GENERATING SYMMETRIC AND ALTERNATING GROUPS WITH ELEMENTS OF FIXED ORDER

JUSTIN LANIER

Many of the commonly-used generating sets for the symmetric group \( \Sigma_n \) and the alternating group \( A_n \) either consist of a number of generators that grows as \( n \) grows or else contain an element whose order grows as \( n \) grows. For instance, \( \Sigma_n \) is generated by the set of adjacent transpositions, and it is also generated by a single transposition along with an \( n \)-cycle. Similarly, \( A_n \) is generated by all 3-cycles, and it is also generated by a single 3-cycle and a longest cycle of odd length.

We show that \( \Sigma_n \) and \( A_n \) can be generated by a uniformly small number of elements of fixed order \( k \). Note that since all permutations of odd order are even permutations, elements of odd order \( k \) cannot generate \( \Sigma_n \). For the case \( k = 2 \), two elements of order 2 cannot generate \( \Sigma_n \) or \( A_n \) except for small values of \( n \), since any group generated by two involutions is a quotient of a dihedral group. Therefore the result by Nuzhin [6] that three elements of order 2 generate \( A_n \) for \( n = 5 \) and \( n \geq 9 \) is the best possible in general.

We take up the cases where \( k \geq 3 \).

**Proposition 1.** Let \( k \geq 3 \) and \( n \geq k \). Then three elements of order \( k \) suffice to generate \( \Sigma_n \) when \( k \) is even and to generate \( A_n \) when \( k \) is odd.

**Proposition 2.** Let \( k \geq 3 \) and \( n \geq k+2 \). Then four elements of order \( k \) suffice to generate \( A_n \) when \( k \) is even.

The bound in Proposition 2 is \( n \geq k+2 \), and this is different from the bound in Proposition 1. In the case when \( k \) is even and \( k = n - 1 \), \( A_n \) is not always generated by elements of order \( k \). For instance, if \( k = n - 1 \) is a power of 2, then the only elements of order \( k \) are the \( k \)-cycles, but these are odd permutations and so cannot generate \( A_n \).

It is possible that two elements of order \( k \) may in fact suffice for \( k \geq 3 \). In this direction, Miller [5] shows that if \( 2 \leq k \leq n \leq 2k - 1 \), two \( k \)-cycles suffice to generate \( \Sigma_n \) when \( k \) is even or \( A_n \) when \( k \) is odd. At the end of the paper, we give a construction for a pair of elements of order \( k \) that have generated \( \Sigma_n \) for \( k \) even and \( A_n \) for \( k \) odd for all values \((k, n)\) that we have tested by computer calculation, excepting a few small values that can be handled separately.

It would be interesting to determine the likelihood of generating \( \Sigma_n \) or \( A_n \) with two (or more) random elements of order \( k \), just as Dixon [2] determined for two random elements without order constraints. One could also ask about the more restrictive case where the random elements are products of the maximum number of disjoint \( k \)-cycles. Showing that either \( \Sigma_n \) or \( A_n \) is generated with positive probability could also be used as an approach to showing the existence of a generating set of two elements of order \( k \).
Prior results. There are of course many results about generating sets for $\Sigma_n$ and $A_n$. We provide here a few examples about generating sets consisting of a universally bounded number of elements of small or fixed order. Miller [4] showed that except for a few cases when $n \leq 8$, every $\Sigma_n$ and $A_n$ is generated by two elements, one of order 2 and one of order 3. Later, Miller [5] showed that whenever $A_n$ contains an element of order $k > 3$, the group may be generated by two elements, one of order 2 and one of order $k$. He also showed that the same holds for $\Sigma_n$, except for the case when $k = 4$ and $n = 6$ and in the cases when $k > 3$ is an odd prime and $n = 2k - 1$. As mentioned above, Nuzhin [6] showed that $A_n$ is generated by three involutions (where two commute) if and only if $n \geq 9$ or $n = 5$. This implies that there is a universal upper bound on the number of involutions needed to generate $A_n$ whenever they generate $A_n$ at all. Annin and Maglione [1] determined that $\max\{2, \lceil(n-1)/(k-1)\rceil\}$ is the smallest number of $k$-cycles needed to generate $\Sigma_n$ when $k$ is even and to generate $A_n$ when $k$ is odd.

Preliminaries. We take $N = \{0, \ldots, n-1\}$ as our underlying permuted set. Denote by $h_{k,n}(a)$ a step $k$-cycle, which is a $k$-cycle of the form $(a, a+1, \ldots, a+k-1)$ with entries taken mod $n$. We further define $s_{k,n}(a,\ell)$ to be a sequential step product so that

$$s_{k,n}(a,\ell) = \prod_{i=1}^{\ell} h_{k,n}(a + (i-1) \cdot k)$$

with entries taken mod $n$. By way of example, we have

$$s_{4,15}(6,3) = (6 7 8 9)(10 11 12 13)(14 0 1 2).$$

Note that in order to obtain a product of disjoint cycles, the largest value that $\ell$ may take is $\lfloor n/k \rfloor$.

The main result about permutation groups that we use in our proof is Jordan’s theorem. Recall that a permutation group $G$ is transitive if it acts transitively on the underlying permuted set, and it is 2-transitive if it acts transitively on ordered pairs of distinct elements of the underlying permuted set. A permutation group $G$ is primitive if it is transitive and if no nontrivial partition of the underlying permuted set is preserved by the action of $G$.

**Theorem** (Jordan). Let $G$ be a primitive subgroup of $\Sigma_n$, and suppose $G$ contains a $p$-cycle where $p$ is prime and $p \leq n - 3$. Then $G$ is either $A_n$ or $\Sigma_n$.

For additional background on primitivity and Jordan’s theorem, see for instance the book of Isaacs [3, Chapter 8B].

**Proof of Proposition 1.** Miller [5] showed that for $n \leq 2k - 1$, two $k$-cycles generate $\Sigma_n$ when $k$ is even and $A_n$ when $k$ is odd. Thus we may assume that $n \geq 2k$. Consider the
permutation group $G$ on the set $N$ generated by the following elements:

\[ a = s_{k,n}(0, \lfloor n/k \rfloor) \]
\[ b = \begin{cases} 
  s_{k,n}(k-1, \lfloor n/k \rfloor), & \text{if } k \nmid n \\
  s_{k,n}(k-1, \lfloor n/k \rfloor - 1), & \text{if } k \mid n 
\end{cases} \]
\[ c = \begin{cases} 
  (0 \ 1 \ 2), & \text{if } k = 3 \\
  (0 \ 1 \ 2) \ h_{k,n}(0) = (1 \ 0 \ 2 \ \cdots \ k - 1), & \text{if } k > 3 
\end{cases} \]

All three elements consist of disjoint $k$-cycles and so have order $k$. As an illustration, here are the three elements in the case $k = 5, n = 18$.

\[ a = (0 \ 1 \ 2 \ 3 \ 4)(5 \ 6 \ 7 \ 8 \ 9)(10 \ 11 \ 12 \ 13 \ 14) \]
\[ b = (4 \ 5 \ 6 \ 7 \ 8)(9 \ 10 \ 11 \ 12 \ 13)(14 \ 15 \ 16 \ 17 \ 0) \]
\[ c = (1 \ 0 \ 2 \ 3 \ 4) \]

To apply Jordan’s theorem, we must show that $G$ contains a small prime cycle and that $G$ is primitive. Since $n \geq 2k \geq 6$, a $3$-cycle will satisfy the small prime cycle requirement in Jordan’s theorem. If $k = 3$, then $c$ is a $3$-cycle. If $k > 3$, the commutator $[a, c]$ is the $3$-cycle $(0 \ 1 \ k - 2)$.

It remains to show that $G$ is primitive, and it suffices to prove the stronger condition that $G$ is $2$-transitive. We thus aim to show that for an arbitrary ordered pair $(i, j) \in N^2$, $i \neq j$, there exists $g \in G$ such that $g(i, j) = (k-2, k-1)$. $G$ is certainly transitive, since the overlapping cycles of $a$ and $b$ allow any element in $N$ to be carried to any other. Let $g_1$ be a product in $a$ and $b$ such that $g_1(i) = k-2$. We now seek a $g_2$ that carries $j$ to $k-1$ while keeping $i$ at $k-2$. We reduce to the case where $g_1(j)$ sits outside of $S = \{0, \ldots, k-1\}$. If $g_1(j)$ sits in $S$, then we may first move $g_1(j)$ outside of $S$ while keeping $i$ at $k-2$. Either $b$ acts on $g_1(j)$ while keeping $i$ at $k-2$—and so can move $g_1(j)$ out of $S$—or else $c^m b c^{-m}$ does so for some power of $c$. Therefore $i$ sits at $k-2$ and $g_1(j)$ sits outside of $S$. Note that $b$ and the product $c^{-1} a$ each fix $k-2$. Since $b$ and $c^{-1} a$ act transitively on $N - \{0, \ldots, k-2\}$, we may form a product $g_2$ in $b$ and $c^{-1} a$ so that $g_2 g_1(i, j) = (k-2, k-1)$. Thus $G$ is $2$-transitive, and so it is primitive.

Applying Jordan’s theorem, we have that $G$ is either $A_n$ or $\Sigma_n$. If $k$ is even, then $G$ contains the odd permutation $c$, and therefore $G \cong \Sigma_n$. If $k$ is odd, then all of the generators are even permutations, and so $G \cong A_n$. 

\[ \square \]

**Proof of Proposition 2.** Take $k$ to be even and $n \geq k + 2$. To show that $A_n$ is generated by four elements of order $k$, we will modify the generating set for $\Sigma_{n-2}$ comprised of three elements of order $k$ from the proof of Proposition 1 or the two $k$-cycles given by Miller. First, add elements $\{a, b\}$ to the underlying set of permuted objects $\{0, \ldots, n-3\}$. For each odd permutation in the generating set for $\Sigma_{n-2}$, multiply it by the transposition $(a \ b)$ so that it becomes an even permutation. For each even permutation of the generating set for $\Sigma_{n-2}$, let it fix $a$ and $b$ so that it remains an even permutation. Finally, add to the generating set the element $t = (a \ b \ 3 \ 4 \ \cdots \ k)(1 \ 2)$. This is an even permutation of order $k$. These elements together generate $A_n$, since every generator is an even permutation.
and every 3-cycle on \( \{0, \ldots, n-3, a, b\} \) is generated by them. To see this last fact, observe that the 3-cycles on \( \{0, \ldots, n-3\} \) are generated by the modified elements and also that any 3-cycle involving \( a \) or \( b \) is a conjugation of one of these 3-cycles by a power of \( t \). Therefore we have a generating set for \( A_n \) comprised of at most four elements of even order \( k \).

\[ \square \]

We would be glad to see the following conjecture resolved.

**Conjecture.** Let \( k \geq 3 \) and \( n \geq k \). Then two elements of order \( k \) suffice to generate \( \Sigma_n \) when \( k \) is even and to generate \( A_n \) when \( k \) is odd.

We give here a candidate construction for resolving this conjecture. Consider the following two permutations on \( N \) of order \( k \).

\[
\begin{align*}
a &= s_{k,n}(0, \lfloor n/k \rfloor), \\
b &= \begin{cases} 
(k - 1 \, k + 1)s_{k,n}(k - 1, \lfloor n/k \rfloor), & \text{if } k \text{ is odd, or } k \text{ is even and } \lfloor n/k \rfloor \text{ is odd} \\
\frac{k}{4}, & \text{if } k \text{ is even, } \lceil n/k \rceil \text{ is even, and } n \neq k - 1 \mod k \\
d, & \text{if } k \text{ is even, } \lfloor n/k \rfloor \text{ is even, and } n = k - 1 \mod k
\end{cases}
\end{align*}
\]

where \( d = s_{2,n}(k(|n/k| - 1) - 1, 2)s_{k,n}(1, |n/k| - 2)h_{k,n}(k|n/k| - 1) \). Our computer calculations have verified that \( a \) and \( b \) generate \( \Sigma_n \) when \( k \) is even and \( A_n \) when \( k \) is odd for all pairs \((k, n)\) where \( n \geq k \geq 3 \), \( n \leq 200 \) and \( k \leq 30 \), except for the three cases \((3, 6)\), \((3, 7)\), and \((3, 8)\). These exceptional cases can be handled by a different construction. We have also checked the construction for 1000 additional random pairs of values where \( k \leq n \leq 1000 \). We have not, however, found a proof that \( a \) and \( b \) generate \( \Sigma_n \) when \( k \) is even and \( A_n \) when \( k \) is odd.

**References**


