

Permutation groups generated by short elements

Peter J. Cameron

draft, 24/10/2005

This document was provoked by a question on the SEQFAN mailing list, which was passed on to me by Simone Severini.

We consider the following four questions. How many subgroups of the symmetric group S_n are generated by

- transpositions;
- 3-cycles;
- transpositions and 3-cycles,
- products of pairs of transpositions?

For each of the four questions there are three ways of counting the subgroups:

- the total number;
- the number up to conjugacy in S_n ;
- the number up to isomorphism.

We solve these problems completely for the first three types of generation (noting incidentally that the numbers of isomorphism and conjugacy classes are the same). The fourth is rather more complicated, and all three counts give different values; but the numbers can in principle be calculated from the analysis given here.

Transpositions

Let T be a set of transpositions generating a subgroup G of S_n . Without loss of generality, T consists of all transpositions in G . Clearly, if $(ab) \in T$ and $(ac) \in T$, then $(bc) \in T$. Hence the relation \sim defined by

$$a \sim b \Leftrightarrow a = b \text{ or } (ab) \in T$$

is an equivalence relation, whose equivalence classes are the orbits of G . (Clearly each equivalence class is a subset of an orbit. But if two points lie in the same orbit, they are connected by a chain of transpositions, and hence are interchanged by a transposition.) Moreover, on each orbit, we have all possible transpositions, and these generate the symmetric group on the orbit.

Hence G is the direct product of symmetric groups, acting in the obvious way.

We see that the number of subgroups G is equal to the number of partitions of $\{1, \dots, n\}$, that is the *Bell number* $B(n)$ (OEIS A000110), and the number up to conjugacy is the number $p(n)$ of partitions of n (OEIS A000041).

The number of subgroups up to isomorphism is also equal to the partition number. For it is not too hard to show that, if a group is a direct product of symmetric groups, then the number of factors and their degrees can be recovered from the isomorphism type of the group. For if G, G', G'', \dots denotes the derived series of G , then

- $|G/G'| = 2^x$, where x is the number of non-trivial symmetric factors;
- $|G'/G''| = 3^y$, where y is the number of factors S_3 or S_4 ;
- $|G''/G'''| = 4^z$, where z is the number of factors S_4 ;
- G''' is the direct product of (simple) alternating groups each of degree at least 5.

3-cycles

Things are very similar for 3-cycles. Again, if G is generated by a set T of 3-cycles, we may assume that T consists of all the 3-cycles in G . Now, a short calculation shows that, if two 3-cycles have intersecting support, then they generate the alternating group of degree at most 5, and so T contains all 3-cycles on the union of the supports. So the relation \sim defined by

$$a \sim b \Leftrightarrow a = b \text{ or } (\exists c)(abc) \in T$$

is an equivalence relation, whose equivalence classes are the orbits, and that T consists of all 3-cycles with support contained in an equivalence class. The 3-cycles generate the alternating group as long as the degree is not 2. So no class can have size 2.

Hence the number of subgroups is equal to the number of partitions of $\{1, \dots, n\}$ with no part of size 2, and the number up to conjugacy is the number of partitions of n with no part of size 2. These are OEIS A097514 and A027336.

The number of subgroups up to isomorphism is equal to the number up to conjugacy, for similar reasons to what happens for transpositions.

Transpositions and 3-cycles

In this case, much as above, G is a product of symmetric and alternating groups. The number of conjugacy classes of such groups is equal to the number of partitions of n , where there are two types of parts of each size greater than 2; this is OEIS A003292. The number up to isomorphism is the same. The number of subgroups is the number of partitions of the set $\{1, \dots, n\}$ with two types of parts of each size greater than 2; this is currently not in the OEIS.

Products of pairs of transpositions

These elements are 3-cycles and double transpositions. Life is more complicated in this case.

Let G be generated by a set T of 3-cycles and double transpositions. As usual, we can assume that T consists of all the 3-cycles and double transpositions in G . Let N be the subgroup of G generated by the 3-cycles in T . Then N is a normal subgroup of G , and is a product of alternating groups. No non-trivial N -orbit can be moved by a double transposition; for any such orbit has size at least 3, and a permutation moving it would move at least 6 points. So the non-trivial N -orbits are also G -orbits, and the group induced on such an orbit is the alternating or symmetric group.

We see also that if a G -orbit is fixed pointwise by N , then the group induced on this orbit is generated by transpositions and double transpositions.

There are four types of double transpositions in T :

- those with support contained in an N -orbit;

- those for which the two transpositions are contained in different N -orbits;
- those for which one transposition is contained in an N -orbit and the other consists of fixed points of N ;
- those whose support consists of fixed points of N .

We can ignore the first type, since they are already contained in N . To handle the third and fourth types, we use the following result.

Lemma Let G be a transitive group generated by transpositions and double transpositions. Then one of the following holds:

- G is the symmetric or alternating group;
- G is the Weyl group of type B_n or D_n , and is imprimitive with n blocks of size 2;
- G is one of the following: Dih_{10} (degree 5), $PSL(2,5)$ (degree 6), $GL(3,2)$ (degree 7), or $AGL(3,2)$ (degree 8).

For suppose first that G is imprimitive. The block size must be 2, since otherwise some generator would move at least 6 points. The group permuting the blocks is generated by transpositions, and so is the symmetric group. Now it is easy to see that there are only two possibilities for G , depending on whether the normal subgroup fixing the blocks consists of all such permutations, or just the even ones.

On the other hand, if G is primitive, then classical results of permutation group theory together with lists of primitive groups of small degree show that either (i) or (iii) must hold. (Note that none of the groups in (iii) contain transpositions, since a primitive group containing a transposition must be the symmetric group.)

The final observation is the following. Let \mathcal{O} be the set of G -orbits, and let \mathcal{O}' be the subset of \mathcal{O} consisting of orbits on which the induced group contains an odd permutation. For each such orbit, there must be a double transposition with one cycle contained in the orbit. So define a relation \sim on \mathcal{O}' by the rule that $O_1 \sim O_2$ if there is a double transposition with one orbit in O_1 and one in O_2 . We claim that \sim is an equivalence relation. To see this, we must note that each possible transitive constituent of G has the property that it acts transitively by conjugation on the transpositions it contains (if any). (This holds because the only ones which contain transpositions are the symmetric groups, which contain

all transpositions, and the Weyl groups of type B_n , where the transpositions are all those whose support is a block of imprimitivity.) So if $O_1 \sim O_2 \sim O_3$, then we can assume that G contains double transpositions $(x_1 y_1)(x_2 y_2)$ and $(x_2 y_2)(x_3 y_3)$, where $x_i, y_i \in O_i$; then G contains $(x_1 y_1)(x_3 y_3)$, and so $O_1 \sim O_3$. Thus \mathcal{O}' is partitioned into equivalence classes.

The set \mathcal{O}' consists of orbits for which the induced transitive constituent is one of S_n or the Weyl group of type B_n . Note that the even permutations in such a group form a transitive subgroup except in the case of S_2 .

Now we can describe all groups generated by products of pairs of transpositions as follows. The ingredients in the construction are

- A group H , which is the direct product of alternating groups, Weyl groups of type D_n , and groups of type (iii) in the Lemma;
- A partition of a set M of size m (say) consisting of the index set of some of the alternating and Weyl factors of H and k (say) additional elements.

Each direct factor H_i in H of alternating or D_n type is a subgroup of index 2 in a larger group G_i (of symmetric or B_n type) generated by the direct factor together with a transposition. Now, let k be the excess of m over the number of alternating and D_n factors. Our group will have k orbits of size 2. For each such orbit, we take H_0 to be the trivial group and G_0 to be the symmetric group of degree 2. Now, for each pair $\{i, j\}$ of elements in M lying in the same part of the partition, take all double transpositions consisting of a transposition in $G_i \setminus H_i$ and a transposition in $G_j \setminus H_j$. Now our group G is generated by H together with these double transpositions.

This description can be recovered from the conjugacy class of G in the symmetric group. However, it cannot be recovered from the isomorphism type of G . For example, $G = \text{PSL}(2, 5)$ is isomorphic to A_5 , and has two non-conjugate actions on a set of size 6 generated by double transpositions: the “natural” action as $\text{PSL}(2, 5)$, and the action as A_5 fixing a point.

At least the number of such groups up to conjugacy can now be counted in principle. We take a partition of n , where we distinguish three types of parts of size 6 and 8 and two of each other even size except 2, and two types of parts of size 5 and 7. Now we take a subset of the parts excluding the third types of size 6 and 8 and the second types of size 5 and 7 but including all parts of size 2, and we partition this set. We identify two partitions if one can be obtained from the other by a type-preserving permutation of the parts.