J. Symbolic Computation (1991) **12**, 517–526

Finding Composition Factors of Permutation Groups of Degree $n \leq 10^6$

WILLIAM M. KANTOR

University of Oregon, Eugene, OR 97403, USA

(*Received* 26 *May* 1989)

Given a subgroup $G = \langle \Gamma \rangle$ of S_n specified in terms of a generating set Γ, when $n \leq 10^6$ we present algorithms to test the simplicity of G, to find all of its composition factors, and to find a composition series. While there are already existing algorithms for these purposes (due to Luks or Neumann) valid for all n, the ones in the present note are designed to replace many group theoretic computations by arithmetic calculations using properties of n and $|G|$.

1. Introduction

Suppose that a subgroup $G = \langle \Gamma \rangle$ of S_n is given in terms of a generating set Γ of permutations. When discussing the structure of G, one of the fundamental problems is: find a composition series for G. There is a beautiful polynomial-time algorithm for solving this problem due to Luks (1987), but this does not presently seem to be sufficiently practical for implementation. There is also an algorithm due to Neumann (1987), parts of which already have been incorporated into CAYLEY (the ERNIE routine for finding an earns: an elementary abelian regular normal subgroup).

The present note is intended to provide algorithms that do much less than this, but seem to have the advantage of speed. We will only consider permutation groups of degree $n \leq 10^6$. For such groups we will provide progressively more complicated (and hence slower) algorithms for solving the following problems.

1. Test simplicity (section 3).
2. Find all composition factors of G (section 4).
3. Find a composition series for G (section 5).

It should be noted that finding all composition factors is drastically weaker than finding a composition series: in the case of solvable groups the composition factors are just cyclic groups of prime order, one for each prime in the factorization of $|G|$ (counting multiplicities). The advantage of our approach over the more general ones in Luks (1987) and Neumann (1987) is that we are able to replace some of the computations in G itself by computations of a purely arithmetic nature concerning $|G|$. Nevertheless, these algorithms follow the same pattern as those in Luks (1987) and Neumann (1987): reduce to the primitive case, apply the O'Nan–Scott Theorem (see section 2), and use the validity of Schreier's Conjecture—"The outer automorphism group of a finite simple group is solvable"—a consequence of the classification of finite simple groups. We will, in fact, need slightly more detailed information than this concerning the finite simple groups: their orders.

2. Background

We will presuppose the basic facts about permutation groups, together with the simpler

0747-7171/91/100517+10 $03.00/0

properties of G that can be readily computed—for example, using CAYLEY (Cannon, 1984)—when we are given $G = \langle \Gamma \rangle \leq \mathrm{Sym}(X)$ in terms of a generating set Γ of permutations. If $Y \subseteq X$ then $G_{(Y)}$ and G_Y will denote, respectively, the pointwise and set stabilizers of Y in G. Throughout, x will always denote a point of X.

The following result is fundamental.

O'NAN-SCOTT THEOREM (Cameron, 1981; Aschbacher-Scott, 1985; Neumann, 1987). *Let G be a primitive permutation group of degree n. Then one of the following holds.*

(I) *G has an elementary abelian regular normal subgroup ("earns") A of order $n = p^d$ for some prime p and some d.*

(II) *The socle of G is $N = S_1 \times \cdots \times S_k$ for isomorphic nonabelian simple groups S_i. Then one of the following holds.*

(a) *X can be identified with a set X_1^k such that $n = n_1^k$, $n_1 = |X_1|$, the action of G on X is the wreathed product action, and there is a faithful primitive permutation representation on X_1 of a group containing S_1 as a normal subgroup. (When $k = 1$, G has a simple normal subgroup.)*

(b) *$n = |S_1|^{(a-1)b}$ for integers a, b with $ab = k > 1$; $N_x = D_1 \times \cdots \times D_b$ where D_i is a diagonal subgroup of $S_{(i-1)a+1} \times \cdots \times S_{ia}$; and G acts transitively on $\{S_1, \ldots, S_k\}$ with block system $\{\{S_{(i-1)a+1}, \ldots, S_{ia}\} \mid i = 1, \ldots, b\}$.*

(c) *$n = |S_1|^k$, $k > 1$,* and G acts transitively on $\{S_1, \ldots, S_k\}$.

(d) *$n = |S_1|^{\frac{1}{2}k}$,* and G has two orbits on $\{S_1, \ldots, S_k\}$ of length $\frac{1}{2}k$.

We will make frequent references to Cases (I), (IIa)–(IId). The following remark is clear:

LEMMA 1. *In (IIa), $|G| = tu \cdot |S_1|^k$ where $t|S_1|^k = |G_{(\Omega)}|$ and $u = |G^\Omega|$ for $\Omega := \{S_1, \ldots, S_k\}$. Here, t is the order of a subgroup of the direct product of k copies of $Aut(S_1)/S_1$; slightly more precisely, t is the order of a subgroup of $(T_1 \times \cdots \times T_k)/(S_1 \times \cdots \times S_k)$ where the T_i are isomorphic and $S_1 \trianglelefteq T_1 \leq Sym(X_1)$.*

We will also need the following easy fact:

LEMMA 2. (i) *If $n^* \leq 15$ and G is a simple subgroup of S_{n^*} of order y, whose normalizer G^+ in S_{n^*} is primitive, then n^* and y are listed in Table 1. In each case, G^+/G has order 1 or 2 except if $n^* = 9$ and $y = 504$, where G^+/G can have order 3, or if $n^* = 10$ and $y = 360$, where G^+/G can have order 4.*

Table 1

n^*	y
5	6!/2
6	5!/2; 6!/2
7	$\|PSL(3,2)\|$; 7!/2
8	$\|PSL(3,2)\|$; 8!/2
9	$\|PSL(2,8)\| = 504$; 9!/2
10	5!/2;6!/2; 10!/2
11	$\|PSL(2,11)\|$; $\|M_{11}\|$; 11!/2
12	$\|PSL(2,11)\|$; $\|M_{11}\|$; $\|M_{12}\|$; 12!/2
13	$\|PSL(3,3)\|$; 13!/2
14	$\|PSL(2,13)\|$; 14!/2
15	6!/2; 7!/2; 8!/2; 15!/2

Table 2

m	u
5	5!/2
6	5!/2; 6!/2
7	$\|PSL(3,2)\|$; 7!/2
8	$\|PSL(3,2)\|$; $\|AGL(3,2)\| = 8 \cdot 168$; 8!/2

(ii) *If $m \leq 8$ and $G = G'$ is a transitive subgroup of S_m of order u, then m and u are listed in Table 2.*

REMARK. Although $|A_8| = |PSL(3,4)|$, whenever we refer to Tables 1 and 2 the relevant simple group of order $8!/2$ will be A_8 since $PSL(3,4)$ does not have a faithful permutation representation of degree <21. In all other cases there is a unique simple group of order y or u (when $u \neq 8 \cdot 168$).

LEMMA 3. *There is no finite simple group G whose order has the following shape: $|G| = tu \cdot y^m$ where y is as in Table 1, m and u are as in Table 2, and either $t = 2^i$ with $i \leq m$, or $t = 2^i$ with $i \leq 2m$ when $y = 360$, or $t = 3^i$ with $i \leq m$ when $y = 504$.*

PROOF. Suppose that G is such a simple group. Each simple sporadic group has a prime $p \geq 11$ dividing its order to the first power. Then G cannot be sporadic, and similarly G cannot be alternating. This leaves us with all of the groups of Lie type. Here it is only necessary to examine the formulas for the orders of the possible groups (see, e.g., Gorenstein (1968, p. 491)). For example, q^4+1 cannot divide $|G|$ for any prime power q, since $|G|$ is only divisible by primes ≤ 13. On the other hand, 3^{m+1} divides $|G|$, as does 5^m or 7^m. A straightforward case-by-case analysis using elementary congruence arguments produces the desired contradiction.

LEMMA 4. *There is no finite simple group G of order $n^2 \leq 10^{12}$ having a maximal subgroup of order n.*

PROOF. The order of a sporadic simple group or an alternating group is divisible by some prime to the first power, so once again we only need to consider the orders of the simple groups of Lie type (Gorenstein, 1968, p. 491). Assume that $|G|$ is a square. Since $|G| \leq 10^{12}$ we obtain bounds on the size of the field and the Lie rank. Elementary arguments eliminate most cases, producing a single situation: $G = PSp(4,q)$ and $q^2+1 = 2v^2$ for an integer v, in which case $|G| = \{q^2(q^2-1)v\}^2$. However, $PSp(4,q)$ has no maximal subgroup of order $q^2(q^2-1)v$ (see, for example, Kantor & Liebler (1982, 5.6)).

Of course, the lemma is undoubtedly true with no restriction on n.

LEMMA 5. *Assume that $G = G'$ is a 2-transitive permutation group of degree $p^m = (q^d-1)/(q-1)$ for a prime p, a prime power q, and integers $m > 1$ and d. If $|G| = |PSL(d,q)|$ then G is simple.*

PROOF. If G has no earns then this follows from the list of 2-transitive groups (contained, for example, in Cameron (1981); note that this list shows that $G \cong PSL(d,q)$, but we will not need this fact). So assume that G has an earns. Then G can be viewed as a subgroup of $AGL(m,p)$.

If $d = 2$ then $p^m = q+1$, so that either $q = 8$ or q is a Mersenne prime. If $q = 8$ then $|G| \nmid |AGL(2,3)|$. If q is prime then the stabilizer G_x of a point x has order $q(q-1)$, and hence has a normal Sylow q-subgroup by Sylow's Theorem; however, the normalizer of a Sylow q-subgroup in $GL(m,2)$ has order $qm < q(q-1)$ (note that $n = 2^m \neq 4$ since $G = G'$).

Consequently, $d > 2$. Then both d and q are primes, by Zsigmondy (1892).

Clearly, $q^{\frac{1}{2}d(d-1)} = |G|_q \,|\, |GL(m,p)|_q$. Let k be the order of p mod q, so that $q < p^k$; and write $l = [m/k]$. Then $|GL(m,p)|_q = (p^k-1)^l_q l!_q$, where $l!_q = q^{[l/q]+[l/q^2]+\cdots} < q^{l/(q-1)}$. It

follows that $q^{\frac{1}{2}d(d-1)} < (p^k-1)^l q^{l/(q-1)} < p^m q^{l/(q-1)} < 2q^{d-1}q^{l/(q-1)}$, so that $\frac{1}{2}d(d-1) < d+l/(q-1)$. Now $q^{\frac{1}{2}d(d-3)(q-1)} < (p^k)^{\frac{1}{2}d(d-3)(q-1)} \leq p^{kl} < 2q^{d-1}$, so that $\frac{1}{2}(d-3) < 1/(q-1) \leq 1$. Since $d>2$ is prime, this leaves us with the case $d=3$. Then it is easy to check that $q \neq 2, 3$, so that $q^3 < 2q^{3-1}q^{l/(q-1)} < q^{\frac{1}{2}}q^2 q^{l/(q-1)}$ implies that $3 < \frac{1}{2}+2+l/(q-1)$. But then $q-1<2l$ produces the contradiction $q^{\frac{1}{2}(q-1)} < q^l < p^{kl} < 2q^{3-1}$.

Needless to say, the arithmetic part of the above argument could be replaced by the use of a list of all perfect 2-transitive groups having an earns.

3. Simplicity

The simplest algorithm in this note is as follows. It emphasizes numerical calculations as much as possible.

SIMPLY
Input: $G \leq S_n = \mathrm{Sym}(X)$, $n \leq 10^6$.
Output: Whether G is or is not simple.

1. If Y is a non-trivial orbit of G find $G_{(Y)}$.
If $G_{(Y)} \neq 1$ then output "G is not simple".
WLOG $G \leq G^Y$. WLOG $Y = X$.
2. Find a block system Σ such that G^Σ is primitive.
Find $G_{(\Sigma)}$. If $G_{(\Sigma)} \neq 1$ then output "G is not simple".
WLOG $G_{(\Sigma)} = 1$. Replace X by Σ. Now G is primitive.
3. Find $|G|$ and G'.
WLOG $G = G' \neq 1$: otherwise output "G is not simple" except if $|G|$ is prime, in which case output "G is simple".
4. If $|G| = n^2$ then output "G is not simple".
WLOG $|G| \neq n^2$.
5. If n is a power of a prime then output "G is not simple" except in each of the following cases:
$|G| = n!/2$,
n is prime,
$n=9$ and $|G| = 504$,
$n=27$ and $|G| = 25\,920$, or
$n = (q^d-1)/(q-1)$ and $|G| = |PSL(d,q)|$ for some q and d, and G is 2-transitive, in which cases output "G is simple".
WLOG n is not a prime power.
6. If the only way to write n as a power $n = n^{*m}$ is with $m<5$ or $n^*<5$, then output "G is simple".
7. WLOG there is at least one way to write $n = n^{*m}$ with $m \geq 5$ and $n^* \geq 5$.
Output "G is not simple" if, for some such n^* and m, $|G|$ can be written in the form $|G| = tu \cdot y^m$ where y is as in Table 1, m and u are as in Table 2, and either $t = 2^i$ with $i \leq m$, or $t = 2^i$ with $i \leq 2m$ when $y = 360$, or $t = 3^i$ with $i \leq m$ when $y = 504$.
If $|G|$ cannot be written in this form for any such n^* and m then output "G is simple".
8. End.

THEOREM 1. The output of SIMPLY is correct.

PROOF. After Step 3, G is primitive and $G = G' \neq 1$. Step 4 is correct by Lemma 4.

Assume that n is a prime power. Then the only way G can be simple is to have one of the exceptional cases in Step 5 (Kantor, 1985*a*; Guralnick, 1983). Conversely, if one of those cases occurs then $G = A_n$ if $|G| = n!/2$; G has a simple normal subgroup if n is prime, and then $G = G'$ is itself simple by Schreier's Conjecture; G is simple if $n = 9$ or 27 and $|G|$ is as in Step 5 (for, $504 \nmid |AGL(2,3)|$, $25\,920 \nmid |AGL(3,3)|$, and it is just as easy to eliminate the other cases in the O'Nan-Scott Theorem); and G is simple if $n = (q^d - 1)/(q-1)$ and G are as in Step 5 (by Lemma 5).

This completely settles the case in which n is a prime power (cf. Case (I) of the O'Nan-Scott Theorem). In Case (IIc), since $G = G'$ we have $k \geq 5$ and $n = |S_1|^k \geq 60^5 > 10^6$, which is not the case. Similarly, Case (IId) cannot occur if $k > 2$; while if $k = 2$ then $G = S_1 \times S_2$ (again by Schreier's Conjecture) which was handled in Step 4.

In Case (IIb), $60^4 > n = |S_1|^{(a-1)b}$ implies that $(a-1)b < 4$, where $ab = k$. Since $G = G'$ while G has a block system of size b, we must have $b = 1$, but then $G = G'$ and $1 < k = a < 5$ yield a contradiction.

This leaves us with the possibility that G is simple or that we are in Case (IIa) with $n = n_1^k$, where we must have $5 \leq k \leq 8$ and $5 \leq n_1 \leq 15$ (again because $n \leq 10^6$), while $|G|$ is as in Step 7 (with $m = k$ and $n^* = n_1$; cf. Lemma 1). Thus, if $|G|$ cannot be written as in Step 7 then G must be simple. On the other hand, by Lemma 3, no simple group has order as in Step 7.

4. Composition Factors

The idea in SIMPLY can be refined slightly as follows.

COMPFY
Input: $G \leq S_n = \mathrm{Sym}(X)$, $n \leq 10^6$.
Output: A list of simple groups: the list of the composition factors of G (including multiplicities).

REMARK. Some clarification is needed concerning the output of COMPFY: how is each of the simple groups S described? In some cases S is obtained as a section of G (up to isomorphism), in which case this is the way S should be viewed. In other cases S is of prime order, in which case only its order needs to be given (or, alternatively, an $|S|$-cycle in the symmetric group of degree $|S|$, if desired).

Finally, there are some situations in the algorithm where S is obtained merely as an abstract group. In that case its "name" is all that is given—implicitly via Table 1. However, here $|S|$ is small, and there is a faithful permutation representation of S on at most 15 points, in which case it is not difficult to use the name in order to reconstruct that permutation representation. Consequently, in all cases one can view the algorithm as outputting a simple permutation group. (Compare the Remark following Lemma 2.)

1. If Y is a non-trivial orbit of G find $G_{(Y)}$.
If $G_{(Y)} \neq 1$ then output recursively found lists for $G_{(Y)}$ and G^Y.
WLOG $G \cong G^Y$. WLOG $Y = X$.
2. Find a block system Σ such that G^Σ is primitive.
Find $G_{(\Sigma)}$. If $G_{(\Sigma)} \neq 1$ then output recursively found lists for $G_{(\Sigma)}$ and G^Σ.

WLOG $G_{(\Sigma)} = 1$. Replace X by Σ. Now G is primitive.

3. Find $|G|$, G_x and G'.

WLOG $|G|$ is not a prime (otherwise output G).

WLOG $G = G'$. (Otherwise output a recursively found list for G', together with a list for the abelian group G/G'—only the prime factorization of $|G/G'|$ is needed in order to find the latter list.)

WLOG $|G| \neq n!/2$, as otherwise output the simple group $G = A_n$.

4. If $|G| = n^2$ then output two copies of the simple group G_x.

WLOG $|G| \neq n^2$.

5. If the only way to write n as a power $n = n^{*m}$ is with $m < 5$ or $n^* < 5$ then either

5.1. n is not a prime power, in which case output the simple group G, or

5.2. n is a prime power and then either

5.2.1. If $n = 9$ and $|G| = |PSL(2,8)| = 504$, or if $n = 27$ and $|G| = |PSp(4,3)| = 25\,920$, then output the simple group G

5.2.2. If $n = (q^d - 1)/(q-1)$ and $|G| = |PSL(d,q)|$ for some q and d, and G is 2-transitive, then output the simple group G or

5.2.3. Otherwise G has an earns, $n = p^d$ for some prime p, so output d copies of $\mathbb{Z}_p$ together with a recursively found list for G_x.

6. WLOG $n = n^{*m}$ for some $n^* \geq 5$ and $m \geq 5$. Find such an n^* and m.

Here $5 \leq m \leq 8$ and $5 \leq n^* \leq 15$ (as $n \leq 10^6$).

7. If $|G|$ *cannot* be written in the form

$|G| = tu \cdot y^m$ where y is as in Table 1, m and u are as in Table 2, and either $t = 2^i$ with $i \leq m$, or $t = 2^i$ with $i \leq 2m$ when $y = 360$, or $t = 3^i$ with $i \leq m$ when $y = 504$, then either

n is not a prime power, in which case output the simple group G, or

n is a prime power, in which case proceed as in 5.2.

8. WLOG $|G|$ *can* be written in the form $|G| = tu \cdot y^m$ as above.

If the pair (n^*, y) is not (8,168), then output m copies of a simple group of order y (see the Remark following Lemma 2), i copies of $\mathbb{Z}_2$ (or $\mathbb{Z}_3$ when $y = 504$), and a simple group of order u—unless $u = 8 \cdot 168$, in which case output instead $PSL(3,2)$ and 3 copies of $\mathbb{Z}_2$.

9. Now $n^* = 8$ and $y = 168$.

Perform each of the following tests. If any fails then there is an earns, so output as in 5.2.3. If all are passed then output as in Step 8.

Test whether G_x has a unique orbit $Y = x'^{G_x}$ of length $7m$; whether there is a non-trivial block B of G_x containing x'; and whether $|B| = 7$.

Test whether $|(G_{x,B})^B| = 21$ or 42. (Since $|B| = 7$ this computation requires little time.)

Test whether the pointwise stabilizer $E := G_{x,(Y-B)}$ has order 21 or 42, and find $e \in E$ of order 7. Test whether e fixes 8^{m-1} points.

Find a subset Δ of G_x of size m such that B^Δ is the block system containing B, and test whether the elements e^d, $d \in \Delta$, all commute.

Let $f \in G$ be such that $x^f = x'$, find $h \in G_{x'}$ with $x \in B^{fh}$, and replace f by fh. (Then $x \in B^f$.)

Test whether $(B \cup \{x\})^{e^f} = B \cup \{x\}$, and whether $\langle e, e^f \rangle^{B \cup \{x\}}$ has two non-commuting involutions. (Since $|B \cup \{x\}| = 8$ these computations require little time.)

End of tests.

10. End.

REMARKS. (i) Step 9 sidestepped ERNIE (Neumann, 1987), a slower—but much more

general—procedure. ERNIE requires finding $C_G(G_{xy})$ for distinct $x, y \in X$, which can be done in polynomial time by working on sets of size $\theta(n^2)$, but that is presently impractical for degrees n as large as we are allowing. CAYLEY finds centralizers using backtracking, and hence requires exponential time. The corresponding algorithm in Luks (1987) requires numerous computations on sets of size $\theta(n^2)$.

(ii) Step 9 concerned, in effect, two ways to have $n = 8^m$: one with an earns and one without. Note that there are two primitive groups of degree $n = 8^m$ having permutation isomorphic stabilizers, so that more than just arithmetic is needed for such an n.

(iii) Steps 3–10 can be viewed as *a test that detects, but does not find, an earns in a primitive group of degree* $n \leq 10^6$.

(iv) COMPFY will output composition factors in the order they occur in some composition series, starting at the bottom of the series.

THEOREM 2. *The output of* COMPFY *is correct.*

PROOF. Everything is similar to Theorem 1 except in Steps 4, 8 and 9.

If $|G| = n^2$ then G is not simple by Lemma 4; n is not a prime power; and if $G = S_1 \times S_2$ is as in Case (IId) then the output of Step 4 is correct. We will have to verify that no other possibility in (II) can arise when $|G| = n^2$. As in Theorem 1, since $n \leq 10^6$ only Case (IIa) needs to be examined. Here we must consider the equation $|G| = tu \cdot y^m = n^{*2m}$ with $n^* \geq 5$ and $m \geq 5$, and t and u as in Step 7. Since t is a power of 2 or 3, while u has a prime divisor 5 or 7 occurring to the first power (Table 2), this equation is impossible.

Assume that $|G|$ can be written as in Step 7. By Lemma 3, G is not simple. First assume that there is no earns—which is certainly the case if n is not a prime power. We can proceed as in Theorem 1 to see that we must be in Case (IIa). Then $n = n_1^k = n^{*m}$. Since m, n^*, k and n_1 are all at least 5, it follows easily that $m = k$ and $n^* = n_1$. Thus, m and n^* are uniquely determined, and then the equation $|G| = tu \cdot y^m$ uniquely determines y, u and t. (Namely, since $m \geq 5$, if p is a prime and $p^m \| |G|$ then $p | y$ by the Tables, and then the Tables easily imply the stated uniqueness.) This justifies Step 8 if there is no earns.

Now assume that there is an earns. We will obtain a contradiction when $(n^*, y) \neq (8,168)$. Recall that $m = 5, 6, 7$, or 8. We have $n = n^{*m} = p^d$, and G_x lies in $GL(p,d)$—and even in $SL(d,p)$ since $G = G'$—with p and d as follows (since $5 \leq n^* \leq 15$): either $p = n^*$ and $d = m$, or $p = 3$, $n^* = 9$ and $d = 2m$, or $p = 2$, $n^* = 8$ and $d = 3m$.

If $n^* = 5$ or 11 then $|G|_3 \geq 3^m > |SL(m,n^*)|_3$ for $m = 5, 6, 7, 8$.

If $n^* = 7$ then $|G|_2 \geq 8^m > |SL(m,7)|_2$.

If $n^* = 9$ then $|G|_7 \geq 7^m > |SL(2m,3)|_7$.

If $n^* = 13$ then $|G|_5 \geq 5^m > |SL(m,13)|_5$.

If $n^* = 8$ and $y = 7!/2$ then $|G|_5 \geq 5^m > |SL(3m,2)|_5$.

This leaves us with the possibility considered in Step 9. There, we must show that the given tests will correctly detect whether or not X can be identified as in (IIa) with X_1^m where $|X_1| = 8$ and each simple group $S_i \cong PSL(2,7)$.

If there is such an identification then it is easy to see that there is a unique shortest orbit Y, where $|Y| = 7m$ and G_x^Y is imprimitive with blocks of size 7: if $x = (\alpha, \alpha, \ldots, \alpha) \in X_1^m$ then B can be taken to be $(X_1 - \{\alpha\}, \alpha, \ldots, \alpha)$. Moreover, G_x acts 2-transitively on the "coordinates", so that there is a unique non-trivial block system. The relation "x' is in the unique shortest non-trivial orbit of G_x" is symmetric (namely, $(x, x')^G$ is the unique shortest non-diagonal orbit of G on $X \times X$), so that $x \in Y^f$ while B^f is a block of $G_{x'}$

on Y^f. Then we can modify f (using h) in order to have $x \in B^f$, after which $Z := B \cup \{x\} = B^f \cup \{x'\}$ is the orbit $(X_1, \alpha, \ldots, \alpha)$ of S_1. Here, $(S_1)_x = E'$ fixes all 8^{m-1} points in $(\alpha, X_1, \ldots, X_1)$, and $G_Z^Z = PSL(2,7)$ or $PGL(2,7)$ has two non-commuting involutions. Since $e \in S_1$, it follows that $\langle e, e^f \rangle^Z = PSL(2,7)$. Moreover, e commutes with all of its conjugates in G_x: each such conjugate lies in the unique Sylow 7-group of $(S_i)_x$ for some i. Thus, all the tests in Step 9 produce correct answers when there is no earns.

On the other hand, assume that there is an earns A and yet all tests are passed. Since $A = C_A(e) \times [A, e]$, we have $|[A, e]| = 8$. Since $|(G_{x,B})^B| = 21$ or 42, $\langle e \rangle \trianglelefteq E$ and hence $\langle e \rangle \trianglelefteq G_{x,B}$, from which it follows that $G_{x,B}$ normalizes $[A, e]$. Then the m subgroups $[A, e^d]$ are permuted by G_x, and hence generate a G_x-invariant subgroup of A. In view of the primitivity of G it follows that A is generated by these m groups $[A, e^d]$ of order 8, and hence is their direct product (since $|A| = 8^m$). Moreover, since the elements e^d, $d \in \Delta$, all commute, each subgroup $[A, e^d] \neq [A, e]$ lies in $C_A(e)$. If we write A additively and identify X with A and x with 0, it follows that $\bigcup \{[A, e^d] \mid d \in \Delta\} - \{0\}$ is the unique G_0-orbit of length $7m$, and then we may assume that $B = [A, e] - \{0\}$. Since $|(G_{x,B})^B| = 21$ or 42, $G_B^B = [A, e]^B (G_{x,B})^B$ is a solvable subgroup of $AGL(3,2)$. In fact, all involutions in $\langle e, e^f \rangle^{B \cup \{x\}}$ lie in $[A, e]^{B \cup \{x\}}$ and hence commute: the last test in Step 9 cannot have been passed. This is the desired contradiction.

5. Composition Series

The final refinement of this approach actually produces subgroups of G. This time we will have to obtain an earns using Neumann (1987).

COMPSER
Input: $G \leq S_n = \mathrm{Sym}(X)$, $n \leq 10^6$.
Output: A composition series for G.

1. Reduce to the case G primitive, $G = G' \neq 1$, and $|G| \neq n!/2$, as in Steps 1-3 of COMPFY.

2. Use ERNIE (Neumann, 1987) to test whether or not G has an earns A. If it does then find G_x and output a composition series for A together with the groups AH for H in a recursively found composition series for G_x.

WLOG G has no earns.

3. Find $|G|$ and G_x.

4. If $|G| = n^2$ then find a set Φ of n elements such that $X = x^\Phi$; then $G = G_x \Phi$. Find all conjugacy classes of involutions in G of size $\leq n/4$. If C is such a class of smallest size then output the series 1, $\langle C \rangle$, G.

5. WLOG $|G| \neq n^2$.

If the only way to write n as a power $n = n^{*m}$ is with $m < 5$ or $n^* < 5$ then output the series 1, G.

WLOG $n = n^{*m}$ for some $n^* \geq 5$ and $m \geq 5$.

6. Compute $|G|$. If this *cannot* be written in the form $|G| = tu \cdot y^m$ where y is as in Table 1, m and u are as in Table 2, and either $t = 2^i$ with $i \leq m$, or $t = 2^i$ with $i \leq 2m$ when $y = 360$, or $t = 3^i$ with $i \leq m$ when $y = 504$, then output the series 1, G (since G is simple).

WLOG $|G|$ *can* be written in the form $|G| = tu \cdot y^m$ as above. (At this point we know that G is not simple; cf. COMPFY. The problem is to use this fact.)

7. Find a shortest orbit $Y = x'^{G_x}$ of G_x on $X - \{x\}$. (This will have length $m(n^* - 1)$ with the following exceptions: length $3m$ or $6m$ for $n^* = 10$, $y = 60$ or $n^* = 15$, $y = 360$, respectively.)

Find a non-trivial block system Σ for G_x^Y such that G_x^Σ is primitive, and let $B \in \Sigma$. (Here $|B| = |Y|/m$.)

Find $G_{x,(Y-B)}$ and $(G_{x,(Y-B)})'$. (These are small groups.)

Let $f \in G$ be such that $x^f = x'$, find $h \in G_{x'}$ with $x \in B^{fh}$, and replace f by fh. (Then $x \in B^f$.)

Find $S := \langle (G_{x,(Y-B)})', (G_{x,(Y-B)})^{tf} \rangle$. (This is a simple group of order y.)

Find a set Δ of m elements of G_x such that $\Sigma = B^\Delta$, and find $\{S_1, \ldots, S_m\} := \{S^d \mid d \in \Delta\}$.

Let $N := S_1 \times \cdots \times S_m$ (this is the socle of G).

Find the kernel K of the action of G on $\{S_1, \ldots, S_m\}$. Find a composition series for G/K. (Here G/K is a simple group unless $m = 8$ and $G/K = AGL(3,2)$, in which case a composition series is easily found.)

Output the groups $S_1 \times \cdots \times S_i$ for $i = 0, \ldots, m-1$; together with groups which, modulo N, are a G/K-composition series for the abelian group K/N of order t; as well as groups which, modulo K, are a composition series for G/K.

8. End.

THEOREM 3. *The output of* COMPSER *is correct.*

PROOF. Everything is similar to Theorem 2 except for Steps 4 and 7—but of course this time we have used ERNIE.

Cases (IIb)-(IId) are almost the same as in Theorem 1, except for (IId) with $k = 1$. Here $G = S_1 \times S_2$. This is handled in Step 4. For, $|G_x \Phi| = n^2 = |G|$ so $G = G_x \Phi$. Then computing conjugacy classes of involutions can be accomplished by brute force since $|G|$ is relatively small. The centralizer in S_1 of one of its involutions has order ≥ 4, so we only need to consider conjugacy classes of size $\leq |S_1|/4$. The smallest size of a conjugacy class evidently can only arise for a class inside S_1 or S_2. (N.B. Alternatively, in the situation of Step 4 one could either use $Z(C_G(G_{xx'}))$ for distinct x, x' just as in Neumann (1987), or the appropriate part of Luks (1987).)

When we get to Step 7 we know (cf. Theorem 2) that we can identify X with X_1^m as in Case (IIa). A simple group of order y acting on a set of size n^* is 2-transitive except in the case of A_5 in degree 10 and A_6 in degree 15 (Table 1). In all cases there is a unique shortest orbit Y of G_x on $X - \{x\}$: if $x = (\alpha, \alpha, \ldots, \alpha) \in X_1^m$ then $Y = (W, \alpha, \ldots, \alpha) \cup \cdots \cup (\alpha, \ldots, \alpha, W)$, where W is the shortest orbit of $(S_1)_x$ on $X_1 - \{\alpha\}$. Then B can be taken to be $(W, \alpha, \ldots, \alpha)$. Moreover, G_x acts 2-transitively on the "coordinates", so that B^{G_x} is the unique non-trivial block system on Y on which G_x acts primitively. Note that B^f is a non-trivial block of the unique shortest orbit Y^f of G_y, and that $x \in Y^f$. Thus, we can modify f (using h) so as to have $x \in B^f$. Now it is easy to check that $\langle (G_{x,(Y-B)})', (G_{x,(Y-B)})^{tf} \rangle = S_1$ in every case appearing in Table 1 (note that $G_{x,(Y-B)}$ can contain outer automorphisms of S_1). The m blocks in Σ correspond to the m direct factors of the socle of G. The remainder of Step 7 is now clear.

6. Concluding Remarks

When $n < 5^5$ some of our methods do not differ significantly from those of Neumann (1987). However, for various values of n he assumes that elements of a suitable prime order p, and Sylow p-subgroups, can be found efficiently; and in some situations he

requires finding the centralizer of a suitable p-element. While there are polynomial-time algorithms for some such problems (Kantor, 1985*b*), there have yet to be algorithms for solving them that are provably efficient in practice in all instances. In fact, finding centralizers is probably not, in general, possible in polynomial time (see Kantor (1988) for remarks concerning this observation of Luks). Our algorithms are designed to avoid these problems in the hope that this will increase efficiency.

While Luks' composition series algorithm (Luks, 1987) is polynomial-time, it requires dealing with sets of size $\theta(n^2)$. As already remarked, this is prohibitive for n somewhat large.

It should also be noted that we have avoided using too many relatively expensive normal closures—the obvious exception being the use of G'.

Finally, we remark that the algorithms presented here are readily extended to somewhat larger values of n by similar but more detailed arguments. We have chosen 10^6 as an arbitrary but reasonable-looking bound.

IMPLEMENTATION. Algorithms SIMPLY and COMPFY have been implemented in Cayley Version 3.7. According to J. J. Cannon, in one sample run the composition factors of PSL(2,7) *wreath* A_5, where $n = 8^5 = 32768$, were obtained in 11 100 seconds, 10 250 of which were consumed finding $|G|$, G_x and G' in Step 3 of COMPFY.

This research was supported in part by NSF Grant DMS 87-01794 and NSA Grant MDA 904-88-H-2040.

References

Aschbacher, M., Scott, L. L. (1985). Maximal subgroups of finite groups. *J. Algebra* **92**, 44–80.

Cameron, P. J. (1981). Finite permutation groups and finite simple groups. *Bull. LMS* **13**, 1–22.

Cannon, J. J. (1984). An introduction to group theory language Cayley. In: (Atkinson, M. D. ed.) *Computational Group Theory*, pp. 145–183. London: Academic Press.

Gorenstein, D. (1968). *Finite Groups.* New York: Harper and Row.

Guralnick, R. M. (1983). Subgroups of prime power index in a simple group. *J. Algebra* **81**, 304–311.

Kantor, W. M. (1985*a*). Some consequences of the classification of finite simple groups. In: (McKay, J. ed.) *Finite Groups—Coming of Age*, pp. 159–173. Contemporary Math. **45**, AMS.

Kantor, W. M. (1985*b*). Sylow's theorem in polynomial time. *J. Comp. Syst. Sci.* **30**, 359–394.

Kantor, W. M. (1988). Algorithms for Sylow p-subgroups and solvable groups. In: *Computers in Algebra* (*Proc. Conf. Chicago 1985*) pp. 77–90. New York: Dekker.

Kantor, W. M., Liebler, R. A. (1982). The rank 3 permutation representations of the finite classical groups. *TAMS* **271**, 1–71.

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

Neumann, P. M. (1987). Some algorithms for computing with finite permutation groups. In: (Robertson, E. F., Campbell, C. M. eds.) *Proceedings of Groups—St. Andrews 1985*, pp. 59–92. *London Math. Soc. Lect. Note* **121**, Cambridge University Press.

Zsigmondy, K. (1892). Zur Theorie der Potenzreste. *Monatsh. Math. Phys.* **3**, 265–284.