JOURNAL OF ALGORITHMS 6, 478–514 (1985)

Polynomial-Time Algorithms for Finding Elements of Prime Order and Sylow Subgroups

WILLIAM M. KANTOR*

Mathematics Department, University of Oregon, Eugene, Oregon 97403

Received April 9, 1983

Assume that generators are given for a subgroup G of the symmetric group S_n of degree n, and that r is a prime dividing $|G|$. Polynomial-time algorithms are given for finding an element of G of order r, and for finding a Sylow r-subgroup of G if G is simple.

1. INTRODUCTION

Assume that generators are given for a subgroup G of S_n, and let r be a prime dividing $|G|$. This paper is devoted to the proofs of the following theorems.

THEOREM A. *An element of G of order r can be found in polynomial time.*

THEOREM B. *If G is simple then a Sylow r-subgroup of G can be found in polynomial time.*

THEOREM C. *In polynomial time it is possible* (i) *to decide whether or not G has a nontrivial abelian normal r-subgroup; and* (ii) *to find one if there is one.*

The study of polynomial-time algorithms for groups has only recently begun. Only a few of the basic, elementary concepts or results of group theory are presently known to have polynomial-time versions. For example, $|G|$ can be found in polynomial time (Sims [22], Furst, Hopcroft, and Luks [9]), as can the centralizer of a normal subgroup of G (Luks [17]) and a composition series for G (Luks [16]). It was the latter result that motivated the present work. Its proof depended on the recently completed, monumental classification of all finite simple groups. Namely, Luks outlined an

* This research was supported in part by NSF Grant MCS 7903130-82.

0196-6774/85 $3.00

algorithm whose validity required information concerning the outer automorphism groups of all finite simple groups (specifically, that they are solvable).

The proofs of Theorems A and B also require the aforementioned classification. Once again an algorithm is outlined whose validity requires information concerning all finite simple groups. However, here we will need much more detailed information, ranging from bounds on permutation representations (Kantor [13a]) to properties of algebraic groups (Steinberg [24]); and this accounts in part for the length of this paper. Needless to say, it would be preferable to have a much more elementary approach to these results.

Theorem C is comparatively elementary, and is closely related to another result of Luks (see (3.10 ii, iii)). Theorems B and C leave much to be desired. It seems to be difficult to find (in polynomial time) a Sylow r-subgroup or the largest normal r-subgroup of an arbitrary group. In fact, these questions are even open in the case of solvable groups. These difficulties are, in turn, intriguing from the point of view of the P vs NP problem. In general, the type of problem considered here lies in NP, but seems harder than many of the standard types of problems in P. It should be emphasized that Theorems A–C are of a theoretical nature. In "practical" problems in computational group theory, efficient algorithms are used which are actually exponential. The difference in points of view can be seen in Cannon [3]: for him, finding elements of prime order is cheap, finding Sylow subgroups is moderately inexpensive, and testing simplicity is expensive.

The algorithm for Theorem C requires time $O(n^6)$. Those for Theorems A and B can be shown to run in time $O(n^9)$—an indication of their impractical nature.

The paper is organized as follows. Sections 2 and 3 contain terminology and statements of known results. Theorem C is proved in Section 4. In Section 5 the proof of Theorem A is reduced to the case of a simple group of order $> n^8$, at which point Theorem A becomes a very special case of Theorem B. Following this reduction, a very rough outline is presented for Theorem B (along with an indication of which portions to omit if one only wants an algorithm for Theorem A). Thus, Section 5 contains a version of a table of contents for the rest of the paper, along with much of the notation used later. The outline is broken into three parts: preliminaries and the case of alternating groups; $PSL(d, q)$; and the remaining classical groups. While the basic method is similar for the different classes of groups, the technical details greatly increase from one part to the next. The reader may wish to follow each part separately, while using Section 5 for an overview.

Lemma 6.1 explains how simplicity and the bound $|G| > n^8$ are used. Namely, this lemma permits us to assume that G is an alternating group, $PSL(d, q)$, or one of the other classical groups, while giving very precise

information concerning the given permutation representation of G. An algorithm is then given which produces a new permutation representation of G which is more manageable than the original one (the Replacement Theorem 6.2); but the proof of this is postponed, since it involves somewhat different arguments for the three classes of simple groups just mentioned.

The proof of Theorem B finally begins in Sections 7 and 8, where the alternating groups and $PSL(d,q)$ are dealt with. The remainder of the paper concerns the remaining classical groups, and is fairly technical. Section 9 contains background material, including a vector space description (9.4) of the sought-after Sylow subgroups. The nature of this description makes it even clearer why our proof of Theorem B is so intricate and long (and involves so much bookkeeping). It also shows that our algebraic problem can be turned into the geometric problem of finding the stabilizer of a certain type of direct sum decomposition of a vector space. Finally, Sections 10–13 contain the end of the proof of Theorem B, together with additional information concerning the situation being studied. We note that all unexplained notation after Section 4 can be found in Sections 5 or 9; and that the arrangement of lemmas is similar to that of the algorithm in Section 5 but is not quite the same.

It may be that the length of our proof corresponds to the unreasonable size of the exponents obtained. One can only hope that they will be simultaneously shortened in the future. On the other hand, our approach has advantages for future group-theoretic algorithms since the Replacement Theorem provides a method for replacing an "arbitrary" permutation representation of a simple group by a fairly concrete one. For example, the following interesting result is proved in (11.4): for a Chevalley group of characteristic p, a set of representatives of all conjugacy classes of p'-elements can be found in polynomial time.

I am grateful to E. Luks for several stimulating discussions concerning group-theoretic algorithms, and, in particular, for posing the question which Theorem A answers. Moreover, I am indebted to G. M. Seitz for his assistance with [24].

2. Preliminaries

We will assume some familiarity with basic group theory, as contained for example in Rotman's text [21]. Nevertheless, we will begin by listing some standard notation and terminology.

Let G be a group. Subgroup containment is denoted by $H \leqslant G$, and normal containment by $H \trianglelefteq G$. A proper subgroup is any subgroup other than 1 or G. If $S \subseteq G$ then $\langle S \rangle$ is the subgroup generated by S. The size of a set X is denoted $|X|$. The index $|G:H|$ of a subgroup H is $|G|/|H|$. If

$g \in G$ then $|g| = |\langle g \rangle|$ is the order of g. If $S \subseteq G$, then $S^g = \{s^g | s \in S\}$, where $s^g = g^{-1}sg$.

If $K, H \leqslant G$ then $C_H(K) = \{h \in H | hk = kh \text{ for all } k \in K\}$ is the centralizer of K in H. In particular, $C_K(K)$ is the center $Z(K)$ of K. The commutator subgroup G' is $\langle a^{-1}b^{-1}ab | a, b \in G \rangle$. The derived series of G is $G, G', G'' = (G')', G''' = (G'')', \ldots$. If p is a prime than $O_p(G)$ is the unique largest normal p-subgroup of G. A minimal normal subgroup of G is a nontrivial normal subgroup of G not properly containing any other nontrivial normal subgroup of G.

Let X be an n-element set, and consider the symmetric group S_n of permutations of X. If $x \in X$ and $g \in G$ we will use exponential notation x^g for the image of x under g. The orbit of x is $x^G = \{x^g | g \in G\}$; the orbits partition X. It is important to note that G *induces* a permutation group $\overline{G}$ on x^G. The kernel of the action of G on x^G is $K = \{g \in G | g \text{ fixes every point of } x^G\}$, and $\overline{G} = G/K$. More generally, if Y is a second set on which G acts, the kernel of the action is $K = \{g \in G | g \text{ fixes every point of } Y\}$, and $G^Y = G/K$ is the induced group of permutations of Y. If $K = 1$ then G is said to be *faithful* on Y.

The stabilizer G_x is $\{g \in G | x^g = x\}$. Here, $(G_x)^h = G_{x^h}$ for $h \in G$. If $x, x', x'', \ldots, \in X$, write $G_{xx'x''\ldots} = G_x \cap G_{x'} \cap G_{x''} \cap \cdots$. Set $G_{\{x,y\}} = \{g \in G | \{x, y\}^g = \{x, y\}\}$. This is just the stabilizer of $\{x, y\}$ in the action of G on the set of 2-subsets of X. More generally, G also acts on the set of subsets of X of each size. Another useful action of G is that on $X \times X$: simply let $g \in G$ send (x, y) to (x^g, y^g).

If $Y \subseteq X$, the *stabilizer* of Y is $\{g \in G | Y^g = Y\}$. This is the set stabilizer, not the pointwise stabilizer. Similarly, when we say that a group *fixes* a set we will always mean "fixes as a set," not pointwise.

Cosets will always be right cosets. If G is transitive on X, and $x \in X$, then the action of G on X can be identified with its action on the set of cosets of G_x in G. (This action is given by $G_x g \to G_x gh$ for $g, h \in G$.)

Assume that G is transitive on X (so that $x^G = X$ for each x). A G-invariant equivalence relation on X is an equivalence relation $\equiv$ such that $x^g \equiv y^g$ whenever $x \equiv y$. A *block system* for G is the set Σ of equivalence classes of a G-invariant equivalence relation. The trivial examples have $|\Sigma| = 1$ or $|X|$. If these are the only examples, then G is said to be *primitive* on X; otherwise, it is *imprimitive*. In any case, G acts on Σ, inducing a transitive permutation group. If Δ is any block system for this permutation group, then Δ determines a G-invariant equivalence relation on X in an obvious manner. A *minimal block system* is a nontrivial block system Σ such that the permutation group induced on Σ is primitive. A *maximal block system* is a block system of size $< |X|$ having no refinement.

Note that G need not be faithful on a block system Σ. For example, if N is a nontrivial intransitive normal subgroup of G then it is easy to see that

the set Σ of orbits of N on X is a nontrivial block system. Clearly, N is in the kernel of the action of G on Σ—although this kernel may be larger than N.

It is straightforward to prove that *G is primitive if and only if G_x is a maximal subgroup of G*. For, if $G_x < H < G$, then $\{x^{Hg} | g \in G\}$ is a nontrivial block system; the converse is equally easy (cf. Wielandt [26, p. 15]). This also shows that the minimal (or maximal) block systems of a transitive group correspond to those subgroups $H \geqslant G_x$ such that H is maximal in G (or G_x is maximal in H, respectively).

Finally, we will need an elementary number-theoretic result (whose proof is left to the reader). If r is a prime and n is an integer, let n_r be the largest power of r dividing n.

LEMMA 2.1. *Let r be a prime, and let q, t, and z be positive integers such that $q > 1$ and $r | q^t - 1$ but $r \nmid q^x - 1$ for $1 \leqslant x < t$. Then the following hold*:

(i) $r | q^z - 1 \Leftrightarrow t | z$.

(ii) $r | q^z + 1 \Leftrightarrow z$ *and* z/t *are odd integers.*

(iii) *If* $t | z$ *then* $(q^z - 1)_r = (q^t - 1)_r (z/t)_r$ *if* $r \neq 2$, *while* $(q^z - 1)_2 = (q^2 - 1)_2 z_2/2$ *if* $r = 2 | z$.

3. SOME KNOWN ALGORITHMS

Throughout this paper, G will denote a subgroup of the symmetric group S_n, given by a set of generating permutations of the underlying n-set X. Our goal will be to study properties of G, using these generators, in time a polynomial in n.

For example, *finding a subgroup H* with certain properties will always mean "finding generators for H in polynomial time." The basis for everything we do is the following fundamental result of Sims [22]; see Furst, Hopcroft, and Luks [9] or Hoffman [11].

THEOREM 3.1. (i) *Let $X = \{1, \ldots, n\}$. Then the subgroups $G_{1 \ldots i}$, $i = 1, \ldots, n$, can all be found in polynomial time.*

(ii) *$|G|$ can be found in polynomial time.*

In (3.1), $|G_{1 \ldots i} : G_{1 \ldots i-1}|$ is the size of the orbit of i under $G_{1 \ldots i-1}$, and hence is at most $n - (i - 1)$. Orbits are very easy to find:

PROPOSITION 3.2. *If $x \in X$ then x^G can be found in polynomial time.*

The indices just mentioned are all less than n. We will require the following extension of (3.1), which is essentially Theorem 5 of Furst, Hopcroft, and Luks [9] (do not assume that their G_{i+1} is normal in G_i).

THEOREM 3.3. *Let* $G = G(0) \geqslant G(1) \geqslant \cdots \geqslant G(m) = 1$, *where the groups* $G(i)$ *have the following properties*:

(a) *generators for* G *are given*;

(b) $|G(i) : G(i+1)| \leqslant p(n)$ *for all* i, *where* $p(n)$ *is a polynomial*;

(c) $m \leqslant p(n)$; *and*

(d) *given* $g \in G$ *and* $i \leqslant m$, *there is a polynomial-time algorithm for deciding whether* $g \in G(i)$.

Then generators for all $G(i)$ *can be found in polynomial time.*

It is useful to note that any subgroup of S_n has at most $n \log_2 n$ generators. In fact, by Lagrange's theorem:

LEMMA 3.4. *If* $G = G(0) > G(1) > \cdots > G(m) = 1$ *then* $m < n \log_2 n$.

Next, consider primitivity. Atkinson [1] proved

THEOREM 3.5. *Assume that* G *is transitive on* X. *Then the following can be obtained in polynomial time*:

(a) *every minimal block system*; *and*

(b) *a maximal block system.*

In this context, we note the following consequence of (3.3).

LEMMA 3.6. *If* G *is transitive on* X, *and* Σ *is a block system, then the following can be obtained in polynomial time* (*where* $B \in \Sigma$):

(a) *the kernel of the action of* G *on* Σ, *and*

(b) $\{g \in G | B^g = B\}$.

Next, we turn to more structural types of properties of groups. Assume that we are given $G \leqslant S_n$.

PROPOSITION 3.7 (Furst, Hopcroft, and Luks [9]). *If* $\varnothing \neq S \subseteq G$ *then* $\langle S^G \rangle = \langle S^g | g \in G \rangle$ *can be found in polynomial time.*

COROLLARY 3.8 (Furst, Hopcroft, and Luks [9]). *The commutator subgroup* G' *can be found in polynomial time.*

PROPOSITION 3.9 (Luks [17]). *Given* $G, H \leqslant S_n$, *where* G *normalizes* H, *there is a polynomial-time algorithm for finding* $C_G(H)$.

A *composition series* for a group G is a sequence $G = G_0 \rhd G_1 \rhd \cdots \rhd G_k = 1$ such that G_i/G_{i+1} is simple for each i.

THEOREM 3.10 (Luks [16]). *In polynomial time, one can determine*

(i) *a composition series for* G;

(ii) *whether or not* G *has a nontrivial solvable normal subgroup; and*

(iii) *a nontrivial solvable normal subgroup if one exists.*

LEMMA 3.11 (Luks [17]). *If* G *has a normal Sylow* p*-subgroup, then that* p*-subgroup can be found in polynomial time.*

When we use (3.11), G will be solvable, in which case the result follows easily from (3.8).

4. PROOF OF THEOREM C

Use (3.10) to determine whether or not G has a nontrivial abelian normal subgroup. If there is no such subgroup, we are finished. If some such subgroup A exists, use (3.10) and (3.8) to find one (cf. (3.4)). We may assume that A is a p-group for some prime p, and also that $p \neq r$. Use (3.9) to find $C_G(A)$. Then $O_r(G) \neq 1 \Leftrightarrow O_r(C_G(A)) \neq 1$. (For, $O_r(C_G(A))$ is a normal r-subgroup of G, and hence belongs to $O_r(G)$. On the other hand, if $R = O_r(G)$ then $R \leqslant C_G(A)$ since $g^{-1}a^{-1}ga \in R \cap A = 1$ for all $g \in R$, $a \in A$.)

Replace G by $C_G(A)$. Then $A \leqslant Z(G)$. Let Y be the set of all A-orbits on X. Find the kernel B of the action of G on Y (using (3.2) and (3.1)). Then B is a p-group. (For, if $b \in B$ is not a p-element and X_1 is any member of Y, then $|X_1|$ is a power of p so that b fixes some $x \in X_1$. Then $b = b^A$ fixes each member of $x^A = X_1$. Thus, $b = 1$.)

Now replace G by $C_G(B)$ (using (3.9) again). Then we have $B \leqslant Z(G)$. It follows that $O_r(G/B) = O_r(G)B/B$, where $O_r(G)B = O_r(G) \times B$.

If $O_r(G) = 1$ then $O_r(G/B) = 1$. Conversely, applying induction to G/B acting on Y, we can determine whether or not $O_r(G/B) \neq 1$; and, if it is nontrivial, we can find a nontrivial abelian normal r-subgroup M/B of G/B. Here, $B \leqslant Z(M)$, so that $\{m \in M | m$ is an r-element$\}$ is a nontrivial abelian normal r-subgroup of G. □

The main obstacle to finding $O_r(G)$ (in Theorem C) seems to be the problem of finding a *minimal* normal r-subgroup of G. For, given such a subgroup an argument similar to the preceding one easily produces $O_r(G)$.

5. REDUCTION AND OUTLINE OF THEOREMS A AND B

The proof of Theorem A can be reduced to the case of simple groups.

LEMMA 5.1. *If Theorem* A *holds for nonabelian simple groups then it holds for all groups.*

Proof. Let $G \leqslant S_n$. Use (3.10) to find a nontrivial normal subgroup N of G. We may assume that $N \neq G$. Label X as $\{1, \ldots, n\}$ and define $G(0) = G$, $G(i) = G_{12\ldots i}N$ and $G(i+n) = N_{12\ldots i}$ for $1 \leqslant i \leqslant n$. Then each $G(i)$ can be found using (3.3). If r divides $|G(i) : G(i+1)|$, observe that $G(i)$ acts transitively on the set X' of $|G(i) : G(i+1)| < n$ cosets of $G(i+1)$ in $G(i)$. For each generator of $G(i)$, determine its action on these cosets. Then replace G by the permutation group on X' generated by these permutations, and apply induction. The resulting element of order r is induced by an element of the original group. Find all powers of the latter element; some power has order r. □

LEMMA 5.2. *Let c be a constant, and let r be a prime. Given $G \leqslant S_n$ with $|G| = r^a b$ and $b \leqslant n^c$, there is a polynomial-time algorithm for finding all Sylow r-subgroups of G.*

Proof. Luks [15, (3.7)] gives an algorithm for finding one Sylow r-subgroup. Since the number of Sylow r-subgroups is $\leqslant b \leqslant n^c$, all can be found in polynomial time. □

In view of (5.2), Theorems A and B hold if $|G| \leqslant n^8$.

Throughout the remainder of this paper, G will denote a simple subgroup of S_n of order $> n^8$. In this situation, we can ignore Theorem A and concentrate on Theorem B.

The remainder of this section consists of a description of our proof of Theorem B. We will outline an algorithm (in effect, in terms of a large number of procedures each of which runs in polynomial time), and at the same time introduce much of the notation required later. References are given to proofs relating to constructions appearing in the outline. The algorithm falls naturally into three parts: (I) Preliminaries and alternating groups, (II) $G \cong PSL(d, q)$, and (III) G is one of the remaining classical groups.

Part I. Preliminaries and Alternating Groups

(B1) Use (3.2) and (3.5) in order to reduce to the case where G is primitive on the n-set X. (From (6.1) we can then conclude that G is an alternating group or a classical group.)

(B2) Find a new set Y on which G acts transitively ((6.2) and (6.3)). In particular, determine the action on Y of each of the given generators of G.

Remark. We will have $|Y| < 2n$, so that polynomial-time algorithms on Y are also polynomial time on X. Thus, we will always implicitly assume that, whenever a subset of G is computed using the generating permutations

on Y, the corresponding subset is also computed on X. The set Y is a very natural object. When $G \cong A_m$, $|Y| = m$. If G is $PSL(d,q)$ or $PSp(d,q)$ then Y can be identified with the set of all 1-spaces of a d-dimensional vector space V on which G acts in the natural manner. In all other cases, Y can be identified with a certain G-orbit of 1-spaces of the vector space V used to define G. However, we will not actually describe the vectors in V: all references to V are for purposes of explanation or proof, and are not involved in the algorithm itself.

The remainder of the algorithm focuses on Y and ignores X. (See (7.4) for a discussion of this point.)

(B3) Decide whether or not G is an alternating group (by checking whether or not $|G| = \frac{1}{2}(|Y|!)$). If it is, directly construct generators of a Sylow r-subgroup of G. (This is straightforward using Y (7.5).)

From this point on, without loss of generality G will be assumed to be a classical group. In the remainder of this preliminary portion of the algorithm we will discuss all classical groups simultaneously.

(B4) Let $y \in Y$, and use (3.2) in order to determine whether or not G_y is transitive on $Y - \{y\}$. (This transitivity occurs if and only if $G \cong PSL(d,q)$ for some d, q, and thus allows us to detect this situation (10.3).)

(B5) Use (3.1) and Theorem C in order to find a prime p such that $O_p(G_y) \neq 1$ for $y \in Y$. (This prime exists and is unique. It is the characteristic of V by (8.2) and (10.2).)

(B6) Find a new set Y^+ containing Y on which G acts, determining the action on Y^+ of each generator of G. (Here, $|Y^+| < 4n^2$. If G is $PSL(d,q)$ or G is symplectic, then $Y^+ = Y$. In all cases G acts on Y^+ exactly as it acts on the set of *all* 1-spaces of V; we will therefore identify these two sets. A procedure producing Y^+ for an orthogonal or unitary group G is outlined in (10.5).) Let $Y^- = Y^+ - Y$.

This essentially ends Part I. All that remains is to provide additional notation to be used in Parts II and III.

DEFINITIONS 5.3. (i) If $A \subseteq Y^+$ regard $\langle A \rangle$ as a subspace of V.

(ii) If $A \subseteq Y^+$ let $G(A) = \bigcap\{(G_a)' | a \in A\}$. (By (8.3) and (10.6), any desired group $G(A)$ can be found in polynomial time.)

(iii) If $a, b \in Y^+$, $a \neq b$, let $[a,b] = \{c \in Y^+ | G_c \geq G(\{a,b\})\}$. (Use (3.1) to find $[a,b]$. Here, $[a,b]$ is the set of all 1-spaces of the 2-space $\langle a,b \rangle$, by (8.3) and (10.6).)

(iv) If $A \subseteq Y^+$ let $[A]$ be the smallest subset of Y^+ containing A such that $a, b \in [A]$, $a \neq b$, $\Rightarrow [a,b] \subseteq [A]$. (Then $[A]$ is the set of all 1-spaces of $\langle A \rangle$, and can be found in polynomial time by (8.3) and (10.6). Clearly, $G(A)$ is the identity on $\langle A \rangle$ and hence on $[A]$. However, for some A there

can be further points of Y^+ fixed by $G(A)$.)

(v) If $A = \{a_1, \ldots, a_s\}$ write $[A] = [a_1, \ldots, a_s]$.

Part II. $G \cong PSL(d, q)$

In (B4) it was decided whether or not $G \cong PSL(d, q)$ for some (yet unknown) d and q. Assume that G has this form.

(B7) Find a subset $\mathscr{B} = \{y_1, \ldots, y_d\}$ of Y recursively by using any y_1 and letting $y_{k+1} \in Y - [y_1, \ldots, y_k]$. (Then $V = \sum_1^d y_i$ and $d = \dim V < n$ (8.4).)

Abbreviation. Throughout Part II we will let $i = y_i$, except when we wish to indicate that y_i is temporarily being regarded as a 1-space of V.

(B8) Let $1 \leqslant i < d$ and find $t_i \in G$ sending $\mathscr{B}$ to itself and inducing the transposition $(i, i+1)$ on $\mathscr{B}$. (Use (3.1); cf. (8.5).) Let $c = t_1 t_2 \cdots t_d$.

(B9) Obtain a conjugate of each cyclic Sylow subgroup of G as follows. Use (3.1) to find $Q = G_{23\ldots d}$. (This is a group of order $< n^2$.) Take each element g in the coset Qc, and take p-powers of g until an element is obtained whose order is not divisible by p. Then *each element of G of order not divisible by p is conjugate to one of the elements just obtained* (8.6).

Remark. (B9) is much stronger than Theorem A. Those interested only in Theorem A should omit the rest of Part II (i.e., (B10)–(B23)).

(B10) If $r = p$ in Theorem B, find a Sylow r-subgroup U of G as follows.

(i) Find subgroups $B(1), \ldots, B(d-1)$ recursively, by setting $B(1) = G_{y_1}$, and using (3.1) to find the stabilizer $B(k+1)$ of $[1, \ldots, k+1]$ in the action of $B(k)$ on $[1, \ldots, k+1]^{B(k)}$. (The latter set has size $< n$.)

(ii) For each generator g of $B(d-1)$ find a Sylow p-subgroup of $\langle g \rangle$ and let U be the subgroup of $B(d-1)$ generated by all of these (8.8).

Throughout the remainder of Part II, assume without loss of generality that $r \neq p$.

(B11) Find q: it is the largest power of p dividing $|Y| - 1$. (In fact, $|Y| = (q^d - 1)/(q - 1)$.)

(B12) If $r = 2$ let $k = 2$. If $r > 2$ let k be the smallest positive integer such that $r | q^k - 1$. (Here, $k < d < n$ since $r \,||G|$.) Let $l = [d/k]$.

If $l = 1$ then a Sylow r-subgroup of G is cyclic (8.10(ii)), and hence one was already found in (B9). Thus, *we may assume without loss of generality that* $l \geqslant 2$.

(B13) Find $H = G_{12\ldots d}$ using (3.1), and let $N = \langle H, t_i | 1 \leqslant i < d \rangle$. (Here $H \lhd N$, $|H| < n$ and $N/H \cong S_d$ (8.9).)

(B14) If $k = 1$ use (B3) or (7.6) to find a Sylow r-subgroup F/H of N/H, and then use (5.2) to find a Sylow r-subgroup R of F. Then R is a Sylow r-subgroup of G (8.10).

Now assume without loss of generality that $k \geqslant 2$.

(B15) For $1 \leqslant i \leqslant d$ find $G(\mathscr{B} - \{i\})$.

(B16) For $1 \leqslant i \leqslant k$ find the set stabilizer T_i of $[1, \ldots, k]$ in $G(\mathscr{B} - \{i\})$. (The orbit of $[1, \ldots, k]$ under the latter group has size $< n$, so that (3.1) can be used.) Let $S = \langle T_i | 1 \leqslant i \leqslant k \rangle$. (Then $S \cong SL(\langle y_1, \ldots, y_k \rangle) = SL(k, q)$ by (8.11).)

(B17) Find a Sylow r-subgroup R_0 of S. (This is possible by induction (8.12).)

Remark. Actually, both here and later in (B29(v)) and (B35) induction is not involved. All that is used is a single minimal situation (namely, (B9) at present and (B27) later).

(B18) Find the group E of all elements of $N_{kl+1,\ldots,d}$ that fix (as a whole) each row of the following array, while permuting the columns.

$$\begin{array}{cccc} 1 & k+1 & & k(l-1)+1 \\ 2 & k+2 & & k(l-1)+2 \\ \vdots & \vdots & \cdots & \vdots \\ k & 2k & & kl \end{array}$$

(Here $H \triangleright E$ and $E/H \cong S_l$, where S_l is induced on each row (8.13).)

(B19) Find a Sylow r-subgroup F/H of E/H, using (7.6).

(B20) Find a Sylow r-subgroup R^* of F (use (5.2), since $|H| < n$).

(B21) Find $\Sigma = \{S^e | e \in E\}$, where $|\Sigma| = l$ (8.15). Then find the R^*-orbits on Σ, and let $S^{e(i)}$ be orbit representatives for $i = 1, \ldots, l'$, where $e(1) = 1$ and l' is the number of R^*-orbits on Σ.

(B22) Let $r \neq 2$. Let $R = \langle R^*, R_0^{e(i)} | i = 1, \ldots, l' \rangle$. Then R is a Sylow r-subgroup of G (8.15).

(B23) Let $r = 2$. Use (5.2) in order to find a Sylow 2-subgroup R of $\langle \langle S^E \rangle, H, R^* \rangle$. Then R is a Sylow 2-subgroup of G (8.15).

Part III. The Remaining Classical Groups

If G is neither A_m nor $PSL(d, q)$ for some m or d, q, then G must be a symplectic, unitary, or orthogonal group defined on a vector space V (6.1). We know the characteristic p of V (B5).

The goal in Part III is to imitate Part II as much as possible. Many of the sets, groups, and elements appearing in Part II have analogues in the

present situation. Eventually, we will wind up able to repeat portions of Part II using these analogues.

DEFINITION 5.4. Define the relations $\sim$ and $\nsim$ as follows: if $y, z \in Y$ and $y \neq z$ then

$$y \sim z \Leftrightarrow O_p(G_{yz}) \neq 1$$
$$y \nsim Z \Leftrightarrow O_p(G_{yz}) = 1.$$

By Theorem C, we can decide whether $y \sim z$ or $y \nsim z$ in polynomial time.

Remark. By (B2), we may identify Y with a certain set of 1-spaces of V. By (10.2), $y \sim z \Leftrightarrow y \subset z^{\perp}$. (Here, $\perp$ is the natural perpendicularity relation induced by the bilinear form on V; cf. Sect. 9.)

(B24) Define a subset $\mathscr{B} = \{y_1, \ldots, y_m, z_1, \ldots, z_m\}$ recursively as follows: y_1 is arbitrary, and $z_1 \nsim y_1$ is arbitrary; if $\{y_1, \ldots, y_i, z_1, \ldots, z_i\}$ has been found, test each $y \in Y$ to see if $y \sim y_j$ and $y \sim z_j$ for all $j \leqslant i$; if no y exists, let $m = i$; if y exists, let $y_{i+1} = y$; testing as above, find $z_{i+1} \nsim y_{i+1}$ such that $z_{i+1} \sim y_j$ and $z_{i+1} \sim z_j$ for $j \leqslant i$; finally, replace $\{y_1, \ldots, y_i, z_1, \ldots, z_i\}$ by its union with $\{y_{i+1}, z_{i+1}\}$. (By (11.1(i)), this procedure terminates and takes polynomial time. By (11.1(ii)), $V = \{\sum_1^m \langle y_i, z_i \rangle\} \oplus V_0$, where V_0 contains no member of Y.)

Abbreviation. Throughout (B25)–(B30) we will write $i = y_i$ and $i' = z_i$ for $1 \leqslant i \leqslant m$.

(B25) Let $1 \leqslant i < m$, and find $t_i \in G$ sending $\mathscr{B}$ to itself and inducing $(i, i+1)(i', (i+1)')$ on $\mathscr{B}$. (Use (3.1); cf. (11.2).) Find $t_m \in G$ sending $\mathscr{B}$ to itself and inducing (m, m') on $\mathscr{B}$, if such an element of G exists. (Use (3.1) to find such an element or to decide that none exists.) If no such element exists, find $t_m \in G$ sending $\mathscr{B}$ to itself and inducing $(m-1, (m-1)')(m, m')$. (There is always a t_m defined in one of these ways (11.2).) Let $c = t_1 t_2 \cdots t_m$ and $c' = c t_m c^{-1} t_m c^{-1}$.

(B26) Find $Q = O_p(G_1)$ as follows. Use Theorem C to find a nontrivial normal p-subgroup Q_0 of G_1. If $|Q_0| > |Y|^{1/2}$ let $Q = Q_0$. Otherwise, regard G_1 as a permutation group on the set of Q_0-orbits, use Theorem C to find a nontrivial normal p-subgroup of that group, and let Q be the preimage of that p-group in G_1 (11.3). (Then $|Q| < 4n^2$ (11.3).)

(B27) Obtain a conjugate of each cyclic Sylow subgroup of G as follows. Use (3.1) to find $H = G_{12 \cdots 2m}$. (Then $|QH| < 64n^6$ (11.3).) Take each element g in the union $Qc \cup QHc'$, and take p-powers of g until an element is obtained whose order is not divisible by p. Then, as in (B9), *each element of G of order not divisible by p is conjugate to one of the elements just obtained* (11.4).

Remark. (B27) *completes the algorithm for Theorem A.* Moreover, when describing an algorithm for Theorem B we may assume that a conjugate of each cyclic Sylow subgroup has already been found.

Convention. "Repeat" will always mean "repeat using the present values of the various variables involved."

(B28) If $r = p$ let $d = m$ and repeat (B10) (11.6).

Throughout the remainder of Part III, we may assume without loss of generality that $r \neq p$.

DEFINITION 5.5. Let $a \in Y^+$. Define a^* as follows. (In each case a^* will be the set of 1-spaces in $a^\perp$ (10.7).)

(i) If $a \in Y$ let $a^* = [\{b \in Y | a \sim b\}]$.

(ii) If $a \in Y^+ - Y$ let $a^* = [\{b \in Y | [a, b] \cap Y = \{b\}\}]$.

DEFINITION 5.6. If $A \subseteq Y^+$ let $A^* = \{b \in Y^+ | A \subseteq b^*\}$. (This is the set of all 1-spaces in $A^\perp$, and can be found in polynomial time (10.7).)

Remark. The cases $Y^+ = Y$ and $Y^+ \neq Y$ are somewhat different (cf. (9.4)). The former case corresponds to symplectic groups (11.5), and will be handled in a manner very closely paralleling Part II (B29).

(B29) If $Y^+ = Y$ proceed as follows:

(i) Repeat (B11) (10.4).

(ii) Let $k = 1$ if $r = 2$, otherwise repeat (B12).

(iii) Let $S = G(\{1, \ldots, k, 1', \ldots, k'\}^*)$. (This is essentially a symplectic group (12.1).)

(iv) Find the group E of all elements of G which fix $\{1, \ldots, m\}, \{1', \ldots, m'\}, kl + 1, \ldots, m$, and act on the array in (B18) as indicated there. (As in (B18), $H \lhd E$ and $E/H \cong S_l$ (12.2).)

(v) Repeat (B17), (B19), and (B20) (12.3).

(vi) If $k > 1$ repeat (B21) and (B22) in order to obtain a Sylow r-subgroup of G (12.4).

(vii) If $k = 1$ use (5.2) in order to find a Sylow r-subgroup R of $\langle \langle S^E \rangle, H, R^* \rangle$. Then R is a Sylow r-subgroup of G (12.5).

From now on *we may assume without loss of generality that* $Y^+ \neq Y$. Recall that $Y^- = Y^+ - Y$ (B6).

(B30) If Q is abelian let q be the largest power of p dividing $|Y| - 1$; otherwise, let q^2 be the largest power of p dividing $|Y| - 1$. (Then q is the "q" in the name $\Omega^{\pm}(d, q)$ or $SU(d, q)$ (10.4), where d will be found in (B32).)

(B31) (i) If $r \neq 2$, or if $r \nmid q+1$ and Q is nonabelian, define Z, S and subsets $Y_0, Y_1, \ldots, Y_b$ recursively as follows. First, $Y_0 = \emptyset$. Next, given Y_i, test each $y \in Y - Y_i$ for the condition $r \,||G(Y_i \cup \{y\})|$. If some such y exists let $Y_{i+1} = [Y_i, y]$; otherwise let $b = i$. Moreover, let $Z = Y_b^*$ and $S = G(Y_b) = G(Z^*)$.

(ii) If $2 \neq r|q+1$ and Q is nonabelian let $u_1 \in Y^-$, $Z = \{u_1\}$ and $S = 1$. If $r = 2$ let $Z = [u_1, u_2]$ and $S = G(Z^*)$, where $u_1, u_2 \in Y^-$, $u_2 \in u_1^*$, and $2 \,||S|$. (The various definitions of Z and S are motivated by (9.4, Case 2); cf. (13.1).)

(B32) Let $u_1, \ldots, u_k \in Z \cap Y^-$ be defined recursively by letting $u_1 \in Z \cap Y^-$ be arbitrary and letting $u_i \in Z \cap Y^-$ satisfy either

(5.7) If $p \neq 2$ or Q is nonabelian then $u_{i+1} \in \{u_1, \ldots, u_i\}^*$,

or

(5.8) If $p = 2$ and Q is abelian then $u_{2j+1}, u_{2j+2} \in \{u_1, \ldots, u_{2j}\}^*$ where $[u_{2j+1}, u_{2j+2}] \cap [u_{2j+1}, u_{2j+2}]^* = \emptyset$.

If there are no u_{i+1} or u_{2j+1}, u_{2j+2} in **(5.7)** or **(5.8)**, let $k = i$ or $2j$, respectively. (Then $\{u_1, \ldots, u_k\}$ arises from a basis of Z, which is orthogonal in the case of **(5.7)**; cf. (13.1).)

(B33) Define d, d', $l = [d'/k]$, and $u_{k+1}, \ldots, u_d$ recursively by requiring that (i) $u_i \in Y^-$ and either **(5.7)** or **(5.8)** holds; (ii) $u_i \in (u_{i-k})^G$ for $k < i \leqslant d'$, and also, in the situation in **(5.8)**, $\{u_{2j+1}, u_{2j+2}\} \in \{u_{2j+1-k}, u_{2j+2-k}\}^G$ for $k < 2j+2 \leqslant d'$; (iii) d' is maximal subject to (ii); and (iv) $\{u_1, \ldots, u_d\}^* = \emptyset$, unless $Y^* \neq \emptyset$, in which case $\{u_1, \ldots, u_{d-1}\}^* \cap Y^* = \emptyset$ and $\{u_1, \ldots, u_{d-1}\}^* = Y^* = \{u_d\}$. (Then $d = \dim V$, and $\{u_1, \ldots, u_d\}$ arises from a basis for V which has been tailored for r (13.1).)

(B34) Find the group E of all elements of G that fix $\{u_1, \ldots, u_d\}$ and act on the subscripts as in (B18). Also, let $H = G_{u_1 \ldots u_d}$. (This is a new value for H (13.2).)

(B35) Repeat (B17), (B19), and (B20) (13.3).

(B36) If $k > 2$ repeat (B21) and (B22) in order to obtain a Sylow r-subgroup of G (13.3).

(B37) If $k \leqslant 2$ repeat (B29(vii)) in order to obtain a Sylow r-subgroup of G (13.3). □

6. Permutation Representations of Simple Groups

The remainder of this paper concerns simple groups (see Sect. 5). In this section we will present an algorithm for passing from a sufficiently large primitive simple group to its "most natural" permutation representation.

We will need the following property of simple groups (compare Cameron [2, (6.1)]).

LEMMA 6.1. *Let G be a primitive simple subgroup of S_n, where $|G| > n^8$. Then one of the following holds:*

(i) *G is A_m acting on the set of k-sets of an m-set, for some k;*

(ii) *G is A_m acting on the set of partitions of an m-set into m/k sets of size k, for some k satisfying $1 < k < m$; or*

(iii) *G is a classical group defined on vector space of dimension at least 9, and the stabilizer of a point is reducible.*

Remarks. For properties of Chevalley groups required in the proof of (6.1), we refer to Carter [4]. For further discussion of classical groups, see Section 9.

In order for (iii) to be accurate, we implicitly use the isomorphism $Sp(2m, 2^i) \cong \Omega(2m + 1, 2^i)$ in order to assume that the underlying vector space has dimension $2m + 1$ in this case.

Proof. Let X and G_x be as usual. We may assume that G is an alternating or Chevalley group (see Gorenstein [10] for a discussion of the classification[1] of all finite simple groups).

If $G \cong A_m$, and M is the m-set upon which G naturally acts, then we may assume that G_x is primitive on M; for otherwise, (i) or (ii) holds. By a classical result of Bochert (Wielandt [26, p. 41]), $n = |G: G_x| \geqslant \frac{1}{2}([\frac{1}{2}(m + 1)]!)$. Thus, $80n^3 > |G|$, which is not the case.

If G is a classical group and if (iii) does not hold, then $|G| < n^8$ by Patton [20], Cooperstein [6], and Kantor [14, Theorems 1, 2].

Suppose that G is not a classical group, and let π be the permutation character of G on X. Then $n = \pi(1)$, while π is the sum of the principal character 1_G of G and some nonprincipal irreducible characters χ. Now $n > \chi(1)$, while $\chi(1)$ is bounded below by the results tabulated in Landazuri and Seitz [27, p. 419]. If $G \neq E_7(q)$, $E_8(q)$ then these bounds imply (using [4, pp. 144, 155, 262; or 10] for $|G|$) that $|G| < \chi(1)^8 < n^8$. If $G = E_7(q)$ or $E_8(q)$ then G is not 2-transitive on X (by [7]) and hence $\pi - 1_G$ is the sum of at least two irreducible characters χ, so that $(n - 1)/2$ is at least the bound in [14]; again a simple calculation yields the desired inequality $|G| < n^8$. □

We now introduce two procedures.

[1]At the time of writing (October, 1982), this classification is not quite complete: the uniqueness of the Monster has not been proved. However, this does not cause any difficulties with our use of the classification.

Pairing. Given G acting transitively on an n-set X, and given $x \in X$, this produces a family $\mathcal{M} = \mathcal{M}(G_x)$ of maximal subgroups, as follows.

(i) For each $y \in X$ find $G_{\{x,y\}}$.

(ii) Find each proper subgroup H of G such that $G_{\{x,y\}}$ is a maximal subgroup of H; if no such H exists let $H = G_{\{x,y\}}$.

(iii) For each such H find each proper subgroup H^* of G such that H is a maximal subgroup of H^*; if no such H exists let $H^* = H$.

(iv) For each H^* find a maximal subgroup M of G containing H^*.

(v) $\mathcal{M}$ consists of those maximal subgroups M for which $|G: M| < 2n$.

Double-Pairing. Given G and X as in *Pairing*, this produces a family $\mathcal{M}'$ of maximal subgroups of G; namely, pick $x \in X$ and let

$$\mathcal{M}' = \cup\{\mathcal{M}(M) | M \in \mathcal{M}(G_x)\}.$$

Remark. If $M \in \mathcal{M}(G_x)$ then each given generator for G acts on the set of cosets of M in G. Since $|G: M| < 2n$, the action on this set can be determined in polynomial time. Note that, by (3.1), (3.2), and (3.5), both *Pairing* and *Double-Pairing* run in polynomial time. Also, since y is allowed to be x in *Pairing*, $\mathcal{M}(G_x) \subseteq \mathcal{M}'$ in *Double-Pairing*.

THEOREM 6.2 (Replacement Theorem). *Given a primitive, simple subgroup G of S_n for which $|G| > n^8$, apply Double-Pairing. Let $M_1 \in \mathcal{M}'$ have maximal size. Let $P = M_1$, unless there is another subgroup $M_2 \in \mathcal{M}'$ satisfying $|G: M_1| < |G: M_2| < 2|G: M_1|$, in which case let $P = M_2$. Then*

(i) *P is unique up to conjugacy in* Aut G *(in fact, in G unless $G \cong PSL(d, q)$ for some d and q);*

(ii) *P and its conjugates are the largest maximal subgroups of G (unless $G \cong Sp(2m, 2)$ for some m, in which case they are the second largest maximal subgroups); and*

(iii) *P can be found in polynomial time.*

The proof of Theorem 6.2 will be given later, in three separate pieces: alternating groups in Section 7, $PSL(d, q)$ in Section 8, and all remaining cases in Section 10. Of course, (iii) is obvious since Double-Pairing runs in polynomial time.

The above theorem is, perhaps, unnecessarily opaque. The use of $2n$ instead of n, and the irritating appearance of M_2, are concessions to the groups $Sp(2m, 2) \cong \Omega(2m + 1, 2)$ defined over $GF(2)$: for technical reasons, M_2 is preferable to M_1. For all other groups G, there is no maximal subgroup M_2 satisfying the inequality in Theorem 6.2, and hence M_2 can be ignored.

DEFINITION 6.3. Y is the set of cosets of P in G. Thus, $|Y| < 2n$.

Once we have found Y, we will work primarily with it, leaving X in the background. In particular, we will assume that the action on Y has been found for the given generators of G (cf. (7.4)).

7. ALTERNATING GROUPS

Many aspects of the proof of Theorem B are much simpler when the simple group G is alternating. Nevertheless, many of the ideas in this case resemble those encountered later.

Throughout this section, $G \leqslant S_n$ will be isomorphic to some alternating group, and $|G| > n^8$. (In fact, we only need $|G| > 80n^3$.)

By (3.2) and (3.5), we may assume that $G \cong A_m$ acts primitively on an n-set X. Thus, (6.1) applies.

Proof of Theorem 6.2 for $G \cong A_m$. It is well known that G has just one conjugacy class of subgroups of index $\leqslant m$ (Wielandt [26, p. 42]). In fact, the method of proof indicated there is the same as the alternating group part of the proof of (6.1), and shows that there is just one conjugacy class of proper subgroups of index $< 2m$. *Thus, we only need to exhibit a subgroup of index m in G produced by Double-Pairing.* In view of (6.1), there are two cases to consider.

Case 1. G_x is the stabilizer of a k-subset K of the m-set Z on which G acts in the usual manner. (Note that we no longer need to worry about finding Z: we are merely studying properties of G.) We may assume that $k \leqslant \frac{1}{2}m$. Pick any k-subset K' of Z such that $|K \cap K'| = 1$, and let G_y be its stabilizer in G. Clearly, $G_{\{x,y\}}$ contains 3-cycles. Consequently, the only proper subgroups of G properly containing $G_{\{x,y\}}$ are the stabilizer of $K \cap K'$, the stabilizer of $K \cup K'$, and the intersection of these groups. It follows that the stabilizer of a point of Z belongs to $\mathscr{M}(G_x)$, and hence also to $\mathscr{M}'$.

It is important to note that we did not need *Double-Pairing* in the preceding case: *Pairing* sufficed.

Case 2. G_x is the stabilizer of a partition Π of Z into $l = m/k$ sets of size k, where $1 < k < m$.

Let $\Pi = \{B_1, \ldots, B_l\}$. Pick any $b_1 \in B_1$ and $b_2 \in B_2$, and let $B_1' = (B_1 - \{b_1\}) \cup \{b_2\}$, $B_2' = (B_2 - \{b_2\}) \cup \{b_1\}$, and $\Pi' = \{B_1', B_2', B_i | 3 \leqslant i \leqslant l\}$. Then $\Pi' \in \Pi^G$, so that the stabilizer of Π' has the form G_y for some $y \in X$. Clearly, $G_{\{x,y\}}$ preserves $\{B_i | 3 \leqslant i \leqslant l\}$, $A = \{b_1, b_2\}$ and $A' = (B_1 \cup B_2) - \{b_1, b_2\}$. Let H be the stabilizer in G of the partition $\{A, A', B_i | 3 \leqslant i \leqslant l\}$; clearly, H is one of the minimal subgroups contain-

ing $G_{\{x,y\}}$. Let H^* be the stabilizer of the partition $\{A \cup A', B_i | 3 \leqslant i \leqslant l\}$. If $l \neq 4$ then the only maximal subgroup M of G containing H^* is the stabilizer of $A \cup A' = B_1 \cup B_2$. (N.B.—If $l = 4$ then the only maximal subgroup of G containing H^* is the stabilizer of the pair $\{B_1 \cup B_2, B_3 \cup B_4\}$ of $2k$-sets. If we had defined a procedure "*Triple-Pairing*," we could revert to the case $l = 2$ and then complete the proof. Instead, we will stick with *Double-Pairing* and proceed somewhat differently when $l = 4$.)

Consequently, if $l \neq 4$ then $\mathscr{M}(G_x)$ contains a maximal subgroup M of the sort already handled in Case 1. Thus, $\mathscr{M}(M)$ contains a subgroup having index m in G, as required.

Now let $l = 4$. We will construct new subgroups H, H^*, and M. Clearly, $n = 4k > 8$. Let $b_1, b_1' \in B_1$, $b_1 \neq b_1'$, $b_2 \in B_2$, and $b_3 \in B_3$. This time, let $B_1' = (B_1 - \{b_1, b_1'\}) \cup \{b_2, b_3\}$, $B_2' = (B_2 - \{b_2\}) \cup \{b_1\}$, $B_3' = (B_3 - \{b_3\}) \cup \{b_1'\}$, and $B_4' = B_4$, and let G_y be the stabilizer of $\{B_1', B_2', B_3', B_4'\}$ in G. Then G_y preserves the sets $A_1 = \{b_1, b_1'\}$, $A_2 = \{b_2, b_3\}$, $A_1' = B_1 - A_1$, $A_2 = B_2 - \{b_2\}$, $A_3 = B_3 - \{b_3\}$, and B_4'. Also, $G_{\{x,y\}}$ preserves the partition $\{A_1, A_2, A_1', A_2 \cup A_3, B_4'\}$ of X. Let H be the stabilizer of this partition, and let H^* be the stabilizer of the partition $\{A_1, A_2, A_1', A_2 \cup A_3 \cup B_4'\}$. Finally, let M be a maximal subgroup of G containing H^*. Then M is the stabilizer of one of the sets $A_1, A_2, A_1', A_1 \cup A_2, A_1 \cup A_1', A_2 \cup A_1'$, or $A_1 \cup A_2 \cup A_1'$ in G, while $M \in \mathscr{M}(G_x)$. By Case 1, $\mathscr{M}(M)$ contains a subgroup having index m in G, as required.

This completes the proof of Theorem 6.2 when $G \cong A_m$. □

Recall that the set Y was defined in (6.3).

LEMMA 7.3. *In polynomial time one can find an element of G inducing any of the following on Y*:

(i) *a 3-cycle*;

(ii) *the product of two 2-cycles on any given 4-set of Y*; *and*

(iii) *an r-cycle on any given r-set of Y, for any odd* $r \leqslant m$.

Remark 7.4. It is crucial, both here and in the remainder of the paper, to understand what is really being "found" in this type of lemma. We start with permutations on an n-set X which generate our group G. Once Y is found, we can determine how each of these generators acts as a permutation on Y as well. In (7.3), the desired permutation g of Y is found as a product of generators and their inverses, and this product is calculated as a permutation of both X and Y. Various of these gs can then be multiplied together, both as permutations of X and of Y.

Proof. Use (3.1) in order to find the pointwise stabilizer of an arbitrary set of $m - 3$ or $m - 4$ points of Y. This readily yields (i) and (ii). If r is as in (iii) and R is any r-set of Y then it is easy to write a product of at most

$r \leqslant m \leqslant n$ 3-cycles on R that is an r-cycle on R. Using the 3-cycles we have found, we can thus find an r-cycle as required in (iii). □

LEMMA 7.5. *Let r be a prime dividing $|G|$. Then a Sylow r-subgroup of G can be found in polynomial time.*

Proof. Let $k = [m/r]$, and fix a partition of Y into a set of size $m - kr$ and a family Σ of k sets of size r. First assume that $r \neq 2$. If $A \in \Sigma$ use (7.3) to find an r-cycle of Y acting as $(a_1, a_2, \ldots, a_r)$ on A; fix this labeling $a_1, \ldots, a_r$ of A. These r-cycles generate a Sylow r-subgroup of G if $k \leqslant 2$, so assume that $k \geqslant 3$. Let A, B, C be distinct members of Σ, and let $(a_1, \ldots, a_r)$, $(b_1, \ldots, b_r)$, and $(c_1, \ldots, c_r)$ be the corresponding r-cycles. Use (7.3(i)) to find the product $(a_1, b_1, c_1) \cdots (a_r, b_r, c_r)$ of 3-cycles. As A, B, and C vary over Σ we obtain $\binom{k}{3}$ elements of order 3 generating a group A_k that normalizes the group generated by our r-cycles. The group of order $r^k|A_k|$ generated by our r-cycles and 3-cycles contains a Sylow r-subgroup of G. Now apply induction.

Next let $r = 2$. Let $A = \{a_1, a_2\}$ and $B = \{b_1, b_2\}$ belong to Σ. Use (7.3(ii)) to find $(a_1, a_2)(b_1, b_2)$ and $(a_1, b_1)(a_2, b_2)$. As A and B vary over Σ, these generate a group of order $2^{k-1}|S_k|$ that is a semidirect product of $\mathbf{Z}_2^{k-1}$ and S_k and that contains a Sylow 2-subgroup of G. It is now straightforward to find such a Sylow subgroup inductively. □

Remark 7.6. A similar result holds when $G \leqslant S_n$ is given and $G \cong S_m$. The proof is the same as that of (7.5).

8. $PSL(d, q)$

We next turn to the situation in which $G \cong PSL(d, q)$, where $d \geqslant 9$ by (6.1). Let V be the d-dimensional vector space for G.

LEMMA 8.1. *If $H < G$ and $|G: H| < 2(q^d - 1)/(q - 1)$ then $|G: H| = (q^d - 1)/(q - 1)$ and H is the stabilizer of a 1-space or a hyperplane of V.*

Proof. Kantor [14, Theorem 1]. In fact, this is an easy consequence of (6.1). □

Proof of Theorem 6.2 for $G = PSL(d, q)$. By (8.1), we only need to exhibit a subgroup of G of index $(q^d - 1)/(q - 1)$ produced by *Pairing*.

There is a proper subspace W of V fixed by G_x. By passing to the dual space of V if necessary, we may assume that $\dim W \leqslant \frac{1}{2}d$. There is an element $g \in G$ such that $W^{g^2} = W$ and $\dim W \cap W^g = 1$. Set $y = x^g$.

Let H be the stabilizer (in G) of both $W \cap W^g$ and $\langle W, W^g \rangle$, and let H^* be the stabilizer of the 1-space $W \cap W^g$. Then $G_{\{x,y\}}$ is a maximal

subgroup of H while H is a maximal subgroup of H^* (e.g., by McLaughlin [18, 19]). Thus, $H^* \in \mathcal{M}(G_x)$ (since $|G: H^*| \leqslant n$ by (8.1)). □

Recall that Y was defined in (6.3) as the set of cosets in G of the subgroup produced by *Double-Pairing*. In view of (8.1), we can replace V by its dual space, if necessary, in order to *identify Y with the set of all 1-spaces of V.*

LEMMA 8.2. *There is a unique prime p such that $O_p(G_y) \neq 1$ for $y \in Y$. This prime divides q, and can be found in polynomial time.*

Proof. Using a basis of V whose first member is "in" y, we find that G_y arises from the matrices

$$\begin{pmatrix} \alpha & 0 & \cdots & 0 \\ \beta_1 & & & \\ \vdots & & A & \\ \beta_{d-1} & & & \end{pmatrix}$$

with $\alpha, \beta_i \in GF(q)$ and $\alpha \det A = 1$. A simple calculation now proves the first part of the lemma. (Note that $O_p(G_y)$ arises from those matrices having $\alpha = 1$ and $A = I$.) Now apply Theorem C in order to find p.

Set $Y^+ = Y$ in (B6) and (5.3) in order to define $\langle A \rangle$, $G(A)$, and $[A]$.

LEMMA 8.3. *Let $A \subseteq Y$. Then*

(i) *$G(A)$ can be found in polynomial time, and induces the identity on $\langle A \rangle$;*

(ii) *$[A]$ is the set of all 1-spaces in $\langle A \rangle$; and*

(iii) *$[A]$ can be found in polynomial time.*

Proof. (i) Fix $y \in Y$. Use (3.1) and (3.8) to find $(G_y)'$. Note that $|G_y: (G_y)'| \leqslant q - 1 < n$ (since $(G_y)'$ is just the stabilizer of a vector $v \in y - \{0\}$). Thus, $|G: (G_y)'| < n^2$. For each $a \in A$ find $g(a) \in G$ with $y^{g(a)} = a$ (use (3.2)). Then $G(A)$ is the pointwise stabilizer of $\{(G_y)'g(a) | a \in A\}$, and hence can be found by applying (3.1) to the permutation representation of G on the set of cosets of $(G_y)'$.

(ii) If $a \neq b$ then $G(\{a, b\})$ moves every vector in $V - \langle a, b \rangle$.

(iii) Let $B \subset A$ and $a \in [A] - [B]$. Then $[B \cup \{a\}] = \cup\{[a, b] | b \in [B]\}$. □

Now define $\mathcal{B} = \{y_1, y_2, \ldots\}$ recursively by starting with an arbitrary y_1, and letting $y_{k+1} \in Y - [y_1, \ldots, y_k]$ whenever the latter set is nonempty.

COROLLARY 8.4. (i) *$|\mathcal{B}| = d$, and $V = \Sigma_1^d y_i$.*

(ii) *$\mathcal{B}$ can be found in polynomial time.*

Proof. (i) By (8.3), $\dim\langle y_1, \ldots, y_k\rangle = k$ for each k.

(ii) See (8.3(iii)). □

Remark. *Throughout this section, matrices will be written with respect to a basis $v_1, \ldots, v_d$ of V for which $v_i \in y_i$.*

LEMMA 8.5. *Let t_i and c be defined as in* (B8).

(i) *As permutations on both X and Y, these elements can be found in polynomial time.*

(ii) $c = (d, \ldots, 2, 1)$ *on* $\mathscr{B}$.

Proof. (i) By elementary linear algebra, t_i exists. Use (3.1) to find the stabilizer of each member of $\mathscr{B} - \{i, i+1\}$ and of $\{i, i+1\}$, and test its generators to find an element moving i. This produces t_i in polynomial time. Once the permutations t_i have been found on X and Y, c can also be found.

(ii) Calculate. □

PROPOSITION 8.6. *Let $PSL(d, q) \cong G \leqslant S_n$, where $|G| > n^8$. Let p be the prime dividing q. Then there is a polynomial-time algorithm for finding a subset of G (of size $< n^2$) such that every element of G of order not divisible by p is conjugate to a power of an element of that set.*

Proof. By (8.3(i)), $G(\mathscr{B} - \{1\})$ arises from the group of all matrices

$$\begin{pmatrix} 1 & \beta_1 & \cdots & \beta_{d-1} \\ & 1 & & \\ & & \ddots & 0 \\ & & & \ddots \\ 0 & & & 1 \end{pmatrix}$$

with $\beta_i \in GF(q)$. Thus, $|G(\mathscr{B} - \{1\})| = q^{d-1} < n^2$. By Steinberg [24, (9.4); or 23, (III.2.11)], the coset $G(\mathscr{B} - \{1\})c$ behaves as indicated. □

Remark 8.7. The group Q appearing in (B9) clearly contains $G(\mathscr{B} - \{1\})$.

The above proof is intended to provide a pattern for (11.4). An elementary proof is obtained by observing that $G(\mathscr{B} - \{1\})c$ contains each element of G arising from the companion matrix

$$\begin{pmatrix} \beta_1 & \beta_2 & \cdots & 1 & \\ 1 & & & & \\ & 1 & & 0 & \\ 0 & & \ddots & & \\ & & & 1 & 0 \end{pmatrix}$$

of each monic polynomial $f(t)$ of degree d and constant term $(-1)^d$. If

$A \in SL(d,q)$ and p does not divide the order of A, let $g(t)$ be its minimal polynomial and set $f(t) = g(t)(t-1)^{d-\deg g}$. Then the above matrix has a power conjugate to A in $SL(d,q)$.

LEMMA 8.8. *A Sylow p-subgroup of G can be found in polynomial time.*

Proof. Define $B(k)$ and U as in (B5). By induction on k, $B(k)$ fixes $\langle y_1\rangle, \ldots, \langle y_1, \ldots, y_k\rangle$: by (8.3), $[y_1, \ldots, y_i]$ is the set of 1-spaces in the $k+1$-space $\langle y_1, \ldots, y_i\rangle$. Thus, $|[y_1, \ldots, y_{k+1}]^{B(k)}| = (q^d - q^k)/(q^{k+1} - q^k) < n$, and $B(k+1)$ can be found in polynomial time using (3.2).

Note that $B(d-1)$ corresponds to all lower triangular matrices in $SL(d,q)$. Also, $B(d-1)'$ arises from lower triangular matrices with ones on the diagonal, and hence is a p-group. It follows that U is the unique Sylow p-subgroup of $B(d-1)$. Since $B(d-1)$ can be found in polynomial time, so can U by (3.11). □

Remark. $B(d-1)$ is a Borel subgroup of G (Carter [4, p. 104]).

From now on, r will be a prime $\neq p$. Since $r \,||G|$, we have $r|\prod_1^{d-1}(q^i - 1)$. Thus, if k is defined as in (B12), then $k < d$ and k can be found in polynomial time.

LEMMA 8.9. *If H and G are as in* (B13) *then* $H \lhd N$, $|H| < n$ *and* $N/H \cong S_d$.

Proof. Note that H arises from all diagonal matrices of determinant 1. Thus, $|H| \leqslant (q-1)^{d-1} < (q^d - 1)/(q-1) \leqslant n$. Since the "transpositions" t_i generate the symmetric group on $\mathscr{B}$, the remaining assertions are obvious. □

Remark. N is the "N" of BN-pair fame (Carter [4, pp. 101–113]).

LEMMA 8.10. (i) *If* $k = 1$ *then* (B14) *produces a Sylow r-subgroup R of G in polynomial time.*

(ii) *If* $l = 1$ *then a Sylow r-subgroup of G is cyclic, and hence is produced in* (B9).

Proof. (i) Since $d < n$ we can find F/H in polynomial time. Since $|H| < n$ by (8.9), we can find R using (5.2). Note that $|G| = \{q^{(1/2)d(d-1)}\prod_1^d(q^i - 1)\}/(d, q-1)$. Thus, since $r \neq 2$, (2.1) implies that $|R|$ is the largest power of r dividing $|G|$ (compare Weir [25]).

(ii) A Sylow r-subgroup R of G has as order the largest power of r dividing $q^k - 1$. On the other hand, $GF(q^k)^*$ acts on $GF(q^k)$ via $x \to ax$, and contains a cyclic subgroup of order $|R|$. Thus, R is cyclic. □

LEMMA 8.11. *The group S in* (B16) *can be found in polynomial time. Moreover,* $S \cong SL(k,q)$, *and S induces* $SL(k,q)$ *on* $V' = \langle y_1, \ldots, y_k\rangle$ *and the identity on* (*the set of all* 1*-spaces of*) $V'' = \langle y_{k+1}, \ldots, y_d\rangle$.

Proof. T_i fixes each vector in the hyperplane $\langle \mathscr{B} - \{y_i\}\rangle$, and acts on the set of k-spaces containing $\langle \{y_1, \ldots, y_k\} - \{y_i\}\rangle$. Since the number of such subspaces if $< (q^d - 1)/(q - 1) \leqslant n$, S can be found in polynomial time. Moreover, S is the identity on V''; it acts on V' by construction, inducing a group containing the restriction of T_i to this space. Those restrictions generate $SL(k, q)$. □

LEMMA 8.12. *A Sylow r-subgroup of S can be found in polynomial time.*

Proof. By (8.11), $S/Z(S) \cong PSL(k, q)$, where $Z(S)$ induces the identity on $[y_1, \ldots, y_k]$ by (8.3). Replace G by $S/Z(S)$ and X by $[y_1, \ldots, y_k]$, and find a Sylow r-subgroup $D/Z(S)$ of $S/Z(S)$. (This is possible by induction, unless $S/Z(S)$ is not simple. But then $|S| \leqslant 24$.) Then the set of all r-elements in D is a Sylow r-subgroup of S, and (3.11) can be applied. □

LEMMA 8.13. *The group E in* (B18) *can be found in polynomial time, and behaves as indicated in* (B18).

Proof. We argue as in (8.5). Namely, if $1 \leqslant i < l - 1$ use (3.1) in order to find an element of N sending $\mathscr{B}$ to itself and inducing $\prod_{j=1}^{k}(k(i-1)+j, ki+j)$ on $\mathscr{B}$. These permutations generate a group S_l of permutations of $\mathscr{B}$. Thus, E can be found and $E/H \cong S_l$. □

LEMMA 8.14. *The groups F and R^* in* (B19) *and* (B20) *can be found in polynomial time.*

Proof. Since E/H acts as S_l on the set $\{ki + 1 | 0 \leqslant i \leqslant l - 1\}$, a Sylow r-subgroup can be found in polynomial time (by (7.6)). This takes care of F, and R^* is obtained using (5.2). □

LEMMA 8.15. *A Sylow r-subgroup R of G can be found in polynomial time using* (B21)–(B23).

Proof. If $e \in E$ and $S^e \neq S$ then S^e acts on V'^e, where $V'^e \subseteq V''$ by the construction. Thus, $\langle V'^e | e \in E\rangle$ is the direct sum of the different members of $\{V'^e | e \in E\}$, and $|\Sigma| = l$. Since $l < n$ we can find suitable elements $e(i)$ in (B21).

Moreover, if we let $D = \langle S^e | e \in E\rangle$ then D is the product of the different groups S^e, $e \in E$, with each pair of these groups commuting elementwise. (More precisely, modulo its center D is the direct product of the projections of the different groups S^e.)

Let $r \neq 2$. We claim that $R_* \doteq \langle R_0^{e(i)f} | 1 \leqslant i \leqslant l', f \in R^*\rangle$ is a Sylow r-subgroup of D. Since $r \nmid q - 1$ (as $k > 1$) we have $r \nmid |Z(D)|$, so that this claim amounts to the assertion that no two of the groups $R_0^{e(i)f}$ lie in the same group S^e. In fact, assume that $R_0^{e(i)f} \leqslant S^e$ with $e = e(i_1)f_1$ for some

i_1 and some $f_1 \in R^*$. By the definition of $e(i)$, $i_1 = i$. Set $g = ff_1^{-1} \in R^*$. Then $1 \neq R_0^{e(i)g} \leqslant S^{e(i)} \cap (S^{e(i)})^g$, so that $S^{e(i)} = (S^{e(i)})^g$. But R^* fixes each row in (B18), and acts the same on each row. Since $g \in R^*$ fixes a column in (B18) (corresponding to $S^{e(i)}$), it follows that g induces the identity on $\mathscr{B}$. However, $r \nmid |H|$. Thus, $g = 1$ and $e(i)f = e$. Then S^e contains a unique one of the groups $R_0^{e(i)f}$, as claimed.

Thus, if $r \neq 2$ then, by definition, $R = R_* R^*$. Using (2.1) in order to compare $|R|$ with $|G|_r$, it is easy to check that R is a Sylow r-subgroup of G (compare Weir [25]).

Finally, let $r = 2$. Note that H normalizes D, while R^* normalizes both H and D. By (2.1), DHR^* contains a Sylow 2-subgroup R of G (compare Carter and Fong [5]). By (8.9), $|H| < n$, and by (8.1), $|D| \leqslant \{q(q^2-1)\}^l \leqslant \{q(q^2-1)\}^{d/2} < n^2$. Thus, (5.2) can be used to find R. □

This completes the discussion of Part II of the algorithm in Section 5.

9. Classical Groups: Preliminaries

This section is a digression from the proof of Theorem B. It contains notation and elementary properties of symplectic, orthogonal and unitary groups (Dieudonné [8] or Kantor [12]).

Let V be a d-dimensional vector space over $GF(q)$. Let $(\ ,\ )$ be a bilinear or hermitian form on V. If $S \subseteq V$ then $S^\perp = \{v \in V | (v, S) = 0\}$ is a subspace of V. An isometry of V is an element $g \in GL(V)$ such that $(u^g, v^g) = (u, v)$ for all $u, v \in V$.

If $(v, v) = 0$ for all $v \in V$, while $V^\perp = 0$, the group of isometries is $Sp(d, q)$. Here, $d = 2m$ for some m. Also, $PSp(2m, q) = Sp(2m, q)/\langle -1 \rangle$.

Assume that $(\ ,\ )$ is hermitian, so that $(\alpha u, \beta v) = \alpha\bar{\beta}(u, v)$ and $(u, v) = \overline{(v, u)}$ for all $\alpha, \beta \in GF(q)$ and $u, v \in V$. (Here, q is a square, and $\bar{\alpha} = \alpha^{q^{1/2}}$.) Then $SU(V) = SU(d, q^{1/2})$ is the group of those isometries lying in $SL(V)$, and $PSU(V) = SU(V)/Z(SU(V))$.

A quadratic form on V is a function $Q: V \to GF(q)$ such that $Q(u+v) - Q(u) - Q(v) = (u, v)$ is bilinear. *Assume that* $0 \notin Q(V^\perp - \{0\})$. Then $V^\perp = 0$, except if q is even, d is odd and $\dim V^\perp = 1$. The orthogonal group $\Omega(V)$ is the derived group of $\{g \in SL(V) | Q(v^g) = Q(v) \text{ for all } v \in V\}$ (unless $d = 4$ and $q = 2$, a situation which will not concern us here).

If W is a subspace, and $V^\perp \cap W = 0$, then $\dim W + \dim W^\perp = d$. Call W *nonsingular* if $W \cap W^\perp = 0$, that is, if $V = W \oplus W^\perp$. Call W *totally isotropic* (or *totally singular*) if $(W, W) = 0$ and V is symplectic or unitary (or $Q(W) = 0$ and V is orthogonal); then $\dim W \leqslant \frac{1}{2}d$.

Let m be the maximal dimension of a totally isotropic or totally singular subspace. Then $d - 2m \leqslant 2$, and vectors e_i and f_i exist for which

$$V = \langle e_1, \ldots, e_m, f_1, \ldots, f_m \rangle \oplus V_0, \tag{9.1}$$

where $(e_i, e_j) = 0 = (f_i, f_j)$, $(e_i, e_j) = \delta_{ij}$, $e_i, f_i \in V_0^{\perp}$, and $V_0 - \{0\}$ contains no isotropic (or singular) vector. We will need the following lemma, which is easy to check.

LEMMA 9.2. *Let V and $G = Sp(d, q)$, $SU(V)$, or $\Omega(V)$ be as above.*

(i) *There is an element of G sending $\langle e_1 \rangle \leftrightarrow \langle e_2 \rangle$, $\langle f_1 \rangle \leftrightarrow \langle f_2 \rangle$, and fixing every other e_i and f_i for $i > 2$.*

(ii) *There is an element of G sending $\langle e_1 \rangle \leftrightarrow \langle f_1 \rangle$ and fixing every e_i and f_i for $i > 1$, unless G is orthogonal and $d = 2m$.*

(iii) *In the case excluded in (ii) there is an element of G sending $\langle e_1 \rangle \leftrightarrow \langle f_1 \rangle$, $\langle e_2 \rangle \leftrightarrow \langle f_2 \rangle$, and fixing every e_i and f_i for $i > 2$.*

The exceptional situation in (iii) is discussed in [8, pp. 50, 65, 86, 87; and 12, p. 18].

Another type of exceptional situation arises when G is orthogonal, $d = 2m + 1$, q is even, and $\dim V^{\perp} = 1$. Here, the natural map $V \to V/V^{\perp}$ induces an isomorphism $\Omega(2m + 1, q) \cong Sp(2m, q)$. In (6.1) we restricted ourselves to $\Omega(2m + 1, q)$ instead of $Sp(2m, q)$, and we will continue to do so.

The following simple result holds in all cases.

LEMMA 9.3. *If $\dim V > 3$ and $0 \neq v \in V$ then $\langle v \rangle^{\perp}$ is spanned by its set of totally isotropic or totally singular 1-spaces.*

Finally, we turn to a description of Sylow r-subgroups of $G = \mathrm{Sp}(2m, q)$, $SU(V)$, and $\Omega(V)$, where r is not the prime p dividing q and $r \,||G|$. More precisely, we will describe certain r-subgroups R of G. That these are Sylow subgroups follows from a comparison of $|R|$ with $|G|_r$ using (2.1) and [4, pp. 144, 155, 259; or 10, p. 135]. For more details, see Weir [25] and Carter and Fong [5].

Construction 9.4 (*Description of a Sylow r-subgroup of G*)

Case 1. $G = Sp(2m, q)$. Let k be the smallest positive integer such that $r | q^k \pm 1$. Let e_i and f_i be as in (9.1). Let $W_i = \langle e_{(i-1)k+j}, f_{(i-1)k+j} | 1 \leqslant j \leqslant k \rangle$ for $1 \leqslant i \leqslant l = [m/k]$, and let E be the group of all elements of G fixing $\{W_1, \ldots, W_l\}$, $\{\langle e_{ik+j} \rangle | 0 \leqslant i < l\}$, and $\{\langle f_{ik+j} | 0 \leqslant i < l\}$ for $1 \leqslant j \leqslant k$, and $\langle e_i \rangle$ and $\langle f_i \rangle$ for $kl < i \leqslant m$.

Imitating (5.3(ii)), let $G(W_i^{\perp})$ be the group of all elements of G inducing the identity on $W_i^{\perp}$. Then a Sylow r-subgroup R of $(G(W_1^{\perp}) \times \cdots \times G(W_l^{\perp}))E$ is also a Sylow r-subgroup of G.

If $r \neq 2$ then a Sylow r-subgroup of $G(W_1^{\perp})$ is cyclic. Assume that $k > 1$. Let R^* be a Sylow r-subgroup of E. Let $W_{f(i)}$, $1 \leqslant i \leqslant l'$, be representatives of the orbits of R^* on $\{W_1, \ldots, W_l\}$, and let $R_{f(i)}$ be a Sylow r-subgroup of $G(W_{f(i)}^{\perp})$. Then $R = \langle R^*, R_{f(i)} | 1 \leqslant i \leqslant l' \rangle$.

Case 2. $G = \Omega^{\pm}(d, q)$ or $SU(d, q)$. This time the definitions of k and W_1^* are somewhat more complicated. If $r \neq 2$, and if $r \nmid q + 1$ in case G is unitary, let k be the smallest positive integer such that $r \,||G(W_1^{\perp})|$ for some nonsingular subspace W_1 of dimension k. If $2 \neq r | q + 1$ and G is unitary, let $k = 1$ and let W_1 be any nonsingular 1-space. Finally, if $r = 2$ let $k = 2$ and let W_1 be a nonsingular 2-space such that $2 \,||G(W_1^{\perp})|$.

Let $\{W_1, \ldots, W_l\}$ be a subset of W_1^G maximal with respect to consisting of pairwise orthogonal subspaces of V. Take any basis $w_1, \ldots, w_d$ of V which, when intersected with each W_i, produces a basis, and such that $w_i \in (w_{i-k})^G$ and $\{w_i, w_j\} \in \{w_{i-k}, w_{j-k}\}^G$ for $k < i, j \leqslant kl$. Let E be the group of all elements of G fixing $\{W_1, \ldots, W_l\}$, $\{\langle w_{ik+j} \rangle | 0 \leqslant i < l\}$ for $1 \leqslant j \leqslant k$, and $\langle w_i \rangle$ for $kl < i \leqslant d$. Then a Sylow r-subgroup R of $(G(W_1^{\perp}) \times \cdots \times G(W_l^{\perp}))E$ is also a Sylow r-subgroup of G.

If $r \neq 2$ then a Sylow r-subgroup of $G(W_1^{\perp})$ is cyclic. Assume that $k > 2$. Then R can be obtained exactly as in the last paragraph of Case 1. □

Remarks. When $k \leqslant 2$ but $r \neq 2$, R can be constructed explicitly in a similar manner; when $r = 2$ an explicit description is slightly more complicated (cf. Carter and Fong [5]). However, when $k \leqslant 2$ we will not need such a precise description of R: since $|G(W_1^{\perp}) \times \cdots \times G(W_l^{\perp})| < (q^8)^l$, (5.2) will allow us to find a Sylow r-subgroup of $(G(W_1^{\perp}) \times \cdots \times G(Wl_l^{\perp}))R^*$.

The fact that $G(W_1^{\perp})$ has cyclic Sylow r-subgroups when $r \neq 2$ will be crucial later. Note that we have not actually constructed these cyclic groups; constructions are given in Weir [25], but we will use Steinberg [24] in order to avoid contending with extension fields.

A comparison of Cases 1 and 2, and especially of the definitions of W_1 and E contained in them, will explain some of the awkwardness inherent in (B29)–(B37).

10. Making Points

In this section we will prove Theorem 6.2 and find all the 1-spaces of V. Let n^* be the number of totally isotropic or totally singular 1-spaces of V. Then n^* is as follows (e.g., Curtis, Kantor, and Seitz [7, p. 13]).

G	n^*
$PSp(2m, q)$	$(q^{2m} - 1)/(q - 1)$
$P\Omega(2m + 1, q)$	$(q^{2m} - 1)/(q - 1)$
$P\Omega^{\pm}(2s, q)$	$(q^s \mp 1)(q^{s-1} \pm 1)/(q - 1)$
$PSU(2m + 1, q)$	$(q^{2m} - 1)(q^{2m-1} + 1)/(q^2 - 1)$
$PSU(2m, q)$	$(q^{2m+1} + 1)(q^{2m} - 1)/(q^2 - 1)$

LEMMA 10.1. *If $H < G$ and $|G: H| < q^3 n^*$ then H is the stabilizer of a 1-space of V. Moreover, if $|G: H| < 2n^*$ then $|G: H| = n^*$ and that 1-space is totally isotropic or totally singular, except perhaps if G is $\Omega(2m + 1, 2)$ for some m and $|G: H| = 2^{m-1}(2^m \pm 1)$.*

Proof. Kantor [14, Theorem 2]. In fact, this is immediate from (6.1). (Note that we are excluding $Sp(2m, 2^i)$ as in (6.1(iii)).) □

Proof of Theorem 6.2. By Sections 7 and 8 we may assume that G is symplectic, unitary, or orthogonal. Since $|G| > n^8$, by (6.1(iii)) we have $\dim V \geqslant 9$. By (10.1) we only need to exhibit a subgroup of G of index n^* belonging to the set $\mathscr{M}'$ produced by *Double-Pairing*.

First, let W be a minimal proper G_x-invariant subspace of V (cf. (6.1)). Then $\dim W \leqslant \frac{1}{2}d$, where $d = \dim V$. Since G_x fixes $W \cap W^{\perp}$, we have $W \cap W^{\perp} = 0$ or $W \subseteq W^{\perp}$. Similarly, if V is orthogonal and $W \subseteq W^{\perp}$ then either W is totally singular or V has characteristic $p = 2$ and $\dim W = 1$. There are three cases to consider: (α) W is totally isotropic or totally singular; (β) $\dim W = 1$; and (γ) $V = W \oplus W^{\perp}$.

(α) Choose $W^g \in W^G$ such that $W^{\perp} \cap W^g = W \cap W^g = W \cap (W^g)^{\perp}$ and $\dim W \cap W^g = 1$ or 2. Set $y = x^g$. Then the only proper subspaces fixed by $G_{\{x,y\}}$ are $W \cap W^g$, $\langle W, W^g \rangle$, $(W \cap W^g)^{\perp}$, and $\langle W, W^g \rangle^{\perp}$. If $G_{\{x,y\}} < H < G$ then H is reducible by Kantor [13], and hence H must fix one of the above subspaces. Since $\langle W, W^g \rangle \cap \langle W, W^g \rangle^{\perp} = W \cap W^g$, it follows that H fixes $W \cap W^g$. Thus, there is a unique maximal subgroup M of G containing H, namely, the stabilizer of $W \cap W^g$; and that maximal subgroup is in $\mathscr{M}(G_x)$.

If possible, choose g so that $\dim W \cap W^g = 1$. Then M is the stabilizer of the 1-space $W \cap W^g$, and $|G: M| = n^*$.

If g cannot be chosen as above then $\dim W = m > 2$ and $G = P\Omega^+(2m, q)$ [8, pp. 50, 65, 86, 87; or 12, p. 18]. Thus, as above $\mathscr{M}(M)$ contains a subgroup of index n^* in G.

(β) Let U be a totally isotropic or totally singular 1-space in $W^{\perp}$, and choose $W^g \in W^G - \{W\}$ inside $\langle W, U \rangle$. Set $y = x^g$. It is easy to check that some element of G interchanges W and W^g. If M is a maximal subgroup of G containing $G_{\{x,y\}}$, then (by [13]) M is the stabilizer of U.

Clearly, $M \in \mathcal{M}(G_x)$.

(γ) Here, $\dim W^\perp \geqslant 4$. By the argument in (β) we may assume that $\dim W \geqslant 2$.

Let U be a totally isotropic or totally singular 1-space in $W^\perp$, and let $W_1 \neq W$ be any hyperplane in $\langle U, W\rangle$ not containing U. Then $W_1 \in W^G$, and some $g \in G$ interchanges W and W_1. Set $y = x^g$.

Let $U_1 = W \cap (W \cap W_1)^\perp$. Since $W \cap W_1$ is a hyperplane of W, $\dim U_1 = 1$. Moreover, $W^\perp \cap W_1 = 0$, $W \cap W_1^\perp \subseteq U_1$, and $W_1 \cap (W \cap W_1)^\perp$ is either 0 or a 1-space U_1'.

Let M be any maximal subgroup containing $G_{\{x,y\}}$. Since $\dim V > 8$, M is reducible by [13]. Then M fixes U, U_1, or U_1'. Thus, we can argue exactly as in (β) in order to show that $\mathcal{M}(M)$ contains a subgroup of G of index n^*. □

As indicated in Section 5, *we will identify Y with the set of totally isotropic or totally singular 1-spaces of V.*

LEMMA 10.2. *Let $y, z \in Y$, $y \neq z$.*

(i) *There is a unique prime p such that $O_p(G_y) \neq 1$. This prime divides q, and can be found in polynomial time.*

(ii) *y and z are perpendicular 1-spaces of V if and only if $O_p(G_{yz}) \neq 1$.*

Proof. (i) See Curtis, Kantor, and Seitz [7, Sect. 3] for the first two assertions. The last part follows from Theorem C.

(ii) If $z \subset y^\perp$ then $G_{yz} \rhd O_p(G_y)_z \neq 1$. Assume that $z \not\subset y^\perp$. Then $V = \langle y, z\rangle \oplus \langle y, z\rangle^\perp$, and hence $O_p(G_{yz}) = 1$ (compare (9.2)). □

COROLLARY 10.3. *The parenthetical remark in* (B4) *holds.*

Proof. Clearly, (6.1(i)) handles the $PSL(d, q)$ case, while (10.2(ii)) deals with the remaining cases. □

LEMMA 10.4. *The integer q defined in* (B29(i)) *or* (B31) *is the "q" appearing in the name $PSp(2m, q)$, $P\Omega^{\pm}(d, q)$, or $PSU(d, q)$.*

Proof. Use the formula for $n^* = |Y|$ in the table at the beginning of this section. □

THEOREM 10.5. *There is a polynomial-time algorithm for finding a set Y^+ on which G acts exactly as it acts on the set of all 1-spaces of V. Moreover, $|Y^+| < 4n^2$.*

Proof. If G is $PSp(2m, q)$ there is nothing to prove: let $Y^+ = Y$. Assume that G is orthogonal or unitary, and proceed as follows:

(1) Let $y \in Y$, and let $z \in Y$ with $z \nsim y$.

(2) Find $L = (G_{y_1})' \cap (G_{z_1})'$.

(3) For each conjugate $L^* \neq L$ of L, find $\langle L, L^* \rangle$, and retain only those L^* for which $\langle L, L^* \rangle \neq G$.

(4) Find a maximal subgroup M of G containing $\langle L, L^* \rangle$.

(5) Let Y^+ be the set of all conjugates of all such maximal subgroups M for which $|G: M| < q^3 n^*$.

We must show that Y^+ can be found in polynomial time, and that Y^+ behaves as desired. Of course, we regard G as acting on Y^+ by conjugation.

As in (8.3(i)) we can find L. Clearly, $|L^G| < n^{*2} < 4n^2$, so we can find each L^* (using (3.1)). Use (3.6) to find M. Certain of these subgroups M will satisfy $|G: M| < q^3 n^*$. Any such M is the stabilizer of a 1-space of V, by (10.1). Thus, it remains to show that every 1-space of V is fixed by a conjugate of some such M.

Note that L is the group of all elements of G inducing the identity on the nonsingular 2-space $\langle y, z \rangle$. Every 1-space of V can be sent into $\langle y, z \rangle$ by an element of G. Consider a 1-space a of $\langle y, z \rangle$, and let $\langle y, z \rangle^g$, $g \in G$, be such that $\langle y, z \rangle \cap \langle y, z \rangle^g = a$ and $\langle y, z \rangle^\perp \cap \langle y, z \rangle^g = 0 = (\langle y, z \rangle^g)^\perp \cap \langle y, z \rangle$. Set $L^* = L^g$. Then a and $a^\perp$ are the only proper subspaces fixed by $\langle L, L^* \rangle$. Let M be as in (4). Then M is reducible by [13]. Thus, $M = G_a$.

Consequently, Y^+ (defined in (5)) consists of all stabilizers of 1-spaces of V. Finally, the number of such 1-spaces is $< |V| < n^{*2}$. □

LEMMA 10.6. *All assertions in* (8.3) *hold.*

Proof. Repeat the proof of (8.3). □

LEMMA 10.7. *In the notation of* (5.6), A^* *is the set of all* 1*-spaces in* $A^\perp$, *and can be found in polynomial time* (*given* A).

Proof. In (5.5(i)), a^* is the set of all 1-spaces in $a^\perp$ by (10.2). The same is true in (5.5(ii)). For, it suffices to check that, if $a \in Y^+ - Y$ and $b \in Y$, then $[a, b] \cap Y = \{b\}$ if and only if a and b are perpendicular. Let $a = \langle u \rangle$ and $b = \langle v \rangle$. If $(u, v) = 0$ then $(u + \alpha v, u + \alpha v) \neq 0$ (or $Q(u + \alpha v) \neq 0$ in the orthogonal case) for all scalars α. Conversely, if $(u, v) \neq 0$ then $\langle u, v \rangle$ is nonsingular and hence contains at least two members of Y.

Thus, A^* is the set of all 1-spaces in $A^\perp$.

Next, note that a^* can certainly be found in polynomial time in (5.5(i)). In (5.5(ii)), simply test $[a, b] \cap Y$ for each $b \in Y$. Next, given A form each b^* and test whether $A \subseteq b^*$. Thus, A^* can be found in polynomial time. □

11. THEOREM A, AND A SYLOW p-SUBGROUP

This section concerns (B24)–(B28). In particular, it contains the end of the proof of Theorem A.

LEMMA 11.1. (i) *The set $\mathscr{B}$ in* (B24) *can be found in polynomial time.*

(ii) *There exist vectors $e_i \in y_i$ and $f_i \in z_i$ behaving as in* (9.1).

Proof. First, z_1 can be found using (10.2(ii)). Let $0 \neq e_1 \in y_1$; there is a vector $f_1 \in z_1$ such that $(e_1, f_1) = 1$. Assume that $y_j = \langle e_j \rangle$ and $z_j = \langle f_j \rangle$ have been found for $1 \leqslant j \leqslant i$ such that $(e_j, e_k) = (f_j, f_k) = 0$ and $(e_j, f_k) = \delta_{jk}$ for $1 \leqslant j, k \leqslant i$. Consider $W = \langle e_1, \ldots, e_i, f_1, \ldots, f_i \rangle^\perp$. If W contains no member of Y, (B24) has us set $i = m$ (compare (9.1)). If W contains a member y_{k+1} of Y then $y_{k+1}^\perp \cap W$ cannot contain all members of Y in W, so that z_{k+1} exists. Now let $y_{k+1} = \langle e_{k+1} \rangle$, and note that $f_{k+1} \in z_{k+1}$ exists satisfying $(e_{k+1}, f_{k+1}) = 1$.

This proves (i), since each test for $y_i \sim z_j$ takes polynomial time. Moreover, $\langle \beta \rangle^\perp$ has no member of Y, so that (9.1) holds. □

LEMMA 11.2. *The elements t_i in* (B25) *can all be found in polynomial time. Moreover, $t_m \neq (m, m')$ if and only if $G = P\Omega^+(2m, q)$.*

Proof. The t_i exist by (9.2), and can be found exactly as in (8.5). □

LEMMA 11.3. (i) *$Q = O_p(G_{y_1})$ can be found in polynomial time. Moreover, $|Q| < 4n^2$.*

(ii) *$H = G_{y_1 \cdots y_m z_1 \cdots z_m}$ can be found in polynomial time. Moreover, $|H| < 16n^4$.*

(iii) $|QH| < 64n^6$.

Proof. (i) By Curtis, Kantor, and Seitz [7, Sect. 3], $|Q| < |V| < n^{*2} < (2n)^2$ and G_{y_1} has at most two nontrivial normal p-subgroups. One of these has order q, while the other has order $\geqslant |V|/q > n^{*1/2}$.

Now consider (B26). We may assume that $|Q_0| = q$. By [7, Sect. 3], G_{y_1}/Q_0 acts faithfully on the set of all Q_0-orbits. In view of Theorem C, this proves (i).

(ii) The first assertion is immediate by (3.1). Also, the restriction of H to $\langle \mathscr{B} \rangle$ arises from diagonal matrices, while $\dim \langle \mathscr{B} \rangle^\perp \leqslant 2$ by (9.1). Thus, $|H| \leqslant q^3 q^{2m} < n^{*4} < 16n^4$.

(iii) By (i) and (ii), $|QH| < 4n^2 \cdot 16n^4$. □

THEOREM 11.4. *Let G be a given subgroup of S_n that is isomorphic to a simple Chevalley group of characteristic p. Then there is a polynomial-time algorithm for finding a set of elements such that every element of G of order not divisible by p is conjugate to a member of the set.*

Proof. Use (3.2), (3.5), (6.1), and (8.6), to reduce to the situation in the present section. We found c, c', and QH in (B25) and (B26). By Steinberg [24, (9.4), (9.5)], each of the desired elements of G is conjugate to a power of an element of $Qc \cup QHc'$. □

Remark. Actually, Steinberg constructs a much smaller set than $Qc \cup QHc'$ which behaves as above. For a discussion of his results, see the Appendix.

The following is another application of (11.3).

PROPOSITION 11.5. *The structure of G can be determined as follows.*

(i) *G is symplectic if and only if $Y^+ = Y$.*

(ii) *G is orthogonal if and only if Q is abelian.*

(iii) *G is unitary if and only if it is not symplectic and Q is nonabelian.*

Proof. See Curtis, Kantor, and Seitz [7, Sect. 3]. (N.B.—Here, (ii) must be interpreted by using the fact that $P\Omega(2m+1, 2^i) \cong PSp(2m, 2^i)$ in order to ignore $PSp(2m, 2^i)$, precisely as in (6.1).) □

LEMMA 11.6. *A Sylow p-subgroup of G can be found in polynomial time.*

Proof. This is proved almost exactly as in (8.8). Here $|[y_1, \ldots, y_{k+1}]^{B(k)}| = \{n^* - (q^k - 1)/(q-1)\}/\{(q^{k+1} - q^k)/(q-1)\} < \frac{1}{2}n^* < n$, where $B(k)$ is defined in (B28) (i.e., (B9)). A simple matrix calculation shows that $B(m)$ has a unique Sylow p-subgroup U (and that $B(m)$ is solvable: $B(m)''$ is a p-group). Thus, U can be found using (3.11). □

12. SYMPLECTIC GROUPS

This section is concerned with the case $Y^+ = Y$ considered in (B29). By (11.5), G is symplectic. In (11.1(ii)) and (10.4) we found m and q such that $G \cong PSp(2m, q)$.

LEMMA 12.1. (i) *In* (B29(ii)), *k can be found in polynomial time.*

(ii) *In* (B29(iii)), *S can be found in polynomial time, and induces $Sp(2k, q)$ on $\langle y_1, \ldots, y_k, z_1, \ldots, z_k \rangle$.*

Proof. (i) Obvious.

(ii) For the first part, see (5.3(ii)) and (5.6). For the second, note that S is the group of all elements of G inducing the identity on (the set of all 1-spaces of) $\langle y_1, \ldots, y_k, z_1, \ldots, z_k \rangle^\perp$. □

LEMMA 12.2. *The group E in* (B29(iv)) *can be found in polynomial time, and $E/H \cong S_l$.*

Proof. The group induced on $\mathscr{B}$ by E is E/H and is isomorphic to a subgroup of S_l. By (B25) and (B27) we can find $N = \langle H, t_1, \ldots, t_m \rangle$. As in the proof of (8.13), elements of N can be found which belong to E and generate S_l modulo H. □

LEMMA 12.3. *Sylow r-subgroups R_0 and R^* of S (resp. E) can be found in polynomial time.*

Proof. Repeat the proofs of (8.12) and (8.14) (essentially verbatim). □

LEMMA 12.4. *If $k > 1$ then* (B29(vi)) *produces a Sylow r-subgroup of G in polynomial time.*

Proof. The proof of (8.15) can be repeated, essentially verbatim (except delete the last paragraph). That R is a Sylow subgroup of G follows from (9.4). □

LEMMA 12.5. *If $k = 1$ then* (B29(vii)) *produces a Sylow r-subgroup of G in polynomial time.*

Proof. Let $D = \langle S^E \rangle$. Then, as in (8.15), $|D| < (q^3)^m < n^2$, while $|H| < 16n^4$ by (11.3). Since H normalizes D and R^* normalizes both H and D, we can apply (5.2) in order to find a Sylow r-subgroup R of $\langle D, H, R^* \rangle = DHR^*$. By (9.4), R is a Sylow r-subgroup of G. □

13. ORTHOGONAL AND UNITARY GROUPS

Finally, we will deal with (B30)–(B37), thereby completing the proof of Theorem B.

Recall that G is an orthogonal or unitary group, and that $Y^- = Y^+ - Y$ "is" the set of all nonsingular 1-spaces of V (by (10.5)). Also, q was found in (10.4).

LEMMA 13.1. *The subset $\{u_1, \ldots, u_d\}$ in* (B33) *can be found in polynomial time. Moreover, $d = \dim V$ and V is the direct sum of the 1-spaces u_i.*

Proof. By (10.6), (10.7), and (3.1), each test $r \mid |G(Y \cup \{y_i\})|$ or $2 \mid |G([u_1, u_2]^*)|$ in (B31) can be performed in polynomial time. Thus, Z and S can be found in polynomial time.

By (10.7), $\{u_1, \ldots, u_i\}^* \cap Z \cap Y^-$ can be found in polynomial time, and the u_i are pairwise orthogonal 1-spaces in (5.7). Similarly, if $u, v \in Y$ then $[u, v] \cap [u, v]^*$ can be found in polynomial time. Thus, (B32) runs in polynomial time.

By (10.6), $[u_1, \ldots, u_k]$ is the set of all 1-spaces of a subspace W_1 of V. In view of (10.7), our construction of W_1 shows that W_1 is nonsingular (compare (9.4)).

Similarly, in (B33) each test in (i), (ii), or (iv) requires polynomial time (by (10.7) and (3.2)), while (iii) is merely a definition. (N.B.—The last portion of (iv) refers to the possibility that $p = 2$ and $\dim V$ is odd, in which case $\dim V^\perp = 1$.) □

LEMMA 13.2. *The groups E and H in* (B34) *can be found in polynomial time. Moreover, $E/H \cong S_l$ or A_l, and $|H| < 16n^4$.*

Proof. Let $G^* = GO(d,q)$ or $GU(d,q)$, let $H^* = (G^*)_{u_1 \cdots u_d}$, and let E^* be the group of all elements of G^* that fix $\{u_1, \ldots, u_d\}$ and act on the subscripts as in (B18). Then $E^*/H^* \cong S_l$. It follows that $E/H \cong S_l$ or A_l. Moreover, $|H| < (q^2)^d < n^{*4} < 16n^4$.

We can find H using (3.1). An element of E inducing any desired 3-cycle within E/H can be found in polynomial time exactly as in the proof of (8.13), as can an element inducing a transposition if one exists. Thus, E can be found in polynomial time. □

LEMMA 13.3. *A Sylow r-subgroup R of G can be found in polynomial time using* (B36) *and* (B37).

Proof. Sylow r-subgroups R_0 and R^* of S (resp. E) can be found in polynomial time by repeating the proofs of (8.12) and (8.14).

If $k > 2$, repeat (B21), (B22), and the first three paragraphs of the proof of (8.15) (replacing V' by $W_1 = \langle u_1, \ldots, u_k \rangle$, V'' by $W_1^\perp$, and $\mathscr{B}$ by $\{u_1, \ldots, u_d\}$). The result is a Sylow r-subgroup $R = R_* R^*$ of $\langle \langle S^E \rangle, R^* \rangle$. We claim that R is a Sylow r-subgroup of G. For, let $W_i = \langle u_{(i-1)k+j} | 1 \leqslant j \leqslant k \rangle$ for $1 \leqslant i \leqslant l$. By construction (B33), $W_i \in W_1^G$, while the W_i are pairwise orthogonal by (10.7). Also, by (B33(iii)), $(W_1 \perp \cdots \perp W_l)^\perp$ has no subspace belonging to W_1^G. This matches the present notation with that of (9.4). Thus, (9.4) proves our claim.

Finally, if $k \leqslant 2$ let $D = \langle S^E \rangle$ and imitate the last paragraph of the proof of (12.5): $|DH| \leqslant (q^3)^{d/2} 16n^4 < n^6$, and (5.2) can be applied in order to find a Sylow r-subgroup R of DHR^*. As above, R is a Sylow r-subgroup of G by (9.4). □

14. CONCLUDING REMARKS

This completes the proof of Theorems A and B. The crucial step involved the construction of a (possibly) new set Y on which G acted in a concrete manner (6.2). It was then possible to pick out special subsets of Y and find their stabilizers, using no more than elementary linear algebra.

On the other hand, (6.2) required that $|G|$ be large: $|G| > n^8$. If $|G| \leqslant n^8$ then the time required to find an element of order r is $O(n^9)$: pick each element of G, and test its order in time $O(n)$. Similarly, if $|G| \leqslant n^8$ then the algorithm referred to in (5.2) produces a Sylow r-subgroup of G in time $O(n^9)$. Note that the known algorithm for (3.10) runs in time $O(n^8)$.

APPENDIX

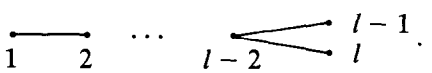
In (B9) and (B27) we quoted results of Steinberg [24]. This Appendix summarizes these results and relates them to (B9) and, especially, (B27).

We will assume familiarity with root systems, root groups, and the twisting process (Carter [4, Chaps. 2, 5, 8, 13]).

Let G denote one of the classical groups $SL(l+1,q)$, $Sp(2l,q)$, $\Omega(2l+1,q)$, $\Omega^+(2l,q)$, $\Omega^-(2m+2,q)$, $SU(2m,q)$, or $SU(2m+1,q)$. (Note the slight change of notation from that of Sects. 8–13: l is used instead of $d-1$ or m, for reasons that will be seen in (II) and (III) below.) In order to simplify our discussion, we will divide it into three parts: (I) untwisted groups, (II) $\Omega^-(2m+2,q)$, (III) unitary groups (the hardest case).

Each group G has a Weyl group $W = N/H$ and a root system. If α is a root there is a corresponding reflection $w_\alpha \in W$. Let s_α be any preimage of w_α in W. We will abuse language by identifying w_α and s_α.

(I) $G = SL(l+1,q)$, $Sp(2l,q)$, $\Omega(2l+1,q)$, or $\Omega^+(2l,q)$, $l \geqslant 3$. With each root α is associated a root group $X_\alpha = \{X_\alpha(t) | t \in GF(q)\}$ [4, p. 68]. Let $\alpha_1, \ldots, \alpha_l$ be a fundamental system of roots, with corresponding reflections $s_1, \ldots, s_l$ [4, p. 13]. We assume that these are ordered from left to right in the Dynkin diagram, so that deletion of α_1 produces a diagram of the same "type" but with one less node. Example:



Then the corresponding parabolic subgroup P_1 is the stabilizer of a 1-space, which is totally isotropic or totally singular if G is symplectic or orthogonal; moreover, $O_p(P_1) = \langle X_\alpha | \alpha > 0, \alpha \text{ involves } \alpha_1 \rangle$ [7, Sect. 3]. Set

$$C = X_{\alpha_1} s_1 X_{\alpha_2} s_2 \cdots X_{\alpha_l} s_l. \tag{A.1}$$

Steinberg showed that *every p'-element of G is conjugate to a power of an element of C.* (Actually, he proved a somewhat stronger result; see [24, (9.4), (9.5)] and [23, (III 2.11)].) Moreover, since $X_\alpha^w = X_{\alpha^w}$ for all $w \in W$, we have (cf. [4, (7.3)])

$$C = X_{\delta_1} X_{\delta_2} \cdots X_{\delta_l} s_1 s_2 \cdots s_l \tag{A.2}$$

where $\delta_i = \alpha_i^{s_{i-1} \cdots s_1} = \alpha_i + \alpha_{i-1} + \cdots + \alpha_1$. Thus,

$$C \subseteq O_p(P_1) s_1 s_2 \cdots s_l. \tag{A.3}$$

We note that the elements s_i can be identified with the elements t_i found in (B8) and (B25) (compare [7, (6.2)], where the action of the s_i is discussed).

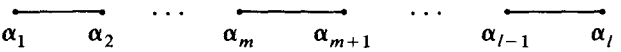
Also, P_1 is the stabilizer of y_1 [7, pp. 8–9]. Thus, the cosets Qc in (B9) and (B28) behave as desired.

(II) $G = \Omega^-(2m+2, q)$, $m \geqslant 3$. Set $l = m+1$ and consider $\Omega^+(2l, q^2)$ as in (I): let α_i and s_i be as in (I). A fundamental system $\beta_1, \ldots, \beta_m$ for G can be obtained by letting $\beta_i = \alpha_i$ for $i \leqslant m-1$ and $\beta_m = (\alpha_m + \alpha_{m+1})/2$; the corresponding reflections are $r_i = s_i$ for $i \leqslant m-1$ and $r_m = s_m s_{m+1}$ [4, (13.1.2), (13.3.2)]. The corresponding root groups for G are $U_{\beta_i} = \{X_{\beta_i}(t) | t \in GF(q)\}$ for $i \leqslant m-1$ and $U_{\beta_m} = \{X_{\alpha_m}(t) X_{\alpha_{m+1}}(t^q) | t \in GF(q^2)\}$ [4, (13.6.3)]. Set

$$\begin{aligned} C &= \left(X_{\alpha_1} s_1 X_{\alpha_2} s_2 \cdots X_{\alpha_{l-1}} s_{l-1} X_{\alpha_l} s_l\right) \cap G \\ &= U_{\beta_1} r_1 U_{\beta_2} r_2 \cdots U_{\beta_m} r_m \\ &= U_{\delta_1} U_{\delta_2} \cdots U_{\delta_m} r_1 r_2 \cdots r_m, \end{aligned} \tag{A.4}$$

where $\delta_i = \beta_i^{r_{i-1} \cdots r_1}$. Then $C \subseteq O_p(P_1) r_1 \cdots r_m$ and every p'-element of G is conjugate to a power of an element of C, as before.

(III) $G = SU(2m, q)$ or $SU(2m+1, q)$, $m \geqslant 3$. The case of $SU(2m, q)$ is contained in that of $SU(2m+1, q)$ (see below), so let $G = SU(2m+1, q)$. Set $l = 2m$, and let $SL(l+1, q^2)$, $\alpha_1, \ldots, \alpha_l$, $s_1, \ldots, s_l$, and X_α be as in (I):



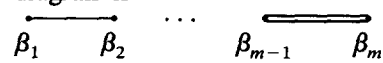
Set $\alpha = \alpha_m + \alpha_{m+1}$.

By [4, (13.3.1) and (13.1.2)], a fundamental system $\beta_1, \ldots, \beta_m$ for G can be obtained as $\beta_i = \alpha_i + \alpha_{l+1-i}$ if $i < m$ and $\beta_m = \alpha$, with corresponding reflections $r_i = s_i s_{l+1-i}$ if $i < m$ and $r_m = s_\alpha$. By [4, (13.6.3)], the corresponding root groups are

$$U_i = \left\{X_i(t) X_{l+1-i}(t^q) | t \in GF(q^2)\right\} \qquad \text{if } i \leqslant m-1,$$

$$U_m = \left\{X_m(t) X_{m+1}(t^q) X_\alpha(u) | t, u \in GF(q^2),\ t + t^q = uu^q\right\}.$$

The resulting Dynkin diagram is



[4, (13.3.8)].

Set $T_\alpha = \langle X_\alpha, X_{-\alpha} \rangle \cap T$, where T is the subgroup of $SL(l+1, q^2)$ called "H" in [4, p. 97]. Set $H = G \cap T$ (so that H is as in (B28)). Note that T normalizes each X_γ and is normalized by each s_i.

Set

$$\begin{aligned} C' &= \left(X_\alpha s_\alpha X_{\alpha_{m-1}} s_{m-1} X_{\alpha_{m+2}} s_{m+2} \cdots X_{\alpha_1} s_1 X_{\alpha_l} s_l\right) \cap G \\ C'' &= \left(X_{\alpha_m} X_{\alpha_{m+1}} X_\alpha s_\alpha T_\alpha X_{\alpha_{m-1}} s_{m-1} X_{\alpha_{m+2}} s_{m+2} \cdots X_{\alpha_1} s_1 X_{\alpha_l} s_l\right) \cap G. \end{aligned} \tag{A.5}$$

In [24, (9.4), (9.5)] (compare [23, proof of (III.2.11)]), Steinberg proved that *every p'-element of G is conjugate to an element* of $C' \cup C''$. Moreover, every p'-element of the group $G^* = \langle X_{\pm\alpha_i}, X_{\pm\alpha} | i \neq m, m+1 \rangle \cap G \cong SU(2m, q)$ is conjugate in G^* to a power of an element of C' [24, (9.12)].

Set $v = r_{m-1} \cdots r_1$. *We will show that* $(C')^v$ *and* $(C' \cup C'')^v$ *are contained in the coset* QHc' constructed in (B28) for $SU(2m, q)$ and $SU(2m+1, q)$, respectively.

By (A.5),

$$C' = \left(X_\alpha r_m X_{\alpha_{m-1}} X_{\alpha_{m+2}} r_{m-1} \cdots X_{\alpha_1} X_{\alpha_i} r_1\right) \cap G$$
$$\subseteq U_{\beta_m} r_m U_{\beta_{m-1}} r_{m-1} \cdots U_{\beta_1} r_1$$

by [4, (13.6.1)]. Then

$$C' \subseteq U_{\gamma_m} U_{\gamma_{m-1}} \cdots U_{\gamma_1} r_m r_{m-1} \cdots r_1,$$

where $\gamma_m = \beta_m$ and, if $i < m$, $\gamma_i = \beta_i^{r_{i+1} \cdots r_m} = \beta_i + \beta_{i+1} + \cdots + \beta_m$. (Note that this implies that $C' \subseteq O_p(P_m) r_m r_{m-1} \cdots r_1$, whereas we are after $O_p(P_1)$.) Then $\gamma_m^v = \beta_m + 2\Sigma_1^{m-1}\beta_j$ and $\gamma_i^v = \gamma_m^v - \Sigma_1^i \beta_j$ for $i \leqslant m-1$. Thus, each γ_i^v involves β_1, so that $C' \subseteq O_p(P_1)(r_m \cdots r_1)^v$. Similarly, $C'' \subseteq O_p(P_1) H (r_m \cdots r_1)^v$.

Finally, P_1 is the stabilizer of y_1 in G [7, Sect. 3]. Thus, $C' \cup C'' \subseteq O_p(G_{y_1}) H (r_m \cdots r_1)^v$. But the present elements r_i are the elements t_i found in (B25), while $c^{-1} = r_m \cdots r_1$ and $v = r_m c^{-1}$. Thus, $c' = (r_m \cdots r_1)^v$ and $C' \cup C'' \subseteq O_p(P_1) H c'$. Intersecting with G^*, we find that C' behaves correctly for G^*.

Thus, we have now seen that Steinberg's results contain the information required in (B9) and (B27).

Remark. In fact, C, C', and $C' \cup C''$ are much smaller than the sets used in (B9) and (B27): the latter sets have size approximately equal to the square of that of the appropriate set C, C', or $C' \cup C''$. However, this does not seem to help improve any of the timing estimates indicated in Section 14.

REFERENCES

1. M. D. ATKINSON, An algorithm for finding the blocks of a permutation group, *Math. Comp.* **29** (1975), 911–913.
2. P. J. CAMERON, Finite permutation groups and finite simple groups, *Bull. London Math. Soc.* **13** (1981), 1–22.
3. J. J. CANNON, Effective procedures for the recognition of primitive groups, *Proc. Symp. Pure Math.* **37** (1980), 487–493.
4. R. W. CARTER, "Simple Groups of Lie Type," Wiley, London/New York/Sydney/Toronto, 1972.

5. R. W. CARTER AND P. FONG, The Sylow 2-subgroups of the finite classical groups, *J. Algebra* **1** (1964), 139–151.
6. B. N. COOPERSTEIN, Minimal degree for a permutation representation of a classical group, *Israel J. Math.* **30** (1978), 213–235.
7. C. W. CURTIS, W. M. KANTOR, AND G. M. SEITZ, The 2-transitive permutation representations of the finite Chevalley groups, *Trans. Amer. Math. Soc.* **218** (1976), 1–57.
8. J. DIEUDONNÉ, "La Géométrie des Groupes Classiques," Springer, Berlin/Göttingen/Heidelberg, 1963.
9. M. FURST, J. HOPCROFT, AND E. LUKS, Polynomial-time algorithms for permutation groups, *in* "Proc. 21st IEEE Sympos. Found. Comput. Sci.," 1980, pp. 36–41.
10. D. GORENSTEIN, "Finite Simple Groups: An Introduction to Their Classification," Plenum, New York, 1982.
11. C. M. HOFFMAN, "Group-Theoretic Algorithms and Graph Isomorphism," Lect. Notes in Comput. Sci. Vol. 136, Springer-Verlag, New York/Berlin, 1982.
12. W. M. KANTOR, Classical groups from a non-classical viewpoint, Maths. Inst. Oxford, 1978.
13. W. M. KANTOR, Subgroups of classical groups generated by long root elements, *Trans. Amer. Math. Soc.* **248** (1979), 347–379.
13a. W. M. KANTOR, Permutation representations of the finite classical groups of small degree or rank, *J. Algebra* **60** (1979), 158–168.
14. V. LANDAZURI AND G. M. SEITZ, On the minimal degrees of projective representations of finite Chevalley groups, *J. Algebra* **32** (1974), 418–443.
15. E. M. LUKS, Isomorphism of graphs of bounded valence can be tested in polynomial time, Proc. 21st I.E.E.E. Symp. Found. Comp. Sci. (1980), 42–49.
16. E. M. LUKS, in preparation.
17. E. M. LUKS, unpublished.
18. J. MCLAUGHLIN, Some groups generated by transvections, *Arch. Math. (Basel)* **18** (1967), 364–368.
19. J. MCLAUGHLIN, Some subgroups of $SL_n(F_2)$, *Illinois J. Math.* **13** (1969), 108–115.
20. W. H. PATTON, The minimum index for subgroups in some classical groups: A generalization of a theorem of Galois, Thesis, Univ. of Illinois at Chicago Circle, 1972.
21. J. J. ROTMAN, "*The Theory of Groups*," 2nd ed., Allyn and Bacon, Boston, 1973.
22. C. C. SIMS, Some group-theoretic algorithms, Springer Lect. Notes in Math. **697** (1978), 108–124.
23. T. A. SPRINGER AND R. STEINBERG, Conjugacy classes, Lect. Notes in Math. Vol. 131, pp. 167–266, Springer-Verlag, New York/Berlin, 1970.
24. R. STEINBERG, Regular elements of semisimple algebraic groups, *Inst. Haute Étude Sci. Publ. Math.* **25** (1965), 281–312.
25. A. J. WEIR, Sylow p-subgroups of the classical groups over finite fields with characteristic prime to p, *Proc. Amer. Math. Soc.* **6** (1955), 529–533.
26. H. WIELANDT, "Finite Permutation Groups," Academic Press, New York, 1964.