ON THE MAXIMAL NUMBER OF ELEMENTS PAIRWISE GENERATING THE SYMMETRIC GROUP OF EVEN DEGREE

FRANCESCO FUMAGALLI, MARTINO GARONZI, AND ATTILA MARÓTI

Abstract. Let G be the symmetric group of degree n. Let $\omega(G)$ be the maximal size of a subset S of G such that $\langle x, y\rangle = G$ whenever $x, y \in S$ and $x \neq y$ and let $\sigma(G)$ be the minimal size of a family of proper subgroups of G whose union is G. We prove that both functions $\sigma(G)$ and $\omega(G)$ are asymptotically equal to $\frac{1}{2}\binom{n}{n/2}$ when n is even. This, together with a result of S. Blackburn, implies that $\sigma(G)/\omega(G)$ tends to 1 as $n \to \infty$. Moreover, we give a lower bound of $n/5$ on $\omega(G)$ which is independent of the classification of finite simple groups. We also calculate, for large enough n, the clique number of the graph defined as follows: the vertices are the elements of G and two vertices x, y are connected by an edge if $\langle x, y\rangle \geq A_n$.

To the memory of Carlo Casolo.

1. Introduction

Let G be a noncyclic finite group. J.H.E. Cohn in [5] defined $\sigma(G)$ to be the minimal number k such that G is the union of k proper subgroups of G. This invariant has been studied by many authors. In particular, M.J. Tomkinson [17] proved that if G is solvable then $\sigma(G) = q+1$, where q is the smallest order of a chief factor of G with more than one complement. In the present work we concentrate on the symmetric group S_n of degree n. In two papers [12, 8] it was shown that $\sigma(S_n) = 2^{n-1}$ for every odd integer $n \geq 3$. The determination of $\sigma(S_n)$ when n is even seems a more difficult task. In case n is divisible by 6, E. Swartz [16] managed to give a formula for $\sigma(S_n)$. Apart from this case, the value of $\sigma(S_n)$ for n even is only known for $n \leq 14$: see [2, 8, 14].

Let G be a finite group which can be generated by 2 elements. A subset S of G is called a pairwise generating set if every subset of S of size 2 generates G. The maximal size of a pairwise generating set for G is denoted by $\omega(G)$. This invariant was first introduced by M.W. Liebeck and A. Shalev in [10], where a general lower bound for $\omega(G)$ was given for G a nonabelian finite simple group:

2010 *Mathematics Subject Classification.* Primary 20B15, 20B30; Secondary 20B40, 20D60, 05D40.

Key words and phrases. Symmetric group, Lovász Local Lemma, group generation, covering.

The second author acknowledges the support of Fundação de Apoio à Pesquisa do Distrito Federal (FAPDF) - demanda espontânea 03/2016, and of Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) - Grant numbers 302134/2018-2, 422202/2018-5. The work of the third author on the project leading to this application has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 741420). He was also supported by the National Research, Development and Innovation Office (NKFIH) Grant No. K132951, Grant No. K115799, Grant No. K138828.

they proved that $\omega(G) \geq c \cdot m(G)$ where c is an absolute positive constant and $m(G)$ denotes the minimal index of a proper subgroup of G. After some initial results in [12], S.R. Blackburn [3] proved that $\omega(S_n) = 2^{n-1}$ provided that n is odd and sufficiently large. Later, in her Ph.D thesis, L. Stringer [15] studied the small odd values of n and showed that $\omega(S_n) = 2^{n-1}$ for every odd integer n at least 17 or belonging to $\{7, 11, 13\}$. Moreover, she showed that $\omega(S_5) < \sigma(S_5)$ and that $\omega(S_9) < \sigma(S_9)$ (see also [8]); the problem of whether $\omega(S_{15}) = \sigma(S_{15})$ or not is still open.

An obvious connection between $\sigma(G)$ and $\omega(G)$ for any noncyclic finite group G is that $\omega(G) \leq \sigma(G)$. Indeed, every proper subgroup of G contains at most one element of any pairwise generating set for G.

Our first result is the following.

Theorem 1. *If n is even then $\sigma(S_n)$ and $\omega(S_n)$ are asymptotically equal to $\frac{1}{2}\binom{n}{n/2}$.*

This, together with S. Blackburn's result mentioned above, implies that the quotient $\sigma(S_n)/\omega(S_n)$ tends to 1 as n tends to infinity, without restrictions on the parity of n.

The idea of the proof of Theorem 1 is to show that there exists a set of pairwise generating elements of S_n, consisting of n-cycles, one in each imprimitive maximal subgroup of S_n with two blocks of imprimitivity. This gives the lower bound in the following chain of inequalities.

$$\frac{1}{2}\binom{n}{n/2} \leq \omega(S_n) \leq \sigma(S_n) \leq \frac{1}{2}\binom{n}{n/2} + \sum_{i=1}^{\lfloor n/3 \rfloor} \binom{n}{i}.$$

The upper bound is obtained noting that S_n is covered by the imprimitive maximal subgroups with 2 blocks and the intransitive maximal subgroups stabilizing sets of size at most $\lfloor n/3 \rfloor$. The result then follows by letting $n \to \infty$.

Let Γ_n be the graph whose vertices are the elements of S_n which are products of exactly three disjoint cycles and there is an edge between two of them if they generate a transitive subgroup of S_n. The main combinatorial obstacle to determine $\omega(S_n)$ and/or $\sigma(S_n)$ is to determine the clique number of Γ_n.

Our proof of Theorem 1 makes use of results about maximal primitive subgroups of S_n (see Lemma 5) that rely on the Classification of Finite Simple Groups (CFSG). However [3] also depends on CFSG.

We remark that, apart from some symmetric groups, the only cases in which the precise value of ω is known are for groups of Fitting height at most 2 [11], for certain alternating groups [3] and for certain linear groups [4].

If we allow the pairs of elements of S_n to generate S_n or A_n (and n is even), then we are able to determine the precise size of certain subsets as in our second theorem.

Theorem 2. *If n is a large enough even integer, then the maximal size of a subset X of S_n with the property that $\langle x, y \rangle \geq A_n$ whenever x, y are two distinct elements of X is $\frac{1}{2}\binom{n}{n/2} + 2^{n-2}$ if $n/2$ is even and 2^{n-2} if $n/2$ is odd.*

At the heart of the proof of Theorems 1 and 2 is the Lovász Local Lemma [7]. In this context, the Local Lemma was first used by S.R. Blackburn [3] and elaborated on by L. Stringer [15] in her Ph.D thesis.

Our last result does not depend on CFSG via a nice theorem of Eberhard and Virchow [6].

Proposition 1. *Both $\omega(S_n)$ and $\omega(A_n)$ are at least $(1-o(1))n$.*

2. The local lemma

Given an event E of a probability space, we denote by $P(E)$ its probability and by $\overline{E}$ its complement. As usual e denotes the base of the natural logarithm.

The following crucial result can be found in [7]. The formulation we use is taken from [1, Corollary 5.1.2] (the "symmetric case").

Theorem 3 (Lovász Local Lemma)**.** *Let $A_1, \dots, A_n$ be events in an arbitrary probability space. Let (V, E) be a directed graph, where $V = \{1, \dots, n\}$, and assume that, for every $i \in V$, the event A_i is mutually independent of the set of events A_j such that $(i,j) \notin E$. Let d be the maximum valency of a vertex of the graph (V, E). If for every $i \in V$*

$$P(A_i) \leq \frac{1}{e(d+1)}$$

then $P(\bigcap_{i \in V} \overline{A_i}) > 0$.

The mutual independence condition mentioned in the Lovász Local Lemma means the following:

$$P(A_i \mid \bigcap_{j \in S} \overline{A_j}) = P(A_i) \qquad \forall i \in V, \qquad \forall S \subseteq \{j \in V \ : \ (i,j) \notin E\}.$$

3. Proof of Theorems 1 and 2

From now on let n be a large even integer. Let also $G := S_n$ be the symmetric group on n letters. Let A_n denote the alternating group on n letters. We will prove both theorems using the same argument.

Let $\mathscr{M}^{(1)}$ be the family of maximal imprimitive subgroups of G with 2 blocks and let $\Pi^{(1)}$ be the set of n-cycles in G. Let $\mathscr{M}^{(2)}$ be the family of maximal subgroups of G that are either imprimitive with 2 blocks or intransitive of type $S_a \times S_b$ with a and b odd, $a \neq b$, $a + b = n$, and let $\Pi^{(2)}$ be the set of elements of G that are either n-cycles or elements of cycle type (a, b) with a and b odd, $a \neq b$, $a + b = n$.

Note that

$$|\mathscr{M}^{(1)}| = \frac{1}{2}\binom{n}{n/2}, \qquad |\mathscr{M}^{(2)}| = \begin{cases} \frac{1}{2}\binom{n}{n/2} + 2^{n-2} & \text{if } n/2 \text{ is even,} \\ 2^{n-2} & \text{if } n/2 \text{ is odd.} \end{cases}$$

Moreover $\mathscr{M}^{(2)}$ is a covering of G, meaning that $\bigcup_{M \in \mathscr{M}^{(2)}} M = G$. To see this, note that the elements whose cycle structure consists of cycles all of even length or of exactly two cycles of equal length are covered by the imprimitive maximal subgroups with 2 blocks, while the elements that admit in the cycle decomposition a cycle of odd length less than $n/2$ are covered by some intransitive subgroup of type $S_a \times S_b$ where a, b are odd and $a \neq b$.

Let $\mathscr{S}^{(1)}$ be the set of subsets of $\Omega = \{1, \ldots, n\}$ of size $n/2$ and containing 1. Let $\mathscr{S}^{(2)}$ be the union of $\mathscr{S}^{(1)}$ with the set of subsets of Ω of odd size less than $n/2$. There is a natural bijection $\mathscr{S}^{(i)} \to \mathscr{M}^{(i)}$, $\Delta \mapsto M_\Delta$ for $i = 1, 2$. Specifically, if $|\Delta| = n/2$ then M_Δ is the stabilizer of the partition $\Delta \cup (\Omega - \Delta)$, and if $|\Delta| < n/2$ then M_Δ is the setwise stabilizer of Δ.

Define two graphs $Q^{(1)}$, $Q^{(2)}$, which both have G as set of vertices. There is an edge between x and y in $Q^{(1)}$ if $\langle x, y\rangle = G$, and there is an edge between x and y in $Q^{(2)}$ if $\langle x, y\rangle \geq A_n$. Note that if $\{x, y\}$ is an edge of $Q^{(i)}$, then x and y do not belong to the same member of $\mathscr{M}^{(i)}$. Since $\mathscr{M}^{(2)}$ is a covering of G, this proves that the clique number of $Q^{(2)}$ is at most $|\mathscr{M}^{(2)}|$. The third author observed in [12] that $\sigma(G) \leq |\mathscr{M}^{(1)}| + \sum_{i=1}^{q} \binom{n}{i}$, where $q := \lfloor n/3 \rfloor$, and this upper bound is asymptotically equal to $|\mathscr{M}^{(1)}|$.

We are left to prove that $|\mathscr{M}^{(i)}| \leq \omega(Q^{(i)})$ for $i = 1, 2$, where $\omega(Q^{(i)})$ denotes the clique number of $Q^{(i)}$, that is, the maximal number of vertices in a complete subgraph of $Q^{(i)}$.

For every $i \in \{1, 2\}$ and for every $\Delta \in \mathscr{S}^{(i)}$ let

$$C(\Delta) := M_\Delta \cap \Pi^{(i)}.$$

Choose, uniformly and independently, an element g_Δ in each $C(\Delta)$, $\Delta \in \mathscr{S}^{(i)}$.

Note that the sets $C(\Delta)$ are pairwise disjoint. If $\Delta \in \mathscr{S}^{(1)}$ then a simple counting argument shows that $|C(\Delta)| = (2/n)(n/2)!^2$. If $\Delta \in \mathscr{S}^{(2)} - \mathscr{S}^{(1)}$ then $|C(\Delta)| = (|\Delta| - 1)!(n - |\Delta| - 1)!$. In particular, we always have

$$|C(\Delta)| \geq (2/n)^2 (n/2)!^2. \tag{1}$$

We define a graph $\Gamma^{(i)}$ for $i = 1, 2$. The vertices are the two element subsets of $\mathscr{S}^{(i)}$. Two distinct vertices v, v' are connected by an edge if and only if $v \cap v' \neq \varnothing$. The valency of every vertex of $\Gamma^{(i)}$ is $2(|\mathscr{S}^{(i)}| - 2) \leq 2^{n+1}$. For every vertex $v = \{\Delta_1, \Delta_2\}$ of $\Gamma^{(i)}$ define E_v to be the event "$\langle g_{\Delta_1}, g_{\Delta_2}\rangle \neq G$" if $i = 1$, and "$\langle g_{\Delta_1}, g_{\Delta_2}\rangle \not\geq A_n$" if $i = 2$.

We will apply Theorem 3 in the case of the graph $\Gamma^{(i)}$ defined above.

Given a vertex v of $\Gamma^{(i)}$, let A be the set of vertices w of $\Gamma^{(i)}$ with the property that $v \cap w = \varnothing$. The condition that E_v is independent of the set of events $\{E_w\}_{w \in A}$, mentioned in Theorem 3, means that

$$P\Big(E_v \cap \bigcap_{w \in A'} \overline{E_w}\Big) = P(E_v) \cdot P\Big(\bigcap_{w \in A'} \overline{E_w}\Big),$$

for every subset A' of A. But this is clear since $v \cap (\bigcup_{w \in A'} w) = \varnothing$ by the definition of $\Gamma^{(i)}$ and so the choices of g_Δ with $\Delta \in v$ are independent of the choices of g_Δ with $\Delta \in \cup_{w \in A'} w$.

The conclusion of Theorem 3 is that there exists a set $S \subseteq G$ containing precisely one element g_Δ in every $C(\Delta)$, for every $\Delta \in \mathscr{S}^{(i)}$, such that $\langle g_{\Delta_1}, g_{\Delta_2}\rangle = G$ for $i = 1$ and $\langle g_{\Delta_1}, g_{\Delta_2}\rangle \geq A_n$ for $i = 2$, for every $g_{\Delta_1} \neq g_{\Delta_2}$ in S. This would imply that

$$\omega(Q^{(i)}) \geq |S| = |\mathscr{S}^{(i)}| = |\mathscr{M}^{(i)}|$$

for $i \in \{1, 2\}$, which is what we need. Note that the fact that $|S| = |\mathscr{S}^{(i)}|$ follows from the fact that the sets $C(\Delta)$ are pairwise disjoint.

We will repeatedly use Stirling's inequalities.

Lemma 1. *For every positive integer m we have*

$$\sqrt{2\pi m}(m/e)^m \leq m! \leq e\sqrt{m}(m/e)^m.$$

For every $H \leq G$ and $\Delta \in \mathscr{S}^{(i)}$ define

$$f_\Delta(H) := \frac{|C(\Delta) \cap H|}{|C(\Delta)|}.$$

Given $d, m > 1$ such that $n = dm$, denote by $\mathcal{W}_{d,m}$ the class of imprimitive maximal subgroups of G isomorphic to $S_d \wr S_m$, that is, stabilizers of partitions of $\{1, \ldots, n\}$ consisting of m blocks of size d each.

Lemma 2. *Let $\Delta \in \mathscr{S}^{(i)}$ and $W \in \mathcal{W}_{d,m}$.*

(1) *Assume $m = 3$. If $\Delta \in \mathscr{S}^{(1)}$ then $f_\Delta(W) \neq 0$ if and only if the intersection of Δ with each block of W has size $n/6$, in which case*

$$f_\Delta(W) \leq \frac{(n/6)!^6}{(n/2)!^2} \cdot n^{O(1)} \leq (1/3)^n \cdot n^{O(1)}.$$

If $\Delta \in \mathscr{S}^{(2)} - \mathscr{S}^{(1)}$ then $f_\Delta(W) \neq 0$ only if 3 divides $a = |\Delta|$ and the elements of $C(\Delta)$ permute transitively the 3 blocks of W, moreover in this case setting $b = n - a$, we have

$$f_\Delta(W) \leq \frac{(a/3)!^3 \cdot (b/3)!^3}{a! \cdot b!} \cdot n^{O(1)} \leq (1/3)^n \cdot n^{O(1)}.$$

(2) *Assume $m = 4$. If $\Delta \in \mathscr{S}^{(1)}$ then $f_\Delta(W) \neq 0$ if and only if Δ is a union of 2 blocks of W, in which case*

$$f_\Delta(W) \leq \frac{(n/4)!^4}{(n/2)!^2} \cdot n^{O(1)} \leq (1/2)^n \cdot n^{O(1)}.$$

If $\Delta \in \mathscr{S}^{(2)} - \mathscr{S}^{(1)}$ then $f_\Delta(W) \neq 0$ only if $a = |\Delta| = n/4$ and Δ is a block of W, moreover in this case setting $b = n - a = 3n/4$, we have

$$f_\Delta(W) \leq \frac{(b/3)!^3}{b!} \cdot n^{O(1)} \leq (1/3)^{3n/4} \cdot n^{O(1)}.$$

Note that $(1/3)^{3/4} < 1/2$.

Proof. The first inequality in each statement follows from bounding $|C(\Delta) \cap H|$ and $|C(\Delta)|$ separately, recalling that the members of $\mathscr{S}^{(2)} - \mathscr{S}^{(1)}$ have odd size. Let k be any constant positive integer and x a positive integer divisible by k. Using Lemma 1 we deduce that

$$\frac{(x/k)!^k}{x!} \leq \frac{e^k x^{k/2} (x/(ke))^x}{(x/e)^x} = (1/k)^x \cdot e^k \cdot x^{k/2}.$$

The second inequality in each statement of the lemma follows from this observation. This concludes the proof. □

Lemma 3 (Lemma 4 of [3]). *Let n be a positive integer. Let M be a fixed subgroup of G. Let g be a fixed element of G, and suppose that g is an n-cycle, or that g is an $(s, n - s)$-cycle for some integer s such that $1 \leq s \leq n/2$. Then g is contained in at most n^2 conjugates of M in G.*

The following lemma is a consequence of [3, Theorem 3].

Lemma 4. *Let $d \geq 2$, $m \geq 5$ be integers such that $n = dm$. Then*

$$|S_d \wr S_m| = d!^m m! \leq (n/5e)^n \cdot n^{O(1)}.$$

From now on i will be 1 or 2.

Let $\mathscr{H}^{(i)}$ be the family of all maximal subgroups of G outside $\mathscr{M}^{(i)}$. Write $\mathscr{H}^{(i)} = \bigcup_{j=1}^{5} \mathscr{H}_j$ where $\mathscr{H}_1$ is the family of intransitive maximal subgroups of G outside $\mathscr{M}^{(i)}$, $\mathscr{H}_2$ is the family of primitive maximal subgroups of G, $\mathscr{H}_j$ is the family of imprimitive maximal subgroups of G with j blocks for $j \in \{3,4\}$ and $\mathscr{H}_5$ is the family of imprimitive maximal subgroups of G with at least 5 blocks. Let $J := \{1,2,3,4,5\}$. For $j \in J$ and $v = \{\Delta_1, \Delta_2\} \in V(\Gamma^{(i)})$, let E_v^j be the event "$g_{\Delta_1}, g_{\Delta_2}$ both belong to some $H \in \mathscr{H}_j$", so that $P(E_v) \leq \sum_{j \in J} P(E_v^j)$.

We will prove that

$$\sum_{j \in J} P(E_v^j) \leq \frac{1}{2^{n+3}},$$

which for sufficiently large n is smaller than $\frac{1}{e(d+1)}$.

Let $[H]$ denote the G-conjugacy class of a subgroup H of G. Let $m_\Delta([H])$ be the number of different conjugates of H that contain a fixed element of $C(\Delta)$. By Lemma 3, $m_\Delta([H]) \leq n^2$ always.

If $H \in \mathscr{M}^{(i)}$ then at least one of $f_{\Delta_1}(H)$ and $f_{\Delta_2}(H)$ is 0 for $\Delta_1 \neq \Delta_2$. Therefore in the computation of $P(E_v)$ we restrict our attention to the maximal subgroups of G outside $\mathscr{M}^{(i)}$.

In the following sum we let $[H]$ vary in the set of conjugacy classes of elements of $\mathscr{H}_j$ with $j \in J$. We have

$$\begin{aligned}
P(E_v^j) &\leq \sum_{[H]} \sum_{K \in [H]} f_{\Delta_1}(K) \cdot f_{\Delta_2}(K) \\
&= \sum_{[H]} \sum_{K \in [H]} \frac{|C(\Delta_1) \cap K|}{|C(\Delta_1)|} f_{\Delta_2}(K) \\
&= \sum_{[H]} \sum_{K \in [H]} \sum_{g \in C(\Delta_1) \cap K} \frac{1}{|C(\Delta_1)|} f_{\Delta_2}(K) \\
&= \sum_{[H]} \sum_{g \in C(\Delta_1)} \frac{1}{|C(\Delta_1)|} \sum_{\substack{K \in [H] \\ g \in K}} f_{\Delta_2}(K) \\
&\leq \sum_{[H]} \sum_{g \in C(\Delta_1)} \frac{1}{|C(\Delta_1)|} \cdot m_{\Delta_1}([H]) \cdot \max_{K \in [H]} f_{\Delta_2}(K) \\
&= \sum_{[H]} m_{\Delta_1}([H]) \cdot \max_{K \in [H]} f_{\Delta_2}(K).
\end{aligned}$$

For $v = \{\Delta_1, \Delta_2\}$ let $c_{v,j}$ be the number of conjugacy classes of subgroups in $\mathscr{H}_j$ such that there exists H in such a class such that $H \cap C(\Delta_1) \neq \varnothing$ and

$H \cap C(\Delta_2) \neq \varnothing$. We deduce that

$$P(E_v^j) \leq c_{v,j} \cdot \min_{\{i_1,i_2\}=\{1,2\}} \left(\max_{\substack{H \in \mathscr{H}_j \\ K \in [H]}} \left(m_{\Delta_{i_1}}([H]) \cdot f_{\Delta_{i_2}}(K) \right) \right). \tag{2}$$

For $v = \{\Delta_1, \Delta_2\}$ denote by $s_{v,j}$ the number of members of $\mathscr{H}_j$ intersecting both $C(\Delta_1)$ and $C(\Delta_2)$ non-trivially. Then

$$P(E_v^j) \leq \sum_{H \in \mathscr{H}_j} f_{\Delta_1}(H) \cdot f_{\Delta_2}(H) \leq s_{v,j} \cdot \max_{H \in \mathscr{H}_j} \left(f_{\Delta_1}(H) \cdot f_{\Delta_2}(H) \right). \tag{3}$$

We will use inequality (2) if $j \neq 4$ or $(|\Delta_1|, |\Delta_2|) \neq (n/2, n/2)$ and we will use inequality (3) if $j = 4$ and $(|\Delta_1|, |\Delta_2|) = (n/2, n/2)$.

Lemma 5. *Let $v = \{\Delta_1, \Delta_2\}$ be a vertex of $\Gamma^{(i)}$ and let $j \in J$. Then $c_{v,2} \leq n$ (for n large enough) and $c_{v,j} \leq 1$ for $j \in \{3, 4\}$. Moreover $c_{v,5} \leq 2\sqrt{n}$. If $(|\Delta_1|, |\Delta_2|) = (n/2, n/2)$ then $s_{v,4} \leq 1$.*

Proof. By [9], $c_{v,2} \leq n$ for n large enough. We remark that this is the only point where we use CFSG. $c_{v,5}$ is at most the number of positive divisors of n less than n, and this is at most $2\sqrt{n}$. If $j \in \{3, 4\}$, then $\mathscr{H}_j$ is a single conjugacy class of subgroups of G, therefore $c_{v,j} \leq 1$.

Assume now that $(|\Delta_1|, |\Delta_2|) = (n/2, n/2)$, so that both $C(\Delta_1)$ and $C(\Delta_2)$ consist of n-cycles. We will prove that $s_{v,4} \leq 1$. Let H be an imprimitive maximal subgroup of G isomorphic to $S_{n/4} \wr S_4$. The two sets $H \cap C(\Delta_1)$ and $H \cap C(\Delta_2)$ are both non-empty only if the four imprimitivity blocks of H are exactly: $\Delta_1 \cap \Delta_2$, $\Delta_1 - \Delta_2$, $\Delta_2 - \Delta_1$ and $\Omega - (\Delta_1 \cup \Delta_2)$, in which case $|\Delta_1 \cap \Delta_2| = n/4$. This implies the result. □

We will bound each $P(E_v^j)$. Note that $P(E_v^1) = 0$ in all cases, since no intransitive subgroup contains n-cycles and the only intransitive maximal subgroups containing elements of cycle type (a, b) with a, b odd are the ones belonging to $\mathscr{M}^{(2)}$.

(i) $j = 2$. By a result of Praeger and Saxl [13], the order of any member of $\mathscr{H}_2$ is at most 4^n. By Lemmas 3, 5, inequalities (1) and (2),

$$P(E_v^2) \leq n^3 \cdot \max_{\substack{H \in \mathscr{H}_2 \\ K \in [H]}} f_{\Delta_2}(K) \leq n^3 \cdot \frac{4^n}{(2/n)^2 (n/2)!^2}.$$

(ii) $j = 3$. By Lemmas 2, 3, 5 and inequality (2),

$$P(E_v^3) \leq n^2 \cdot \max_{\substack{H \in \mathscr{H}_3 \\ K \in [H]}} f_{\Delta_2}(K) \leq (1/3)^n \cdot n^{O(1)}.$$

(iii) $j = 4$. If $(|\Delta_1|, |\Delta_2|) \neq (n/2, n/2)$ then, without loss of generality, we may assume $|\Delta_2| \neq n/2$. In this case, by Lemmas 2, 3, 5 and inequality (2),

$$P(E_v^4) \leq n^2 \cdot \max_{\substack{H \in \mathscr{H}_4 \\ K \in [H]}} f_{\Delta_2}(K) \leq (1/3)^{3n/4} \cdot n^{O(1)}.$$

Assume now that $(|\Delta_1|, |\Delta_2|) = (n/2, n/2)$. Since $s_{v,4} \leq 1$ by Lemma 5, we have

$$P(E_v^4) \leq \max_{H \in \mathscr{H}_4} (f_{\Delta_1}(H) \cdot f_{\Delta_2}(H)) \leq (1/4)^n \cdot n^{O(1)},$$

by inequality (3) and Lemma 2.

(iv) $j = 5$. Fix $H \in \mathscr{H}_5$. Then, by Lemma 4, inequality (1) and Lemma 1,

$$f_\Delta(H) \leq \frac{|H|}{|C(\Delta)|} \leq \frac{(n/5e)^n \cdot n^{O(1)}}{(n/2)!^2} \leq \frac{(n/5e)^n \cdot n^{O(1)}}{(n/2e)^n} = (2/5)^n \cdot n^{O(1)}.$$

The set $\mathscr{H}_5$ contains at most $2\sqrt{n}$ classes of subgroups. For every $H \in \mathscr{H}_5$, we have $m_{\Delta_1}([H]) \leq n^2$ by Lemma 3, hence

$$P(E_v^5) \leq 2\sqrt{n} \cdot n^2 \cdot \max_{\substack{H \in \mathscr{H}_5 \\ K \in [H]}} f_{\Delta_2}(K) \leq (2/5)^n \cdot n^{O(1)},$$

by inequality (2).

Combining everything, we deduce that

$$P(E_v) \leq \sum_{j \in J} P(E_v^j) \leq (1/3)^{3n/4} \cdot n^{O(1)},$$

which is smaller than 2^{-n-3} for every large enough n.

4. Proof of Proposition 1

Eberhard and Virchow [6, Theorem 1.1] proved, without CFSG, that for every $\epsilon > 0$ the probability $p(n)$ that a random pair of elements from S_n generates S_n or A_n is

$$1 - \frac{1}{n} + \Theta(n^{-2+\epsilon}),$$

for every sufficiently large n. The same asymptotic formula holds [6, Theorem 1.2] for the probability $a(n)$ that a random pair of elements from A_n generates A_n. Let $b(n)$ be the probability that a random pair of elements from $S_n \setminus A_n$ generates S_n. Let $c(n)$ be the probability that a random element from A_n and a random element from $S_n \setminus A_n$ generate S_n. Observe that $b(n) = c(n)$ since $\langle x, y\rangle = \langle xy^{-1}, y\rangle$ where x and y are in $S_n \setminus A_n$. Since

$$p(n) = \frac{a(n) + b(n) + 2c(n)}{4},$$

it follows that $b(n) = (4p(n) - a(n))/3$. Fix $\epsilon > 0$. We have universal positive constants c_1 and c_2 by [6] such that $1 - n^{-1} - c_1 n^{-2+\epsilon}$ is smaller than both $p(n)$ and $a(n)$ and $a(n) < 1 - n^{-1} + c_2 n^{-2+\epsilon}$. Thus $1 - n^{-1} - (1/3)(4c_1 + c_2)n^{-2+\epsilon} < b(n)$.

Following Liebeck and Shalev [10], define graphs $A(n)$ and $B(n)$ with vertex sets A_n and $S_n \setminus A_n$ respectively such that there is an edge between vertices x and y if and only if x and y generate A_n in the first case and S_n in the second case. The largest size of a complete subgraph in $A(n)$ is $\omega(A_n)$ and the largest size of a complete subgraph in $B(n)$ is at most $\omega(S_n)$.

Turán's [18] theorem states that a simple graph on m vertices which does not contain a complete subgraph of size $r+1$ has at most $(1 - \frac{1}{r})\frac{m^2}{2}$ edges. We apply this theorem to the graphs $A(n)$ and $B(n)$ with $m = n!/2$ vertices. Consider the graph $A(n)$. (The argument for the case of $B(n)$ is the same.) Let $r := \omega(A_n)$. Since A_n is not a cyclic group, observe that $A(n)$ has more than $(1 - \frac{1}{n} - c_1 n^{-2+\epsilon})\frac{m^2}{2}$ edges. It follows that

$$\left(1 - \frac{1}{n} - c_1 n^{-2+\epsilon}\right)\frac{m^2}{2} < \left(1 - \frac{1}{r}\right)\frac{m^2}{2},$$

giving $r > n - c_1 n^\epsilon = (1 - o(1))n$.

5. Acknowledgements

We would like to thank the referees for helpful comments, in particular, for improving the statement and proof of Proposition 1.

References

[1] N. Alon, J. H. Spencer. The probabilistic method. Fourth edition. *Wiley Series in Discrete Mathematics and Optimization.* John Wiley and Sons, Inc., Hoboken, NJ, 2016.

[2] A. Abdollahi, F. Ashraf, and S. M. Shaker. The symmetric group of degree six can be covered by 13 and no fewer proper subgroups. *Bull. Malays. Math. Sci. Soc. (2)*, 30(1):57–58, 2007.

[3] S. R. Blackburn. Sets of permutations that generate the symmetric group pairwise. *J. Combin. Theory Ser. A* 113 (2006), no. 7, 1572–1581.

[4] J. R. Britnell, A. Evseev, R. M. Guralnick, P. E. Holmes, A. Maróti. Sets of elements that pairwise generate a linear group. *J. Combin. Theory Ser. A* 115 (2008), no. 3, 442–465.

[5] J. H. E. Cohn, On n-sum groups. *Math. Scand.*, 75(1) (1994), 44–58.

[6] S. Eberhard, S.C. Virchow. The probability of generating the symmetric group. ArXiv:1611.02501.

[7] P. Erdős, L. Lovász. Problems and results on 3-chromatic hypergraphs and some related questions, *A. Hajnal, R. Rado, V. Sós (Eds.), Colloquium Math. Society Janos Bolyai, vol. 11, North-Holland, Amsterdam,* 1973, pp. 609–627.

[8] L.-C. Kappe, D. Nikolova-Popova, and E. Swartz. On the covering number of small symmetric groups and some sporadic simple groups. *Groups Complex. Cryptol.* 8(2):135–154, 2016.

[9] M.W. Liebeck, A. Shalev, Maximal subgroups of symmetric groups, *J. Combin. Theory Ser. A* 75 (1996) 341–352.

[10] M.W. Liebeck, A. Shalev. Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky. *J. Algebra* 184 (1996), no. 1, 31–57.

[11] A. Lucchini, A. Maróti. On the clique number of the generating graph of a finite group. *Proc. Amer. Math. Soc.* 137 (2009), no. 10, 3207–3217.

[12] A. Maróti. Covering the symmetric groups with proper subgroups. *J. Combin. Theory Ser. A*, 110(1):97–111, 2005.

[13] C. Praeger, J. Saxl. On the order of primitive permutation groups. *Bull. London Math. Soc.* **12**, (1980), 303–308.

[14] R. Oppenheim and E. Swartz. On the covering number of S_{14}. *Involve*, 12(1):89–96, 2019.

[15] L. Stringer. Pairwise generating sets for the symmetric and alternating groups. PhD thesis. *Royal Holloway, University of London*, 2008.

[16] E. Swartz. On the covering number of symmetric groups having degree divisible by six. *Discrete Math.* 339(11):2593–2604, 2016.

[17] M. J. Tomkinson. Groups as the union of proper subgroups. *Math. Scand.*, Volume 81, Year 1997, Number 2, Pages 191–198.

[18] P. Turán. An extremal problem in graph theory. *Mat. Fiz. Lapok* Vol. 48, 1941, 436–452.

Dipartimento di Matematica e Informatica 'Ulisse Dini', Viale Morgagni 67/A, 50134 Firenze, Italy

Email address: francesco.fumagalli@unifi.it

Departamento de Matemática, Universidade de Brasília, Campus Universitário, Darcy Ribeiro, Brasília-DF, 70910-900, Brazil

Email address: mgaronzi@gmail.com

Alfréd Rényi Institute of Mathematics, Reáltanoda utca 13-15, H-1053, Budapest, Hungary

Email address: maroti.attila@renyi.hu