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

Random Remarks on Permutation Group Algorithms

WILLIAM M. KANTOR

I

Quite a few papers in these Proceedings concern goal–oriented Computational Group Theory, aimed at producing software and leading to important applications. There are also a number of papers concerned with algorithms and their inherent limitations, from a somewhat more theoretical point of view; their goal is new data structures and new mathematical approaches more than the immediate production of software. The present note is partly in the latter direction, but also partly points elsewhere: the production of new, purely mathematical theorems and directions, having algorithmic applications but capable of standing by themselves without any algorithmic components. It is my contention that such theorems can not only be of value within algorithmic contexts, but also within other areas of mathematics.

Let me start with some examples of theorems I have in mind.

- Orders of primitive subgroups G of S_n: $|G| < n^{C \log n}$ *for some constant* C *unless* $n = \binom{m}{k}^{\ell}$ *and* G *is a subgroup of* $S_m \text{wreath} S_\ell$ *containing* $(A_m)^\ell$ *for some* m, k, ℓ, *where* S_m *acts on the* $k-$*sets of an* $m-$*set and the wreathed product has the product action.* This result is due to Cameron [**Cam**], based on work on permutation representations of classical groups [**Ka1**] as well as the classification of finite simple groups. (In [**Li**] it is shown that one can use $C = 9$ here; in fact, $C = 5$ will do.) The theorem, and refinements of it, have been of great importance to some of the work described in other papers in these Proceedings (by Babai–Luks–Seress, Seress–Weisz and Sarawagi–Cooperman–Finkelstein), and would have been discovered due to their need. However, the

1991 *Mathematics Subject Classification.* Primary 20B40, 20P05.
Research supported in part by the NSF and the NSA.
This is the final version of this paper.

results in [**Cam**] and [**Ka1**] arose in the context of very classical questions concerning primitive groups.

- Orders of primitive solvable subgroups G of S_n: $|G| < n^{3.25}$ (Pálfy [**Pá**], Wolf [**Wo**]). While Pálfy was motivated by possible algorithmic applications, Wolf was not. For him this was a natural question in the context of properties of solvable groups he was studying.

- Orders of primitive subgroups G of S_n: *If every noncyclic composition factor of G has order bounded by some constant b, then $|G| = O(n^{c(b)})$ for some constant $c(b)$* (Babai-Cameron-Pálfy [**BCP**]). While this theorem certainly stands by itself, it was motivated by algorithmic applications.

- *The classification of subgroups of $GL(n,q)$ containing an irreducible element subject to suitable additional assumptions.* Results of this type are discussed in the paper by Praeger in these Proceedings. Other results of the same sort were obtained by Hering, initially for applications to projective planes, and later in order to study 2–transitive permutation groups (cf. [**Ka3**] for a discussion of those and more recent theorems). Penttila and Praeger are working on extensions of research that was initiated by Neumann and Praeger for algorithmic purposes; and these extensions will very likely lead to other purely geometric applications as well.

There are other examples. An additional one will be discussed later. For now, the preceding examples should suffice to make the point concerning "stand alone" theorems that have algorithmic implications. The direction of all of the above results is, to some extent, towards Asymptotic Group Theory; compare Pyber's contribution to these Proceedings (and also [**Ka4**]).

II

If $G \leq S_n$, what can be said about a random element of G? What can be said about a random subgroup G of S_n? What can be said about a random transitive subgroup G of S_n?

Answers to questions like these could be of great value to Computational Group Theory. However, it may well be that random subgroups of S_n have an uninteresting structure. Namely, whether "random" refers to averaging over all subgroups of S_n, or only up to conjugacy in S_n, it seems likely that

- Prob($G \leq S_n$ *is nilpotent*) $\to 1$ as $n \to \infty$.

Worse than this, it may even be true that the word "nilpotent" can be replaced here by "abelian". However, it seems as if this is not the correct type of question: it appears to take one outside the realm of those permutation groups studied the most often. A result with a similar flavor was conjectured at the Workshop: *a random subgroup G of S_n has exponential order.* This was proved soon after

the Workshop by Pyber (see his paper in these Proceedings for a more precise statement, as well as for numerous other related results), but it also may not be sufficiently useful in computational contexts. This discussion leads to the

- Metaquestion: *What are the correct questions to ask about the average behavior of permutation groups*?

In particular, this question needs to be addressed by those interested in *using* permutation group algorithms. What are the types of groups to which algorithms are most often applied? They are certainly not just the simple groups. They usually are transitive, or even primitive. However, in the course of recursion many other groups, in particular $p-$groups, may occur. While these do not seem interesting in the context of permutation groups, they appear to be unavoidable and can produce algorithmic difficulties. A significant instance of this is provided by a result of Blaha: the Greedy Algorithm cannot be expected to yield a near–optimal base for a permutation group, for example if that group is the direct product of isomorphic groups, such as cyclic groups of prime order or alternating groups of degree 5 (cf. [**Bl**]). If such "boring" groups could *usually* be avoided then algorithms could be developed in that direction. If such simple–minded groups are inherently unavoidable and occur fairly often — in particular, if a random subgroup of S_n happens to be "boring" — then the average behavior of algorithms might be of less significance than worst–case behavior.

One further remark is needed concerning the notion of "random" subgroups of S_n. A lovely and well–known theorem of Dixon [**Dix**] states that a random pair of elements of S_n generates S_n or A_n with probability $\to 1$ as $n \to \infty$. There are analogous results for most (and probably all) finite simple groups [**KL**]. Therefore, it is not at all clear how one would even go about *choosing* a random subgroup of any such group.

III

A standard question in Computational Group Theory is that of finding an element of order p, where p is a prime dividing the order of G. Such elements are needed, for example, as starting points towards Sylow subgroups. The only provably "efficient" algorithm for finding such an element seems impractical [**Ka2**]. The usual approach is to pick an element of G randomly a few times, and hope that an element of order divisible by p is obtained. Choosing an element at random is quite easy, assuming that a base B is available. For example, if $B = \{1, 2, \ldots, b\}$, if $G_{(i)}$ is the stabilizer of the points $1, 2, \ldots, i$ (so $G_{(0)} = G$ and $G_{(b)} = 1$), and if T_i is a set of coset representatives of $G_{(i+1)}$ in $G_{(i)}$, simply choose a random element $t_i \in T_i$ for each i; then $g = t_{b-1} \cdots t_1 t_0$ is a random element of G.

J. Cannon observed that, when randomly picking an element of the subgroup $\mathrm{PSL}(2, p)$ of S_{p+1}, Cayley often takes a long time to produce an element of order

p. He hoped something could be done to handle this difficulty. First, observe that $\mu_p(\mathrm{PSL}(2,p)) = 2/p = 2/(n-1)$, where for any group G let $\mu_p(G)$ denote the probability that an element of G has order divisible by p (i.e., $\mu_p(G)$ is the proportion of such elements of G). Note that the stabilizer G_1 of a point in $\mathrm{PSL}(2,p)$ is a Frobenius group of order $p \cdot \frac{1}{2}(p-1)$, and $\mu_p(G_1) = 2/p$. However, it is certainly easy to use a commutator or two of any given generators of G_1 in order to obtain an element of order p.

Clearly $\mathrm{PSL}(2,p)$ is a standard type of group occurring in group–theoretic computations. There are many examples of permutation groups exhibiting bad behavior from the present point of view. Some further examples are as follows:

$G = \mathrm{PSL}(2,p) < S_{\binom{p+1}{2}}$, where $\mu_p(G) \sim \sqrt{2/n}$;

$G = \mathrm{PSL}(2,2^e) \leq S_{2^e+1}$, where $\mu_2(G) = 1/(n-1)$;

$G = S_p,\ p = n$, where $\mu_p(G) = 1/p = 1/n$; and

G is sharply 2–transitive and n is a power of p, where $\mu_p(G) = 1/n$.

These should be compared with the following

THEOREM [**IKS**]. *If $G \leq S_n$ and p is a prime dividing $|G|$, then $\mu_p(G) \geq 1/n$. Equality holds only in the last two examples given above.*

Clearly, this is another example of a "stand alone" theorem. From a computational point of view, there are two ways to view this theorem: (i) *the optimistic view*: no more than n random choices should be needed in order to obtain an element of order divisible by p; and (ii) *the pessimistic view*: there can be some situations where random selection will work too poorly to be of value. As noted above, there are many other "bad" situations for the random method — perhaps not as bad as in the theorem, but bad enough. Of course, there are other ways of dealing with some of them — the case $G = S_p,\ p = n$ being especially easy (just add a subroutine to write a cycle). However, all of this points towards a need to develop algorithms that will try random selection, but will then do something else if not successful after a few tries.

It should be possible to go somewhat further than the Theorem. There is no doubt that all permutation groups of degree n such that $\mu_p(G) \leq 2/n$ can be classified. It may be possible to give a reasonable description of those groups G for which $\mu_p(G) \leq c/n$ for some constant c. For purposes of applications it would be ideal to be able to show that $\mu_p(G) \leq 1/\log n$ for "most" groups, whatever that means; but this seems extremely difficult to state, much less prove.

Nevertheless, it would be interesting to know from a user's point of view what types of theorems in this direction might be desirable.

The proof of the above theorem uses the classification of finite simple groups. First there is a reduction to the primitive case, then to the (almost) simple case, and finally to simple groups of Lie type in characteristic $\neq p$. These reductions

are relatively straightforward, and not especially enlightening. The remainder of the proof is more interesting, leading to the following

THEOREM [**IKS**]. *If G is a simple group of Lie type of characteristic $\neq p$, then $\mu_p(G) \geq 1/p^2$ — independent of the group G — and also $\mu_p(G) \geq (1-1/p)/2h$.*

(Here, h is the Coxeter number of the corresponding group over an algebraically closed field; for example, $h = n$ when $G = \mathrm{PSL}(n, q)$.) This requires a counting argument involving groups of Lie type, fairly general considerations using partitions in the case of classical groups, and a case by case calculation with Weyl groups and cyclotomic polynomials for the exceptional groups of Lie type. (Cyclotomic polynomials arise as follows: p divides the order of G, which is essentially a product of cyclotomic polynomials evaluated at a prime power q. The proof then considers which of these polynomials a given prime p might divide.)

The following amusing result is easily deduced from the preceding theorem:

COROLLARY [**IKS**]. *If G is any group having a simple homomorphic image that is neither cyclic nor Lie type of characteristic 2, then $\mu_2(G) \geq 1/4$.*

Thus, for such a group G it is "easy" to find involutions.

All of this leaves open a much more important question: is there any way to choose random subgroups in order to obtain nice ones — such as Sylow subgroups? Once again, [**Dix**] as well as related results [**KL**] present obstacles to the most obvious notions of randomness.

REFERENCES

[BCP] L. Babai, P. J. Cameron and P. Pálfy, *On the order of primitive groups with restricted nonabelian composition factors*, J. Algebra **79** (1982), 161–168.

[Bl] K. D. Blaha, *Minimum bases for permutation groups: The greedy approximation*, J. Algorithms **13** (1992), 297–306.

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

[Dix] J. D. Dixon, *The probability of generating the symmetric group*, Math. Z. **110** (1969), 199–205.

[IKS] I. M. Isaacs, W. M. Kantor, and N. Spaltenstein, *On the probability that a group element is $p-$singular* (to appear in J. Algebra).

[Ka1] W. M. Kantor, *Permutation representations of the finite classical groups of small degree or rank*, J. Algebra **60** (1979), 158–168.

[Ka2] ———, *Polynomial–time algorithms for finding elements of prime order and Sylow subgroups*, J. Algorithms **6** (1985), 478–514.

[Ka3] ———, *$2-$Transitive and flag–transitive designs* (to appear in Proc. Marshall Hall Conf. 1990).

[Ka4] ———, *Some topics in asymptotic group theory*, Groups, Combinatorics and Geometry (eds. M. W. Liebeck and J. Saxl), LMS Lecture Notes 165, 1992, pp. 403–421.

[KL] W. M. Kantor and A. Lubotzky, *The probability of generating a finite classical group*, Geom. Ded. **36** (1990), 67–87.

[Li] M. W. Liebeck, *On the minimal degrees and base sizes of primitive groups*, Arch. Math. **43** (1984), 11–15.

[Pá] P. P. Pálfy, *A polynomial bound for the orders of primitive solvable groups*, J. Algebra **77** (1982), 127–137.

[Wo] T. R. Wolf, *Solvable and nilpotent subgroups of* $GL(n, q^m)$, Can. J. Math. **34** (1982), 1097–1111.

Department of Mathematics, University of Oregon, Eugene, OR 97403

E-mail address: kantor@bright.uoregon.edu