remark V.71)
$(\mathcal{B}, \mathcal{B}') \leftarrow$ MATCH-BASES$((U \perp E), (\phi \perp \phi'), \mathcal{B}, \mathcal{B}')$ (Problem V.100)
let $t : E \rightarrow U$ be the linear map defined by $t(\mathcal{B}') = \mathcal{B}$ { $\mathcal{B}, \mathcal{B}'$ are *ordered* bases }
choose $g \in \langle A \rangle$ with order $q^k + 1$
let $g_1 \in GL(E)$ be the map $u \mapsto ug$
{$\overline{g} = g^{-1}$ so g_1 preserves ϕ'; $t^{-1}g_1 t \in GL(U)$ preserves ϕ and has order $q^k + 1$}
return the power of $g_2 = t^{-1}g_1 t$ that has the largest p-power order $\diamond$

Lemma V.124 *FIND-IRREDUCIBLE is correct and in NC.*

Proof: As noted in the procedure, if U is unitary, $d = \dim(U)$ is odd. Then $e \mapsto \overline{e}$ induces the involutory automorphism of F. It then follows that H' is, indeed, Hermitian: $Tr(v\overline{u}) = Tr(\overline{u\overline{v}}) = \overline{Tr(u\overline{v})}$. Nonsingularity is straightforward here, and in the symplectic and unitary cases too. By the proof of Proposition 15.2 in [17], $g_2 \in GL(U)$ preserves the form ϕ and has order $q^k + 1$. FIND-IRREDUCIBLE

returns an element whose order is the largest p-power that divides $q^k + 1$, which is the largest p-power that divides $|\mathrm{Isom}(U)|$, by Facts V.17, V.18, and V.19. FIND-IRREDUCIBLE is in NC since $|E|$ is polynomial in $|U|$. Moreover, the procedures FIND-IRREDUCIBLE invokes are in NC, as are the constructions of B', H', and Q'. Only the cases considered in the procedure for Problem V.123 are relevant, by Lemma V.114. □

Problem V.125 SYLFIND-CYCLIC$(G^*, V, \phi, U, \mathcal{B}, p)$

GIVEN: $(G^*, V, \phi) \in \mathcal{G}^*$ where $G^* \ncong SL(V)$, $V \cong F_q^n$, or $V \cong F_{q^2}^n$ if G^* is unitary, an odd prime $p \neq char(V)$, a standard basis $\mathcal{B} = \{h_1, \ldots, h_e; k_1, \ldots, k_e; u_1, \ldots, u_s\}$ for a nonsingular subspace U of V, where U is in the standard decomposition for some Sylow p-subgroup P^* of G^* (but $U \neq C_V(P^*)$,

FIND: a Sylow p-subgroup of $(G^*)^U_{\{U\}}$.

Procedure for Problem V.125:
let e be the order of q mod p
let r be the highest power of p dividing $q^e - 1$
if ((G^* is symplectic **or** orthogonal) **and** e is even) **or**
(G^* is unitary **and** (e is even **and** $\frac{e}{2}$ is odd)) **then** { see Lemma V.114 }
{ find a cyclic Sylow p-subgroup of isometries acting irreducibly on U}
$C \leftarrow$FIND-IRREDUCIBLE$(U, \phi, \mathcal{B}, p)$ (Problem V.123)
{ $\langle C \rangle$ is a Sylow p-subgroup of $\mathrm{Isom}(U)$ }
return $\langle C \rangle \cap (G^*)^U_{\{U\}}$ (Problem II.21, using the permutation action on U)
else { we seek a cyclic p-group that splits U into $U_1 \oplus U_2$, each of dimension e }
$A \leftarrow$ COMPANION(e, p, q) (Problem V.121)
let $U_1 = \langle h_1, \ldots, h_e \rangle$ and $U_2 = \langle k_1, \ldots, k_e \rangle$ { in this case $s = 0$ }
let $M = \begin{bmatrix} A & 0 \\ 0 & \overline{A}^{-t} \end{bmatrix}$ if V is unitary, or $\begin{bmatrix} A & 0 \\ 0 & A^{-t} \end{bmatrix}$ otherwise
let T be the linear transformation of V such that $[T]_{\mathcal{B}} = M$
return $\langle T \rangle$ ◇

Lemma V.126 *SYLFIND-CYCLIC is correct and in NC.*

Proof: If G^* is symplectic or orthogonal and e is even, or if G^* is unitary and e is even and $\frac{e}{2}$ is odd, then we seek a group that acts irreducibly, by Lemma V.114. SYLFIND-CYCLIC returns a Sylow p-subgroup of Isom(U) because FIND-IRREDUCIBLE returns a Sylow p-subgroup of the full isometry group of U. Otherwise, the group we seek acts reducibly on U, and irreducibly on U_1 and U_2 by Lemma V.114. T has order p^r, the p-part of $q^e - 1$. The p-part of $|(G^*)^U_{\{U\}}|$ is also equal to the p-part of $q^e - 1$, by Facts V.17, V.18, and V.19. Hence $\langle T \rangle$ is a Sylow p-subgroup of $(G^*)^U_{\{U\}}$. SYLFIND-CYCLIC is in NC since the procedures it invokes are in NC, and by Lemma V.38. □

SYLFIND for Classical Groups

This section presents algorithms to find Sylow subgroups of a group G^* for which $(G^*, V, \phi) \in \mathcal{G}^*$. This is done using SYLFIND-PSL, if $G^* \cong \mathrm{PSL}(n, q)$, or using SYLFIND-CLASSICAL, if G^* is symplectic, unitary, or orthogonal.

Problem V.127 INDUCE($G^*, V, \mathcal{W}, \mathcal{B}, \sigma$)

GIVEN: $(G^*, V) \in \mathcal{G}^*$, a decomposition $\mathcal{W} = \{W_1, \ldots, W_a\}$ of V, a set of pairwise isometric standard bases $\mathcal{B} = \{\mathcal{B}_1, \ldots, \mathcal{B}_a\}$ (see Definition V.98), where $W_i = \langle \mathcal{B}_i \rangle$ for all i, and a permutation $\sigma \in \mathrm{Sym}(\{1, \ldots, a\})$ ($G^* \cong SL(V)$ permitted; see Remark V.99),

FIND: an isometry h_σ of V such that $\mathcal{B}_i^{h_\sigma} = \mathcal{B}_{i^\sigma}$ for all $i = 1, \ldots, a$.

Procedure for Problem V.127:
if $G^* \cong SL(V)$ **then**
  let $\mathcal{B}_j = \{v_1^j, \ldots, v_t^j\}$ for $j = 1, \ldots, a$
  return the isometry h_σ induced by $v_i^j \mapsto v_i^{j^\sigma}$ for $i = 1, \ldots t$ and $j = 1, \ldots, a$
    { note $\mathcal{B}_i^{h_\sigma} = \mathcal{B}_{i^\sigma}$ for $i = 1, \ldots, a$ }
else { G^* is symplectic, unitary, or orthogonal }
  let $\mathcal{B}_j = \{e_1^j, \ldots, e_t^j; f_1^j, \ldots, f_t^j; u_1^j, \ldots, u_s^j\}$ for $j = 1, \ldots, a$
  return the isometry h_σ induced by $(e_i^j \mapsto e_i^{j^\sigma}; f_i^j \mapsto f_i^{j^\sigma};\ u_k^j \mapsto u_k^{j^\sigma})$,
  for $j = 1, \ldots, a$, $i = 1, \ldots, t$, and $k = 1, \ldots, s$ { note $\mathcal{B}_i^{h_\sigma} = \mathcal{B}_{i^\sigma}$ for $i = 1, \ldots, a$ }
$\diamond$

Lemma V.128 *INDUCE is correct and in NC.*

Proof: h_σ is an isometry because it maps a set of standard bases to isometric standard bases, and by construction, h_σ induces σ on $\mathcal{W}$. INDUCE, in fact, runs in constant time, and is hence in NC. □

Problem V.129 SYLFIND-GL(V, p)

GIVEN: a vector space $V = F_q^n$ with $n \geq 2$ and a prime p,

FIND: a Sylow p-subgroup of $GL(V)$.

Procedure for Problem V.129:
let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be the standard basis for V
if p divides q **then**
  let $\mathcal{M} = \{I + E_{ij}(\alpha) \mid 1 \leq i < j \leq n, \alpha \in F_q\}$
    where $E_{ij}(\alpha)$ is the zero matrix except for an α in the i,j position, and $\alpha \in F_q$
  let $\mathcal{T} = \{T \in GL(V) \mid [T]_{\mathcal{B}} \in \mathcal{M}\}$
  { $\mathcal{T}$ is the set of linear transformations with upper triangular unipotent
    matrices with respect to $\mathcal{B}$ }
  return $\langle \mathcal{T} \rangle$
else { p does not divide q }
  if $p > 2$ **then** $e \leftarrow$ order of q modulo p **else** $e \leftarrow 2$
  $a \leftarrow \left[\frac{n}{e}\right]$
  let $V_c = \langle \mathcal{B}_c \rangle$ where $\mathcal{B}_c = \{v_{ae+1}, \ldots, v_n\}$
  for each $i = 1, \ldots, a$ **in parallel**
    let $W_i = \langle \mathcal{B}_i \rangle$ where $\mathcal{B}_i = \{v_{(i-1)e+1}, \ldots, v_{ie}\}$
    if $p > 2$ **then** $\mathcal{M} \leftarrow \{\text{COMPANION}(e, p, q)\}$ (Problem V.121)
    else { $p = e = 2$ }
      $\Phi \leftarrow$ a set of generators for SYLFIND-SMALL$(GL(W_1), 2)$
      let $\mathcal{M} = \{[R]_{\mathcal{B}_1} \mid R \in \Phi\}$ (Problem V.65)
      { $[R]_{\mathcal{B}_1}$ denotes the matrix of R with respect to the basis $\mathcal{B}_1$,
        so $\mathcal{M}$ is a collection of $e \times e$ matrices }
    $\mathcal{T}_i \leftarrow \{T \in GL(V) \mid T|_{W_j} = I_{W_j}$ if $j \neq i$; $[T|_{W_i}]_{\mathcal{B}_i} \in \mathcal{M}\}$
    { $\mathcal{T}_i$ is a set of $|\mathcal{M}|$ matrices which can be formed in parallel }
  let Ψ be a set of generators of SYLFIND-SYM$(\{1, \ldots, a\}, p)$ (Problem V.59)
  for each $\sigma \in \Psi$ **in parallel**
    $h_\sigma \leftarrow$ INDUCE$(G^*, V, \{W_i\}, \{\mathcal{B}_i\}, \sigma)$ (Problem V.127)
    { h_σ normalizes $\langle \mathcal{T}_1, \ldots, \mathcal{T}_a \rangle$ since $\mathcal{T}_i^{h_\sigma} = \mathcal{T}_{i^\sigma}$ }
  $H \leftarrow \{h_\sigma \mid \sigma \in \Psi\}$
  { H acts on $\{\mathcal{T}_1, \ldots, \mathcal{T}_a\}$, hence normalizes $\langle \mathcal{T}_1, \ldots, \mathcal{T}_a \rangle$ }
  return $P = \langle \mathcal{T}_1, \ldots, \mathcal{T}_a, H \rangle$ $\diamond$

Lemma V.130 *SYLFIND-GL is correct and in NC.*

Proof: The subgroup $P \leq GL(V)$ returned by SYLFIND-GL is a p-group since the p-group H normalizes the p-group $\langle \mathcal{T}_1, \ldots, \mathcal{T}_a \rangle$. $P \cap SL(V)$ and the decomposition

$\{V_1, \ldots, V_a; V_c\}$ satisfy all the conditions of Theorem V.113. SYLFIND-GL is in NC since the procedures it invokes are in NC, and since the $\frac{1}{2}n^2q$ elements $E_{ij}(\alpha)$ can be written down in NC, as can the sets $\mathcal{T}_i$. □

Problem V.131 SYLFIND-PSL$(G, \overline{V}, p)$

GIVEN: $(G, \overline{V}) \in \mathcal{G}$ where $G \cong PSL(V)$, and a prime p,

FIND: a Sylow p-subgroup of G.

Procedure for Problem V.131:
let $\mathcal{E}$ be a basis for V found by choosing one nonzero vector from each of the
1-spaces found by FIND-INDEPENDENT-SET$(G, \overline{V})$ (Problem V.47)
$G^* \leftarrow$ TRANSLATE-GROUP$(G, \overline{V}, V, \mathcal{E})$ (Problem V.78)
$P^* \leftarrow$ SYLFIND-GL(V, p) (problem V.129)
$P^\# \leftarrow P^* \cap G^*$ { note that $G^* = SL(V)$ } (Problem II.21)
{ $P^\#$ is a Sylow p-subgroup of $SL(V)$ }
return $(P^\#)^{\overline{V}}$ ◇

Lemma V.132 *SYLFIND-PSL is correct and in NC.*

Proof: Correctness follows from the definition of $PSL(V)$; SYLFIND-PSL is in NC because the procedures it calls are. □

Problem V.133 SYLFIND-CLASSICAL$(G, \overline{V}, p)$

GIVEN: $(G, \overline{V}) \in \mathcal{G}$ where $G \ncong PSL(V)$, and a prime p dividing $|G|$,

FIND: a Sylow p-subgroup P of G.

Procedure for Problem V.133:

$G^* \leftarrow$ TRANSLATE-GROUP$(G, \overline{V}, V)$ (Problem V.78)
  $\{G^* \leq SL(V)$, $G^* = G^{*\prime}$, and G^* induces G on $\overline{V}$ $\}$
$\phi \leftarrow$ CONSTRUCT-FORM(G^*, V) (Problem V.87)
{ now $(G^*, V, \phi) \in \mathcal{G}^*$; see Definition V.31* }
if $p = char(V)$ **then** (Problems II.16,V.106)
  $\{e_1, \ldots, e_m; f_1, \ldots, f_m; u_1, \ldots, u_s\} \leftarrow$ STANDARD-BASIS1(V, ϕ)(Problem V.94)
  let $\mathcal{F}$ be the flag $\{E_1, \ldots, E_m\}$ where $E_i = \langle e_1, \ldots, e_i \rangle$, $i = 1, \ldots, m$
  $P^* \leftarrow$ SYLFIND-SOLVABLE(STABILIZE-FLAG$(G^*, V, \phi, \mathcal{F}), p)$
else { $p \neq char(V)$ }
  $\{(U_1, \mathcal{B}_1), \ldots, (U_a, \mathcal{B}_a); (U_c, \mathcal{B}_c)\} \leftarrow$ MAKE-DECOMP(G^*, V, ϕ, p)
    (Problem V.118) { U_c may be 0 }
  $(\mathcal{B}_1, \ldots, \mathcal{B}_a) \leftarrow$ MATCH-BASES$(V, \phi, \mathcal{B}_1, \ldots, \mathcal{B}_a)$ (Problem V.100)
  let $\mathcal{B}_j = \{e_1^j, \ldots, e_t^j; f_1^j, \ldots, f_t^j; u_1^j, \ldots, u_s^j\}$ for $j = 1, \ldots, a$
  if $p = 2$ **then** $\hat{P}_1 \leftarrow$ SYLFIND-CYCLIC$(G^*, V, \phi, U_1, \mathcal{B}_1, p)$ (Problem V.125)
  else $\hat{P}_1 \leftarrow$ SYLFIND-SMALL$((G^*)^{U_1}_{\{U_1\}}, U_i, 2)$ (Problem V.65)
  let P_1 be the group of isometries of V whose generators are obtained from
    those of $\hat{P}_1$ by requiring that they are the identity on U_i for $i \neq 1$
  for each $j = 2, \ldots, a$ for which U_j is isometric to U_1 **in parallel**
    $g_j \leftarrow$ the isometry of V induced by the permutation
      $\Pi_{i=1}^{t}(e_i^1, e_i^j)(f_i^1, f_i^j)\ \Pi_{k=1}^{s}(u_k^1, u_k^j) \in \mathrm{Sym}(\cup_{i=1}^{a}\mathcal{B}_i \cup \mathcal{B}_c)$
    $P_j \leftarrow P_1^{g_j}$
  if $p = 2$ and $\dim(U_i) < 2$ **then** $P_i \leftarrow$ SYLFIND-SMALL$((G^*)^{U_i}_{\{U_i\}}, U_i, 2)$
  let Ψ be a set of generators of SYLFIND-SYM$(\{1, \ldots, a\}, p)$ (Problem V.59)
  for each $\sigma \in \Psi$ **in parallel**
    $h_\sigma \leftarrow$ INDUCE$(G^*, V, \{U_i\}, \{\mathcal{B}_i\}, \sigma)$ (Problem V.127)
    { h_σ normalizes $\langle P_1, \ldots, P_a; P_c \rangle$ since $P_i^{h_\sigma} = P_{i\sigma}$ for all i }
  $H \leftarrow \{h_\sigma \mid \sigma \in \Psi\}$ { H normalizes $\langle P_1, \ldots, P_a; P_c \rangle$ }
  $P^* \leftarrow \langle P_1 \cdots P_a P_c, H \rangle \cap G^*$ (Problem II.21, applied to the action on V)
return $(P^*)^{\overline{V}}$, the group P^* induces on $\overline{V}$ $\quad \diamond$

Lemma V.134 *SYLFIND-CLASSICAL is correct and in NC.*

Proof: The subgroup $P^* \leq G^*$ returned by SYLFIND-CLASSICAL is a p-group, since the p-group H normalizes the p-group $\hat{P}$. P^* is a Sylow p-subgroup of G^* since

P^* and the decomposition $\{U_1, \ldots, U_a; U_c\}$ satisfy all the conditions of Theorem V.113. SYLFIND-CLASSICAL is in NC since the procedures it invokes are in NC. □

SYLFIND for Simple Groups

The following procedure, SYLFIND-SIMPLE, utilizes the machinery so far developed in this chapter to solve SYLFIND for simple groups. This procedure is in fact, a more detailed and formal version of the summary description of the algorithm given in the opening section of this chapter.

Problem V.135 SYLFIND-SIMPLE(G, p)

GIVEN: a simple group $G \leq Sym(\Omega)$ and a prime p,

FIND: a Sylow p-subgroup P of G.

Procedure for Problem V.135:
$X \leftarrow$ PRIMITIVE-ACTION(G, Ω) (Problem II.32)
{ G acts primitively on X }
if $|G| \leq |X|^8$ **then**
  $P^X \leftarrow$ SYLFIND-SMALL(G^X, p) (Problem V.65)
  $P^\Omega \leftarrow$ lifting of P^X to Ω (Remark II.3)
  return P^Ω
else
  $Y \leftarrow$ NATURAL-ACTION(G, X) (Problem V.35)
  $N \leftarrow$ IDENTIFY(G, Y) (Problem V.55)
  if N is *"alternating"* **then**
    $P^Y \leftarrow$ SYLFIND-ALT(Y, p) (Problem V.60)
    $P^X \leftarrow$ lifting of P^Y to X (Remark II.3)
  else {G is a classical group }
    $(V, f) \leftarrow$ COORDINATIZE(G, Y) (Problem V.69)
    { $f : Y \rightarrow V$ and $Y \leftrightarrow \overline{V}$ }
    if N is *"PSL"* **then**
      $P^{\overline{V}} \leftarrow$ SYLFIND-PSL$(G, \overline{V}, p)$ (Problem V.131)
    if N is *"some other classical group"* **then**
      $P^{\overline{V}} \leftarrow$ SYLFIND-CLASSICAL$(G, \overline{V}, p)$ (Problem V.133)
    $P^X \leftarrow$ lifting of $P^{\overline{V}}$ to X (Remark II.3)
  $P^\Omega \leftarrow$ lifting of P^X to Ω
  return P^Ω $\diamond$

SYLCONJ for Classical Groups

Problem V.136 SYLCONJ-IRRED-CYCLIC(V, ϕ, P_1^*, P_2^*)

GIVEN: a vector space $V \cong F_q^n$, a nonsingular or 0 form ϕ on V, and two cyclic groups P_1^*, P_2^* that are Sylow p-subgroups of Isom(V) and act irreducibly on V,

FIND: an isometry g of V for which $P_1^g = P_2$.

Procedure for Problem V.136:
if p divides $q-1$ **then** { $\dim(V) \leq 2$ }
{ q is the size of field over which V is defined }
  obtain the permutation action of G^* on V (see Lemma V.73) and
  return SYLCONJ-SMALL(Isom(V), V, P_1^*, P_2^*) (Problem V.66)
else
  let S be a generator for P_1^* and T be a generator for P_2^*
  choose a nonzero vector $u \in V$
  { $V = \langle u, Su, S^2u, \ldots S^{n-1}u \rangle$ since P_1^* acts irreducibly on V }
  for each $j = 1, \ldots, |P_1^*| - 1$ **in parallel**
    for each vector $w \in V$ **in parallel**
      test if the linear transformation g given by
        $g : S^i u \rightarrow (T^j)^i w$, $i = 0, \ldots, n-1$ is an isometry
  return one such successfully tested g $\diamond$

Lemma V.137 *SYLCONJ-IRRED-CYCLIC is correct and in NC.*

Proof: S and T^j are conjugate in Isom(V) for some $0 < j < |P_1^*|$, hence have the same orbit structure. Hence some choice of j and w yields a linear transformation g which is an isometry. The procedure is in NC since all vectors of V, and all powers of T, are considered in parallel. □

Problem V.138 SYLCONJ-CYCLIC($G^*, V, \phi, P_1^*, P_2^*$)

GIVEN: $(G^*, V, \phi) \in \mathcal{G}^*$ and two cyclic Sylow p-groups P_1^*, P_2^* of G^*, where either P_1^* acts irreducibly on V, or V is the direct sum of two totally isotropic or totally singular subspaces, on each of which P_1^* acts irreducibly,

FIND: an isometry g of V for which $P_1^g = P_2$.

Procedure for Problem V.138:

if SPAN-VECTORS$(G^*, V, O) = V$ for every orbit O of P_1^* on $V \setminus \{0\}$ **then**
  return SYLCONJ-IRRED-CYCLIC(V, ϕ, P_1^*, P_2^*) (Problem V.136)
else { P_1^* and P_2^* are reducible on V }
  $\mathcal{V}_1 \leftarrow$ { SPAN-VECTORS$(G^*, V, O) \mid O$ an orbit of P_1^* on $V \setminus \{0\}$ }
    { each subspace in $\mathcal{V}_1$ is P_1^*-invariant }
  $\mathcal{V}_2 \leftarrow$ { SPAN-VECTORS$(G^*, V, O) \mid O$ an orbit of P_2^* on $V \setminus \{0\}$ }
    { each subspace in $\mathcal{V}_2$ is P_2^*-invariant }
  $U_1, U_2 \leftarrow$ distinct proper P_1^*-invariant subspaces in $\mathcal{V}_1$ such that $V = U_1 \oplus U_2$
  $W_1, W_2 \leftarrow$ distinct proper P_2^*-invariant subspaces in $\mathcal{V}_2$ such that $V = W_1 \oplus W_2$
  $\mathcal{B}_1 = \{e_1, \ldots, e_t; f_1, \ldots, f_t;\} \leftarrow$ STANDARD-BASIS2(G^*, V, ϕ, U_1, U_2)
    (Problem V.96)
    { so $U_1 = \langle e_1, \ldots, e_t \rangle$ and $U_2 = \langle f_1, \ldots, f_t \rangle$ }
  $\mathcal{B}_2 = \{e'_1, \ldots, e'_t; f'_1, \ldots, f'_t;\} \leftarrow$ STANDARD-BASIS2(G^*, V, ϕ, W_1, W_2)
    { so $W_1 = \langle e'_1, \ldots, e'_t \rangle$ and $W_2 = \langle f'_1, \ldots, f'_t \rangle$ }
  $k \leftarrow$ isometry defined by $e_i \mapsto e'_i, f_i \mapsto f'_1$, for $i = 1, \ldots, t$
  $h_1 \leftarrow$ SYLCONJ-IRRED-CYCLIC$(W_1, \phi|_{W_1}, (P_1^k)^{W_1}_{\{W_1\}}, (P_2)^{W_1}_{\{W_1\}})$
  let A be the matrix of h_1 with respect to the basis $\{e'_1, \ldots, e'_t\}$
  let $M = \begin{bmatrix} A & 0 \\ 0 & \overline{A}^{-t} \end{bmatrix}$ if V is unitary, otherwise $\begin{bmatrix} A & 0 \\ 0 & A^{-t} \end{bmatrix}$ (*)
  $\hat{h}_1 \leftarrow$ the isometry on V with matrix M with respect to the basis $\mathcal{B}_2$
  return $g = k\hat{h}_1$ $\diamond$

Lemma V.139 *SYLCONJ-CYCLIC is correct and in NC.*

Proof: The isometry k maps U_1 and U_2 to W_1 and W_2, respectively. Hence $(P_1^*)^k$ and P_2^* have the same invariant subspaces, W_1 and W_2. Any isometry on V that maps W_1 to itself and W_2 to itself and conjugates $(P_1^{*k})^{W_1}_{\{W_1\}}$ to $(P_2)^{W_1}_{\{W_1\}}$ is forced to have the form given in line (*). P_1^{*g} and P_2^* both fix W_1 and W_2 and agree on W_1 (and hence on W_2). Hence $P_1^g = P_2$. □

Problem V.140 MAP-DECOMP($G^*, V, \phi, \mathcal{U}, P_1^*, \mathcal{W}, P_2^*$)

GIVEN: $(G^*, V, \phi) \in \mathcal{G}^*$, two Sylow p-subgroups P_1^*, P_2^* of G^* (where $(p, char(V)) = 1$), and their respective decompositions $\mathcal{U} = \{U_1, \ldots, U_a; U_c\}$ and $\mathcal{W} = \{W_1, \ldots, W_a; W_c\}$ (Theorem V.113) ($G^* \cong SL(V)$ permitted; see Remark V.99),

FIND: an isometry g for which $\mathcal{U}^g = \mathcal{W}$ and a collection $\mathcal{C} = \{\mathcal{B}_1, \ldots, \mathcal{B}_a; \mathcal{B}_c\}$ of bases such that $U_i = \mathcal{B}_i$ for $i = 1, \ldots, a, c$ and if $W_i, W_j \in \mathcal{W}$ are isometric, then $\mathcal{B}_i$ is isometric to $\mathcal{B}_j$.

Procedure for Problem V.140:
let $\mathcal{O}$ be the set of P_1-orbits on $\mathcal{U}$
let $\mathcal{O}'$ be the set of P_2-orbits on $\mathcal{W}$
for each P_1^*-orbit $O \in \mathcal{O}$ **in parallel**
  choose a P_2^*-orbit $O' \in \mathcal{O}'$ such that $|O| = |O'|$
    renumber so $O = \{U_1, \ldots, U_b\}$ and $O' = \{W_1, \ldots, W_b\}$
  for each $i = 1, \ldots, b$ **in parallel**
    let $\mathcal{B}_i = \{e_1^i, \ldots, e_t^i; f_1^i, \ldots, f_t^i; u_1^i, \ldots, u_s^i\} \leftarrow$ STANDARD-BASIS1($U_i, \phi|_{U_i}$)
    let $\mathcal{C}_i = \{\epsilon_1^i, \ldots, \epsilon_t^i; \delta_1^i, \ldots, \delta_t^i; \mu_1^i, \ldots, \mu_s^i\} \leftarrow$ STANDARD-BASIS1($W_i, \phi|_{W_i}$)
      (Problem V.94)
  $(\mathcal{B}_1, \mathcal{C}_1) \leftarrow$ MATCH-BASES($V, \phi, \mathcal{B}_1, \mathcal{C}_1$) (Problem V.100)
  $(\mathcal{B}_1, \ldots, \mathcal{B}_a) \leftarrow$ MATCH-BASES($V, \phi, \mathcal{B}_1, \ldots, \mathcal{B}_a$)
  $(\mathcal{C}_1, \ldots, \mathcal{C}_a) \leftarrow$ MATCH-BASES($V, \phi, \mathcal{C}_1, \ldots, \mathcal{C}_a$)
  $(\mathcal{C}_c) \leftarrow$ MATCH-BASES($V, \phi, \mathcal{B}_c, \mathcal{C}_c$)
  $g_O \leftarrow$ isometry of V that maps $\mathcal{B}_j$ to $\mathcal{C}_j$ for all $j = 1, \ldots, a, c$
    (i.e., $e_j^l \mapsto \epsilon_j^l$, $f_j^l \mapsto \delta_j^l$, $u_j^m \mapsto \mu_j^m$ for $l = 1, \ldots, t$ and for $m = 1, \ldots, s$)
return the isometry $g = \prod_{O \in \mathcal{O}} g_O$ and the collection of bases $\mathcal{C} = \{\mathcal{C}_1, \ldots, \mathcal{C}_a, \mathcal{C}_c\}$
◇

Lemma V.141 *MAP-DECOMP is correct and in NC.*

Proof: After the calls to MATCH-BASES, all of the bases $\mathcal{B}_1, \ldots, \mathcal{B}_a, \mathcal{C}_1, \ldots, \mathcal{C}_a$ are isometric; also the bases $\mathcal{B}_c$ and $\mathcal{C}_c$ are isometric. The element g is an isometry, since it carries standard bases to isometric standard bases. □

Problem V.142 FIND-DECOMP(G^*, V, ϕ, p, P^*)

GIVEN: $(G^*, V, \phi) \in \mathcal{G}^*$, a prime p, and a Sylow p-subgroup P^* of G^* ($G^* \cong SL(V)$ permitted; see Remark V.99),

FIND: the standard decomposition of V upon which P^* acts.

Procedure for Problem V.142:

$\mathcal{V} \leftarrow$ { SPAN-VECTORS(O) | O an orbit of P^* on $V \setminus \{0\}$ }
{ each space in $\mathcal{V}$ is P^*-invariant }
$\mathcal{W}^* \leftarrow$ minimal subspaces of $\mathcal{V}$ (under $\leq$)
for each subspace X in $\mathcal{W}^*$ that is totally isotropic or totally singular **in parallel**
  find a subspace X' in $\mathcal{W}^*$ not orthogonal to X
  { such a subspace exists by Theorem V.113.2b }
  $\hat{X} \leftarrow \langle X, X' \rangle$
$\mathcal{X} \leftarrow \{\hat{X} \mid X$ totally isotropic or totally singular in $\mathcal{W}^*\}$
let $\mathcal{W}$ be the union of $\mathcal{X}$ and the set of nonsingular subspaces in $\mathcal{W}^*$ not in $C_V(P^*)$
{ $\mathcal{W}$ is the set of minimal nonsingular P^*-invariant subspaces not in $C_V(P^*)$ }
for each $W \in \mathcal{W}$ **in parallel**
  for each nonzero $v \in W$ **in parallel**
    $W_v \leftarrow C_V(P_v^*)$ (the set of vectors in V fixed by P_v^*)
  $\Pi(W) \leftarrow \{W_v \mid |P_v^*|$ is maximal for nonzero $v \in W$ }
  $\Pi^1(W) \leftarrow \{W_v \mid |P_v^*|$ is maximal or next-to-maximal for nonzero $v \in W\}$
  $\Pi^2(W) \leftarrow$ $\{\langle V_i, V_j \rangle \mid V_i, V_j \in \Pi(W)$ and $\langle V_i, V_j \rangle$ contains more than two members of $\Pi(W)\}$
  $\Pi^{12}(W) \leftarrow$ $\{\langle V_i, V_j \rangle \mid V_i, V_j \in \Pi^1(W)$ and $\langle V_i, V_j \rangle$ contains more than two members of $\Pi^1(W)\}$
if $p \neq 2$ or G symplectic **then**
  return$(\cup_{W \in \mathcal{W}} \Pi(W)) \cup C_V(P^*)$
else ($p = 2$ and G not symplectic)
  if $G^* \cong SL(d,q)$ and $q \equiv 1 \pmod 4$ **or** $G^* \cong SU(d,q)$ and $q \equiv -1 \pmod 4$
    then return $(\cup_{W \in \mathcal{W}} \Pi^{12}(W)) \cup$ { 1-spaces of V fixed by P^* }
  else return $(\cup_{W \in \mathcal{W}} \Pi^2(W)) \cup$ { 1-spaces of V fixed by P^* } $\diamond$

Lemma V.143 *FIND-DECOMP is correct and in NC.*

Proof: $\mathcal{W}^*$ is the collection of minimal P^*-invariant subspaces. Each subspace in

$\mathcal{W}^*$ is either nonsingular, the direct sum of two totally isotropic or totally singular subspaces, or a 1-space in $C_V(P^*)$. By construction, $\mathcal{W}$ is the set of minimal nonsingular P^*-invariant subspaces not in $C_V(P^*)$. Having found the set $\mathcal{W}$, Theorem 5.10 of [18] then applies, from which the correctness of FIND-DECOMP follows. FIND-DECOMP is in NC since the orbits of P^* (Problem II.5) and the span of an orbit (Problem V.82) can be found in NC. □

Problem V.144 FIND-ISOM(W, V, ϕ)

GIVEN: a nonsingular subspace W of a vector space V and a nonsingular form ϕ on V,

FIND: the full isometry group Isom(W).

Procedure for Problem V.144:

$\mathcal{B} \leftarrow \{e_1, \ldots, e_m; f_1, \ldots, f_m; u_1, \ldots, u_s\}$ STANDARD-BASIS1($W, \phi|_W$) (Problem V.94)

let $\mathcal{M} = \{\begin{bmatrix} D & 0 \\ 0 & U \end{bmatrix} \mid D$ is a $2m \times 2m$ diagonal matrix ; U is an $s \times s$ matrix $\}$

let $\Delta = \{T \in GL(W) \mid [T]_{\mathcal{B}} - I$ has at most two nonzero entries, or $[T]_{\mathcal{B}} \in \mathcal{M}\}$

if ϕ is bilinear or Hermitian **then**

  let $\mathcal{S} = \{T \in \Delta \mid \phi(Tu, Tw) = \phi(u, w) \forall u, w \in W\}$ { test all u, w in parallel }

else { ϕ is quadratic }

  let $\mathcal{S} = \{T \in \Delta \mid \phi(Tu) = \phi(u) \forall u \in W\}$ { test all u in parallel }

for each $T \in \mathcal{S}$ **in parallel**

  let $\hat{T}$ be the isometry of V that fixes each vector of $V \setminus W$ and induces T on W

return $\hat{\mathcal{S}} = \{\hat{T} \mid T \in S\}$ ◇

Lemma V.145 *FIND-ISOM is correct and in NC.*

Proof: Correctness follows from [17] Proposition 14.3; the algorithm is in NC because W is part of the input. □

Problem V.146 SYLCONJ-CLASSICAL(G^*, V, p, P_1^*, P_2^*)

GIVEN: $(G^*, V) \in \mathcal{G}^*$ (Definition V.31), a prime p, and Sylow p-subgroups $P_1^*, P_2^* \leq G^*$ ($G^* \cong SL(V)$ permitted; see Remark V.99),

FIND: an element $g \in G^*$ for which $P_1^{*g} = P_2^*$.

Procedure for Problem V.146:

$\phi \leftarrow$ CONSTRUCT-FORM(G^*, V) (Problem V.87)
{ now $(G^*, V, \phi) \in \mathcal{G}^*$ as in Definition V.31* }
if $p \neq char(V)$ **then**
  $\mathcal{U} = \{U_1, \ldots, U_a; U_c\} \leftarrow$ FIND-DECOMP(G^*, P_1^*, V, ϕ) (Problem V.142)
  $\mathcal{W} = \{W_1, \ldots, W_a; W_c\} \leftarrow$ FIND-DECOMP(G^*, P_2^*, V, ϕ)
  $(g, \mathcal{C}) \leftarrow$ MAP-DECOMP($G^*, V, \phi, \mathcal{U}, P_1^*, \mathcal{W}, P_2^*$) (Problem V.140)
  { $\mathcal{C} = \{\mathcal{C}_1, \ldots, \mathcal{C}_a, \mathcal{C}_c\}$ where $\mathcal{C}_i$ is a basis for W_i for each $i = 1, \ldots, a, c$ }
  { P_1^{*g} and P_2^* act on $\mathcal{W}$ and induce Sylow p-subgroups of Sym($\mathcal{W}$)
    by Theorem V.113.5 }
  $\sigma \leftarrow$ SYLCONJ-SYM($\mathcal{W}, (P_1^{*g})^{\mathcal{W}}, (P_2^*)^{\mathcal{W}}$) (Problem V.61)
  $h \leftarrow$ INDUCE($G^*, V, \mathcal{W}, \mathcal{C}, \sigma$) (Problem V.127)
  { P_1^{*gh} and P_2^* induce the *same* Sylow p-subgroup of Sym($\mathcal{W}$) }
  $K_1 \leftarrow$ kernel of the action of P_1^{*gh} on $\mathcal{W}$ (Problem II.18)
  $K_2 \leftarrow$ kernel of the action of P_2^* on $\mathcal{W}$
  { $K_1^{W_i} = (P_1^{*gh})^{W_i}_{\{W_i\}}$ and $K_2^{W_i} = (P_2^*)^{W_i}_{\{W_i\}}$ for each $i = 1, \ldots, a, c$
    by Theorem V.113.2 }
  for each $W_i \in \mathcal{W}$ **in parallel** { find f_i s.t. $(K_1^{W_i})^{f_i} = K_2^{W_i}$ }
    if $p > 2$ **and** $|(G^*)^{W_i}_{\{W_i\}}| > |W_i|^8$ **then** { $((G^*)^{W_i}_{\{W_i\}}, W_i) \in \mathcal{G}^*$ }
      $f_i \leftarrow$ SYLCONJ-CYCLIC($(G^*)^{W_i}_{\{W_i\}}$, $W_i, \phi|_{W_i}, K_1^{W_i}, K_2^{W_i}$) (Problem V.138)
    else $f_i \leftarrow$ SYLCONJ-SMALL(Isom(W_i), $W_i, K_1^{W_i}, K_2^{W_i}$)
      (Problems V.66,V.144)
  $f \leftarrow \prod_i f_i$
  $L \leftarrow$ Isom(W_1) $\times \cdots \times$ Isom(W_a) $\times$ Isom(W_c) (Problem V.144)
  return any $b \in ghfL \cap G^*$ (Problem II.22, using action on Sym(V))
  { ensure answer is in G^* }
else { $p = char(V)$ }
  $\mathcal{F}_1 \leftarrow$ FIND-FLAG(G^*, V, ϕ, P_1^*) { find a flag stabilized by P_1^* }
  $\mathcal{F}_2 \leftarrow$ FIND-FLAG(G^*, V, ϕ, P_2^*) { find a flag stabilized by P_2^* }
  $g \leftarrow$ MAP-FLAG($G^*, V, \phi, \mathcal{F}_1, \mathcal{F}_2$) (Problems V.108 and V.110)
  return g $\diamond$

Lemma V.147 *SYLCONJ-CLASSICAL is correct and in NC.*

Proof: First, consider the case where p is not the characteristic of V. Since g maps the decomposition $\mathcal{U}$ to the decomposition $\mathcal{W}$, P_1^{*g} and P_2^* both act on the same decomposition $\mathcal{W}$. P_1^{*gh} also acts on $\mathcal{W}$, and furthermore, P_1^{*gh} and P_2^* induce the same Sylow p-subgroup on $\mathcal{W}$. The stabilizers of W_i in P_1^{*gh} and P_2^* may be different, but the element f conjugates $(P_1^{*gh})_{\{W_i\}}^{W_i}$ to $(P_2^*)_{\{W_i\}}^{W_i}$ for each W_i. So P_1^{*ghf} and P_2^* act the same on the decomposition $\mathcal{W}$. The element ghf is an isometry, but possibly not an element of G^*. By construction of L, any isometry that conjugates P_1^* to P_2^* must be in $ghfL$. By Sylow's theorem, there exists some element of G^* that conjugates P_1^* to P_2^*, hence $ghfL \cap G^*$ must be nonempty.

If p is the characteristic of V, then every Sylow p-subgroup stabilizes a unique maximal flag of totally isotropic or totally singular subspaces. Let g be an isometry in G^* that maps the flag stabilized by P_1^* to the flag stabilized by P_2^*. Then $(P_1^*)^g$ and P_2^* stabilize the same flag, and hence are equal. □

SYLCONJ for Simple Groups

The following procedure, SYLCONJ-SIMPLE, utilizes the machinery so far developed in this chapter to solve SYLCONJ for simple groups. This procedure is in fact, a more detailed and formal version of the summary description given in the opening section of this chapter.

Problem V.148 SYLCONJ-SIMPLE(G, p, P_1, P_2, Ω)

GIVEN: a simple group $G \leq Sym(\Omega)$, a prime p, and Sylow p-subgroups P_1, P_2,

FIND: an element $g \in G$ for which $P_1^g = P_2$.

Procedure for Problem V.148:

$X \leftarrow$ PRIMITIVE-ACTION(G, Ω) (Problem II.32)
{ G acts primitively on X }
if $|G| \leq |X|^8$ **then**
  $g^X \leftarrow$ SYLCONJ-SMALL(G, X, P_1, P_2) (Problem V.66)
  $g^\Omega \leftarrow$ lifting of g^X to Ω (Remark II.3)
else
  $(G^Y, Y) \leftarrow$ NATURAL-ACTION(G, X) (Problem V.35)
  lift P_1 and P_2 to P_1^Y, P_2^Y (Remark II.3)
  $N \leftarrow$ IDENTIFY(G, Y) (Problem V.55)
  if N is *"alternating"* **then**
    $g^Y \leftarrow$ SYLCONJ-ALT(G^Y, P_1^Y, P_2^Y, Y)
  else {G is a PSL or classical group }
    $(V, f) \leftarrow$ COORDINATIZE(G, Y) (Problem V.69)
    { $f : Y \rightarrow V$ and $Y \leftrightarrow \overline{V}$ }
    let $\mathcal{E}$ be the standard basis for V
    { find groups that act on V that induce G^Y, P_1^Y, P_2^Y on $\overline{V}$ }
    $G^* \leftarrow$ TRANSLATE-GROUP$(G^{\overline{V}}, \overline{V}, V, \mathcal{E})$ (Problem V.78)
    $P_1^* \leftarrow$ TRANSLATE-p-GROUP$(P_1, G, \overline{V}, V, \mathcal{E})$ (Problem V.80)
    $P_2^* \leftarrow$ TRANSLATE-p-GROUP$(P_2, G, \overline{V}, V, \mathcal{E})$
    $g^* \leftarrow$ SYLCONJ-CLASSICAL(G^*, P_1^*, P_2^*, V) (Problem V.146)
    $g^Y \leftarrow$ element induced by g^* on $Y = \overline{V}$
  $g^X \leftarrow$ lifting of g^Y to X (Remark II.3)
  $g^\Omega \leftarrow$ lifting of g^X to Ω
  return g^Ω $\diamond$

The above procedure is, in effect, a summary explanation of how the the procedures developed earlier are used to solve Problem V.148 using a case analysis depending upon the simple group type. This procedure is in NC because all the procedures it invokes are in NC.

BIBLIOGRAPHY

[1] Artin, E. *The orders of the classical simple groups,* Comm.Pure Appl. Math. 8, 1955, 455-472.

[2] Babai, L. *Monte Carlo algorithms in graph isomorphism testing,* Tech. Rep. 79-10 Dép. Math. et Stat. Univ. de Montréal, 1979.

[3] Babai, L. *On the length of subgroup chains in the symmetric group,* Communications in Algebra 14, 1986, 1729-1736.

[4] Babai, L., Cameron, P.J., and Pálfy, P., *On the order of primitive groups with restricted non-abelian composition factors,* J. Algebra 79, 1982, 161-168.

[5] Babai, L. and Moran S. *Arthur-Merlin games: A randomized proof system and a hierarchy of complexity classes,* J. Comp. Sys. Sci. 36, 1988, 254-276.

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

[7] Berkowitz, S., *On computing the determinant in small parallel time using a small number of processors,* Info. Proc. Letters 18, 1984, 147-150.

[8] Borodin, A., von zur Gathen, J., and Hopcroft, J., *Fast parallel matrix and GCD computations,* Inform. and Control, 52, 1982, 241-256.

[9] Carter, R. *Simple groups of Lie type,* John Wiley & Sons, New York, 1972, 1989.

[10] Chistov, A. L., *Fast parallel calculation of the rank of matrices over a field of arbitrary characteristic,* Proc. Conf. Foundations of Computation Theory, Lect. Notes in Comput. Sci., Springer-Verlag 1985, 63-69.

[11] Csanky, L., *Fast parallel matrix inversion algorithms,* SIAM J. Comput., 5, 1976, 618-623.

[12] Feit, W. and Thompson, J. *Solvability of groups of odd order,* Pac. Jour. Math., 13, 775-1029, 1963.

[13] Furst, M. L., Hopcroft, J. and Luks, E. M. *Polynomial time algorithms for permutation groups,* Proc. 21th IEEE FOCS, 1980, 36-41.

[14] Hall, M. *Theory of groups,* Chelsea, New York, 1959.

[15] Herstein, I. N. *Topics in Algebra,* John Wiley & Sons, New York, 1975.

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

[17] Kantor, W. M. *Sylow's theorem in polynomial time,* J. Comp. Sys. Sci. 30, 1985, 359-394.

[18] Kantor, W. M. *Finding Sylow normalizers in polynomial time,* J. Algorithms 11, 1990, 523-563.

[19] Kantor, W. M. and Luks, E. M. *Computing in quotient groups,* Proc. 22nd ACM STOC, 1990, 524-534.

[20] Kantor, W.M, Luks, E.M., Mark, P.D. *Sylow's theorem in NC,* to appear.

[21] Luks, E. M., *Isomorphism of graphs of bounded valence can be tested in polynomial time,* J. Comp. Sys. Sci., 25 1982, 42-65.

[22] Luks, E. M., *Computing the composition factors of a permutation group in polynomial time,* Combinatorica 7 1987, 87-99.

[23] Luks, E. M. and McKenzie, P. *Parallel algorithms for solvable permutation groups,* J.Comp. Sys. Sci. 37, 1988, 39-62.

[24] Luks, E. M., *Parallel algorithms for permutation groups and graph isomorphism,* Proc. 27th IEEE FOCS, 1986, 292-302.

[25] Luks, E. M. *Permutation groups and polynomial time computation,* in Groups and Computation, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, AMS 1993.

[26] McKenzie, P., Cook, S. *The parallel complexity of abelian permutation group problems,* SIAM J. Comput. 16, 1987, 880-909.

[27] Mulmuley, K. *A fast parallel algorithm to compute the rank of a matrix over an arbitrary field,* Combinatorica 7, 1987, 101-104.

[28] Pálfy, P. P., *A polynomial bound for the orders of primitive solvable groups,* J. Algebra 77 (1982), 127-137.

[29] Pippinger, N., *On simultaneous resource bounds,* Proc. 24th IEEE FOCS, 1979, 307-311.

[30] Rotman, J. J. *The theory of groups,* 3rd ed.Allyn and Bacon, 1984.

[31] Sims, C. C., *Some group-theoretic algorithms,* in Springer Lecture Notes in Math. Vol 697, (1978) 108-124.

[32] Taylor, D., *The geometry of the classical groups*, Heldermann-Verlag, Berlin, 1992.

[33] Wielandt, H. *Finite permutation groups*, Academic Press, 1964.