JOURNAL OF ALGORITHMS 9, 1–17 (1988)

Polynomial-Time Versions of Sylow's Theorem

W. M. KANTOR*

University of Oregon, Eugene, Oregon 97403

AND

D. E. TAYLOR

University of Sydney, Sydney, N.S.W. 2006, Australia

Received December 28, 1983

Let G be a subgroup of S_n, given in terms of a generating set of permutations, and let p be a prime divisor of $|G|$. If G is solvable—and, more generally, if the nonabelian composition factors of G are suitably restricted—it is shown that the following can be found in polynomial time: a Sylow p-subgroup of G containing a given p-subgroup, and an element of G conjugating a given Sylow p-subgroup to another. Similar results are proved for Hall subgroups of solvable groups and a version of the Schur–Zassenhaus theorem is obtained. © 1988 Academic Press, Inc.

1. INTRODUCTION

While subgroups of the symmetric group S_n can be large, each such subgroup can be described (in polynomial time) in terms of a small number of generating permutations. It is natural to ask what portions of finite group theory have polynomial-time versions. A number of such algorithms are known [1, 4, 6, 7, 8, 9, 11]. For example, given a permutation group G, the following can be determined in polynomial time: $|G|$, the pointwise stabilizer of any given subset, all orbits of G, the derived series of G, a composition series for G, and an element whose order is any given prime divisor of $|G|$.

Sylow's theorem is one of the fundamental results concerning finite groups. It is presently unknown whether or not Sylow subgroups can be found in polynomial time. An elementary result in this direction is given in [8]. In [7] a sledgehammer approach is used to find a Sylow subgroup of G

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

0196-6774/88 $3.00

when it is known that G is simple. In this paper we will obtain other versions of Sylow's theorem as well as related group-theoretic theorems.

Our main results are as follows. Assume that all nonabelian composition factors of G are suitably bounded (as explained in Section 3).

(1) If (generators for) a p-subgroup P of G are given, then (generators for) a Sylow p-subgroup containing P can be found in polynomial time (Section 4).

(2) If Sylow p-subgroups P_1 and P_2 of G are given, then an element of G can be found conjugating P_1 to P_2 (Section 4).

(3) A version of the Schur–Zassenhaus theorem is proved (Section 6).

(4) Analogues of (1) and (2) are proved for Hall subgroups of solvable groups (Section 5).

The proofs of these results turn out to be surprisingly elementary. Of fundamental importance is the fact, outlined in [8] on the basis of [3], that in polynomial time it is possible to find the intersection of G (restricted as above) with any coset of any subgroup of S_n. The principal group-theoretic idea in our proofs involves the so-called Frattini argument—especially its proof (see (G.2) in Section 2).

Section 2 contains some elementary group-theoretic preliminaries, while Section 3 lists the known polynomial-time group-theoretic algorithms that we use. This list can be viewed almost as a collection of axioms restricting our ability to do traditional group theory.

Section 4 contains algorithmic versions of Sylow's theorem. It is worth noting that, on the one hand, we make use of Sylow's theorem in proving the validity of our algorithms but, on the other hand, standard proofs of Sylow's theorem do not lead to polynomial-time algorithms. For example, in (1) above we do not know whether or not the normalizer $N_G(P)$ of a p-group P can be found in polynomial time, so that we cannot simply search for a p-element of $N_G(P) - P$.

Sections 5 and 6 deal with solvable groups and the Schur–Zassenhaus theorem, respectively. In Section 7 we indicate further variations on Sylow's theorem of a more technical nature. In particular, we observe that the problem of finding Sylow subgroups of arbitrary subgroups of S_n is polynomial-time reducible to the *intersection problem*.

2. Preliminaries I: Group Theory

This section begins with a description of some of the notation we use throughout the paper and concludes with a collection of elementary results on permutation groups. Further details can be found in [5 or 12].

Let X be a finite set and consider the *symmetric group* $\mathrm{Sym}(X)$ of all permutations of X. The letter n will always denote $|X|$, and we will also denote $\mathrm{Sym}(X)$ by S_n.

Suppose that G is a subgroup of $\mathrm{Sym}(X)$. The letter x will always denote an element of X with *stabilizer* G_x and *orbit* $x^G = \{x^g | g \in G\}$. Recall that $|G : G_x| = |x^G|$.

If Y is any subset of X and $g \in G$, then Y^g is the set $\{y^g | y \in Y\}$. The *setwise stabilizer* of Y is $G_Y = \{g \in G | Y^g = Y\}$ and its *pointwise stabilizer* is $G_{(Y)} = \{g \in G | y^g = y$ for all $y \in Y\}$. If $G = G_Y$ then Y is said to be *G-invariant*, and in this case each element $g \in G$ restricts to a permutation $g^Y \in \mathrm{Sym}(Y)$. Define G^Y to be the group $\{g^Y | g \in G\}$, and notice that G^Y is isomorphic to $G/G_{(Y)}$. If $G_{(Y)} = 1$, we say that G acts *faithfully* on Y.

Since G acts on the set of subsets of X, the groups G_Σ, $G_{(\Sigma)}$ and $(G_\Sigma)^\Sigma$ are well-defined whenever Σ is a set of subsets of X. For example, $G_{(\Sigma)} = \{g \in G | Y^g = Y$ for all $Y \in \Sigma\}$, and if $g \in G_\Sigma$, then g^Σ is the element of $(G_\Sigma)^\Sigma$ induced by g.

The following elementary results will be used frequently throughout the paper. Any notation not already explained can be found in [5, 12] or any book on basic group theory:

(G.1) *Suppose that* $G \leq \mathrm{Sym}(X)$ *and that a subgroup* H *of* G *is transitive on an orbit* x^G. *Then* $G = G_x H$.

Proof. If $g \in G$ then, for some $h \in H$, $x^g = x^h$ and consequently $gh^{-1} \in G_x$. Thus $g \in G_x H$, as required.

(G.2) (The Frattini argument.) *If* K *is a normal subgroup of a group* G *and if* P *is a Sylow* p*-subgroup of* K, *then* $G = N_G(P)K = KN_G(P)$.

Proof. Let G act by conjugation on the set X of all Sylow p-subgroups of K. The stabilizer of P in G is $N_G(P)$, so the result follows from (G.1).

(G.3) *Let* Σ *be the set of orbits of a subgroup* K *of* $\mathrm{Sym}(X)$. *Then* $N_{\mathrm{Sym}(X)}(K) \leq \mathrm{Sym}(X)_\Sigma$.

Proof. If $g \in N_{\mathrm{Sym}(X)}(K)$, then for all $Y \in \Sigma$ and all $k \in K$, $(Y^g)^h = (Y^{ghg^{-1}})^g = Y^g$. Thus Y^g is K-invariant and contains no proper K-invariant subsets. That is, $Y^g \in \Sigma$ whenever $Y \in \Sigma$. Thus $g \in \mathrm{Sym}(X)_\Sigma$.

(G.4) *Let* $S, L \leq G \leq \mathrm{Sym}(X)$, *where* $(|S|, |L|) = 1$. *Let* Σ *and* Λ *be the sets of orbits of* S *and* L, *respectively. If* $G = G_\Sigma = G_\Lambda$, *then* (i) $G_{(\Sigma)} \cap G_{(\Lambda)} = 1$, *and* (ii) *G acts faithfully on* $\Sigma \cup \Lambda$.

Proof. Let $Y \in \Sigma$ and $Z \in \Lambda$, where $Y \cap Z \neq \varnothing$. Then $Y \cap Z$ is a block of each of the transitive groups S^Y and L^Z. Consequently, $|Y \cap Z|$ divides $(|S|, |L|) = 1$. This proves that each member of Σ has at most one element of X in common with each member of Λ. Thus, each element of X is fixed by $G_{(\Sigma)} \cap G_{(\Lambda)}$. This proves (i) and then (ii) is immediate.

(G.5) *If $Q \leq G \leq \mathrm{Sym}(X)$, where Q is a q-subgroup and $Q \leq Z(G)$, and if Σ is the set of orbits of Q on X, then $G_{(\Sigma)}$ is a q-group.*

Proof. Apply (G.4) to $S = Q$ and any Sylow p-subgroup L of $G_{(\Sigma)}$, where $p \neq q$. Then $L \leq G_{(\Sigma)} \cap G_{(\Lambda)} = 1$.

Of course (G.5) is very easy to prove directly.

For the next result, recall that a *composition series* for G is a sequence $G = G_0 \rhd G_1 \rhd \cdots \rhd G_k = 1$ such that, for $1 \leq i \leq k$, G_{i-1}/G_i is a simple group. The *normal closure* of a subset S of G is the group $\langle S^G \rangle = \langle S^g | g \in G \rangle$ generated by the conjugates $S^g = g^{-1}Sg$ of S in G; it is the smallest normal subgroup of G that contains S.

(G.6) *Suppose that $G = G_0 \rhd G_1 \rhd \cdots \rhd G_k = 1$ is a composition series for G. If G_{k-1} is cyclic of order q then $\langle G_{k-1}^G \rangle$ is a q-group, otherwise G_{k-1} is a nonabelian simple group and $\langle G_{k-1}^G \rangle$ is the direct product of the conjugates of G_{k-1} in G.*

Proof. Suppose that G_{k-1} is cyclic of order q. By induction the normal closure Q of G_{k-1} in G_1 is a q-group. Then for all $g \in G$, Q^g is a normal q-subgroup of G_1. It follows that $\langle G_{k-1}^G \rangle = \langle Q^G \rangle$ is also a q-group.

Now suppose that G_{k-1} is nonabelian and let G act by conjugation on the set X of conjugates of G_{k-1} in G. If Y is an orbit of G_1, then by induction $\langle Y \rangle$ is the direct product of the members of Y. If Y_1 and Y_2 are distinct orbits of G_1, it follows from [5, Theorem 2.1.5] that $\langle Y_1 \rangle \cap \langle Y_2 \rangle = 1$ and hence that $\langle Y_1, Y_2 \rangle = \langle Y_1 \rangle \times \langle Y_2 \rangle$. This shows that each member of X is normal in $\langle X \rangle$. Since X consists of nonabelian simple groups it follows from [5, *ibid.*] that $\langle X \rangle$ is the direct product of the members of X, as required.

(G.7) *Suppose that $G \leq S_n$ and that $G_1 < G_2 < \cdots < G_m = G$ is a sequence of distinct subgroups of G. Then $m < n^2$.*

Proof. For $1 \leq i < m$, $|G_{i+1} : G_i| \geq 2$, so $m < n \log_2 n < n^2$.

Remarks. (i) A more detailed analysis has been carried out in [2] and shows that $m < 2n$.

(ii) This simple result is extremely useful in later sections. All of our algorithms involve reductions that replace the given group by a proper subgroup and then proceed by recursion to this smaller group. The result just proved shows that the depth of recursion is bounded above by n^2.

3. Preliminaries II: Algorithms

In this section we present various known algorithms which, when applied to a "suitably described" permutation group G acting on a set X of size n, produce subgroups or elements of G. These will be the building blocks of the algorithms of later sections.

The input for an algorithm will usually include a set of generators for G, given as a set Γ of permutations of X. By means of Sims' algorithm [11, 4, 6] we can use Γ to find a new set, of at most n^2 permutations, that also generate G. This can be done in a time that is polynomial in $|\Gamma|$ and n. From now on we will assume that this reduction has been carried out, so that $G = \langle \Gamma \rangle$, where $|\Gamma| \leq n^2$. This is the sense in which we regard G as being "suitably described."

Most of the following algorithms can be described by saying that there is a procedure that "finds" a subgroup H satisfying some condition (in time that is polynomial in n). By "finding" H we mean that the algorithm produces generators for H that are realized as permutations of the underlying set.

Our algorithms depend on the main result of [3]. Consequently, we will eventually need to impose restrictions on the group G. For any positive integer b, let $\mathrm{CF}(b)$ denote the class of finite groups each of whose composition factors is either

(i) cyclic,

(ii) an alternating group A_k for $k \leq b$,

(iii) a classical group of dimension at most b,

(iv) an exceptional group of Lie type, or

(v) a nonabelian simple group of order at most b.

It is shown in [3] that *there is a constant $c = c(b)$ such that, for any primitive group G of degree n in the class* $\mathrm{CF}(b)$, $|G| \leq n^c$. Notice that for all b, $\mathrm{CF}(b)$ includes all solvable groups.

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

(A.1) *Given $Y \subseteq X$, find $G_{(Y)}$ and $|G_{(Y)}|$.*

This is a special case of Sims' algorithm. Details can be found in [4, 6, or 11].

(A.2) *Find all the orbits of G on X.*

(A.3) [1] *Given that* $G \neq 1$ *is transitive on* X, *find a block system* $\Sigma \neq \{X\}$ *such that* G^{Σ} *is primitive.*

(A.4) *Given a G-invariant partition* Π, *find* $G_{(\Pi)}$.
This follows easily from (A.1).

(A.5) [4] *Given a nonempty subset* S *of* G, *find the normal closure* $\langle S^G \rangle$.

(A.6) [4] *Find the derived series of* G.

(A.7) [9] *Given a subgroup* H *of* $\mathrm{Sym}(X)$ *normalized by* G, *find* $C_G(H)$. *In particular, find* $Z(G)$.

(A.8) *Given that* G *is in* $\mathrm{CF}(b)$, *given any subgroup* $H \leq \mathrm{Sym}(X)$ *and given any* $f \in \mathrm{Sym}(X)$, *find* $G \cap Hf$.

Remarks. (i) To "find" $G \cap Hf$ means to decide whether or not this set is empty and, if it is nonempty, to construct generators for $G \cap H$ and an element f' such that $G \cap Hf = (G \cap H)f'$.

(ii) The main result of [3] shows that the algorithm beginning on page 61 of [8] can be used to find $G \cap Hf$.

The following constructions are all straightforward consequences of (A.8).

(A.9) *Given that* G *is in* $\mathrm{CF}(b)$ *and that* Y *is a subset of* X, *find* G_Y. To do this, find $\mathrm{Sym}(X)_Y$ and then use (A.8) to find $G \cap \mathrm{Sym}(X)_Y$. Observe that $G_Y = G \cap \mathrm{Sym}(X)_Y$.

(A.10) *Given that* G *is in* $\mathrm{CF}(b)$ *and given subsets* Y_1 *and* Y_2 *of* X, *decide if there exists* $g \in G$ *such that* $Y_1^g = Y_2$, *and, if so, find such an element.* In doing this we may assume that $|Y_1| = |Y_2|$ and then find $f \in \mathrm{Sym}(X)$ such that $Y_1^f = Y_2$. Next use (A.8) to find $G \cap (\mathrm{Sym}(X)_{Y_1})f$, and observe that either this intersection is empty (in which case no element of G takes Y_1 to Y_2) or else it equals $(G_{Y_1})g$, where $g \in G$ and $Y_1^g = Y_2$.

(A.11) *Given that* G *is in* $\mathrm{CF}(b)$ *and given a partition* Π *of* X, *find* G_{Π}.
This generalizes (A.9) and can be obtained from (A.8) by the same method. The next construction is the analogous generalization of (A.10).

(A.12) *Given that* G *is in* $\mathrm{CF}(b)$ *and given partitions* Π_1 *and* Π_2 *of* X, *decide if there exists* $g \in G$ *such that* $\Pi_1^g = \Pi_2$ *and, if so, find such an element.*

(A.13) *Given that* G *is in* $\mathrm{CF}(b)$ *and given a subset* S *of* $\mathrm{Sym}(X)$, *find* $C_G(S)$.
To do this, find $C_{\mathrm{Sym}(X)}(S)$ and then use (A.8) to find $C_G(S) = G \cap C_{\mathrm{Sym}(X)}(S)$.

(A.14) *Given that* G *is in* $\mathrm{CF}(b)$ *and given* h_1 *and* h_2 *in* $\mathrm{Sym}(X)$, *decide if there exists* $g \in G$ *such that* $h_1^g = h_2$ *and, if so, find such an element.*

If h_1 and h_2 have different cycle structures, no such g exists. Otherwise it is possible to find $f \in \mathrm{Sym}(X)$ such that $h_1^f = h_2$. Next find $C = C_{\mathrm{Sym}(X)}(h_1)$ and use (A.8) to find $G \cap Cf$. Either $G \cap Cf$ is empty (in which case no element of G conjugates h_1 to h_2) or else $G \cap Cf = (G \cap C)g$, where $g \in G$ and $h_1^g = h_2$.

The next construction is a special case of [9]. The original proof in [9] uses the classification of finite simple groups. However, in the case of groups in CF(b) the classification can be avoided. We conclude this section with an outline of how this is done.

(A.15) *Given that G is in* CF(b), *then* (i) *find a set Y on which G acts such that $|Y| \leq n$ and G^Y is simple, and* (ii) *find a composition series for G.*

In (i) note that $G_{(Y)}$ is a maximal normal subgroup of G of index at most $n!$. Thus (ii) follows from (i) by (G.7) and iteration.

For purposes of recursion we actually find a maximal subgroup of index at most n in G containing a given proper normal subgroup N. First use (A.2) to find the set Π of orbits of N and then use (A.4) to find $G_{(\Pi)}$. If $G = G_{(\Pi)}$, then $G = NG_x$ by (G.1) and we solve the problem by recursion to G_x. If $G_{(\Pi)} \neq 1$ or G, we solve the problem by recursion to G^Π. Thus we may now assume that $G_{(\Pi)} = 1$ and that $N = 1$. Use (A.2) to find a nontrivial orbit Y of G on X and use (A.3) to find a block system Σ on Y such that G^Σ is a nontrivial primitive group. Then either we solve the problem by recursion to a smaller group or else $G \simeq G^\Sigma$. So from now on we may assume that G is primitive on X. By [3], $|G| \leq n^{c(b)}$. Using (A.5) we find the normal closure of each element of G, either concluding that G is simple—in which case we are finished—or else finding a proper normal subgroup K of G. In the latter case, $G = KG_x$ (since G is primitive). If M is a maximal subgroup of index at most n in G_x, then KM is a maximal subgroup of index at most n in G.

In the preceding argument, and throughout the remainder of this paper, it is straightforward to check that the indicated algorithm runs in polynomial time.

4. Sylow Subgroups

In this section we prove three polynomial-time versions of Sylow's theorem: conjugacy, existence, and embedding of p-groups. The algorithm that constructs a Sylow subgroup uses the conjugacy algorithm and the embedding algorithm uses both conjugacy and existence.

THEOREM (4.1). *There is a polynomial-time algorithm which, when given a group $G \leq \mathrm{Sym}(X)$ in* CF(b) *and Sylow p-subgroups P_1 and P_2 of G, finds $g \in G$ such that $P_2^g = P_1$.*

Proof. 1. Use (A.2) to find the set Π_i of orbits of P_i for $i = 1, 2$.

2. Use (A.12) to find $f \in G$ such that $\Pi_2^f = \Pi_1$, and let $P_3 = P_2^f$. (Sylow's theorem implies that f exists. Note that Π_1 is the set of orbits of $\langle P_1, P_3\rangle$.)

3. *Case* $\Pi_1 \neq \{X\}$.

3.1. Pick any $Y \in \Pi_1$, and let $Z = X - Y$.

3.1. Recursively find $h \in \langle P_1, P_3\rangle$ such that $(P_3^h)^Y = P_1^Y$.

3.3. Recursively find $k \in \langle P_1, P_3^h\rangle$ such that $(P_3^{hk})^Z = P_1^Z$. Then $P_2^g = P_1$, where $g = fhk$. (By construction $(P_2^g)^Y = (P_3^{hk})^Y = P_1^Y$ and $(P_2^g)^Z = (P_3^{hk})^Z = P_1^Z$, so that $\langle P_2^g, P_1\rangle$ is a p-group.)

4. (From now on we may assume that P_1 and P_2 are transitive on X.)

5. Use (A.7) to find $Z(P_1)$ and $Z(P_2)$.

6. Pick any element $z_2 \neq 1$ of $Z(P_2)$. Use (A.14) to find $h \in G$ such that $z_2^h \in Z(P_1)$. (By Sylow's theorem such an element h exists. Since P_1 is transitive, $|Z(P_1)|$ divides n by [12, (4.3)]. For each $z_1 \in Z(P_1)$, apply (A.14) to the pair z_1, z_2 until h is found.)

7. Let $z = z_2^h$, $P_4 = P_2^h$, and $K = \langle P_1, P_4\rangle$. Use (A.2) to find the set Σ of orbits of $\langle z\rangle$ on X. (Then $z \in Z(P_1) \cap Z(P_4) \leq Z(K)$.)

8. Recursively find $k \in K$ such that $(P_4^k)^\Sigma = P_1^\Sigma$, and let $g = hk$. Then $P_2^g = P_1$. (Since $z \in Z(K)$, $K_{(\Sigma)}$ is a p-group by (G.5); since it is normal in K it is contained in every Sylow p-subgroup of K. Then $(P_4^k)^\Sigma = P_1^\Sigma$ implies that $P_4^k = P_1$; hence $P_2^{hk} = P_4^k = P_1$.) □

COROLLARY (4.2). *There is a polynomial-time algorithm which, when given $G \leq S_n$ in* CF(b), *$N \trianglelefteq G$, and a Sylow p-subgroup P of N, finds a subgroup H such that $P \trianglelefteq H$ and $G = NH$.*

Proof. Let Γ be the given set of generators of G. For each $g \in \Gamma$, use Theorem (4.1) to find $m \in N$ such that $(P^g)^m = P$. (Note that P^g and P are Sylow p-subgroups of N.) Then let Γ' be the resulting set of elements gm (one for each $g \in \Gamma$) and let $H = \langle P, \Gamma'\rangle$. (Then $G = \langle\Gamma'\rangle N$, since $gN = gmN$.) □

Remark. The preceding corollary is a polynomial-time version of the Frattini argument (G.2). However, note that we did not find $N_G(P)$: indeed we do not know how to find $N_N(P)$.

THEOREM (4.3). *There is a polynomial-time algorithm which, when given a group $G \leq$* Sym(X) *in* CF(b) *and a prime p, finds a Sylow p-subgroup of G.*

Proof. 1. Use (A.15) to find a set Y such that $|Y| \leq n$ and G^Y is a simple group.

2. Use (A.1) to find $M = G_{(Y)}$.

3. *Case G^Y is nonabelian.*

 3.1. Find $H \leq G$ such that the image of H in G^Y is a Sylow p-subgroup. (By [3], $|G^Y| \leq |Y|^c \leq n^c$ for some constant $c = c(b)$. Thus the following brute force approach can be used. If P is any p-subgroup of G^Y other than a Sylow p-subgroup, simply check each p-element of $G^Y - P$ until an element g is found that normalizes P. Replace P by $\langle P, g\rangle$. By (G.7), this process eventually produces a Sylow p-subgroup.)

 3.2. Recursively find a Sylow p-subgroup of H, and hence of G. (Since H^Y is a p-group while G^Y is not, $H < G$. Also, H contains a Sylow p-subgroup of G since it contains M and induces a Sylow p-subgroup of G^Y.)

4. *Case G^Y has prime order q.* Let g be one of the given generators of G lying in $G - M$.

 4.1. Recursively find a Sylow p-subgroup P of M.

 4.2. Use Theorem (4.1) to find $m \in M$ such that $(P^g)^m = P$.

 4.3. Find the Sylow p-subgroup $\langle h\rangle$ of $\langle gm\rangle$. Then $\langle P, h\rangle$ is a Sylow p-subgroup of G. (The element $Mg = Mgm$ of G/M has order q. If $q \neq p$, then $h \in M$ and P is already a Sylow p-subgroup of G. If $q = p$, then Mh has order p and $\langle P, h\rangle$ is a p-group properly containing P. Since $G = M\langle h\rangle$, it follows that $\langle P, h\rangle$ is a Sylow p-subgroup of G.) □

In [7] an unsuccessful attempt was made to find the largest normal p-subgroup $O_p(G)$ of a given group $G \leq S_n$. When $G \in \mathrm{CF}(b)$, this can now be done.

COROLLARY (4.4). *There is a polynomial-time algorithm which, when given a group $G \leq \mathrm{Sym}(X)$ in $\mathrm{CF}(b)$ and a prime p, finds $O_p(G)$.*

Proof. 1. Use Theorem (4.3) to find a Sylow p-subgroup P of G.

2. For each of the given generators g of G, find H^g and test if H equals H^g. (Use A.1) to find $|H|$ and $|\langle H, H^g\rangle|$.)

3. If $H^g \neq H$, use (A.8) to find $H \cap H^g$. Replace H by $H \cap H^g$ and return to Step 2. (By (G.7), H becomes $O_p(G)$ after at most n^2 replacements.) □

THEOREM (4.5). *There is a polynomial-time algorithm which, when given a group $G \leq \mathrm{Sym}(X)$ in $\mathrm{CF}(b)$ and a p-subgroup K of G, finds a Sylow p-subgroup of G containing K.*

Proof. We may assume that K is not a Sylow p-subgroup of G. By (G.7), it suffices to find a p-subgroup of G properly containing K:

1. *Case G is intransitive on X.*

1.1. Let Y be any orbit of G, and let $Z = X - Y$.

1.2. Recursively find a Sylow p-subgroup of G^Y containing K^Y, and use (A.1) to find its preimage T in G.

1.3. Recursively find a subgroup P of T whose image in T^Z is a Sylow p-subgroup containing K^Z. Then P is a Sylow p-subgroup of G. (The groups $\langle P, K\rangle^Y$ and $\langle P, K\rangle^Z$ are both p-groups.)

2. (We may assume that G is transitive on X.) Use (A.2) to find the set Π of orbits of K on X. Then use (A.11) to find G_Π. Use (A.1) to test if $G_\Pi < G$.

3. *Case* $G_\Pi < G$. Recursively find a Sylow p-subgroup of G_Π properly containing K. (By (G.3), $N_G(K) \leq G_\Pi$. Also, a Sylow p-subgroup of $N_G(K)$ properly contains K as K is not a Sylow p-subgroup of G.)

4. (We may assume that $G_\Pi = G$.) Use Theorem (4.3) to find a Sylow p-subgroup of G^Π, and use (A.1) to find its preimage T in G. If $T < G$, recursively find a Sylow p-subgroup of T that contains K.

5. (We may assume that G^Π is a p-group.)

6. *Case* $G^\Pi \neq 1$.

6.1. Find a normal subgroup of G^Π of index p and use (A.4) to find its preimage M in G.

6.2. If K is not a Sylow p-subgroup of M, recursively find a Sylow p-subgroup of M containing K.

6.3. (We may assume that K is a Sylow p-subgroup of M.) Use Theorem (4.3) to find a Sylow p-subgroup P of G. Then use Theorem (4.1) to find $m \in M$ such that $K = (P \cap M)^m$. (Since M is normal in G and P is a Sylow subgroup of G, it follows that $P \cap M$ is a Sylow subgroup of M.) Then $K < P^m$.

7. *Case* $G^\Pi = 1$. (Here K is transitive on X since $G = G_{(\Pi)}$ is transitive on X.)

7.1. Use (A.7) to find $Z(K)$. For each $z \neq 1$ in $Z(K)$, use (A.13) and (A.1) to find $C_G(z)$ and $|C_G(z)|$. (Since K is transitive on Z, $|Z(K)|$ divides n by [12, (4.3)].)

7.2. Find $z \neq 1$ in $Z(K)$ such that a Sylow p-subgroup of $C_G(z)$ has order greater than $|K|$. (The group K is a proper normal subgroup of a p-group $L \leq G$ and so $K \cap Z(L) \neq 1$. If $1 \neq z \in K \cap Z(L)$, then $z \in Z(K)$ and $K < L \leq C_G(z)$.)

7.3. *Case* $C_G(z) < G$. Recursively find a Sylow p-subgroup of $C_G(z)$ properly containing K.

7.4. *Case* $C_G(z) = G$. Use (A.2) to find the set Σ of orbits of $\langle z \rangle$ on X. Recursively find a Sylow p-subgroup of G^{Σ} containing K^{Σ}, and use (A.4) to find its preimage P in G. Then P is a Sylow p-subgroup of G containing K. (By (G.5), $G_{(\Sigma)}$ is a p-group. Consequently, P is also a p-group.) □

5. Hall Subgroups

Let π be a set of primes. A group H is a π-group if every prime divisor of $|H|$ belongs to π. A *Hall π-subgroup* of a group G is a π-subgroup H such that no prime divisor of $|G : H|$ belongs to π. A subgroup of G is a Hall subgroup if and only if its order and index are relatively prime.

In this section we will prove analogues of the results of Section 4 for Hall π-subgroups of solvable groups. (The existence and conjugacy of Hall π-subgroups of solvable groups is a basic result due to P. Hall; cf. [5, Section 6.6.4].)

Theorem (5.1). *There is a polynomial-time algorithm which, when given a solvable group $G \leq \mathrm{Sym}(X)$, a set π of primes and Hall π-subgroups H_1 and H_2 of G, finds $g \in G$ such that $H_2^g = H_1$.*

Proof. 1. Use (A.6) to find the derived group G' of G.

2. Find a group M such that $G' \leq M < G$ and $|G : M|$ is a prime q. (Since G/G' is abelian, this is straightforward—observe that it is just another version of Steps 1 and 2 of Theorem (4.3).)

3. Recursively find $m \in M$ such that $(H_2 \cap M)^m = H_1 \cap M$. (Since $M \leq G$ and H_1 is a Hall subgroup of G, H_i is a Hall subgroup of M.)

4. If $q \notin \pi$, then m is the desired element.

5. If $q \in \pi$, use Theorem (4.3) to find Sylow q-subgroups Q_i of H_i for $i = 1, 2$. (These are Sylow q-subgroups of G.) Next use Theorem (4.3) to find $h \in \langle H_1, H_2^m \rangle$ such that $Q_2^{mh} = Q_1$. Let $g = mh$.

(Since $H_1 \cap M = H_2^m \cap M$ is a normal subgroup of $\langle H_1, H_2^m \rangle$, we have $H_2^{mh} = ((H_2^m \cap M)Q_2^m)^h = (H_1 \cap M)Q_2^{mh} = H_1$.) □

Corollary (5.2). *There is a polynomial-time algorithm which, when given a solvable group $G \leq S_n$, $N \trianglelefteq G$, and a Hall subgroup K of N, finds a subgroup H such that $K \trianglelefteq H$ and $G = NH$.*

Proof. Proceed as in Corollary (4.2). □

THEOREM (5.3). *There is a polynomial-time algorithm which, when given a solvable group $G \leq \mathrm{Sym}(X)$ and a set π of primes, finds a Hall π-subgroup of G.*

Proof. 1. Use Steps 1 and 2 of Theorem (5.1) to find $M \trianglelefteq G$ with $|G : M|$ a prime q. We may assume that $q \in \pi$.

2. Proceed as in Steps 4.1, 4.2, and 4.3 of Theorem (4.3) to obtain a Hall π-subgroup P of M and a q-element $h \in G - M$ normalizing P. Then $\langle P, h\rangle$ is a Hall π-subgroup of G. (For, $G = M\langle h\rangle$.) □

COROLLARY (5.4). *There is a polynomial-time algorithm which, when given a solvable group $G \leq \mathrm{Sym}(X)$ and a set π of primes, finds the largest normal π-subgroup $O_\pi(G)$ of G.*

Proof. Proceed exactly as in Corollary (4.4). □

Remark. The proofs of Theorems (4.3), (4.5), and (5.3) worked from the top down: a maximal normal subgroup was used (in conjunction with Theorems (4.1) and (5.1)). In earlier proofs of those results we worked from the bottom up, starting with a normal q-subgroup or a normal subgroup that was a direct product of nonabelian simple groups. The present proofs are much simpler to understand, and also significantly shorter. However, the proof of Theorem (4.5) does not generalize to the case of π-subgroups of K. (Steps 3 and 6.1 of Theorem (4.5) can fail.) Therefore, the remainder of this section is a last vestige of the former approach. It seems likely that further group-theoretic algorithms in more complicated situations will require both of the methods. In any event, it appears that the bottom up approach allows somewhat more delicate arguments. We leave it to the reader to decide which method is preferable.

The main idea is to arrange to use (G.4 (ii)) with $|\Sigma \cup \Lambda| < n$.

THEOREM (5.5). *There is a polynomial-time algorithm which, when given a solvable group $G \leq \mathrm{Sym}(X)$, a set π of primes and a π-subgroup K of G, finds a Hall π-subgroup of G containing K.*

Proof. We may assume that K is not a Hall π-subgroup of G. It suffices to find a π-subgroup of G properly containing K.

1. Use Step 1 of Theorem (4.5) to reduce to the case in which G is transitive on X.

2. Use (A.6) to find the derived series of G, and let q be a prime dividing the order of its last nontrivial term. Let L be the smallest term that is not a q-group.

3. Construct a q-group Q and an r-group R of G such that $q \neq r$, $1 \neq Q \trianglelefteq G$ and $Q \neq QR \trianglelefteq G$. Do this as follows.
   3.1. *Case L is the last term of the derived series.* Find the Sylow q-subgroup Q and the Sylow r-subgroup $R \neq 1$ of L for some $r \neq q$. (Since L is abelian, this is straightforward.)
   3.2. *Case L is not the last term of the derived series.* Let $Q = L'$ and use Theorem (4.3) to find a Sylow r-subgroup $R \neq 1$ of L for some $r \neq q$.

4. Use (A.2) to find the set Σ of orbits of R on X, and use (A.11) to find G_Σ. Use (A.1) to test if $G_\Sigma = G$.

5. *Case $G_\Sigma = G$.* Use (A.2) to find the set Λ of orbits of Q on X. Recursively find a Hall π-subgroup of $G^{\Sigma \cup \Lambda}$. (By (G.4(ii)), G acts faithfully in $\Sigma \cup \Lambda$. Since G is transitive on X we have $|\Sigma| \leq n/r$, $|\Lambda| \leq n/q$ and hence $|\Sigma \cup \Lambda| < n$.)

6. (From now on we may assume that $G_\Sigma < G$.) Use (A.11) to find $(QK)_\Sigma$, then use Theorem (5.3) to find a Hall π-subgroup K_1 of $(QK)_\Sigma$.

7. Recursively find a Hall π-subgroup H of G_Σ containing K_1. (Recall that $G_\Sigma < G$.)

8. (Note that by (G.2) and (G.3) $G = QRN_G(R) = QG_\Sigma$ and therefore $QK = Q(QK)_\Sigma$. Thus $QK = QK_1$.)

9. *Case $q \in \pi$.* In this case QH is a Hall π-subgroup of G containing K. (Since $G = QG_\Sigma$, QH is a Hall π-subgroup of G containing QK_1.)

10. *Case $q \notin \pi$.* Use Theorem (5.1) to find $g \in QK$ such that $K_1^g = K$. Then H^g is a Hall π-subgroup of G containing K. (Since $q \notin \pi$, both K and K_1 are Hall π-subgroups of $QK = QK_1$, so that Theorem (5.1) can be applied. Moreover, $H^g \geq K_1^g = K$. Finally, since $G = QG_\Sigma$, both H and H^g are Hall π-subgroups of G. □

6. The Schur–Zassenhaus Theorem

Another standard group-theoretic result is the Schur–Zassenhaus theorem [5, Theorem 6.2.1]: if $N \trianglelefteq G$ and $(|N|, |G/N|) = 1$, then there is a subgroup K of G such that $G = NK$ and $N \cap K = 1$ (i.e., a complement to N in G), and any two such subgroups are conjugate in G. In standard proofs (of the conjugacy part) of this theorem it is assumed that either N or G/N is solvable. By the Feit–Thompson Theorem, this is always the case.

In this section we will obtain polynomial-time versions of this theorem. The conjugacy part is very easy.

Theorem (6.1). *There is a polynomial-time algorithm which, when given a group $G \leq \mathrm{Sym}(X)$ in $\mathrm{CF}(b)$, a subgroup $N \trianglelefteq G$ such that $(|N|, |G/N|) = 1$, and two complements H_1 and H_2 to N in G, finds $g \in G$ such that $H_2^g = H_1$.*

Proof. Use Steps 1, 2, and 3 of Theorem (4.1) to reduce to the case in which H_1 and H_2 are transitive on X. In this situation $|X|$ divides $|H_1|$, so that $(|X|, |N|) = 1$. Moreover, as N is a normal subgroup of G, each orbit of N on X has length dividing both $|N|$ and $|X|$. Thus $N = 1$ and $H_1 = H_2$. □

LEMMA (6.2). *There is a polynomial-time algorithm which, when given a group $G \leq \mathrm{Sym}(X)$ in $\mathrm{CF}(b)$ and a normal subgroup N such that $(|N|, |G/N|) = 1$ and G/N is a direct product of nonabelian simple groups $W_1/N, \ldots, W_m/N$, finds a complement to N in G.*

Proof. 1. *Case $m = 1$.* (We will use the notation of [5, p. 221].)

1.1. For each coset α of N in G, find a coset representative $x_\alpha \in G$. (By [3] and (G.7), $|G/N|$ is bounded by a power of $|X|$, so this can be done in polynomial time.)

1.2. Let $\overline{\Gamma}$ be the set of cosets corresponding to a set Γ of generators for G. For each coset α and each $\delta \in \overline{\Gamma}$, calculate $f(\alpha, \delta) = x_{\alpha\delta}^{-1} x_\alpha x_\delta$ and then let $g(\delta) = \prod_\alpha f(\alpha, \delta)$.

1.3. Use (A.6) to find the derived group N' of N. (By the Feit–Thompson Theorem, N is solvable, so that $N \neq N'$.)

1.4. Find an integer r such that $r|G/N| \equiv 1 \pmod{|N/N'|}$.

1.5. If $N' = 1$, the elements $x_\delta g(\delta)^{-r}$ (where $\delta \in \overline{\Gamma}$) generate a complement to N in G. If $N' \neq 1$, replace G by the group generated by N' and the elements $x_\delta g(\delta)^{-r}$, then return to Step 1.1. (The proof of Theorem 6.2.1 in [5] shows that this procedure constructs a complement to N.)

2. *Case $m > 1$.*

2.1. Find a complement K_1 to N in W_1.

2.2. Use (A.13) to find $C_G(K_1)$.

2.3. Recursively find a complement L to $C_N(K_1)$ in $C_G(K_1)$. Then $K_1 L$ is a complement to N in G. (Since $K_1 \leq C_G(K_1)$, recursion can be applied. By the Schur–Zassenhaus theorem, there is a complement K to N in G such that $K > K_1$. Then $K \simeq G/N$, so that $K = K_1 \times M$ for some group M. Clearly, M is a complement to $C_N(K_1)$ in $C_G(K_1)$. By the Schur–Zassenhaus theorem, L and M are conjugate in $C_G(K_1)$. Thus $K_1 L$ behaves as desired.) □

THEOREM (6.3). *There is a polynomial-time algorithm which, when given a group $G \leq \mathrm{Sym}(X)$ in $\mathrm{CF}(b)$ and a subgroup $N \trianglelefteq G$ such that $|N|$ and $|G/N|$ are relatively prime, finds a complement to N in G.*

Proof. 1. (We may assume that $N \neq G$.) Use (A.15) to find a composition series for G. Let L be the smallest term not contained in N. (Use (A.1) to compare $|N|$ with $|\langle L, N\rangle|$.) Use (A.5) to find $M = \langle (NL)^G \rangle$. (By (G.6) applied to G/N, either M/N is an r-group for some r or it is a direct product of nonabelian simple groups.)

2. Use either Theorem (4.3) or Lemma (6.2) to find a complement R to N in M.

3. For each of the given generators g of G, apply Theorem (6.1) to the subgroups R and R^g of M to find $m \in M$ such that $g' = gm$ normalizes R. Let H be the subgroup of G generated by R and the elements g' just found. (Since $gM = g'M$, we have $G = MH = NRH = NH$.)

4. If $H < G$, recursively find a complement K to $H \cap N$ in H. Then K is a complement to N in G.

5. (We may assume that $R \trianglelefteq G$.) Use (A.2) to find the set Σ of orbits of R on X.

6. Recursively find a complement to N^Σ in G^Σ, and use (A.4) to find its preimage T in G. Then T is a complement to N in G. For, since $(|R|, |N|) = 1$, $R \trianglelefteq G$, and $N \trianglelefteq G$, it follows from (G.3) and (G.4) that $N_{(\Sigma)} = 1$. Then $T_{(\Sigma)} \cap N = 1$ and $T^\Sigma \cap N^\Sigma = 1$, so that $T \cap N = 1$. (Clearly $G^\Sigma = N^\Sigma T^\Sigma$ implies $G = NT$.) □

7. Concluding Remarks

(i) We have already mentioned that we do not have a polynomial-time algorithm for finding $N_G(R)$ when $R \leq G$. We cannot even solve this problem when G is solvable and R is elementary abelian.

(ii) Several other standard group-theoretic results are consequences of Theorems (6.1) and (6.3). For example, if $G \in \mathrm{CF}(b)$ and G is π-solvable, then Hall π-subgroups can be found in polynomial time, and any given one can be conjugated to any other one in polynomial time (cf. [5, Section 6.3]). There are also polynomial-time versions of standard results on relatively prime actions [5, Theorem 6.2.2 (i)–(iii)].

(iii) In [9, 7] it is shown that the following can be accomplished in polynomial time (given $G \leq S_n$ as usual).

(A.15′) *Find a composition series for G.*

(A.16) *Given that G is simple and given a prime p, find a Sylow p-subgroup of G.*

Neither algorithm was needed in previous sections. Both depend upon the classification of finite simple groups.

Consider the following problems (given $G \leq S_n$):

SYLOW EXISTENCE. *Given a prime p, find a Sylow p-subgroup of G.*

SYLOW CONJUGACY. *Given Sylow p-subgroups P_1 and P_2 of G, find an element of G conjugating P_2 to P_1.*

INTERSECTION. *Given $G, H \leq S_n$ and $f \in S_n$, find $G \cap Hf$.*

Clearly, this paper has been primarily concerned with the first two of these problems, while the last problem contains the basic tool (A.8) as a special case. Of course, given an algorithm for **intersection**, it is trivial to obtain analogues of (A.9)–(A.14).

The importance of **intersection** was made clear in [8]: the **graph isomorphism** problem is polynomial-time reducible to **intersection**. In view of the proofs in the present paper, it is not surprising that **Sylow existence** *and* **Sylow conjugacy** *are polynomial-time reducible to* **intersection**. The proofs are identical to those of Theorems (4.1) and (4.2), except that (A.15′) and (A.16) must be inserted at the appropriate points.

In fact, the proof of Theorem (4.2) shows that **Sylow existence** is polynomial-time reducible to **Sylow conjugacy**.

(iv) The argument in Theorem (4.2) can be pushed slightly further in yet another way. All that is needed is a "local" version of the **intersection** property. Assume that there is an $O(n^c)$ algorithm for finding $\bar{K} \cap Hf$ whenever the following conditions all hold: $K \leq G$, $K \rightarrow \bar{K}$ is a homomorphism from K onto a subgroup of $\bar{K}$ of $\mathrm{Sym}(Y)$ for some set Y for which $|Y| \leq n$, $H \leq \mathrm{Sym}(Y)$, and $f \in \mathrm{Sym}(Y)$. If G has the above property and p is a prime, then a Sylow p-subgroup of G can be found in polynomial time. (The proof involves minor modifications of the proof of Theorem (4.2) using (A.15′) and (A.16).)

For example, the above local intersection property holds when G is known to have a subgroup of polynomial index belonging to $\mathrm{CF}(b)$. A typical way this can occur is when the pointwise stabilizer of some set of 2001 points is in $\mathrm{CF}(b)$.

REFERENCES

1. M. D. ATKINSON, An algorithm for finding the blocks of a permutation group, *Math. Comp.* **29** (1975), 911–913.
2. L. BABAI, On the length of subgroup chains in the symmetric group. *Comm. Algebra* **14** (1986) 1729–1736.
3. L. BABAI, P. J. CAMERON, AND P. P. PÁLFY, On the orders of primitive groups with restricted nonabelian composition factors, *J. Algebra* **79** (1982), 161–168.
4. M. FURST, J. HOPCROFT, AND E. LUKS, Polynomial-time algorithms for permutation groups, *in* "Proceedings 21st IEEE Sympos. Foundations of Computer Science, Syracuse, 1980," pp. 36–41, IEEE, New York, 1980.
5. D. GORENSTEIN, "Finite Groups," Harper & Row, New York, 1968.

6. C. M. HOFFMAN, "Group Theoretic Algorithms and Graph Isomorphism," Lect. Notes Comput. Sci. Vol. 136, Springer, Berlin/Heidelberg/New York, 1982.

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

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

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

10. P. P. PÁLFY, A polynomial bound for the orders of primitive solvable groups; *J. Algebra* **77** (1982), 127–137.

11. C. C. SIMS, Some group theoretic algorithms, *in* Lect. Notes math. Vol. 697, pp. 108–124, Springer, Berlin/Heidelberg/New York, 1978.

12. H. WIELANDT, "Finite Permutation Groups," Academic Press, New York, 1964.