RANDOM WALKS IN LARGE FINITE GROUPS

Marston Conder

University of Auckland, Private Bag Auckland, New Zealand

ABSTRACT

The use of random element generation is described as a means of accounting for representatives of certain classes of elements in large finite groups (when the production or storage of such classes is restricted by the available computing resources), in the context of solving the genus problem for some of the sporadic finite simple groups.

1. INTRODUCTION

Analysis of the structure of a given finite group can often be performed with the aid of a computer, and the CAYLEY system in particular, provided the group has a concrete representation (either as a permutation group, or matrix group, or in terms of generators and relations). Certain questions can often be answered using a mixture of theoretical and computational techniques, and even when the representation is large, successful approaches to some quite difficult problems may be found. One such approach involves the use of random element generation, in the case where the production or storage of large classes of elements is restricted by the resources available. This sort of approach is discussed in this paper, in the context of solving the genus problem for some of the sporadic finite simple groups.

Before explaining the background to the genus problem, we acknowledge that this has little to do with random walks in their usual sense — and apologise for any confusion the title may cause. On the other hand, however, it does show how a technique from "applied mathematics" can be used to answer questions in what is essentially "pure mathematics".

The *symmetric genus* $\sigma(G)$ of a finite group G was defined by Tom Tucker in [9] as the smallest genus of all those closed orientable surfaces (2-manifolds) on which G acts faithfully as a group of automorphisms, that is, homeomorphisms of the surface onto itself, preserving the local structure but allowing reversal of the surface's orientation.

Australasian Journal of Combinatorics 4(1991),pp 49-57

Also he defined the *strong symmetric genus* $\sigma^{\circ}(G)$ of G to be the smallest genus of those surfaces on which G acts faithfully as a group of orientation-preserving automorphisms, so that $\sigma(G) \le \sigma^{\circ}(G)$ in general — although in many cases these two numbers coincide (for instance when G has no subgroup of index two).

By extending a theorem of Hurwitz, Tucker showed that if $\sigma(G) > 1$ (that is, if G does not act faithfully on either the sphere or the torus), then both $|G|/(\sigma(G)-1)$ and $|G|/(\sigma^{\circ}(G)-1)$ are bounded above, by 168 and 84 respectively; furthermore, he showed that when values close to these bounds are attained, the group G has at least one generating-set of a given number of types, determined by the orders of the generators and their products (or their commutators).

He also considered what is known simply as the *genus* $\gamma(G)$ of G, namely the smallest genus of all such surfaces into which can be embedded some Cayley graph for G, and showed that $\gamma(G) \le \sigma(G) \le \sigma^{\circ}(G)$: any generating-set which corresponds to the action of G on some surface of genus $\sigma(G)$ provides a Cayley graph embeddable in that surface; on the other hand the regular action of G on one of its Cayley graphs need not necessarily extend to an action of G on an embedding surface, so $\gamma(G)$ and $\sigma(G)$ do not always coincide.

Whichever type of "genus" is of interest, the Riemann-Hurwitz equation may be used to enumerate the types of generating-sets that need to be considered for a given group.

For example, when $\sigma^{\circ}(G)$ satisfies $6(\sigma^{\circ}(G)-1) < |G| < 84(\sigma^{\circ}(G)-1)$, the exact value of $\sigma^{\circ}(G)$ may be determined by finding from among the following types of sets one which gives the smallest possible value of the quantity M :

(i) a generating-triple (x, y, z) of elements of orders p, q and r respectively, such that xyz is the identity element, and $M = 1-(1/p+1/q+1/r)$;

(ii) a generating-quadruple (x, y, z, w) of elements of orders p, q, r and s respectively, such that xyzw is the identity, and $M = 2-(1/p+1/q+1/r+1/s)$.

In the optimal case, $\sigma^{\circ}(G)$ is then given by $\sigma^{\circ}(G) = 1 + {}^{1}\!/_{2}M|G|$ (see [**9**] or [**10**]).

Precisely this sort of information has been used to calculate the "genus" (in one form or other) of a number of finite groups — see [**2**], [**3**], [**5**], [**6**] and [**10**]. In particular, the determination of the symmetric genus of all but three of the sporadic finite simple groups is announced in [**6**].

Some of the methods most commonly used in this context are discussed briefly in the next Section, and further techniques involving random element generation are described in Section 3.

2. FURTHER BACKGROUND

The usual approach when attempting to determine the symmetric genus of a given finite group is to first make a list of types of possible generating-set, ranked in ascending order of the associated genus (given by the Riemann-Hurwitz formula), and then to eliminate each possibility in turn until one is found that succeeds. For simple groups (which have no subgroup of index 2), this often amounts to enumerating triples (p, q, r) of orders of elements of the group, ranked according to the value of $M = 1 - (1/p + 1/q + 1/r)$, and then finding the first such triple for which the group can be "(p, q, r)-generated" — that is, generated by elements x , y and z of elements of orders p, q and r respectively, with xyz the identity element. For example, in the case of the Mathieu group M_{12} (which has elements of orders 1 , 2 , 3 , 4 , 5 , 6 , 8, 10 and 11 only), such a check-list begins with the possibilities of (2, 3, 8)-, (2, 4, 5)- and (2, 3, 10)-generation, and once the first two cases are eliminated, and (2, 3, 10)-generation is established, the symmetric genus of M_{12} is found to be $1 + {}^1\!/_2(1 - ({}^1\!/_2 + {}^1\!/_3 + {}^1\!/_{10}))\,|M_{12}|$, that is, 3169.

There are numerous ways of establishing the generation or non-generation of a group G by a given type of set. Perhaps the most powerful methods involve the use of character theory and local analysis, as illustrated in the final Section of [**10**], for example. On the other hand, when it comes to eliminating possibilities of certain types, there are a couple of simple tricks which can be easier to apply and yet just as effective.

One such trick involves a theorem of Ree [**8**] on permutations: if $x_1, x_2, \ldots, x_m$ are permutations generating a transitive group on a set Ω of size n , such that $x_1x_2 \ldots x_m$ is the identity permutation, and c_i is the number of orbits of $\langle x_i \rangle$ on Ω for $1 \leq i \leq m$, then $c_1 + c_2 + \ldots + c_m \leq (m-2)n + 2$. (In other words, the generating permutations cannot have more than $(m-2)n + 2$ cycles between them.) For alternative proofs of this result and a similar one for matrix representations, see [**4**] and the references listed there.

Ree's theorem places an obvious restriction on the cycle structures of possible generators in any known transitive permutation representation of the group G; but of course the inequality can still be satisfied by permutations which generate a proper, imprimitive, or even intransitive subgroup of the image group, in which case other means may be required to eliminate the associated type(s) of possible generating-set.

In the case of generating-triples, the standard character-theoretic formula for the calculation of class multiplication constants is particularly useful for determining the actual number of triples of a given type. Specifically, if K_1, K_2 and K_3 are conjugacy classes of elements in the group G, the number of pairs (x, y) with $x \in K_1$, $y \in K_2$ and $xy \in K_3$ is given by

$$\frac{|K_1|\,|K_2|\,|K_3|}{|G|} \sum_{i=1}^{m} \frac{\chi_i(K_1)\,\chi_i(K_2)\,\overline{\chi_i(K_3)}}{\chi_i(1)}$$

where $\chi_1, \chi_2, \dots, \chi_m$ are the irreducible complex characters of G, $\chi_r(K_s)$ denotes the common value of the character χ_r on the class K_s, and $\overline{}$ is complex conjugation.

This formula is easy to apply, given the character table for G. The problem is to determine which triples (if any) generate the whole group, rather than a proper subgroup, and often that may involve some extensive local analysis.

One way around this problem, especially suitable in the case of groups which have permutation representations of small degree, involves the use a computer. In particular, the CAYLEY system (see [**1**]) can be used to create a list of all the appropriate triples, by enumerating the elements of the class K_1, and then for any fixed $z \in K_3$, checking every element x in K_1 to see whether $x^{-1}z \in K_2$; once the set of all such x is found, the order (and other properties) of the subgroup generated by each triple $(x, x^{-1}z, z)$ can be computed. Alternatively — and this applies not only in the cases of triples — subgroups of small index may be found in the abstract group whose presentation is given by the type of possible generating-set, and the corresponding factor groups (induced by the natural action on cosets) analysed to see if G occurs (*c.f.* [**2, 5**]).

3. USE OF RANDOM ELEMENT GENERATION

In the case of permutation groups of somewhat larger degree, the computing methods referred to at the end of the previous Section may no longer be appropriate — especially so for the "low index subgroups" method, as the time taken to find subgroups of index n in a given finitely-presented group increases exponentially with n. Nevertheless, as long as the computer is able to handle the given permutation representation in a comfortable fashion (and for CAYLEY, this can now mean representations of degrees up to several thousand), answers to questions like those which arise from the genus problem may often be found.

Incidentally, we note that storage of permutation groups in CAYLEY is achieved through the use of a *base* and a *strong generating set* (see [**1**] for references). In rough terms, a base is a set of points with the property that every element of the group is uniquely determined by its effect on those points, and a strong generating set is a particular set of generators for the group, constructed in such a way that every element has a unique expression as a word in those generators, determined by its effect on a given base. Thus a relatively small amount of space can be used to store quite large finite groups — that is, without actually listing all their elements.

CAYLEY also has the facility for generating (pseudo-) random elements of a group, and indeed this is an integral part of some of its other capabilities, such as the enumeration of element conjugacy classes.

The latter process is a useful initial step in a search for the sorts of minimal generating-sets required for genus questions, but sometimes — as in the case of permutation groups of large degree — it cannot be successfully completed, for whatever reasons. On the other hand, usually not all the conjugacy classes are required, and an interactive search can be made for representatives of the classes that are of interest. For example, in the case of the simple Conway group Co_2, whose smallest-degree faithful permutation representation is on 2300 points, random generation might produce an element with cycle structure $20^{112}\,10^5\,4^2\,2^1$, and then its 4 th power would be an element from the class 5B, its 5 th power a representative of the class 4G, and its 10 th power a representative of the class 2C (*c.f.* the ATLAS [7]). Even such a näive approach as this takes little time to produce the required representatives.

The same sort of idea may obviously be used also in producing a selection of triples of elements of the required type: if x and z are known representatives of the classes K_1 and K_2 (as denoted in Section 2), then for every choice of a random element g one may check whether $(g^{-1}xg)^{-1}z$ is in K_2, by looking at its order or cycle structure perhaps, and if it is, then $(g^{-1}xg, (g^{-1}xg)^{-1}z, z)$ will be a suitable triple of elements from the classes K_1, K_2 and K_3 respectively.

In this way generation of the group G by a set of a particular type may easily be established, that is, after a brief random selection of conjugates of a fixed element of the class K_1.

What is more difficult is to prove that none of the triples of a given type generate G.

In the case of small groups, one can always resort to an enumeration of all elements of K_1 (or of K_2 or K_3). When it comes to larger groups, however, such an exhaustive enumeration may be impossible; but still it may be possible to account for the appropriate triples, again by random selection:

First note that the number of pairs (x, y) with $x \in K_1$, $y \in K_2$, and product xy equal to a fixed element $z \in K_3$, is obtainable from the formula given in Section 2.

Also note that these pairs fall into equivalence classes under conjugation by elements of the centralizer of z in G: if $c \in C_G(z)$ then $(c^{-1}xc, c^{-1}yc)$ is an equivalent pair, with $c^{-1}xc\,c^{-1}yc = c^{-1}xyc = c^{-1}zc = z$, and $\langle c^{-1}xc, c^{-1}yc \rangle = c^{-1}\langle x, y \rangle c \cong \langle x, y \rangle$. In particular, all that really needs to be done is to account for representatives of all $C_G(z)$-classes of such pairs.

An easy way to set about doing this involves again letting g run through a random selection of elements of G, checking in each case to see whether $(g^{-1}xg)^{-1}z$ is in K_2, but this time keeping a record of representatives of those distinct $C_G(z)$-classes of elements of K_1 that have been met. Then whenever a random conjugate of x is found to provide a pair of the required sort, but is a conjugate by some element in $C_G(z)$ of an element previously found to have this property, it is discarded, and the next one chosen. If the next random conjugate is of the right sort and does not provide a pair that is equivalent to one found already, then it is added to the set of representatives.

Such a method is invoked in the following CAYLEY procedure, where x, y and z are initial representatives of the conjugacy classes K_1, K_2 and K_3 of elements of the group called "g":

```
cz=centralizer(g,z);
oy=order(y); csy=cycle structure(y);
repset=[]; nxs=0; ncs=0;
for i=1 to 2000 do
  r=ranelt(g);m=order(r);
  for j=1 to m-1 do  u=u^r;
    if order(u^-1*z) eq oy then
      if cycle structure(u^-1*z) eq csy then
        uc=u^cz;
        if order(uc meet repset) eq 0 then
          repset=repset join [u];
          nxs=nxs+order(uc); ncs=ncs+1;
          print ' '; print ncs,order(uc),nxs,order(<u,z>);
         end;
       end;
     end;
   end;
  if nxs eq ntr then break; end;
 end;
```

Here the variables " repset ", " nxs " and " ncs " respectively stand for the set of representatives of $C_G(z)$-classes of conjugates of x, the number of conjugates of x found so far to provide pairs of the required sort, and the number of $C_G(z)$-classes of such pairs found so far. The constant "ntr" is the actual number of pairs that need to be accounted for, obtained from the formula given earlier, and the variable "r" is of course a randomly chosen element of the group.

At any particular stage of the process, the variable " u " is a conjugate of x, and the command " u = u^r " replaces u by $r^{-1}ur$, another random conjugate of x. Also, rather than choosing a new random element r every step of the way, the procedure uses the current r as many times as it can (that is, up to $m-1$ times, where m is its order), without obviously obtaining the same u as obtained a few steps previously. Even in this non-standard fashion, the steps used in obtaining such conjugates of x may be thought of as part of a random walk through the group G. The command " uc = u^cz " enumerates the elements of the class cu of all conjugates of u by elements of $C_G(z)$, denoted by cz; this class is of course expected to be much smaller than the whole of K_1, and hence capable of temporary storage. The other parts of the procedure should be self-explanatory.

Analogues of this procedure were used successfully by the author in a joint project with Robert Wilson and Andrew Woldar on determining the symmetric genus of some of the sporadic finite simple groups — and specifically, the groups McL, Suz and Co_2, which have smallest-degree faithful permutation representations on 275, 1782 and 2300 points respectively.

The answers are announced in [6], with the details expected to appear in a sequel, however one of the cases that had to be eliminated provides a good illustration of the method outlined here, namely the possibility of generation of Co_2 by a pair of elements from the classes 2C and 4G with product in the class 5B. The group Co_2 itself has order 42 305 421 312 000, the class 2C has size 28 690 200, and the centralizer of an element of 5B has order 600; and given any element z in 5B, there are 18000 pairs (x, y) with x in 2C, y in 4G, and $xy = z$. Obviously it would be impractical to enumerate all the elements of 2C, and for this reason the random conjugates method was adopted. As it turned out (after several hours of computing time), all 18000 pairs were found to generate proper subgroups of Co_2, as follows:

9 $C_G(z)$-classes of pairs, each class of size 600, generate subgroups of order 88 704 000,

6 $C_G(z)$-classes of pairs, each class of size 600, generate subgroups of order 1 351 680,

8 $C_G(z)$-classes of pairs, each class of size 600, generate subgroups of order 368 640,
8 $C_G(z)$-classes of pairs, each class of size 300, generate subgroups of order 5 120,
1 $C_G(z)$-classes of pairs, of size 600, generate subgroups of order 600, and
4 $C_G(z)$-classes of pairs, each class of size 300, generate subgroups of order 120.

Incidentally, we note that this information may lead to a proof by hand that (2C, 4G, 5B)-generation of Co_2 is impossible — indeed the results of such computation often point the way for the appropriate local analysis.

Finally we consider some of the probabilistic aspects of this method. First of all, every time a new random conjugate of x is taken, there is a fixed probability that it will provide a pair of the required sort — namely n/K, where $K = |K_1|$ and n is the number of these pairs (given by the character-theoretic formula). Hence, as the search progresses, one might reasonably expect to find such a pair, say, every s seconds (where s depends on the speed of the machine). On the other hand, as the stored set of representatives gets larger, the probability of finding a new pair — that is, a pair not equivalent to any found already — will decrease.

This is like sampling from a population with replacement, and naturally what is of interest to us is the expected waiting time before the whole population is exhausted (*c.f.* [7; Section IX.3]). If we forget about the partitioning into $C_G(z)$-classes for the moment, the expected number of pairs to be tested before accounting for all of them would be $n({}^1/_n + {}^1/_{n-1} + \dots + {}^1/_2 + 1)$, which is rather large. If however, we make the simplifying assumption that there are, say, m classes, each of the same size, the expected number reduces to $m({}^1/_m + {}^1/_{m-1} + \dots + {}^1/_2 + 1)$, and an estimate of the waiting time is then $m({}^1/_m + {}^1/_{m-1} + \dots + {}^1/_2 + 1)\,s$ seconds. Clearly this may not be the most accurate of estimates, but at least it serves as a useful guide.

ACKNOWLEDGMENT

Computations were performed with the aid of CAYLEY on a SUN Sparc-station, the purchase of which was funded jointly by the New Zealand Lottery Grants Board and the N.Z. University Grants Committee. The author is grateful to these bodies for their support, and also to Alan Lee for the reference to population sampling.

REFERENCES

1. J.J. CANNON, An introduction to the group theory language CAYLEY. In: "Computational Group Theory", ed. M. Atkinson, Academic Press (San Diego/London, 1984), pp. 145–183.

2. M.D.E. CONDER, Some results on quotients of triangle groups, *Bull. Australian Math. Soc.* **30** (1984), 73–90.

3. M.D.E. CONDER, The symmetric genus of alternating and symmetric groups, *J. Combinatorial Theory Ser. B* **39** (1985), 179–186.

4. M.D.E. CONDER & J. McKAY, A necessary condition for transitivity of a finite permutation group, *Bull. London Math. Soc.* **20** (1988), 235–238.

5. M.D.E. CONDER, The symmetric genus of the Mathieu groups, *Bull. London Math. Soc.*, to appear.

6. M.D.E. CONDER, R.A. WILSON & A.J. WOLDAR, The symmetric genus of sporadic groups: announced results, *Proceedings of the Marshall Hall Jr. Memorial Conference (Vermont, 1990)*, to appear.

7. J.H. CONWAY, R.T. CURTIS, S.P. NORTON, R.A. PARKER & R.A. WILSON, "An ATLAS of Finite Groups", Oxford University Press (London/New York), 1985.

8. W. FELLER, *An Introduction to Probability Theory and its Applications*, vol. 1, 3rd ed. (Wiley, 1968).

9. H. GLOVER & D. SJERVE, The genus of $PSL_2(q)$, *J. Reine Angew. Math.* **380** (1987), 59–86.

10. R. REE, A theorem on permutations, *J. Combinatorial Theory Ser. A* **10** (1971), 174–175.

11. T.W. TUCKER, Finite groups acting on surfaces and the genus of a group, *J. Combinatorial Theory Ser. B* **34** (1983), 82–98.

12. A.J. WOLDAR, On the symmetric genus of simple groups, *preprint*.