JOURNAL OF ALGORITHMS 11, 523–563 (1990)

Finding Sylow Normalizers in Polynomial Time*

WILLIAM M. KANTOR

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

Received May 1987; revised June 1989

Given a set Γ of permutations of an n-set, let G be the group of permutations generated by Γ. If p is any prime, it is known that a Sylow p-subgroup P of G can be found in polynomial time. We show that the normalizer of P can also be found in polynomial time. In particular, given two Sylow p-subgroups of G, all elements conjugating one to the other can be found (as a coset of the normalizer of one of the Sylow p-subgroups). Analogous results are obtained in the case of Hall subgroups of solvable groups. © 1990 Academic Press, Inc.

1. INTRODUCTION

In [KT, Ka1, Ka2] polynomial-time versions of Sylow's theorem were obtained. In particular, it was shown that, in polynomial time, an element of a subgroup G of S_n could be found conjugating one given Sylow p-subgroup P_1 to another one P_2. In the present continuation of those papers, we will further investigate the transitive action of G on its set of Sylow p-subgroups (a set that generally does not have polynomial size). Namely, we will determine the stabilizer of a Sylow p-subgroup in this action. This will then also determine the set of elements conjugating P_1 to P_2 as a coset of the normalizer of P_1, thereby dealing with the *counting problem* naturally associated to the results in [Ka2].

THEOREM 1.1. *There is a polynomial-time algorithm which, when given a Sylow p-subgroup P of a group $G \le S_n$, finds the normalizer $N_G(P)$ of P in G.*

Of course, $N_G(P)$ is specified in terms of a set of generating permutations (as are all groups in this paper). The algorithms in [Ka2], for finding a Sylow p-subgroup in polynomial time and for conjugating one of them to another one, depend on the classification of finite simple groups for their

*This research was supported in part by NSF Grant DMS 87-01794.

0196-6774/90 $3.00

validity. The same is true of (1.1). Note that we are only able to study the transitive action of G on its set of Sylow p-subgroups in a very indirect manner. For example, it seems to be extremely difficult to determine the stabilizer of two Sylow p-subgroups in this action.

More elementary versions of the results in [Ka2] had been obtained earlier in [KT] (see also the Appendix in [Ka2]). Those versions dealt not only with Sylow subgroups, but also with Hall π-subgroups of solvable groups for any set π of primes. Recall that a *π-subgroup* of G is a subgroup H such that $|H|$ is divisible only by primes in π, and that a *Hall π-subgroup* is a π-subgroup H such that $|G:H|$ is divisible by no member of π. In the above papers it was shown that, for any π and any solvable subgroup G of S_n, in polynomial time one can find a Hall π-subgroup and conjugate one of them to another of them. The analogue of (1.1) is then

THEOREM 1.2. *There is a polynomial-time algorithm which, when given a solvable subgroup G of S_n, a set π of primes, and a Hall π-subgroup P of G, finds $N_G(P)$.*

Of course, if $\pi = \{p\}$ then (1.2) is just (1.1) for solvable groups. The proof of (1.2) is significantly simpler than that of (1.1) and will be presented first (Section 3). In order to further simplify matters, the reader may first wish to read Section 3 assuming that $\pi = \{p\}$, replacing "Hall π-subgroup" by "Sylow p-subgroup" throughout the section. The case $\pi = \{p\}$ of (1.2) can also be found in [Ka3].

The proofs of the above theorems are similar to those in [KT, Ka1, Ka2]. Section 4 reduces (1.1) to a special case involving a simple group. Then the bulk of this paper (Sections 5–6) deals with that special case by what is, for the most part, a straightforward and boring imitation of the technical arguments in [Ka1, Ka2]. In addition, some procedures needed for (1.1) produce significant improvements for some of the algorithms in [Ka2]; these improvements are presented in Section 6 (and, to some extent, also in Section 5). Some subsidiary results and procedures, notably (5.10) and (5.15), are of independent interest. Finally, in Section 7 we deduce slightly stronger forms of the above theorems.

As in [KT, Ka1, Ka2], the algorithm for (1.1) is not practical. However, as in the Appendix of [Ka2] the algorithm for (1.2) should be moderately efficient—though not as efficient as the ones in that Appendix.

2. PRELIMINARIES

In this section we will briefly review the notation used in [Ka1, Ka2]. We will consider $G = \langle \Gamma \rangle \leq S_n = \mathrm{Sym}(X)$, where $|X| = n$. If necessary, Sims' algorithm [Si, FHL] can be used to arrange that $|\Gamma| \leq n^2$.

The orbit of $x \in X$ is x^G, while the stabilizer $G_x = \{g \in G | x^g = x\}$. More generally, if $Y \subset X$, 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.

The derived group of G is G', while $O_\pi(G)$ is the largest normal π-subgroup of G. If $A, B \leq G$ then $[A, B] = \langle a^{-1}b^{-1}ab | a \in A, b \in B \rangle$. Note that A normalizes B if and only if $[A, B] \leq B$.

Throughout this paper, p will always denote a prime. If m is an integer then m_p denotes the largest power of p dividing m.

We will frequently use (without explicit mention) the trivial fact that any strictly increasing sequence of subgroups of S_n has at most $n \log n$ terms. (For the sharper bound $2n - 3$, see [Ba].) This will be an essential ingredient for recursion.

We note the following three elementary facts.

LEMMA 2.1 (Frattini argument; cf. [Gor (1.3.7)]). *Let $L \trianglelefteq G$.*

(i) *If P is a Sylow p-subgroup of L then $G = LN_G(P)$.*

(ii) *If L is solvable and P is a Hall subgroup of L then $G = LN_G(P)$.*

LEMMA 2.2. *Let A be a p-group acting as a group of automorphisms of a group M of order not divisible by p. Then the following hold*:

(i) $N_M(A) = C_M(A)$.

(ii) *For any prime q, there is an A-invariant Sylow q-subgroup Q of M; and for any such Q, $C_Q(A)$ is a Sylow q-subgroup of $C_M(A)$; and*

(iii) *If K is an A-invariant normal subgroup of M then $C_{M/K}(A) = C_M(A)K/K$.*

See [Gor, pp. 224–225] for (ii) and (iii). Proof of (i): $[A, N_M(A)] \leq A \cap [A, M] \leq A \cap M = 1$ since $p \nmid |M|$, so that $N_M(A) \leq C_M(A)$.

LEMMA 2.3 (cf. [Ka2, (2.1)]). *Let $T \triangleleft M \triangleleft G$ and let K be the largest normal subgroup of G contained in T. Then every prime dividing $|M/K|$ also divides $|M/T|$. Moreover, if M/T is simple then M/K is the direct product of simple groups isomorphic to M/T, and these are permuted transitively by G if M/T is nonabelian.*

List of Some Known Algorithms

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

(A.1) [Si, FHL] *Given $Y \subset X$, find $G_{(Y)}$ and $|G_{(Y)}|$.*

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

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

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

(A.5) [FHL] *Given $S \subseteq G$ and $H \leq G$, find $\langle S^H \rangle := \langle S^h | h \in H \rangle$.*

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

(A.7) *Given $H \leq S_n$ normalizing G,*
(i) [FHL] *Find $G \cap H$, and*
(ii) [Lu3] *Find $C_H(G)$.*

(A.8) [Lu2] (i) *Given $R \lhd G$ find a set X' on which G acts such that $G^{X'}$ is simple $R^{X'} = 1$ and $|X'| \leq n$.*
(ii) *Given normal subgroups $A < B$ of G, find a composition series for G containing A and B.*

When combined with (A.5), (A.8ii) yields:

(A.9) *Given normal subgroups $A < B$ of G, find a normal series for G containing A and B and such each successive quotient group is a direct product $S_1 \times \cdots \times S_l$ of simple groups S_i which are either of the same prime order or are nonabelian and permuted transitively by G; and for each S_i find a subgroup of G projecting onto it.*

(A.10) [KT, Ka2] *If π is a set of primes and if G is solvable, find $O_\pi(G)$; find a Hall π-subgroup of G; and given two Hall π-subgroups H_1 and H_2 of G, find $g \in G$ such that $(H_1)^g = H_2$.*

(A.11) [Ka2] *If p is a prime, find $O_p(G)$; find a Sylow p-subgroup of G containing a given p-subgroup of G; and, given two Sylow p-subgroups P_1 and P_2 of G, find $g \in G$ such that $(P_1)^g = P_2$.*

(A.12) [KT, Ka2] *Given $R \leq M \trianglelefteq G$, find D such that $R \leq D \leq N_G(R)$ and $G = DM$ in* **either** *of the following situations:*
(i) *G is solvable and R is a Hall subgroup of M; or*
(ii) *R is a Sylow subgroup of M.*

Note that (A.12) is an algorithmic version of the Frattini argument (2.1) (cf. Section 7).

Rónyai [Ro1, Ro2] has shown that a chief series of G can be found in polynomial time. However, instead of this beautiful result, we will only need a very elementary observation (pointed out by Rónyai) involving undergraduate linear algebra:

(LA) *Given an m-dimensional vector space V over $GF(p)$ and a set Γ of linear transformations, there is a polynomial (in m, p and $|\Gamma|$) time algorithm that finds the space of fixed vectors of Γ.*

Namely, first find the space of fixed vectors of each member of Γ, and then intersect these subspaces, using standard matrix computations.

3. Proof of (1.2)

The following algorithm takes care of (1.2).

HALLNORMALIZER.

Input: A solvable subgroup G of S_n, a set π of primes, and a Hall π-subgroup P of G.

Output: $N_G(P)$.

1. Find a maximal normal subgroup M of G, so that $|G/M|$ is a prime p. (Use (A.6).)

2. *Case $p \notin \pi$.* (Here, P is a Hall subgroup of M.)

Use (A.12) to find a subgroup D such that $D \le N_G(P)$ and $G = DM$.

Recursively find $N_M(P)$.

Output $DN_M(P)$. (Namely, $N_G(P) = N_{DM}(P) = DN_M(P)$.)

3. WLOG $p \in \pi$ and $G \neq P$.

Find normal subgroups M_0, L of G such that $L < M_0 \le M, G/M_0$ is a π-group and M_0/L is an elementary abelian q-group for some prime $q \notin \pi$. (Use (A.9)—but actually, in this solvable case essentially just (A.6) is needed—in order to find a normal series for G passing through M with elementary abelian quotients. Then M_0 is the smallest term of this series such that G/M_0 is a π-group, and L is the next term just below M_0.)

Then $M_0 \leftarrow M$. (Now G/M is a π-group, and G/L is not. Note that $G = PM$.)

4. Let "bar" (denoted $\bar{\ }$) be the natural homomorphism $G \to \bar G = G/L$. Use (LA) to find $C/L := C_{\bar M}(\bar P)$. (Since $\bar M$ is an elementary abelian q-group it can be regarded as a vector space over $GF(q)$. Moreover, $\bar P$ induces a group of linear transforinations, whose space of fixed vectors is precisely $C_{\bar M}(\bar P)$.)

5. If $G > PC$ (tested using (A.1)) then recursively find and output $N_{PC}(P)$.

(Certainly P normalizes C, so that PC is a group. By (2.2i), $N_{\bar M}(\bar P) = C_{\bar M}(\bar P) = \bar C$. Then $\overline{N_G(P)} \le N_{\bar G}(\bar P) = N_{\overline{PM}}(\bar P) = \bar P N_{\bar M}(\bar P) = \overline{PC}$. Thus, $N_G(P) \le PC$ since $L \le C$, and hence $N_G(P) = N_{PC}(P)$.)

6. If $G = PC$ then find a subgroup $C_0 \ge L$ of index q in C, and let $M_0 = \langle P, C_0 \rangle$.

(Here, $\bar G = \overline{PC} = \bar P \times \bar C$; for, $\bar P$ centralizes $\bar C$, while $\bar P \cap \bar C = 1$ as $\bar P$ is a π-group while $\bar C$ is a π'-group. Also $\bar C \neq 1$, as otherwise $G/L = PC/L = PL/L$ would be a π-group. Since $\bar C$ is elementary abelian, it is easy to find C_0. Note that M_0 is a maximal normal subgroup of G containing PL.)

Now $M \leftarrow M_0$ and return to 2. (This replaces M by the new maximal normal subgroup M_0 for which $|G : M_0|$ is a prime $q \notin \pi$. Thus, 2 produces the desired output.) □

4. Reduction to Simple Groups

In this section we will show that the proof of (1.1) can be reduced to a situation involving simple groups. Consider the following two problems.

SYLOWNORMALIZER.

Input: A subgroup G of S_n, a prime p, and a Sylow p-subgroup P of G.

Output: $N_G(P)$.

Of course, this is precisely the situation in (1.1).

SIMPLENORMALIZER.

Input: $L \triangleleft G \leq S_n$ with G/L a nonabelian simple group of order divisible by p; the natural homomorphism "bar" (denoted $\bar{\ }$) from G to $\bar{G} = G/L$; and a Sylow p-subgroup P of G.

Output: $H < G$ such that $L \leq H$, $N_{\bar{G}}(\bar{P}) \leq \bar{H}$ and $\bar{H}$ is normalized by $N_{\mathrm{Aut}(\bar{G})}(\bar{P})$.

Remark. Of course $\bar{H} = N_{\bar{G}}(\bar{P})$ behaves as required by SIMPLENORMALIZER. However, generally it will be more convenient to produce a subgroup $\bar{H}$ larger than this. Namely, in general (e.g., if $|\bar{G}| > n^8$ and $\bar{P}$ is noncyclic) $\bar{H}$ will merely be the set-stabilizer in $\bar{G}$ of a suitable family of subsets canonically determined by $\bar{P}$ in a suitable permutation representation of $\bar{G}$ (cf. (6.1)).

Theorem 4.1. *SYLOWNORMALIZER is polynomial-time reducible to SIMPLENORMALIZER.*

Proof. 1. Use (A.8) to find a set X' on which G acts such that $G^{X'}$ is simple and $|X'| \leq n$.

Find $M := G_{(X')}$ (using (A.4)).

2. *Case* $G^{X'} = G/M$ *is nonabelian of order divisible by* p.

Use SIMPLENORMALIZER to find a subgroup $H \geq M$ such that $N_{G/M}(PM/M) \leq H/M < G/M$.

Recursively find and output $N_H(P)$.

(Since $N_G(P)M/M \leq N_{G/M}(PM/M) \leq H/M$ we have $N_G(P) \leq H < G$, while $N_G(P) = N_H(P)$.)

3. *Case* $G^{X'}$ has order not divisible by p. (Here, P is a Sylow subgroup of M.)

Use (A.12) to find a subgroup D such that $D \leq N_G(P)$ and $G = DM$.

Recursively find $N_M(P)$.

Output $DN_M(P)$. (Namely, $N_G(P) = N_{DM}(P) = DN_M(P)$.)

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

Find normal subgroups M_0, L of G such that $L < M_0 \leq M$, G/M_0 is a p-group, G/L is not a p-group, and M_0/L is the direct product of simple groups which are either of the same prime order or are nonabelian and permuted transitively by G. (Find a normal series for G passing through M behaving as in (A.9). Then let M_0 be the smallest term of this series such that G/M_0 is a p-group, and let L be the next term just below M_0.)

Then $M_0 \leftarrow M$. (Now G/M is a p-group and G/L is not. Moreover, $G = PM$.)

Let "bar" (denoted $\bar{\ }$) be the natural homomorphism from G to $\overline{G} = G/L$.

5. *Case* $p \nmid |\overline{M}|$. (Then $N_{\overline{M}}(\overline{P}) = C_{\overline{M}}(\overline{P})$, by (2.2i).)

5.1. Let q be a prime dividing $|\overline{M}|$.

5.1.1. Find a Sylow q-subgroup Q of M (using (A.11)).

5.1.2. Use (A.12) to find a subgroup D_q of $N_G(Q)$ such that $G = MD_q$.

5.1.3. Find a Sylow p-subgroup P_q of D_q, find $g \in G$ with $(P_q)^g \leq P$, and then $Q \leftarrow Q^g$ and $P_q \leftarrow (P_q)^g$. (Use (A.11). Note that $\overline{P_q} = \overline{P}$ since $P_q \leq P$ and $G = MD_q = MP$.)

5.1.4. Find $N_{QP_q}(P_q)$ by applying (1.2) to the Sylow p-subgroup P_q of the solvable group QP_q, and find $C_q := Q \cap N_{QP_q}(P_q) = N_Q(P_q)$ using (A.7i).

(Here, QP_q is a group since P_q normalizes Q. By (2.2i), $C_q = N_Q(P_q) = C_Q(P_q)$, so that $C_q \cdot (Q \cap M)/Q \cap M = C_Q(P_q)(Q \cap M)/Q \cap M = C_{Q/Q \cap M}(P_q)$ (by (2.2iii) with $K = Q \cap M$). Then $\overline{C_q} = C_{\overline{Q}}(\overline{P_q})$. By (2.2ii), $C_{\overline{Q}}(\overline{P_q})$ is a Sylow q-subgroup of $C_{\overline{M}}(\overline{P_q})$. Since $\overline{P_q} = \overline{P}$, it follows that $\overline{C_q}$ is a Sylow q-subgroup of $C_{\overline{M}}(\overline{P})$.)

5.2. Let C be the subgroup of M generated by L together with groups C_q, one for each prime $q \mid |\overline{M}|$. (Then $\overline{C}$ contains a Sylow q-subgroup $\overline{C_q}$ of $C_{\overline{M}}(\overline{P})$ for each q, so that $\overline{C} = C_{\overline{M}}(\overline{P})$.)

5.3. If $G > PC$ then recursively find and output $N_{PC}(P)$.

(Since $L \leq C$ and $\overline{P}$ centralizes $\overline{C}$, P normalizes C, so that PC is a group. Since $N_{\overline{M}}(\overline{P}) = C_{\overline{M}}(\overline{P}) = \overline{C}$ we have $\overline{N_G(P)} \leq N_{\overline{G}}(\overline{P}) = N_{\overline{PM}}(\overline{P}) = \overline{P}N_{\overline{M}}(\overline{P}) = \overline{P}\overline{C}$. Thus, $N_G(P) \leq PC$ since $L \leq C$, and hence $N_G(P) = N_{PC}(P)$.)

5.4. If $G = PC$ then find a maximal normal subgroup $M_0 \geq PL$ of G (using (A.8)).

(Here, $\overline{G} = \overline{P}\overline{C}$ and $\overline{C}$ centralizes $\overline{P}$. Also, $\overline{P} \cap \overline{C} \leq \overline{P} \cap \overline{M} = 1$ (as $\overline{P}$ and $\overline{M}$ have relatively prime orders.) Thus, $\overline{G} = \overline{P} \times \overline{C}$, while $\overline{G} > \overline{P}$ since $\overline{G}$ is not a p-group, so that $PL \lhd G$. Consequently, there is such a subgroup M_0.)

Now $M \leftarrow M_0$ and return to 3. (This replaces M by the new maximal normal subgroup $M_0 \geq PL$ for which $p \nmid |G : M_0|$. Consequently, 3 outputs a subgroup behaving as required.)

6. WLOG $\overline{M}$ is the direct product $\overline{M_1} \times \cdots \times \overline{M_l}$ of nonabelian simple groups $\overline{M_i}$, each of order divisible by p, where $L < M_i \le M$. Moreover, $G = PM$ acts transitively on $\{\overline{M_1}, \ldots, \overline{M_l}\}$, and hence so does P.

Find $M_1, \ldots, M_l$ using (A.9).

Find $P_i := P \cap M_i$. (Use (A.7i), since $P \cap M_i = (P \cap M) \cap M_i$.)

(Note that $\overline{P}_i$ is a Sylow subgroup of $\overline{M_i}$, and hence is nontrivial. Since $\overline{P} \cap \overline{M_i}$ is a p-group containing that Sylow subgroup, we have $\overline{P} \cap \overline{M_i} = \overline{P_i}$. Then $\overline{P} \cap \overline{M} = \overline{P_1} \times \cdots \times \overline{P_l}$. Also, since $\overline{P}$ acts transitively on $\{\overline{M_1}, \ldots, \overline{M_l}\}$ it is transitive on $\{\overline{P_1}, \ldots, \overline{P_l}\}$; and the stabilizer $N_P(\overline{P_1})$ normalizes $\overline{M_1}$.)

7. Use SIMPLENORMALIZER to find a group H_1 such that $L \le H_1 < M_1$ and $N_{\overline{M_1}}(\overline{P_1}) \le \overline{H_1} < \overline{M_1}$, and such that $N_P(\overline{P_1})$ normalizes $\overline{H_1}$.

8. Find $E := \langle H_1^P \rangle$ using (A.5).

Recursively find and output $N_{PE}(P)$.

Comments. We claim that $\overline{M_1}$ contains exactly one conjugate of $\overline{H_1}$ under the action of $\overline{P}$. For, suppose that $\overline{H_1}^{\bar{g}} \le \overline{M_1}$ with $\bar{g} \in \overline{P}$. Then $\bar{g}$ normalizes $\overline{M_1}$ (since $\overline{P}$ acts on $\{\overline{M_1}, \ldots, \overline{M_l}\}$), and hence $\bar{g}$ induces an automorphism of $\overline{M_1}$ that also normalizes $\overline{P} \cap \overline{M_1}$, where $\overline{P} \cap \overline{M_1} = \overline{P_1}$ by 6. By a basic property of the output H_1 in 7, this implies that $\bar{g}$ normalizes $\overline{H_1}$. Thus, $\overline{H_1}^{\bar{g}} = \overline{H_1}$, as claimed.

Since $\overline{P}$ permutes $\{\overline{M_1}, \ldots, \overline{M_l}\}$ transitively, it follows that each group $\overline{M_i}$ contains a unique conjugate $\overline{H_i}$ of $\overline{H_1}$ under the action of $\overline{P}$. Thus, $\overline{E} = \overline{H_1} \times \cdots \times \overline{H_l} < \overline{M}$. Also $N_{\overline{M}}(\overline{P}) = N_{\overline{M_1}}(\overline{P_1}) \times \cdots \times N_{\overline{M_l}}(\overline{P_l}) \le \overline{H_1} \times \cdots \times \overline{H_l} = \overline{E}$.

On the other hand, $\overline{N_G(P)} \le N_{\overline{G}}(\overline{P}) = N_{\overline{P}\overline{M}}(\overline{P}) = \overline{P} N_{\overline{M}}(\overline{P}) \le \overline{P}(\overline{H_1} \times \cdots \times \overline{H_l}) = \overline{P}\overline{E}$, so that $N_G(P) \le PE$ (since $L \le E$) and hence $N_G(P) = N_{PE}(P)$. Clearly $\overline{P}$ normalizes the proper subgroup $\overline{E}$ of $\overline{M}$, while $\overline{G} = \overline{P}\overline{M}$ does not, so that $PE < G$, as required for recursion. □

5. Simple Groups

This section is a review and elaboration of some of the results contained in [Ka1, Ka2]. These consist of the Replacement Theorem (in Subsection 5A), the structure of Sylow subgroups (in Subsection 5B), and some technical algorithms (Subsections 5C and 5D).

(5A) *The Replacement Theorem*

The following results were proved in [Ka1; Ka2, Part III].

THEOREM 5.1 (Replacement Theorem). *There is a polynomial-time algorithm which, when given a nonabelian simple subgroup G of S_n such that $|G| > n^8$, produces a set Y on which G acts such that $|Y| < n^2$ and one of the following holds*:

(I) *$G \cong A_m$, $|Y| = m$, and G acts on Y in the natural manner.*

(II) *G is a classical group defined on a vector space V over a field F, and G acts on Y as it does on the set of all 1-spaces of V. Both V and F are also found, and $|V| < n^2$. If G is symplectic, orthogonal, or unitary then the form on V involved in the definition of G is also found.*

We will also need numerous consequences of (5.1II); see (5.12)–(5.13).

Convention. The notion of a nonsingular subspace is standard when V is equipped with a form. When $G = PSL(V)$ we will view all subspaces as being "nonsingular," and the symbols "$\perp$" and "$\oplus$" will be interpreted as being identical; moreover, any two subspaces will be viewed as being perpendicular to one another.

In (5.1II) let Isom(V) denote the group of all isometries of V (using the zero form if $G = PSL(V)$, so that $\mathrm{Isom}(V) = GL(V)$). For background concerning the classical groups, see (for example) [Di].

(5B) *Sylow Subgroups*

If G is as above then we must describe one of its Sylow p-subgroups P in terms of its behavior on Y or V. This behavior depends on whether or not G is classical and, if so, on whether or not p is the characteristic of V. The descriptions given here were used in [Ka1] in order to construct Sylow subgroups of the simple group G.

(5.2) *The alternating group $G = A_m$.* We will assume that $m > 6$, in which case $\mathrm{Aut}(G) = S_m$. Write $m = \Sigma a_i p^i$ in base p. Partition Y into a_i subsets of size p^i for those i for which $a_i > 0$. Then the set-stabilizer of this partition in G contains a Sylow p-subgroup P of G. Note that the indicated partition of Y is just the set of orbits of P.

This reduces many considerations to the case $m = ap^i$ with $a < p$, and even to the case $m = p^i$. In the latter case let $g \in G$ be the disjoint product of p^{i-1} cycles of length p. Then it is easy to check that $C_G(g)$ contains a Sylow p-subgroup P of G, and that $Z(P) = \langle g \rangle$ (since $m \neq 4, 5$). Consequently, there is an obvious recursive construction for P.

LEMMA 5.3. *Let $G = A_m$, let P be a p-Sylow subgroup of G, and set $N = N_{S_m}(P) = N_{\mathrm{Aut}(G)}(P)$.*

(i) *If P is intransitive and has exactly $a_i > 0$ orbits on Y of size p^i for certain values of i, then N induces the direct product of symmetric groups of degree a_i on the set of orbits of P on Y.*

(ii) *If $m = p$ then N/P is cyclic of order $p - 1$.*

Proof. (i) Since N permutes the set Π of orbits of P we may assume that $m = ap^i$ with $a < p$. Certainly, $(S_m)_\Pi^\Pi = S_a$, while $(S_m)_\Pi = (S_m)_{(\Pi)} \cdot N$ by the Frattini argument (2.1). Thus, $N^\Pi = (S_m)_\Pi^\Pi = S_a$.

(ii) Here N can be identified with the group of all permutations $x \mapsto ax + b$ of $GF(p)$, where $a \neq 0$ and b are in $GF(p)$. □

Throughout the remainder of this subsection G will be a classical group. As above let V be the corresponding vector space over a field F. Recall that $\Gamma L(V)$ denotes the group of all semilinear transformations of V, while $P\Gamma L(V) = \Gamma L(V)/Z(\Gamma L(V))$ is the group of projective transformations induced by $\Gamma L(V)$. We may assume that Y is the set of 1-spaces of V.

Let V^* denote the dual space of V, and let Y^* be its set of points (i.e., the set of hyperplanes of V).

LEMMA 5.4. (i) *If G is not isomorphic to any of the groups* $\mathrm{Sp}(4, q)$ *with q even, $P\Omega^+(8, q)$, or $PSL(V)$ with* $\dim V > 2$, *then* $\mathrm{Aut}(G) = N_{P\Gamma L(V)}(G)$.

(ii) *If $G = PSL(V)$ with* $\dim V > 2$ *then* $\mathrm{Aut}(G) = P\Gamma L(V)\langle\tau\rangle$, *where τ is any isomorphism between V and V^*. In particular,* $\mathrm{Aut}(G) \leq \mathrm{Sym}(Y \cup Y^*)$, *and* $\mathrm{Aut}(G)$ *acts on the set of all subspaces of V.*

Proof. See [Di, Chap. IV] (compare [Ca, p. 211]). □

From now on,

(5.5) *We will assume that* $\dim V > 4$, *and* $\dim V > 8$ *if G is an orthogonal group.*

(Otherwise, it is easy to check that $|G| < |V|^4$, whereas we will be in the situation of the Replacement Theorem 5.1, where $|G| > n^8 > |V|^4$.) Then G is simple, so that there is a unique subgroup G^* of $SL(V)$ such that $G^* = (G^*)'$ and $G^*/Z(G^*) = G$; here, $Z(G^*)$ consists of scalar transformations of V, and G^* preserves the form on V.

(5.6) If $p | q$ then a Sylow p-subgroup P of G fixes a unique 1-space y and a unique hyperplane of V, where y is totally isotropic or totally singular if $G \neq PSL(V)$. Moreover, $N_{\mathrm{Aut}(G)}(P)$ normalizes the stabilizer in G of this pair of subspaces.

(5.7) *Sylow subgroups when $p \nmid q$* (cf. [Ka2, (14.8), (14.5)], based on [We, CF]; also [GoLy (10-1)]).

Let P be a Sylow p-subgroup of G, let $G^* = (G^*)' \leq SL(V)$ project onto G (modulo scalars) and preserve the form on V, and let P^* be the largest p-subgroup of G^* projecting onto P. There is a decomposition $V = V_1 \perp \cdots \perp V_s$ such that the following all hold:

(a) P and P^* act on $\Omega := \{V_1, \ldots, V_s\}$.

(b) If the space $C_V(P^*)$ of fixed vectors of P^* is nonzero, then $C_V(P^*)$ is one of the V_i, say $V_c, c > 1$. (If $C_V(P^*) = 0$, write $V_c = 0$.)

(c) One of the following holds:

(c1) If $p \neq 2$ then, for each $V_i \neq V_c$, the set-stabilizer $P^*_{V_i}$ induces a cyclic group acting fixed-point-freely on V_i, and either

(c1.1) $P^*_{V_i}$ is irreducible on V_i, or

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

(c2) If $p = 2$ then $\dim V_i \leq 2$ and $P^*_{V_i}$ is irreducible on V_i for each $V_i \neq V_c$; moreover, $\dim V_1 = 2$.

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

(e) The set-stabilizer G_Ω induces the symmetric group on $V_1^G \cap \Omega$ while fixing each member of Ω not in $V_1^G \cap \Omega$.

Remarks 5.8. (a) *The isometry type of V_i is determined as follows*, assuming that $V_i \neq V_c$ and that $\dim V_i > 1$ when $p = 2$ (i.e., assuming that $V_i \in V_1^G$, in view of (5.7d)).

If $p > 2$ then V_i is a nonsingular subspace of minimal dimension subject to the condition that $p \mid |(G^*_{V_i})^{V_i}|$. Moreover, $|(V_1)^{G_\Omega}| = [(\dim V)/(\dim V_1)]$.

If $p = 2$ then the isometry type of the nonsingular 2-space V_i is determined by the requirement that $8 \mid |(G^*_{V_i})^{V_i}|$. If G is not orthogonal, or has odd dimension, then $|(V_1)^{G_\Omega}| = [\frac{1}{2}\dim V]$. In the even-dimensional orthogonal case $|(V_1)^{G_\Omega}| = \frac{1}{2}\dim V$ or $\frac{1}{2}\dim V - 1$, depending upon whether or not V is the orthogonal sum of subspaces isometric to V_1.

In each case, the various parameters implicit in (5.7) are completely determined by the form, field, dimension of V, and p.

(b) There is a further parity condition in (5.7c1.2):

if G is symplectic or orthogonal then $\frac{1}{2}\dim V_i$ *is odd*; and
if G is unitary then $\frac{1}{2}\dim V_i$ *is even*.

When G is symplectic or orthogonal, and $(G^*_{V_i})^{V_i} \trianglerighteq \mathrm{Sp}(2m, q)$ or $\Omega^+(2m, q)$, respectively, the irreducibility of $(P^*_{V_i})^{V_i}$ on a (totally isotropic or totally singular) subspace of V_i of dimension $m = \frac{1}{2}\dim V_i$ implies that $p \mid q^m - 1$ but $p \nmid q^i - 1$ for $1 \leq i < m$. If $m = 2l$ then $p \mid q^l + 1$, so that $(G^*_{V_i})^{V_i}$ contains a subgroup $\mathrm{Sp}(2l, q) \times \mathrm{Sp}(2l, q)$ or $\Omega^-(2l, q) \times \Omega^-(2l, q)$ such that each factor has order divisible by p, whereas $(P^*_{V_i})^{V_i}$ is cyclic.

This contradiction shows that m is odd. Similarly, if G is unitary and $(G^*_{V_i})^{V_i} \trianglerighteq SU(2m, q)$ with m odd, then a subgroup $SU(m, q) \times SU(m, q)$ produces the same contradiction.

(c) *In* (5.7c1.2), *there are exactly two* $(P^*_{V_i})^{V_i}$*-invariant subspaces other than* 0 *and* V_i, *and they are not* $(P^*_{V_i})^{V_i}$*-isomorphic.*

For, there are two $(P^*_{V_i})^{V_i}$-invariant subspaces U_1 and U_2 of dimension $\frac{1}{2}\dim V_i$ such that $V_i = U_1 \oplus U_2$. Then (c) is clear if U_1 and U_2 are not $(P^*_{V_i})^{V_i}$-isomorphic, which can be proved as follows.

There are bases $e_1, \dots, e_m$ of U_1 and $f_1, \dots, f_m$ of U_2 such that $(e_i, f_j) = \delta_{ij}$ for all i, j. The group $G^*_{U_1} \cap G^*_{U_2}$ consists of linear transformations whose matrices with respect to the basis $e_1, \dots, e_m, f_1, \dots, f_m$ have the form $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ for $m \times m$ matrices A and B satisfying $AB^t = I$ when G is symplectic or orthogonal and $A\bar{B}^t = I$ when G is unitary (where t denotes transpose, and $\bar{\ }$ is the involutory field automorphism of the underlying field $F = GF(q^2)$, so that $\bar{\zeta} = \zeta^q$ for $\zeta \in GF(q^2)$). In particular, each eigenvalue of B (in an algebraic closure of $GF(q)$) has the form ζ^{-1} (or $\bar{\zeta}^{-1}$) for an eigenvalue ζ of A.

With this in mind we can now consider a generator g of the cyclic group $(P^*_{V_i})^{V_i}$. This can be realized as follows (cf. [Hu, pp. 187–188]). Write $q' = q$ for G symplectic or orthogonal, and $q' = q^2$ for G unitary. We can identify U_1 with $GF(q'^m)$ so that the restriction of g to U_1 is field multiplication $v \mapsto \alpha v$ for a generator α of the Sylow p-subgroup of the multiplicative group of the field U_1. The eigenvalues of g on U_1 are $\alpha^{q'^i}$, $0 \le i \le m - 1$. Then the eigenvalues of g on U_2 are $\alpha^{-q'^i}$ (or $\bar{\alpha}^{-q'^i}$ in the unitary case).

Now assume that U_1 and U_2 are $(P^*_{V_i})^{V_i}$-isomorphic. Then the eigenvalues of g on these subspaces must be the same. Thus, whenever $0 \le i \le m - 1$ there must be a j such that $0 \le j \le m - 1$ and $\alpha^{q'^i} = \alpha^{-q'^j}$ (or $\alpha^{q'^i} = \bar{\alpha}^{-q'^j}$ in the unitary case). In particular, there is a j such that $0 \le j \le m - 1$ and $\alpha = \alpha^{-q'^j}$ (or $\alpha = \bar{\alpha}^{-q'^j}$).

In order to derive a contradiction, we first consider the symplectic and orthogonal cases. Here $\alpha^{1+q^j} = 1$. Clearly, $j \ne 0$, as otherwise we would have $\alpha^2 = 1$. Thus, $\alpha^{q^{2j}-1} = 1$ with $0 < j \le m - 1$. The irreducibility of $(P^*_{V_i})^{V_i}$ on U_1 implies that m is the smallest positive integer l such that $\alpha^{q^l-1} = 1$. Thus, $m|2j < 2m$, so that $m = 2j$ is even, which contradicts Remark (b).

Now consider the unitary case. Here, $\alpha\bar{\alpha}^{q'^j} = 1$, or, equivalently, $\alpha\alpha^{q^{2j+1}} = 1$. Then $\alpha^{q^{2j+1}+1} = 1$, so that $\alpha^{q^{4j+2}-1} = 1$. The irreducibility of $(P^*_{V_i})^{V_i}$ on U_1 implies that m is the smallest positive integer l such that $\alpha^{q^{2l}-1} = 1$. Thus, $m|2j + 1$, so that m is odd, which again contradicts Remark (b). This proves (c).

Notation. Let P_i be the subgroup of $\mathrm{Isom}(V)$ agreeing with $P^*_{V_i}$ on V_i and inducing the identity on each $V_j \neq V_i$. Then $P_1 \times \cdots \times P_s$ is a subgroup of $\mathrm{Isom}(V)$ containing the kernel $P^*_{(\Omega)}$ of the action of P^* on Ω. Clearly, $P_c = 1$, where $V_c = C_V(P^*)$.

Define Ω' as follows: $\Omega' = \Omega - \{V_c\}$ if $p \neq 2$, while if $p = 2$ then Ω' is obtained from Ω by removing any 1-spaces in Ω.

LEMMA 5.9. *All P_i are isomorphic for $V_i \in \Omega'$, and $P^*_{(\Omega)} \leq P_1 \times \cdots \times P_s$. Moreover, if $\delta := |P_1 \times \cdots \times P_s : P^*_{(\Omega)}|$ then $\delta = 1$ unless one of the following holds*:

(i) *All $V_i \in \Omega$ have dimension 1, and either $G = SL(d,q)$, $p|q-1$, or $G = SU(d,q)$, $p|q+1$, in which cases $\delta = |P_1| = (q-1)_p$ or $(q+1)_p$, respectively*;

(ii) *$p = 2$, $\delta = |P_1 : P_1 \cap P^*|$, and either $G = SL(d,q)$, $\delta = (q-1)_2$, or $G = SU(d,q)$, $\delta = (q+1)_2$; or*

(iii) *G is orthogonal, $p = 2$, and $\delta = |P_1 : P_1 \cap P^*| = 4$.*

In all cases, if V_i, $V_j \in \Omega$ are distinct then they are nonisomorphic $P^*_{(\Omega)}$-modules, and $C_{P^*}(V_j)^{V_i} = (P^*_{V_i})^{V_i}$.

Proof. By (5.7e), $\Omega' = (V_1)^{G_\Omega}$. By the Frattini argument (2.1), $N_{G_\Omega}(P_1 \times \cdots \times P_s)$ is transitive on Ω', which proves the first assertion of the lemma. Clearly, $P^*_{(\Omega)} \leq P_1 \times \cdots \times P_s$.

We must consider the possibility that $P^*_{(\Omega)} < P_1 \times \cdots \times P_s$. Determinants show that this can happen only if $p \,|\, |F| - 1$, and then $\dim V_i = 1$ or 2 by (5.7c).

If $G^* = \mathrm{Sp}(d,q)$ then $\dim V_i = 2$, so that $P_i \leq \mathrm{Isom}(V_i) = \mathrm{Sp}(2,q) \leq G^*$ and hence $P^*_{(\Omega)} = P_1 \times \cdots \times P_s$. Similarly, if $G^* = SU(d,q)$ and $2 \neq p|q-1$ then $\dim V_i = 2$ (since $|GU(1,q)| = q+1$), so that $(P_i)^{V_i} \cong P_i$ is a Sylow subgroup of $\mathrm{Isom}(V_i) = GU(2,q)$, and hence also of $SU(2,q)$ (since $|GU(2,q) : SU(2,q)| = q+1$), where $SU(2,q) \leq G^*$. Once again, $P^*_{(\Omega)} = P_1 \times \cdots \times P_s$. The case $G^* = \Omega^{\pm}(d,q)$, $p \neq 2$, is also similar. For, here $\dim V_i = 2$ and a Sylow p-subgroup of $\mathrm{Isom}(V_i)$ lies in $\Omega^{\pm}(V_i)$ (since $|\mathrm{Isom}(V_i) : \Omega^{\pm}(V_i)|$ divides 4), and once again $P^*_{(\Omega)} = P_1 \times \cdots \times P_s$.

Next, assume that $G^* = SL(d,q)$ or $SU(d,q)$, in which case we are left with the possibilities $p|q-1$ or $p|q+1$, respectively. Moreover, $\dim V_i \leq 2$ (and this dimension is 2 only if $p = 2$). An element of $P_1 \times \cdots \times P_s$ lies in $P^*_{(\Omega)}$ if its determinant is 1. This proves that $\delta = (q \pm 1)_p$. By (5.5), $\dim V > 4$, so that there are at least three subspaces V_i in Ω'. If $k \neq i, j$ then $(P_iP_k \cap P^*)^{V_i} = (P_i)^{V_i}$ in view of the determinant restriction, while $(P_iP_k \cap P^*)^{V_j} = 1$. This proves the lemma in this case.

Finally, suppose that $G^* = \Omega^{\pm}(d,q)$ and $p = 2$. By (5.5), $d > 8$. By (5.7d, e), $\dim V_1 = 2$ and at most two of the subspaces V_k are not in

$\Omega' = (V_1)^{G_\Omega}$, each such V_k having dimension 1. It follows that $|\Omega'| \geq 3$. If V_i, V_j, V_k are three distinct members of Ω' then $(P_iP_k \cap P^*)^{V_i} = (P_i)^{V_i}$, since, for every reflection $r_i \in P_i$, there is a reflection $r_k \in P_k$ such that r_ir_k lies in G^* and hence in P^*; clearly, $(P_iP_k \cap P^*)^{V_j} = 1$. The cases V_i or $V_j \notin \Omega'$ are handled similarly using reflections (but are even easier). Since P_1 contains representatives of each conjugacy class of reflections, we also have $\delta = |P_1 : P_1 \cap P^*| = 4$. □

In order to be able to find the normalizer of P we will need to locate a proper subgroup of G containing that normalizer. The crucial step is the next proposition. First we need more notation. If G^* and P^* are as in (5.7), and if W is any minimal nonsingular P^*-invariant subspace, write

$$\begin{aligned}
\Pi(W) &:= \{C_V(P_v^*) \mid |P_v^*| \text{ is maximal for } 0 \neq v \in W\},\\
\Pi^2(W) &:= \{\langle X, Y\rangle \mid X, Y \in \Pi(W) \text{ and } \langle X, Y\rangle \text{ contains more than two}\\
&\qquad \text{members of } \Pi(W)\},\\
\Pi^1(W) &:= \{C_V(P_v^*) \mid |P_v^*| \text{ is maximal or next-to-maximal for } 0 \neq v \in W\},\\
\Pi^{12}(W) &:= \{\langle X, Y) \mid X, Y \in \Pi^1(W) \text{ and } \langle X, Y\rangle \text{ contains more than two}\\
&\qquad \text{members of } \Pi^1(W)\}.
\end{aligned}$$

THEOREM 5.10. *Let $p \nmid q$ and let P, P^* and Ω be as in (5.7). Then either*

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

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

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

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

In particular, the set Ω is uniquely determined by P.

Proof. By the last statement in (5.9) together with (5.8c), V is the direct sum of $C_V(P^*)$ and pairwise nonisomorphic nontrivial irreducible $P^*_{(\Omega)}$-modules, so that each irreducible $P^*_{(\Omega)}$-module lies in some member of Ω. Let W be one of the subspaces in (i) or (ii). By Maschke's Theorem, W is the direct sum of the irreducible $P^*_{(\Omega)}$-modules it contains. Thus, W is direct sum of $W \cap C_V(P^*)$ and of various nontrivial irreducible $P^*_{(\Omega)}$-modules, each of the latter being perpendicular to $W \cap C_V(P^*)$. Since W is nonsingular, it follows from (5.7c) that W is the perpendicular sum of $W \cap C_V(P^*)$ and of members of Ω; by minimality, $W \cap C_V(P^*) = 0$ and

P^* permutes these members of Ω transitively. Thus, V is the perpendicular sum of $C_V(P^*)$ and the various subspaces W under consideration in (5.10)—along with the 1-spaces fixed by P^* in the case of (ii). Consequently, all we need is to recover the members of Ω lying in a given W.

We may assume that $\Omega' = (V_1)^{G_\Omega} = \{V_1, \dots, V_t\}$, where $t := |\Omega'|$. By (5.7e), $P^{*\Omega'} \cong P^{*\Omega}$ is a Sylow subgroup of S_t.

Let $Q = P^*(P_1 \times \cdots \times P_s)$ (this is a Sylow p-subgroup of $\mathrm{Isom}(V)_\Omega$). Let $\delta := |P_1 \times \cdots \times P_s : P^*_{(\Omega)}| = |Q : P^*|$ be as in (5.9).

Fix W as in (i) or (ii). Let s' be the number of members of Ω contained in W, so that s' is a power of p (since P^* permutes these members of Ω transitively). Consider an arbitrary nonzero vector $v \in W$. Then $v = v_{i_1} + \cdots + v_{i_r}$ is the sum of $r \geq 1$ nonzero vectors $v_{i_j} \in V_{i_j} \subseteq W$ for $r \leq s'$ distinct values of the subscript i_j; we may assume that $i_1 = 1$. The stabilizer Q_v permutes the V_{i_j} and hence also the v_{i_j}, so that $|(Q_v)^\Omega| \leq \{r!(s'-r)!(t-s')!\}_p$. Also, Q_v contains the direct product of the groups P_i, where i is not one of the subscripts i_j.

Case $p \neq 2$. Here, $(Q_{v_i})^{V_i} = 1$ for any i whenever $0 \neq v_i \in V_i$ (cf. (5.7c)). Recall from (5.7d) that $\Omega' = \Omega$ or $\Omega - \{V_c\}$, where $P_c = 1$. Then $|Q_v| \leq \{r!(s'-r)!(t-s')! \cdot |P_1|^{t-r}\}_p$, and equality holds when $r = 1$. By (5.9), either $\delta = 1$ or δ corresponds to a determinant condition. If $r < t$ and $\delta \neq 1$ then δ elements of P_i, for i none of the i_j but $V_i \in \Omega'$, can be used to satisfy this determinant condition, so that $|P_v^*| \leq \{r!(s'-r)!(t-s')!|P_1|V^{t-r}/\delta\}_p$.

Claim. $|P_v^*|$ is maximal precisely when $r = 1$. For, assume that $r > 1$. Then

$$\{|P_1|^{t-1}(s'-1)!(t-s')!/\delta\}_p \Big/ \{|P_1|^{t-r}r!(s'-r)!(t-s')!/\delta\}_p$$
$$= \left\{\left(|P_1|^{r-1}/r\right)\binom{s'-1}{r-1}\right\}_p > 1,$$

which proves the claim if $r < t$. Suppose that $r = t$. Then $s' = t$ is a power of p. This time $\{|P_1|^{t-1}(s'-1)!(t-s')!/\delta\}_p/\{t!\}_p = |P_1|^{t-1}/\delta t$. Since $\delta \leq |P_1|$ (cf. (5.9)) and $t \geq p \geq 3$, we have $|P_1|^{t-1}/\delta t > 1$ unless $\delta = |P_1| = t = 3$; but then $\dim \mathrm{V}_1 = 1$ (which holds since $\delta > 1$, in view of (5.9)) and we obtain the contradiction $\dim \mathrm{V} = 3$ (cf. (5.5)). This proves our claim.

Since $C_W(P_{v_1}^*) = V_1$ for $0 \neq v_1 \in V_1$ (by the final assertion in (5.9)), this proves (i) when $p \neq 2$.

Case $p = 2$. Here, $(Q_{v_1})^{V_1} = (P_{v_1}^*)^{V_1}$ can be nontrivial for some nonzero vectors $v_1 \in V_1$. The possibilities for this group can be found in [CF] (this merely involves calculations with 2×2 matrices). If G is symplectic then

$(Q_{V_1})^{V_1}$ is fixed-point-free of order $|P_1| \geq 8$, and we are in the same situation as in the preceding case. Therefore, we may assume that G is not symplectic. Then $(Q_{V_1})^{V_1}$ contains a dihedral group of order 8; any noncentral involution of the latter group fixes some nonzero vector, so that the stabilizer of that vector in $(Q_{V_1})^{V_1}$ has order at least 2. Moreover, if μ is the maximal order of the stabilizer of a nonzero vector of V_1, then the stabilizer of each nonzero vector of V_1 has order 1, 2, or μ. Here, $\mu = 2$ except in the following cases: $G = PSL(d, q)$ or $PSU(d, q)$, $q \equiv \varepsilon \pmod 4$ with $\varepsilon = 1$ or -1, respectively, and then $|P_1| = |(Q_{V_1})^{V_1}| = 2(q - \varepsilon)_2^2$, $\mu = (q - \varepsilon)_2$. (These situations for which $\mu > 2$ correspond exactly to part (iia) of the theorem.) In all cases, $|P_1| = |(Q_{V_1})^{V_1}| \geq 2\mu^2$. Note that $\mu = \delta$ if G is not orthogonal.

By (5.7d), $C_V(P^*) = 0$ and each of the $s - t$ members of $\Omega - \Omega'$ has dimension 1. If $V_i \in \Omega - \Omega'$ then $|P_i| = \mu$ (as is seen by checking all cases). Thus, $|Q_{(\Omega)}| = |P_1|^t \mu^{s-t}$.

If $0 \neq w \in V_1 \subseteq W$ then $(Q_{(\Omega)w})^{V_1} = (Q_w)^{V_1}$, so that $|Q_{(\Omega)w}| = |P_1|^{t-1}\mu^{s-t}|(Q_w)^{V_1}|$, where $|(P_{1w})^{V_1}| = |(Q_w)^{V_1}| = 1, 2$, or μ. We will only consider those vectors w for which the latter order is 2 or μ. Then $|Q_w| = |Q_{(\Omega)w}|\{(s' - 1)!(t - s')!\}_2 \geq \{2|P_1|^{t-1}\mu^{s-t}(s' - 1)!(t - s')!\}_2$, and hence $|P_w^*| \geq \{2|P_1|^{t-1}\mu^{s-t}(s' - 1)!(t - s')!/\delta\}_2$.

On the other hand, $|Q_v| \leq \{\mu^r|P_1|^{t-r}\mu^{s-t}r!(s' - r)!(t - s')!\}_2$. Moreover, if $t > r$ then (by (5.9ii, iii)) we can use P_1, for i none of the i_j but $V_i \in \Omega'$, in order to see that $|Q_v : P_v^*| = \delta$. Similarly, if $G = PSL(d, q)$ or $PSU(d, q)$ with d odd then $s = t + 1$, and we can use P_s to see that $|Q_v : P_v^*| = \delta$ in this case as well. Thus, one of the following holds:

(A) $|P_v^*| \leq \{\mu^r|P_1|^{t-r}\mu^{s-t}r!(s' - r)!(t - s')!/\delta\}_2$; or

(B) $|P_v^*| \leq \mu^r\mu^{s-t}t!_2$, $t = r$ (in which case $s' = t$ as well, so that t is a power of 2), and either G is orthogonal or $\dim V$ is even.

We are assuming that v has a nonzero projection v_1 into V_1. This time we claim that $|P_v^*|$ is maximal when $r = 1$ and $v = w$ is a vector in V_1 for which $|(Q_w)^{V_1}| = \mu$; and that, if $\mu > 2$, then $|P_v^*|$ is next-to-maximal when $r = 1$ and $v = w$ is a vector in V_1 for which $|(Q_w)^{V_1}| = 2$. For, suppose that $r > 1$, and first consider (A). Here

$$\begin{aligned}|P_w^*|/|P_v^*| &\geq \{2|P_1|^{t-1}\mu^{s-t}(s' - 1)!(t - s')!/\delta\}_2/\\ &\qquad \{\mu^r|P_1|^{t-r}\mu^{s-t}r!(s' - r)!(t - s')!/\delta\}_2\\ &= \left\{\{2|P_1|^{r-1}/r\mu^r\}\binom{s' - 1}{r - 1}\right\}_2 > 1,\end{aligned}$$

since $2|P_1|^{r-1} \geq 2(2\mu^2)^{r-1} > r\mu^r$. On the other hand, in (B) we have

$$|P_w^*|/|P_v^*| \geq \{2|P_1|^{t-1}\mu^{s-t}(t-1)!/\delta\}_2/\{\mu^t\mu^{s-t}t!\}_2$$
$$= 2|P_1|^{t-1}/\delta t\mu^t \geq 2(2\mu^2)^{t-1}/\delta t\mu^t = 2^t\mu^{t-2}/\delta t > 1,$$

since one of the following holds: G is orthogonal, $\delta = 4$ and hence $t \geq 4$ (since $\dim V > 8$ by (5.5) and t is a power of 2); or G is not orthogonal, $\delta = \mu$, and $t \geq 4$ (since t is a power of 2, $s - t = 0$ or 1 by (5.7d), $\dim V = 2t + (s - t)$ is even in the non-orthogonal subcase of (B), and $\dim V > 4$ by (5.5)). This proves our claim.

Moreover, in each case, $C_W(P_w^*) = \langle w \rangle$ by (5.9). Thus, $\Pi(W)$ or $\Pi^1(W)$ consists of the 1-spaces $\langle w \rangle$ contained in some $V_i \subseteq W$ such that $|(P_w^*)^{V_i}| \geq 2$, and $\Pi^1(W)$ occurs only when $\mu > 2$, which is the situation in (iia).

Finally, as already noted, there are at least four 1-spaces X of V_1 centralized by nontrivial elements of $(Q_{V_1})^{V_1} = (P_{V_1}^*)^{V_1}$, and then $X \in \Pi(W)$ or $\Pi^1(W)$ depending upon the value of μ. If X and Y are two of these 1-spaces such that $\langle X, Y \rangle$ contains a third member of $\Pi(W)$ or $\Pi^1(W)$, then X and Y lie in some V_i; and each $V_i \in \Omega'$ contains such pairs X, Y. Consequently, $\Pi^2(W)$ or $\Pi^{12}(W)$ (depending on the value of μ) behaves as required.

In order to prove the last remark in the theorem, note that G^* is uniquely determined by G, so that P^* is uniquely determined by P. The subspaces W are uniquely determined by P^*, and hence so are $\Pi(W)$, $\Pi^1(W)$, $\Pi^2(W)$, and $\Pi^{12}(W)$. Thus, so is Ω. □

Remark. The preceding theorem implies a uniqueness statement for $P_{(\Omega)}$. Another, more group-theoretic (and more easily proved) description is as follows when $p > 2$: $P_{(\Omega)}$ is the set of elements in P that commute with all their conjugates. In fact, if $g \in P - P_{(\Omega)}$ then g does not commute with g^h for some $h \in P_{(\Omega)}$. However, it is not clear how to convert this description into an algorithm, whereas an algorithm is implicit in the theorem (cf. (5.13ii)).

PROPOSITION 5.11. *Let $p \nmid q$.*

(i) *$N_G(P)$ lies in the set-stabilizer G_Ω of $\Omega := \{V_1, \ldots, V_s\}$ (cf. (5.7)).*

(ii) *Each element of $P\Gamma L(V)$ normalizing both G and P preserves Ω and hence normalizes G_Ω. (Hence, if G is not $PSL(V)$ then $N_{\mathrm{Aut}(G)}(P)$ normalizes G_Ω.)*

(iii) *If $s = 1$ and P is irreducible then P is cyclic. If g is a linear transformation of V inducing a generator of P, then the additive group E of linear transformations generated by g is closed under multiplication and is isomorphic to the field $GF(|V|)$. Moreover, V can be identified with E. Write*

$E^* := E - \{0\}$ and let r be the characteristic of E. Then $N_{\Gamma L(V)}(\langle g \rangle) = N_{\Gamma L(V)}(E^*) = E^* \rtimes \langle \rho \rangle$, where ρ is the semilinear transformation of V induced by the automorphism $e \mapsto e^r$ of E.

(iv) *If $s = 1$ and P is reducible then the following all hold: $G \neq PSL(V)$, P is cyclic, $p > 2$, and $V = U_1 \oplus U_2$ for totally singular or totally isotropic subspaces U_1, U_2 such that each element of $P\Gamma L(V)$ normalizing both G and P also normalizes $G_{\{U_1, U_2\}}$.*

(v) *If G is $PSL(V)$ then $N_{\mathrm{Aut}(G)}(P)$ normalizes G_Ω.*

Proof. Let G^* and P^* be as in (5.7). Certainly $N_{\Gamma L(V)}G^*) \cap N_{\Gamma L(V)}(P^*)$ leaves invariant the nonsingular subspace $V_c = C_V(P^*)$.

(i), (ii) These are immediate consequences of (5.10). (The parenthetical remark in (ii) requires (5.4) and (5.5).)

(iii) See [Hu, pp. 187–188] for the description of $N_{\Gamma L(V)}(P^*)$.

(iv) See (5.7c) and (5.8c).

(v) View the dual space V^* of V as the set of linear forms on V, and let $V_i^\#$ be the subspace of V^* consisting of those linear forms vanishing on all of the V_j for $j \neq i$. Then $V_i^\#$ is isomorphic to the dual of V_i. We have $V^* = V_1^\# \oplus \ldots \oplus V_l^\#$, where this P^*-invariant decomposition has the same properties relative to V^* as the decomposition of V we have been dealing with (cf. (5.7)). Some element of $N_{\mathrm{Aut}(G)}(P)$ sends Ω to $\{V_1^\#, \ldots, V_l^\#\}$ and hence normalizes G_Ω. Then $|N_{\mathrm{Aut}(G)}(P) : N_{P\Gamma L(V)}(P)| = 2$, and (v) holds. □

(5C) *Linear Algebra*

Much more than the Replacement Theorem 5.1 is actually proved in [Ka2] in the case of classical groups. The net effect of the results in Part III of [Ka2] is that permutation group considerations can be replaced by linear algebra. This permits the desired properties of G to be computed much more directly and concretely. Many of these results will be needed later and can be summarized as follows (see Subsection 5A for the convention concerning the term "nonsingular").

PROPOSITION 5.12 [Ka2, Sections 13, 14]. *In the situation of* (5.1II), *there are polynomial-time algorithms for each of the following problems.*

(i) *Find (the set of all vectors in) the subspace of V spanned by a given subset of V. (In particular, find a basis of V.)*

(ii) *Given a semilinear transformation t of V (in terms of a given basis of V), find the permutation of 1-spaces induced by t. In particular, decide whether or not t has the same action as an element of G on the set Y of 1-spaces of V.*

(iii) *Find $G^* \leq SL(V)$ preserving the form on V such that $G^* = (G^*)'$ and G^* projects onto G modulo scalar transformations; find the preimage in G^* of any given subgroup of G.*

(iv) *Given a nonsingular, totally isotropic or totally singular subspace U of V, find the set-stabilizers G_U and G_U^*.*

(v) *Given nonsingular, totally isotropic or totally singular subspaces U_1 and U_2 of V, decide whether or not $U_2 \in U_1^G$; and if $U_2 \in U_1^G$ then find $g \in G$ with $U_2 = U_1^g$.*

(vi) *Given a decomposition $V = V_1 \perp \cdots \perp V_s$ into nonsingular subspaces V_i, find the set-stabilizers of $\{V_1, \dots, V_s\}$ in both G and G^*.*

(vii) *Given decompositions $V = V_1 \perp \cdots \perp V_s = V_1' \perp \cdots \perp V_s'$ of V into nonsingular subspaces V_i and V_i' such that $\{V_1', \dots, V_s'\} \in \{V_1, \dots, V_s\}^G$, find $g \in G$ with $\{V_1', \dots, V_s'\} = \{V_1, \dots, V_s\}^g$.*

(viii) *Given a subgroup P^* of G^* of order relatively prime to the characteristic of V, find all P^*-irreducible subspaces and all minimal nonsingular P^*-invariant subspaces of V; find P^*-irreducible subspaces $V_1, \dots, V_r$ such that $V = V_1 \oplus \cdots \oplus V_r$; and find minimal nonsingular P^*-invariant subspaces $W_1, \dots, W_s$ such that $V = W_1 \perp \cdots \perp W_s$.*

(ix) *Given conjugate elements t_1, t_2 of G^* (or* Isom(V)*) each of which is irreducible on V, find g in G^* (or* Isom(V)*, respectively) such that $t_1^g = t_2$.*

Corollary 5.13. (i) *In* (5.6), *the unique P-invariant* 1*-space, the unique P-invariant hyperplane, and the stabilizer in G of this pair, can be found in polynomial time.*

(ii) *A decomposition* (5.7), *and its set-stabilizer, can be found in polynomial time.*

(iii) *The groups $N_{\Gamma L(V)}(\langle g \rangle) = N_{\Gamma L(V)}(E^*)$ and $N_{G^*}(\langle g \rangle)$ in* (5.11iii) *can be found in polynomial time.*

(iv) *A decomposition $V = U_1 \oplus U_2$ in* (5.11iv), *and its set-stabilizer $G_{\{U_1, U_2\}}$, can be found in polynomial time.*

Proof. (i) These are just point-stabilizer problems: use (A.1).

(ii) Each subspace W in (5.10) can be found, and all computations involved in the definitions of $\Pi(W)$, $\Pi^2(W)$, $\Pi^1(W)$, and $\Pi^{12}(W)$ can be carried out in polynomial time, using (A.1) and (5.12i, viii). Thus, by (5.10), Ω can be constructed in polynomial time. The stabilizer G_Ω can then be found using (5.12vi).

(iii) All of the computations implicit in (5.11iii) can be carried out in polynomial time, using (5.12i, ii). Then $|N_{\Gamma L(V)}(E^*)|$ is small (certainly $< |V|^2$), so that all of its elements can simply be listed and tested for membership in G^*.

(iv) Use (5.12i) in order to recursively find a basis $e_1, f_1, \dots, e_m, f_m$ of V such that, for all i and j, $e_i \in U_1$, $f_j \in U_2$, e_i and f_j are isotropic or singular, and $(e_i, f_j) = \delta_{ij}$. Write matrices with respect to the ordered basis $e_1, \dots, e_m, f_1, \dots, f_m$. Let Δ be the set of matrices $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ preserving the form on V such that $A - I$ and $B - I$ have at most two nonzero entries (compare [Ka2, p. 378]). Then $\langle \Delta \rangle$ is the group of all elements of $\mathrm{Isom}(V)$ that fix U_1 and U_2. Let M be the matrix of the linear transformation defined by sending $e_i \to f_i \to e_i$ in the orthogonal and unitary cases, and $e_i \to f_i \to -e_i$ in the symplectic case $(i = 1, \dots, m)$. This linear transformation interchanges U_1 and U_2 and preserves the form on V. Let H be the group of linear transformations of V determined by the matrix group $\langle \Delta, M \rangle$. Then $H \cap G^* = G^*_{\{U_1, U_2\}}$, and this can be found using (A.7i) since $G^* \trianglelefteq \mathrm{Isom}(V)$. The group of permutations of the 1-spaces of V induced by $G^*_{\{U_1, U_2\}}$ is the desired stabilizer $G_{\{U_1, U_2\}}$. □

(5D) *Centralizers in Classical Groups*

This subsection will not be needed for the proof of (1.1). It is included both because of its relevance to complexity issues regarding permutation groups and because it can be used to obtain a slightly different (and more complicated) approach to one of the results in [Ka2] (cf. SYLEMBEDSIMPLE + SYLEMBED1SIMPLE below in Subsection 6B).

We begin with an example before dealing with the general case in (5.15).

(5.14) Example. Assume that $G = PSL(V) = PSL(d, q)$ with q odd, and that t is an involution in $P\Gamma L(V)$. Then some preimage t^* of t in $\Gamma L(V)$ behaves in one of the following ways [Di, pp. 5–10]: (i) t^* is an involutory linear transformation, so that $C_V(t^*)$ is a proper subspace of V; (ii) t^* is a field automorphism, so that $C_V(t^*)$ is a d-dimensional vector space over $GF(\sqrt{q})$; or (iii) t^* is a linear transformation, $C_V(t^*) = 0$, and $-1 \in \langle t^* \rangle$. In each of these cases *we will determine $C_G(t)$ in polynomial time*. Let $G^* = SL(V)$.

(i) Here $V = C_V(t^*) \oplus C_V(-t^*)$. Use (5.12i) to find a basis $v_1, \dots, v_d$ of V such that $v_1, \dots, v_k$ is a basis of $C_V(t^*)$ and $v_{k+1}, \dots, v_d$ is a basis of $C_V(-t^*)$. Let Δ consist of those $d \times d$ matrices A such that $\det A = 1$, the i, j entry is 0 for $i \le k < j$ or $j \le k < i$, and such that $A - I$ has at most two nonzero entries. Then the group of linear transformations determined by $\langle \Delta \rangle$ with respect to the basis $v_1, \dots, v_d$ is precisely $C_{G^*}(t^*)$. If $k \neq \frac{1}{2}d$ then $C_{G^*}(t^*) = N_{G^*}(\langle -1, t^* \rangle)$, and $C_{G^*}(t^*)$ projects (modulo scalars) onto $C_G(t)$.

If $k = \frac{1}{2}d$ then let g be the linear transformation such that $v_i^g = v_{i+k}$ for $i \leq k$, $v_i^g = v_{i-k}$ for $k < i < d$, and $v_d^g = (-1)^k v_k$. Then $\langle C_{G^*}(t^*), g\rangle = N_{G^*}(\langle -1, t^*\rangle)$, and $\langle C_{G^*}(t^*), g\rangle$ projects onto $C_G(t)$.

(ii) Use (5.12i) to find a basis $v_1, \ldots, v_d$ of V belonging to $C_v(t^*)$. Let Δ consist of those $d \times d$ matrices A such that $\det A = 1$, $A - I$ has at most two nonzero entries, and those entries lie in $GF(\sqrt{q})$. Then the group of linear transformations determined by $\langle \Delta \rangle$ with respect to the basis $v_1, \ldots, v_d$ is precisely $C_{G^*}(t^*)$. The subgroup of G it projects onto is $C_G(t)$.

(iii) Find the $GF(q)$-space E of linear transformations generated by the linear transformation t^*. Then E is a field and is isomorphic to $GF(q^2)$. Now V can be viewed as a $\frac{1}{2}d$-dimensional vector space over E. Find a basis $v_1, \ldots, v_{\frac{1}{2}d}$ of this vector space using (5.12i). Let Δ consist of those nonsingular $\frac{1}{2}d \times \frac{1}{2}d$ matrices A (over E) such that $\det A = 1$ and $A - I$ has at most two nonzero entries. Then the group of linear transformations determined by $\langle \Delta \rangle$ with respect to the basis $v_1, \ldots, v_{\frac{1}{2}d}$ is precisely $C_{G^*}(t^*)$. This time we must go slightly further to obtain $C_G(t)$. Consider an element $g \in G^*$ such that t^g and t agree modulo scalars. Then g acts on E as a field automorphism and is $GF(q)$-linear, so that g induces either 1 or the involutory field automorphism β of E. Let β' denote the β-semilinear transformation of V (viewed as an E-space) fixing each v_i, in which case β' is linear over $GF(q)$. Then, if we view V as a $GF(q)$-space, the group of linear transformations determined by $\langle \Delta, \beta' \rangle$ projects onto $C_G(t)$.

THEOREM 5.15. *There is a polynomial-time algorithm which, when given an element t of prime order p in the automorphism group of a classical simple group G of characteristic not p—where G is given as a subgroup of S_n for some n—finds $C_G(t)$.*

Proof. If $|G| \leq n^8$ then brute force can be used, so we will assume that $|G| > n^8$. Using the Replacement Theorem 5.1, we can switch sets in order to assume that we are given G acting on the set Y of 1-spaces of a d-dimensional vector space V over a field F. By (5.5), $\dim V > 4$ and G is not $P\Omega^+(8, q)$.

The theorem is more or less implicit in [GoLy (8-1), (8-2), (9-1)], except when $p = 2$ and t arises from a linear transformation or when $G = PSL(V)$ and t does not act projectively on V (i.e., does not act on Y). The latter case is postponed until (5.16). Let G^* be as in (5.7), and let t^* be a semilinear transformation projectively preserving the form on V (if any) and inducing t on Y. We will only sketch the description of $C_{G^*}(t^*)$ provided in [GoLy (8-1), (8-2), (9-1)], as well as the required algorithm.

Case 1. t^* is linear and can be chosen of order p.

First we will find $C_{\mathrm{Isom}(V)}(t^*)$. This group is described in [GoLy (8-1)] when $p \neq 2$. Here, $C_{\mathrm{Isom}(V)}(t^*)$ is the direct product of centralizers of restrictions of t^* to easily found (via (5.12viii)) subspaces U, and on which it can be assumed that t^* acts "orthogonally homogeneously": the perpendicular sum of minimal t^*-invariant nonsingular subspaces, on each of which t^* acts as in (5.7c), all of which are equivalent under transformations in $\mathrm{Isom}(V)$ (and hence all of which have the same dimension k). It is easy to reduce to the case $V = U$. Find the F-space E of linear transformations generated by t^*. Then E is a field, and $[E:F] = m$, where $mk = d$ or $\frac{1}{2}d$ depending on the nature of G. Moreover, V can be viewed as a vector space over E, possibly equipped with a form (which again depends on the nature of G). Now $C_{\mathrm{Isom}(V)}(t^*)$ can be found as in (5.14).

Then $C_{G^*}(t^*)$ can be found using (A.7i), and so can its projection into G. This projection is just $C_G(t)$ except in the following situations: (A) $G = PSL(d,q)$, $p|q-1$, and t^* has p eigenspaces each of dimension d/p; or (B) $G = PSU(d,q)$, $p|q+1$, and t^* has p pairwise orthogonal eigenspaces, each of dimension d/p.

Assume that (A) or (B) holds. Find a linear transformation g of determinant 1 and order p permuting the eigenspaces in a p-cycle, and preserving the form if (B) holds. Namely, such a linear transformation can be found in (A) using bases of the eigenspaces exactly as in (5.14i). The same is true in (B) provided that orthogonal bases of the eigenspaces are used; and such bases can be found easily using (5.1II) and (5.12i).

Let $s \in G^*$ be the scalar transformation obtained by multiplication by an element of F^* of order p. Then $N_{G^*}(\langle s, t^*\rangle) = \langle C_{G^*}(t^*), g\rangle$, and this group projects onto $C_G(t)$.

The case $p = 2$ is handled in the same manner.

Case 2. t^* is linear and cannot be chosen to have order p.

The F-space E of linear transformations generated by t^* is again a field, there is a form on V, and $N_{\mathrm{Isom}(V)}(\langle t^*\rangle)$ can be described [GoLy, (8-2)], and then generated, as in (5.14iii). This group acts on $\langle t^*\rangle/\langle t^{*p}\rangle = \langle t\rangle$, so that $C_G(t)$ can be found using (A.1). The case $p = 2$, not discussed in [GoLy], is handled in the same manner.

Case 3. t^* is nonlinear.

Here t^* has order p and is a field automorphism, and $C_{\mathrm{Isom}(V)}(t^*)$ can be described [GoLy, (9-1)], and then generated, as in (5.14); and then so can $C_G(t)$. □

LEMMA 5.16. *Given $G = PSL(V)$ as a subgroup of S_n for some n, given V, and given an involutory automorphism t of G that does not act projectively on V, the centralizer $C_G(t)$ can be found in polynomial time.*

Proof. By [Di, pp. 10–13], t arises from a nonsingular alternating, symmetric, or hermitian form on V. This form is easily computed. (Namely, the map $t: Y \to Y^*$ is induced by an invertible semilinear transformation $\tau: V \to V^*$, and then the form is $(u, v) := (u)v^{\tau}$.) Then $C_G(t)$ is the image, under the projection from $G^* = SL(V)$ to G, of the group of isometries of this form having determinant 1. This group of linear transformations can be generated as above by using matrices most of whose entries are 0. □

Remark 5.17. If G has characteristic p then it is harder to describe $C_G(t)$. However, in this situation (5.16) continues to take care of the case in which t does not act projectively on V. If t acts projectively on V then $C_G(t)$ lies in the set-stabilizer of the set Y_0 of fixed points of t on Y. Here Y_0 is the set of 1-spaces either of a vector space of dimension dim V over a subfield of F, or else of a subspace W of V. In the first case $C_G(t)$ can be found as above. In the second case $W' := W \cap W^{\perp}$ can be found, as can the space W'' spanned by the singular vectors in W' (which is relevant only when $p = 2$ and G is orthogonal); then (5.12iv) will *output a proper subgroup* G_W, $G_{W'}$, *or* $G_{W''}$ *of* G *containing* $C_G(t)$ *and invariant under the action of* $C_{\mathrm{Aut}(G)}(t)$. All of this takes polynomial time.

Remark 5.18. There is a polynomial-time algorithm which, when given an element t of prime order p in the automorphism group of an alternating group G—where G is given as a subgroup of S_n for some n—finds $C_G(t)$.

Namely, it is easy to reduce to the case $G\langle t \rangle = A_n$ or S_n, in which case finding $C_G(t)$ is elementary.

Remark 5.19. The Graph Isomorphism Problem can be reduced to the problem of finding centralizers of involutions in arbitrary permutation groups [Lu3] (cf. [Ka3]). Consequently, centralizers have relevance outside of the specific context of this paper. However, none of the algorithms presented here seem to produce any information concerning the special cases of the centralizer problem relevant to the Graph Isomorphism Problem.

6. Completion of the Proof of Theorem 1.1

In Section 4 we saw that the proof of Theorem 1.1 reduces to the consideration of simple groups. In this section we will first complete that proof (in Subsection 6A) and then conclude with comments concerning the corresponding portions of [Ka2] (in Subsection 6B).

TABLE 1

G	P	H
Small $\|G\|$	Arbitrary	$N_G(P)$
Alternating	Intransitive	Stabilizer of the set of orbits
	Transitive, noncyclic	Stabilizer of the set of orbits of $Z(P)$
	Transitive, cyclic	$N_G(P)$
Classical over F	$p \mid \|F\|$	Stabilizer of fixed {1-space, hyperplane}
	Reducible, noncyclic, $p \nmid \|F\|$	Stabilizer of orthogonal decomposition (5.7)
	Reducible, cyclic, and no fixed 1-space	Stabilizer of decomposition (5.11iv)
	Irreducible, cyclic	$N_G(P)$

(6A) *Simple Groups*

All that was needed in Section 4 was a polynomial-time algorithm for the following problem.

SIMPLENORMALIZER.

Input: $L \lhd G \leq S_n$ with G/L a nonabelian simple group of order divisible by p; the natural homomorphism "bar" (denoted $\bar{\ }$) from G to $\bar{G} = G/L$; and a Sylow p-subgroup P of G.

Output: $H < G$ such that $L \leq H$, $N_{\bar{G}}(\bar{P}) \leq \bar{H}$ and $\bar{H}$ is normalized by $N_{\mathrm{Aut}(\bar{G})}(\bar{P})$.

Remark 6.1. Table 1 indicates the choices of H we will make in the various cases, assuming that $L = 1$. For alternating or classical groups G the description is in terms of the action of P on the set or vector space involved in the definition of G.

We now turn to SIMPLENORMALIZER.

1. Call (A.8i) in order to reduce to the case $L = 1$.

2. If $|G| \leq n^8$ then $N_G(P)$ can be found by brute force. Output $H = N_G(P)$.

3. WLOG $|G| > n^8$.

Apply the Replacement Theorem 5.1 in order to obtain a new set Y of size $< n^2$.

(Now G is an alternating group A_m or a classical group, and Y is either the m-set involved in the definition of A_m or the set of all 1-spaces of the vector space V involved in the definition of the classical group.)

4. *Case* G is A_m. (Since $|G| > n^8, m > 6$ and hence $\mathrm{Aut}(G) = S_m$.)

4.1. If $m = p$ then an element of order $p - 1$ normalizing P can easily be written down (see the proof of (5.3ii)).

4.2. If $m = p^i > p$ then find the set Ω of orbits of $Z(P)$ on Y, and find and output $H = G_\Omega$. (Finding $G_\Omega = (S_m)_\Omega \cap G$ is straightforward, since $(S_m)_\Omega$ is generated by a symmetric group of degree p on one member of Ω, together with a symmetric group $S_{m/p}$ acting faithfully on Ω.)

4.3. If m is not a power of p then find the set Π of orbits of P on Y, and find and output $H = G_\Pi$. (As above, G_Π is easily found.)

Note. The same Π appeared in Steps 2–5 of the proof of [Ka2, (16.2)], as did Ω (but unnamed). The statement there about the structure of G_Π is strange since $G_\Pi = (S_m)_\Pi \cap G$, where $(S_m)_\Pi$ is the direct product of wreath products of symmetric groups with symmetric groups, all of which are easily found.

5. WLOG G is classical. Then (5.1) produces the underlying vector space V, field F and form (if any) on V.

(By (5.5) and (5.4), if $G \neq PSL(V)$ then Aut(G) acts projectively on the underlying vector space V.)

If $p \mid |F|$ then there is a unique P-invariant pair {1-space, hyperplane} (cf. (5.6)), whose stabilizer H can be found using (5.13i). Output H. (Then H behaves as required, by (5.6).)

6. WLOG $p \nmid |F|$.

If P is noncyclic use (5.13ii) in order to construct a family of subspaces of V, and the set-stabilizer H in G of that family, such that $N_G(P) \leq H$ (cf. (5.10i)). Output H. (Then H is $N_{\mathrm{Aut}(G)}(P)$ invariant, by (5.11i, v).)

7. WLOG P is cyclic (so that $p > 2$ by (5.7c)).

Use (5.12viii) to test the irreducibility of P. If P is reducible, then use (5.13iv) to find a decomposition (5.11iv) and its set-stabilizer H in G, and output H. (By (5.11iv), H behaves as required, since $G \neq PSL(V)$ so that Aut(G) acts projectively on V by 5.)

8. WLOG P is irreducible.

Find and output $N_G(P)$, using (5.13iii). □

This completes the proof of Theorem 1.1.

(6B) *Finding and Conjugating Sylow Subgroups*

In view of some of the results presented earlier in this paper (especially (5.10), (5.11), (5.13)—but not (1.1) or (1.2)!), simplifications are possible in [Ka2]. This subsection contains revised versions of algorithms in [Ka2] and, in general, should be viewed primarily as commentary on [Ka2].

The simpler algorithms SYLFIND, SYLCONJ, SYLCONJ1, and SYLEMBED in [Ka2] are merely overly terse. The following modified versions of the algorithms SYLCONJSIMPLE, SYLEMBED1, SYLEM-

BEDSIMPLE, and SYLEMBED1SIMPLE of [Ka2] represent significant simplifications, and do not presuppose that the reader has studied their counterparts in [Ka2]. (At the end of this subsection yet another (combined) version of SYLEMBEDSIMPLE and SYLEMBED1SIMPLE is also presented, based on (5.15)–(5.18).) All of these new algorithms also correct or sidestep minor errors and misprints occurring in [Ka2]. They also correct omissions in [Ka2] concerning timing analyses involving classical groups (analyses which were glibly omitted in that paper, and which turn out to be more complicated than realized there and hence are better circumvented).

In order to set the stage, let $G \leq S_n$ and p be as usual. Recall from [Ka2] that SYLFIND easily reduced finding a Sylow p-subgroup to SYLCONJ, conjugating Sylow p-subgroups. SYLCONJ was, in turn, easily reduced to two special cases of itself, SYLCONJ1 (conjugating when, in effect, a Sylow p-subgroup has order p) and SYLCONJSIMPLE:

SYLCONJSIMPLE.
Input: Sylow p-subgroups P_1, P_2 of the nonabelian simple group G.
Output: $f \in G$ with $P_1^f = P_2$.

1. WLOG $|G| > n^8$ (as otherwise the permutation representation of G on the set of conjugates of P_1 can be determined, by brute force).

Use the Replacement Theorem 5.1 together with (5.12iii) to find a set Y such that $|Y| < n^2$ and either

(i) G is A_m and Y is an m-set on which G acts in the natural manner, or

(ii) G is a classical group and Y is the set of 1-spaces of the vector space involved in the definition of G. In the latter case, also find all elements of the underlying vector space V (and field F), also of size $< n^2$; a group $G^* = (G^*)'$ of linear transformations of V preserving the form on V and projecting onto G (so that $G^*/Z(G^*) = G$); and the quadratic, bilinear, or hermitian form on V (if G is not $PSL(V)$) involved in the definition of G.

2. *Case G is A_m*. (Here, $|Y| = m$.)
2.1. *Subcase P_1 is intransitive on Y.*
2.1.1. Find the set Σ_i of orbits of P_i on Y.
Find $g \in G$ such that $\Sigma_1^g = \Sigma_2$, and $P_1 \leftarrow P_1^g$. (Finding g is elementary, since G acts on Y as the full alternating group.)
Now $\Sigma := \Sigma_1$ coincides with Σ_2.
2.1.2. For each $Y' \in \Sigma$, recursively find $f(Y') \in G$ such that $P_1^{f(Y')}$ and P_2 coincide on Y', while $f(Y') = 1$ on $Y - Y'$.

(Note that it is straightforward to pass from $\mathrm{Alt}(Y')$ to $\mathrm{Sym}(Y')$. Namely, if $p > 2$ then $P_1^{Y'}$ and $P_2^{Y'}$ are Sylow subgroups of $\mathrm{Alt}(Y')$, so that recursion produces $f(Y')$ such that $f(Y')^{Y'} \in \mathrm{Alt}(Y')$. On the other hand, if $p = 2$ then $P_1^{Y'} \cap \mathrm{Alt}(Y')$ is a Sylow 2-subgroup of $\mathrm{Alt}(Y')$, and it is easy to see that $P_1^{Y'}$ coincides with its normalizer in $G_{Y'}^{Y'}$ if $|Y'| \neq 4, 5$. Recursively find $f' \in G_{Y'}^{Y'}$ conjugating $P_1^{Y'} \cap \mathrm{Alt}(Y')$ to $P_2^{Y'} \cap \mathrm{Alt}(Y')$. Then modify f' so it conjugates $P_1^{Y'}$ to $P_2^{Y'}$ (where no modification is needed if $|Y'| \neq 4, 5$, while if $|Y'| = 4$ or 5 then the modification is trivial to accomplish). Finally let $f(Y')$ be the identity on $Y - Y'$ and let $f(Y') = f'$ or $f't$ on Y', where t is a transposition in $P_2^{Y'}$ and the choice is designed to make $f(Y')$ an even permutation.)

2.1.3. Output the product f of all these elements $f(Y')$ of G.

(Here f behaves as required. For, $\langle P_1^f, P_2 \rangle$ induces 1 on Σ, and induces a p-group on each member of Σ. Then $\langle P_1^f, P_2 \rangle$ is itself a p-group, and hence coincides with both P_1^f and P_2; that is, $P_1^f = P_2$.)

2.2. *Subcase P_1 is transitive on Y.*

2.2.1. Find $Z(P_i)$ and its set Σ_i of orbits. (Use (A.7ii). As noted in (5.2), since we are assuming that $|G| > n^8$ and hence that $|Y| > 5$, $Z(P_i)$ is cyclic; it is generated by an element of order p having no fixed points on Y. Then $|\Sigma| = |Y|/p$.)

Find $g \in G$ such that $\Sigma_1^g = \Sigma_2$ and $P_1 \leftarrow P_1^g$.

Now $\Sigma := \Sigma_1$ coincides with Σ_2.

2.2.2. If $P_1 = Z(P_1)$ (tested using (A.2)) then P_1 is cyclic of order $p = |Y|$, and it is elementary to conjugate a generator of P_1 to one of P_2.

WLOG P_1 is noncyclic. (Then $|\Sigma| > 1$.)

2.2.3. Recursively, find $g \in G$ such that $(P_1^\Sigma)^g = P_2^\Sigma$, and $P_1 \leftarrow P_1^g$.

(An additional remark is needed if $p = 2$. In that case P_1^Σ is a Sylow 2-subgroup of the symmetric group G_Σ^Σ. Recursion produces an element $g \in G$ conjugating $P_1^\Sigma \cap \mathrm{Alt}(\Sigma)$ to $P_2^\Sigma \cap \mathrm{Alt}(\Sigma)$, and then $(P_1^\Sigma)^g = P_2^\Sigma$ if $|\Sigma| \neq 4$, since it is easy to check that P_1^Σ is the normalizer of $P_1^\Sigma \cap \mathrm{Alt}(\Sigma)$ in G_Σ^Σ. However, if $|\Sigma| = 4$ then $|Y| = 8$, so that brute force can be used.)

Now $P_1^\Sigma = P_2^\Sigma$.

2.2.4. Find an element f of $G_{(\Sigma)}$ conjugating $P_{1(\Sigma)}$ to $P_{2(\Sigma)}$. (As in 2.2.2, it is straightforward to find such an f.)

Output f. (Namely, $P_1^f = P_2$ for the reason given in 2.1.3.)

3. WLOG G is classical. (In 1 we found the underlying vector space V and field F, as well as a group $G^* = (G^*)'$ of linear transformations preserving the form on V, if any, and projecting onto G.)

Find the largest p-subgroup P_i^* of G^* projecting onto P_i for $i = 1, 2$. (Use (5.12iii).)

Then $G \leftarrow G^*$ and $P_i \leftarrow P_i^*$ for $i = 1, 2$.

(Now G is a group of linear transformations of V. We must still conjugate P_1 to P_2.)

4. *Case* $p \| F|$. Find $y_i \in Y$ fixed by P_i (cf. (5.6)).

Find $g \in G$ with $y_1^g = y_2$ (using (A.3)) and $P_1 \leftarrow P_1^g$. Now $y_1 = y_2$.

Similarly (and recursively), for each $j = 1, \dots, \dim V - 1$, find a j-space V_{ij} fixed by P_i, and repeatedly conjugate P_1 in order to have $V_{1j} = V_{2j}$ for each j. (Namely, P_1 acts on the set of $(j+1)$-spaces containing V_{1j}, and there are fewer than $|V|$ such subspaces.)

Then it is easy to check that now $P_1 = P_2$.

5. WLOG $p \nmid |F|$.

Use P_1 and (5.13ii) in order to decompose V as $V = V_1 \perp \cdots \perp V_s$ as in (5.7). Let $\Omega = \{V_1, \dots, V_s\}$.

Note. This is *not* the approach taken in [Ka2], where P_i-irreducible subspaces were used.

5.1. Find an analogous decomposition $V = V_1' \perp \cdots \perp V_s'$ using P_2.

5.2. Find $g \in G$ sending the first decomposition to the second. (Since P_1 canonically determines Ω by (5.10), such an element g exists by Sylow's Theorem. It can be found using (5.12vii).)

5.3. Then $P_1^g \leftarrow P_1$.

(Now both P_1 and P_2 produce the same family Ω and decomposition $V = V_1 \perp \cdots \perp V_s$ (so that P_1 and P_2 both lie in the set-stabilizer G_Ω).)

6. Use (5.12vi) to find G_Ω.

Use 2 to find $g \in G_\Omega$ such that $(P_1^\Omega)^g = P_2^\Omega$, and $P_1 \leftarrow P_1^g$.

(Here G_Ω^Ω fixes at most two members of Ω and induces the symmetric group on the remainder of Ω, by (5.7e). Since P_1^Ω and P_2^Ω induce Sylow subgroups of this symmetric group, P_1^Ω can be conjugated to P_2^Ω exactly as described in 2.1.2.)

Note. Now P_1 *and* P_2 *agree in their action on the set* Ω. The kernel of the action of P_1 is contained in the direct product $(P_{1V_1})^{V_1} \times \cdots \times (P_{1V_s})^{V_s}$, just as in (5.9) (where, however, P_1 had a different meaning). The latter group lies in $\mathrm{Isom}(V)$. At this point it *suffices* to find an element $f \in G_\Omega$ sending each V_i to itself and conjugating $(P_{1V_i})^{V_i}$ to $(P_{2V_i})^{V_i}$ for each i. For, if f behaves in this manner then $\langle P_1^f, P_2 \rangle$ induces a p-group on Ω, while the kernel of its action on Ω is a p-group, so that $\langle P_1^f, P_2\rangle$ is itself a p-group, and hence coincides with both P_1^f and P_2 (compare 2.1.3 and 2.2.4).

7. For each i find the subgroup $G_{[i]}$ of elements of G inducing the identity on all V_j, $j \neq i$ (using (A.1)).

Similarly, find $P_{k[i]} := P_k \cap G_{[i]}$ for $k = 1, 2$. (This group is cyclic if $p \neq 2$, by (5.7c1).)

8. Assume that i is such that $(P_{1[i]})^{V_i}$ is irreducible.

Find an element $f(i) \in G_{[i]}$ conjugating $(P_{1V_i})^{V_i}$ to $(P_{2V_i})^{V_i}$, as follows:

If $(P_{1V_i})^{V_i} = (P_{1[i]})^{V_i} \leq (G_{[i]})^{V_i} \cong G_{[i]}$ and $p > 2$ then apply (5.12ix) to generators of the cyclic subgroups $(P_{1V_i})^{V_i}$ and $(P_{2V_i})^{V_i}$ of $(G_{[i]})^{V_i}$.

If $(P_{1V_i})^{V_i} > (P_{1[i]})^{V_i}$, or if $p = 2$, then $p \mid |F| - 1$ and $\dim V_i \leq 2$ (cf. (5.9)). If $\dim V_i = 1$ then $f(i) = 1$ works. If $\dim V_i = 2$ then $p = 2$ (as $(P_{k[i]})^{V_i}$ is irreducible), and it is easy to check that there is, indeed, an element $f(i) \in G_{[i]} \cong (G_{[i]})^{V_i}$ behaving as required; since $|G_{[i]}| \leq |GL(V_i)|$ is small, $f(i)$ can be found by brute force.

9. Assume that i is such that $(P_{1[i]})^{V_i}$ is reducible. (By (5.7c, 5.8c), there are exactly two proper $(P_{1V_i})^{V_i}$-invariant subspaces of V_i; they are totally isotropic or totally singular, and V_i is their direct sum. Moreover, $p > 2$.)

9.1. Use (5.13iv) to find the two proper $(P_{1[i]})^{V_i}$-invariant subspaces and the two proper $(P_{2[i]})^{V_i}$-invariant subspaces.

9.2. Find an element $g'' \in G_{[i]}$ sending the first of these decompositions of V_i to the second one. Also, find the stabilizer R_i in $G_{[i]} \cong (G_{[i]})^{V_i}$ of the second one.

(Use the first decomposition of V_i to find a basis of V_i behaving as in the proof of (5.13iv), and then do the same for the second decomposition. Let g'' map the first basis to the second one while inducing the identity on all V_j, $j \neq i$; it is easy to modify this g'', if needed, in order to make it lie in G and even in $G_{[i]}$ while still behaving as required in 9.2. Use (5.13iv) in order to find R_i. Here $R_i \trianglerighteq SL(d_i, F)$, where $d_i := \frac{1}{2}\dim V_i$. Note that the two proper $(P_{1V_i})^{V_i}$-invariant subspaces and the two proper $(P_{2V_i})^{V_i}$-invariant subspaces of V_i are in the same $G_{[i]}$-orbit by Sylow's Theorem.)

9.3. Find an element $g' \in G_{[i]} \cong (G_{[i]})^{V_i}$ conjugating $((P_1^{g''})_{V_i})^{V_i}$ to $(P_{2V_i})^{V_i}$, as follows.

If $(P_{1V_i})^{V_i} = (P_{1[i]})^{V_i}$ then apply (5.12ix) to R_i.

If $(P_{1V_i})^{V_i} > (P_{1[i]})^{V_i}$ then $p \mid |F| - 1$ and $\dim V_i = 2$ (cf. (5.9)).

Find $g' \in G_{[i]}$, conjugating $((P_{1[i]})^{g''})^{V_i}$ to $(P_{2[i]})^{V_i}$. (By Sylow's Theorem, g' exists, and it can be found by brute force since $|GL(V_i)|$ is small. Moreover, g' conjugates $((P_1^{g''})_{V_i})^{V_i}$ to $(P_{2V_i})^{V_i}$. Namely, for $j = 1, 2$, the centralizer of $(P_{j[i]})^{V_i}$ in $GL(V_i)$ is an abelian group, so that $(P_{j[i]})^{V_i}$ lies in exactly one Sylow p-subgroup of $GL(V_i)$.)

9.4. Let $f(i) = g''g' \in G_{[i]} \le G$. (Then $f(i)$ conjugates $(P_{1V_i})^{V_i}$ to $(P_{2V_i})^{V_i}$.)

10. Let $f := f(1) \cdots f(s)$ be the product of all of the elements $f(i)$ found in 8 and 9.

Output f. (This behaves as required, by the Note in 6.) □

SYLCONJSIMPLE is the only revision to be given here of the algorithms in [Ka2] for finding or conjugating Sylow subgroups. We turn next to SYLEMBED, an algorithm for embedding a given p-subgroup P of G (not Sylow in G) into a Sylow p-subgroup of G. By a reduction that is precisely as in [Ka2] (and hence omitted here), SYLEMBED is readily reduced to three related procedures SYLEMBED1, SYLEMBEDSIMPLE, and SYLEMBED1SIMPLE. We now present revised versions of these three.

SYLEMBED1.

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

Output: A p-subgroup of G properly containing P as a normal subgroup.

(These hypotheses state, among other things, that $G/P \cap M \trianglerighteq (M/P \cap M) \rtimes (P/P \cap M)$.)

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

Use (A.8) to find a set X' on which M acts such that $M^{X'}$ is simple, $(P \cap M)^{X'} = 1$, and $|X'| \le n$.

Use (A.4) to find $T := M_{(X')}$. (Then $T \ge P \cap M$ and $M/T \cong M^{X'}$.)

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

2. Let Y be the set of cosets of $M_{x'}$ in G. Determine the action of (the generators of) G on Y. (Note that $|Y| = |G : M| \cdot |M : M_{x'}| = |G/M| \cdot |X'| \le n^2$ since G/M is cyclic.)

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

(Note that $P \cap M \le K \le T \le M_{x'} < M$ and $P \cap M = P \cap M \cap K = P \cap K$.)

3. If G/K is a cyclic p-group then $M \leftarrow K$ and return to 1. (Observe that $|K| < |M|$ and, as just noted, $P \cap K = P \cap M$. In particular, this loop can occur at most $\log|G| + \log|M|$ times in the recursion for

SYLEMBED1. Note that this loop can turn a situation in which $G = PM$ into one in which $G > PM$; this is the reason why we did not assume that $G = PM$ in the input.)

We may now assume that G/K is noncyclic *if* it is a p-group.

4. Let $PM/M = \langle fM \rangle$ with $f \in P$. (Then $P = \langle P \cap M, f \rangle = \langle P \cap K, f \rangle$. Also, $\langle fK \rangle \cap (M/K) = 1$ since any power of f lying in M must lie in $P \cap M \leq K$.)

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

5.1. *Subcase* P is not Sylow in $K\langle f \rangle = KP$. Then $G \leftarrow K\langle f \rangle$, $M \leftarrow K$ and use recursion. (Here, $P \cap K \trianglelefteq K\langle f \rangle$, P lies in $K\langle f \rangle$ but is not Sylow, and $K \trianglelefteq K\langle f \rangle$ with $K\langle f \rangle/K$ a cyclic p-group. Also, $G > K\langle f \rangle$ by 3. Thus, recursion can be applied.)

5.2. *Subcase* P is Sylow in $K\langle f \rangle$. Find $m \in M - K$ with Km centralized by f. (Since M/K is a vector space over $GF(p)$ by (2.3), there is such a vector, and it is easily found using linear algebra.)

Find $k \in K$ such that $P^{mk} = P$. (Since $[m, K\langle f \rangle] \subseteq K$, m acts on $K\langle f \rangle$. Then P^m and P are conjugate by an element of $K\langle f \rangle$ and hence by an element of K. At this point we have available an algorithm for conjugating Sylow subgroups, so that m can be found in polynomial time.)

Let $\langle g' \rangle$ be the Sylow p-subgroup of $\langle mk \rangle$, and output $\langle P, g' \rangle$. (Since $m \in M - K$ we have $m \notin K\langle f \rangle$, so that $|K\langle f, m \rangle : K\langle f \rangle| = p$. Then g' is a p-element lying in $N_G(P) - P$. Thus, the output behaves as required.)

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

Suppose that $G > PM$.

6.1. If P is not Sylow in PM then $G \leftarrow PM$ and use recursion.

6.2. If P is Sylow in PM then let $g \in G - PM$; find $h \in PM$ with $(P^g)^h = P$; find the Sylow p-subgroup $\langle g' \rangle$ of $\langle gh \rangle$; and output $\langle P, g' \rangle$. (Since G/M is cyclic, $PM \lhd G$. Then P^g is Sylow in PM. Thus, we are proceeding exactly as at the end of 5.2.)

WLOG $G = PM$. (Now $G/P \cap M = (M/P \cap M) \rtimes (P/P \cap M)$, where $M/P \cap M$ has order divisible by p since $P/P \cap M$ is not Sylow in $G/P \cap M$. Moreover, $G = M\langle f \rangle$.)

7. If $p \nmid |M/T|$ then $G \leftarrow \langle K, f \rangle$ and $M \leftarrow K$, and use recursion. (Clearly $P \cap K = P \cap M \lhd K\langle f \rangle$, while $P = \langle P \cap K, f \rangle$. By (2.3), $p \nmid |M/K|$, so that P is not Sylow in $K\langle f \rangle$. Moreover, $K\langle f \rangle/K$ is a cyclic p-group while G/K is not, so that $K\langle f \rangle < G$. Thus, recursion can be applied.)

8. WLOG M/T is a nonabelian simple group *of order divisible by* p. Use (A.9) to find simple subgroups $S_1, \dots, S_l$ of M/K permuted transitively by $\langle f \rangle$ such that $M/K = S_1 \times \cdots \times S_l$. (See (2.3).)

9. Let $\langle f_1 K \rangle$ be the stabilizer in $\langle fK \rangle$ of S_1 (and hence the pointwise stabilizer of $\{S_1, \dots, S_l\}$ in $\langle fK \rangle$, since $\langle fK \rangle$ induces a regular group on $\{S_1, \dots, S_l\}$).

(Note that $S_1 \langle f_1 K \rangle$ acts faithfully on Y since G/K does.)

9.1. Apply SYLEMBED1SIMPLE (see below) to the p-subgroup $P_0 := \langle f_1 K \rangle$ of the group $G_0 := S_1 \langle f_1 K \rangle \le \mathrm{Sym}(Y)$ having the simple normal subgroup $M_0 := S_1$. (Note that SYLEMBED1SIMPLE can be used. For, P_0 is not Sylow in G_0 since $P_0 \cap M_0 = 1$ (cf. 4), while $p \mid |M/T|$ implies that $p \mid |S_1| = |M_0|$. Since $G_0 = P_0 M_0$ and G_0/M_0 is clearly cyclic, the requirements of SYLEMBED1SIMPLE are met.)

This produces a group $M_1 > K$ such that the following all hold:

$M_1/K < S_1$, $\langle f_1 K \rangle$ normalizes M_1/K, and $p \mid |M_1/K|$.

9.2. Find $M^* := \langle M_1^{\langle f \rangle} \rangle \le M$ and $G^* := M^* \langle f \rangle$.

(Then $G^* \triangleright M^*$. Also, $\langle fK \rangle$ acts transitively on $\{S_1, \dots, S_l\}$, with the stabilizer $\langle f_1 K \rangle$ of S_1 normalizing M_1/K. It follows that $M^*/K = M_1/K \times \cdots \times M_l/K$ with each factor M_i/K the unique $\langle fK \rangle$-image of M_1/K lying in the corresponding simple group S_i.)

9.3. Now $G^* \leftarrow G$ and $M^* \leftarrow M$, and use recursion. (Namely, $P = \langle P \cap K, f \rangle \le G^*$, so that $G^* = M^* \langle f \rangle = M^* P$. Also, $M^* \lhd G^*$, where $G^*/M^* = \langle fM^* \rangle$ is a cyclic p-group. Since $p \mid |M_1/K|$, P is not Sylow in G^*. Finally, $P \cap M^* = P \cap K \cap M^* = P \cap M \lhd G^*$. Thus, recursion can be applied.) □

Remark. We have just simultaneously handled all of the individual situations treated at greater length in the original version of Steps 9–11 in [Ka2].

SYLEMBEDSIMPLE.

Input: A p-subgroup P of a nonabelian simple group G that is not a Sylow subgroup of G.

Output: A proper subgroup H of G containing P such that P is not Sylow in H.

1. WLOG $|G| > n^8$ (as otherwise brute force can be used to test each element of $G - P$ until a p-element g is found in $G - P$ normalizing P, in which case output $\langle P, g \rangle$).

Use the Replacement Theorem 5.1 together with (5.12iii) to find a set Y such that $|Y| < n^2$ and either

(i) G is A_m and Y is an m-set on which G acts in the natural manner, or

(ii) G is a classical group, and Y is the set of 1-spaces of the vector space involved in the definition of G. In the latter case, also find all elements of the underlying vector space V (and field F), also of size $< n^2$; a group G^* of linear transformations of V preserving the form on V and projecting onto G (so that $G^*/Z(G^*) = G$) and such that $(G^*)' = G^*$; and the quadratic, bilinear, or hermitian form on V (if G is not $PSL(V)$) involved in the definition of G.

2. Suppose that G is an alternating group. (Here, $|Y| = m$ if G is A_m.)

If P is intransitive on Y then find and output the set-stabilizer G_Π of the set Π of P-orbits on Y. (Finding the set-stabilizer is straightforward. Since $N_G(P) \leq G_\Pi$ and there is a p-subgroup of G properly containing P as a normal subgroup, G_Π behaves as required.)

If P is transitive on Y, find $Z(P)$ using (A.7ii), and test each $z \in Z(P) - \{1\}$ as follows. Find the set Π of orbits of $\langle z \rangle$ on Y, find G_Π, and find $|G_\Pi|$. For some z, P will not be Sylow in G_Π (tested using (A.1)), in which case output G_Π.

(First note that $|Z(P)|$ divides $|Y|$ since P is transitive on Y, so there are fewer than $|Y|$ elements z to test. If Q is a Sylow p-subgroup of $N_G(P)$, then one of the tested elements z belongs to $P \cap Z(Q)$, and then G_Π behaves as required.)

3. From now on, WLOG G is a classical group. (In 1 we found the underlying vector space V and field F, as well as a group $G^* = (G^*)'$ of linear transformations preserving the form on V, if any, and projecting onto G.)

WLOG $P \neq 1$. (At this point we have available an algorithm for finding Sylow subgroups.)

Find the largest p-subgroup P^* of G^* projecting onto P (using (5.12iii)).

Then $G \leftarrow G^*$ and $P \leftarrow P^*$.

(Now G is a group of linear transformations of V, and P is a p-subgroup of G that contains a non-scalar element and is not a Sylow subgroup of G. We must find a proper subgroup H of G containing P such that P is not Sylow in H.)

4. *Case P is reducible.*

4.1. If V has characteristic p, find a 1-space $y \in Y$ fixed by P—and which is totally isotropic or totally singular if $G \neq SL(V)$; then use (A.1) to find and output G_y. (See (5.6).)

WLOG V does not have characteristic p.

4.2. Find the subspace $C_V(P)$ of fixed vectors of P. (This is a nonsingular subspace. For, we may assume that $G \neq SL(V)$. If $0 \neq v \in C_V(P)$ and $V \neq \langle v \rangle \perp v^{\perp}$, then $v \in v^{\perp}$ so that (by Maschke's Theorem) $V = v^{\perp} \oplus \langle u \rangle$ for some P-invariant 1-space $\langle u \rangle$; if $h \in P$ then $(u^h - u, v) = (u^h, v^h) - (u, v) = 0$, where $u^h - u \in \langle u \rangle$, so that $u, v \in C_V(P)$ while $V = \langle v, u \rangle \perp \langle v, u \rangle^{\perp}$. Continue in this manner in order to see that $C_V(P)$ is nonsingular.)

If $C_V(P) \neq 0$ then find and output $G_{C_V(P)}$. (Use (5.12iv).)

4.3. WLOG $C_V(P) = 0$.

Find a minimal nonsingular P-invariant subspace U and a P-invariant subspace U^+ such that $V = U \perp U^+$. (Use (5.12viii); recall the convention in Subsection 5A.)

4.4. If $U^+ = 0$, find a P-irreducible subspace W of V.

(Use (5.12viii). We will need to know that W is totally isotropic or totally singular. First note that, in the present situation, P is reducible but there is no proper nonsingular P-invariant subspace of V. Embed P in a Sylow p-subgroup Q of G. Then there is no proper nonsingular Q-invariant subspace of V. By (5.7c) this implies that V is equipped with a form. Moreover, if $V = V_1 \perp \cdots \perp V_s$ is the decomposition (5.7) corresponding to Q then P is transitive on $\{V_1, \ldots, V_s\}$, by the minimality of $U = V$. It follows that $p > 2$ and W is the direct sum of totally isotropic or totally singular subspaces, one in each V_i (cf. (5.7c), (5.8c)). This proves that W is totally isotropic or totally singular, as asserted.)

Find and output G_W, using (5.12iv). (We just saw that G_W contains a Sylow p-subgroup of G.)

4.5. WLOG $U^+ \neq 0$.

Find G_U using (5.12iv).

If P is not Sylow in G_U (tested using (A.1)) then output G_U.

WLOG P is Sylow in G_U.

4.6. Find minimal nonsingular P-invariant subspaces $U_1, \ldots, U_l$ such that $V = U_1 \perp \cdots \perp U_l$, using (5.12viii).

WLOG P is Sylow in G_{U_i} for each i. (In 4.5 let U range through $\{U_1, \ldots, U_l\}$.)

4.7. Find and output $G_{\{U_1, \ldots, U_l\}}$, using (5.12vi).

(The argument in (5.9) shows that, if $\dim U_j \leq \dim U_i$, then $C_P(U_j)^{U_i} \neq 1$, so that the P-modules U_j are pairwise nonisomorphic. In particular, $N_G(P) \leq G_{\{U_1, \ldots, U_l\}}$. Since P is not Sylow in G it is not Sylow in $N_G(P)$, and hence also not in $G_{\{U_1, \ldots, U_l\}}$. Thus, $G_{\{U_1, \ldots, U_l\}}$ behaves as required.)

5. WLOG *P is irreducible on V.*

Find the set Ω of all nonsingular subspaces V_1 of V such that

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

(ii) Either $p > 2$ and V_1 is a minimal nonsingular h-invariant subspace for some $h \in P - \{1\}$, or $p = 2 = \dim V_1$.

Comments. It is easy to use (5.7) in order to check that $|P| = O(|V|^3)$. Hence, we can search through P for a choice of an element h one of whose minimal nonsingular h-invariant subspaces behaves as in (i). (These minimal nonsingular h-invariant subspaces can all be found using (5.12viii).) Note that it is not necessary to find all of V_1^P once two non-perpendicular members are obtained. If $p = 2$ then we can search through all of the subspaces of V of dimension 2 in order to test condition (i). Thus, Ω can be found in polynomial time.

It remains to show that $\Omega \neq \varnothing$. Consider a Sylow p-subgroup of G containing P, and let $\{V_1, \dots, V_s\}$ be the associated family as in (5.7). We claim that this subspace V_1 lies in Ω.

Since P is irreducible it is transitive on $\{V_1, \dots, V_s\}$. Moreover, P_{V_1} is irreducible on V_1. (For, if $U \subseteq V_1$ is a P_{V_1}-invariant subspace and if $U^g \subseteq V_1$, $g \in P$, then $V_1^g = V_1$, so that $g \in P_{V_1}$ and hence $U^g = U$. Then the P-invariant subspace $\langle U^P \rangle$ is the direct sum of s images of U under the action of P. Since P is irreducible it follows that $U = V_1$.)

If $p = 2$ then $\dim V_1 = 2$ by (5.7c2), so that $V_1^P = \{V_1, \dots, V_s\}$ and hence $V_1 \in \Omega$.

Let $p > 2$. Then $(P_1)_{V_1}$ induces a cyclic group on V_1 by (5.7c1). Let $h \in P_{V_1}$ be such that h^{V_1} generates $(P_{V_1})^{V_1}$. Then V_1 is a minimal nonsingular h-invariant subspace behaving as in (i).

This proves that the required type of decomposition exists and can be found.

(N.B.—Condition 5(ii) is a slight modification of the corresponding one used in [Ka2].)

6. For each $V_1 \in \Omega$, decompose $V = V_1 \perp \cdots \perp V_l$ as in 5. Find $H := G_{\{V_1, \dots, V_l\}}$ using (5.12vi). Test whether P is Sylow in H. If it is not, and if $l > 1$, output H. (As already noted in 5, for some choice of $V_1 \in \Omega$ the group H contains a Sylow p-subgroup of G.)

7. WLOG $l = 1$ for every $V_1 \in \Omega$. (We saw in 5 that some $V_1 \in \Omega$ arises from a decomposition (5.7) of V. Thus, we will now be assuming that there is only a single summand in (5.7). By (5.7c), $p \neq 2$ since $\dim V > 2$, and P is cyclic.)

Let $P = \langle f \rangle$.

Find a Sylow subgroup $\langle h \rangle$ of G. (At this point we have available an algorithm for finding Sylow subgroups.)

8. Use (5.12ix) 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, (5.12ix) applies.) Output $\langle h \rangle^g$. □

SYLEMBED1SIMPLE.

Input: A cyclic p-subgroup P of G; $M \lhd G$ with M nonabelian and simple of order divisible by p, $G = PM$, and $P \cap M = 1$.

Output: A proper subgroup of M normalized by P and having order divisible by p.

1. WLOG $|M| > n^8$ (as otherwise brute force can be used to find an element of M of order p that is centralized by P).

Let $P = \langle t \rangle$.

Use the Replacement Theorem 5.1 to find a set Y such that $|Y| < n^2$ and either

(i) M is A_m and Y is an m-set on which M acts in the natural manner, or

(ii) M is a classical group, and Y is the set of 1-spaces of the vector space V involved in the definition of M. In the latter case, also find the underlying vector space V (and field F), also of size $< n^2$; and the quadratic, bilinear, or hermitian form on V (if M is not $PSL(V)$) involved in the definition of M.

2. Find $C_G(M)$ (using (A.7ii)).

Find the set Π of orbits of $C_G(M)$ on X. (Note that G^Π, M^Π, and P^Π satisfy the requirements of an input for SYLEMBED1SIMPLE. For otherwise $M^\Pi = 1$ by simplicity, so that $M = M_{(\Pi)}$. Then M has the same orbits as the cyclic group $C_G(M)$ it centralizes, which is absurd.)

If $C_G(M) \neq 1$, recursively find a proper subgroup $\overline{H}$ of M^Π normalized by P^Π and having order divisible by p. Output the preimage H of $\overline{H}$ in M (using (A.4)).

WLOG $C_G(M) = 1$.

(Now $G/M \cong P$ is a group of *outer* automorphisms of M.)

3. Let $y \in Y$.

3.1. Find M_y (using (A.1)).

3.2. Find the set Y' of all cosets of M_y in G. (Here $|Y'| = |G : M| \cdot |M : M_y| \leq n \cdot n$; in fact, $|Y'| = |Y|$ or $2|Y|$ by the following Note.)

3.3. Determine the action of (the generators of) G on Y'.

Note. G acts faithfully on Y', since the kernel of the action is a normal subgroup of the simple group M. In effect, all work will now take place inside Sym(Y'). Since $|M| > n^8$ we have $|Y| > 6$, so that either $Y' = Y$ or we are in case (ii) of Step 1 and $Y' - Y$ can be identified with the set of hyperplanes of V (cf. (5.4) and (5.5)).

4. Suppose that M is A_m. (Here, $|Y| = m$.)

Then $Y = Y'$ and $G^Y = A_m$ or S_m (by the above Note). Moreover, $|c| = p = 2$ (by 2).

Clearly $P^Y = \langle t^Y \rangle$ normalizes $\langle c \rangle$ for any nontrivial cycle c of t^Y. Let d be the product cc' of c with either another 2-cycle c' of t^Y or (if $t^Y = c$) a transposition c' fixing every point of Y moved by t^Y, and output the preimage of $\langle d \rangle$.

5. From now on, WLOG M is a classical group. In 1 we found the underlying vector space V, set Y of 1-spaces, field F, and form (if any) associated with M. We will think of subspaces of V as subsets of Y (i.e., projectively). In 3 we found a set Y' on which G also acts, where if $Y' \neq Y$ then $Y' - Y$ can be thought of as the set of hyperplanes of V.

6. If $t^2 = 1$ then take any $y \in Y$, find $y' := y^t \in Y'$, and then use (A.1) to find and output $M_{y,y'}$. (It is easy to see that this group has even order.)

WLOG $t^2 \neq 1$. In particular, every proper subgroup of P acts on Y.

7. Suppose that a Sylow p-subgroup of M is cyclic and fixes no 1-space (i.e., member of Y). (This can be tested by finding such a Sylow subgroup using SYLFIND, but it is really a simple arithmetic question by (5.8a). Note that the hypotheses of 7 imply that $p \neq 2$, by (5.7), and hence $P \leq P\Gamma L(V)$ by (5.4) and (5.5).)

7.1. Let P_1 be the subgroup of order p in P.

Let Y_1 be the set of fixed points of P_1 on Y.

(In order to see the structure Y_1 inherits, note that our present hypothesis that M has cyclic Sylow p-subgroups, combined with (5.7), implies that $MP_1 = M\langle \theta \rangle$ for a field automorphism θ of M of order p. If Q is a Sylow p-subgroup of M normalized by P then we may assume that $QP_1 = Q\langle \theta \rangle$. Using the description of Q and $Q\langle \theta \rangle$ given in (5.11iii) or (5.11iv) (compare [Ka2, Section 15]), it is easy to check that P_1 is a group of field automorphisms. Thus, Y_1 is the set of 1-spaces of a vector space V_1 over a subfield F_1 of the original field F, and $\dim_{F_1} V_1 = \dim_F V$. Moreover, if V is equipped with a form then so is V_1.)

7.2. Find generators for the subgroup H of $C_M(P_1)$ generated by all the r-elements of $C_M(P_1)$, where r is the prime dividing $|F|$. (If M is $PSL(V)$ then H is generated by all transvections of V_1, all of which can be easily written down. If there is a form on V_1 then H is found exactly as in (5.13iv) or (5.14). In fact, the method in (5.13iv) or (5.14) will find all of $C_M(P_1)$.)

Output H. (For, H is clearly normalized by P.)

8. WLOG we are not in the situation hypothesized at the start of 7.

8.1. For each $y \in Y$ (i.e., 1-space of V) find $W := \langle y^{P \cap P\Gamma L(V)} \rangle$ (using (5.12i)).

(Recall that $P \cap P\Gamma L(V)$ acts on Y, and that $P \cap P\Gamma L(V) = P$ except perhaps if $M = PSL(V)$ and $p = 2$.)

8.2. Find all such subspaces $W \neq V$ that are either nonsingular or satisfy $(W, W) = 0$ (tested using the form on V.)

If V is orthogonal of characteristic 2 and if $(W, W) = 0$ then also find $W^0 := \{w \in W | w \text{ is singular}\}$. (This is a subspace of codimension 0 or 1 in W.)

8.3. For each such W find M_W or M_{W^0} using (5.12iv). (Either W is nonsingular, or else W or W^0 is totally isotropic or totally singular.)

8.4. If P acts on Y, then for each such $W \neq V$ test whether $W^P = W$; and if so, test whether p divides $|M_W|$ or $|M_{W^0}|$.

Output a group M_W or M_{W^0} of order divisible by p.

8.5. If P does not act on Y then choose W in 8.2 of minimal dimension, find $(M_W)^t$; and find the shortest orbit W^* of $(M_W)^t$ on Y. (Since t interchanges Y and $Y - Y'$, W^* is a subspace of V.)

Find and output M_{W,W^*}. (By the minimality of dim W, either $V = W \oplus W^*$ or $W \subseteq W^*$. Use (5.12iv, vi) to find M_{W,W^*}. This is clearly a group of even order normalized by P.)

Comments. All computations run in polynomial time. We must show that y can be chosen in 8.1 so as to make 8.4 or 8.5 output correctly. This is clear in the case of 8.5, so we may assume that G acts on Y.

If $p \mid |F|$ then P fixes some 1-space y, in fact a totally isotropic or totally singular 1-space if V is equipped with a form (cf. (5.6)). For this y, $p \mid |M_W|$.

If $p = 2$ then M_W and M_{W^0} are proper subgroups of M normalized by P, and it is easy to see that they have even order.

Now assume that $p \nmid |F|$ and $p \neq 2$. Let Q be a Sylow p-subgroup of M normalized by P, and let $V = V_1 \perp \cdots \perp V_s$ be the corresponding decomposition of V in (5.7). Then $s > 1$ (this is, in effect, the first sentence in 8).

Let $W_1 \subseteq V_1$ be a P_{V_1}-irreducible subspace. Consider any $y \in W_1$ and let $W = \langle y^P \rangle$. If P fixes V_1 then it normalizes the nontrivial subgroup $C_{Q^*}(V_1)$ of M_W^* (where M^* and Q^* are linear groups defined as for (5.7), and $C_{Q^*}(V_1) \neq 1$ by (5.9)). Thus, we may assume that P moves V_1.

Since PQ acts on $\{V_1, \ldots, V_s\}$ by (5.11i), each image of y under an element $g \in P$ lies in some member of $\{V_1, \ldots, V_s\}$; and if $y^g \in V_1$ then $g \in P_{V_1}$ so that $y^g \in W_1$. Then the various distinct images $W_1, \ldots, W_{s'}$, say, of W_1 under the elements of P lie in different members of Ω, so that

$W = W_1 \perp \cdots \perp W_{s'}$. Since $p \neq 2$ it follows that the W_i are all isometric. (N.B. If $p = 2$ and V is orthogonal then there are automorphisms of M preserving the form on V projectively and sending each nonsingular subspace of odd dimension to a subspace not isometric to the original one. This is why we handled the case $p = 2$ separately.)

Clearly s' is a power of p; and $s' > 1$ since P moves V_1. Thus, there is a linear isometry of W acting on $\{W_1, \dots, W_{s'}\}$ and inducing a permutation of order p there. By Witt's Theorem [Di, pp. 21, 36] this can be extended to an element of $\mathrm{Isom}(V)$, after which it is easy to see that there is also an element of M acting on $\{W_1, \dots, W_{s'}\}$ as a permutation of order p. Thus, $p \,||M_W|$, while $M_W < M$. In the case of orthogonal groups of characteristic 2, if $(W, W) = 0$ then $M_W \leq M_{W^0}$, so that $p\,||M_{W^0}|$. Consequently, at least for the stated choice of y, 8.4 outputs as required.

```
9. WLOG $V = \langle y^{P \cap P\Gamma L(V)} \rangle$ for *each* $y \in Y$.
  9.1. For each $y \in Y$, and for each subgroup $P_0 < P$,
         find $W := \langle y^{P_0} \rangle$ (here $P_0$ acts on $Y$ by 6),
         successively determine members of $W^{P \cap P\Gamma L(V)}$, discarding $y$
       if two members are non-perpendicular, and
         if $\{W_1, \dots, W_k\} := W^{P \cap P\Gamma L(V)}$ consists of pairwise perpen-
       dicular subspaces (so that $V = W_1 \perp \cdots \perp W_k$, since $V =$
       $\langle W^{P \cap P\Gamma L(V)} \rangle$), then find $M_{\{W_1, \dots, W_k\}}$ using (5.12vi).
  9.2. For some choice of $y$ and $P_0$, the following all hold: $V = W_1$
       $\perp \cdots \perp W_k$, $k > 1$, $P$ normalizes $M_{\{W_1, \dots, W_k\}}$, and
       $p\,||M_{\{W_1, \dots, W_k\}}|$.
         Output $M_{\{W_1, \dots, W_k\}}$.
```

Comments. All subgroups of the cyclic group P are readily found. At most $\dim V$ members of $W^{P \cap P\Gamma L(V)}$ can be pairwise perpendicular, so that each test performed in 9.1 requires polynomial time. We must show that 9.2 actually produces an output.

Let Q be a Sylow p-subgroup of M normalized by P. Let $V = V_1 \perp \cdots \perp V_s$ be the canonical decomposition of V associated with Q in (5.7), and write $\Omega := \{V_1, \dots, V_s\}$. Then QP normalizes M_Ω by (5.11). Also, $s > 1$ (by the first sentence of 8).

Let $P_0 := P_{V_1}$, so that $P_0 < P$ (since $V = \langle V_1^{P \cap P\Gamma L(V)} \rangle$ by the first sentence in 9) and hence $P_0 \leq P \cap P\Gamma L(V)$; and let y be any 1-space of V_1. Precisely as in 8, the various distinct images of $W := \langle y^{P_0} \rangle$ under $P \cap P\Gamma L(V)$ lie in different members of Ω. Moreover, $\langle W^{P \cap P\Gamma L(V)} \rangle = \langle \langle y^{P_0} \rangle^{P \cap P\Gamma L(V)} \rangle = V$. Thus, the distinct images of W are precisely the members of Ω. Consequently, for this choice of P_0 and y the procedure does indeed output a subgroup behaving as required in 9.2. □

The preceding was an elaboration of [Ka2] assisted by (5.9). It may seem to be a lot of effort using ad hoc arguments instead of merely applying the algorithms sketched in (5.15)–(5.18). However, before applying these it is perhaps worth mentioning that a more complete version of (5.15), written out in greater detail, would involve rewriting portions of [GoLy] using the methods just employed in SYLEMBEDSIMPLE and SYLEMBED1SIMPLE. With this proviso, the following is a "short" combined algorithm replacing both of those procedures.

SYLEMBEDSIMPLE + SYLEMBED1SIMPLE.

Input: A cyclic p-subgroup P of G; $M \trianglelefteq G$ with M nonabelian and simple of order divisible by p such that $G = PM$ and P is not Sylow in G.

Output: A proper subgroup H of M normalized by P such that P is not a Sylow subgroup of PH.

WLOG $|M| > n^8$, in which case apply (5.1) in order to obtain first a new set Y on which M acts and then a set Y' on which G acts such that $|Y'| \leq 2|Y| < 2n^2$ (cf. Step 3 of SYLEMBED1SIMPLE). In particular, M is now an alternating or classical group. Let R be the subgroup of order p in P. Then (5.15)–(5.18) find a proper subgroup H of M containing $C_M(R)$ and normalized by $N_G(R)$ (where $H = C_M(R)$ except in (5.17)). Output H. (Namely, $P \leq N_G(R)$ normalizes H, so that PH is a subgroup containing $C_{PM}(R) = C_G(R)$. Here, $C_G(R)$ contains a Sylow p-subgroup of $N_G(P)$. Since P is not Sylow in G it is not Sylow in $N_G(P)$, and hence also not in PH. Thus, H behaves as required.) □

7. Closing Remarks

The proofs in this paper relied heavily on the version of the Frattini argument contained in (A.12). This enabled us to approximate the desired normalizers. However, once (1.1) and (1.2) have been proved, these approximations can be made much more precise.

Corollary 7.1. *There is a polynomial-time algorithm which, when given a Sylow subgroup P of $M \trianglelefteq G \leq S_n$, finds $N_G(P)$.*

Corollary 7.2. *There is a polynomial-time algorithm which, when given a Hall subgroup P of a solvable normal subgroup M of $G \leq S_n$, finds $N_G(P)$.*

Proof of (7.1) *and* (7.2). Find $N_M(P)$ using (1.1) or (1.2). Find $D \leq N_G(P)$ such that $G = DM$, using (A.12). Then $DN_M(P)$ is the desired normalizer. □

The methods used here yield much more in the case of a solvable group G. For example, system normalizers and Carter subgroups can be found, and one such subgroup can be conjugated to another one, in polynomial time.

REFERENCES

[Ba] L. BABAI, On the length of subgroup chains in the symmetric group, *Comm. Algebra* **14** (1986), 1729–1736.

[BKL] L. BABAI, W. M. KANTOR, AND E. M. LUKS, Computational complexity and the classification of finite simple groups, *in* "Proceedings 24th IEEE Sympos. Found. Comput. Sci., 1983, pp. 162–171.

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

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

[FHL] M. FURST, J. HOPCROFT AND E. LUKS, Polynomial-time algorithms for permutation groups, *in* "Proceedings 21st IEEE Sympos. Found. Comput. Sci., 1980," pp. 36–41.

[Gor] D. GORENSTEIN, "Finite Groups," Harper & Row, New York, 1968.

[GoLy] D. GORENSTEIN AND R. LYONS, The local structure of finite groups of characteristic 2 type, *AMS Mem.* **276** (1983).

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

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

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

[Ka3] W. M. KANTOR, Algorithms for Sylow p-subgroups and solvable groups, *in* "Computers in Algebra" (Proc. Conf. Chicago 1985), pp. 77–90, Dekker, New York, 1988.

[KT] W. M. KANTOR AND D. E. TAYLOR, Polynomial-time versions of Sylow's theorem, *J. Algorithms* **9** (1988), 1–17.

[Lu1] E. LUKS, Isomorphism of graphs of bounded valence can be tested in polynomial time, *J. Comput. System Sci.* **25** (1982), 42–65.

[Lu2] E. LUKS, Computing the composition factors of a permutation group in polynomial time, *Combinatorica* **7** (1987), 87–99.

[Lu3] E. LUKS, unpublished.

[Ro1] L. RÓNYAI, "Zero divisors and invariant subspaces," Technical Report CIS-TR 85-12, Department of Computer and Information Science, University of Oregon, 1985.

[Ro2] L. RÓNYAI, Simple algebras are difficult, *in* "Proceedings ACM Sympos. Theory of Comput., 1987," pp. 398–408.

[Si] C. C. SIMS, Some group-theoretic algorithms, "Lect. Notes in Math., Vol. 697," pp. 108–124, Springer-Verlag, Berlin/Göttingen/Heidelberg, 1978.

[We] A. WEIR, A Sylow p-subgroup of the classical groups over finite fields with characteristic prime to p, *Proc. Amer. Math. Soc.* **6** (1955), 529–533.