Generating alternating and symmetric groups with two elements of fixed order

Daniele Garzoni

Abstract

We answer a question raised by Lanier [3] about the possibility of generating \( A_n \) and \( S_n \) with two elements of order \( k \), where \( n \geq k \geq 3 \). We show that this can always be done apart from some clear exceptions.

1 Introduction

Results about generating sets of groups with order constraints have a long history. For alternating and symmetric groups, they go back to the beginning of the 20th century with a paper of Miller [7]. Miller showed that, except for some cases with \( n \leq 8 \), \( A_n \) is generated by an element of order 2 together with an element of order \( k = 3 \). He later [8] extended the result to the case \( k \geq 4 \), and he discussed the same question for symmetric groups. Results of similar flavour can be found for instance in [9].

Recently Lanier [3] addressed the problem of generating mapping class groups of surfaces with a small number of elements of fixed order \( k \geq 5 \). He showed that, if the genus of the surface is sufficiently large, then 3 elements suffice, except for the case \( k = 5 \), where he showed that 4 elements suffice. He then considered the same question for alternating and symmetric groups. The author finally combined the results for mapping class groups and alternating groups in order to obtain similar results for some automorphism groups of free groups and for \( \text{SL}(n, \mathbb{Z}) \).

Concerning alternating and symmetric groups, Lanier showed that if \( n \geq k \geq 3 \), then 3 elements of order \( k \) suffice to generate \( S_n \) if \( k \) is even and to generate \( A_n \) if \( k \) is odd. He then conjectured that 2 elements should in fact be enough. Moreover, he showed that, if \( 3 \leq k \leq n - 2 \) with \( k \) even, 4 elements of order \( k \) are sufficient in order to generate \( A_n \).

There are some obvious restrictions in this problem. First of all, if \( k \) is odd then the elements of order \( k \) lie in \( A_n \), so that they cannot generate \( S_n \). Moreover, if \( k \in \{n - 1, n\} \) is a power of 2, then the elements of order \( k \) coincide with the \( k \)-cycles: that, being odd permutations, cannot generate \( A_n \). Finally, for \( n = 6 \) the only elements of order 6 are the 6-cycles and the elements with cycle-shape \((2, 3, 1)\), both of which are odd permutations and cannot generate \( A_6 \).
In this note we show that no other restriction exists. In other words, we confirm the conjecture raised by Lanier and we improve his result for $A_n$ and $k$ even, including in our analysis also the case $k \in \{n-1, n\}$.

In order to make the statement of the result more concise, we introduce some terminology. Let $k$ be a positive integer, and let $G$ be a group. When $G$ is generated by finitely many elements of order $k$, we denote with $d_k(G)$ the smallest cardinality of a generating set of $G$ in which all elements have order $k$.

**Theorem 1.1.** Let $n \geq k \geq 3$ be natural numbers. The following hold:

(i) if $k$ is even, then $d_k(S_n) = 2$. Moreover, $d_k(A_n) = 2$ unless $k \in \{n-1, n\}$ is a power of 2 or $(n,k) = (6,6)$.

(ii) if $k$ is odd, then $d_k(A_n) = 2$ (unless $n = 3$ in which case $d_3(A_3) = 1$).

Consider now the free group $F_n$ on $n$ letters. There exists a map $\text{Aut}(F_n) \to \text{GL}(n, \mathbb{Z})$ induced by the projection $F_n \to F_n/\langle F_n \rangle \cong \mathbb{Z}^n$. The preimage of $\text{SL}(n, \mathbb{Z})$, that we denote with $\text{Aut}^+(F_n)$, is called the special automorphism group of $F_n$. Starting with $\text{Out}(F_n) = \text{Aut}(F_n)/\text{Inn}(F_n)$, with the same construction we can define $\text{Out}^+(F_n)$.

Theorem 1.1 gives immediately the following improvement of [3] Theorem 1.3 (see the proof of [3] Theorem 1.3).

**Theorem 1.2.** Let $n$ and $k$ be natural numbers, with $k \geq 5$ and $n \geq 2(k-1)$, and let $G$ be among $\text{Aut}^+(F_n)$, $\text{Out}^+(F_n)$ and $\text{SL}(n, \mathbb{Z})$. Then, $d_k(G) \leq 6$. If in addition $k \geq 6$ and $n \geq 2k$, then $d_k(G) \leq 5$.

**Acknowledgements**

I would like to thank László Pyber, for bringing [3] to my attention; and Justin Lanier, for some comments on his paper.

**2 Proof of Theorem 1.1**

The proof will be divided in two cases: $k \leq n/2$ and $k > n/2$. In every case, we will find two elements $a$ and $b$ of order $k$ such that $\langle a, b \rangle$ is primitive. At this point, in the literature there are several results — some of them going back to the 19th century — that ensure that a given primitive group $G$ with some additional properties must be either alternating or symmetric.

For instance, if $G$ is 2-transitive and contains an element with sufficiently small support, then it is either alternating or symmetric; this is due to Bochert [1]. Manning [5] proved a similar statement replacing 2-transitivity with 6-transitivity (see also [13], 16 p. 42). In the same spirit, Wielandt [12] showed that if $G$ is $t$-transitive and $t$ is large enough depending on $n$,
then $G$ is either alternating or symmetric. For us these results are enough; we summarise them in the following theorem. Recall that the support of a permutation is the set of points moved by the permutation.

**Theorem 2.1.** Let $G$ be a primitive permutation group of degree $n$. Then, $G$ contains $A_n$ provided one of the following conditions is satisfied:

(i) $G$ is 2-transitive and contains a nontrivial element $g$ with $|\text{supp}(g)| < n/3 - 2\sqrt{n}/3$.

(ii) $G$ is 6-transitive and contains a nontrivial element $g$ with $|\text{supp}(g)| < 3n/5$.

(iii) $G$ is $t$-transitive with $t \geq 3 \log n$ (here and elsewhere, logs in base 2).

The previous conditions require $G$ to be multiply transitive. An old result of Marggraff [6], with a short proof by Levingston and Taylor [4], gives a method to obtain this property.

**Theorem 2.2.** Let $G$ be a primitive permutation group of degree $n$. If $G$ contains a cycle fixing $m$ points, then $G$ is $(m + 1)$-transitive.

We remark that Theorem 2.1 can be dramatically strengthened using the CFSG. For instance, using the Schreier Conjecture O’Nan [10] [11] showed that in point (iii) it is possible to take $t = 6$. Point (ii) becomes therefore useless. Moreover, combining Theorem 2.2 with the classification of 4-transitive groups, it turns out that a primitive group containing a cycle fixing at least 3 points is either alternating or symmetric (see for instance [2]). For our purposes, however, these improvements would help only in small degree ($n \leq 90$), so that it does not seem the case to rely on them.

Once we have found $a$ and $b$ such that $\langle a, b \rangle$ is primitive and satisfies one of the conditions of Theorem 2.1, in order to conclude the proof of Theorem 1.1 it will be sufficient to control the parity of $a$ and $b$. More precisely, we will be able to choose $a$ and $b$ both odd (in which case $\langle a, b \rangle = S_n$) and both even (in which case $\langle a, b \rangle = A_n$).

It seems that we are proving too much choosing $a$ and $b$ both odd. However, the same pair $(a, b)$ will be even for some values of $n$ and $k$, and will be odd for some other values: so that, essentially, we will prove the statement for $A_n$ and $S_n$ all at once (see the proof of Claim 1 and the table after it).

As this may help in the exposition, we restate Theorem 1.1 in view of the last considerations. We say that an element of $S_n$ has sign $+1$ (resp. sign $-1$) if it is an even permutation (resp. odd permutation).

**Theorem 2.3.** Consider the set $\Omega$ of all triples $(n, k, s)$ such that $n \geq k \geq 3$ are natural numbers, $s \in \{+1, -1\}$, and the following conditions are satisfied:
(i) if $k$ is odd, then $s = +1$.

(ii) if $k \in \{n-1,n\}$ is a power of 2, then $s = -1$.

(iii) $(6,6,+1) \notin \Omega$.

Then, for every $\omega = (n,k,s) \in \Omega$, $S_n$ contains two elements $a_\omega$ and $b_\omega$ of order $k$, of sign $s$, such that $(a_\omega, b_\omega)$ is primitive and satisfies one of the conditions of Theorem 2.1.

Rather than dividing neatly all the cases, the strategy is to start with two somehow reasonable $a$ and $b$, and to modify them suitably whenever they do not work. With no risk of confusion, along the proofs the dependence on $\omega$ will be omitted: so that our elements will be $a$ and $b$. Also the symbol $s$ will often be omitted.

2.1 The case $k \leq n/2$

This is the case that will require the most computations. Here we will always apply Theorem 2.2 in order to use condition (iii) in Theorem 2.1. In other words, we will show that $(a, b)$ contains a cycle fixing at least $\lceil 3 \log n - 1 \rceil$ points. The cycle we are looking for will always be $a^{-1} b$.

We will first obtain $a$ and $b$ in every case, showing that $a^{-1} b$ is a cycle, but not caring about the number of points it fixes. Then, once all the $a$’s and $b$’s will be defined, we will make sure that enough points are fixed; and finally we will show that $(a, b)$ does not preserve any system of blocks. This is perhaps logically backwards, but the primitivity is the longest part, while the number of fixed points is fast, so that we prefer to present the proof in this order. Throughout, when we write the cycle decomposition of an element of $S_n$ we usually avoid to write the fixed points.

Claim 1. For every $\omega = (n,k,s) \in \Omega$ with $k \leq n/2$, there exist $a_\omega$ and $b_\omega$ of order $k$, of sign $s$, such that $(a_\omega, b_\omega)$ is transitive and $a_\omega^{-1} b_\omega$ is a cycle.

Proof. Consider $a = (1, \ldots, k)(k+1, \ldots, 2k) \cdots ((\lfloor n/k \rfloor - 1)k + 1, \ldots, \lfloor n/k \rfloor k)$ and $b$ the translation of $a$ on the right of $k - 1$ positions, that is, $b = (k, \ldots, 2k - 1)(2k, \ldots, 3k - 1) \cdots ((\lfloor n/k \rfloor k, \ldots, (\lfloor n/k \rfloor + 1)k - 1)$, where all the entries are viewed mod $n$. Throughout, these will be called the original $a$ and $b$. It is clear that $(a, b)$ is transitive. Moreover, unless specifically pointed out, any modification we will perform on $a$ and $b$ will only (possibly) unify some of their orbits, so that transitivity will not be compromised. Let $j$ be defined by the conditions $j \in \{0, \ldots, k-1\}$ and $n \equiv j \mod k$.

If $j = k-1$, direct computation shows that $a^{-1} b$ is a cycle: $a^{-1} b = (1, k+1, 2k+1, \ldots, \lfloor n/k \rfloor k + 1, \lfloor n/k \rfloor k + 2, \ldots, n, \lfloor n/k \rfloor k, (\lfloor n/k \rfloor - 1)k, \ldots, k - 1, \ldots, 2)$, where what happens in the dots should be clear. We choose these $a$ and $b$ when $j = k - 1$ and the sign is good. Note that if $k$ is odd then $s = +1$; hence certainly we choose these $a$ and $b$ when $k$ is odd. In order to
change sign, we multiply $a$ and $b$ respectively by $(\lfloor n/k \rfloor k + 1, \lfloor n/k \rfloor k + 2)$ and $(k - 2, k - 1)$. Note that the support of these transpositions is disjoint from the support of, respectively, $a$ and $b$, so that the new elements still have order $k$. Moreover, the result of this modification on $a^{-1}b$ amounts to multiplying it on the left by $(\lfloor n/k \rfloor k + 1, \lfloor n/k \rfloor k + 2)$ and on the right by $(k - 2, k - 1)$. Since the points of each transposition are consecutive points in the cycle $a^{-1}b$, the resulting element is the same cycle, in which though $k - 1$ and $\lfloor n/k \rfloor k + 2$ have disappeared.

If $j \neq k - 1$, the (original) $a^{-1}b$ is not a cycle; it is instead the product of 2 cycles of equal length (plus 1-cycles). However, it is easy to turn this element into a cycle: it is sufficient to multiply it on the right by $(k, k + 1, k + 2)$. This is equivalent to multiplying $b$ on the right by $(k, k + 1, k + 2)$, that is, to swapping $k$ and $k + 1$ in the first cycle of $b$. It is easy to check that the resulting cycle is $(k + 1, 2k + 1, \ldots, \lfloor n/k \rfloor k + 1, \lfloor n/k \rfloor k + 2, \ldots, n, 1, k + 2, k, k - 1, \ldots, k - j, \lfloor n/k \rfloor k, (\lfloor n/k \rfloor - 1)k, \ldots, 2k)$.\footnote{If $j = 1$, $\lfloor n/k \rfloor k + 1 = n$ and it is meant that $\lfloor n/k \rfloor k + 2$ does not appear in the writing. In the same way, if $j = 0$ it is meant that $k - 1$ does not appear; and if $\lfloor n/k \rfloor = 2$ it is meant that $(\lfloor n/k \rfloor - 1)k$ does not appear.} We choose these $a$ and $b$ when $j \neq k - 1$ and the sign is good (as above, certainly when $k$ is odd).

In order to change sign, we divide the cases $j \in \{0, 1\}$ and $j \notin \{0, 1\}$.

If $j \notin \{0, 1\}$, we may act exactly as in the case $j = k - 1$. If $j \in \{0, 1\}$, however, there is no space for multiplying by a transposition. We then go back to the original $a$ and $b$, and split the last cycle of the original $a$ and the last cycle of the original $b$ in two parts of length $k/2$. Note that, since $j \in \{0, 1\}$, the first $(k/2)$-cycle of $b$ contains $n$. It is easy then to see that $\langle a, b \rangle$ is transitive.

In fact, the first $(k/2)$-cycle of $b$ contains 1 unless $(k, j) = (4, 1)$. This feature implies different behaviors. In particular, if $(k, j) = (4, 1)$ then $a^{-1}b$ is a cycle: $a^{-1}b = (1, 5, \ldots, n - 4, n - 2, n, n - 1, n - 5, \ldots, 4, 3)$, where the steps in the dots again should be clear. In the other cases, instead, $a^{-1}b$ is a product of 2 cycles of equal length (plus 1-cycles). As we have already done, multiplying on the right by $(k, k + 1, k + 2)$ turns it into a cycle: $a^{-1}b = (k + 1, 2k + 1, \ldots, (\lfloor n/k \rfloor - 1)k + 1, (\lfloor n/k \rfloor - 1/2)k + 1, \lfloor n/k \rfloor k + 1, 1, k + 2, k, k - j, (\lfloor n/k \rfloor + 1/2)k, \lfloor n/k \rfloor k, (\lfloor n/k \rfloor - 1)k, \ldots, 2k)$ (where if $\lfloor n/k \rfloor = 2$ then $2k + 1$ and $(\lfloor n/k \rfloor - 1)k$ do not appear; and if $j = 0$ then $\lfloor n/k \rfloor k + 1$ and $k - j$ do not appear).

Although perhaps not strictly necessary, for the convenience of the reader we list $a$ and $b$ in the different cases.

Here (and only here) we adopt the notation used in [3], as it may help in compacting writings. For every $1 \leq i \leq n$, we denote with $h_i(a)$ a step $i$-cycle starting at $a$, namely, the cycle $(a, a + 1, \ldots, a + i - 1)$, where all the entries are viewed mod $n$. We set moreover $s_i(a, l) = \prod_{m=0}^{l-1} h_i(a + im)$, where all the entries are viewed mod $n$ and $1 \leq l \leq [n/i]$. For instance, the original $a$
and $b$, that were defined in the proof of Claim 1, are respectively $s_k(1, \lfloor n/k \rfloor)$ and $s_k(k, \lfloor n/k \rfloor)$. Since we will write these elements several times below, we take the chance to further compact notations and we call them respectively $a_0$ and $b_0$. Consider the following pair of $a$’s and $b$’s (the meaning of the conditions on $j$ are explained below; recall that $j \in \{0, \ldots, k-1\}$ and $n \equiv j \mod k$).

(i) $a = a_0$
    
    $b = b_0$ \quad $j = k - 1$

(ii) $a = a_0$
    
    $b = b_0 \cdot s_3(k, 1)$ \quad $j \neq k - 1$

(iii) $a = a_0 \cdot s_2(\lfloor n/k \rfloor k + 1, 1)$
    
    $b = b_0 \cdot s_2(k - 2, 1)$ \quad $j = k - 1$

(iv) $a = a_0 \cdot s_2(\lfloor n/k \rfloor k + 1, 1)$
    
    $b = b_0 \cdot s_2(k - 2, 1) \cdot s_3(k, 1)$ \quad $j \notin \{0, 1, k - 1\}$

(v) $a = s_k(1, \lfloor n/k \rfloor - 1) \cdot s_{k/2}(E_1 k + 1, 2)$
    
    $b = s_k(k, \lfloor n/k \rfloor - 1) \cdot s_{k/2}(k, 2) \cdot s_3(k, 1)$ \quad $j \in \{0, 1\}$, $(k, j) \neq (4, 1)$

(vi) $a = s_k(1, \lfloor n/k \rfloor - 1) \cdot s_{k/2}(E_1 k + 1, 2)$
    
    $b = s_k(k, \lfloor n/k \rfloor - 1) \cdot s_{k/2}(k, 2)$ \quad $(k, j) = (4, 1)$

In each pair, $a$ and $b$ have the same sign. Moreover, elements in (i) - (ii) have the same sign, opposite with respect to elements in (iii) - (vi). In order to obtain a generating pair we proceed as follows. Given $G_n \in \{A_n, S_n\}$, we look at the pairs which consist of even permutations if $G_n = A_n$, and of odd permutations if $S_n = A_n$. As already noticed in the proof of Claim 1, we look at (iii) - (vi) only if $k$ is even. Indeed, if $k$ is odd then $G_n = A_n$ and the even elements are (i) - (ii).

Once we have chosen among the two parts (i) - (ii) and (iii) - (vi), there is a unique pair depending on the congruence of $n$ mod $k$: that is the generating pair we are looking for. Actually, the cases $(n, k, s) = (6, 3, +1), (7, 3, +1), (8, 3, +1)$ are exceptions that will be handled separately.

It is of course possible to give a concrete description of the different cases. More precisely, if $G_n = A_n$ we must look at (i) - (ii) if and only if either $k$ is odd or $k$ and $\lfloor n/k \rfloor$ are both even. Conversely, if $G_n = S_n$ we must look at (i) - (ii) if and only if $k$ is even and $\lfloor n/k \rfloor$ is odd.

We go on with the proof. Now we look at the number of points fixed by the cycle $a^{-1}b$. 

6
Claim 2. For every \( \omega = (n, k, s) \in \Omega \), with \( k \leq n/2 \) and \( n \geq 90 \), \( a_\omega^{-1} b_\omega \) fixes at least \( [3 \log n - 1] \) points. If \( n < 90 \), the thesis of Theorem 2.3 is satisfied. It is necessary to change \( a_\omega \) and \( b_\omega \) only in the cases \((6, 3, +1), (7, 3, +1)\) and \((8, 3, +1)\).

**Proof.** Consider the supports of the \( k \)-cycles of the original \( a \), that is, \( c_i = \{ik + 1, ik + 2, \ldots, (i + 1)k\} \), \( i = 0, \ldots, \lfloor n/k \rfloor - 1 \). It is easy to check that, except for \( c_0, c_1 \) and \( c_{\lfloor n/k \rfloor - 1} \), each of the other \( c_i \)'s contains \( k - 2 \) points that are fixed by \( a^{-1} b \) in every case (namely, all the entries but those \( \equiv 0, 1 \mod k \)). Moreover, in \( c_1 \) there are at most 4 points not fixed by \( a^{-1} b \) (the maximum is attained when \( \lfloor n/k \rfloor = 2 \) and the second cycle of \( a \) has been split, in which case \( k + 1, k + 2, k + k/2 + 1, 2k \) are not fixed by \( a^{-1} b \)). Therefore, \( a^{-1} b \) fixes at least

\[
m := (\lfloor n/k \rfloor - 3)(k - 2) + (k - 4)
\]

points, where the first term appears only if \( \lfloor n/k \rfloor \geq 3 \) and the last term only if \( k \geq 4 \). Since either \( k \geq \sqrt{n} \) or \( \lfloor n/k \rfloor \geq \sqrt{n} - 1 \), it is clear that \( m \) is larger than \( 3 \log n - 1 \) provided \( n \) is large enough. Now we get some more concrete estimates.

Assume \( k = 3 \). Then \( \lfloor n/3 \rfloor \geq n/3 - 1 \) and it is easy to check that, for \( n \geq 90 \), \( m \) is larger than \( 3 \log n - 1 \). In the same way we can check that the same holds for \( k = 4, 5 \). On the other hand, if \( \lfloor n/k \rfloor = 2 \) then \( k \geq n/3 \) and \( m \geq 3 \log n - 1 \). In the same way we can check that the same holds for \( \lfloor n/k \rfloor = 3, 4 \) (for \( \lfloor n/k \rfloor = 3, n \geq 90 \) is sharp). Hence we may assume \( k \geq 6 \) and \( \lfloor n/k \rfloor \geq 5 \). Now either \( k \geq \sqrt{n} \) or \( \lfloor n/k \rfloor \geq \sqrt{n} - 1 \). In both cases, \( n \geq 90 \) is enough in order to have \( m \geq 3 \log n - 1 \).

For \( n \leq 89 \), it is possible to check that, except for the cases \((6, 3, +1), (7, 3, +1)\) and \((8, 3, +1)\), the \( a \)'s and \( b \)'s that we defined work: they generate \( A_n \) when \( s = +1 \) and \( S_n \) when \( s = -1 \). This can be done using a computer (or cheating and using the CFSG — there are very few cases in which \( a^{-1} b \) fixes less than 3 points! — see after Theorem 2.2).

In the three remaining cases, we modify \( b \). In the case \((6, 3, +1)\) we may take \( b = (3, 4, 5) \); in the case \((7, 3, +1)\) we may take \( b = (1, 2, 7)(3, 4, 5) \); and in the case \((8, 3, +1)\) we may take \( b = (1, 6, 7)(2, 5, 8) \).

\[ \square \]

Claim 3. For every \( \omega = (n, k, s) \in \Omega \), with \( k \leq n/2 \), \( \langle a_\omega, b_\omega \rangle \) is primitive.

**Proof.** Since in every case \( \langle a, b \rangle \) is transitive, there remains to show that \( \langle a, b \rangle \) does not preserve any system of blocks. Consider \( t \) a nontrivial divisor of \( n \), and consider a system of blocks in which each block has cardinality \( t \). Assume this system is preserved by some \( \langle a, b \rangle \); we want to get to a contradiction. Throughout the proof, for every \( i \in \{1, \ldots, n\} \) we indicate with \( B_i \) the block containing \( i \). We also write the action of \( S_n \) on \( \{1, \ldots, n\} \).
on the right. Recall that if a permutation $g$ preserves a system of blocks, if $c$ is a cycle in the cycle decomposition of $g$, and if $\Lambda_1, \ldots, \Lambda_r$ are the blocks that have nonempty intersection with $\text{supp}(c)$, then $|\Lambda_i \cap \text{supp}(c)| = |\Lambda_j \cap \text{supp}(c)|$ for every $i, j$, and $|\text{supp}(c)| = r \cdot |\Lambda_1 \cap \text{supp}(c)|$. In the following, when we mention cases (i) - (vi) we refer to those after Claim 1.

Note that the transitivity of $\langle a, b \rangle$ implies that there does not exist a block fixed by both $a$ and $b$. It is easy to see that, for every $(n, k, s)$, every $k$-cycle of $a$ either moves a fixed point of $b$ or moves some point in the same way as $b$ does.\footnote{With a unique exception, namely, when $k = 3$ and we are in case (ii). Then $(4, 5, 6)$ sends 4 to 5, as $b^{-1}$ — and not $b$ — does. For our argument there is no difference.} The same sentence holds true if we swap $a$ and $b$. Therefore, the support of a $k$-cycle of $a$ or $b$ intersects at least 2 blocks. The same holds for the transpositions $(\lfloor n/k \rfloor k + 1, \lfloor n/k \rfloor k + 2)$ and $(k - 2, k - 1)$ that we used to change parity to $a$ and $b$. Now $a$ and $b$ might have also $(k/2)$-cycles (cases (v), (vi)). If $k \geq 6$, the same consideration as above holds. If $k = 4$, however, direct check shows that the argument does not apply (when $j = 0$) to the transposition $(n - 1, n)$ of $a$ and to the transposition $(n, 1)$ of $b$; and (when $j = 1$) does not apply to the transposition $(n - 2, n - 1)$ of $a$. Nevertheless we can quickly see that not even such transpositions can fix a block.

For the last case ($j = 1$), assume $B_{n-2} = B_{n-1}$. Then $n - 5 = (n - 2)b$ and $n = (n - 1)b$ lie in $B_{n-2}b$; but $a$ fixes $n$ and $n - 5$ belongs to a 4-cycle of $a$, which contradicts what we said above. For the case $j = 0$, if $B_{n-1} = B_n$, then $B_{n-1}b^2 = B_{n-1}$ since $n$ belongs to a transposition of $b$. Then $n - 2 = (n - 1)b^3 \in B_{n-1}b^3 = B_{n-1}b$; but also $n - 2 = (n - 1)b^2a \in B_{n-1}b^2a = B_{n-1}$, contradiction. Similarly we can see that $B_n = B_1$ cannot occur. Therefore, we have that, for every $(n, k, s)$, the support of an $m$-cycle of $a$ or $b$ is contained in one block if and only $m = 1$.

(1)

In particular, some blocks are made of the points fixed by $a$, and this implies $j \neq 1$, as otherwise a block would consist of 1 point.

Assume now $a$ has fixed points. Since $j \neq 1$, the last cycles of $a$ and $b$ have not been split (that is, we are not in cases (v), (vi)). The set of points fixed by $a$ is some $\{n - t, \ldots, n\}$, with $\lfloor n/k \rfloor k + 1 \leq n - t \leq n - 1$, and some blocks are made of these points. However, it is easy to check that $b$ takes only the point $n$ outside of this set, hence it cannot preserve these blocks. Therefore, $a$ has no fixed points, and either $j = 0$ or $j = 2$ and the original $a$ has been multiplied by $(n - 1, n)$.

In the latter case (case (iv)), by (1) $B_{n-1} \neq B_n$, and a suitable $k$-cycle $c$ of $a$ collaborates to exchange these blocks. Recall now that $a^{-1}b$ is a cycle. Its support contains $k$ and $k + 2$, and $kb = k + 2$, hence by transitivity of $\langle a, b \rangle$ the support of $a^{-1}b$ must intersect more than 1 block. In particular, $a^{-1}b$ fixes 1 block if and only if it fixes it pointwise (the same argument works also for the case $j = 0$).

(2)
points fixed by $a^{-1}b$ and $k/2$ points not fixed by $a^{-1}b$, in such a way that a point fixed by $a^{-1}b$ is followed by a point not fixed by $a^{-1}b$ and vice versa. However, it is easy to see that $a$ does not have a $k$-cycle with this property. Therefore, $j = 0$.

In this case, the points not fixed by $a^{-1}b$ are all the $i \equiv 0, 1 \mod k$, $k + 2$ and possibly (case (v)) $n - k/2 + 1$ and $k/2$. Note that $(k+1)b = k$, and $kb = k + 2$. By (1), $B_{k+1} \neq B_k$. If $k + 2 \in B_{k+1}$, then $k \neq 3$ as $(4, 3, 5)$ should intersect the blocks in the same number of points (as noticed at the beginning of the proof). Hence $k + 3 = (k + 2)b \in B_{k+2} = B_k$, and since $k$ is not fixed by $a^{-1}b$, by (2) we obtain that $k + 3$ is not even fixed. Looking at the list of (non)fixed points above, the unique possibility is $n - k/2 + 1 = k + 3$: looking mod $k/2$ we get $k = 4$ and $n = 8$, case that we can check singularly.

Therefore, $B_{k+1}, B_k, B_{k+2}$ are pairwise distinct. Let $k + 1 \neq i \in B_{k+1}$. Then by (2) we should have that $i, ib, ib^2$ are pairwise distinct, different from $k + 1, k, k + 2$ and not fixed by $a^{-1}b$. However, it is easy to check that an $i$ with this property does not exist.

\[\square\]

2.2 The case $k > n/2$

Here we will apply points (i) and (ii) of Theorem 2.1. Moreover, we further divide in two cases. More precisely, for the moment we exclude the case of alternating groups and $k \in \{n - 1, n\}$ even. In other words, in the language of Theorem 2.3 we assume that the following condition, call it (A), holds: $k > n/2$, and whenever $k$ is even and $s = +1$, then $k \leq n - 2$.

Proof of Theorem 2.3 in case (A). The case in which it is possible to choose $k$-cycles (namely, $k$ odd or $k$ even and $s = -1$) were dealt already in [8]. Anyway, for completeness we exhibit generating pairs here. If $k \leq n - 1$ we can take $a = (1, 2, \ldots, k)$ and $b = (1, 2, \ldots, 2k - n, k + 1, k + 2, \ldots, n)$. In the case $(n, k) = (6, 4)$ actually we should change something and take for instance $b = (1, 3, 5, 6)$. If $k = n$, we can take the same $a$ and $b = a(1, 2, 3)$. We omit the details of the verification since they are straightforward (and very similar to those that we present below).

Now we deal with the case in which it is not possible to choose $k$-cycles, namely, $k$ even and $s = +1$. Consider $a = (1, 2, \ldots, k)(k + 1, k + 2)$ and $b = (1, 2, \ldots, 2k - n, k + 1, k + 2, \ldots, n)(2k - n + 1, 2k - n + 2)$. It is easy to check that $\langle a, b \rangle$ is transitive; now we show that $\langle a, b \rangle$ is primitive as well.

Assume $\langle a, b \rangle$ preserves some system of blocks. The transposition of $a$ exchanges 2 blocks otherwise, since $(k + 1)b = k + 2$, a block would be fixed by both $a$ and $b$. Since the $k$ cycle of $a$ sends $2k - n + 1$ to $2k - n + 2$, also the transposition of $b$ exchanges these 2 blocks, and since $\langle a, b \rangle$ is transitive there cannot be other blocks. This implies that $a$ and $b$ do not have fixed points, namely, $k = n - 2$. Therefore, in the case $k \leq n - 3 \langle a, b \rangle$ is primitive. In the
case $k = n - 2$, instead, $(a, b)$ preserves the blocks $\{1 \leq i \leq n, i \text{ even}\}$ and $\{1 \leq i \leq n, i \text{ odd}\}$. If $n \geq 8$, we can multiply $b$ on the right by $(1, 2, 3)$: it is easy to see that, with this modification, $(a, b)$ cannot preserve any system of blocks. For $n = 6$, we choose $b = (1, 3, 5, 6)(2, 4)$: it works.

Both in the cases $k \leq n - 3$ and $k = n - 2$, we can check that $a^{-1}b$ is a cycle that fixes for instance the point $k + 2$. Hence, by Theorem 2.2 $(a, b)$ is 2-transitive. Now direct computation shows that $a^{-1}bab^{-1} = b^3b^{-1}$ moves at most 8 points. Therefore, by Theorem 2.1 (i) we are done provided $8 < n/3 - 2\sqrt{n}/3$. The cases $n \leq 36$ can be checked singularly, so that the proof is complete.

Finally, we deal with the remaining case, namely, $k \in \{n - 1, n\}$ and we cannot choose $k$-cycles. In other words, the following condition (B) holds: $k \in \{n - 1, n\}$ is even, is not a prime power and $s = +1$.

Proof of Theorem 2.3 in case (B). Write $k = 2^mq$, where $m \geq 1$ and $q \geq 3$ is odd. Consider the following cycle-shape: $z = (q, 2^m, \ldots, 2^m, 2, \ldots, 2)$, where there are $(2^m)$-cycles in number $t \geq 1$ and (if $m \geq 2$) 2-cycles in number $0 \leq l \leq 2^{m-1} - 1$, in such a way that $n - 1 \leq q + 2^mt + 2l \leq n$. In other words, we start with a $q$-cycle, then we put as many $2^m$-cycles as we can, and finally we put as many 2-cycles as we can.

Observe that if $q + 2^{m+1} \leq k = q2^m$, that is, $2^{m+1}/(2^m - 1) \leq q$, then $t \geq 2$. Now $2^{m+1}/(2^m - 1)$ is decreasing for $m \geq 2$, and $3/(2^2 - 1) < 3 < q$, hence $t \geq 2$ in this case. If $m = 1$, $t \geq 2$ unless $q = 3$, that is, $k = 6$. For the moment we exclude this case, so that we have $t \geq 2$.

Now we consider $z$ as a partition of $n$, adding 1 at the end if necessary. If it defines an odd permutation, we split the first $(2^m)$-cycle into $(2^m - 1)$-cycles (so that we get 1-cycles in the case $m = 1$). Now we put the numbers $\{1, \ldots, n\}$ into the cycles, from left to right, obtaining an element of $S_n$ that we call $a$: $a = (1, 2, \ldots, q)(q + 1, q + 2, \ldots, q + 2^m)(\ldots)$ (of course, if the first $(2^m)$-cycle has been splitted then $a$ is different). Since $a$ has still at least a $(2^m)$-cycle, it has order $2^mq = k$. Moreover, by construction $a$ lies in $A_n$. We then define $b$ as the element of $A_n$ which has the same cycle-shape of $a$, and which is obtained translating $a$ on the right of $q - 2$ positions, that is, $b = (q - 1, q, \ldots, 2q - 2)(2q - 1, 2q, \ldots, 2q + 2^m - 2)(\ldots)$, where of course the translation is seen mod $n$.

It is easy to see that $(a, b)$ is transitive. The key point is that $q$ and $2q - 2$ are nonequivalent mod 2, and nothing changes if we add cycles of even length: this allows to pass back and forth cycles of $a$ and cycles of $b$, until reaching the last cycle of $b$. Since such cycle contains the point $n$, we have that $(a, b)$ is indeed transitive.

Assume now that $(a, b)$ preserves some system of blocks, each block having cardinality $t$. Call $c$ the $q$-cycle of $a$, and call $d$ the $q$-cycle of $b$. Note that $c$ cannot fix a block, for $(q - 1)b = q$ would imply that $b$ also fixes the

\[\]
block. Therefore, the support of $c$ intersects $r > 1$ blocks, with $r$ divisor of $q$. Since $r$ is odd, it does not divide the length of any other cycle of $a$, hence $c$ permutes all the points of these $r$ blocks. Clearly, the same consideration holds for $d$. Now, employing the notation used in the proof of Claim 3, we have $B_{q-1} \neq B_q$. Hence $B_{q-1}$ and $B_q$ should be contained in the support of both $c$ and $d$. However, the intersection of such supports is $\{q-1, q\}$, and we obtain a contradiction. Therefore, $\langle a, b \rangle$ is primitive.

There remains to conclude that $\langle a, b \rangle = A_n$. A suitable power of $a$ is a $q$-cycle, and $q \leq n/2$; hence by Theorem 2.2 $G$ is 6-transitive provided $n/2 \geq 5$, which is true since we assumed $(n, k) \neq (7, 6)$. Now $q \leq n/2 < 3n/5$, hence we conclude by Theorem 2.1 (ii).

In the case $(n, k) = (7, 6)$, it is easy to verify that $a = (1, 2, 3)(4, 5)(6, 7)$ and $b = (2, 3, 4)(5, 6)(7, 1)$ generate $A_7$ (these are exactly the kind of elements we have used in this proof).

\[\square\]

References

[1] A. Bochert, Über die Classe der Transitiven Substitutionengruppen, Math. Ann. 49 (1897), 131-144.

[2] G.A. Jones, Primitive permutation groups containing a cycle, Bulletin of the Australian Mathematical Society 89(01) (2014), 159-165.

[3] J. Lanier, Generating mapping class groups with elements of fixed finite order, available at https://arxiv.org/abs/1710.04680.

[4] R. Levingston, D. E. Taylor, The theorem of Marggraff on primitive permutation groups which contain a cycle, Bulletin of the Australian Mathematical Society 15(1) (1976), 125-128.

[5] W.A. Manning, The degree and class of multiply transitive groups, III. Transactions of the American Mathematical Society, 35(3) (1933), 585-599.

[6] B. Marggraff, Über primitive Gruppen mit transitiven Untergruppen geringeren Grades, Buchdruckerei O. Lange, 1889.

[7] G.A. Miller, On the groups generated by two operators. Bulletin of the American Mathematical Society 7(10) (1901), 424-426.

[8] G.A. Miller, Possible orders of two generators of the alternating and of the symmetric groups, Transactions of the American Mathematical Society 30(1) (1928), 24-32.

[9] Ya N. Nuzhin, Generating triples of involutions of alternating groups, Mathematical Notes 51(4) (1992), 389-392.
[10] M. O’Nan, Normal structure of the one-point stabilizer of a doubly-transitive permutation group I, Transactions of the American Mathematical Society 214 (1975), 1-42.

[11] M. O’Nan, Normal structure of the one-point stabilizer of a doubly-transitive permutation group II, Transactions of the American Mathematical Society 214 (1975), 43-74.

[12] H. Wielandt, Abschätzungen für den Grad einer Permutationsgruppe von vorgeschriebenem Transitivitätsgrad, Schriften des Math. Sem. und des Inst. für angew. Math. der Univ. Berlin 2 (1934), 151-174.

[13] H. Wielandt, Finite Permutation Groups, Academic Press, New York, 1964.

Daniele Garzoni, Università degli Studi di Padova, Dipartimento di Matematica “Tullio Levi-Civita”, Via Trieste 63, 35121 Padova, Italy
E-mail address: daniele.garzoni@phd.unipd.it