Available online at www.sciencedirect.com
ScienceDirect
Journal of Combinatorial Theory, Series A 113 (2006) 1572–1581
Journal of Combinatorial Theory Series A
www.elsevier.com/locate/jcta

Note

Sets of permutations that generate the symmetric group pairwise

Simon R. Blackburn

Department of Mathematics, Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK

Received 23 August 2005

Available online 21 February 2006

Abstract

The paper contains proofs of the following results. For all sufficiently large odd integers n, there exists a set of 2^{n-1} permutations that pairwise generate the symmetric group S_n. There is no set of $2^{n-1}+1$ permutations having this property. For all sufficiently large integers n with $n \equiv 2 \bmod 4$, there exists a set of 2^{n-2} even permutations that pairwise generate the alternating group A_n. There is no set of $2^{n-2}+1$ permutations having this property.

Keywords: Alternating group; Symmetric group; Subgroup covering; Local lemma

1. Introduction

Let G be a finite group that can be generated by two elements. We say that a subset $X \subseteq G$ *generates G pairwise* if for all $g_1, g_2 \in X$ with $g_1 \neq g_2$ we have that g_1 and g_2 generate G. We write $\mu(G)$ for the largest cardinality of a set X that generates G pairwise. The purpose of this paper is to prove the following two theorems.

Theorem 1. *For all sufficiently large odd integers n, we have that $\mu(S_n) = 2^{n-1}$.*

Theorem 2. *For all sufficiently large integers n such that $n \equiv 2 \bmod 4$, we have that $\mu(A_n) = 2^{n-2}$.*

E-mail address: s.blackburn@rhul.ac.uk.

0097-3165/$ – see front matter
doi:10.1016/j.jcta.2006.01.001

Theorem 1 partially answers a question of Maróti [10]. Indeed, Maróti [10, Theorem 1.2] proves Theorem 1 in the case when we restrict n to be a prime greater than 23 and not of the form $(q^k - 1)/(q - 1)$ for a prime power q and integer k.

The integer $\sigma(G)$ is defined to be the smallest integer k such that G may be written as a union of k proper subgroups. Cohn [6] studied this quantity in 1994, although the study of groups as unions of proper subgroups has a much longer history [4,8,13]. The integers $\mu(G)$ and $\sigma(G)$ are related. Indeed, since a set X that generates G pairwise cannot contain two elements of any proper subgroup, we must have that $\mu(G) \leqslant \sigma(G)$. Let n be an integer such that $n > 3$. Maróti [10, Theorem 1.1] proves $\sigma(S_n) = 2^{n-1}$ when n is odd, except possibly $n = 9$, and that $\sigma(A_n) = 2^{n-2}$ when $n \equiv 2 \bmod 4$. Thus Theorems 1 and 2 show that $\mu(S_n) = \sigma(S_n)$ whenever n is large and odd, and $\mu(A_n) = \sigma(A_n)$ whenever n is large and $n \equiv 2 \bmod 4$.

As Maróti points out, an alternative motivation for the study of $\mu(G)$ comes from its relationship with the commuting graph of a group G. The *commuting graph* of G is a graph Γ whose vertices are the elements of G and where distinct $x, y \in G$ are joined by an edge if and only if they commute; see Pyber [12], for example. Brown [2,3] investigates the maximum cardinality $\alpha(G)$ of an empty induced subgraph of Γ and the minimum number $\beta(G)$ of a covering of the vertices of Γ by complete subgraphs in the case when $G = S_n$. It is clear that $\alpha(S_n) \leqslant \beta(S_n)$; Brown shows that $\alpha(S_n)$ and $\beta(S_n)$ are close to each other, but are never equal when $n \geqslant 16$. When G is a group that is generated by two elements, we may define another graph Γ' whose vertices are the elements of G and where distinct $x, y \in G$ are joined by an edge if and only if $\langle x, y\rangle$ is a proper subgroup of G. When G is non-abelian, it is easy to see that Γ' may be obtained by adding edges to Γ. Now $\mu(G)$ may be interpreted as the maximum cardinality of an empty subgraph of Γ'. Define $\nu(G)$ to be the minimum covering of the vertices of Γ' by complete subgraphs. It is easy to see that $\mu(G) \leqslant \nu(G) \leqslant \sigma(G)$. Our proof that $\mu(S_n) = \sigma(S_n)$ for all sufficiently large odd integers n shows that $\mu(S_n) = \nu(S_n)$ for all sufficiently large odd integers n, which is in stark contrast to Brown's result for the commuting graph referred to above.

Our proof of Theorems 1 and 2 use probabilistic methods. In particular, the proofs do not construct specific sets X that generate the symmetric or alternating group pairwise. It would be interesting to find explicit constructions for these sets X.

The known results regarding $\sigma(S_n)$ and $\sigma(A_n)$ depend heavily on whether n is even or odd. (For example, Maróti [10, Theorem 1.1] has shown that $\sigma(S_n) \leqslant 2^{n-2}$ when n is even.) This indicates that it might not be straightforward to generalise Theorem 1 to the case when n is an arbitrary sufficiently large integer. Similarly, Theorem 2 might not easily generalise to the case when n is odd, or when 4 divides n.

It would be interesting to know how far the results of this paper are true in a more general setting. In a preprint of this paper, I asked whether it is the case that $\mu(G) = \sigma(G)$ for all but finitely many non-abelian finite simple groups G. Beth Holmes (personal communication) tells me that she has proved that $\mu(\mathrm{Sz}(q)) < \sigma(\mathrm{Sz}(q))$, and thus this question is settled in the negative. Maybe something weaker is true, namely that $\sigma(G)/\mu(G) \to 1$ as the order of the finite simple group G tends to infinity?

The remainder of this paper is divided into four sections. The first section introduces some notation and briefly explains the strategy behind our proof of Theorem 1. Section 3 proves various results concerning maximal subgroups of the symmetric group that we require. Section 4 introduces our main combinatorial tool (the Local lemma) and proves Theorem 1. Finally, Section 5 sets out what changes to the proof of Theorem 1 are needed in order to produce a proof of Theorem 2.

2. Preliminaries and motivation

The purpose of this section is to motivate our proof of Theorem 1, and to introduce some of the notation we need for this proof. We defer any discussion of Theorem 2 until Section 5.

Let n be an odd integer. We think of the elements of S_n as being permutations on the set Ω, where $\Omega = \{1, 2, \ldots, n\}$. It is not difficult to see that S_n may be expressed as the union of A_n and the maximal intransitive subgroups of S_n. (For if a permutation g is not contained in any intransitive subgroup of S_n then g is an n-cycle and so g is even since n is odd.) There are $2^{n-1} - 1$ partitions of Ω with exactly 2 parts, and such partitions correspond to maximal intransitive subgroups of S_n. So there is a covering of S_n by 2^{n-1} proper subgroups $M_1, M_2, \ldots, M_{2^{n-1}}$. Let X generate S_n pairwise. Now

$$|X| = |X \cap S_n| = \left| X \cap \left(\bigcup_{i=1}^{2^{n-1}} M_i \right) \right| \leqslant \sum_{i=1}^{2^{n-1}} |X \cap M_i| \leqslant 2^{n-1}, \tag{1}$$

since any set X that generates S_n pairwise can contain at most one element in any proper subgroup of S_n. Thus $\mu(S_n) \leqslant 2^{n-1}$. So in order to prove Theorem 1 it suffices to show that for all sufficiently large odd integers n there exists a subset $X \subseteq S_n$ of cardinality 2^{n-1} that generates S_n pairwise. Note that (1) shows that any set X of cardinality 2^{n-1} that generates S_n pairwise must have $|X \cap M_i| = 1$ for $i \in \{1, 2, \ldots, 2^{n-1}\}$; moreover any element of X can be contained in at most one of the subgroups M_i. This motivates our method for proving the existence of such a set X.

Let $\ell_1, \ell_2, \ldots, \ell_r$ be positive integers such that $\ell_1 \leqslant \ell_2 \leqslant \cdots \leqslant \ell_r$. We say that a permutation $g \in S_n$ is an $(\ell_1, \ell_2, \ldots, \ell_r)$-*cycle* if g consists of r disjoint cycles, of lengths $\ell_1, \ell_2, \ldots, \ell_r$. (We include cycles of length 1, so $\ell_1 + \ell_2 + \cdots + \ell_r = n$.) When $r = 1$, we say that g is an n-cycle rather than an (n)-cycle.

Let $\Delta \subseteq \Omega$ be such that $0 < |\Delta| < n/2$. Define $C(\Delta)$ to be the set of all $(|\Delta|, n - |\Delta|)$-cycles g such that $\Delta g = \Delta$. Thus a permutation in $C(\Delta)$ is simply a permutation made up of two disjoint cycles, one involving all the elements of Δ and the other involving all the elements of the complement $\overline{\Delta}$ of Δ in Ω. We extend this definition to the case when $\Delta = \emptyset$ in the natural way, by defining $C(\emptyset)$ to be the set of all n-cycles in S_n. Note that when $|\Delta| = k$, we have that $|C(\Delta)| = (k-1)!(n-k-1)!$, where we use the convention that $(-1)! = 1$.

There are 2^{n-1} subsets Δ of Ω with $0 \leqslant |\Delta| < n/2$. For each such subset Δ, we will choose a permutation $g_\Delta \in C(\Delta)$ (and we will choose the permutations g_Δ uniformly and independently at random). We define

$$X = \{ g_\Delta \colon\ \Delta \subseteq \Omega,\ |\Delta| < n/2 \}.$$

Our aim is to prove that with non-zero probability X generates S_n pairwise. To do this, we establish an upper bound on the probability p that a fixed pair $g_{\Delta_1}, g_{\Delta_2}$ of elements from X generates a proper subgroup of S_n. We use a combinatorial tool (the Lovász Local lemma) to deduce from this upper bound that the probability that X generates S_n pairwise is non-zero.

We use some facts about the maximal subgroups of S_n to give an upper bound on p; these facts are given in Section 3. Section 4 uses the material developed in Section 3 to derive the upper bound we need, and then applies the Local lemma to finish the proof of Theorem 1.

3. Maximal subgroups

Our proof of Theorem 1 uses the following information about the maximal subgroups of S_n. We use standard notation from permutation group theory without explanation; see Cameron [5] for a good introduction to the area.

Theorem 3. *There exists a constant c with the property that for any positive odd integer n and any maximal subgroup M of S_n one of the following statements holds*:

(i) *M is intransitive. So there exist positive integers k and ℓ with $k+\ell=n$ such that $M \cong S_k \times S_\ell$.*
(ii) *$M \cong A_n$.*
(iii) *$M \cong S_{n/3} \operatorname{wr} S_3$ (in its imprimitive action).*
(iv) *$|M| \leqslant (\frac{n}{5e})^n e^{c \log n}$.*

Proof. Suppose that M is a transitive maximal subgroup of S_n, and suppose that $M \ncong A_n$. If M is primitive, then $|M| \leqslant 4^n$ by a result of Praeger and Saxl [11], and hence $|M| \leqslant (\frac{n}{5e})^n e^{O(\log n)}$. So we may assume that M is imprimitive. Now $M \cong S_k \operatorname{wr} S_\ell$ where k and ℓ are integers such that $k \geqslant 2$, $\ell \geqslant 2$ and $k\ell = n$. Since n is odd, ℓ is odd. If $\ell = 3$ then we are in case (iii) of the theorem, and so we may assume that $\ell \geqslant 5$. But in this case $|M| = k!^\ell \ell!$ and it is not difficult to prove that we are in case (iv) of the theorem; we use the following corollary of Stirling's formula:

$$r! \leqslant e^{r\log r - r + \frac{1}{2}\log r + 2}.$$

(See, for example, Whittaker and Watson [15, Section 12.33] for a proof of Stirling's formula.) □

We now state two lemmas that are concerned with $(s, n-s)$-cycles and maximal subgroups of S_n.

Lemma 4. *Let n be a positive integer. Let M be a fixed subgroup of S_n. Let g be a fixed element of S_n, and suppose that g is an n-cycle, or that g is an $(s, n-s)$-cycle for some integer s such that $1 \leqslant s \leqslant n/2$. Then g is contained in at most n^2 conjugates of M in S_n.*

Proof. We first consider the case when g is an $(s, n-s)$-cycle. Let $a_s(M)$ be the number of conjugates of M that contain a fixed $(s, n-s)$-cycle. The fact that all $(s, n-s)$-cycles in S_n are conjugate shows that this number does not depend on the $(s, n-s)$-cycle we choose. We need to show that $a_s(M) \leqslant n^2$.

Let $b_s(M)$ be the number of $(s, n-s)$-cycles in M (or any conjugate of M). Clearly $b_s(M) \leqslant |M|$.

When $s \neq n/2$, there are $n!/(s(n-s))$ elements of S_n that are $(s, n-s)$-cycles; when $s = n/2$, there are $n!/(2s(n-s))$ elements of S_n that are $(s, n-s)$-cycles. Thus the number of $(s, n-s)$-cycles in S_n is at least $n!/n^2$. There are $|S_n/N_{S_n}(M)|$ conjugates of M in S_n, and since $M \leqslant N_{S_n}(M)$ this number is at most $n!/|M|$. If we count pairs (h, H), where H is a conjugate of M and where $h \in H$ is an $(s, n-s)$-cycle, in two ways we find that

$$\frac{n!}{n^2} a_s(M) \leqslant \frac{n!}{|M|} b_s(M).$$

Hence $a_s(M) \leqslant n^2(b_s(M)/|M|) \leqslant n^2$, as required.

When g is an n-cycle, we may use the fact that S_n contains $n!/n$ elements that are n-cycles to show that g is contained in at most n conjugates of M, using the same argument as above. Since $n \leqslant n^2$, the lemma follows. □

The proof of the following lemma is elementary, and so we omit it.

Lemma 5. *Let n be a positive integer. Let k and ℓ be integers such that $k \geqslant 2$, $\ell \geqslant 2$ and $k\ell = n$. Let M be a wreath product isomorphic to $S_k \operatorname{wr} S_\ell$ in its standard action on the set Ω. Let $g \in M$ be an $(s, n-s)$-cycle on Ω. Then one of the following two cases occurs.*

(i) *We have that $s = xk$ for some integer x. The two orbits of g are unions of x and $\ell - x$ blocks, respectively. The permutation g induces an $(x, \ell - x)$-cycle in S_ℓ.*
(ii) *We have that $s = x\ell$ for some integer x. One orbit of g intersects every block in a set of size x, and the other orbit intersects every block in a set of size $k - x$. The permutation g induces an ℓ-cycle in S_ℓ.*

Any n-cycle in M induces an ℓ-cycle in S_ℓ.

If g is an $(s, n-s)$-cycle that falls under part (i) of Lemma 5, we say that g *acts respectfully*. If g is an $(s, n-s)$-cycle that does not act respectfully, or if g is an n-cycle, then we say that g *acts disrespectfully*.

4. The proof of Theorem 1

The combinatorial tool we shall use is the Lovász Local lemma [7] (see also Shearer [14] and Alon and Spencer [1]), which may be stated as follows.

Lemma 6. *Let Γ be a finite graph with maximum valency d. Suppose that we associate an event E_v to every vertex $v \in \Gamma$, and suppose that E_v is independent of any subset of the events $\{E_u\colon u \nsim v\}$. Let p be such that $\Pr(E_v) < p$ for all v. Then $\Pr(\bigcap_{v\in\Gamma} \overline{E_v}) > 0$ whenever $ep(d+1) < 1$. (Here e is the base of the natural logarithm.)*

We now prove Theorem 1. Our strategy is as follows. Define

$$I = \bigl\{\Delta \subset \{1, 2, \ldots, n\}\colon |\Delta| < n/2\bigr\}.$$

Note that $|I| = 2^{n-1}$. We choose our set X of elements of S_n by choosing elements $g_\Delta \in C(\Delta)$ uniformly and independently at random and defining $X = \{g_\Delta\colon \Delta \in I\}$. To establish Theorem 1 it is sufficient to show that the probability that X generates S_n pairwise is non-zero.

Define a graph Γ as follows. The vertices of Γ are the two element subsets of I. We join vertices J and J' by an edge if and only if $J \cap J' \neq \emptyset$. Note that every vertex of Γ has valency d, where $d = 2(2^{n-1} - 2)$.

For a vertex $\{\Delta_1, \Delta_2\} \in \Gamma$, define E_{Δ_1,Δ_2} to be the event that $\langle g_{\Delta_1}, g_{\Delta_2}\rangle$ is a proper subgroup of S_n. It is clear that E_{Δ_1,Δ_2} is independent of any subset of the events E_u where $u \in \Gamma$ is not joined to $\{\Delta_1, \Delta_2\}$ by an edge. Now, the event that every pair of elements from X generates S_n is exactly the event $\bigcap_{v\in\Gamma} \overline{E_v}$. Hence Theorem 1 follows by Lemma 6, provided that we can show that for all sufficiently large odd integers n we have that $\Pr(E_v) < p$ for all $v \in \Gamma$, where p is such that $ep(d+1) < 1$. So it is sufficient to show that for all sufficiently large odd integers n

$$\Pr(E_{\Delta_1,\Delta_2}) = o\bigl(2^{-n}\bigr) \tag{2}$$

for all $\{\Delta_1, \Delta_2\} \in \Gamma$.

Let Δ_1 and Δ_2 be fixed. Recall the constant c that we introduced in the statement of Theorem 3. Write E_1 for the event that $\langle g_{\Delta_1}, g_{\Delta_2}\rangle \leqslant M$, where $|M| \leqslant (\frac{n}{5e})^n e^{c\log n}$. Write E_2 for the event that $\langle g_{\Delta_1}, g_{\Delta_2}\rangle \leqslant M$, where M is a maximal subgroup isomorphic to $S_{n/3} \operatorname{wr} S_3$. (So $E_2 = \emptyset$ when 3 does not divide n.)

Lemma 7. *We have that* $\Pr(E_{\Delta_1,\Delta_2}) \leqslant \Pr(E_1) + \Pr(E_2)$.

Proof. Suppose that $\langle g_{\Delta_1}, g_{\Delta_2}\rangle$ is a proper subgroup H of S_n. Then $H \leqslant M$ for some maximal subgroup M of S_n. Since $\Delta_1 \neq \Delta_2$, we find that g_{Δ_1} and g_{Δ_2} always generate a transitive subgroup of S_n, and so M is transitive. Now g_Δ is even if and only if $\Delta = \emptyset$ (since n is odd). Hence at least one of g_{Δ_1} and g_{Δ_2} is odd and thus $M \neq A_n$. Thus, by Theorem 3, we find that $M \cong S_{n/3} \operatorname{wr} S_3$ or $|M| \leqslant (\frac{n}{5e})^n e^{c\log n}$. We have shown that $E_{\Delta_1,\Delta_2} \subseteq E_1 \cup E_2$, and so the lemma follows. $\square$

Lemma 8. $\Pr(E_1) \leqslant (\frac{2}{5})^{n+O(\log n)} = o(2^{-n})$.

Proof. Let $M_1, M_2, \ldots, M_r$ be a complete set of representatives of the conjugacy classes of maximal subgroups of S_n of order at most $(\frac{n}{5e})^n e^{c\log n}$. The number of such conjugacy classes is rather small: Liebeck and Shalev [9, Corollary 4.5] proved that S_n has at most $(\frac{1}{2} + o(1))n$ conjugacy classes of maximal subgroups, and so we find that $r \leqslant (\frac{1}{2} + o(1))n$. If we write $[M_i]$ for the set of subgroups of S_n that are conjugate to M_i, we find that

$$\begin{aligned}
\Pr(E_1) &\leqslant \sum_{i=1}^{r} \sum_{H\in[M_i]} \Pr(g_{\Delta_1}, g_{\Delta_2} \in H)\\
&= \sum_{i=1}^{r} \sum_{H\in[M_i]} \frac{1}{|C(\Delta_1)|} \sum_{g_{\Delta_1}\in C(\Delta_1)} \Pr(g_{\Delta_1}, g_{\Delta_2} \in H)\\
&= \sum_{i=1}^{r} \sum_{H\in[M_i]} \frac{1}{|C(\Delta_1)|} \sum_{g_{\Delta_1}\in C(\Delta_1)\cap H} \Pr(g_{\Delta_2} \in H)\\
&= \sum_{i=1}^{r} \frac{1}{|C(\Delta_1)|} \sum_{g_{\Delta_1}\in C(\Delta_1)} \sum_{g_{\Delta_1}\in H\in[M_i]} \Pr(g_{\Delta_2} \in H)\\
&\leqslant \sum_{i=1}^{r} \frac{1}{|C(\Delta_1)|} \sum_{g_{\Delta_1}\in C(\Delta_1)} \sum_{g_{\Delta_1}\in H\in[M_i]} \frac{1}{|C(\Delta_2)|}|M_i|\\
&\leqslant \sum_{i=1}^{r} \frac{1}{|C(\Delta_1)|} \sum_{g_{\Delta_1}\in C(\Delta_1)} \frac{n^2}{|C(\Delta_2)|}|M_i|,
\end{aligned}$$

the last inequality following by Lemma 4. Thus

$$\begin{aligned}\Pr(E_1) &\leqslant \sum_{i=1}^{r} \frac{1}{|C(\Delta_1)|} \sum_{g_{\Delta_1}\in C(\Delta_1)} \frac{n^2}{|C(\Delta_2)|}\left(\frac{n}{5e}\right)^n e^{c\log n} = \frac{rn^2}{|C(\Delta_2)|}\left(\frac{n}{5e}\right)^n e^{c\log n}\\ &\leqslant \left(\frac{1}{2}+o(1)\right)n^3 \frac{1}{|C(\Delta_2)|}\left(\frac{n}{5e}\right)^n e^{c\log n} = \frac{1}{|C(\Delta_2)|}\left(\frac{n}{5e}\right)^n e^{O(\log n)}.\end{aligned}$$

Now, writing $s = |\Delta_2|$ we have that

$$\left|C(\Delta_2)\right| = (s-1)!(n-s-1)! \geqslant \frac{n-1}{2}!\frac{n-3}{2}! = \left(\frac{n}{2e}\right)^n e^{O(\log n)}$$

by Stirling's formula. Hence

$$\Pr(E_1) \leqslant (2/5)^n e^{O(\log n)} = (2/5)^{n+O(\log n)},$$

as required. □

Lemma 9. $\Pr(E_2) \leqslant 2^{-(4/3)n+o(n)} = o(2^{-n})$.

Proof. When 3 does not divide n, $\Pr(E_2) = 0$ and the lemma follows in this case. So we may assume that $n = 3k$ for some integer k.

Recall Lemma 5, and the terminology introduced below that lemma. Write E_A for the event that $\langle g_{\Delta_1}, g_{\Delta_2}\rangle \leqslant M$ where $M \cong S_k \operatorname{wr} S_3$ and where g_{Δ_2} embeds disrespectfully in M. Similarly, write E_B for the event that $\langle g_{\Delta_1}, g_{\Delta_2}\rangle \leqslant M$ where $M \cong S_k \operatorname{wr} S_3$ and where g_{Δ_1} embeds disrespectfully in M. Finally, write E_C for the event that $\langle g_{\Delta_1}, g_{\Delta_2}\rangle \leqslant M$ where $M \cong S_k \operatorname{wr} S_3$ and where both g_{Δ_1} and g_{Δ_2} embed respectfully in M. Clearly $E_2 = E_A \cup E_B \cup E_C$, and so

$$\Pr(E_2) \leqslant \Pr(E_A) + \Pr(E_B) + \Pr(E_C). \tag{3}$$

We begin by providing an upper bound on $\Pr(E_A)$. We write $[S_k \operatorname{wr} S_3]$ for the set of maximal subgroups of S_n that are conjugate to $S_k \operatorname{wr} S_3$. For a subgroup $H \in [S_k \operatorname{wr} S_3]$ and a subset $\Delta \subseteq \Omega$, we write $d_\Delta(H)$ for the set of elements of $C(\Delta)$ that embed disrespectfully in H,

$$\begin{aligned}\Pr(E_A) &\leqslant \sum_{H\in[S_k \operatorname{wr} S_3]} \Pr\bigl(g_{\Delta_1} \in H \text{ and } g_{\Delta_2} \in d_{\Delta_2}(H)\bigr)\\ &= \sum_{H\in[S_k \operatorname{wr} S_3]} \frac{1}{|C(\Delta_1)|} \sum_{g_{\Delta_1}\in C(\Delta_1)} \Pr\bigl(g_{\Delta_1} \in H \text{ and } g_{\Delta_2} \in d_{\Delta_2}(H)\bigr)\\ &= \sum_{H\in[S_k \operatorname{wr} S_3]} \frac{1}{|C(\Delta_1)|} \sum_{g\in C(\Delta_1)\cap H} \Pr\bigl(g_{\Delta_2} \in d_{\Delta_2}(H)\bigr)\\ &\leqslant \frac{1}{|C(\Delta_1)|} \sum_{g\in C(\Delta_1)} \sum_{g\in H\in[S_k \operatorname{wr} S_3]} \max_{H\in[S_k \operatorname{wr} S_3]} \Pr\bigl(g_{\Delta_2} \in d_{\Delta_2}(H)\bigr)\\ &\leqslant n^2 \max_{H\in[S_k \operatorname{wr} S_3]} \Pr\bigl(g_{\Delta_2} \in d_{\Delta_2}(H)\bigr),\end{aligned}$$

the last inequality following by Lemma 4.

Let $H \in [S_k \operatorname{wr} S_3]$ be fixed, and let B_1, B_2, B_3 be the blocks of imprimitivity under the action of H on Ω. If $|\Delta_2 \cap B_i|$ depends on i, then g_{Δ_2} cannot act disrespectfully and so $\Pr(g_{\Delta_2} \in d_{\Delta_2}(H)) = 0$. So we may assume that there exists an integer x such that $|\Delta_2 \cap B_i| = x$ for all i. In this case there are $2(k-x)!^2(k-x-1)!x!^2(x-1)!$ elements of $C(\Delta_2)$ that act disrespectfully (where we use the convention that $(-1)! = 1$). Moreover, $|\Delta_2| = 3x$ and so $|C(\Delta_2)| = (3x-1)!(3k-3x-1)!$. Hence Stirling's formula shows that

$$\Pr\bigl(g_{\Delta_2} \in d_{\Delta_2}(H)\bigr) = \frac{2((k-x))!^2(k-x-1)!x!^2(x-1)!}{(3x-1)!(3k-3x-1)!} = \frac{(\frac{k-x}{e})^{3k-3x}(\frac{x}{e})^{3x}}{(\frac{3x}{e})^{3x}(\frac{3k-3x}{e})^{3k-3x}} e^{O(\log n)}$$
$$= 3^{-n} e^{O(\log n)} = o\bigl(2^{-(4/3)n}\bigr).$$

Hence $\max_{H\in[S_k \operatorname{wr} S_3]} \Pr(g_{\Delta_2} \in d_{\Delta_2}(H)) = o(2^{-(4/3)n})$ and so we find that $\Pr(E_A) = o(2^{-(4/3)n})$, as required.

A similar argument with the roles of Δ_1 and Δ_2 reversed shows that $\Pr(E_B) = o(2^{-(4/3)n})$.

Finally, we estimate $\Pr(E_C)$. Suppose that $\Pr(E_C) > 0$, and so there are choices for g_{Δ_1} and g_{Δ_2} that lie in a subgroup $H \in [S_k \operatorname{wr} S_3]$ and act respectfully. Note that an n-cycle cannot act respectfully, and so Δ_1 and Δ_2 are non-empty. Now Δ_1 is a union of blocks, and so $|\Delta_1| = n/3$ and Δ_1 is a block. Similarly, $|\Delta_2| = n/3$ and Δ_2 is a block. Since Δ_1 and Δ_2 are distinct blocks, they are disjoint. So the blocks of imprimitivity of H are determined: they are Δ_1, Δ_2 and the complement $\overline{\Delta_1 \cup \Delta_2}$ of $\Delta_1 \cup \Delta_2$ in Ω. In particular, H is determined by Δ_1 and Δ_2. Writing $r_\Delta(H)$ for the number of elements of $C(\Delta) \cap H$ that act respectfully, we find that

$$\Pr(E_C) = \Pr(g_{\Delta_1} \in H, g_{\Delta_2} \in H) = \frac{r_{\Delta_1}(H) r_{\Delta_2}(H)}{|C(\Delta_1)||C(\Delta_2)|} = \left(\frac{(n/3)!^3/(n/3)^2}{((n/3)-1)!((2n/3)-1)!}\right)^2$$
$$= \left(\frac{(\frac{n}{3e})^n}{(\frac{n}{3e})^{n/3}(\frac{2n}{3e})^{2n/3}}\right)^2 e^{O(\log n)} = 2^{-(4/3)n+O(\log n)}$$

by Stirling's formula. The lemma now follows by our bounds on $\Pr(E_A)$, $\Pr(E_B)$ and $\Pr(E_C)$ together with the inequality (3). □

We observed above that Theorem 1 follows once we have established the inequality (2). But this inequality follows from Lemmas 7, 8 and 9, and so we have proved Theorem 1.

5. The proof of Theorem 2

Let n be an even integer, and suppose 4 does not divide n. Let $\Omega = \{1, 2, \ldots, n\}$. Define collections I_1, I_2 and I of subsets of Ω by

$$I_1 = \bigl\{\Delta \subseteq \Omega\colon\ |\Delta| \text{ is odd and } |\Delta| < n/2\bigr\},$$
$$I_2 = \bigl\{\Delta \subseteq \Omega\colon\ |\Delta| = n/2 \text{ and } 1 \in \Delta\bigr\},$$
$$I = I_1 \cup I_2.$$

Note that

$$|I| = \binom{n}{1} + \binom{n}{3} + \cdots + \binom{n}{(n/2)-2} + \frac{1}{2}\binom{n}{n/2} = 2^{n-2}.$$

For $\Delta \in I_1$, define $M_\Delta = (S_\Delta \times S_{\overline{\Delta}}) \cap A_n$. For $\Delta \in I_2$, define M_Δ to be the subgroup of A_n that preserves the partition $\Delta, \overline{\Delta}$ of Ω. (So $M_\Delta \cong (S_{n/2} \operatorname{wr} S_2) \cap A_n$ in this case.) As Maróti [10] observes, it is not difficult to show that A_n is covered by the subgroups M_Δ where $\Delta \in I$. Hence $\mu(A_n) \leqslant \sigma(A_n) \leqslant |I| = 2^{n-2}$.

In order to prove Theorem 2 it suffices to show that whenever n is sufficiently large there exists a set X of cardinality 2^{n-2} that generates A_n pairwise. Our strategy is to choose elements $g_\Delta \in$

$C(\Delta)$ where $\Delta \in I$ uniformly and independently at random, and set $X = \{g_\Delta\colon\ \Delta \in I\}$. (Note that $C(\Delta) \subseteq A_n$ for any $\Delta \in I$, since n is even and Δ is non-empty.) We need to prove that the probability that X generates A_n pairwise is non-zero whenever n is sufficiently large. Let E_{Δ_1,Δ_2} be the event that $\langle g_{\Delta_1}, g_{\Delta_2}\rangle$ is a proper subgroup of A_n. By using the Local lemma (Lemma 6) just as in the proof of Theorem 1 we find that it is sufficient to prove that $\Pr(E_{\Delta_1,\Delta_2}) = o(2^{-n})$ for any distinct $\Delta_1, \Delta_2 \in I$. To prove this bound we use the following analogue of Theorem 3.

Theorem 10. *There exists a constant c with the property that for any positive integer n with* $n \equiv 2 \bmod 4$ *and any maximal subgroup M of* A_n *one of the following statements holds*:

(i) *There exist positive integers k and ℓ with* $k + \ell = n$ *and* $k < n/2$ *such that* $M \cong (S_k \times S_\ell) \cap A_n$ *(in its natural intransitive action).*
(ii) $M \cong (S_{n/2} \operatorname{wr} S_2) \cap A_n$ *(in its imprimitive action).*
(iii) $M \cong (S_{n/3} \operatorname{wr} S_3) \cap A_n$ *(in its imprimitive action).*
(iv) $|M| \leqslant (\frac{n}{5e})^n e^{c \log n}$.

Given the fact [5, Section 4.6] that the maximal subgroups of A_n are all of the form $M \cap A_n$ where M is a maximal subgroup of S_n, it is easy to prove Theorem 10 (and the proof is similar to the proof of Theorem 3). Note that we may assume that $k < n/2$ in case (i) of the theorem, since $(S_{n/2} \times S_{n/2}) \cap A_n \leqslant (S_{n/2} \operatorname{wr} S_2) \cap A_n$. Also note that the theorem depends on the fact that 4 does not divide n, since subgroups of the form $(S_{n/4} \operatorname{wr} S_4) \cap A_n$ do not fall under any of the cases (i) to (iv) of the theorem.

Let $\Delta_1, \Delta_2 \in I$ be distinct. Suppose that $\langle g_{\Delta_1}, g_{\Delta_2}\rangle \leqslant M$ for some maximal subgroup M of A_n. Since $\Delta_1 \neq \Delta_2$ and $\Delta_1 \neq \overline{\Delta_2}$, we find that g_{Δ_1} and g_{Δ_2} always generate a transitive subgroup of A_n, and so M never falls under case (i) of Theorem 10. An element of $C(\Delta)$ where $\Delta \in I$ is contained in at most one maximal subgroup isomorphic to $(S_{n/2} \operatorname{wr} S_2) \cap A_n$, by Lemma 5. Indeed, if $\Delta \in I_1$ then no element of $C(\Delta)$ is contained in a subgroup of this type and if $\Delta \in I_2$ then it is contained in only one such subgroup, namely the subgroup that preserves the partition with parts Δ and $\overline{\Delta}$. (We are using the fact that $n \equiv 2 \bmod 4$ here, since when $n \equiv 0 \bmod 4$ any element of $C(\Delta)$ with $\Delta \in I_2$ is contained in three subgroups of the form $(S_{n/2} \operatorname{wr} S_2) \cap A_n$.) Since Δ_1 and Δ_2 are distinct, this shows that M can never fall under case (ii) of Theorem 10. Thus, just as in the proof of Theorem 1, we find that

$$\Pr(E_{\Delta_1,\Delta_2}) \leqslant \Pr(E_1) + \Pr(E_2),$$

where E_1 is the event that $\langle g_{\Delta_1}, g_{\Delta_2}\rangle \leqslant M$ for a maximal subgroup M such that $|M| \leqslant (\frac{n}{5e})^n e^{c \log n}$, and where E_2 is the event that $\langle g_{\Delta_1}, g_{\Delta_2}\rangle \leqslant M$ for a maximal subgroup M that is isomorphic to $(S_{n/3} \operatorname{wr} S_3) \cap A_n$. The proofs that $\Pr(E_1) = o(2^{-n})$ and that $\Pr(E_2) = o(2^{-n})$ are essentially the same as the proofs of Lemmas 8 and 9, respectively, and so we omit the details; it is easy to see that the two results that are used in Lemma 8 (namely Lemma 4 and the result of Liebeck and Shalev on the number of conjugacy classes of maximal subgroups of S_n) are also true for alternating groups. Thus $\Pr(E_{\Delta_1,\Delta_2}) \leqslant \Pr(E_1) + \Pr(E_2) = o(2^{-n})$ and so Theorem 2 follows. □

Acknowledgments

The author is grateful to Martin Liebeck for pointing out a reference for a result used in an earlier version of this paper, and thanks Cheryl Praeger and Peter Neumann for their encouragement during the early stages of writing the paper and Attila Maróti for comments on a late draft.

References

[1] N. Alon, J. Spencer, The Probabilistic Method, Wiley–Interscience, New York, 1992.
[2] R. Brown, Minimal covers of S_n by abelian subgroups and maximal subsets of pairwise noncommuting elements, J. Combin. Theory Ser. A 49 (1988) 294–307.
[3] R. Brown, Minimal covers of S_n by abelian subgroups and maximal subsets of pairwise noncommuting elements. II, J. Combin. Theory Ser. A 56 (1991) 285–289.
[4] M. Bruckheimer, A.C. Bryan, A. Muir, Groups which are the union of three subgroups, Amer. Math. Monthly 77 (1970) 52–57.
[5] P.J. Cameron, Permutation Groups, London Math. Soc. Stud. Texts, vol. 45, Cambridge Univ. Press, Cambridge, UK, 1999.
[6] J.H.E. Cohn, On n-sum groups, Math. Scand. 75 (1994) 44–58.
[7] P. Erdős, L. Lovász, Problems and results on 3-chromatic hypergraphs and some related questions, in: A. Hajnal, R. Rado, V. Sós (Eds.), Colloquium Math. Society Janos Bolyai, vol. 11, North-Holland, Amsterdam, 1973, pp. 609–627.
[8] S. Haber, A. Rosenfeld, Groups as unions of proper subgroups, Amer. Math. Monthly 66 (1959) 491–494.
[9] M.W. Liebeck, A. Shalev, Maximal subgroups of symmetric groups, J. Combin. Theory Ser. A 75 (1996) 341–352.
[10] A. Maróti, Covering the symmetric groups with proper subgroups, J. Combin. Theory Ser. A 110 (2005) 97–111.
[11] C.E. Praeger, J. Saxl, On the orders of primitive permutation groups, Bull. London Math. Soc. 37 (1980) 303–307.
[12] L. Pyber, How abelian is a finite group?, in: The Mathematics of Paul Erdős, I, in: Algorithms Combin., vol. 13, Springer-Verlag, Berlin, 1997, pp. 372–384.
[13] G. Scorza, I gruppi che possono pensarsi come somma di tre loro sottogruppi, Boll. Unione Mat. Ital. 5 (1926) 216–218.
[14] J.B. Shearer, On a problem of Spencer, Combinatorica 5 (1985) 241–245.
[15] E.T. Whittaker, G.N. Watson, A Course of Modern Analysis, fourth ed., Cambridge Univ. Press, Cambridge, UK, 1963.