Chapter 19. Some Other Algorithms

This chapter presents a brief discussion of algorithms for permutation groups which are not treated in the book. The algorithms and the ideas behind them are important, but not fundamental enough to warrant a detailed presentation in this book. Pointers to the literature are given.

Single Coset Enumeration

There are several different kinds of problems addressed when enumerating the (left or right) cosets of a subgroup H of a permutation group G.

Problem 1: Given a permutation $g \in G$, determine a canonical representative of the coset $g \times H$.

Problem 2: Determine a set of coset representatives of H in G.

Problem 3: Determine the action of G on the cosets of H in G. That is, provide a permutation representation of G of degree $|G:H|$ such that H is isomorphic to the point stabiliser in this representation.

A solution to Problem 1 provides a solution to the other problems. However, one can often solve Problem 3 without defining a canonical coset representative.

The first approach for permutation groups relies on the ordering of elements of G induced from an ordering of the points such that the base points come first in the ordering. The canonical coset representative is the first element in the coset, and is formed by a process similar to testing membership. It is discussed in C.C. Sims, "*Computation with permutation groups*", **SYMSAM '71** (Proc. 2nd Symp. Symbolic and Algebraic Manipulation, Los Angeles, 1971), S.R. Petrick (ed.), ACM, New York, 1971, pp.23-28; J.S. Richardson, **GROUP: A computer system for group-theoretical calculations.** M.Sc. Thesis, University of Sydney, 1973; G. Butler, "*Effective computation with group homomorphisms*", J. Symbolic Comp., **1** (1985) 143-157.

Other orderings of the elements allow one to inductively work up the stabiliser chain, see D.F. Holt, "*The calculation of the Schur multiplier of a permutation group*", **Computational Group Theory,** M.D. Atkinson (ed.), Academic Press, Academic Press, 1984, pp.307-319, for hints.

A special case, important in enumerating combinatorial objects, has G equal to the symmetric group-see M. Furst, J.E. Hopcroft, and E. Luks, "*Polynomial-time algorithms for permutation groups*", Proc. 21st IEEE Foundations of Computer Science, 1980, pp.36-41; L. Allison, "*Generating coset representatives for permutation groups*", J. Algorithms **2** (1981) 227-244; M. Jerrum, "*A compact representation for permutation groups*", Proc. 23rd IEEE Foundations of Comp. Science, 1982, pp.126-133. (and J. Algorithms **7** (1986) 60-78.) Jerrum formulates Problem 1 and 2 in terms of topological sorts of a complete labelled branching of H.

Recently, the problems have been addressed by working up chains of subgroups involving set or block stabilisers: J.D. Dixon, and A. Majeed, "*Coset representatives for permutation groups*", Portugaliae Mathematica **45**, 1 (1988) 61-68; Wang DaFang, "*A new method for computation of permutation representations of a finite group*", manuscript, 1988.

A very space-efficient solution to Problem 3 is described in G. Cooperman and L. Finkelstein, "*New methods for using Cayley graphs in interconnection networks*", to appear in Discrete Applied Mathematics.

Double Coset Enumeration

There are several different kinds of problems addressed when enumerating the double cosets $H \times g \times K$ of subgroups H and K of a permutation group G.

Problem 1: Given a permutation $g \in G$, determine a canonical representative of the coset $H \times g \times K$.

Problem 2: Determine a set of double coset representatives of H and K in G.

The obvious way to approach the task is to solve Problem 3 of the single cosets of H, and then form the orbits of K. Each orbit of K in this representation corresponds to a double coset. This approach is used in D.F. Holt, "*The calculation of the Schur multiplier of a permutation group*", **Computational Group Theory,** M.D. Atkinson (ed.), Academic Press, Academic Press, 1984, pp.307-319.

Problem 1 has been addressed in G. Butler, "*On computing double coset representatives in permutation groups*", **Computational Group Theory,** M.D. Atkinson (ed.), Academic Press, Academic Press, 1984, pp. 283-290, where the canonical representative is the first element in the coset under the usual induced lexicographical ordering.

Several papers deal with the special case where G is the symmetric group, and the subgroups H and/or K are Young subgroups (that is, partition stabilisers in the symmetric group). H. Brown, L. Hjelmeland, and L. Masinter, "*Constructive graph labeling using double cosets*", Discrete Mathematics **7** (1974) 1-30; H. Brown, "*Molecular structure elucidation III*", SIAM J. Applied Math. **32**, 3 (1977) 534-551; R. Grund, **Computerunterstützte Konstruktion von speziellen Doppelnebenklassentransversalen und deren Anwendungen auf die konstruktive Kombinatorik**, Diplomarbeit, Universität Bayreuth, 1989; R. Grund, "*Symmetrieklassen von Abbildungen und die Konstruktion von diskreten Strukturen*", Bayreuther Mathematische Schriften **31** (1990) 19-54. B. Schmalz, **Computerunterstützte Konstruktion von Doppelnebenklassenrepräsentanten mit Anwendungen auf das Isomorphieproblem der Graphentheorie**, Diplomarbeit, Universität Bayreuth, 1989; B. Schmalz, "*Verwendung von Untergruppenleitern zur Bestimmung von Doppelnebenklassen*", Bayreuther Mathematische Schriften **31** (1990) 109-143.

Verify

An algorithm to verify that a base and strong generating set is correct was developed by Sims during the construction of several sporadic simple groups. It has been implemented by John Brownie and John Cannon to handle more general cases, and is effective for permutation groups of degree one million. See C.C. Sims, "*A method for constructing a group from a subgroup*", **Topics in Algebra,** (Proceedings of 18th Summer Research Institute, Canberra, 1978), M.F. Newman (ed.), Lecture Notes in Mathematics **697**, Springer-Verlag, Berlin, 1978, and forthcoming papers.

Conjugacy Classes of Elements

The conjugacy classes of elements of a group G plays a critical role in many algorithms concerned with the global structure of a group, such as algorithms for computing the lattice of subgroups or normal subgroups, the character table, the automorphism group, and the maximal subgroups.

For small groups, the obvious approach is to consider the group G acting on its elements by conjugation, and to compute the orbits.

For highly transitive groups, a method of Sims computes representatives of the orbits of G on k-tuples (for small values of k), and then considerings brackettings of the points in the tuple as cycles of possible canonical representatives of the conjugacy classes. See C.C. Sims, "*Determining the conjugacy classes of a permutation group*", **Computers in Algebra and Number Theory,** G. Birkhoff and M. Hall, Jr (eds), SIAM-AMS Proc., **4**, Amer. Math. Soc., Providence, R.I., 1971, pp.191-195. The method was implemented and studied by G. Butler, **Computational Approaches to Certain Problems in the Theory of Finite Groups**, Ph. D. Thesis, University of Sydney, 1980, but does not appear to be generally effective.

The thesis also introduces a random method for finding class representatives that is effective for groups of moderate degree and order which are close to being simple.

An inductive approach, which uses a lot of group-theoretic knowledge and algorithms is described in G. Butler, "*An inductive schema for computing conjugacy classes in permutation groups*", TR 394, Basser Department of Computer Science, University of Sydney, 1990.

Cohomology

The work of Derek Holt on cohomology has integrated many machine representations of groups to tackle a complex problem, and has led to several new algorithms that have fundamental significance : D.F. Holt, "*A computer program for the calculation of the Schur multiplier of a permutation group*", **Computational Group Theory,** M.D. Atkinson (ed.), Academic Press, Academic Press, 1984, pp. 307-319; D.F. Holt, "*A computer program for the calculation of a covering group of a finite group*", J. Pure Applied Algebra **35** (1985) 287-295; D.F. Holt, "*The mechanical computation of first and second cohomology groups*", J. Symbolic Comp. **1** (1985) 351-361.

Group Recognition

Given a set of generators for a group G, it is useful to be able to recognise whether G is the alternating or symmetric group of the same degree, because these groups are very large and may be the worst cases for the algorithm one is about to apply (even though the answer in these cases may be obvious). Much work has been done on this problem, see J.J. Cannon, "*A computational toolkit for finite permutation groups*", **Proceedings of the Rutgers Group Theory Year, 1983-1984,** M. Aschbacher, D. Gorenstein, R. Lyons, M. O'Nan, C. Sims, W. Feit (editors), CUP, New York, 1984, pp.1-18.

It is also useful to be able to recognize a group G as an explicit abstract group in some classification, such as the doubly-transitive groups, or primitive groups, or simple groups. In the latter case, one may first have to show the group is simple. These problems are addressed in J.J. Cannon, "*Effective procedures for the recognition of primitive groups*", **The Santa Cruz Conference on Finite Groups,** AMS Proc. Symp. Pure Mathematics **37** (1980) 487-493; P.M. Neumann, "*Some algorithms for computing with permutation groups*", **Groups - St Andrews 1985**, E.F. Robertson and C.M. Campbell (eds), London Mathematics Society Lecture Notes **121**, Cambridge University Press, Cambridge, 1986, pp. 59-92.

Composition factors

The composition factors of a group G are the simple groups which occur as factors groups H/N, for some subgroup H of G and normal subgroup N of H. The algorithms reduce to the primitive case, and then utilise the O'Nan-Scott Theorem and the classification of finite simple groups. Of theoretical interest is E.M. Luks, "*Computing the composition factors of a permutation group in polynomial time*", Combinatorica **7** (1987) 87-99. Implementations by John Cannon follow the algorithms described in P.M. Neumann, "*Some algorithms for computing with permutation groups*", **Groups - St Andrews 1985**, E.F. Robertson and C.M. Campbell (eds), London Mathematics Society Lecture Notes **121**, Cambridge University Press, Cambridge, 1986, pp. 59-92; and more recently, the algorithm of W.M. Kantor, "*Finding composition factors of permutation groups of degree* 10^6", to appear in J. Symbolic Comp.

Some Ideas From Complexity Results

There are several exciting advances in the complexity of group theoretic problems, that may indeed impact upon methods for effective computation. We highlight those we consider most significant or most accessible to the reader: L. Babai, E. Luks, A. Seress, "*Fast management of permutation groups*", Proc. 28th IEEE Symposium on Foundations of Computer Science, 1988, pp.272-282; G. Cooperman, L. Finkelstein and E. M. Luks, "*Reduction of group constructions to point stabilizers*", **ISSAC 89**, (Proc. 1989 ACM Symposium on Symbolic and Algebraic Computation, Portland, Oregon), ACM Press, New York, 1989, pp.351-356; W.M. Kantor and E.M. Luks, "*Computing in quotient groups*", Proc. 22nd ACM Symposium on Theory of Computing, Baltimore, 1990, pp.524-534; L. Babai, "*Local expansion of vertex-transitive graphs and random generation in finite groups*", Proc. 23nd ACM Symposium on Theory of Computing, 1991, to appear; L. Babai, G. Cooperman, L. Finkelstein, E. Luks, A. Seress, "*Fast Monte Carlo algorithms for permutation groups*", Proc. 23nd ACM Symposium on Theory of Computing, 1991, to appear.