NOTE ON POLYNOMIAL-TIME GROUP THEORY

W.M. Kantor*
University of Oregon

Given a "small" subset Γ of S_n, what properties of $G = \langle\Gamma\rangle$ can be found efficiently? This question has been important for the construction of sporadic groups, and for Cannon's Cayley [2], where "efficient" meant "reasonably cheap to implement on a computer". There is another meaning of the word "efficient" within the context of theoretical Computer Science: "requiring polynomial time". This note is a brief survey of some recent work on polynomial-time group theoretic algorithms.

Consider $G \leq S_n = \mathrm{Sym}(X)$, where $|X| = n$. We are concerned with algorithms requiring at most $p(n)$ steps, where $p(n)$ is a polynomial in n. (Here, we are assuming that $|\Gamma|$ is small: of polynomial size.) For example, in $n(n-1)/2$ steps you can examine every 2-element subset of X. On the other hand, it would take $n!$ steps to examine each element of S_n, and many subgroups of S_n also fail to have polynomial orders. Thus, polynomial time (i.e., a polynomial number of steps) imposes restrictions not normally encountered in ordinary group theory.

The most basic algorithm is that of Sims [9] (cf. [3]), which finds $|G|$ and generators for G_x, $x \in X$, in polynomial time. More generally, given $Y \subseteq X$, this algorithm finds the pointwise stabilizer of Y in G in polynomial time. Moreover, Sims' algorithm produces a generating set of size $\leq n^2$ for G. (N.B. - We are dealing with generating permutations, not with generators and relations: no relations are available.)

The following can also be found in polynomial time, and the proofs are all easy ([1], [3], [8]): all orbits of G; if G is transitive, a complete system of imprimitivity Σ such that $|\Sigma| > 1$ and G^Σ is primitive; $\langle S^G\rangle$ for any given subset S of G; the derived series of G; and the center of G.

Centralizers present an enormous stumbling block. It is not

*Supported in part by NSF Grant MCS 7903130-82.

difficult to show that, if a polynomial-time algorithm for finding (generators for) $C_G(t)$, $t \in G$, $t^2 = 1$, were available, then there would be a polynomial-time algorithm for the Graph Isomorphism problem ("Given two n-vertex graphs, are they isomorphic?"). This is an important open problem in Computer Science (cf. [7]). Therefore, centralizers cannot be used, so that many of the familiar techniques of group theory must be avoided. On the other hand, this prohibition also suggests that group theoretic algorithms can lead to new results within Computer Science [7]. In any event, the restriction on time forces a rethinking of many group theoretic methods and problems.

The classification of finite simple groups has entered into this area. There is a polynomial-time algorithm for finding a composition series of G [8]. The validity of this algorithm depends upon the truth of Schreier's conjecture. There is also a polynomial-time algorithm for finding an element of order p, given a prime p [5]. Here, one easily reduces to the case in which G is simple and primitive on X, at which point tedious use of the results of [4] and linear algebra produce the desired element. Once again, the validity of the algorithm depends upon the classification. (N.B. - The algorithm used by Cayley involves the random selection of a few elements of G, each of which is checked to see if p divides its order. This process requires exponential time, as does Sims' centralizer algorithm used by Cayley.

Polynomial-time versions of Sylow's theorem have yet to be found. (One cannot use the familiar approach involving centralizers.) However, special cases have been obtained, when G is simple [5], solvable [6], or has all its noncyclic composition factors suitably restricted [6]. Specifically, assume that a bound b is given, and that each noncyclic composition factor either has order $\leq b$, is an exceptional Chevalley group, or is a classical group of dimension $\leq b$. Then the following can be done in polynomial time (the polynomial depending on b) [6]: any given p-subgroup can be embedded in a Sylow p-subgroup; and given (generators for) two Sylow p-subgroups of G, an element of G can be found conjugating the first to the second. In [6] there are also polynomial-time versions of the standard results concerning Hall subgroups of solvable groups, as well as versions of both parts of the Schur-Zassenhaus theorem when G is restricted as above.

It should be clear that the results just described primarily concern algorithmic versions of undergraduate-level group theory (even

though some proofs require the classification). But then, the subject of this note is just in its infancy. In order to make this fact even clearer, we conclude with some problems that are presently OPEN. (1) Prove Sylow's theorem for arbitrary G (both finding Sylow subgroups and conjugating them). (2) Given m, determine whether G has an element of order m. (This is even open if m is a prime power.) (3) Find a minimal normal subgroup of G. (4) If $G \rhd N$ and the extension splits, find a complement. (5) If G is solvable, find a system normalizer and a Carter subgroup. (6) If $G, H \leq S_n$, find (generators for) $G \cap H$. (A polynomial-time algorithm for this problem would, however, settle the Graph Isomorphism problem.)

REFERENCES

1. Atkinson, M.D. (1975). An algorithm for finding the blocks of a permutation group. Math. of Comp. 29, 911-913.
2. Cannon, J.J. (1980). Effective procedures for the recognition of primitive groups. Proc. Symp. Pure Math. 37, 487-493.
3. Furst, M., Hopcroft, J. & Luks, E. (1980). Polynomial-time algorithms for permutation groups. Proc. 21st IEEE Symp. Found. Comp. Sci., 36-41.
4. Kantor, W.M. (1979). Permutation representations of the finite classical groups of small degree or rank. J. Algebra. 60, 158-168.
5. Kantor, W.M. Polynomial-time algorithms for finding elements of prime order and Sylow subgroups. (submitted)
6. Kantor, W.M. & Taylor, D.E. Polynomial-time versions of Sylow's theorem. (in preparation)
7. Luks, E. (1982). Isomorphism of graphs of bounded valence can be tested in polynomial time. J. Comp. Syst. Sci. 25, 42-65.
8. Luks, E. (unpublished)
9. Sims, C.C. (1978). Some group-theoretic algorithms. Springer Lecture Notes in Math. 697, 108-124.