Contemporary Mathematics

Enumerating subgroups of the symmetric group

Derek F. Holt

Abstract. We announce our successful computation of a list of representatives of the conjugacy classes of subgroups of S_n for $n \leq 18$, including the 7 274 651 classes of subgroups of S_{18}.

1. Introduction

Early attempts to enumerate complete lists of primitive subgroups and transitive subgroups of the symmetric group S_n for low values of n, up to conjugacy in S_n, began with Ruffini in 1799 and continued until about 1912. We refer the reader to [11] for details and references.

There was little further work on this problem until about 1970 when, with the assistance of computers, Sims [12] compiled a list of primitive permutation groups of degree up to 20. More recently, primitive permutation groups of degree up to 4095 have been enumerated [4, 10] as have transitive group of degree up to 32 [6, 7]. The lists of groups (currently with primitive groups up to degree 2499 and transitive groups up to degree 31) are available as libraries in GAP [5] and Magma [1]. With libraries of this kind containing large numbers of groups, it would be desirable to have some kind of compact storage method that allowed easy reconstruction, but for small-degree permutation groups one cannot do much better than store minimal sized generating sets for each group.

The problem of listing representatives of all conjugacy classes of subgroups of S_n has received relatively little attention. Lists for $n \leq 12$ and also of the subgroups of A_n for $n \leq 13$ are available from the website of Götz Pfeiffer [9], although the subgroups of S_{13} can now be computed routinely in Magma in a few hours simply by calling the function `Subgroups(Sym(13))`.

The purpose of this note is to announce the author's enumeration of representatives of the conjugacy classes of S_n for $n \leq 18$. The computations were carried out in Magma on a 2.40GHz Intel PC with 4GB of memory. These lists are currently available from the author on request, although it is to be hoped that they will eventually be accessible from GAP and Magma.

In the table below, we list the numbers of conjugacy classes of primitive, transitive, and all subgroups of S_n in the first three columns. Note that the number of classes of subgroups of S_n that act fixed-point-freely can be obtained by subtracting

1991 *Mathematics Subject Classification.* Primary 20B35; Secondary 20B40.

Degree	Primitive	Transitive	All (classes)	All (total)
1	1	1	1	1
2	1	1	2	2
3	2	2	4	6
4	2	5	11	30
5	5	5	19	156
6	4	16	56	1455
7	7	7	96	11 300
8	7	50	296	151 221
9	11	34	554	1 694 723
10	9	45	1593	29 594 446
11	8	8	3094	404 126 228
12	6	301	10 723	10 594 925 360
13	9	9	20 832	175 238 308 453
14	4	63	75 154	5 651 774 693 595
15	6	104	159 129	117 053 117 995 400
16	22	1954	686 165	5 320 744 503 742 316
17	10	10	1 466 358	125 889 331 236 297 288
18	4	983	7 274 651	7 598 016 157 515 302 757
19	8	8		
20	4	1117		
21	9	164		
22	4	59		
23	7	7		
24	5	25 000		
25	28	211		
26	7	96		
27	15	2392		
28	14	1854		
29	8	8		
30	4	5712		
31	12	12		
32	7	2 801 324		

the number for S_{n-1} from that of S_n. The final column contains the total number of subgroups of S_n.

It might be possible with a considerable amount of effort and large-scale use of computer power to extend the enumeration to degree 19 or perhaps even to degree 20 in the foreseeable future, but it is doubtful to what extent this would be worthwhile given the very large number of groups that are likely to be involved, and it seems highly unlikely that it could be extended much further than this.

In the following section we describe briefly the methods used to enumerate the subgroups of S_n, and then in the final section we discuss an application that motivated the author to undertake these computations.

2. Methods used

The problem of listing representatives of the conjugacy classes of subgroups of S_n subdivides naturally into a large number of subproblems, each of which can

be dealt with independently, so the main problem is highly parallelizable. Since we can assume that the subgroups of S_m are already known for $m < n$, and subgroups of S_n that fix $n-m$ points are conjugate in S_n if and only if they are conjugate in S_m, we can restrict our attention to the fix-point-free subgroups H. The lengths of the orbits of H defines a partition of n in which no component is 1, so we can handle the different partitions individually. The transitive subgroups are already known and available in MAGMA for $n \leq 18$, so we need consider only nontrivial partitions.

Furthermore, for each such partition $n = n_1 + n_2 + \cdots + n_k$ with $k > 1$ and $1 < n_1 \leq n_2 \leq \cdots \leq n_k$, the induced action of H on the i-th orbit is a transitive subgroup of S_{n_i}. So each choice of transitive subgroups H_i of S_{n_i} gives rise to the subproblem of enumerating those H for which the induced action on the i-th orbit is H_i. Of course, if some of the n_i are equal – say $n_j = n_{j+1} = \cdots = n_k$ then, since we are enumerating subgroups up to conjugacy in S_n, we only consider one of the possible orderings of each choice of subgroups H_i for $j \leq i \leq k$.

So we have to solve the following type of subproblem. Given a partition of n, $n = n_1 + n_2 + \cdots + n_k$, and transitive subgroups H_i of S_{n_i} as above, let P be the direct product of the H_i. Then we must find the conjugacy classes in S_n of subdirect products of P; that is, the subgroups of P that project onto each of the factors H_i. The conjugacy test for subgroups can be carried out in an appropriate wreath product of symmetric groups. More precisely, if $H_1 = H_2 = \cdots = H_{i_1}$, $H_{i_1+1} = H_{i_1+2} = \cdots = H_{i_2}$, $\ldots$, $H_{i_{l-1}+1} = \cdots = H_{i_l}$ with no other equalities between the H_i, then the conjugacy test takes place in the direct product of the permutation wreath products $S_{n_{i_j}} \wr S_{m_j}$ for $1 \leq j \leq l$, where $m_j = i_{j+1} - i_j$.

The author tried two methods of finding the subdirect products of P. The more straightforward was to compute maximal subgroups repeatedly using the algorithm described in [3], where we keep only those subgroups that project onto each H_i, and at each stage we remove any subgroups that are conjugate to one that is already on the list. For the second method, we employ the algorithm presented in [2] for finding all subgroups of a permutation group. This involves the initial computation of a series of normal subgroups $1 < P_1 < P_2 < \cdots < P_k < P$ of P in which P_k is the solvable radical of P, and each factor group P_j/P_{j-1} is elementary abelian. We then find the subgroups of P/P_k, $P/P_{k-1}, \ldots, P/P_1$, P successively, where at each stage we remove those subgroups that do not project onto each H_iP_{j-1}/P_{j-1}.

Testing subgroups for conjugacy can be inherently slow in large permutation groups, since all currently known methods involve the use of backtrack searches with potentially exponential complexity. The advantage of the second method is that the lifting process of finding the subgroups of P/P_{j-1} from those of P/P_j involves no explicit conjugacy testing of subgroups. This is replaced by an equivalent orbital computation on the vectors of a vector space over a prime field, which is still theoretically of exponential complexity, but is much faster in practice. So we generally used the first method described above to find the subgroups of the top layer P/P_k and then used the second method for the lifting process.

These techniques proved adequate for finding the subgroups of S_n for $n \leq 17$. The process times in seconds for $n = 13$, 14, 15, 16, and 17 were respectively 105, 653, 1190, 20 234, and 26 640.

Unfortunately, they failed to cope with a few of the partitions of 18 within the memory constraint of 4GB RAM. The problem arose from the direct products P having elementary abelian quotients of order 2^9, which gave rise to inordinately

large numbers of subgroups during the lifting process. The difficult cases all involved partitions with $n_1 = 2$, and we devised more specialized techniques for dealing with those.

Consider, for example, the partition $3 \times 2 + 3 \times 4$ of 18. Other partitions were handled in similar fashion, with minor variations. Rather than start with a direct product of six transitive groups, we start with $P = H_1 \times H_2$, where $H_1 \leq S_6$ and $H_2 \leq S_{12}$ are groups from the lists that we have already computed in degrees 6 and 12, and whose orbits lengths form the partitions $2 + 2 + 2$ and $4 + 4 + 4$ respectively. Since H_1 is elementary abelian, a subdirect product of H_1 and H_2 has the form $\{(h_1, h_2) \mid \phi_1(h_1) = \phi_2(h_2)\}$, where ϕ_1, ϕ_2 are epimorphisms of H_1 and H_2 onto an elementary abelian 2-group of order at most 2^3.

We proceed as follows. Before considering the different possible groups H_1 and H_2, for each e with $0 \leq e \leq 3$, let E be elementary abelian of order 2^e and pre-compute a complete list of subdirect products D of $E \times E$ with $|D| = 2^e$. Then consider each pair H_1, H_2 in turn, and let N_i be the normalizer of H_i in the symmetric group for $i = 1, 2$. Now, for each e with $0 \leq e \leq 3$ and $i = 1, 2$, we find representatives, up to conjugation in N_i, of the normal subgroups K_i of H_i in which H_i/K_i is elementary abelian of order 2^e. For each of our subgroups D in the precomputed list described above, we can now define a subdirect product H of $H_1 \times H_2$ that contains $K_1 \times K_2$ as a subgroup of index 2^e with $H/(K_1 \times K_2) = D$. For fixed K_1 and K_2, we test the resulting list of groups (one for each subgroup D) for conjugacy under the action of $N_{N_1}(K_1) \times N_{N_2}(K_2)$. It is not hard to show that this results in the required list of groups for this partition.

The complete calculation of the 5 808 293 fixed-point-free subgroups of S_{18} using these techniques took approximately four cpu-days.

3. An application

The *support* $s(g)$ of a permutation g is the set of points moved by g. The *minimal degree* $m(G)$ of a permutation group $G \leq S_n$ is defined by:

$$m(G) = \min\{|s(g)| \mid 1 \neq g \in G\}.$$

So, for example, $m(S_n) = 2$ for $n \geq 2$, $m(A_n) = 3$ for $n \geq 3$, and if all elements of G act fixed-point-freely then $m(G) = n$.

Large groups with large minimal degrees are interesting and give rise to potential applications to quantum computing and coding theory. There are, however, a number of results saying that very large groups G (i.e. those whose order is exponential in the degree n) must have small minimal degrees. A recent result of this type, proved in [8], is that if $m \leq \log_2 n$ then $|G| \leq n^{10n/m}$, whereas if $m \geq \log_2 n$ then $|G| \leq 2^{10n}$.

To answer the more specific question, given n and $m \leq n$, what is the largest subgroup G of S_n with $m(G) \geq m$, there appears to be no approach other than to carry out an exhaustive search of all possible G. So the lists described in this paper now enable us to answer this question for $n \leq 18$. We list some examples in which the largest such G is unusually large in the table below. Note that the example $L_2(8){:}3 \times L_2(7){:}2 \leq S_{17}$ is intransitive on its support, which demonstrates that it is not sufficient to restrict our attention to transitive groups.

n	m	Group	Order
8	4	$2^3{:}L_3(2)$	1344
9	6	$L_2(8){:}3$	1512
11	8	M_{11}	7920
12	8	M_{12}	95040
16	12	$2^4{:}A_7$	40320
17	6	$L_2(8){:}3 \times L_2(7){:}2$	508032

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust, *The* Magma *algebra system I: The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[2] J.J. Cannon, B.C. Cox, and D.F. Holt, *Computing the subgroups of a permutation group*, J. Symbolic Comput. **31** (2001), 149–161.

[3] J.J. Cannon and D.F. Holt, *Computing maximal subgroups of finite groups*, J. Symbolic Comput. **37** (2004), 589–609.

[4] H.J. Coutts, M. Quick, and C.M. Roney-Dougal, *The primitive permutation groups of degree less than* 4096. Submitted.

[5] The GAP Group, GAP – *Groups, Algorithms, and Programming, Version 4.4.12* (2008), available at `http://www.gap-system.org`.

[6] J.J. Cannon and D.F. Holt, *The transitive groups of degree 32*, Experimental Mathematics **17** (2008), 307–314.

[7] A. Hulpke, *Constructing transitive permutation groups*, J. Symbolic Comput. **39** (2005), 1–30.

[8] J. Kempe, L. Pyber, and A. Shalev, *Permutation groups, minimal degrees and quantum computing*, Groups, Geometry, and Dynamics **1** (2007), 553–584.

[9] G. Pfeiffer, available at `http://schmidt.nuigalway.ie/subgroups/`.

[10] C.M. Roney-Dougal, *The primitive groups of degree less than* 2500, J. Algebra **292** (2005), 154–183.

[11] M.W. Short, *The Primitive Soluble Permutation Groups of Degree Less than* 256, Lecture Notes in Mathematics, vol. 1519, Springer-Verlag, 1992.

[12] Charles C. Sims, *Computational methods in the study of permutation groups*, Computational problems in abstract algebra (J. Leech, ed.), Pergamon Press, Oxford, 1970, pp. 169–183.

Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK
E-mail address: `D.F.Holt@warwick.ac.uk`