JOURNAL OF COMPUTER AND SYSTEM SCIENCES 30, 359–394 (1985)

Sylow's Theorem in Polynomial Time

WILLIAM M. KANTOR*

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

Received May 16, 1984; revised March 1, 1985

Given a set Γ of permutations of an n-set, let G be the group of permutations generated by Γ. If p is a prime, a Sylow p-subgroup of G is a subgroup whose order is the largest power of p dividing $|G|$. For more than 100 years it has been known that a Sylow p-subgroup exists, and that for any two Sylow p-subgroups P_1, P_2 of G there is an element $g \in G$ such that $P_2 = g^{-1}P_1 g$. We present polynomial-time algorithms that find (generators for) a Sylow p-subgroup of G, and that find $g \in G$ such that $P_2 = g^{-1}P_1 g$ whenever (generators for) two Sylow p-subgroups P_1, P_2 are given. These algorithms involve the classification of all finite simple groups.

PART I

1. *Introduction*

Sylow's theorem is one of the standard topics in senior-level abstract algebra. It is also one of the most fundamental results used in group theoretic research. In this paper we will prove an algorithmic version of Sylow's theorem:

MAIN THEOREM. *There are polynomial-time algorithms which, when given a subgroup G of the symmetric group S_n and a prime p, solve the following problems:*

(i) *given a p-subgroup P of G, find a Sylow p-subgroup of G containing P; and*

(ii) *given Sylow p-subgroups P_1, P_2 of G, find $g \in G$ conjugating P_1 to P_2.*

Here, G is specified as $\langle \Gamma \rangle$, the subgroup of S_n generated by a given subset Γ of S_n. Similarly, all of the p-groups appearing in the theorem are given in terms of generating permutations.

Note that the Main Theorem contains, in particular, the problem of finding a Sylow p-subgroup of G (just let $P = 1$). Special cases of this problem were solved in [10, 11, and 12], where the structure of G was assumed to be greatly restricted. Similarly, a special case of (ii) appears in [11]. Another problem attacked (unsuccessfully) in [10 and 11] is that of finding the largest normal p-subgroup $O_p(G)$ of G. Since that group is the intersection of all the Sylow p-subgroups of G, recursion

* This research was supported in part by NSF Grant MCS 7908130-82.

0022-0000/85 $3.00

571/30/3-8

easily produces the following consequence of the theorem (see the proof of [11, (4.4)]).

COROLLARY. *Given $G \leqslant S_n$ and a prime p, $O_p(G)$ can be found in polynomial time.*

The proof of the Main Theorem (and hence of the corollary) involves the classification of finite simple groups (cf. [6]). The algorithms are long, involved, and impractical (running in time $O(n^9)$), due to the complicated nature of these simple groups. On the other hand, when specialized to the case of solvable groups G, the algorithms become pleasant and are probably practical (see the Appendix).

The present paper is a continuation of [10 and 11]. In [10], we proved the initial stages of the recursive proof of the Main Theorem. Moreover, [10 and 11] contain most of the ideas in the proof. These ideas will be outlined as we describe the structure of the paper.

Part I consists of the introduction (Sect. 1) and preliminaries (Sect. 2). The latter section briefly reviews standard notation and known polynomial-time group theoretic algorithms.

Part II is the most interesting part of the paper. It contains various polynomial-time reductions. These reduce the Main Theorem to special cases of that theorem in which the structure of G is greatly restricted: G is either simple or has a simple normal subgroup of index p. In effect, similar reductions appear in [11], but special cases of the Intersection Problem [12] were used in the course of those reductions. We have now been able to avoid the restrictions on G imposed in [11], by avoiding the Intersection Problem entirely. Nevertheless, as in [11], the main idea is that conjugacy (part (ii) of the Main Theorem) can be used to construct Sylow subgroups. As in [11], the reductions to simple groups rely on a theorem of Luks [13], which finds a composition series in polynomial time. The classification of finite simple groups is involved in these reductions, both in the use of [13] and in the more detailed information concerning finite simple groups required in the Replacement Theorem (cf. [10] and Sect. 9).

Part III is essentially an independent short paper. It amounts to a commentary on the Replacement Theorem proved in [10] (see (9.1) below), which takes any simple group $G \leqslant S_n$ with $|G| > n^8$ and produces an especially nice new permutation representation of G (in polynomial time). Theorem 9.3 goes one step further in the case of a simple classical group G: it reconstructs the vector space V and the form used in the definition of G. The proof involves classical projective geometry. Half of Part III consists of consequences of the construction of V.

Finally, Part IV contains the end of the proof of the Main Theorem. Here we again need the algorithms concerning simple groups G that were obtained in Part III and in [10] (all with the help of the classification of finite simple groups). The arguments resemble those of [10], where they were used to find Sylow subgroups of simple groups. However, they are not quite as ugly as the corresponding portions of [10], due in part to the use of recursion in our much more general setting.

In the Appendix we have provided specializations of our algorithms to the case of

solvable groups. The reader may wish to begin the paper there, in order to obtain an elementary introduction to our methods. There are also extensions of parts of the Main Theorem to the case of Hall π-groups (as in [11]). All of the results (but not the algorithms) in the Appendix can also be found in [11].

The importance of group theoretic algorithms in computational complexity has been made very clear in [12]. In particular, a restricted version of Sylow's theorem plays a significant role in that paper. On the other hand, it should be noted that the standard proofs of Sylow's theorem produce Sylow p-subgroups in exponential time—even when $p=2$. Moreover, even in CAYLEY [1] the Sylow subgroup algorithm involves backtrack and hence is exponential. On the other hand, neither in CAYLEY nor elsewhere (except for [11]) does there seem to be an efficient version of the conjugacy part of Sylow's theorem. In the solvable case, the algorithms in the Appendix appear to provide moderately practical algorithms for these purposes.

2. *Preliminaries*

In this section we will briefly review the notation used in [10 and 11].

We will consider $G=\langle \Gamma \rangle \leqslant S_n = \mathrm{Sym}(X)$, where $|X|=n$. If necessary, Sims' algorithm [15, 5] can be used to arrange that $|\Gamma| \leqslant n^2$.

The orbit of $x \in X$ is x^G, while the stabilizer $G_x = \{ g \in G \mid x^g = x \}$. More generally, if $Y \subseteq X$, its pointwise stabilizer is $G_{(Y)}$, its set stabilizer is G_Y, and $G_Y^Y \cong G_Y/G_{(Y)}$ is the group induced by G_Y on Y. Similarly, if Y is any set on which G acts then $G_{(Y)}$ is its pointwise stabilizer and G^Y is the group induced by G on Y.

We will frequently use (without explicit mention) the fact that any strictly increasing sequence of subgroups of S_n has at most $n \log_2 n$ terms. This will be an essential ingredient for recursion.

List of Some Known Algorithms

Given a group $G \leqslant S_n = \mathrm{Sym}(X)$, each of the following constructions can be carried out in polynomial time.

(A.1) [15; 5] *Given $Y \leqslant X$, find $G_{(Y)}$ and $|G_{(Y)}|$.*

(A.2) [5] *Given $h \in S_n$, determine whether or not $h \in G$.*

(A.3) *Find all orbits of G.*

(A.4) [5] *Given a set Y of polynomial size on which G acts, find $G_{(Y)}$.*

(A.5) [5] *Given $S \subseteq G$, find $\langle S^G \rangle$.*

(A.6) [5] *Find the derived series of G.*

(A.7) [5] *Given H normalizing G, find $G \cap H$.*

(A.8) [13] *Given $H \trianglelefteq G$, find the centralizer $C_G(H)$. In particular, find $Z(G)$.*

(A.9) *If $H \lhd G$ with $|H| = q^a$ and $|G/H| = p$ for distinct primes p, q, and if P_1 and P_2 are Sylow p-subgroups of G, find $f \in G$ with $P_1^f = P_2$.* (This is a very special case of [11, (4.1)].)

(A.10) [13] *Given $R \lhd G$, find a set X' on which G acts such that $G^{X'}$ is simple, $R^{X'} = 1$ and $|X'| \leqslant n$.*

(A.11) [10] *If G is simple and p is a prime, find a Sylow p-subgroup of G.*

Finally, we will need the following result.

LEMMA 2.1. *Let $T \lhd M \lhd G$ with M/T simple. Let K be the kernel of the permutation representation of G on the cosets of T. Then either $|M/T|$ is a prime q and $|M/K|$ is a q-group, or the following hold.*

(i) *$M/K = S_1 \times \cdots \times S_l$, where $S_i \cong M/T$.*

(ii) *$\{S_1, \ldots, S_l\}$ is the set of minimal normal subgroups of M/T, and G/M is transitive on this set.*

(iii) *S_i is nonabelian.*

(iv) *If $G \leqslant \mathrm{Sym}(X)$ then $\{S_1, \ldots, S_l\}$ can be found in polynomial time.*

Proof. (i)–(iii) WLOG $K = 1 \neq T$. Let S be a minimal normal subgroup of G contained in T. Then $S \not\leqslant T^g$ for some $g \in G$, so that $T^g \lhd ST^g \trianglelefteq M$. Thus, $M = ST^g$ and $S \cong M/T^g$ is simple (note that $S \cap T^g = 1$).

We claim that, if $|M/T| = q$ is a prime, then M is a q-subgroup. For, $\langle S^G \rangle$ is a q-group. If $M > \langle S^G \rangle$, simply pass modulo $\langle S^G \rangle$ and induct.

Now we may assume that S is nonabelian. Let $S_1, \ldots, S_l$ be the conjugates of S in G. Then $[S_i, S_j] \leqslant S_i \cap S_j = 1$ for $i \neq j$, so that $S_i S_j = S_i \times S_j$.

Similarly, $[S, T^g] \leqslant S \cap T^g = 1$, so that $M = S \times T^g$. Thus, for each S_i there is a conjugate T_i of T^g such that $M = S_i \times T_i$. If $j \neq i$ then $S_j \leqslant T_i$ (as $1 \neq S_i S_j \cap T_i \lhd S_i \times S_j$ and $S_i S_j \cap T_i \neq S_i$).

Now $M = S_1 \times T_1$ implies that $T_2 = S_1 \times (T_1 \cap T_2)$, so that $M = S_1 \times S_2 \times (T_1 \cap T_2)$. Continuing in this manner, we find that $M = S_1 \times \cdots \times S_l \times \bigcap_1^l T_i = S_1 \times \cdots \times S_l \times K = S_1 \times \cdots \times S_l$.

(iv) Intersect conjugates of T in order to find $H \rhd K$ with $H/K = S_i$ for some i. Then $S_i^G = \{S_1, \ldots, S_l\}$ can be found as well. ∎

PART II. REDUCTIONS

3. *Outline of Proofs*

Given $G \leqslant S_n$, we will consider the following eight problems:

SYLFIND
Input: Prime p.
Output: A Sylow p-subgroup of G.

SYLCONJ
Input: Sylow p-subgroups P_1, P_2 of G.
Output: $f \in G$ with $P_1^f = P_2$.

SYLCONJ1
Input: Sylow p-subgroups P_1, P_2 of G; $M \lhd G$ with $|G/M| = p$ and $P_1 \cap M = P_2 \cap M \lhd G$.
Output: $f \in G$ with $P_1^f = P_2$.

SYLCONJSIMPLE Same as SYLCONJ with G simple.

SYLEMBED
Input: A p-subgroup P of G.
Output: A Sylow p-subgroup containing P.

SYLEMBED1
Input: A p-subgroup P of G that is not a Sylow p-subgroup; $M \lhd G$ with $P \cap M \lhd G$ and G/M a cyclic p-group.
Output: A p-subgroup of G properly containing P.

SYLEMBEDSIMPLE Same as SYLEMBED with G simple.

SYLEMBED1SIMPLE
Input: Same as SYLEMBED1 with M simple and $P \cap M = 1$.
Output: $m \in M$ of order p centralized by P.

The proof of the Main Theorem will proceed in the following stages.

THEOREM 3.1. *SYLFIND is reducible to SYLCONJ.*

THEOREM 3.2. *SYLCONJ is reducible to the combination of SYLCONJ*1 *and SYLCONJSIMPLE.*

THEOREM 3.3. *SYLCONJ*1 *is reducible to SYLCONJSIMPLE.*

THEOREM 3.4. *There is a polynomial-time algorithm for SYLCONJSIMPLE.*

While the proof of Theorems 3.1–3.3 are pleasant and not difficult, that of Theorem 3.4 is, in effect, an ugly case analysis. In any event, the preceding results contain more than half of the Main Theorem:

COROLLARY 3.5. *There are polynomial-time algorithms for SYLFIND and SYLCONJ.*

THEOREM 3.6. *SYLEMBED is reducible to the combination of SYLCONJ, SYLEMBED*1, *and SYLEMBEDSIMPLE.*

THEOREM 3.7. *SYLEMBED*1 *is reducible to the combination of SYLCONJ and SYLEMBED*1*SIMPLE.*

THEOREM 3.8. *There is a polynomial-time algorithm for SYLEMBED*1*SIMPLE.*

THEOREM 3.9. *There is a polynomial-time algorithm for SYLEMBEDSIMPLE.*

Clearly, Theorems 3.1–3.9 imply the Main Theorem. Theorems (3.1)–(3.4) and (3.6)–(3.9) are handled in the following sections:

(3.1), 4; (3.2), 5; (3.3), 6; (3.4), 7; (3.6), 7; (3.7), 8; (3.8), 18; (3.9), 19.

Note that SYLFIND is not mentioned in Theorems 3.2–3.4 and is a special case of SYLEMBED. However, the proof of Theorem 3.1 is short, and its main ideas reappear (and are referred to) later.

Theorems 3.4, 3.8, and 3.9 are not actually proved as stated. For example, in Section 17 we introduce a procedure called SYLCONJSIMPLE in which the procedure SYLCONJ used to prove Theorem 3.2 appears as a subprocedure applied recursively to proper subgroups of G. While this intertwining of procedures could have been avoided, it has the advantage of cutting down the amount of technical linear algebra.

4. *Procedure SYLFIND*

In this section we will present a procedure called SYLFIND behaving as required in Theorem 3.1.

SYLFIND
Input: Prime p.
Output: A Sylow p-subgroup of G.

1. Use (A.10) to find a set X' on which G acts such that $G^{X'}$ is simple and $|X'| \leqslant n$.

Use (A.4) to find $M = G_{(X')}$.

2. If $|G/M| \neq p$, use (A.11) to find a Sylow p-subgroup H/M of G/M. Then $G \leftarrow H$ and use recursion. (Here, H contains a Sylow p-subgroup of G.)

3. WLOG $|G/M| = p$. Recursively find a Sylow p-subgroup P of M.

4. Let $g \in G - M$ (use one of the given generators of G).

Use the hypothesized SYLCONJ subprocedure to find $m \in M$ with $(P^g)^m = P$. (Note that P and P^g are both Sylow in M.)

5. Find the Sylow p-subgroup $\langle g' \rangle$ of $\langle gm \rangle$. Then $\langle P, g' \rangle$ is a Sylow p-subgroup of G. (For, $g' \notin M$, so that $|\langle P, g' \rangle| = |P| \cdot p$.) ∎

Note that the preceding procedure is virtually identical to that of [11, (4.3)].

5. *Procedure SYLCONJ*

In this section we will simultaneously prove Theorem 3.2 and present a procedure called SYLCONJ that will be called later (in Sect. 17).

SYLCONJ
Input: Sylow p-subgroups P_1, P_2 of G.
Output: $f \in G$ with $P_1^f = P_2$.

1. Use (A.10) to find a set X' on which G acts such that $G^{X'}$ is simple and $|X'| \leqslant n$. Use (A.4) to find $M = G_{(X')}$.

2. If $G^{X'}$ is nonabelian, use the hypothesized SYLCONJSIMPLE subprocedure to find $g \in G$ with $(P_1^{X'})^g = P_2^{X'}$.

Then $G \leftarrow \langle P_1^g, P_2 \rangle$ (and $P_1 \leftarrow P_1^g$), and use recursion. (Note that $\langle P_1^g, P_2 \rangle^{X'}$ is a p-group while $G^{X'}$ is not.)

3. If $|G^{X'}|$ is a prime $\neq p$ then $G \leftarrow M$.

4. WLOG $|G^{X'}| = p$.

Recursively find $m \in M$ with $(P_1 \cap M)^m = P_2 \cap M$. Let $G^* = \langle P_1^m, P_2 \rangle$ and $M^* = M \cap G^*$ (use (A.7)).

5. Use the hypothesized SYLCONJ1 subprocedure to find $g \in G^*$ with $(P_1^m)^g = P_2$, and let $f = mg$.

(Since $P_i \cap M \lhd P_i$, both P_1^m and P_2 normalize $P_1^m \cap M = P_2 \cap M$. Then $P_2 \cap M \lhd G^*$. Also, $P_1^m \not\leqslant M$, so that $|G^*/M^*| = p$. Thus, SYLCONJ1 is applicable.) ∎

Remark. It is important to note that neither n nor $|G|$ increased at any step, so that we may use the above procedure SYLCONJ as a subprocedure later.

6. *Procedure SYLCONJ1*

In this section we will present a procedure called SYLCONJ1 behaving as required in Theorem 3.3.

SYLCONJ1

Input: Sylow p-subgroups P_1, P_2 of G; $M \lhd G$ with $|G/M| = p$ and $P_1 \cap M = P_2 \cap M \lhd G$.

Output: $f \in G$ with $P_1^f = P_2$.

(We begin by constructing a new set Y on which G acts, where $|Y| \leqslant n^2$ (see step 2).)

1. WLOG $P_1 \cap M < M$. (Otherwise $= P_1 = P_2$.)

Use (A.10) to find a set X' on which M acts such that $M^{X'}$ is simple, $R^{X'} = 1$, and $|X'| \leqslant n$.

Use (A.4) to find $T = M_{(X')}$. (Then $T \geqslant R$ and $M/T \cong M^{X'}$.)

Use (A.1) to find $H = M_{x'}$ for some $x' \in X'$.

2. Let Y be the set of cosets of H in G. Determine the action of (the generators of) G on Y. (Note that $|Y| \leqslant p|X'| \leqslant n^2$.)

Use (A.4) to find $K = G_{(Y)}$.

3. If $g \in G$ and $G^* = \langle P_1^g, P_2 \rangle \neq G$ then $M \leftarrow M \cap G^*$, $G \leftarrow G^*$, and $P_1 \leftarrow P_2^g$, and use recursion. (Find $M \cap G^*$ using (A.7). Note that $P_2 \cap M = (P_1 \cap M)^g = P_1^g \cap (M \cap G^*)$.)

4. If $|M/T| = q$ is a prime, use (A.9) to find $g \in G$ with $(P_1^Y)^g = P_2^Y$. Let $G^* = \langle P_1^g, P_2 \rangle$ and return to 3.

(By Lemma 2.1, M/K is a q-group, so that G^Y is solvable. Note that G^{*Y} is a p-group while G^Y is not.)

5. WLOG M/T is a nonabelian simple group S. Let $d_i \in P_i - R$.

6. *Case* $M/K \neq M/T$.

6.1. Use Lemma 2.1(iv) to find subgroups $S_1, \ldots, S_p$ of M/K such that $M/K = S_1 \times \cdots \times S_p$, $S_j \cong S$, and G/M is transitive on $\{S_1, \ldots, S_p\}$.

6.2. Pick a prime $q \mid |S_1|$. Use (A.11) to find a Sylow q-subgroup Q of S_1.

6.3. For $i = 1, 2$, let $d = d_i^Y$ and $Q_i = \langle Q^{\langle d \rangle} \rangle$.
Find $g \in M$ such that $Q_1^g = Q_2$.

(Since P/R is Sylow in G/R, $|d| = p$. Thus, there are exactly p groups Q^{d^j}, $0 \leqslant j \leqslant p-1$, and these belong to different factors S_j. Consequently, Q_i is a Sylow q-subgroup of $S_1 \times \cdots \times S_p$. Clearly, $Q = Q_i \cap S_1$. Recursively apply the hypothesized SYLCONJSIMPLE subprocedure to each S_j in order to conjugate $Q_1 \cap S_j$ to $Q_2 \cap S_j$ for each j. This produces the desired g.)

6.4. Let $G^* = \langle P_1^g, P_2 \rangle$ and return to 3. (Both d_1^g and d_2 normalize $Q_1^g = Q_2$. Then $\langle R, d_1^g, d_2 \rangle^Y = \langle P_1^g, P_2 \rangle^Y$ normalizes Q_2 whereas G^Y certainly does not: each S_j is simple. Thus, $G^* \neq G$.)

7. *Case* $M/K = M/T = S$.

7.1. If $|S| \leqslant n^8$ or $C_{G/K}(S) \neq 1$, find $g \in G$ with $(P_1^Y)^g = P_2^Y$ and return to 3.

(If $|S| \leqslant n^8$ use brute force to find g.
Use (A.8) to find $C_{G/K}(S)$ (recall that $G/K \cong G^Y$). If this group is nontrivial then $G/K \cong S \times \mathbb{Z}_p$ and $P_1^Y = P_2^Y$.)

7.2. We may assume that neither situation in 7.1 occurs. Then S is not a sporadic simple group, and G/M induces an outer automorphism of S.

7.3. Use the Replacement Theorem (9.1) to find a proper subgroup L of S of index $\leqslant |X'|^2 \leqslant n^2$.

7.4. Replace L by one of its conjugates so that d_2 normalizes L.
Find $g \in G$ so that d_1^g normalizes L.

Comments. We have $G^Y \rhd M^Y = S$, and G^Y/M^Y induces (by conjugation) a group $\langle \theta \rangle$ of automorphisms of the simple group S. Here, $|\theta| = p$ and $p \nmid |S|$. Thus, S is not an alternating group.

It follows that S is a Chevalley group of characteristic $u \neq p$. Now θ acts on the set of Sylow u-subgroups of S, and hence normalizes one of them, U say. Then θ also normalizes $B = N_S(U)$, and permutes the set of subgroups of S containing B. Since $|\theta| = p \nmid |S|$, θ must normalize each such subgroup (see [2, pp. 112, 199–202, 211]). One of these subgroups is conjugate in S to L (cf. Theorem 9.1(iii)). Since L has at most n^2 conjugates in S, the action of (the generators of) S on this set of conjugates can be determined in polynomial time.

We may assume that θ is just the automorphism induced by d_2^Y, and that d_2^Y normalizes L.

Similarly, d_1^Y normalizes some conjugate of L, so that g can be found.

7.5. Let $G^* = \langle P_1^g, P_2 \rangle$ and return to 3.
($\langle R, d_1^g, d_2 \rangle^Y = \langle P_1^g, P_2 \rangle^Y$ normalizes L^Y while G^Y does not.) ▮

7. *Procedure SYLEMBED*

In this section we will describe a procedure called SYLEMBED behaving as required in Theorem 3.6.

SYLEMBED
Input: A p-subgroup P of G.
Output: A Sylow p-subgroup containing P.

1. Use (A.10) to find a set X' on which G acts such that $G^{X'}$ is simple and $|X'| \leqslant n$.

Use (A.4) to find $M = G_{(X')}$.

2. If $|G/M| \neq p$, use the hypothesized SYLEMBEDSIMPLE subprocedure to embed $P^{X'}$ in a Sylow p-subgroup $H^{X'}$ of $G^{X'}$, where $H \geqslant M$.

Then $G \leftarrow H$ and use recursion. (Note that $G^{X'} > H^{X'}$, and that H contains a Sylow p-subgroup of G.)

3. WLOG $|G/M| = p$.

Case $P \leqslant M$. If P is not a Sylow p-subgroup of M, then $G \leftarrow M$ and use recursion.

If P is Sylow in M, repeat Steps 4 and 5 of Section 4 (using SYLCONJ), in order to obtain a p-group properly containing P.

4. *Case* $P \not\leqslant M$.

4.1. Recursively find $Q \leqslant M$ with $P \cap M \lhd Q$ and $|Q/(P \cap M)| = p$. (Note that $P \cap M$ cannot be Sylow in M, since P is not Sylow in G and $|G: M| = |P: P \cap M|$.)

4.2. Let $G^* = \langle P, Q \rangle$. Find $M^* = M \cap G^*$ using (A.7). (Note that $P \cap M \lhd G^*$. Also, $P \cap M$ is not Sylow in M^* since $Q \leqslant M^*$, so that P is not Sylow in G^*.)

4.3 Apply the hypothesized SYLEMBED1 subprocedure to the triple G^*, M^*, P. ▮

8. *Procedure SYLEMBED1*

In this section we will present a procedure called SYLEMBED1 behaving as required in Theorem 3.7.

SYLEMBED1
Input: A p-subgroup P of G that is not a Sylow p-subgroup; $M \lhd G$ with $P \cap M \lhd G$ and G/M a cyclic p-group.
Output: A p-subgroup of G properly containing P.

1. WLOG $P \cap M < M$. (Otherwise, G is a p-group.)

Use (A.10) to find a set X' on which M acts such that $M^{X'}$ is simple, $(P \cap M)^{X'} = 1$ and $|X'| \leqslant n$.

Use (A.4) to find $T = M_{(X')}$. (Then $T \geqslant P \cap M$.)

Use (A.1) to find $H = M_{x'}$ for some $x' \in X'$.

2. Let Y be the set of cosets of H in G. Determine the action of (the generators of) G on Y. (Note that $|Y| = |G/M| \cdot |X'| \leqslant n^2$ since G/M is a cyclic p-group.)

Use (A.4) to find $K = G_{(Y)}$. (Then $G > M > H \geqslant T \geqslant K \geqslant P \cap M$.)

3. If G/K is a cyclic p-group, $M \leftarrow K$ and return to 1. (Note that $|K| < |M|$.) We may now assume that G/K is noncyclic if it is a p-group.

4. Let $PM/M = \langle fM \rangle$ with $f \in P$.

5. *Case* $|M/T| = p$.

5.1. Let $M^* = \langle K, f \rangle$. (By Lemma 2.1, G/K is a p-group, and hence is noncyclic by 3. Thus, $G > M^* \geqslant (P \cap M)\langle f \rangle = P$.)

5.2. Find $G^* \leqslant G$ with $M^* \lhd G^*$ and $|G^*/M^*| = p$. (Since M^*/K is a proper subgroup of the p-group G/K, it is easy to find G^*.)

5.3. If P is not Sylow in M^* then $G \leftarrow M^*$ and $M \leftarrow K$ and use recursion. (Since $M^* = K\langle f \rangle$, M^*/K is a cyclic group.)

5.4. If P is Sylow in M^* then $G \leftarrow G^*$ and $M \leftarrow M^*$, and use SYLCONJ exactly as in steps 4 and 5 of Section 4 in order to find a p-subgroup properly containing P.

6. WLOG $|M/T| \neq p$.

If $G > PM$ then either P is not Sylow in PM, in which case $G \leftarrow PM$ and use recursion; or P is Sylow in PM, where $PM \lhd G$, in which case $M \leftarrow PM$ and use SYLCONJ and steps 4 and 5 of Section 4 in order to find a p-subgroup properly containing P.

WLOG $G = PM$. (Now $G = \langle f \rangle M$.)

7. If $p \nmid |M/T|$, then $G \leftarrow \langle f, K \rangle$ and $M \leftarrow K$, and use recursion. (By 6 and Lemma 2.1, $PK/K = \langle f \rangle K/K$ is Sylow in G/K. However, P is not Sylow in $\langle f, K \rangle$ since that group contains a Sylow p-subgroup of G.)

8. WLOG M/T is a nonabelian simple group of order divisible by p.

Use Lemma 2.1(iv) to find simple subgroups $S_1, \ldots, S_l$ of M/K permuted transitively by $\langle f \rangle$ such that $M/K = S_1 \times \cdots \times S_l$.

9. *Case* $l = 1$. (Here $G/K = (M/K)\langle fK \rangle$ with M/K simple.)

9.1. If $G/K = (M/K) \times \langle fK \rangle$ use (A.11) to find $m \in M$ with $|mK| = p$. Then $G \leftarrow \langle K, m, f \rangle$ and $M \leftarrow \langle K, m \rangle$, and use recursion. (Note that $\langle K, m, f \rangle \geqslant \langle P \cap M, f \rangle = P$ and $|\langle K, m \rangle / K| = p$, while $f \notin \langle K, m \rangle$.)

9.2. WLOG f acts nontrivially on M/K.

Find $f' \in \langle f \rangle$ such that f' induces an automorphism of M/K of order

p. (Test successive powers of f to find the last one that does not centralize some generator of M/K.)

9.3. Find $m \in M$ such that $|mK| = p$ and f^r centralizes in K. (Apply the hypothesized SYLEMBED1SIMPLE subprocedure to the group $(M/K)(\langle f \rangle / \langle f^{r^p} \rangle$.)

9.4. Let $G^* = \langle K, m, f \rangle$. Find $M \cap G^*$ using (A.7).
Now $G \leftarrow G^*$ and $M \leftarrow M \cap G^*$, and use recursion. (Note that $G^*/K = \langle (mK)^{\langle fK \rangle} \rangle \langle fK \rangle$ is a p-group. Since G/K is not a p-group, $G^* < G$. Since $P \cap M \leqslant K$, $mK \notin \langle fK \rangle$, so that $G^*/K > \langle fK \rangle = PK/K$ and P is not Sylow in G^*.)

10. *Case* $l > 1$.

10.1. Find the stabilizer $\langle f_1 \rangle$ of S_1 in $\langle f \rangle$. (Then f_1 normalizes each S_i, since $\langle f \rangle$ is transitive on $\{S_1, \ldots, S_l\}$.)

10.2. If $f_1 K$ centralizes S_1, use (A.11) to find $m \in M$ such that $mK \in S_1$ and $|mK| = p$.
Let $G^* = \langle K, m, f \rangle$.
Find $M \cap G^*$ using (A.7). Then $G \leftarrow G^*$ and $M \leftarrow M \cap G^*$, and use recursion.
(Note that $\langle f \rangle$ conjugates $\langle mK \rangle$ to l groups of order p, one in each S_i. Thus, G^*/K is a p-group and hence $G^* < G$. Also, $G^* \geqslant (P \cap M)\langle f \rangle = P$, $G^* = (M \cap G^*)\langle f \rangle$, $m \notin \langle K, f \rangle$, and P is not Sylow in G^*.)

10.3. WLOG $f_1 K$ acts nontrivially on S_1.
Find $f' \in \langle f_1 \rangle$ such that $f'K$ induces an automorphism of S_1 of order p.
Find $m \in M$ with $mK \in S_1$, $|mK| = p$, and $f'K$ centralizing mK, by applying the hypothesized SYLEMBED1SIMPLE subprocedure to the group $S_1 \langle f' \rangle / \langle f'^p \rangle$.

10.4. Let $G^* = \langle K, m, f \rangle$. Find $M \cap G^*$ using (A.7).
Now $G \leftarrow G^*$ and $M \leftarrow M \cap G^*$, and use recursion (compare 10.2).

Timing. Only one comment is needed here, concerning the reduction to the situation in which G/K is a noncyclic p-group (see step 3). This is accomplished by repeated use of steps 1–3, until either G/K is a noncyclic p-group or $|M/T| \neq p$. Since M cannot decrease more than $n \log_2 n$ times, this reduction only requires polynomial time. ∎

PART III. REPLACEMENT THEOREM: LINEAR VERSION

9. *Replacement Theorem (Two Versions)*

The following two theorems were proved in [10]:

THEOREM 9.1 (Replacement Theorem). *There is a polynomial-time algorithm*

which, when given a simple subgroup G of S_n such that $|G| > n^8$, produces a set Y on which G acts satisfying the following conditions:

(i) $|Y| < 2n$;

(ii) *if* $G \cong A_m$ *then* $|Y| = m$ *and* G *acts on* Y *as* A_m;

(iii) *if* $G \ncong A_m$ *then* G *is a classical group defined on a vector space over a field* F, *and* G *acts on* Y *as it does on the unique orbit of* 1*-spaces of this vector space of size relatively prime to* $|F|$;

(iv) *no proper subgroup of* G *has index* $< |Y|$, *except when* $G \cong \mathrm{Sp}(2m, 2)$ *for some* m, *in which case there is a unique conjugacy class of proper subgroups of index* $< |Y|$; *and*

(v) *there is only one conjugacy class of subgroups of* G *of index* $|Y|$, *except when* $G \cong \mathrm{PSL}(d, q)$ *in which case there are exactly two such conjugacy classes.*

THEOREM 9.2 [10, (10.5)]. *In the situation of Theorem* 9.1(iii), *there is also a polynomial-time algorithm that finds a set* $\bar{Y} \supseteq Y$ *on which* G *acts exactly as it acts on the set of all* 1*-spaces of the vector space involved in the definition of* G. *Moreover,* $|\bar{Y}| < n^2$.

A number of further properties of $\bar{Y}$ were also proved. In Sections 11–13 we will provide a means for proving even more properties of $\bar{Y}$. While linear algebra is implicit in Sections 8–15 of [10], the following result will allow us to ignore the sets Y and $\bar{Y}$ in Theorems 9.1–9.2 and work directly with the relevant vector space (and even directly with matrices).

THEOREM 9.3 (Replacement Theorem: Linear Version). *There is a polynomial-time algorithm which, when given a simple subgroup* G *of* S_n *such that* $|G| > n^8$ *and* G *is isomorphic to a classical group, produces the following*:

(i) *a vector space* V (*of size* $< n^2$) *over a field* F *such that* G *acts on its set* $\bar{V}$ *of* 1*-spaces as a projective special linear, symplectic, orthogonal, or unitary group defined on* V;

(ii) *a group* $G^* = (G^*)'$ *of linear transformations of* V *such that* G^* *induces* G *on* $\bar{V}$;

(iii) *the form on* V *used to define* G^*, *if* G^* *is symplectic, orthogonal, or unitary*;

(iv) *a standard basis of* V (*defined in* (13.5));

(v) *an orthogonal basis of* V, *if one exists*;

(vi) *the matrix of a given* $g \in G^*$ *with respect to a basis* (iv) *or* (v);

(vii) *a matrix inducing a given* $g \in G$ *with respect to a basis* (iv) *or* (v); *and*

(viii) *whether or not a given matrix induces an element of* G.

In other words, any question concerning G can be restated as a question concern-

ing G^* and V. Moreover, elements of G can be constructed having nice actions (viii).

Throughout Sections 10–15 *we will assume the hypotheses of Theorem* 9.3.

Convention 9.4. As in [10], we will never consider the groups $\Omega(2m+1, 2^e)$. Instead, we will only deal with the isomorphic groups $\mathrm{Sp}(2m, 2^e)$. Thus, in Theorem 9.3 the space V will not have a radical. (Note that this convention is already implicit in Theorem 9.1(iv).)

10. *Projective Subspaces*

In this section we briefly review further properties of the sets Y and $\bar{Y}$ (cf. Theorems 9.1, 9.2) that were proved in [10]. First note that $\bar{Y}$ is the set of points of a projective geometry, so that it is natural to discuss *subspaces of* $\bar{Y}$.

(10.1) [10, (8.3), (10.6)]. Given $A \subseteq \bar{Y}$, the subspace $[A]$ determined by A can be found in polynomial time.

(10.2) [10, (10.3), (11.5); (8.1), (8.4), (10.4)]. In polynomial time it can be determined whether $G \cong \mathrm{PSL}(d, q)$, $\mathrm{PSp}(2m, q)$, $P\Omega^+(d, q)$, or $\mathrm{PSU}(d, q)$ for some d, q; and, moreover, d or m and q can be found.

Note that $|\bar{Y}| = (q^d-1)/(q-1)$, $(q^{2m}-1)/(q-1)$, or $(q^{2d}-1)/(q^2-1)$, so that once the prime divisor of q is known it is easy to find q and d.

(10.3) [10, (10.7)]. If G is symplectic, orthogonal, or unitary and if $A \subseteq \bar{Y}$ is given, the set A^* of all elements of $\bar{Y}$ perpendicular to A can be found in polynomial time.

In particular, given $y, z \in Y$, whether or not they are perpendicular can be determined in polynomial time.

(10.4) [10, (11.1(i))]. For G as in (10.3), a subset $\mathscr{B} = \{y_1, \ldots, y_m, z_1, \ldots, z_m\}$ of Y can be found such that the only nonperpendicular pairs of members of $\mathscr{B}$ are $\{y_i, z_i\}$, $i = 1, \ldots, m$, and moreover such that $\mathscr{B}^* \cap Y = \varnothing$.

11. *Construction of V*

In this section we will construct the vector space V required in Theorem 9.3(i), using classical projective geometry.

All we need is (10.1): the specific properties of G, and the form on V, are not relevant here. The point is that $\bar{Y}$ has the structure of a projective space, and all we have to do is introduce coordinates. For this purpose, we will first need to explicitly construct a field F, and then label each point of $\bar{Y}$ by a symbol $\langle a_1, \ldots, a_d \rangle$, where $(a_1, \ldots, a_d)$ is in the subset $(F^d)_1$ of $F^d - \{0\}$ consisting of all vectors whose last nonzero coordinate is 1. (Here $\langle a_1, \ldots, a_d \rangle$ is really just an abbreviation for $\langle (a_1, \ldots, a_d) \rangle$, the 1-space of F^d spanned by $(a_1, \ldots, a_d)$.)

PROPOSITION 11.1. *The following can be found in polynomial time: a field F, and a labeling of the points of $\bar{Y}$ by symbols $\langle v\rangle$, $v\in(F^d)_1$, such that the map $v\to\langle v\rangle$ induces an isomorphism from the projective space of F^d to the one on $\bar{Y}$.*

Proof. 1. Recursively find $x_1,\ldots,x_d\in\bar{Y}$ as follows: x_1 is arbitrary; if $x_1,\ldots,x_i$ have been obtained, use (10.1) to find $W_i=[x_1,\ldots,x_i]$, test whether $W_i=\bar{Y}$, and if not pick $x_{i+1}\in V-W_i$.

Comments. The x_i arise from a basis of the desired vector space. We will recursively introduce coordinates in W_i for $i=3,\ldots,d$, thereby inducing isomorphisms of projective spaces.

2. *Case* $i=3$. (Here we will also have to construct a field.)

2.1. Pick $u\in W_3-([x_1,x_2]\cup[x_2,x_3]\cup[x_3,x_1])$.

2.2. Let F be a set in $1-1$ correspondence with $[x_3,u]-\{u\}$.

2.3. Label the points of $[x_3,u]-([x_3,u]\cap W_2)$ as $\langle a,a,1\rangle$, where a runs through F and $0,1\in F$ are defined by $x_3=\langle 0,0,1\rangle$, $u=\langle 1,1,1\rangle$. Label $x_1=\langle 1,0,0\rangle$, $x_2=\langle 0,1,0\rangle$.

2.4. Label $[x_1,x_3]\cap[\langle a,a,1\rangle,x_2]=\langle a,0,1\rangle$ and $[x_2,x_3]\cap[\langle a,a,1\rangle,x_1]=\langle 0,a,1\rangle$. (This completes the labeling of the "x axis" and the "y axis".)

2.5. If $x\in W_3-W_2$, find $[x,x_2]\cap[x_1,x_3]=\langle a,0,1\rangle$ and $[x,x_1]\cap[x_2,x_3]=\langle 0,b,1\rangle$. Then label $x=\langle a,b,1\rangle$.

2.6. For each $\langle a,1,1\rangle\in[x_1,u]-\{x_1\}$, label $[x_3,\langle a,1,1\rangle]\cap W_2=\langle a,1,0\rangle$.

(At this stage, each point of W_3 has been labeled using an element of $F^3-\{(0,0,0)\}$ whose last nonzero coordinate is 1.)

2.7 (Definition of a binary operation $(a,b)\mapsto a+b$ on F.) Let $a,b\in F$. Find $\langle c_1,c_2,1\rangle=[\langle 0,b,1\rangle,\langle 1,1,0\rangle]\cap[\langle a,a,1\rangle,x_2]$. Define $a+b=c_2$.

2.8 (Definition of a binary operation $(a,b)\mapsto ab$ on F.) Let $a,b\in F$. If a or b is 0, define $ab=0$. If $a,b\neq 0$, find $\langle c_1,c_2,1\rangle=[\langle b,0,1\rangle,x_2]\cap[\langle 1,a,1\rangle,x_3]$. Define $ab=c_2$.

(Then F is a field, and the natural map $F^3\to\bar{Y}$ induces the desired isomorphism [7, Chap. 20].)

3. *Case* $3\leqslant i<d$. (Each $x\in W_i$ has been labeled using $(F^i)_1$. Each $x\in W_{i+1}$ will be labeled using $(F^{i+1})_1$.)

3.1. Relabel each $y=\langle a_1,\ldots,a_i\rangle\in W_i$ as $y=\langle a_1,\ldots,a_i,0\rangle$.

3.2. Label $x_{i+1}=\langle 0,\ldots,0,1\rangle$.
Pick $u\in[x_{i+1},\langle 1,\ldots,1,0\rangle]-\{x_{i+1},\langle 1,\ldots,1,0\rangle\}$, and label it $\langle 1,\ldots,1,1\rangle$.

3.3. Let $x \in W_{i+1} - (W_i \cup [x_{i+1}, u])$, and determine a label for it as follows.
Find $y = [x_{i+1}, x] \cap W_i$ and $z = [u, x] \cap W_i$.
Let $y = \langle a_1,..., a_i, 0\rangle$ and $z = \langle b_1,..., b_i, 0\rangle$ be labeled by a recursive call. Determine $c, c' \in F$ such that

$$(b_1,..., b_i, 0) = c(1,..., 1, 0) + c'(a_1,..., a_i, 0).$$

(Since $y, z, \langle 1,..., 1, 0\rangle \in [x_{i+1}, u, x] \cap W_i$ and $(F^i)_1 \to W_i$ induces an isomorphism of projective spaces, c and c' exist. They can be found by brute force.)
Let $f = -c'/c$. (Since $y \neq z$, $c \neq 0$.)
Label $x = \langle fa_1,..., fa_i, 1\rangle$.

3.4. Let $x \in [x_{i+1}, u] - \{\langle 1,..., 1, 0\rangle\}$. Find $y = [x_1, x] \cap [\langle 1, 0,..., 0, 1\rangle, \langle 1,..., 1, 0\rangle]$. If $y = \langle a_1, a_2,..., 1\rangle$, label $x = \langle a_2,..., a_2, 1\rangle$. (Note that, in fact, $a_2 = \cdots = a_i = a_1 - 1$.)

Comments. We have now labeled each point in W_{i+1} by a unique element of $(F^{i+1})_1$. The labeling was designed to be consistent with that of W_i. Moreover, the choice of labels for x_{i+1} and u forced all remaining labels.

Since the projective spaces for F^{i+1} and W_{i+1} are isomorphic, there is a unique map $\varphi: F^{i+1} \to W_{i+1}$ agreeing with our map $(F^i)_1 \to W_i$, sending $(0,..., 0, 1) \to x_{i+1}$ and $(1,..., 1) \to u$, and inducing an isomorphism of projective spaces. It is easy to check that φ agrees with the map $(F^{i+1})_1 \to W_{i+1}$ induced by our labeling. Thus, we have indeed defined an isomorphism of projective spaces. In particular, we obtain the desired isomorphism between the projective space for F^d and that of $W_d = V$. ∎

DEFINITION 11.2. Let $V = F^d$. Let $\bar{V}$ be the set of 1-spaces of V. Identify $\bar{V}$ with $\bar{Y}$ via the map in Proposition 11.1. Then G acts on $\bar{V}$.

COROLLARY 11.3. $|V| < n^2$.

Proof. If $\bar{Y} = Y$ then $|V| = 1 + (q-1)|Y| < n^2$ by Theorem 9.1(i). If $\bar{Y} \neq Y$ then $|Y| < 2n$ by Theorem 9.1(i), while $|V| \leqslant |F|^6 |Y| \leqslant |Y|^2/4$ by the table in [10, Sect. 10]. ∎

COROLLARY 11.4. *If $S \subseteq V$, the subspace $\langle S\rangle$ spanned by S can be found in polynomial time.*

Proof. Use Proposition 11.1 to pass to a subset A of $\bar{Y}$, and then use (10.1) to find $[A]$. Finally, use Proposition 11.1 again in order to determine the 1-spaces in $\langle S\rangle$. ∎

12. *Bases and Matrices*

It is easy to find bases of V. The recursive construction is standard: if $v_1,..., v_i$ are linearly independent, find $\langle v_1,..., v_i\rangle$ using Corollary 11.4; if this is not V, pick $v_{i+1} \in V - \langle v_1,..., v_i\rangle$ (compare step 1 in Proposition 11.1).

Fix any ordered basis $v_1,\ldots, v_d$ of V, and consider matrices with respect to this basis.

LEMMA 12.1. *If M is any invertible $d\times d$ matrix with entries in F, then the permutation h of V induced by M can be found in polynomial time.*

Proof. Recall (Corollary 11.3) that $|V|<n^2$. Thus, we can take each $\sum a_i v_i \in V$ and identify its image under h. ∎

LEMMA 12.2. *If $g\in G$, in polynomial time a matrix M can be found inducing g on $\bar{V}$.*

Proof. Fix i, and consider $\langle v_i\rangle^g$. This has the form $\langle \sum_j a_{ij}v_j\rangle$ for some scalars a_{ij}. Since $|V|<n^2$, we can run through all vectors to find such scalars (which are unique up to a common scalar factor).

Now for each of the $|V|$ choices of scalars $c_1,\ldots, c_d$, form the matrix $M=(c_i a_{ij})$. By Lemma 12.1, each such M induces a permutation of $\bar{V}$. Test each to see if this permutation coincides with g. ∎

PROPOSITION 12.3. *There is a uniquely determined group $G^*=(G^*)'\leqslant SL(V)$ inducing G on $\bar{V}$. This group can be found in polynomial time.*

Proof. The first statement is clear. Let $G=\langle \Gamma\rangle$. For each $g\in\Gamma$ let M_g be a matrix produced by Lemma 12.2. Let g^* be the corresponding permutation of V (Lemma 12.1), so $g^*\in GL(V)$. Let

$$G^*=\langle g^* \mid g\in\Gamma\rangle'\leqslant \mathrm{Sym}(V).$$

(Use (A.6) to find the indicated commutator group.) Then G^* has the desired properties (since G is simple). ∎

LEMMA 12.4. *If $g^*\in G^*$, a matrix can be found inducing g^* on V.*

Proof. Find $v_i^{g^*}=\sum_j a_{ij}v_j$. ∎

LEMMA 12.5. *If M is as in Lemma* 12.1, *with corresponding permutation h, then in polynomial time it can be determined whether or not $h\in G^*$ (and hence, whether or not h induces an element of G).*

Proof. Since $h\in\mathrm{Sym}(V)$, (A.2) applies. ∎

COROLLARY 12.6. *If $G=\langle\Gamma\rangle$ then a subset Γ^* of G^* can be found in polynomial time such that $|\Gamma^*|=|\Gamma|$ and Γ^* acts on $\bar{V}$ exactly as Γ does.*

Proof. If $g\in\Gamma$, repeat the proof of Lemma 12.2, using Lemma 12.5 to find M such that the corresponding permutation g^* of V is in G^*. Let $\Gamma^*=\{g \mid g\in\Gamma\}$. ∎

LEMMA 12.7. *If $t\in\mathrm{Sym}(\bar{V})$ is induced by a semilinear transformation of V, then such a transformation can be found in polynomial time.*

Proof. As in Lemma 12.2, write $\langle v_i \rangle^t = \langle \sum_j a_{ij} v_j \rangle$. Let $c_1, \ldots, c_d$ be scalars in F, and let $\theta \in \mathrm{Aut}(F)$. Define t^* by letting $t^*: \sum_i b_i v_i \mapsto \sum_i b_i^\theta c_i \sum_j a_{ij} v_j$. Then t^* permutes the 1-spaces of V. Test each t^* until one is found agreeing with t on $\bar{V}$. (Note that $\mathrm{Aut}(F)$ merely consists of the mappings $a \to a^{p^i}$ for $a \in F$, where $0 \leqslant p^i < q$.) ∎

13. *Construction of the Forms*

In this section we will construct the form on V required in Theorem 9.3(iii). (For background, see [4 and 10, especially Sect. 9].)

1. Let G^* be as in (12.3).
   Let y_1, y_2, z_1, z_2 be as in (10.4).
   Let $y_1 = \langle e_1 \rangle$, $z_1 = \langle f_1 \rangle$, where $e_1, f_1 \in V$.
   Find $\langle e_1, e_2 \rangle$ using Corollary 11.4.
2. Define the form B on $\langle e_1, f_1 \rangle$ by

$$B(e_1, e_1) = B(f_1, f_1) = 0, \qquad B(e_1, f_1) = 1,$$

and $B(f_1, e_1) = 1$ unless G is symplectic, in which case $B(f_1, e_1) = -1$. Now extend by F-linearity to all of $\langle e_1, f_1 \rangle$.

3. Pick $e_2 \in y_2, f_2 \in z_2$, such that the ordered pair (e_2, f_2) lies in $(e_1, f_1)^{G^*}$. Then extend the form to $V' = \langle e_1, e_2, f_1, f_2 \rangle$ by requiring that all inner products be 0 except that $B(e_2, f_2) = B(e_1, f_1)$ and $B(f_2, e_2) = B(f_1, e_1)$.

4. Now let $u, v \in V$. Define $B(u, v) = B(u', v')$ when $(u', v') \in (u, v)^{G^*}$ for some $u', v' \in V'$.

LEMMA 13.1. *B is a bilinear or hermitian form on V preserved by G^* (and constructed in polynomial time).*

Proof. There is a bilinear or hermitian form B' on V preserved by G^* and uniquely determined up to a scalar factor. We may assume that B' coincides with B on $\langle e_1, f_1 \rangle$. Then preservation by G^* implies that $B' = B$, since V' contains a representative of each orbit of G^* on $V \times V$. ∎

The preceding lemma settles all but the case of orthogonal groups in characteristic 2, where a quadratic form is also needed.

LEMMA 13.2. *If G^* is $\Omega^{\pm}(d, q)$, the corresponding quadratic form can be obtained in polynomial time.*

Proof. Define $Q(ae_1 + bf_1) = ab$ for $a, b \in F$. If $v \in V$, define $Q(v) = Q(v')$, where $v' \in \langle e_1, f_1 \rangle \cap v^{G^*}$. As in Lemma 13.1, this defines the required quadratic form. ∎

COROLLARY 13.3. *If $v \in V$ and $\langle v \rangle \in Y$ then $B(v, v) = 0$ (and, moreover, $Q(v) = 0$ in Lemma* 13.2). ∎

LEMMA 13.4. *If $S \subseteq V$ then $S^\perp = \{v \in V \mid B(v, S) = 0\}$ can be found in polynomial time.*

Proof. Use Proposition 11.1 to pass to a subset A of $\bar{Y}$, and then use (10.3) to find A^*. Finally, use Proposition 11.1 in order to determine the 1-spaces in $S^\perp$. ∎

Of course, there is a direct recursive proof for Lemma 13.4.

Notation. Throughout the remainder of this paper, we will write $G = \mathrm{PSL}(d, q)$, $\mathrm{PSp}(2m, q)$, etc., instead of $G \cong \mathrm{PSL}(d, q)$, $\mathrm{PSp}(2m, q)$, etc. For, at this point G is no longer an abstract group: we have at our disposal "the" vector space involved in its definition.

DEFINITION 13.5. For V in Theorem 9.3(i), a *standard basis* is defined as follows:

(i) if $G = \mathrm{PSL}(d, q)$, any basis of V is standard; and

(ii) if $G \neq \mathrm{PSL}(d, q)$, a standard basis has the form

$$e_1, \ldots, e_m, \qquad f_1, \ldots, f_m, \qquad u_1, \ldots, u_s$$

where, for $1 \leqslant i, j \leqslant m$, $\langle e_i \rangle, \langle f_i \rangle \in Y$ (i.e., e_i and f_i are isotropic or singular), $B(e_i, e_j) = B(f_i, f_j) = 0$, $B(e_i, f_j) = \delta_{ij}$, and $\langle e_1, \ldots, e_m, f_1, \ldots, f_m \rangle^\perp$ is the s-space $\langle u_1, \ldots, u_s \rangle$ (with $s = 0$, 1, or 2) and contains no member of Y. (Compare [10, (9.1)].)

DEFINITION 13.6. Let $m = d$ in Definition 13.5(i); otherwise define m as in Definition 13.5(ii).

LEMMA 13.7. *A standard basis can be found in polynomial time.*

Proof. This is obvious in Definition 13.5(i), while in (ii) there is a simple recursive construction using Lemma 13.4 (compare [10, (11.1(i)]). ∎

LEMMA 13.8. *If V has an orthogonal basis, then such a basis $v_1, \ldots, v_d$ with $B(v_i, v_i) = B(v_1, v_1)$ for $i = 1, \ldots, d-1$ can be found in polynomial time.*

Proof. Once again the recursive construction is easy (compare [10, (13.1)]). ∎

Proof of Theorem 9.3. At this point we have already proved Theorem 9.3 (i) in (11.1)–(11.3); (ii) in (12.3); (iii) in (13.1)–(13.2); (iv) in (13.7); (v) in (13.8); (vi) and (vii) in (12.4); and (viii) in (12.5). ∎

LEMMA 13.9. *If $u_1, \ldots, u_d$ and $v_1, \ldots, v_d$ are bases of V, then in polynomial time it can be determined whether or not there exists $g \in G^*$ with $u_i^g = v_i$ for $1 \leqslant i \leqslant d$, and one can be found if there is one.*

Proof. Define $(\sum a_i u_i)^g = \sum a_i v_i$ for $a_i \in F$, and use (A.2) to test whether $g \in G^*$. ∎

PROPOSITION 13.10. *Let h_1 and h_2 be conjugate elements of G^* such that $\langle h_i \rangle$ is irreducible on V. Then $g \in G^*$ with $h_1^g = h_2$ can be found in polynomial time.*

Proof. Let $(u_1,..., u_k)$ be one of the cycles of h_1 on $V-\{0\}$. (Since $\langle h_1\rangle$ is irreducible, $u_1,..., u_d$ is a basis of V. Also, $(u_d)^{h_1}=\sum_1^d a_i u_i$, where $(a_1,..., a_d)$ is the last row of the companion matrix of h_1.)

For each $v_1\in V$ such that there is a k-cycle $(v_1,..., v_k)$ in h_2, use Lemma 13.9 to test whether there is an element $g\in G^*$ such that $u_i^g=v_i$ for $1\leqslant i\leqslant d$; and if there is one, find one. Then $h_1^g=h_2$.

Comments. If g is an element of G^* conjugating h_1 to h_2, define $v_i=u_i^g$ for each i (mod k). Then $(v_i)^{h_2}=(v_i)^{g^{-1}h_1 g}=(u_i)^{h_1 g}=(u_{i+1})^g=v_{i+1}$. Moreover, g is the only linear transformation sending u_i to v_i for $1\leqslant i\leqslant d$.

Conversely, let $(v_1,..., v_k)$ be a k-cycle in h_2 such that $u_i^g=v_i$, $1\leqslant i\leqslant k$, for some $g\in G^*$. Then h_1^g sends $v_1\to v_2\to\cdots\to v_d\to\sum_1^d a_i v_i$. Since h_1^g and h_2 are conjugate, they have the same characteristic polynomial. Thus, $h_1^g=h_2$. ∎

14. *Decompositions of V*

It is easy to find stabilizers of subsets and partitions in S_n. We will need analogous results for G^*: stabilizers of subspaces and of suitable direct sum decompositions of V. In addition we will need to be able to find elements of G^* sending one subspace or decomposition to another one. These results will be used in a manner reminiscent of [10].

Note that $\dim V>4$, since $|G|>n^8$.

Conventions 14.1. Write $V=V_1\perp\cdots\perp V_l$ for subspaces V_i if $V=V_1\oplus\cdots\oplus V_l$ and if, moreover, the V_i are pairwise perpendicular when $G\neq \mathrm{PSL}(d, q)$. If G is $\mathrm{PSL}(d, q)$, the words "isometric" and "isometry" will always mean "isomorphic" and "isomorphism"; all subspaces will be regarded as simultaneously nonsingular, totally isotropic and totally singular. (Recall that usually nonsingular means that $W\cap W^\perp=0$, totally isotropic means that $W\subseteq W^\perp$ for G not orthogonal, and totally singular means that $Q(W)=0$ for G orthogonal.) Standard bases written as in Definition 13.5(ii) should be viewed as any basis when $G=\mathrm{PSL}(d, q)$.

The above convention will allow us to consider all possibilities for G simultaneously—but at the expense of language. The opposite point of view was taken in [10], where the simplest $\mathrm{PSL}(d, q)$ case was handled separately. We refer to [4] for further information concerning G.

It will be convenient to work with a slightly larger group than G^*. Let $G^\#$ be the group of all isometries of V (where $G^\#=\mathrm{GL}(d, q)$ if G is $\mathrm{PSL}(d, q)$).

LEMMA 14.2. (i) $G^*\trianglelefteq G^\#$.

(ii) *If G is not orthogonal then $G^\#=\langle G^*, t\rangle$ for a suitable diagonalizable transformation t.*

(iii) *If G is orthogonal then $G^\#/G^*$ is isomorphic to the direct product of $2(2, q-1)$ groups of order 2.*

(iv) *$G^\#$ can be found in polynomial time.*

Proof. For (i) see [4]: $G^* = (G^\#)'$. If $G = \mathrm{PSp}(2m, q)$ then $G^\# = G^*$. If $G = \mathrm{PSL}(d, q)$ or $\mathrm{PSU}(d, q)$, let $v_1, \ldots, v_d$ be an orthonormal basis (Lemma 13.8) and let $t = \mathrm{diag}(a, 1, \ldots, 1)$, where $|a|$ is as large as possible and $a\bar{a} = 1$ in the unitary case. Then $t \in G^\#$ and $G^\# = \langle G^*, t \rangle$. (For, if $g \in G^\#$ then $\det g \in \langle \det t \rangle$.)

When G is orthogonal we will need some further notation both here and later in this section. Define Q and B as in Lemmas 13.1, 13.2. Whenever $u \in V$ and $Q(u) \neq 0$, let $r_u: v \mapsto v - B(u, v)\, u/Q(u)$ (this is a reflection if q is odd and a transvection if q is even). Then $\det r_u = -1$, and $G^\# = \langle r_u \mid Q(u) \neq 0 \rangle$ [4, pp. 51, 65]. Moreover, $G^* = \langle r_u r_w \mid Q(u) = Q(w) = 1 \rangle$. Thus, (iii) holds, and (iv) is now obvious. ∎

PROPOSITION 14.3. *Let W be a subspace of V that is either nonsingular or totally isotropic or totally singular. Then G^*_W and $G^\#_W$ can be found in polynomial time.*

Proof. Since $G^*_W = G^* \cap G^\#_W$, by (A.7) we only need to consider $G^\#_W$. By (A.1), WLOG $\dim W > 1$.

First suppose that W is totally isotropic or totally singular. Use Lemma 13.4 to find a standard basis (13.5) $e_1, \ldots, e_m, f_1, \ldots, f_m, u_1, \ldots, u_s$ of V such that $e_1, \ldots, e_r$ is a basis of W (recall (14.1)). We will use this to construct a group $H \leqslant G^\#$ such that $H^W = (G^\#_W)^W$; and then we will have found $G^\#_W = \langle G^\#_{(W)}, H \rangle$ using (A.1). Note that we need to have $H^W = GL(W)$, except when $\dim W = m$, q is odd, $G = P\Omega^+(2m, q)$, or $P\Omega(2m+1, q)$, and $|GL(W): H^W| = 2$. This suggests the following construction.

Let Δ be the set of all elements of $G^\#_W$ whose matrix A with respect to our basis behaves in one of the following ways: (i) $A - I$ has at most two nonzero entries, or (ii) $A = \left(\begin{smallmatrix} D & 0 \\ 0 & U \end{smallmatrix}\right)$ for a $2m \times 2m$ diagonal matrix D and an $s \times s$ matrix U. (Note that $|\Delta| \leqslant |F|^2 d^2 + |V| \cdot |F|^s$. Membership in $G^\#$ is tested using (A.2).) The matrices (i) already generate an $SL(W)$ on W, while those in (ii) yield $GL(W)$ or its required subgroup of index 2. Thus, $H = \langle \Delta \rangle$ works. ∎

LEMMA 14.4. *Let U and W be subspaces of V that are nonsingular or totally isotropic or totally singular. Then in polynomial time it is possible to*

(i) *decide whether or not $W \in U^{G^*}$, and*

(ii) *find $g \in G^*$ with $W = U^g$, if $W \in U^{G^*}$.*

Proof. WLOG $\dim U = \dim W > 2$ by (A.3).

Pick a subspace U' of U satisfying one of the conditions: (1) if U is totally isotropic or totally singular then U' is a hyperplane of U, or (2) if U is nonsingular then U' is a maximal nonsingular subspace of U. (Then $\dim U' \geqslant \dim U - 2$.)

In case (1), WLOG W is totally isotropic or totally singular. Let W' be any hyperplane of W. Then $\dim W' = \dim W$ implies that $W' \in U'^{G^*}$ (cf. [4]). Recursively find $f \in G^*$ such that $W'^f = U'$. Find $H = G^*_{U'}$ using Proposition 14.3. Let $u \in U - U'$, and use (A.3) to find u^H. If $u^H \cap W^f \neq \varnothing$, let $u^h \in W^f$, $h \in H$; then $U^{hf^{-1}} = W$. If $u^H \cap W^f = \varnothing$ then $W \notin U^{G^*}$. (N.B.—Only when $G = P\Omega^+(2m, q)$ and $\dim U = m$ can it happen that $W \notin U^{G^*}$ for some W isometric to U.)

In case (2), WLOG $G \neq \mathrm{PSL}(d, q)$. Find a sequence W' of W such that W' is nonsingular and $W'^{\perp} \cap W \in (U'^{\perp} \cap U)^{G^*}$; if no such W' exists then $W \notin U^{G^*}$. (Since $U'^{\perp} \cap U$ has dimension 1 or 2, its G^*-orbit has size $< |V|^2$. Test each member W_0 of this orbit to see if $W_0 \subset W$, and if it is let $W' = W_0^{\perp} \cap W$.)

WLOG W' exists. Recursively, WLOG $U' = W'^f$ for some $f \in G^*$. (For, G_U^{*U} is transitive on the set of members of U'^{G^*} lying in U. Thus, if $W' \notin U'^{G^*}$ then $W \notin U^G$.)

Use Proposition 14.3 to find $H = G_{U'}^*$. Use (A.3) to find $h \in H$ with $(W'^{\perp} \cap W)^f = (U'^{\perp} \cap U)^h$; then $U^{hf^{-1}} = W$. If no such h exists then $W \notin U^{G^*}$. (For, G_U^{*U} is transitive on the set of members of $(U'^{\perp} \cap U)^{G^*}$ lying in U.) ∎

We note that there is an alternative proof of Lemma 14.4 using standard bases.

PROPOSITION 14.5. *Let $V = V_1 \perp \cdots \perp V_l$ with each V_i nonsingular, and let $\Omega = \{V_1, \ldots, V_l\}$. Then*

(i) *$H = G_\Omega^*$ can be found in polynomial time; and*

(ii) *if $\Sigma = V_1^{G^*} \cap \Omega$ then H induces at least $\mathrm{Alt}(\Sigma)$ on Σ, and is transitive on Σ.*

Proof. Obtain $H_i \leqslant GL(V)$ by starting with $(G_{V_i}^*)^{V_i}$ (see Lemma 14.4) and extending this to V by letting $H_i = 1$ on $\langle V_j \mid j \neq i \rangle$. Then $H^\# = \langle H_i \mid 1 \leqslant i \leqslant l \rangle \leqslant G^\#$. Use (A.7) to find $H^\# \cap G^*$; this is the kernel of $H \to H^\Omega$. Thus, we have reduced (i) to the problem of determining the subgroup H^Ω of Ω.

Clearly, H fixes Σ. Thus, we are led to consider (i) and (ii) simultaneously. WLOG $|\Sigma| > 1$ and $V_2 \in \Sigma$. Use Lemma 14.4 to find $g \in G^*$ with $V_1^g = V_2$. Define a linear transformation t on V by letting $t = g$ on V_1, $t = -g^{-1}$ on V_2, and $t = 1$ on $\langle V_j \mid j > 2 \rangle$. (Then $\det t = 1$.) If G is $\mathrm{PSL}(d, q)$, $\mathrm{PSp}(2m, q)$, or $\mathrm{PSU}(d, q)$, then $t \in G^*$, t^Ω is a transposition, and hence $H^\Sigma = \mathrm{Sym}(\Sigma)$.

Now let G be orthogonal, and define r_u as in the proof of Lemma 14.2.

If q is even, let $u \in V_1$ with $Q(u) = 0$. Then either t or tr_u is in G^* (Lemma 14.2(iii)), and this can be tested using (A.2). Thus, t or tr_u is in G^*, and $H^\Sigma = \mathrm{Sym}(\Sigma)$ again.

Now suppose that q is odd. If they exist, find $u, w \in \bigcup \{V_i \mid 1 \leqslant i \leqslant l\}$ with $Q(u)\,Q(w)$ a nonsquare (by checking each pair u, w in the union). Then $G^\# \cap SL(d, q) = G^* \langle r_u r_v \rangle$ (Lemma 14.2(iii)). Thus, either t or $tr_u r_w$ is in G^*, and $\mathrm{Sym}(\Sigma)$ is again induced.

Finally, assume that there is no such pair u, w. This means that each V_i is a 1-space, and can be written $\langle v_i \rangle$ with $Q(v_i) = Q(v_1)$ for all i. In this situation we can find $G^*_{\{V_1, V_2\} V_3 \cdots V_l}$ using (A.1), in order to test for transpositions. On the other hand, $l = \dim V > 2$. Then $r_{v_1 + v_2} r_{v_2 + v_3}$ induces the 3-cycle (V_1, V_3, V_2) on Ω, and lies in G^* since $Q(v_1 + v_2) = Q(v_2 + v_3)$. Thus, H^Ω contains all 3-cycles and hence contains A_l. ∎

LEMMA 14.6. *If $V = V_1 \perp \cdots \perp V_l = W_1 \perp \cdots \perp W_l$ for nonsingular subspaces V_i*

and W_i, and if $\{W_1,..., W_l\} \in \{V_1,..., V_l\}^{G^*}$, then in polynomial time $g \in G^*$ can be found such that $\{W_1,..., W_l\} = \{V_1,..., V_l\}^g$.

Proof. Use Lemma 14.4 to renumber the W_i and then to find $h_i \in G^*$ sending V_i to W_i for each i. Define $h \in GL(V)$ by letting $h = h_i$ on V_i. Then h is an isometry of V. As in Proposition 14.5, we will modify h in order to obtain an element of G^*.

If G is symplectic then $h \in G^\# = G^*$.

If G is unitary, or if G is orthogonal of odd characteristic, find orthogonal bases of V_i for each i, and take their union (compare Lemma 13.8). Write down each diagonal matrix $\mathrm{diag}(a, 1,..., 1)$ with $a \in F$, let f be the corresponding linear transformation with respect to our basis, and test whether fh is in G^* (when G is unitary) or in $G^*\langle r_u r_w\rangle$ (when G is orthogonal and $Q(u)\,Q(w)$ is a nonsquare); compare Lemma 12.5. Eventually, this produces an element of G^* or $G^*\langle r_u r_w\rangle$. (All we are doing is finding an isometry of determinant 1 taking $\{V_1,..., V_l\}$ to $\{W_1,..., W_l\}$.)

This takes care of the unitary case. Suppose that G is orthogonal. If q is even and $u \in V_1$ satisfies $Q(u) \neq 0$, then either h or $r_u h$ is in G^* (Lemma 14.2(iii)), and behaves as desired.

Suppose that q is odd. If possible, find $u, w \in \bigcup \{V_i \mid 1 \leqslant i \leqslant l\}$ with $Q(u)\,Q(w)$ a nonsquare. Then either h or $r_u r_w h$ behaves as desired.

This leaves the possibility that $V_i = \langle v_i\rangle$ and $Q(v_i) = Q(v_1)$ for all i. Let $f = r_{v_1} r_{v_1+v_2}$. Then either h or fh behaves as desired.

(For, let $g \in G^*$ send $\{V_1,..., V_l\}$ to $\{W_1,..., W_l\}$. By Lemma 14.6(ii), we can modify g so as to have hg^{-1} inducing 1 or a transposition on $\{V_1,..., V_l\}$. Then $g' = hg^{-1}$ or fhg^{-1} induces 1 on $\{V_1,..., V_l\}$, and $\det g' = 1$. Now g' arises from a diagonal matrix with respect to the orthogonal basis $v_1,..., v_l$, and hence is the product of an even number of G^*-conjugate reflections r_{v_i}. Thus, $g' \in G^*$. Since $g \in G^*$, it follows that h or fh is in G^* and sends $\{V_1,..., V_l\}$ to $\{W_1,..., W_l\}$.) ∎

LEMMA 14.7. *Let $P \leqslant G^*$ with $(q, |P|) = 1$. Then the following can be found in polynomial time:*

(i) *all minimal P-invariant subspaces of V;*

(ii) *all minimal nonsingular P-invariant subspaces; and*

(iii) *minimal nonsingular P-invariant subspaces $V_1,..., V_l$ such that $V = V_1 \perp \cdots \perp V_l$.*

Proof. (i) For each $v \in V - \{0\}$ find $\langle v^P\rangle$ using (A.3) and Corollary 11.4. Then sort these subsets of V.

(ii) WLOG $G \neq \mathrm{PSL}(d, q)$. Whenever $u, v \in V - \{0\}$ find $W = \langle u^P, v^P\rangle$. For each such subspace W, test whether W is nonsingular (use Lemma 13.4 to find $W^\perp$, and then check whether $W \cap W^\perp = 0$). Then sort all of the nonsingular subspaces found in this manner. (In order to see that this produces all minimal nonsingular P-invariant subspaces, consider such a subspace U. We may assume that U is P-reducible. By Maschke's theorem [7, p. 253], $U = U_1 \oplus \cdots \oplus U_k$ for $k \geqslant 2$ sub-

spaces U_i already found in (i). WLOG $U_2 \not\subseteq U_1^\perp$ since U is nonsingular. Then $U_1 \cap U_2^\perp$ is P-invariant, so that $U_1 \cap U_2^\perp = 0$ and $U_1 \oplus U_2$ is nonsingular. Thus, $U = U_1 \oplus U_2$ by minimality.)

(iii) Start with any V_1. If $V_1,\ldots, V_i$ have been found and $V \neq \langle V_1,\ldots, V_i\rangle = V_1 \perp \cdots \perp V_i$, let V_{i+1} be any minimal nonsingular P-invariant subspace of $\langle V_1,\ldots, V_i\rangle^\perp$ (or any minimal P-invariant subspace not contained in $\langle V_1,\ldots, V_i\rangle$ if G is PSL(d, q)). Then $\langle V_1,\ldots, V_{i+1}\rangle = V_1 \perp \cdots \perp V_{i+1}$. ∎

Finally, we indicate why (14.5)–(14.7) will be very relevant to the proof of the Main Theorem. Namely, we will describe how Sylow subgroups arise from such decompositions (without any restrictions on dim V). For more information (and proofs), we refer to [16; 3; and 10, Sects. 8, 9].

PROPOSITION 14.8. *Let p be a prime dividing $|G|$ but not q. Then a Sylow p-subgroup P of $G^\#$ preserves a decomposition $V = V_1 \perp \cdots \perp V_l$ having the following properties*:

(a) *Each V_i is a minimal nonsingular P_{V_i}-invariant subspace.*

(b) *If $p \neq 2$ then $(P_{V_i})^{V_i}$ is cyclic.*

(c) *If $p \neq 2$ let E be a nonsingular subspace of V minimal with respect to the condition $p \mid |G_E^{*E}|$; if $p = 2$, let E be a nonsingular 2-space (such that, if G is orthogonal, a Sylow 2-subgroup of G_E^{*E} is as large as possible). Then $V' = \langle V_i \mid V_i$ is not isometric to $E\rangle$ has no subspace isometric to E.*

(d) *$P^{V'} = 1$, except perhaps if $p = 2$ and* dim $V' \leqslant 2$. *Moreover,* dim $V' = 2 = p$ *only if G is orthogonal.*

(e) *If P is irreducible then it is transitive on $\{V_1,\ldots, V_l\}$ and $(P_{V_i})^{V_i}$ is irreducible.*

15. *Irreducible Cyclic Groups*

This section is a digression from the proof of the main theorem. We will prove the following results.

PROPOSITION 15.1. *In polynomial time an element $h \in GL(V)$ can be found acting transitively on $V - \{0\}$.*

PROPOSITION 15.2. *If $G^* = \mathrm{Sp}(2m, q)$, $\Omega^-(2m, q)$, or $\mathrm{SU}(d, q)$, then an element of $GL(V)$ can be found in polynomial time that* (i) *preserves the form on V, and* (ii) *has order $q^m + 1$ or $q^d + 1$, respectively.*

Remark. Both of these results can be proved as in [10, (8.6), (11.4)]. In fact, if the cyclic groups in Propositions 15.1 and 15.2 are intersected with G^* then [10, (8.6), (11.4)] contain the above propositions as very special cases. Our goal here is to give much more direct and elementary proofs.

Proof of Proposition 15.1. Find a basis $v_1,\dots, v_d$ of V. (Any basis will do, since h has nothing to do with any form on V.)

For each vector $(a_1,\dots, a_d)\in F^d$, $a_1\neq 0$, find the permutation h induced on V by the linear transformation defined by $v_1\to v_2\to\cdots\to v_d\to\sum a_iv_i$, using Lemma 12.1.

Test each h until one is found satisfying $|h|=|V|-1$.

(If, say, $F=GF(q)$, then a generator of $GF(q^d)^*$ induces a $GF(q)$-linear transformation of order q^d-1 on $GF(q^d)$. Its companion matrix has the desired form for some $(a_1,\dots, a_d)$.) ∎

Proof of Proposition 15.2. The proof falls into two parts: construct a form on a new vector space E, and transfer the form to V.

1. Define k by $|V|=q^{2k}$. (Then $k=m$ if $G^*=\mathrm{Sp}(2m,q)$ or $\Omega^-(2m,q)$, while $k=d$ otherwise.)

2. Find h as in Proposition 15.1. Let $E=\langle h\rangle\cup\{0\}$. (Then E is a ring of linear transformations of V isomorphic to $GF(q^{2k})$.)

3. For $e\in E$ define $\bar e=e^{q^k}$ and $\mathrm{Tr}(e)=\sum_{i=0}^{d-1}e^{|F|^i}$. (Then "$^-$" is the involutory automorphism of E, while Tr is the trace map $E\to F$. Note that all calculations can be made in polynomial time.)

4. Define the following functions B', H', Q' (where $u, v\in E$):

$$B'(u,v)=\mathrm{Tr}(u\bar v-\bar u v),$$
$$H'(u,v)=\mathrm{Tr}(u\bar v)\qquad\text{when}\quad F=GF(q^2),$$
$$Q'(u)=\mathrm{Tr}(u\bar u).$$

Comments. B' is an alternating $GF(q)$-bilinear form on E, and turns E into a symplectic geometry.

H' is a hermitian form over $GF(q^2)$, and turns E into a unitary geometry.

Q' is a quadratic form over $GF(q)$, and turns E into an orthogonal geometry. The corresponding bilinear form is $\mathrm{Tr}(u\bar v+\bar u v)$. (See, e.g., [16 or 8].)

5. Define $t: E\to V$ in one of the following ways.

5.1. *Symplectic case.* Find a standard basis $e_1',\dots, e_m', f_1',\dots, f_m'$ of E (compare Lemma 13.7).
Then extend $e_i'\to e_i$, $f_i'\to f_i$ to a linear transformation t.

5.2. *Unitary case.* Find orthonormal bases $u_1,\dots, u_d$ and $u_1',\dots, u_d'$ of V and E, respectively, and let $t: u_i'\mapsto u_i$ for each i.

5.3. *Orthogonal case.* Find standard bases $e_1,\dots, e_m, f_1,\dots, f_m, u_1, u_2$ of V and $e_1',\dots, e_m', f_1',\dots, f_1',\dots, f_m', u_1', u_2'$ of E. (By [16 or 8] Q' turns E into a space isometric to V.) For each basis u_1'', u_2'' of $\langle u_1', u_2'\rangle$ test to see whether $t: e_i'\mapsto e_i$, $f_i'\mapsto f_i$, $u_i''\mapsto u_i$ extends to an isometry $E\to V$. Let t be any isometry obtained in this manner.

6. Let $g \in \langle h \rangle$ have order q^k+1. Define $g_1 \in GL(E)$ by $u \mapsto ug$. (Then $\bar{g} = g^{-1}$, so that g_1 preserves B', H', and Q'.)

Then $g_2 = t^{-1} g_1 t \in GL(V)$ preserves the form on V in Theorem 9.3(iii). Also, $|g_2| = q^k + 1$. ∎

PART IV. MAIN THEOREM

16. *Alternating Groups*

In Sections 16–19 we will study p-subgroups of alternating and classical groups in order to prove Theorems 3.4, 3.8, and 3.9. This section concerns the simplest case, that of alternating groups. More precisely, we will deal with the following situation.

HYPOTHESIS 16.1. (i) $G \cong A_m$ *for some* m.

(ii) $G \leqslant S_n$ *and* $|G| > n^8$.

(iii) p *is a prime dividing* $|G|$.

(iv) *In Lemma* 16.2, *there is a* SYLCONJ *procedure available whenever the input group has order a proper divisor of* $|G|$.

(v) *In Lemma* 16.4, *there is a* SYLEMBED *procedure available whenever the input group has order a proper divisor of* $|G|$.

Remarks. The recursion implicit in (iv) and (v) can easily be avoided. However, it produces extremely short procedures, which also can be regarded as previews of those seen later in the classical group case. Also, the alternating group cases of Theorems 3.4, 3.8, and 3.9 could have been presented later, at the same time as the main part of the proofs. We have chosen the present organization in order not to clutter the next three sections.

The arguments closely resemble those of [11, Sect. 4].

Preliminary construction. Use Theorem 9.1 to find a new set Y of size m on which G acts as A_m.

LEMMA 16.2. *If* P_1 *and* P_2 *are Sylow* p*-subgroups of* G, *then* $f \in G$ *with* $P_1^f = P_2$ *can be found in polynomial time.*

Proof. 1. Find the set Π_i of orbits of P_i on Y.

2. Find $h \in G$ with $\Pi_1^h = \Pi_2$. (Since such an h exists by Sylow's theorem, it is easy to find one.)

Then $P_1 \leftarrow P_1^h$. Also, $\Pi \leftarrow \Pi_1$. (Now P_1 and P_2 are contained in the set stabilizer G_Π of Π.)

3. Find G_Π. (This is the intersection of the alternating group G with the direct product of the groups $\mathrm{Sym}(B)$, $B \in \Pi$.)

4. If $|\Pi| > 1$, use recursion (16.1(iv)).

5. WLOG P_i is transitive. Use (A.7) to find $Z(P_i)$.

6. Let $z_i \in Z(P_i)$ have order p. (Then z_i is the product of n/p pairwise disjoint p-cycles.) Find $h \in G$ such that $z_1^h = z_2$, and $P_1 \leftarrow P_1^h$. (It is easy to find such an h.)

7. Apply recursion (16.1(iv)) to $\langle P_1, P_2 \rangle$. (Since $z_1 = z_2 \in Z(P_1) \cap Z(P_2)$, $\langle P_1, P_2 \rangle \neq G$.) ∎

LEMMA 16.3. *Let $G \lhd G(t) \leqslant S_n$ with $|t| = p$. Then an element of order p in $C_G(t)$ can be found in polynomial time.*

Proof. By Theorem 9.1(v) or [17, p. 42], t acts on $\{G_y \mid y \in Y\}$. Thus, by identifying Y with this conjugacy class, we may assume that t acts on Y.

If $t^Y = 1$ then t centralizes G, and any element of G of order p lies in $C_G(t)$. W.l.o.g. $t^Y \neq 1$. If $(y_1, \ldots, y_p)$ is any p-cycle of t then it centralizes t and lies in G unless $p = 2$.

Let $p = 2$. If t is a transposition, use the product of two transpositions in $C_G(t)$. If t is not a transposition it has two 2-cycles, whose product lies in $C_G(t)$. ∎

LEMMA 16.4. *Let P be a p-subgroup of G that is not Sylow. Then a p-subgroup of G properly containing P can be found in polynomial time.*

Proof. 1. *Case* P intransitive. Find the set Π of orbits of P on Y. Find the set stabilizer G_Π.

Apply recursion to G_Π (16.1(v)). (Clearly, $N_G(P) \leqslant G_\Pi$.)

2. *Case* P transitive.

Find $Z(P)$. (Use (A.8). Note that $|Z(P)| \mid n$.)

Test each $z \in Z(P) - \{1\}$ as follows. Let Π be the set of orbits of $\langle z \rangle$. Find G_Π. If P is not Sylow in G_Π, use recursion (16.1(v)). (For some z this will be possible, namely, when $z \in P \cap Z(Q)$ for a Sylow p-subgroup Q of $N_G(P)$.) ∎

17. *Procedure SYLCONJSIMPLE*

In this section we will present a procedure called SYLCONJSIMPLE behaving as required in Theorem 3.4.

Preliminary reductions. WLOG $|G| > n^8$ (as otherwise brute force works). If G is alternating, use Lemma 16.2.

WLOG G is a classical group. Use Theorem 9.3 in order to find a vector space V and a group G^* of linear transformations. Let $d = \dim V$ and let q be as in the "name" of G (cf. (10.2)). Since $|G| > n^8$, $d > 2$. Define m as in (13.6).

Since $G^*/Z(G^*) \cong G$, our problem reduces to the following one.

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

Convention 17.1. In the course of dealing with (*) we will occasionally use recursion: SYLCONJ will be called for pairs of Sylow p-subgroups P_3, P_4 of a group $H \leqslant G^*$, and a conjugating element $h \in H$ will then be obtained. Any such call amounts to the following: we will need to know that $HZ^*/Z^* < G$, where

$Z^* = Z(G^*)$; and then $h \in H$ will be any element of H projecting (mod Z^*) onto an element conjugating P_3Z^*/Z^* to P_4Z^*/Z^*.

We also note that we will be using Conventions 14.1 as well.

We are now ready to complete the proof of Theorem 3.4 via (*).

1. *Case* P_i reducible.

   1.1. Find a minimal P_1-invariant subspace W_1, and then a P_2-invariant subspace $W_2 \in W_1^{G^*}$, using Lemmas 14.7 and 14.4. (The existence of W_2 follows from Sylow's theorem.)

   1.2. Find $g \in G^*$ with $W_1^g = W_2$, using Lemma 14.4. Let $H = \langle P_1^g, P_2 \rangle$. (Then $HZ^*/Z^* \neq G$.) Now apply recursion (17.1).

2. WLOG P_i is irreducible. (In particular, $p \nmid q$. Also, $|P_i| = O(n^5)$. For, if $V \rtimes P$ is represented on the cosets of P_i, the result is a solvable primitive group of degree $|V|$. Then $|VP_i| = O(|V|^{3.5})$ by [14], while $|V| < n^2$ by Theorem 9.3.)

3. Whenever $h \in P_1 - Z^*$, use Lemma 14.7 to find each minimal nonsingular h-invariant subspace. For each such subspace V_1, and for each nonsingular 1- or 2-space V_1 if $p = 2$, test whether $V = V_1 \perp \cdots \perp V_l$ with $(V_1)^{P_1} = \{V_1, \ldots, V_l\}$. (Recall (14.1).)

Let $\{V_1, \ldots, V_l\}$ be such a family of subspaces. (One exists by Proposition 14.8, since P_1 is irreducible. Since $|P_1| = O(n^5)$ each $h \in P_1 - Z^*$ can be tested using Corollary 11.4, and Lemmas 13.4, 14.7; and some h produces V_1 if $p \neq 2$, by Proposition 14.8(iii).)

4. Repeat step 3 for P_2 in place of P_1 in order to decompose V as $V = W_1 \perp \cdots \perp W_l$ with P_2 transitive on $\{W_1, \ldots, W_l\}$ and $\{W_1, \ldots, W_l\} \in \{V_1, \ldots, V_l\}^{G^*}$; and find $g \in G^*$ with $\{W_1, \ldots, W_l\} = \{V_1, \ldots, V_l\}^g$ (use Lemma 14.6). (Once again, existence follows from Sylow's theorem.)

5. Let $H = \langle P_1^g, P_2 \rangle$. (This is contained in $G^*_{\{W_1, \ldots, W_l\}}$.)
   If $l > 1$ apply recursion (17.1) to HZ^*/Z^*.

6. WLOG $l = 1$. (Since $d > 2$, $p \neq 2$ and P_i is cyclic by Proposition 14.8.)
   Let $P_1 = \langle h_1 \rangle$. (Then h_1 is conjugate to an element of P_2.)
   For each h_2 such that $P_2 = \langle h_2 \rangle$, use the algorithm in Proposition 13.10. Eventually, Proposition 13.10 produces an $f \in G^*$ such that $h_1^f = h_2$. Then $P_1^f = P_2$. ∎

18. *Procedure SYLEMBED1SIMPLE*

In this section we will present a procedure called SYLEMBED1SIMPLE behaving as required in Theorem 3.8.

First of all, we will have to alter the notation in Section 3. Our input will be $G \lhd G\langle t \rangle \leqslant S_n$ with $|t| = p$, where $p \mid |G|$, while the desired output will be an element of order p in $C_G(t)$.

Preliminary reductions. WLOG $|G| > n^8$ (as otherwise brute force works). Use

Theorem 9.1. If G is alternating, use Lemma 16.3. WLOG G is a classical group. Use Theorem 9.3 to find V and G^*.

Remark 18.1. We cannot work only with V, since t may not act on V, or even on the set $\bar{V}$ of 1-spaces of V. However, by Theorem 9.1(v) (or [2 or 4]), this can happen if and only if $G = \mathrm{PSL}(d, q)$, in which case t acts on $\bar{V} \cup \bar{V}^*$, where V^* is the set of hyperplanes of V.

We will assume that a SYLEMBED1 subprocedure is available for groups of order a proper divisor of $|G\langle t\rangle|$.

We are now ready to complete the proof of Theorem 3.8.

1. Find $C_{G\langle t\rangle}(G)$ using (A.8).

If $C_{G\langle t\rangle}(G) \neq 1$, then $G\langle t\rangle = G \times \langle u\rangle$ for some u of order p. (Here, $\langle u\rangle = C_{G\langle t\rangle}(G)$.) If $t \in \langle u\rangle$, any element of G of order p (found using (A.11)) is in $C_G(t)$. If $t \notin \langle u\rangle$, use (A.2) to find i with $tu^i \in G$, and then tu^i is an element of order p in $C_G(t)$.

2. WLOG $C_{G\langle t\rangle}(G) = 1$.

Let $G\langle t\rangle$ act on $\bar{V}$ or $\bar{V} \cup \bar{V}^*$, where $\bar{V}^*$ is as in Remark 18.1. (Since $|\bar{V}^*| = |\bar{V}|$, this action can be determined.)

3. If t does not act on $\bar{V}$, let $x \in \bar{V}$, let $y = x^t$, find G_{xy} (using (A.1)), and recursively apply SYLEMBED1 to $G_{xy}\langle t\rangle$. (Since t interchanges $\bar{V}$ and $\bar{V}^*$, $p = 2$ and t interchanges x and y. Thus, $G_{xy}\langle t\rangle$ is a proper subgroup of G.)

4. WLOG $G\langle t\rangle$ acts on $\bar{V}$.

Use Lemma 12.7 to find a semilinear transformation t^* of V that agrees with t on $\bar{V}$ and is a p-element (cf. [4, Chap. IV]).

5. Find $v \in V$ such that either

(i) $W = \langle v^{\langle t^*\rangle}\rangle \neq V$, or

(ii) $V = W_1 \perp \cdots \perp W_p$, where $\{W_1, \ldots, W_p\} = \langle v\rangle^{\langle t^*\rangle}$.

Then find G^*_W or $G^*_{W_1 \cdots W_p}$ using Proposition 14.3 or (A.1), respectively, and recursively call SYLEMBED1 for $(G_W)\langle t\rangle$ or $(G_{W_1 \cdots W_p})\langle t\rangle$.

Comments. We must show that such a v exists. In view of (i), WLOG $p \neq 2$ since $d > 2$. Let P be a Sylow p-subgroup of G^* normalized by t^*. Then $P\langle t^*\rangle$ preserves a decomposition $V = V_1 \perp \cdots \perp V_l$ as in Proposition 14.8. (This is proved as in [16 or 10, Sect. 8 and (9.4)], using Aut G^* [4, Chap. IV].)

Assume that $l > 1$. Using v in V_i, we see that (i) holds unless $l = 1$ and $\dim V_i = 1$, in which case (ii) holds.

Now assume that $l = 1$. Then $P = \langle h\rangle$ is cyclic by Proposition 14.8(b), and there are no scalars of order p. Thus, $|t^*| = p$ and $P\langle t^*\rangle = P\langle\theta\rangle$ for a field automorphism θ [4, Chap. IV]. Here, θ acts on $\langle h\rangle$ as an automorphism of order p acts on a Sylow p-subgroup of $GF(r^p)^*$ for a suitable $r \equiv 1 \pmod p$. Then $h^\theta = zh$, where $|z| = p$. It is easy to check that $\langle h, \theta\rangle$ has exactly p subgroups of order p other than $\langle z\rangle$, and all are conjugate to $\langle\theta\rangle$. In particular, t^* fixes some nonzero vector and (i) holds for some v. ∎

19. *Procedure SYLEMBEDSIMPLE. Proof of Main Theorem*

In this section we will present a procedure called SYLEMBEDSIMPLE behaving as required in Theorem 3.9. This will complete the proof of the Main Theorem.

Preliminary reductions. Same as in Section 17. This time we need to consider the problem

(*) Given a p-subgroup P of G^* that is not Sylow, find a larger p-subgroup of G^*.

(The larger p-group might project onto the same subgroup of $G \cong G^*/Z(G^*)$ as P does, but that makes no difference since (*) can be repeated.)

Convention 19.1. Recursive calls to SYLEMBED will be made for p-subgroups P of subgroups H of G^*, but only when $HZ^*/Z^* < G$, where $Z^* = Z(G^*)$.

We can now complete the proof of Theorem 3.9 via (*).

1. *Case* P reducible.

1.1. WLOG $P \neq 1$ (by (A.11)).
If $p \mid q$, find a 1-space x fixed by P, find $H = G_x^*$ using (A.1), and use recursion (19.1).
WLOG $p \nmid q$.

1.2. Find a minimal nonsingular P-invariant subspace U and a P-invariant subspace $U^\perp$ such that $V = U \perp U^\perp$ (use Lemma 14.7; recall (14.1)).

1.3. If $U^\perp = 0$, find nontrivial P-invariant subspaces W, W' such that $V = W \oplus W'$. (Use Lemma 14.7(i); W and W' are totally isotropic or totally singular [10, (9.4)].)
Find $H = G_W^*$ using Proposition 14.3, and use recursion (19.1). (By [10, (9.4)], H contains a Sylow p-subgroup of G^*.)

1.4. WLOG $U^\perp \neq 0$. Find $H = G_U^*$ using Proposition 14.3. If P is not Sylow in H, use recursion (19.1).

1.5. WLOG P is Sylow in H.

1.6. Find nonsingular subspaces $V_1, \ldots, V_l$ such that the following all hold:

(i) $V = V_1 \perp \cdots \perp V_l$.

(ii) P permutes the V_j.

(iii) U and $U^\perp$ are sums of some of the V_j.

(iv) Each V_i is a minimal nonsingular P_{V_i}-invariant subspace.

(v) If $p \neq 2$ then $(P_{V_i})^{V_i}$ is cyclic.

(vi) If $p \neq 2$ let E be a nonsingular subspace of U or $U^\perp$ minimal with respect to the condition $p \mid |G_E^{*E}|$; if $p = 2$ let E be a nonsingular 2-space (such that, if G is orthogonal, a Sylow 2-subgroup of G_E^{*E} is as large as possible). Then $V' = \langle V_i \mid V_i$ is not isometric to $E \rangle$ has no subspace isometric to E.

(vii) $P^{V'}=1$, except perhaps if $p=2$ and $\dim V' \leqslant 2$. Moreover, $\dim V'=2=p$ only if G is orthogonal.

Comments. By Proposition 14.8, U has a decomposition $V=V_1 \perp \cdots \perp V_t$ into nonsingular subspaces V_i permuted transitively by P (since V is a minimal nonsingular P-invariant subspace). Similarly, if $P^{U^\perp} \neq 1$ then (by 1.5) $U^\perp$ has a decomposition $U^\perp = V_{t+1} \perp \cdots \perp V_l$ as in Proposition 14.8. This takes care of (i)–(v).

If E is as in (vi) then E contains a representative of each G^*-orbit of nonsingular subspaces of dimension $<\dim E$. Thus, at least if $p \neq 2$, E has the same isometry type for U and (if $P^{U^\perp} \neq 1$) for $U^\perp$ (cf. [4]). This proves (vi). Note that $V' \subseteq U^\perp$. Thus, (vii) holds as well. Consequently, we have proven (i)–(vii) for any $U^\perp$ and any choice of $V_1, \ldots, V_l$ obtained as indicated.

It remains to show that the V_i can be found in polynomial time. Use Lemma 14.7 to decompose V as $U_1 \perp \cdots \perp U_b$ for minimal nonsingular P-invariant subspaces U_j. WLOG $U=U_1$ and $U^\perp = \langle U_j \mid j>1 \rangle$. Suppose that U_j contains a copy of E. Then P is Sylow in $G^*_{U_j}$ (by 1.5). Repeat step 3 of Section 17 (temporarily letting $V=U_j$ and $P_1=P^{U_j}$). This produces subspaces V_i of U_j permuted transitively by P. Letting j vary, we obtain all the required V_i isometric to E. The remaining subspaces V_i are those U_j lying in $U^\perp$ and not isometric to E.

1.7. Find $G^*_{\{V_1,\ldots,V_l\}}$ using Proposition 14.5, and use recursion (19.1). Since $P \neq 1$, some of the V_j are isometric to E. Thus, the decomposition $V=V_1 \perp \cdots \perp V_l$ satisfies all of the conditions listed in Proposition 14.8. The first paragraph of the proof of Lemma 14.6 shows that these two decompositions have isomorphic stabilizers in G^*. Thus, $G^*_{\{V_1,\ldots,V_l\}}$ contains a Sylow p-subgroup of G^*.)

2. WLOG P is irreducible. (As in Sect. 17, step 2, $|P|=O(n^5)$.)

3. Find the set Ω of all nonsingular subspaces V_1 such that

(i) $V=V_1 \perp \cdots \perp V_l$ with $V_1^P=\{V_1,\ldots,V_l\}$, and

(ii) Either $\dim V_1 \in \{1, 2, 6\}$, or V_1 is a minimal nonsingular h-invariant subspace for some $h \in P-Z^*$ with $h^p \in Z^*$.

Comments. Since $|P|=O(n^5)$, we can find Ω by using Corollary 11.4 and Lemmas 13.4 and 14.7. We need to show that Ω is both nonempty and relevant.

Let P_1 be a Sylow p-subgroup of G^* containing P, and let $\{V_1,\ldots,V_l\}$ be as in Proposition 14.8. Since P is irreducible it must be transitive on $\{V_1,\ldots,V_l\}$. Moreover, P_{V_1} is irreducible on V_1 (as $\langle U^P \rangle$ is a P-invariant subspace of V whenever $U \subset V_1$ is P_{V_1}-invariant). In particular, if $P_{V_1} \leqslant Z^*$ then $\dim V_1 = 1$, so that $V_1 \in \Omega$.

Similarly, if $p=2$ then $\dim V_1 \leqslant 2$ by Proposition 14.8, so that $V_1 \in \Omega$.

Let $p>2$. Then $(P_1)_{V_1}$ induces a cyclic group on V_1 (Proposition 14.8), and this cyclic group is irreducible (since $(P_{V_1})^{V_1}$ already is). By [18], each element of $(P_1)_{V_1}-Z^*$ is irreducible on V_1, unless $q=2$ and $\dim V_1=6$. Once again, this situation is covered in (ii), so that $V_1 \in \Omega$.

4. For each $V_1 \in \Omega$, decompose $V = V_1 \perp \cdots \perp V_l$ as in step 3, and find $H = G^*_{\{V_1,\ldots,V_l\}}$ using Proposition 14.5(i). Test whether P is Sylow in H. If it is not, and if $l > 1$, use recursion (19.1). (As noted in step 3, for some choice of V_1 the group H contains a Sylow p-subgroup of G^*.)

5. WLOG $l = 1$. (Then, as in Sect. 17, step 6, $p \neq 2$ and P is cyclic.) Let $P = \langle f \rangle$.

6. Let $\langle h \rangle$ be the cyclic group found in Proposition 15.1 if $G = \mathrm{PSL}(d, q)$ or in Proposition 15.2 otherwise. Let $\langle h' \rangle$ be a Sylow p-subgroup of $\langle h \rangle \cap G^*$. (By [16], $\langle h' \rangle$ is Sylow in G^*.)

7. Use Proposition 13.10 to find $f' \in \langle h' \rangle$ and $g \in G^*$ such that $f'^g = f$. Then $\langle h' \rangle^g$ is a Sylow p-subgroup of G^* containing P. (Since P is irreducible, so is its conjugate lying in $\langle h' \rangle$. Thus, Proposition 13.10 applies.) ▮

20. *Concluding Remarks*

1. As in [11, (4.2)], the Main Theorem (part (ii)) implies the following algorithmic version of the Frattini argument (compare Sect. 4, steps 4 and 5).

COROLLARY. *Given $N \trianglelefteq G \leqslant S_n$ and a Sylow subgroup P of N, in polynomial time a subgroup H of $N_G(P)$ can be found such that $G = HN$.*

Proof. Let Δ be the set of those given generators g of G not lying in N. Since P^g is Sylow in N, by (ii) we can find $m \in N$ such that $(P^g)^m = P$. Let Δ' be the set of elements gm obtained in this way (one per g). Let $H = \langle \Delta' \rangle$. Then $G = \langle \Delta, N \rangle = \langle \Delta', N \rangle = HN$. ▮

2. Part (ii) of the Main Theorem is an unusual type of result. It is concerned with the transitivity of G on the set of all Sylow p-subgroups of G, even though that set usually does not have polynomial size. Moreover, only one element g of G is produced: finding *all* such g seems to be extremely difficult. Namely, we have no idea how to find $N_G(P)$ for a Sylow p-subgroup P of G (compare the preceding corollary). In fact, even finding normalizers in S_n of subgroups of S_n seems very hard.

3. *Timing.* The algorithms in the Main Theorem run in time $O(n^9)$. The large exponent is caused by the Replacement Theorem's n^8 and the $O(n^8)$ algorithm (A.10).

A number of estimates used here were very crude. For example, $|V| \leqslant q^3 n$ by [10, Sect. 10, Table], whereas we have used the much weaker inequality $|V| \leqslant n^2$. For example, in Section 19, step 3 we actually only considered $< |V|^6/q^{21} < n^6$ subspaces, rather than $< n^{12}$ subspaces.

4. *Was* (A.11) *actually needed*? While it was certainly needed, the answer is "no." (A.11) can be avoided by a repackaging of the proof of the Main Theorem, as follows.

Delete Corollary 3.5. Add to Theorems 3.1, 3.3, 3.7, and 3.8 the assumption that

a SYLEMBEDSIMPLE subprocedure is available. (The proofs of these results, and of Theorem 3.9, were the only places (A.11) was invoked.) Now consider Section 19. Here (A.11) appears only once, in step 1.1, where we used the fact that $P \neq 1$. Thus, all we need to do is to produce an element of order p in the variant $P = 1$ of Section 19, step 1.1.

WLOG $p \nmid |G^*_{\langle v \rangle}|$ for each $v \in V - \{0\}$ (by recursion). (Then a Sylow p-subgroup P_1 of G^* has the property that V is a minimal nonsingular P_1-invariant subspace.)

Find the cyclic group $\langle h \rangle$ in Proposition 15.1 if $G = \mathrm{PSL}(d, q)$, or in Proposition 15.2 otherwise. If $p \mid |h|$ we are finished. WLOG $p \nmid |h|$.

Use Lemma 13.7 to find a totally isotropic or totally singular m-space W. Find G^*_W using Proposition 14.3. Use recursion.

(We claim that $p \mid |G^*_W|$. For, by (14.8) P_1 is cyclic. Then P_1 is reducible, as otherwise it would have been conjugate to a subgroup of $\langle h \rangle$. Thus, G is $\mathrm{PSp}(2m, q)$, $\mathrm{PSU}(2m, q)$, or $P\Omega^+(2m, q)$, and P_1 fixes a totally isotropic or totally singular m-space.) ∎

5. Also, (A.9) can be proved directly and easily: see HALLCONJ1 in the Appendix.

6. Now that the Main Theorem has been proved, it seems very desirable to have an entirely different proof avoiding the classification of finite simple groups. In view of the first sentence of this paper, our use of the classification can best be described as ludicrous.

APPENDIX: Solvable Groups

In this Appendix we will prove two theorems: a special case of the Main Theorem, and another result already contained in [11].

THEOREM A.1. *There are polynomial-time algorithms which, when given a solvable subgroup G of S_n and a prime p, solve the following problems*:

(i) *given a p-subgroup P of G, find a Sylow p-subgroup of G containing P; and*

(ii) *given Sylow p-subgroups P_1, P_2 of G, find $g \in G$ conjugating P_1 to P_2.*

As indicated in the Introduction, the proof of this special case contains the basic ideas in the proof of the Main Theorem, but the algorithms are much more efficient (and are no longer repulsive). Complete proofs will be given for Theorem A.1 and the next result. First, recall that if π denotes a set of primes then a *π-group* is a group whose order is divisible only by primes in π, and a *Hall π-subgroup* of G is a π-subgroup H of G such that $|G: H|$ is divisible by no member of π. The fundamental results of P. Hall assert that each π-subgroup of G is contained in a Hall π-subgroup, and that any two Hall π-subgroups are conjugate.

THEOREM A.2. *There are polynomial-time algorithms which, when given a solvable subgroup G of S_n and a set π of primes, solve the following problems*:

(i) *find a Hall π-subgroup of G; and*

(ii) *given Hall π-subgroups H_1, H_2 of G, find $g \in G$ conjugating H_1 to H_2.*

Note that Theorem A.2(i) is not as strong as the corresponding result Theorem A.1(i). The more general version is proved in [11], but using a very different and less efficient algorithm. It would be desirable to have a proof of this generalization of Theorem A.1(i) in the spirit of the present paper.

We will prove Theorem A.2, and then Theorem A.1(i), by presenting procedures that parallel those of Section 3. *Throughout the discussion G, n, and π or p will be as above; in particular, G will be solvable.*

HALLFIND
Input: G, π.
Output: A Hall π-subgroup of G.

1. Use (A.6) to find a normal subgroup M of G such that $|G/M| = p$ is a prime. (Since G is solvable, $G > G'$.) Recursively find a Hall π-subgroup H of M.
2. Let $g \in G - M$ (use one of the given generators of G). Call HALLCONJ in order to find $m \in M$ with $(H^g)^m = H$.
3. Find the Hall π-subgroup $\langle g' \rangle$ of the cyclic group $\langle gm \rangle$. Then $\langle H, g' \rangle$ is a Hall π-subgroup of G. (For, if $|G/M| \neq p$ then H is a Hall π-subgroup of G; while if $|G/M| = p$ then $g' \notin M$ and g' normalizes H.) ▮

HALLCONJ
Input: Hall π-subgroups H_1, H_2 of G.
Output: $f \in G$ with $H_1^f = H_2$.

1. Use (A.5) to find a normal subgroup M of G such that $|G/M| = p$ is a prime.
   Recursively find $m \in M$ with $(H_1 \cap M)^m = H_2 \cap M$. (Here $H_i \cap M$ is a Hall π-subgroup of M.) If $p \notin \pi$ then $H_i \cap M = H_i$, $i = 1, 2$, so WLOG $p \in \pi$.
2. Let $G^* = \langle H_1^m, H_2 \rangle$ and $M^* = M \cap G^*$ (use (A.7)). Call HALLCONJ1 in order to find $g \in G^*$ with $(H_1^m)^g = H_2$, and let $f = mg$. (Since $H_i \cap M \trianglelefteq H_i$, both H_1^m and H_2 normalize $H_1^m \cap M = H_2 \cap M$. Also, $H_1^m \not\leq M$, so that $|G^*/M^*| = p$. Thus, HALLCONJ1 is applicable to the quadruple G^*, M^*, H_1^m, H_2.) ▮

HALLCONJ1
Input: Hall π-subgroups H_1, H_2 of G; $M \lhd G$ with $|G/M| = p$ a prime in π and $H_1 \cap M = H_2 \cap M \lhd G$.
Output: $f \in G$ with $H_1^f = H_2$.

1. WLOG $H_1 \cap M < M$ (as otherwise $G = H_1 = H_2$).
2. Let $h \in H_1 - (H_1 \cap M)$. Let $h_2 \in H_2 - (H_2 \cap M)$ such that $t := h^{-1}h_2 \in M$. (Clearly, G/M is cyclic, and we can use (A.2) in order to test the powers of h_2.)

3. Find $u \in \langle t \rangle$ such that $u^p t^{-1} \in H_1 \cap M$. (Since $H_1 \cap M$ is a Hall π-subgroup of M, we have $(p, |M/(H_1 \cap M)|) = 1$. Then $u = t^i$ where $ip \equiv 1 \pmod{|M/(H_1 \cap M)|}$. Thus, while u can be found by testing the powers of t and using (A.2), a faster approach is to use the Eucidean Algorithm.)
4. Let $g = u^h (u^2)^{h^2} \cdots (u^{p-1})^{h^{p-1}}$.
5. Replace G, M, H_1, H_2 by $\langle H_1, H_2^g \rangle$, $\langle H_1, H_2^g \rangle \cap M$, H_1, H_2^g, and recursively call HALLCONJ1.

Comments. We must show that $G^* := \langle H_1, H_2^g \rangle$, $M^* := G^* \cap M$, H_1 and H_2^g behave as required in the input for HALLCONJ1, and moreover that $G^* < G$.

Clearly $G^* = H_1 M^*$, so that $|G^*/M^*| = p$. Also, $H_1 \cap M^* = H_1 \cap M = H_2 \cap M = (H_2 \cap M)^g = H_2^g \cap M^*$.

Therefore, all that is left is to show that $G^* < G$. Let K be a normal subgroup of G containing $H_1 \cap M$ and maximal with respect to being properly contained in M. (Recall that $M > H_1 \cap M$.) Let bar denote the natural homomorphism $G \to G/K$.

Note that $\bar{M} = M/K$ is an elementary abelian q-group for some prime q, and $q \neq p$ since $(p, |M/(H_1 \cap M)|) = 1$. We will regard $\bar{M}$ as a vector space over $\mathbb{Z}_q$, and write everything in terms of linear algebra. Namely, $\bar{h}$ induces a linear transformation x of $\bar{M}$, and $x^p = 1$ (as $h^p \in H_1 \cap M$). Moreover, $\bar{u}$ and $\bar{g}$ lie in $\bar{M}$. In view of the maximality of K, $\langle x \rangle$ acts irreducibly on $\bar{M}$.

If $x = 1$ then $\bar{G} = \langle \bar{g}, \bar{M} \rangle = \langle \bar{g} \rangle \times \bar{M}$ since $p \neq q$, and hence $\bar{H}_1 = \langle \bar{g} \rangle = \bar{H}_2 = \bar{H}_2^g$. Then $\bar{G}^* = \langle \bar{H}_1, \bar{H}_2^g \rangle = \langle \bar{g} \rangle < \bar{G}$.

Assume that $x \neq 1$. By irreducibility, there is no eigenvalue 1. Since x satisfies $x^p - 1 = 0$, it also satisfies $\sum_{i=0}^{p-1} x^i = 0$. Then, in view of the definition of g,

$$\bar{g}(x-1) = \left(\sum_{i=1}^{p-1} i\bar{u}x^i \right)(x-1) = \bar{u} \left\{ \sum_{i=1}^{p-1} ix^{i+1} - \sum_{i=1}^{p-1} ix^i \right\}$$

$$= \bar{u} \left\{ (p-1)x^p - \sum_{i=2}^{p-1} x^i - x \right\} = \bar{u}\{(p-1)+1\} = p\bar{u} = \bar{t}.$$

In other words, $\bar{g}^{\bar{h}} \bar{g}^{-1} = \bar{t}$. It follows that $\bar{h}^{\bar{g}^{-1}} = \bar{h}\bar{t} = \bar{h}_2$, so that $\bar{H}_1 = \langle \bar{h} \rangle = \langle \bar{h}_2 \rangle^{\bar{g}} = \bar{H}_2^{\bar{g}}$. Thus, $\bar{G}^* = \bar{H}_1$ is a p-group whereas $\bar{G}$ is not. This proves that $G^* < G$.

Clearly, HALLCONJ1 runs in polynomial time. It easily follows that HALLFIND and HALLCONJ also do. *This completes the proof of Theorem* A.2.

We note that the preceding proof differs from that in [11] because of the procedure HALLCONJ1, and especially because of the explicit calculation involved in steps 4 and 5 of that procedure. Moreover, HALLCONJ1 (in fact, a very special case of this procedure) provides a very simple proof of (A.9). (In fact, the case of (A.9), in which H is elementary abelian and G acts irreducibly on H, is exactly what is needed in the only application of (A.9): Section 6, step 4. This is the precise situation in the group G/K occurring in the comments at the end of HALLCONJ1.)

It remains to deal with Theorem A.1(i).

SSYLEMBED
Input: A p-subgroup P of G.
Output: A Sylow p-subgroup containing P.

1. Use (A.5) to find a normal subgroup M of G with $|G/M|$ a prime. If $|G/M| \neq p$ call SSYLEMBED recursively for the pair M, P.
2. WLOG $|G/M| = p$.
   Case $P \leqslant M$.
   If P is not a Sylow p-subgroup of M then $G \leftarrow M$ and use recursion.
   If P is Sylow in M then repeat steps 2 and 3 of HALLFIND (using HALLCONJ) in order to find a p-group properly containing P.
3. *Case* $P \not\leqslant M$.
   3.1. Recursively find $Q \leqslant M$ with $P \cap M \lhd Q$ and $|Q/(P \cap M)| = p$. (Note that $P \cap M$ cannot be Sylow in M since P is not Sylow in G and $|G: M| = |P: P \cap M|$.)
   3.2. Let $G^* = \langle P, Q \rangle$. Find $M^* = M \cap G^*$ using (A.7).
   3.3. Call SSYLEMBED1 for the triple G^*, M^*, P.
   (Note that $P \cap M^* = P \cap M \lhd G^*$. Also, $P \cap M$ is not Sylow in M^* since $Q \leqslant M^*$, and hence P is not Sylow in G^*. Thus, the conditions of SSYLEMBED1 are satisfied.) ▮

SSYLEMBED1
Input: A p-subgroup P of G that is not a Sylow p-subgroup; $M \lhd G$ with $P \cap M \lhd G$ and G/M a cyclic p-group.
Output: A p-subgroup of G properly containing P.

1. WLOG $P \cap M < M$.
   Use (A.6) to find a normal subgroup T of M such that $|M/T|$ is a prime and $T \geqslant P \cap M$.
2. Let Y be the set of cosets of T in G. Determine the action of (the generators of) G on Y. (Note that $|Y| = |G/M| \cdot |M/T| \leqslant n^2$ since G/M is a cyclic p-group.)
   Use (A.4) to find $K = G_{(Y)}$. (Then $G > M > T \geqslant K \geqslant P \cap M$.)
3. If G/K is a cyclic p-group, $M \leftarrow K$ and return to 1. (Note that $K < M$.)
   We may now assume that G/K is noncyclic if it is a p-group.
4. Let $PM/M = \langle fM \rangle$ with $f \in P$.
5. *Case* $|M/T| = P$.
   5.1. Let $M^* = \langle K, f \rangle$. (By Lemma 2.1, G/K is a p-group, and hence is noncyclic by 3. Thus, $G > M^* \geqslant (P \cap M)\langle f \rangle = P$.)
   5.2. Find $G^* \leqslant G$ with $M^* \lhd G^*$ and $|G^*/M^*| = p$. (Note that M^*/K is a proper subgroup of the p-group G/K.)
   5.3. If P is not Sylow in M^* then $G \leftarrow M^*$ and $M \leftarrow K$ and use recursion. (Note that $M^*/K = K\langle f \rangle/K$ is cyclic.)

5.4. If P is Sylow in M^* then $G \leftarrow G^*$ and $M \leftarrow M^*$, and use HALLCONJ exactly as in steps 2 and 3 of HALLFIND in order to find a p-subgroup properly containing P.

6. *Case* $|M/T| = q \neq p$.

6.1. If $G > PM$ then either P is not Sylow in PM, in which case use recursion; or P is Sylow in PM, in which case $M \leftarrow PM$ and proceed exactly as in steps 2 and 3 of HALLFIND in order to find a p-subgroup of G properly containing P.

6.2. If $G = PM = \langle f \rangle M$ then $G \leftarrow \langle f, K \rangle$ and $M \leftarrow K$, and use recursion. (By 6.1 and Lemma 2.1, $PK/K = \langle f \rangle K/K$ is Sylow in G/K. However, P is not Sylow in $\langle f, K \rangle$, since that group contains a Sylow p-subgroup of G.) ▮

This completes the proof of Theorem A.1.

REFERENCES

1. J. J. CANNON, Effective procedures for the recognition of primitive groups, *Proc. Sympos. Pure Math.* **37** (1980), 487–493.
2. R. W. CARTER, "Simple Groups of Lie Type," Wiley, London/New York/Sydney/Toronto, 1972.
3. R. W. CARTER AND P. FONG, The Sylow 2-subgroups of the classical groups, *J. Algebra* **1** (1964), 139–151.
4. J. DIEUDONNÉ, "La géométrie des groupes classiques," Springer, Berlin/Göttingen/Heidelberg, 1963.
5. 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.
6. D. GORENSTEIN, "Finite Simple Groups: An Introduction to Their Classification," Plenum, New York, 1982.
7. M. HALL, JR., "The Theory of Groups," Macmillan, New York, 1959.
8. B. HUPPERT, Singer-Zyklen in klassischen Gruppen, *Math. Z.* **117** (1970), 141–150.
9. W. M. KANTOR, Permutation representations of the finite classical groups of small degree or rank, *J. Algebra* **60** (1979), 158–168.
10. W. M. KANTOR, Polynomial-time algorithms for finding elements of prime order and Sylow subgroups, *J. Algorithms* **6**, No. 2 (1985).
11. W. M. KANTOR AND D. E. TAYLOR, Polynomial-time versions of Sylow's theorem, *J. Algorithms*, in press.
12. E. LUKS, Isomorphism of graphs of bounded valence can be tested in polynomial time, *J. Comput. System Sci.* **25** (1982), 42–65.
13. E. LUKS, unpublished.
14. P. P. PÁLFY, A polynomial bound for the orders of primitive solvable groups, *J. Algebra* **77** (1982), 127–137.
15. C. C. SIMS, Some group-theoretic algorithms, *in* Springer Lecture Notes in Math. Vol. 697, pp. 108–124, 1978.
16. 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.
17. H. WIELANDT, "Finite Permutation Groups," Academic Press, New York, 1964.
18. K. ZSIGMONDY, Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892), 265–284.