DIMACS Series in Discrete Mathematics
and Theoretical Computer Science
Volume **00**, 0000

Group Membership for Groups with Primitive Orbits

NAMITA SARAWAGI, GENE COOPERMAN, AND

LARRY FINKELSTEIN

ABSTRACT. This paper considers a permutation group $G = \langle S \rangle$ of degree n with t orbits such that the action on each orbit is primitive. It presents a $O(tn^2 \log^c(n))$ time Monte Carlo group membership algorithm for some constant c. The algorithm is notable for its use of a new theorem showing how to find $O(t \log^2 n)$ generators in $O\tilde{}(|S|n)$ time under a more general form of the above hypotheses. The algorithm relies on new combinatorial methods for computing with groups [**CF92**] and previous work of Babai, Luks and Seress [**BLS88**]. In addition, it makes extensive use of a structure theorem for primitive groups by Cameron [**Cam81**], which can be derived from results of Kantor [**Kan79**] and the classification of finite simple groups.

1. Introduction

New combinatorial methods for computing with permutation groups have recently been developed which have led to Monte Carlo algorithms for solving fundamental problems that have superior worst case asymptotic performance [**BCF$^+$91, BCF^{++}91, CF92**]. The main objective of this paper is to explore the power of these methods when additional assumptions are made concerning the nature of the action on the underlying point set. In particular, we prove the following result. We use the notation $O\tilde{}(f(n))$ to mean $O(f(n) \log^c n)$ for some constant c. This work is based on the thesis of Sarawagi [**Sar92**].

THEOREM 1.1. *Let $G = \langle S \rangle$ be a group acting on Ω, such that $S \subseteq \mathrm{Sym}(\Omega)$, $|\Omega| = n$, G has t orbits, and the action of G on each orbit is primitive. Then*

1991 *Mathematics Subject Classification.* Primary 20C40, 20P05.
The authors were supported in part by NSF Grants # CCR-8903952 and CCR-9204469.
This paper is in final form and no version of it will be submitted for publication elsewhere.

©0000 American Mathematical Society
0000-0000/00 $1.00 + $.25 per page

a strong generating set for G can be determined in $O^{\sim}(n|S| + tn^2)$ Monte Carlo time.

The proof of Theorem 1.1 is based on the procedure `SGS_Primitive_Orbits` in section 2 and given in Theorem 2.1.

The algorithm used to prove Theorem 1.1 relies on a classification of the orbits of a permutation group (Theorem 3.8). This classification of the primitive orbits makes extensive use of the classification of finite simple groups through a result of Cameron [**Cam81**], which in turn relies on work of Kantor [**Kan79**]. For our purposes, if G is a permutation group on an n-element set Ω and O is an orbit of G with G^O primitive, then O is a *small base* orbit if $|G^O| < |O|^{5 \log |O|}$ (Definition 3.13). The *Cameron* orbits (Definition 3.7) include all orbits that are not small base. In the latter case the structure of G^O is well determined by Theorem 3.9. In the special case where G^O contains $\mathrm{Alt}(O)$ we use an elegant algorithm for finding a 3-cycle due to Babai, Luks and Seress [**BLS88**]. If such an orbit is not small base, it is called a *giant* (Definition 3.13), as in [**BLS87**]. Note that if O is a giant orbit, then $|O| \geq 35$ (since otherwise $|G^O| < |O|^{5 \log |O|}$).

The algorithm proceeds in two phases. As a pre-processing step, the giant orbits are recognized and the points are re-ordered so that the points of the giant orbits are last in the ordering.

The first phase, described in section 3, uses a typical Sims-type control structure [**Sim**]. One finds a strong generating set for the action of the group on a non-giant orbit O, and generators for the pointwise set stabilizer of O. The action of the stabilizer subgroup on the next non-giant orbit is then considered. The key to this phase is controlling the number of Schreier generators for each point stabilizer subgroup as we proceed through a sequence of base points in O. Two techniques are used to achieve this control. First, it is noted that if O is a Cameron orbit, then the action on O, of the point stabilizer subgroup, is faithful on its second smallest orbit. Further, the length of that orbit is at most $3\sqrt{|O|}$. Second, a new theorem on reduction of generators is proved (Theorem 3.15), which shows that if we are given $O^{\sim}(t)$ generators for the current point stabilizer subgroup, then one can efficiently construct a generating set of size $O^{\sim}(t)$ for the next point stabilizer subgroup which guarantees that the total time to "process" the orbit is $O^{\sim}(nt|O|)$ Monte Carlo time. This reduction is accomplished using a generalization of combinatorial techniques first introduced in [**BCF$^+$91**] (see also [**CF92**] in this volume) rather than sifting. An interesting consequence of these techniques is the following corollary to Theorem 3.15 (for $H = G$).

Corollary 1.2. *Let $G = \langle S \rangle$ be a group acting on Ω with $|\Omega| = n$, and suppose G has t orbits, and the action of G on each orbit is primitive. Then a generating set for G containing $O(t \log^2 n)$ elements can be constructed in $O^{\sim}(n|S|)$ Monte Carlo time.*

In the second phase, described in section 5, one begins with generators for a normal subgroup N of G which is the pointwise set stabilizer in G of all non-giant orbits. Initially one works with the socle of N, denoted $\mathrm{Soc}(N)$. Because each giant orbit has size at least 35, the projection of $\mathrm{Soc}(N)$ on a remaining orbit is either trivial or a giant. The key to finding a strong generating set for $\mathrm{Soc}(N)$ is the "fast-giant" technique developed by Babai, Luks and Seress [**BLS88**], which allows the construction of a 3-cycle from a generating set for a giant in $O^{\sim}(n^2)$ Las Vegas time. Also needed is a fast normal closure algorithm described in [**BCF$^+$91**] The full strong generating set can then be constructed by viewing $N/\mathrm{Soc}(N)$ as a subgroup of an elementary abelian 2-group, and employing techniques of linear algebra.

The algorithms we present in this paper are all Monte Carlo. A Monte Carlo algorithm is a randomized algorithm whose reliability (probability of success) can be increased at the cost of additional time. The Monte Carlo nature of the main algorithm arises through multiple invocations of Monte Carlo subroutines. The subroutines have some small probability of returning an incorrect answer, and multiple invocations of the algorithms can lead to a large overall probability of error. However, all of the subroutines satisfy the property that if they run in time c for some input, and if they are allowed to run for an additional factor of time, t, then the probability of error will be ce^{-t}. Under these circumstances, one can always argue that if such an algorithm is invoked k times, then allowing an additional factor of $t = \log k$ time for each invocation will cause the overall probability of error to be bounded by c. The details of the argument are contained in Theorem A.2 of the appendix of [**CF92**], and formal definitions and related theorems are contained in the same appendix. Thus, some additional number of $\log n$ factors suffice to retain a reasonably small probability of error and for this reason, we may omit explicit proofs of reliability.

2. Overview of the Main Algorithm

In this section, we provide an overview of our main algorithm and the supporting subroutines. In order to highlight the underlying algorithmic ideas, we defer the formal timing analyses until later sections.

The ordering of Ω ultimately is determined by the algorithm as it processes the orbits in a top down fashion. We will denote by O_j, the j^{th} orbit which has been processed and set $O^{(i)} = \cup_{j=1}^{i-1} O_j$ for $1 \leq i \leq t+1$.

Procedure `SGS_Primitive_Orbits`
Input: (S, Ω) where $\langle S \rangle = G$ acts on Ω and has t primitive orbits
Output: A set U which is an SGS for G

Replace S by S' such that $G = \langle S' \rangle$ and $|S'| = O^{\tilde{}}(t)$
`Test_Giants`(S, Ω)
Reorder $\Omega = \cup_{i=1}^{t} O_i$ such that giant orbits are last

Initialize $S'' \leftarrow S'$, $i \leftarrow 1$ and $U \leftarrow \emptyset$
While $i \leq t$ and O_i is a non-giant orbit do
  $(U', S'') \leftarrow$ `SGS_Non-Giant_&_Orbit_Stabilizer`(S', S'', O_i, Ω)
    $[U'$ is a SGS for $G^{O_i}_{O^{(i)}}$ and $G_{O^{(i+1)}} = \langle S'' \rangle]$
  Add U' to U
Let A be the union of non-trivial orbits of $\langle S'' \rangle$
Add `SGS_Giant_Orbits`(S'', A) to U
Return U

THEOREM 2.1. *The procedure* ***SGS_Primitive_Orbits*** *is correct and runs in* $O^{\sim}(n|S| + tn^2)$ *Monte Carlo time.*

PROOF. The first step is to ensure that $|S|$ is not too large. This is accomplished using Theorem 3.3, which shows how to replace S by a generating set S' so that $|S'| = O^{\sim}(t)$ in $O^{\sim}(n|S|)$ Monte Carlo time. The algorithm then classifies the orbits into types giant and non-giant. This can be done in $O^{\sim}(tn^2)$ time (see Section 4). Using this classification, the orbits are reordered so that the non-giant orbits appear before the giant orbits. Let t' be the number of non-giant orbits.

For each i, $1 \leq i \leq t'$, `SGS_Non-Giant_&_Orbit_Stabilizer`(S', S'', O_i, Ω) is invoked. This routine outputs a SGS, U', for $G^{O^{(t'+1)}}$ and generators S'' for $G_{O^{(t'+1)}}$ in $O^{\sim}(tn|O_i| + n^2)$ Monte Carlo time by Theorem 3.1. Furthermore, the size of S'' is $O^{\sim}(t)$.

Continuing with i, $t' < i \leq t$, either $G^{O_i}_{O^{(t'+1)}}$ is a giant or acts trivially. If the action is that of a a giant, the algorithm invokes the procedure `SGS_Giant_Orbits` using the generators for $G_{O^{(t'+1)}}$. It is shown in Theorem 5.2 that this phase is correct and takes $O^{\sim}(tn^2)$ Monte Carlo time. Hence `SGS_Primitive_Orbits` is correct and runs in the stated time. □

3. Non-Giant Primitive Orbits

The iterative step in the main algorithm for a non-giant orbit can be formulated as follows. We are given a generating set S of size $O^{\sim}(t)$ for the normal subgroup $N = G_{O^{(i)}}$ of G. We must produce a set U of strong generators for $N^{O^{(i)}}$ and a generating set S' for $N_{O^{(i)}} = G_{O^{(i+1)}}$ of size $O^{\sim}(t)$. This is accomplished by the next procedure.

Procedure `SGS_Non-Giant_&_Orbit_Stabilizer`
  Input: (S, S', O, Ω) where $S, S' \subset \mathrm{Sym}(\Omega)$, $|S| = O^{\sim}(t)$, $|S'| = O^{\sim}(t)$,
    $N = \langle S' \rangle \trianglelefteq G = \langle S \rangle$, G has t primitive orbits and
    O is a non-giant G orbit.
  Output: A set $U \subset N$ which is an SGS for N^O
    and a generating set S'' for N_O of size $O^{\sim}(t)$.

  Let x_1 be an arbitrary point of O

Let O'_{x_1} be the smallest orbit of G_{x_1} acting on $O \setminus \{x_1\}$
Reorder the points of O such that x_1 is first followed by O'_{x_1}
Set $S'' \leftarrow S'$, $U \leftarrow \emptyset$
For each consecutive base point x_i ($i \geq 1$) in O do
  Let T be $O^{\sim}(1)$ elements of $\langle S'' \rangle$ such that $x_i^{\langle T \rangle} = x_i^{N_{x_1,\ldots,x_{i-1}}}$
    [T is constructed using Lemma 3.2(ii).]
  Add T to U
  Let C be a transversal for $N_{x_1,\ldots,x_i}$ in $N_{x_1,\ldots,x_{i-1}}$ built from T
  Let S_i be a set of Schreier generators for $N_{x_1,\ldots,x_i}$ built from S'' and C
  Replace S'' by a generating set for $N_{x_1,\ldots,x_i}$ of size $O^{\sim}(t)$ built from S_i
    [S'' is constructed using the argument in Theorem 3.15]
Output U and S''

THEOREM 3.1. *The procedure* ***SGS_Non-Giant_&_Orbit_Stabilizer*** *runs in Monte Carlo time $O^{\sim}(n|O|t)$ and outputs a generating set of size $O^{\sim}(t)$ for the point stabilizer of O.*

PROOF. The proof can be understood by quoting results from Sections 3.2 and 3.3 and deferring formal definitions and proofs of these results until those sections.

We analyze the time to construct S'' through each iteration of the loop, since this will dominate the running time for the procedure. First observe that by Lemma 3.17 the hypotheses of Theorem 3.15 are satisfied with regard to the subgroup $N_{x_1,\ldots,x_i}$.

If $\log |G^O| \leq 5 \log^2 n$ (O is a small base orbit), then there are $O^{\sim}(t|O|)$ Schreier generators, for $N_{x_1,\ldots,x_i}$. By Theorem 3.15, this generating set can be reduced to one of size $O^{\sim}(t)$ in Monte Carlo time $O^{\sim}(t|O|n)$. Since there are at most $O(\log^2 n)$ base points on O, the total time spent in a small base orbit O is $O^{\sim}(t|O|n)$.

If $\log |G^O| > 5 \log^2 n$, then O is a Cameron type orbit for which the smallest orbit of G_{x_1} on $O \setminus \{x_1\}$ has length at most $3\sqrt{|O|}$, by Lemma 3.12. There are $O^{\sim}(t|O|)$ Schreier generators for N_{x_1} and so the time to find $O^{\sim}(t)$ generators for N_{x_1} is $O^{\sim}(t|O|n)$, as for the small base case. For successive point stabilizers with $i > 1$, there are at most $O^{\sim}(t\sqrt{|O|})$ Schreier generators. One can replace them with $O^{\sim}(t)$ Schreier generators in $O^{\sim}(t\sqrt{|O|}n)$ Monte Carlo time by Theorem 3.15. Since there are at most $3\sqrt{|O|}$ base points on this orbit, that bounds the number of iterations, and the total time spent on a Cameron type orbit is also $O^{\sim}(t|O|n)$. □

3.1. Random Subproducts and Subgroup Chain Lengths. The algorithms presented in this paper make heavy use of combinatorial methods for computing with groups based on the notion of random subproducts. This has led to a rich supply of new randomized tools for computing with groups. In

this section, we will briefly review the specific ideas we require for this paper, and refer the reader to [**CF92**] in this volume for a more through treatment, including proofs.

A *random subproduct* of a sequence of group elements $(g_1, g_2, \ldots, g_k)$ is a product of the form ${g_1}^{e_1} {g_2}^{e_2} \cdots {g_k}^{e_k}$ where $e_i \in \{0, 1\}$ are selected independently from the uniform distribution over $\{0, 1\}$. Given a set, S, of generators of a group, G, and a transversal T of a point stabilizer subgroup G_x in G, a *random Schreier subproduct* is formed as follows. Form a random subproduct, g, of the sequence of group elements in S (for $h \in G$, let $\overline{h}$ be the unique element in T such that $h\overline{h} \in G_x$), form all Schreier generators $tg(\overline{tg})^{-1}$ for $t \in T$, and then form a random subproduct on this set of Schreier generators.

Random subproducts and random Schreier subproducts, though not purely random elements of G and G_x, respectively, have useful properties. The following lemmas describe these properties.

LEMMA 3.2. *Let $G = \langle S \rangle$ be an arbitrary permutation group acting on Ω with $|\Omega| = n$.*

(i) *Let $H < G$ be a proper subgroup. Then the probability that a random subproduct r (formed using S) is not in H is at least $1/2$.*

(ii) *There exists a constant $c > 0$ such that for arbitrary $d \geq 1$, if S' is a set of $cd \log n$ random subproducts on S, then with probability at least $1 - 1/n^d$, $\langle S' \rangle$ has the same orbit structure on Ω as G.*

(iii) *Let $x \in \Omega$, T a transversal of G_x in G, and $\overline{H} < G_x$ is a proper subgroup then the probability that a random Schreier subproduct, r_x, formed using S and T, is not in $\overline{H}$, is at least $1/4$.*

The proof of (i) and (ii) can be found in [**BCF$^+$91**] or [**CF92**]. The next theorem is a generalization of Theorem 2.3 in [**BCF$^+$91**]. For convenience, we base the proof on the version appearing as Theorem 2.9 in [**CF92**].

THEOREM 3.3. *Let $G = \langle S \rangle$ be a finite group. Let $H \leq G$, and let $\widehat{L}$ be a known upper bound on the length of all subgroup chains from H to G. Then for any fixed parameter p such that $0 < p < 1$, with probability at least p one can find a set $\widehat{S}$ with $|\widehat{S}| = O(\widehat{L} \log(1/(1-p)))$ using $O(|S| (\log \widehat{L}) \log(1/(1-p)))$ group operations such that $\langle \widehat{S}, H \rangle = G$.*

PROOF. The proof is given as a modification of the proof of Theorem 2.9 in [**CF92**] (this volume). One must initialize the S' of the original proof to T, a generating set for H, instead of the empty set, and interpret the L of the original proof as $|T| + \widehat{L}$. Further, if one replaces $\langle g_1, \ldots, g_{i-1} \rangle$ by $\langle H, g_1, \ldots, g_{i-1} \rangle$ everywhere, then the logic of the proof generalizes verbatim to the current theorem. The new generating set $\widehat{S}$ is then chosen as $S' \setminus T$, and $\langle \widehat{S}, H \rangle = G$. □

THEOREM 3.4. (*Cameron et al.* [**CST89**]*) Any subgroup chain of a permutation group of degree n has length at most $3n/2$.*

Another variation of the above theorem was proved by Babai [**Bab86**] with a bound of $2n - 3$.

LEMMA 3.5. (*Scott* [**Sco79**]) *Let $G = H_1 \times \ldots \times H_r$ be the direct product of non-abelian simple groups H_i, $1 \leq i \leq r$. Let M be a subgroup of G which projects onto each H_i for $1 \leq i \leq r$. Then there exists a partition $\{B_1, \ldots, B_s\}$ of $\{1, \ldots, r\}$ such that $M = D_1 \times \ldots \times D_s$ where each D_i is a diagonal subgroup of $\times_{j \in B_i} H_j$.*

COROLLARY 3.6. *Let W be the disjoint union of r sets W_i, each of size at least 2. Suppose that H is a subgroup of $G = \mathrm{Alt}(W_1) \times \cdots \times \mathrm{Alt}(W_r)$ and H projects onto $\mathrm{Alt}(W_i)$ for each i. Then the length of any chain of proper subgroups from H to G is at most $2r$.*

The proof follows easily from Lemma 3.5. If $|W_i| \neq 4$ for all i, then the alternating groups are simple, and a bound of at most r on the chain can be found. Otherwise, $2r$ subgroups may be needed.

3.2. Cameron Groups. We begin by defining a class of primitive groups referred to as *Cameron* groups.

DEFINITION 3.7. Let (k, r, s) be a triple of positive integers such that $k \geq 5$ and $s \leq k/2$. Let C be the disjoint union of r sets $B_1, \ldots, B_r$ each of size k and let $A = \{X \subset C \mid \forall i, |X \cap B_i| = s\}$. If G is a transitive subgroup of $\mathrm{Sym}(C)$ for which each B_i, $1 \leq i \leq r$, is a block of imprimitivity and if G contains $\mathrm{Alt}(B_1) \times \cdots \times \mathrm{Alt}(B_r)$, then G^A is a primitive group (as can be seen by noting that the point stabilizer subgroup must be maximal in G). G^A is said to be a *Cameron type group* with parameters (k, r, s). G^C is called the *natural* or *imprimitive Cameron action*.

In the discussion to follow, we often directly identify elements $X \in A$ with subsets of C satisfying the property $|X \cap B_i| = s$ for $1 \leq i \leq r$. Note that the socle, $\mathrm{Soc}(G)$, has a faithful representation on C as $\mathrm{Alt}(B_1) \times \cdots \times \mathrm{Alt}(B_r)$, and that $\mathrm{Soc}(G)$ is a single minimal, normal subgroup. It is easy to verify that the action of G on the set $\{X \subset C \mid |X \cap B_i| = s\}$ is primitive, by noting that the point stabilizer subgroup must be maximal in G. Maximality follows from the characterization of the point stabilizer subgroup in Lemma 3.14.

The motivation for defining Cameron groups is the following theorem due to Cameron [**Cam81**]. It is based on the classification of finite simple groups, and on work by Kantor on permutation representations of classical groups [**Kan79**].

THEOREM 3.8. [**Cam81**] *Let G be a primitive group acting on n points. If $|G| \geq n^{5 \log n}$, then $n = \binom{k}{s}^r$ and G is a Cameron group of type (k, r, s).*

The following lemma gives some properties of a Cameron group. The calculations are based on those in [**BLS87, BLS88**], but have been re-calculated to achieve tighter bounds. The logarithmic base is 2 unless otherwise specified.

LEMMA 3.9. *Let G be a Cameron type group with parameters (k, r, s) acting on A. Let $|A| = n$. Then,*

(i) $n = \binom{k}{s}^r$;
(ii) $rs \log(k/s) \leq \log n$;
(iii) $k \leq \sqrt{2n}$ *when* $r > 1$ *or* $s > 1$, *otherwise* $k = n$;
(iv) $\log |G| < \frac{(\log n)\ \log\log n}{s \log(k/s)} + \frac{k}{s} \log n + \frac{k}{s} \log n \frac{\log s}{\log(k/s)}$;

PROOF. Part (i) is clear. Part (ii) follows from $(\frac{k}{s})^{rs} \leq \binom{k}{s}^r$. In part (iii), for fixed n, k is maximized when $r = 1$ and $s = 2$, and the bound follows from (i). For part (iv), the inequality follows from $|G| \leq r!(k!)^r \leq r!\binom{k}{s}^{rk/s}(s!)^{rk/s} = r!n^{k/s}(s!)^{rk/s}$. After applying part (ii), $\log |G| \leq r \log r + k/s \log n + rk/s \log(s!) < \frac{(\log n)\ \log\log n}{s \log(k/s)} + \frac{k}{s} \log n + \frac{k}{s} \log n \frac{\log s}{\log(k/s)}$. □

DEFINITION 3.10. Let $G = G^A$ be a Cameron type group with parameters (k, r, s). For $X \in A$ (and $B_1, \ldots, B_r$ as in Definition 3.7), define the G_X-orbit $\Sigma_1(X)$ to be the set

$$\{Y \in A \mid \exists j,\ 1 \leq j \leq r,\ \forall i \neq j,\ |Y \cap X \cap B_j| = s - 1,\ Y \cap B_i = X \cap B_i\}.$$

It is clear that $\Sigma_1(X) \subset A$ is an orbit of the point stabilizer subgroup G_X. The next lemma provides a finer estimate of calculations based on Theorem 4.1 of [**BLS87**].

LEMMA 3.11. *Let $G = G^A$ be a Cameron type group. For arbitrary $X \in A$, the action of G_X on $\Sigma_1(X)$ is faithful. If G is not a giant, then $|\Sigma_1(X)| \leq 3\sqrt{n} - 1$, and therefore $\Sigma_1(X) \cup \{X\}$ is a base for G of size at most $3\sqrt{n}$. If $\log |G| > 5(\log n) \log\log n$, then $\Sigma_1(X)$ is the smallest orbit of G_X in $A \setminus \{X\}$.*

PROOF. The action of G_X on C has orbits $X \cap B_j$ and $(C \setminus X) \cap B_j$ for $1 \leq j \leq r$. To see that the action is faithful, we show that the kernel is trivial. Let $g \in G_X^C$ be non-trivial. Let $g' \in G_X^A$ correspond to g under the permutation equivalence. There is a $y \in B_j \subseteq C$ for some j, such that $y^g \neq y$. If $y \in X \cap B_j$, choose $Y \in \Sigma_1(X)$ such that $Y \cap B_i = X \cap B_i$ for $i \neq j$, and $Y \cap B_j = ((B_j \cap X) \setminus \{y\}) \cup \{z\}$ for arbitrary $z \in B_j \setminus X$. If $y \in B_j \setminus X$, choose $Y \in \Sigma_1(X)$ such that $Y \cap B_i = X \cap B_i$ for $i \neq j$, but $Y \cap B_j = ((B_j \cap X) \setminus \{z\}) \cup \{y\}$ for arbitrary $z \in B_j \cap X$. Since $y^g \neq y$, it is clear that $Y^{g'} \neq Y$, and so G_X is faithful on $\Sigma_1(X)$.

The length of $\Sigma_1(X)$ is $rs(k - s)$. If G is not a giant, then $r > 1$ or $s > 1$, and Lemma 3.9(ii, iii) yields $rs(k-s) \leq (k-s)(\log n)/\log(k-s) < k\,(\log n)/\log k \leq 2^{3/2}\sqrt{n} < 3\sqrt{n}$. Direct calculation shows that $\Sigma_1(X)$ is the smallest orbit of G_X in $A \setminus \{X\}$ except possibly when $s \geq \lfloor (k-1)/2 \rfloor$. Consider an orbit $\Sigma_2(X)$ with parameters t_1 and t_2 such that for all $Y \in \Sigma_2(X)$, $|Y \cap B_i \setminus X| = t_1 > 0$ and $|Y \cap B_j \setminus X| = t_2 > 0$ for some $i \neq j$. (It is clear that this property will be preserved for all points in the same orbit.) Then $|\Sigma_2(X)| \geq q\binom{s}{t_1}\binom{k-s}{t_1}\binom{s}{t_2}\binom{k-s}{t_2} > |\Sigma_1(X)|$ when $s = t < \lfloor (k-1)/2 \rfloor$. Here, q is

the number of distinct intersection patterns, $(|Y \cap B_1 \setminus X|, \ldots, |Y \cap B_r \setminus X|)$, for $Y \in \Sigma_2(X)$. It is easy to show that $q \geq r$, using the transitivity of the action of G on $\{B_1, \ldots, B_r\}$. Next, consider an orbit $\Sigma_3(X)$ with parameter t such that for all $Y \in \Sigma_3(X)$, $|Y \cap B_i \setminus X| = t > 1$ and $|Y \cap B_j \setminus X| = 0$ for some i and for all $j \neq i$. Then $|\Sigma_3(X)| = r\binom{s}{t}\binom{k-s}{t} > |\Sigma_1(X)|$ when $s = t < \lfloor (k-1)/2 \rfloor$.

If $\Sigma_1(X)$ is not the smallest orbit, then $s \geq \lfloor (k-1)/2 \rfloor$, and one has the estimates $s \geq 2$, $2 \leq k/s \leq 5/2$, $n \geq 10$, and $\log s \leq \log\log n$. (The last inequality follows from Lemma 3.9(ii).) Applying Lemma 3.9(iv) shows that $\log |G| \leq 5(\log n) \log\log n$. So, $\Sigma_1(X)$ is the smallest orbit of G_X when $\log |G| > 5(\log n) \log\log n$. □

COROLLARY 3.12. *If G is primitive of degree $n \geq 2$, and $\log |G| > 5\log^2 n$, then G is of Cameron type and the second smallest orbit of its point stabilizer subgroup, G_x, is $\Sigma_1(x)$. Further, the action of G_x on $\Sigma_1(x)$ is faithful. If G is not a giant, then $|\Sigma_1(x)| < 3\sqrt{n}$.*

PROOF. For $n \geq 2$, Theorem 3.8 shows that G is of Cameron type. Since $5\log^2 n > 5(\log n)\log\log n$ for $n \geq 2$, the remaining conclusions follow from Lemma 3.11. □

This motivates the next definition. The restriction of *giants* to groups of degree n at least 35 avoids certain pathological case that would have arisen in section 5 if $n = 4$ or $n = 6$.

DEFINITION 3.13. A *small base group* is a group of degree n such that $\log |G| \leq 5\log^2 n$. A *giant* is a group of the form S_n or A_n that is not of type small base. This implies that $n > 10$ for giants. An orbit of G is identified as large, small base, or Cameron type according to whether the action of G on that orbit is a group of the corresponding type.

LEMMA 3.14. *Let $G = G^A$ be a primitive Cameron group with parameters (k, r, s) such that $|A| = n$ and let G^C be the imprimitive Cameron action. Let $X \in A$ and let $Y_1, \ldots, Y_m$ be a sequence of points in $\Sigma_1(X)$. Let $H = G_{X,Y_1,\ldots,Y_m}$. Then H has a normal subgroup K such that K^C has orbits $U_i = X_i \cap Y_1 \cap \cdots \cap Y_m$ and $V_i = (B_i \setminus X_i) \cap (B_i \setminus Y_1) \cap \cdots \cap (B_i \setminus Y_m)$, $1 \leq i \leq r$ and $K^C = \mathrm{Alt}(U_1) \times \mathrm{Alt}(V_1) \times \cdots \times \mathrm{Alt}(U_r) \times \mathrm{Alt}(V_r)$. Furthermore, H^C acts faithfully on $(\cup_{i=1}^r U_i) \cup (\cup_{i=1}^r V_i)$ (and hence permutes the set $\{U_1, V_1, \ldots, U_r, V_r\}$).*

PROOF. Note that G_X satisfies the conclusion. Note that $X \setminus Y_i$ and $Y_i \setminus X$ are trivial orbits of $G_{X,Y_1,\ldots,Y_i}$ for $1 \leq i \leq m$. Each non-trivial orbit of $G_{X,Y_1,\ldots,Y_{i-1}}$ is formed from the set difference of an orbit of $G_{X,Y_1,\ldots,Y_i}$ and the union of the two trivial orbits. So, the conclusion will continue to be satisfied for all i. □

3.3. Main Result. There are two situations where we require reduction of generators. The first is in `SGS_Primitive_Orbits` when we are given the initial generating set S for G and want to reduce it to one of size $O^{\sim}(t)$. The second occurs in `SGS_Non-Giant_&_Orbit_Stabilizer` when we construct the Schreier

generators for a point stabilizer and want to reduce it to one of size $O^{\sim}(t)$ for the next round. The hypotheses of the following result are designed to capture both instances.

THEOREM 3.15. *Let G acting on Ω have t primitive orbits. Let $H = \langle S \rangle$ be a subgroup of G that acts faithfully on $A \subseteq \Omega$, where A is a union of some of the G-orbits, $O_1, \ldots, O_t$. Each O_i is either a small base orbit or a Cameron orbit or both. Without loss of generality, assume that the Cameron orbits appear as $O_1, \ldots, O_r$ for $r \leq t$. Assume that if G^{O_i} is a Cameron orbit with parameters (k_i, r_i, s_i) and C_i supports the natural action of G^{O_i}, then the following holds for H^{C_i}.*

(i) *There exist mutually disjoint subsets $V_1^i, \ldots, V_{\ell_i}^i$ of C_i such that H^{C_i} acts faithfully on $U_i = \cup_{j=1}^{\ell_i} V_j^i$.*
(ii) *$\mathrm{Alt}(V_1^i) \times \cdots \times \mathrm{Alt}(V_{\ell_i}^i)$ is normal in H^{U^i} (and so H^{U^i} permutes the sets $\{V_1^i, \ldots, V_{\ell_i}^i\}$).*
(iii) *$\ell_i \leq 2r_i \leq 2 \log n$.*

Then in $O^{\sim}(|S|n)$ Monte Carlo time, one can construct a generating set S' for H such that $|S'| = O(t \log^2 n)$.

The proof of Theorem 3.15 follows directly from Lemma 3.16 and Theorem 3.3.

LEMMA 3.16. *Assume the hypotheses of Theorem* 3.15 *Let M be a subgroup of H generated by $\Omega(\log n)$ random subproducts of S. Then $L(M, H) = O(t \log^2 n)$.*

PROOF. Assume first that each of the orbits O_i is a Cameron orbit. Let $U = \cup_{i=1}^{t} (\cup_{j=1}^{\ell_i} V_j^i)$, so that G acts faithfully on U and permutes the sets $\{V_j^i \mid 1 \leq j \leq \ell_i, 1 \leq i \leq t\}$.

For each V_j^i, let $d_j^i = \min(|V_j^i| - 2, 6)$ and define the set $\binom{V_j^i}{d_j^i}$ to be the set of all subsets of V_j^i of size d_j^i. Let $\mathcal{U} = \cup_{i=1}^{t} (\cup_{j=1}^{\ell_i} \binom{V_j^i}{d_j^i})$. Then H acts faithfully on $\mathcal{U}$ and $|\mathcal{U}| \leq \sum_{i=1}^{t} (\sum_{j=1}^{\ell_i} |V_j^i|^6) \leq \sum_{i=1}^{t} |U_i|^6 \leq \sum_{i=1}^{t} |C_i|^6 \leq \sum_{i=1}^{t} |O_i|^6 \leq n^6$. By Lemma 3.2, $\Omega(\log n)$ random subproducts on S will generate a subgroup M which has high probability of having the same orbits on $\mathcal{U}$ as H. Since $H_{\{V_j^i\}}^{V_j^i}$ contains $\mathrm{Alt}(V_j^i)$ it follows that $\binom{V_j^i}{d_j^i}$ is contained in an orbit of $M^{\mathcal{U}}$. But any element of M^U that which takes one d_j^i subset of V_j^i to another must stabilize V_j^i. So the set stabilizer $M_{\{V_j^i\}}$ is d_j^i-transitive on V_j^i. So, $M_{\{V_j^i\}}^{V_j^i}$ contains $\mathrm{Alt}(V_j^i)$. We will use this property to show that $L(M, H) = O(t \log^2 n)$. Note that the orbits of M on U are the same as those of H on U.

Define $\widehat{H} = H^{U_1} \times \cdots \times H^{U_t} \leq \mathrm{Sym}(U)$. We will show that $L(M, \widehat{H}) = O^{\sim}(t)$, which suffices since $M \leq H \leq \widehat{H}$. Let

$$\widehat{K} = \bigvee_{\substack{1 \leq i \leq t \\ 1 \leq j \leq \ell_i}} \mathrm{Alt}(V_j^i),$$

so that $\widehat{K} \leq \widehat{H}$. Consider the (possibly unfaithful) action of $\widehat{H}$ on $\{V_j^i \mid 1 \leq j \leq \ell_i, 1 \leq i \leq t\}$. By (iii), there are at most $2t \log n$ elements in this set. Moreover, the kernel of the action contains $\widehat{K}$ with index at most $2^{2t \log n}$. It then follows from this and the bound on the length of subgroup chains in symmetric groups (Theorem 3.4), that $L(\widehat{K}, \widehat{L}) = L(\widehat{H}/\widehat{K}) \leq 2t \log n + 3/2(2t \log n) \leq 5t \log n = O^{\sim}(t)$.

Since $\widehat{K}$ is normal in $\widehat{H}$, it remains to estimate $L(M, \widehat{K})$. Let $M = M_0 < M_1 < \cdots < M_p = \widehat{H}$ be a proper chain of subgroups. By retaining only the subgroups in the chain that satisfy $M_{i+1} \cap \widehat{K} > M_i \cap \widehat{K}$, we construct a new chain

$$M \cap \widehat{K} = K_0 < K_1 < \cdots < K_{p'} \leq \widehat{K}$$

for $p' \leq p$, such that for each r with $1 \leq r \leq p$ there is a unique s such that $K_r = M_s \cap \widehat{K}$. Note that $L(M \cap \widehat{K}, \widehat{H}) \leq p' + L(\widehat{K}, \widehat{H})$. So, we must estimate p', which will be an upper bound on $L(M, \widehat{K})$.

We show that $(K_r)^{V_j^i}$ is either the alternating or trivial group. Let s correspond to r, so that $M_s \cap \widehat{K} = K_r$. Note that $M_s \cap \widehat{K} \lhd M_s$ and $(M_s)^{V_j^i}_{\{V_j^i\}} \geq \mathrm{Alt}(V_j^i)$. So, $(M_s \cap \widehat{K})^{V_j^i} \lhd (M_s)^{V_j^i} \cap \mathrm{Alt}(V_j^i)$. Thus, if $d_j^i \neq 4$, then $(K_r)^{V_j^i} = (M_s \cap \widehat{K})^{V_j^i}$ is either $\mathrm{Alt}(V_j^i)$ or the trivial group. Hence, this is true for all K_r, $1 \leq r \leq p'$.

For each K_r, the action on each component with $d_j^i \neq 4$ must be alternating or trivial. Let u_r be the number of components on which there is an alternating action. By Lemma 3.5, the action on the u_r alternating components decomposes into the direct product of $v_r \leq u_r$ actions, where each of the v_r actions is a diagonal of alternating actions on a subset of the $\{V_j^i\}$. Further, if $K_{r+1} < K_r$, then $u_{r+1} > u_r$ or $v_{r+1} > v_r$. Since $u_{p'} \leq 2t \log n$ and $v_{p'} \leq 2t \log n$, $p' \leq 4t \log n$. On the other hand, if each of the orbits have length 4, then a similar argument, in conjunction with Corollary 3.6 shows that $v_{p'} \leq 4t \log n$ and so $p' \leq 6t \log n$.

We have shown that the result holds in the case where all the orbits O_i are Cameron orbits. The general case now follows easily by applying this result to the action of G on the union of the Cameron orbits and observing that the kernel of the action is faithfully represented on a union of small base group orbits of G on Ω. The kernel has order at most $2^{2t \log^2 n}$ by Theorem 3.8, yielding a bound of $2t \log^2 n$ for the subgroup chain length. □

The final result in this section describes the situation in which Theorem 3.15 is invoked.

LEMMA 3.17. *Let G acting on Ω have t primitive orbits and let N be a normal subgroup of G. Let O be a G-orbit and $x_1, \ldots, x_\ell$ a sequence of base points in O for N^O chosen so that x_i, $2 \leq i \leq \ell$ is in the smallest orbit of G_{x_1} acting on O. Let A be the union of O and all G-orbits O_j such that $N_O^{O_j}$ is non-trivial. Then $N_{x_1,\ldots,x_{i-1}}$ and A satisfy the hypotheses of Theorem* 3.15*, where $N_{x_1,\ldots,x_{i-1}}$ is identified with H.*

PROOF. It is clear that N acts faithfully on A. Let $O_j \subseteq A$ be a Cameron type orbit with $O \neq O_j$. Since $N_O^{O_j}$ is a non-trivial normal subgroup of G^{O_j}, $N_O^{O_j}$ contains the socle of G^{O_j}. This is also true for $N_{x_1,\ldots,x_\ell}^{O_j}$, and so the hypotheses of Theorem 3.15 are satisfied with regard to $N_{x_1,\ldots,x_\ell}$ and O_j whenever O_j is a non-giant Cameron orbit. It remains to verify the hypotheses when O is a non-giant Cameron orbit. But this follows directly from Lemma 3.14 and the assumption on how the sequence $x_1, \ldots, x_\ell$ is chosen. □

4. A Monte Carlo Test for Giant Action

In the main procedure `SGS_Primitive_Orbits`, it is necessary to classify the t primitive orbits of G into types giant and non-giant. In this section we present a $O^{\sim}(tn^2)$ Monte Carlo time algorithm for accomplishing this task. The procedure `Test_Giants` is based on repeated application of Theorem 3.15. This allows for a simple exposition of the algorithm.

Procedure `Test_Giants`
  Input: (S, Ω) where $S \subseteq \mathrm{Sym}(\Omega)$, $|S| = O^{\sim}(t)$,
    $G = \langle S \rangle$ and G has t primitive orbits.
  Output: Each orbit is identified as type giant or non-giant

  For each orbit O of G do
    If $|O| < 35$ then mark O as non-giant
    Else set $S' \leftarrow S$
      Choose points $x_1, \ldots, x_6$ in O
      For $i \leftarrow 1$ to 6 do
        Let T be $O^{\sim}(1)$ random subproducts of $\langle S' \rangle$ such that
          $x_i^{\langle T \rangle} = x_i^{G_{x_1,\ldots,x_{i-1}}}$
        If $|x_i^{\langle T \rangle}| \neq |O| - i + 1$ then
          Mark O as a non-giant and break from the loop
        Let C be a transversal for $G_{x_1,\ldots,x_i}$ in $G_{x_1,\ldots,x_{i-1}}$ built from T
        Let S'' be a set of Schreier generators for $G_{x_1,\ldots,x_i}$ built from S'' and C
        Replace S' by a generating set for $G_{x_1,\ldots,x_i}$ of size $O^{\sim}(t)$ built from S''

THEOREM 4.1. *Procedure `Test_Giants` is correct and runs in Monte Carlo time $O(tn^2)$.*

PROOF. The algorithm simply tests whether G^O is 6-transitive. The correctness of this approach is a consequence of the classification of finite simple groups [**Gor82**]. In addition, we need to invoke Lemma 3.17 in order to ensure that the the hypotheses of Theorem 3.15 apply. The time for each orbit is easily seen to be $O^{\sim}(t|O|n)$ from Theorem 3.15 and this then leads to the stated time bound.
□

5. Giant Orbits

In this section, we describe the procedure `SGS_Giant_Orbits`. When this procedure is called, `SGS_Primitive_Orbits` has computed a set of $O^{\sim}(t)$ generators for the pointwise stabilizer of all the non-giant orbits. Since this subgroup is normal, the action on the remaining non–trivial orbits must be of giant type. This justifies the assumptions made for the input to `SGS_Giant_Orbits`. The procedure constructs a strong generating set for the input group in two stages. First, `SGS_Alt_Orbits` (described later) is invoked to compute a strong generating set for the alternating action on each orbit and then a standard linear algebra argument is invoked in order to complete the strong generating set to one for the entire group. Corollary 5.1 reveals the structure of G as a direct product of alternating groups which act diagonally on subsets of the orbits.

Procedure `SGS_Giant_Orbits`
  Input: (S, A) where $\langle S\rangle = G \leq Sym(\Omega)$, G acts faithfully on $A \subseteq \Omega$,
    A is a union of giant orbits $O_1, \ldots, O_t$ of G and $|S| = O^{\sim}(t)$.
  Output: T such that T is a SGS for G with respect to an ordering
    determined by the algorithm.

  $T \leftarrow$ `SGS_Alt_Orbits`(S, A)
    [T is a SGS for $G \cap (\mathrm{Alt}(O_1) \times \cdots \times \mathrm{Alt}(O_t))$]
  Let $S' = \{s \in S \mid s|_{O_i}$ is odd for some $O_i\}$
  [Simulate Gaussian elimination on G/G']
  For $i \leftarrow 1$ to t do
    Let s' be the first element of S' such that $s'|_{O_i}$ is odd (if it exists)
    If such an s' exists then
      Set $S' \leftarrow S' \setminus \{s'\}$
      Set $s' \leftarrow$ the residue of sifting s' through T on O_i
      [$s'|_{O_i}$ is now a 2-cycle]
      Set $T \leftarrow T \cup \{s'\}$
      Set $S' \leftarrow S's'^{-1}$
    Replace each $s \in S'$ by the residue of sifting s through T on O_i
      [S'^{O_i} is now trivial]
  Return T

The next procedure makes use of a fast normal closure routine, developed in [**BCF+91**], and described further in [**CF92**] (this volume). It also refers to a procedure `Three_Cycle` due to Babai, Luks and Seress and is described in [**BLS88**]. If a group specified by a generating set of size $O^{\sim}(n)$ contains the alternating group, then this procedure will construct a three-cycle in $O^{\sim}(n^2)$ Las Vegas time.

Procedure `SGS_Alt_Orbits`
Input: (S, A) as in `SGS_Giant_Orbits`
Output: a SGS, T, for $G \cap (\mathrm{Alt}(O_1) \times \cdots \times \mathrm{Alt}(O_t))$
with respect to an ordering determined by the algorithm.

Initialize $T \leftarrow \emptyset$
Let all orbits be unmarked.
Mark the first orbit, O_1, of G
Let $x \in O_1$ and S' a set of Schreier generators for G_{x_1} formed from S
For $i \leftarrow 2$ to t do
If S' has a fixed point on O_i then mark O_i
[In our setting, this is true if and only if $G_{O_1}^{O_i}$ is trivial.]
Let T' be a SGS for $G^{O_1} \cap \mathrm{Alt}(O_1)$ whose elements act as 3-cycles on O_1
[By invoking `3-Cycle`]
Replace each element in T' by its square [This ensures that $T' \subseteq \mathrm{Alt}(\Omega)$]
For each unmarked orbit O of G do
Let S'' be a generating set for $S^{O_1 \cup O}$ of size $O^{\sim}(1)$
[Found by applying Theorem 3.15]
Set $\sigma_{\overline{O}} \leftarrow$ `Element_Fixing_an_Orbit`(S'', O_1, O)
Let $\mathcal{O}$ be the set unmarked orbits on which $\sigma_{\overline{0}}$ acts non-trivially
Let $\overline{O} = \cup_{O \in \mathcal{O}} O$ and $n_{\overline{O}} = |\mathcal{O}|$
Let $\sigma'_{\overline{O}}$ be the residue of sifting $\sigma_{\overline{O}}$ through T
[$\sigma'_{\overline{O}}|_{\overline{O}} = \sigma_{\overline{O}}|_{\overline{O}}$ and is trivial elsewhere.]
Let $S'_{\overline{O}}$ be a set of $O(n)$ generators for the normal closure of $\langle \sigma'_{\overline{O}} \rangle$ in G
[The "fast normal closure" routine is used"]
Let $S''_{\overline{O}}$ be a reduced set of $O^{\sim}(n_{\overline{0}})$ generators for $\langle S'_{\overline{O}} \rangle$
Set $T \leftarrow$ `Prepend` (`SGS_Alt_Orbits`$(S''_{\overline{O}}, \overline{O})$, T)
Mark all orbits in $\overline{O}$
Set $T \leftarrow$ `Prepend`(T', T)
Return T

Procedure `Element_Fixing_an_Orbit`
Input: (S, O_1, O_2) where O_1 and O_2 are unlinked giant
orbits for $G = \langle S \rangle$ and $|S| = O^{\sim}(1)$.
Output: An element of G_{O_1} which acts non-trivially on O_2.

$\sigma \leftarrow$ `Three_Cycle` (S, O_1)
Set $\sigma \leftarrow \sigma^2$ [to ensure that $\sigma \in \mathrm{Alt}(O_1 \cup O_2)$]
Let $\sigma|_{O_1} = (a\ b\ c)$, $\sigma|_{O_2} = \delta$
If δ is non-trivial then
  Let U be a set of $O^{\sim}(1)$ generators for $G_{a,b,c}$
    [Found by repeated application of Theorem 3.15]
  Let g be an element of U such that $[g, \sigma] = [g, \delta] \neq 1$
    [Since $\mathrm{Alt}(O_2) \leq \langle S \rangle^{O_2}$, δ is not centralized by S]
  Return($[g, \sigma]$)
Else [$\delta = (a\ b\ c)$]
  Let T be a SGS for G^{O_1} constructed from $(a\ b\ c)$ with $T \subseteq G_{O_2}$
  For each $s \in S$ do
    Let $s' \in G_{O_1}$ be the residue of s sifted through T
    If $s' \neq 1$ return(s')

5.1. Giant Orbits: Proof of Correctness. The proof of correctness for `SGS_Alt_Orbits` follows directly from the following result.

COROLLARY 5.1. *Assume that $G \leq \mathrm{Sym}(\Omega)$ and that $\mathrm{Soc}(G)$ acts as the full alternating group on each orbit O_i, $1 \leq i \leq t$ of G. Then there exists a partition of $\{O_1, \ldots, O_t\}$ into subsets $\{B_1, \ldots, B_s\}$ such that $\mathrm{Soc}(G)$ is the direct product of alternating groups, with each direct factor acting as a diagonal subgroup on the orbits in precisely one of the blocks B_i and fixes pointwise the orbits in the other blocks. Furthermore, if $\sigma \in \mathrm{Soc}(G)$, then the normal closure of $\langle \sigma \rangle$ in G is the product of the diagonal subgroups corresponding to the blocks B_i on whose orbits σ acts non-trivially.*

THEOREM 5.2. *Let $G = \langle S \rangle$ act on Ω with $|\Omega| = n$. Assume that G has t giant orbits and that $|S| = O^{\sim}(t)$. Then the procedure `SGS_Giant_Orbits` constructs a SGS for G in $O^{\sim}(tn^2)$ Monte Carlo time.*

PROOF. The proof of correctness and the timing for `SGS_Giant_Orbits` is clear once the corresponding results have been proved for `SGS_Alt_Orbits`.

The correctness of `SGS_Alt_Orbits` relies on Corollary 5.1. As long as there are unmarked orbits, the procedure will construct a non-identity element $\sigma'_{\overline{O}}$ which fixes pointwise each marked orbit and acts non-trivially on the union $\overline{O}$ of a subset of unmarked orbits. In the notation of Corollary 5.1, $\overline{O}$ is the union of a certain number of the $B'_i s$. Thus the normal closure of $\sigma'_{\overline{O}}$ in G is a direct factor of $\mathrm{Soc}(G)$ consisting of the pointwise stabilizer in $\mathrm{Soc}(G)$ of $\Omega \setminus \overline{O}$. A recursive call is made and once a strong generating set has been computed it is prepended to the set T which holds elements of the strong generating set currently being accumulated.

In analyzing the timing, it is straightforward to show that the top-level call to `SGS_Alt_Orbits` takes time $O(tn^2)$ aside from the recursive calls to smaller problems. By induction, each recursive call to a subproblem takes time $O(n_{\overline{O}}n^2)$, where $n_{\overline{O}}$ is the number of orbits O_i in $\overline{O}$ and $\overline{O}$ is a union of blocks B_j as given in Corollary 5.1. Since a recursive call at the top-level never involves an orbit O_i more than once, the total time spent on the recursive calls is $O^{\sim}(tn^2)$. □

References

[Bab86] L. Babai. On the length of chains of subgroups in the symmetric group. *Comm. in Algebra*, 14:1729–1736, 1986.

[BCF+91] L. Babai, G. Cooperman, L. Finkelstein, E.M. Luks, and Á. Seress. Fast Monte Carlo algorithms for permutation groups. In *Proc. 23rd ACM STOC*, pages 90–100, 1991.

[BCF++91] L. Babai, G. Cooperman, L. Finkelstein, and Á. Seress. Nearly Linear Time Algorithms for Permutation Groups with a Small Base. In *Proc. ISSAC '91* (International Symposium on Symbolic and Algebraic Computation '91), ACM Press, pages 200–209, 1991.

[BFP89] C.A. Brown, L. Finkelstein, and P.W. Purdom. A new base change algorithm for permutation group. *SIAM J. Computing*, 18:1037–1047, 1989.

[BLS87] L. Babai, E. Luks, and Á. Seress. Permutation groups in NC. In *Proc. 19th ACM STOC*, pages 409–420, 1987.

[BLS88] L. Babai, E. Luks, and Á. Seress. Fast management of permutation groups. In *Proc. 19th IEEE FOCS*, pages 272–282, 1988.

[Cam81] P.J. Cameron. Finite permutation groups and finite simple groups. *Bull. London Math. Soc.*, 13:1–22, 1981.

[CF92] G. Cooperman and L. Finkelstein. Combinatorial tools for computational group theory. In *DIMACS Proceedings* (this volume), 1992.

[CFS90] G. Cooperman, L. Finkelstein, and N. Sarawagi. A random base change algorithm for permutation groups. In *Proc. of 1990 International Symposium on Symbolic and Algebraic Computation*, pages 161–168, Tokyo, Japan, August 1990. ACM Press and Addison-Wesley.

[CST89] P.J. Cameron, R. Solomon, and A. Turull. Chains of subgroups in symmetric groups. *J. of Algebra*, 127:340–352, 1989.

[Gor82] D. Gorenstein. The Classification of Finite Simple Groups, Vol. 1. Plenum Press, New York, 1982.

[Kan79] W.M. Kantor. Permutation representations of the finite classical groups of small degree or rank. *J. Algebra*, 60:158–168, 1979.

[Luk90] E. Luks. Lectures on polynomial-time computation in groups. Technical Report NU-CCS-90-16, College of Computer Science, Northeastern University, 1990.

[Sar92] N. Sarawagi. Computational Group Theory and Applications to Search. Ph.D. Thesis, Northeastern University, 1992.

[Sco79] L. Scott. Representations in characteristic p. The Santa Cruz Conference on Finite Groups, 1980, Amer. Math. Soc., 319–322.

[Sim] C.C. Sims. Computation with permutation groups. In *Proc. Second Symposium on Symbolic and Algebraic Manipulation*, ACM Press, New York, 1971, pages 23–28.

College of Computer Science, Northeastern University, Boston, Massachusetts 02115

Current address: Namita Sarawagi, Department of Mathematics and Computer Science, Rhode Island College, N. Providence, RI 02911

E-mail address: gene@ccs.northeastern.edu, laf@ccs.northeastern.edu, and FACSARAWAGI@ric.edu