Open Research Online

The Open University's repository of research publications
and other research outputs

Large minimal invariable generating sets in the finite symmetric groups

Journal Item

oro.open.ac.uk

LARGE MINIMAL INVARIABLE GENERATING SETS IN THE FINITE SYMMETRIC GROUPS

DANIELE GARZONI AND NICK GILL

ABSTRACT. For a finite group G, let $m_I(G)$ denote the largest possible cardinality of a minimal invariable generating set of G. We prove an upper and a lower bound for $m_I(S_n)$, which show in particular that $m_I(S_n)$ is asymptotic to $n/2$ as $n \to \infty$.

1. INTRODUCTION

Let G be a group, and let $I = \{\mathcal{C}_1, \ldots, \mathcal{C}_k\}$ be a set of conjugacy classes of G. We say that I *invariably generates* G if $\langle x_1, \ldots, x_k \rangle = G$ for all $x_1 \in \mathcal{C}_1, \ldots, x_k \in \mathcal{C}_k$. The set I is a *minimal invariable generating set* (or *MIG-set* for short) if I invariably generates G and no proper subset of I invariably generates G. We let $m_I(G)$ denote the largest possible cardinality of a MIG-set for the group G.

We state our main theorem.

Theorem 1.1. *Let $n \geqslant 2$ be an integer, and let $G = S_n$ be the symmetric group on n letters. Then*

$$\frac{n}{2} - \log n < m_I(G) < \frac{n}{2} + \Delta(n) + O\left(\frac{\log n}{\log \log n}\right),$$

where $\Delta(n)$ is the number of divisors of n.

(Logarithms are in base 2.) It is well known that $\Delta(n) = n^{o(1)}$, therefore Theorem 1.1 implies that $m_I(S_n)$ is asymptotic to $n/2$ as $n \to \infty$.

The parameter $m_I(G)$ is the "invariable" analogue of the parameter $m(G)$, which denotes the largest possible cardinality of a minimal generating set of G (with analogous definition). See Subsection 1.2 for more context.

In [GL20], it was asked whether $m_I(G) \leqslant m(G)$ holds for every finite group G, and it was proved that $m_I(G) = m(G)$ in case G is soluble. In particular, $m_I(S_n) = m(S_n)$ for $n \leqslant 4$.

In the upper bound in Theorem 1.1, we will in fact prove a more explicit estimate, which will have the following consequence.

Corollary 1.2. *If $G = S_n$ with $n \geqslant 5$, then $m_I(G) < m(G)$.*

As we shall explain in the next subsection, this was known for large enough n.

1.1. **Methods of proof.** For a finite group G, we denote by $k(G)$ the number of conjugacy classes of G. We begin with an elementary observation.

Lemma 1.3. *Suppose that $I = \{\mathcal{C}_1, \ldots, \mathcal{C}_t\}$ is a set of conjugacy classes of a nontrivial finite group G. Then, I is a MIG-set if and only if the following conditions are both satisfied:*

(a) *There exists a set of maximal subgroups $J = \{M_1, \ldots, M_t\}$ of G such that, for every $i \neq j$, $\mathcal{C}_i \cap M_j \neq \varnothing$.*
(b) *No proper subgroup of G has non-empty intersection with $\mathcal{C}_i$ for all $i = 1, \ldots, t$.*

In particular, with notation as in the previous lemma, we have the following two consequences:

⋄ For every $j = 1, \ldots, t$, M_j has non-empty intersection with at least $t - 1$ non-trivial G-conjugacy classes, and therefore $k(M_j) \geqslant t$.
⋄ For every $i \neq j$, M_i and M_j are not G-conjugate.

The lower bound. Let us see how Lemma 1.3 can be exploited to give a lower bound for $m_I(S_n)$. Each conjugacy class $\mathcal{C}$ of S_n corresponds to a particular partition, $X_\mathcal{C}$, of the integer n. On the other hand, if M is an *intransitive* subgroup of S_n, then M is the stabilizer of some i-subset of $\{1, \ldots, n\}$.

We say that *the integer i is a partial sum of the partition* $\mathfrak{p} = (a_1, \ldots, a_t)$ if we can write $i = a_{j_1} + a_{j_2} + \cdots + a_{j_\ell}$ for some $1 \leqslant j_1 < \cdots < j_\ell \leqslant t$. It is clear that the intersection $\mathcal{C} \cap M$ is non-empty if and only if i is a partial sum of $X_\mathcal{C}$. We will prove the following:

Proposition 1.4. *Let $n \geqslant 5$ be an integer. There is a set X of partitions of n with the following properties:*

(1) *There is no integer $1 \leqslant i \leqslant n/2$ which is a partial sum in x for every $x \in X$;*
(2) *For every $x \in X$, there exists an integer $1 \leqslant i \leqslant n/2$ which is a partial sum in y for every $y \in X \setminus \{x\}$;*
(3) $|X| > \frac{1}{2}n - \log n$.

Proposition 1.4 is almost enough to yield the lower bound in Theorem 1.1 straight away. To complete the proof of that lower bound, we must take care of Lemma 1.3(b) for proper transitive subgroups of S_n.

Our feeling is that the construction we give in our proof of Proposition 1.4 is pretty close to being as large a set X as is possible.

Question 1. Is it true that the largest cardinality of a set X of partitions of n satisfying properties (1) and (2) of Proposition 1.4 is at most $\frac{1}{2}n - \log n + O(1)$?

Note that we certainly have $|X| \leqslant \frac{1}{2}n$.

The upper bound. In view of Lemma 1.3 and of the considerations following it, it is clear that the upper bound in Theorem 1.1 will be established once we prove the following result.[1]

Proposition 1.5. *Suppose that $\{M_1, \ldots, M_t\}$ is a set of maximal subgroups of the symmetric group S_n such that (a) $k(M_i) \geqslant \frac{1}{2}n$ for every i; (b) if $i \neq j$, then M_i*

---

[1]The idea we are using here is laid out explicitly in [GL20]: For every maximal subgroup M of G, denote by M^* the set of G-conjugacy classes having non-empty intersection with M. Let

$$\mathcal{M}(G) = \{M^* \mid M \text{ maximal subgroups of } G\}.$$

We say that a subset $\{X_1, \ldots, X_t\}$ of $\mathcal{M}(G)$ is *independent* if, for every $1 \leqslant i \leqslant t$, the intersection $\cap_{j \neq i} X_j$ properly contains $\cap_j X_j$. We denote by $\iota(G)$ the largest cardinality of an independent subset of $\mathcal{M}(G)$. It is not hard to see, first, that $m_I(G) \leqslant \iota(G)$ ([GL20, Lemma 4.2]) and, second, that Proposition 1.5 yields an upper bound for $\iota(S_n)$.

and M_j are not S_n-conjugate. Then

$$t \leqslant \frac{n}{2} + \Delta(n) + O\left(\frac{\log n}{\log \log n}\right), \tag{1}$$

where $\Delta(n)$ is the number of divisors of n.

The main point in the proof of Proposition 1.5 is to deal with the family of almost simple primitive subgroups of S_n; see Theorem 3.1. The key ingredient is [GG20, Theorem 1.2], which determines the almost simple primitive subgroups G of S_n such that $k(G) \geqslant \frac{1}{2}n$.

We remark that a theorem of Liebeck and Shalev gives a general upper bound for the number of conjugacy classes of maximal subgroup of S_n of the form $\frac{n}{2} + o(n)$ [LS96]. This immediately gives an upper bound for $m_I(S_n)$ and, in light of the easy fact that $m(S_n) \geqslant n - 1$, yields Corollary 1.2 provided n is large enough (this was observed also in [GL20]). We note that in Proposition 1.5 we do not use [LS96], but we use [GG20], which relies on upper bounds for the number of conjugacy classes of almost simple groups of Lie type by Fulman–Guralnick [FG12].

We remark, moreover, that although Proposition 1.5 only states an upper bound for the number of maximal subgroups with at least $\frac{1}{2}n$ conjugacy classes, results in §3 outline specific families of maximal subgroups. In particular, the first two terms of (1) correspond to the intransitive and imprimitive subgroups of S_n, respectively.

This is important because our original aim in this paper was to prove that $|m_I(G) - \frac{n}{2}| = O(\log n)$. We have managed this with the lower bound but not with the upper, precisely because $\Delta(n) - 2$, which is the number of conjugacy classes of maximal imprimitive subgroups of S_n, is not $O(\log n)$. To achieve our original aim, it would be sufficient to establish that, in the following question, $t \leqslant \frac{n}{2} + O(\log n)$. We state the question in terms of properties of S_n – it is easy enough to recast it as a number-theoretic question concerning partitions, similar to Question 1 above.[2]

Question 2. For a positive integer n, how large can t be such that we can find sets with the following properties?

    (1) $\{\mathcal{C}_1, \ldots, \mathcal{C}_t\}$ is a set of conjugacy classes of S_n;
    (2) $\{M_1, \ldots, M_t\}$ is a set of maximal subgroups of S_n, all of which are intransitive or imprimitive;
    (3) For $i = 1, \ldots, t$, $\mathcal{C}_i \cap M_i = \varnothing$;
    (4) For $i, j = 1, \ldots, t$, if $i \neq j$, then $\mathcal{C}_i \cap M_j \neq \varnothing$.

Proposition 1.4 shows that $t > n/2 - \log n$. In truth, we believe that, at least for large enough n, a MIG-set of S_n of size $m_I(S_n)$ should involve only intransitive subgroups (in the sense that the set J from Lemma 1.3 should contain only intransitive subgroups). This would imply that $m_I(S_n) \leqslant \frac{n}{2}$, and the problem of determining $m_I(S_n)$ would be reduced to the purely combinatorial problem addressed in Proposition 1.4 and Question 1.

---

[2]Yet another way to think of this question uses the terminology of the previous footnote. We are effectively asking the following: Let t be a positive integer and let $M_1, \ldots, M_t$ be maximal subgroups of S_n that are either intransitive or imprimitive. If $\{M_1^*, \ldots, M_t^*\}$ is independent, then how large can t be?

1.2. **Context.** The concept of invariable generation was introduced by Dixon, with the motivation of recognizing S_n as the Galois group of polynomials with integer co-efficients [Dix92]. See for instance Kantor–Lubotzky–Shalev [KLS11] for interesting results related to invariable generation of finite groups.

In [GL20], the invariant $m_I(G)$ was introduced and studied. This is the "invariable" version of the invariant $m(G)$, which is the largest possible cardinality of a minimal generating set of G. See Lucchini [Luc13a, Luc13b] for results concerning $m(G)$ where G is a general finite group.

Assume now $G = S_n$. It is easy to see that $m(S_n) \geqslant n - 1$, by considering the $n - 1$ transpositions $(1, 2), \ldots, (n - 1, n)$. Using CFSG, Whiston [Whi00] proved that in fact $m(S_n) = n - 1$. But more is true. Cameron–Cara [CC02] showed that a minimal generating set of S_n of size $n - 1$ is very restrictive: either it is made of $n - 1$ transpositions, or it is made of a transposition, some 3-cycles, and some double transpositions (see [CC02, Theorem 2.1] for a precise statement).

One can hardly hope for a similar "elegant" result for $m_I(S_n)$, for the simple reason that a minimal invariable generating set of S_n of size t must contain t distinct partitions which do not have a common partial sum. Still, it is true that in the proof of the lower bound in Theorem 1.1, we feel somewhat restricted about the choice of the relevant partitions – but we are not able to make any precise statement in this direction.

In [GL20], it was shown that, if G is a finite soluble group, then $m_I(G) = m(G)$, which in turn is equal to the number of complemented chief factors in a chief series of G. Moreover, it was asked whether $m_I(G) \leqslant m(G)$ is true for every finite group. It seems that, "often", for a finite non-soluble group G, the strict inequality $m_I(G) < m(G)$ holds. Corollary 1.2 confirms this feeling in case $G = S_n$.

We recall, however, that $m_I(\mathrm{PSL}_2(p)) = m(\mathrm{PSL}_2(p))$ for infinitely many primes p (see [GL20, Section 5]).

1.3. **Structure of the paper and notation.** In §2 we prove the lower bound on $m_I(G)$ given in Theorem 1.1. In §3 we prove the upper bound on $m_I(G)$ given in Theorem 1.1, along with Corollary 1.2.

We will use exponential notation for partitions, so the partition $(a_1^{n_1}, a_2^{n_2}, \ldots, a_t^{n_t})$ has n_1 parts of length a_1, n_2 parts of length $a_2, \ldots$, and n_t parts of length a_t. For a positive real number x, $\log(x)$ denotes a logarithm in base 2. For a positive integer x, $\Delta(x)$ denotes the number of divisors of x.

2. The lower bound

In this section we prove the lower bound in Theorem 1.1. We first prove a lemma, then we prove Proposition 1.4, and finally we give a proof for the lower bound.

Lemma 2.1. *Let n and i be positive integers, with $i < n/3$. Then there exist a partition $\mathfrak{p}_{i,n}$ of n with the following properties:*

(1) *If $n \neq 4i + 2$ and $(n, i) \neq (8, 1)$, then $\mathfrak{p}_{i,n}$ does not have i and $n - i$ as partial sums, and everything else is a partial sum.*

(2) *If $n = 4i + 2$ or $(n, i) = (8, 1)$, then $\mathfrak{p}_{i,n}$ does not have $i, n - i$ and $\frac{n}{2}$ as partial sums, and everything else is a partial sum.*

Proof. Define
$$\mathfrak{p}_{i,n} = (1^{i-1}, i + 1, (i + 2)^j, (i + 1)^k, c)$$

where $j \in \{0, 1\}$, $k \geqslant 0$, and $i + 1 \leqslant c \leqslant 2i + 1$. To complete the definition we must specify j, k and c. To do this we consider a partial sum q, adding from left to right: we first sum the 1's and $(i + 1)$ to obtain $q = 2i$. Now there are three cases:

(1) If $n - q \leqslant 2i + 1$, then we set $c = n - q$.
(2) If $n - q = 2i + 2$, then we set $k = 1$, $j = 0$ and $c = i + 1$.
(3) If $n - q \geqslant 2i + 3$, then we set $j = 1$, $k = 0$ and set $q = 2i + (i + 2) = 3i + 2$.

In the first and second cases, we are done; notice that the partition has the stated properties (in the first case we use the fact that $i < n/3$ to obtain $i + 1 \leqslant c \leqslant 2i + 1$ as required). If we are in the third case, then we proceed in a loop as follows:

(1) If $n - q \leqslant 2i + 1$, then we set $c = n - q$.
(2) If $n - q \geqslant 2i + 2$, then we set $k = k + 1$ and set $q = q + (i + 1)$.

It turns out that there is one situation – when $n = 4i + 4$ and $(n, i) \neq (8, 1)$ – where our definition needs to be adjusted. In this case, we make the following definition:
$$\mathfrak{p}_{i,n} = (1^{i-1}, i + 1, i + 3, i + 1).$$
Now our definition is complete. We now let m be an integer such that $1 \leqslant m \leqslant n/2$ and we study when m is a partial sum of $\mathfrak{p}_{i,n}$ with a view to proving items (1) and (2) of the lemma.

Both items are clear for $m \leqslant 2i$, thus we may assume that $m \geqslant 2i + 1$. In particular this means that $n \geqslant 4i + 2$.

If $n = 4i + 2$, then we are in item (2) of the lemma, $\mathfrak{p}_{i,n} = (1^{i-1}, (i + 1)^3)$, and the statement holds.

If $n \geqslant 4i + 3$, note first that $j = 1$. Suppose, first, that $k = 0$. There are two possibilities: first, if $c \neq i + 2$, then $\mathfrak{p}_{i,n} = (1^{i-1}, i + 1, i + 2, c)$, and the statement holds. If instead $c = i + 2$, then $n = 4i + 4$. If $(n, i) = (8, 1)$, then $\mathfrak{p}_{1,8} = (2, 3, 3)$ and we are in item (2) of the lemma. Otherwise, we are in the exceptional case in our definition where $\mathfrak{p}_{i,n} = (1^{i-1}, i + 1, i + 3, i + 1)$, and the result holds.

We are left with the case in which $k \geqslant 1$, i.e. $\mathfrak{p}_{i,n}$ contains at least two $(i + 1)$'s (excluding c which may also equal $i + 1$).

We work here by induction on m: assuming that some $2i \leqslant m < n/2$ can be written *without using* c, we want to show that the same holds for $m + 1$. Since $m \geqslant 2i \geqslant i + 1$, in writing m without c we have certainly used at least one of $i + 1$ and $i + 2$. We now divide into three cases.

(1) In writing m we have not used all 1's. Then add a 1.
(2) In writing m we have not used $i + 2$. Then remove an $i + 1$ and add $i + 2$.
(3) In writing m we have used all 1's and $i + 2$. Suppose, first, that at least two $(i + 1)$'s have not been used; then remove all 1's, remove $i + 2$ and add two $(i + 1)$'s and we are done. On the other hand, suppose (for a contradiction) that in writing m as a partial sum all but one of the $i + 1$'s have been used. Then $c + (i + 1) > n/2$ and, since $c \leqslant 2i + 1$, we obtain that $n/2 < 3i + 2$. However the partial sum m has used all 1's, one $i + 1$ and one $i + 2$, so $m \geqslant 3i + 2$. Since $m < n/2$, we get $n/2 > 3i + 2$, which is a contradiction. □

2.1. **Proof of Proposition 1.4.** Now we prove Proposition 1.4. The proof we give below is constructive – we define an explicit set X with the given properties. We have decided not to define the set X outside of this proof, as the construction is built up in pieces as the proof proceeds.

In deducing the lower bound in Theorem 1.1, we will be interested in the properties of the partitions of X listed in the statement of Proposition 1.4, rather than their explicit construction. The paragraphs involving exceptions to this are labelled **(C1)**, **(C2)**, **(C3)** and **(C4)** in the following proof.

Proof of Proposition 1.4. Throughout the proof, we will use the notation $\mathfrak{p}_{t,n}$ to refer to the partitions in the statement of Lemma 2.1 (so we allow any partition having the properties of the statement).

If $5 \leqslant n \leqslant 10$, we have $n/2 - \log n < 2$, and the statement is easy to check. Therefore assume $n \geqslant 11$.

(C1) For $n = 11$, we set $x_1 = (2^2, 3, 4)$, $x_2 = (1, 3^2, 4)$, $x_3 = (1^2, 9)$. For $n = 12$, we set $x_1 = (2^2, 3, 5)$, $x_2 = (1, 3, 4^2)$, $x_3 = (1^2, 10)$. The statement holds by setting $X = \{x_1, x_2, x_3\}$.

From now on we assume that $n > 12$. This has the advantage that in the proof that follows, all partitions of the form $\mathfrak{p}_{i,\ell}$ that we consider will have $\ell > 8$ or $i > 1$, and so we need not worry about the case $(\ell, i) = (8, 1)$ mentioned in Lemma 2.1.

For $1 \leqslant t < n/3$, define
$$x_t = \mathfrak{p}_{t,n}.$$
(C2) We want to modify partition x_1. Namely, define
$$x_1 = \begin{cases} (3, 5, 2^k, 4^j) & \text{if } n = 14, 16 \\ (3, 2^k, 4^j) & \text{if } n = 13, 15, 17 \\ (3^\ell, 7, 2^k, 4^j) & \text{if } n \geqslant 18 \end{cases}$$

where $\ell = 1$ or 2 according to whether n is even or odd, and $j \in \{0, 1\}$ is defined by the condition that x_1 has an odd number of cycles of even length (and k is consequently uniquely defined). It is easy to see that, in every case, every $2 \leqslant i \leqslant n/2$ is a partial sum in x_1.

Now, in order to go further, we will use a slightly different method. The partitions we are going to define will depend on a parameter j. We could define all of them at once, but to give an idea of the overall strategy, let us go through the first step explicitly.

We set $\alpha_1 = \lceil n/6 - 1 \rceil$ and, for every integer $\lceil n/3 \rceil \leqslant t \leqslant t_1 = 5n/12$ we define
$$x_t = (\mathfrak{p}_{\alpha_1, \alpha_1 + t}, c_t).$$
where $c_t = n - \alpha_1 - t$. Let us justify this definition:

(a) Observe first that $1 \leqslant \alpha_1 < (\alpha_1 + t)/3$ hence the partition $\mathfrak{p}_{\alpha_1, \alpha_1 + t}$ is well-defined.

(b) Next note that
$$c_t = n - \alpha_1 - t$$
$$> n - \left\lceil \frac{n}{6} - 1 \right\rceil - \frac{5n}{12}$$
$$> \frac{5n}{12} \geqslant t > \alpha_1,$$
and so α_1 and t are not partial sums of x_t.

(c) We can easily check that either $4\alpha_1 + 2 > \alpha_1 + t$ or else $(\alpha_1, t, n) = (1, 5, 12)$. The second possibility is excluded by our assumption $n > 12$. The first possibility implies that Lemma 2.1(1) holds, and so all numbers up to $\alpha_1 + t$ are partial sums, apart from α_1 and t.

(d) Finally observe that

$$\alpha_1 + t \geqslant \left\lceil \frac{n}{6} - 1 \right\rceil + \left\lceil \frac{n}{3} \right\rceil \tag{2}$$

$$\geqslant \left\lceil \frac{n}{2} - 1 \right\rceil.$$

We conclude that all numbers up to n are partial sums in x_t apart from α_1, t and (possibly) $n/2$. In fact, checking (2) more carefully, it is clear that $\alpha_1 + t \geqslant \lfloor n/2 \rfloor$ unless $n \equiv 0 \pmod 6$ and $t = n/3$.

Conclusion 1: For $n/3 < t \leqslant 5n/12$, the partition x_t admits all partial sums up to n except α_1 and t.

Conclusion 2: For $t = n/3$, the partition x_t admits all partial sums up to n except α_1 and t and (if n is even) $n/2$.

Now our aim is to extend this definition to other parameters t_i that are larger than t_1. More precisely, for integer $1 \leqslant j \leqslant \log(n/6)$ we define

$$\alpha_j = \left\lceil \frac{n}{2^{j-1} \cdot 6} - 1 \right\rceil, \qquad t_j = \frac{(2^{j-1} \cdot 6 - 1)n}{2^j \cdot 6}.$$

For $j = 1$ this is consistent with the previous definition. Now for integers $2 \leqslant j \leqslant \log(n/6)$ and $\lfloor t_{j-1} \rfloor + 1 \leqslant t \leqslant \lfloor t_j \rfloor$ we define

$$x_t = (\mathfrak{p}_{\alpha_j, \alpha_j + t}, c_t)$$

where $c_t = n - \alpha_j - t$. Now, similarly to before, we must check four properties. Assume that $j \geqslant 2$.

(a) Observe that $1 \leqslant \alpha_j < (\alpha_j + \lfloor t_{j-1} \rfloor + 1)/3$ and so the partition $\mathfrak{p}_{\alpha_j, \alpha_j + t}$ is well-defined.

(b) Next note that $c_t = n - \alpha_j - t > t > \alpha_j$ and so α_j and t are not partial sums of x_t.

(c) Notice that the second case of Lemma 2.1 does not occur. Indeed, $4\alpha_j + 2$ is strictly smaller than $\alpha_j + \lfloor t_{j-1} \rfloor + 1$. Moreover, it is easy to check that the case $(\ell, i) = (8, 1)$ cannot occur.

(d) Finally observe that $\alpha_j + \lfloor t_{j-1} \rfloor + 1 \geqslant \lfloor n/2 \rfloor$, and we conclude that all numbers up to n are partial sums in x_t apart from α_1 and t.

Conclusion 3: Set $m = \lfloor \log(n/6) \rfloor$. For $j = 2, \ldots, m$ and $\lfloor t_{j-1} \rfloor + 1 \leqslant t \leqslant \lfloor t_j \rfloor$, the partition x_t admits all partial sums up to n, except α_j and t.

We have now constructed $\lfloor t_m \rfloor$ partitions of n; set $X_0 = \{x_1, \ldots, x_{\lfloor t_m \rfloor}\}$. Notice that, by the choice of m, $2^{m+1} \cdot 6 > n$. Then

$$|X_0| = \lfloor t_m \rfloor > \frac{(2^{m-1} \cdot 6 - 1)n}{2^m \cdot 6} - 1 \tag{3}$$

$$= \frac{n}{2} - \frac{n}{2^m \cdot 6} - 1$$

$$> \frac{n}{2} - 3.$$

Now we will remove some elements from X_0. First, observe that $\alpha_j < n/6$ for every j; we start by taking the subset X obtained by removing x_{α_j} for every $j \geqslant 1$.

(C3) Lemma 2.1, and the three conclusions listed above imply that, for each t satisfying $1 \leqslant t \leqslant t_m$, the partition x_t is the unique partition in X which does not admit t as a partial sum. Now we divide into two cases.

(1) There exists an integer belonging to the interval $(t_m, n/2]$ which is a partial
    sum for all $x_t \in X$. Then, the minimum such integer is $\lfloor t_m \rfloor + 1$; we add
    one further partition to X:

$$z = (1^{\lfloor t_m \rfloor}, n - \lfloor t_m \rfloor).$$

(2) No integer in $(t_m, n/2]$ is a partial sum in all x_t's. Observing that $t_m \leqslant$
    $n/2-1$, Lemma 2.1 and the three conclusions above imply that $t_m = n/2-1$,
    i.e., $n = 2^m \cdot 6$. In this case we could leave X unchanged, and the statement
    would be proved. However, we prefer to immediately modify the set X.
    Notice that $\alpha_m = 1$ and $t_{m-1} = n/2 - 2$; it follows that $x_1 = \mathfrak{p}_{1,n} \notin X$,
    and X contains a unique partition, namely x_{t_m}, of the form $(\mathfrak{p}_{1,1+t}, c_t)$.
    Then, we remove such partition and we reintegrate the partition x_1 in X.
    Moreover, we add to X one further partition

$$z = (1^{n/2-2}, n/2 + 2).$$

(C4) Our construction is finished. Let us make one observation, before concluding
the proof. In case (2) above, by construction $x_1 \in X$. We claim that the same
holds in case (1). Indeed, one can easily check that $\alpha_m = 1$ if and only if $n = 2^m \cdot 6$,
and otherwise $\alpha_j > 1$ for every j. Therefore, in case (1), in our procedure we did
not remove x_1 from X_0, hence clearly $x_1 \in X$.

We are now ready to conclude the proof of the statement. The considerations
above imply that items (1) and (2) of the statement hold. Regarding item (3),

$$\begin{aligned}
|X| &\geqslant |X_0| + 1 - \log(n/6) \\
&\geqslant \frac{n}{2} - 2 - \log n + \log 6 \\
&> \frac{n}{2} - \log n.
\end{aligned}$$

The proposition is now proved. $\square$

We now deduce the lower bound of Theorem 1.1 from Proposition 1.4.

Proof of the lower bound of Theorem 1.1. For $n = 2$, $n/2 - \log n = 0$ and the
statement is trivial. For $3 \leqslant n \leqslant 10$, we have $n/2 - \log n < 2$. Since certainly
$m_I(S_n) \geqslant 2$, the statement holds and we may assume $n \geqslant 11$.

Consider the set X of partitions constructed in the proof of Proposition 1.4. We
will consider the elements of X as conjugacy classes of S_n. We want to show that
X is a MIG-set for S_n.

It is easy to check the statement for $n = 11, 12$ (see the paragraph **(C1)** in the
proof of Proposition 1.4). Assume now $n \geqslant 13$. By Proposition 1.4(1), the classes of
X cannot have non-empty intersection with an intransitive subgroup of S_n. On the
other hand, by Proposition 1.4(2), if we drop one class from X, then the remaining
classes have non-empty intersection with some intransitive subgroup.

Now we deal with transitive groups. Note that X is not contained in A_n, since x_1
corresponds to an odd permutation (see the paragraphs **(C2)** and **(C4)**). Moreover,
a power of x_1 corresponds to a cycle of prime length fixing at least 3 points, which
belongs to no primitive group different from A_n and S_n by a classical theorem of
Jordan. Assume now the classes of X preserve a partition of $\{1, \ldots, n\}$ made of
$r > 1$ blocks of size $k > 1$. Recall that X contains a partition $z = (1^{n-\ell}, \ell)$, with
$\ell = n/2 + 2$ or $\ell = n - \lfloor t_m \rfloor$ (see the paragraph **(C3)**). By eq. (3) in the proof of
Proposition 1.4, we have $n/2-3 < \lfloor t_m \rfloor < n/2$, and in particular $n/2 < \ell < n/2+3$.

n	G	$k(G)$
22	$M_{22}.2$	21
40	$\mathrm{SU}_4(2).2$	25
45	$\mathrm{SU}_4(2).2$	25

TABLE 1. Some maximal almost simple primitive subgroups, G of S_n, for which $k(G) \geqslant \frac{n}{2}$. In every case there is a single S_n-conjugacy class of primitive subgroups isomorphic to G.

We have that k must divide ℓ. Since k also divides n, we get $k < 6$. If $n \neq 15$, then x_1 cannot preserve blocks of size at most 5. If $n = 15$, we note that X contains $x_4 = \mathfrak{p}_{4,15}$, and we may take $\mathfrak{p}_{4,15} = (1^3, 5, 7)$, which does not preserve any nontrivial partition of $\{1, \ldots, 15\}$. The proof is now concluded. $\qquad\square$

3. The upper bound

In this section we prove the upper bound in Theorem 1.1, and we prove Corollary 1.2. Our main tool is the following result, which follows quickly from [GG20]. Recall that $k(G)$ denotes the number of conjugacy classes of a finite group G.

Theorem 3.1. *Let G be a maximal almost simple primitive subgroup of S_n, and assume $k(G) \geqslant \frac{n}{2}$. Then one of the following occurs:*

(1) *G is listed in Table 1;*
(2) *$G = A_n$, or $G = S_d$ and the action of G on n points is isomorphic to the action on the set of k-subsets of $\{1, \ldots, d\}$ for some $2 \leqslant k < d/2$.*
(3) *$G = \mathrm{P\Gamma L}_d(q)$ and the action of G on n points is isomorphic to the action on the set of 1-subspaces of $\mathbf{F}_q^d$.*

Note that the subgroups mentioned at item (2) satisfy $n = \binom{d}{k}$ for some integer k with $1 \leqslant k < d/2$; and the subgroups mentioned at item (3) satisfy $n = (q^d - 1)/(q - 1)$.

Proof. The statement follows from [GG20, Theorem 1.2], by checking with [GAP19] which of the entries in [GG20, Table 1] correspond to maximal subgroups of S_n. $\quad\square$

As we observed in the introduction, the upper bound in Theorem 1.1 follows immediately from Proposition 1.5, which we prove now.

Proof of Proposition 1.5. We make use of the families of maximal subgroups given in the Aschbacher–O'Nan–Scott theorem, in particular the description given in [LPS88].

(1) **Intransitive subgroups**: There are exactly $\lfloor \frac{n}{2} \rfloor$ conjugacy classes of these.
(2) **Imprimitive subgroups**: There are $\Delta(n) - 2$ of these, where Δ is the divisor function.
(3) **Affine subgroups**: There is at most 1 conjugacy class of these.
(4) **Almost simple subgroups**: If M is almost simple and $k(M) \geqslant \frac{n}{2}$, then it is among the possibilities listed by Theorem 3.1, as follows.
  (a) There are three possibilities for degrees $22, 40, 45$ listed in Table 1.

   (b) There is at most one conjugacy class of maximal subgroups isomorphic
to $\mathrm{P\Gamma L}_d(q)$ whenever $n = \frac{q^d-1}{q-1}$; we let a_n be the number of pairs (q,d)
where q is a prime power, d is a positive integer, and $\frac{q^d-1}{q-1} = n$.

   (c) There is at most one conjugacy class of maximal subgroups with socle
A_d whenever $n = \binom{d}{k}$ for some k; we let b_n be the number of pairs
(d,k) where d and k are positive integers with $k \leqslant d/2$ and $\binom{d}{k} = n$.

(5) **Diagonal subgroups**: [GG20, Theorem 1.1] states that $k(M) < \frac{n}{2}$ in this
case, so we can ignore these subgroups.

(6) **Product action subgroups**: In this case we have maximal subgroups
isomorphic to $S_d \wr S_k$, where $n = d^k$ and $k > 1$. For fixed values of d and
k, there is one conjugacy class, thus the number of conjugacy classes in S_n
is equal to the number of pairs (d,k) where d and k are positive integers
with $k > 1$ and $n = d^k$; we write this number as c_n.

(7) **Twisted wreath subgroups**: These are never maximal, as they are de-
fined to be subgroups of groups with a product action [LPS88] and so can
be ignored (and in any case, $k(M) < \frac{n}{2}$ by [GG20, Theorem 1.1]).

Observe that the number of conjugacy classes of maximal subgroup in S_n that
are either imprimitive, affine, or given in Table 1 is at most $\Delta(n) - 1$. Therefore, if
$\{M_1, \ldots, M_t\}$ is a set of maximal subgroups as in the statement, we have

$$t \leqslant \left\lfloor \frac{n}{2} \right\rfloor + \Delta(n) + a_n + b_n + c_n - 1. \tag{4}$$

(We will use this in the proof of Corollary 1.2.) In order to prove Proposition 1.5,
it is clearly enough to show that

$$a_n + b_n + c_n = O\left(\frac{\log n}{\log\log n}\right).$$

To bound a_n, observe that if

$$\frac{q_1^{d_1}-1}{q_1-1} = \frac{q_2^{d_2}-1}{q_2-1},$$

then q_1 and q_2 must be coprime. We obtain that a_n must be bounded above by the
number of distinct prime divisors of $n - 1$. In [Rob83] it is proved that this number
is

$$O\left(\frac{\log(n-1)}{\log\log(n-1)}\right),$$

whence the same upper bound holds for a_n.

To bound b_n we refer to a result of Kane [Kan07], which asserts that[3]

$$b_n = O\left(\frac{\log n \log\log\log n}{(\log\log n)^3}\right).$$

To bound c_n, we first recall (see [Apo76, Theorem 13.12]) that, for a positive
integer x,

$$\Delta(x) \leqslant \exp_2\left\{\frac{(1+o(1))\log x}{\log\log x}\right\}.$$

---

[3]Singmaster's conjecture [Sin71] asserts that b_n is bounded above by an absolute constant;
de Weger proposes that in fact this constant can be taken to be 4 [dW97], and evidence for the
veracity of this conjecture is given in [BBD17]; in particular this is known to be true if $n \leqslant 10^{60}$.

Now consider the prime factorization of n: $n = p_1^{a_1} \cdots p_t^{a_t}$. If $n = d^k$ then $p_1 \cdots p_t$ divides d and k divides $a := \gcd\{a_1, \ldots, a_t\}$. Therefore, the number of choices for k is at most the number of divisors of a different from 1. Now note that $a \leqslant \log n$, and therefore

$$c_n \leqslant \exp_2 \left\{ \frac{(1 + o(1)) \log \log n}{\log \log \log n} \right\}.$$

In particular we see that each of a_n, b_n, c_n is $O(\log n / \log \log n)$. This proves the proposition. $\qquad\square$

We conclude with the proof of Corollary 1.2.

Proof of Corollary 1.2. It is easy to see that $\{(1,2), (2,3), (3,4), \ldots, (n-1,n)\}$ is a minimal generating set of size $n-1$. It is, therefore, enough to show that $m_I(S_n) < n - 1$.

From eq. (4) in the proof of Proposition 1.5, we deduce that

$$m_I(S_n) \leqslant \left\lfloor \frac{n}{2} \right\rfloor + \Delta(n) + a_n + b_n + c_n - 1,$$

therefore it is sufficient to show that $\Delta(n) + a_n + b_n + c_n < n/2$. Very weak estimates are enough here. First assume that $n \geqslant 71$.

As remarked in the proof of Proposition 1.5, a_n is bounded above by the number of distinct prime divisors of $n - 1$, which is at most $\log n$. Moreover, c_n is bounded above by $\max\{\Delta(x) : x \leqslant \lfloor \log n \rfloor\}$, which is at most $\log n$. Let us consider b_n. Let $(d_1, k_1), \ldots, (d_b, k_b)$ be pairs such that $\binom{d_i}{k_i} = n$ for all $i = 1, \ldots, b$. Order so that $i < j$ implies that $k_i < k_j$ and observe that then $k_b \geqslant b$ and $d_b \geqslant 2b$. This implies that $n \geqslant \binom{2b}{b} > 2^b$. In particular $b < \log n$.

Finally we need to bound $\Delta(n)$. For every real number $a \in (0, n]$, we have $\Delta(n) < n/a + a$. By choosing $a = \sqrt{n}$, we deduce $\Delta(n) < 2\sqrt{n}$.

Therefore $\Delta(n) + a_n + b_n + c_n < 2\sqrt{n} + 3 \log n$, and it is sufficient to show that $2\sqrt{n} + 3 \log n \leqslant n/2$. Since $n \geqslant 71$, this is indeed the case.

For $n \leqslant 70$ we use [GAP19] to find that, except when $n \in \{5, 6, 8, 12\}$, S_n has less than $n - 1$ conjugacy classes of maximal subgroup and the result follows immediately.

For the remaining cases, say that two cycle types are *equivalent* if one is a power of the other one; e.g., $(2, 2)$ is equivalent to (4), $(2, 3, 3)$ is equivalent to $(2, 1^6)$, etc. Note that a MIG-set of S_n of size t must contain t pairwise non-equivalent cycle types.

For $n \in \{5, 8, 12\}$, there are exactly $n - 1$ conjugacy classes of maximal subgroups of S_n. However, in each case, there is one which does not intersect at least $n - 3$ pairwise non-equivalent cycle types, and the result follows. (For $n = 5$ we may take $\mathrm{AGL}_1(5)$, for $n = 8$ we may take $\mathrm{PGL}_2(7)$, and for $n = 12$ we may take $\mathrm{PGL}_2(11)$.)

For $n = 6$, we note that a MIG-set of size $t \geqslant 5$ must contain 5 distinct non-trivial cycle types, each of which intersects non-trivially 4 pairwise non-conjugate maximal subgroups. A direct check shows that the cycle types with this property are

$$(2), (2^2), (2^3), (3), (3^2), (4), (4, 2). \qquad\qquad (\star)$$

Now, a set of 4 pairwise non-equivalent cycle types, each intersecting non-trivially $\mathrm{PGL}_2(5)$, must contain the cycle type (5), which does not appear in $(\star)$. Therefore, we deduce that a MIG-set of size $t \geqslant 5$ must contain 5 distinct cycle types, each of which intersects non-trivially 4 pairwise non-conjugate maximal subgroups, not

isomorphic to $\mathrm{PGL}_2(5)$. We see that (4) does not have this property. All other cycle types appearing in $(\star)$ intersect non-trivially $S_3 \wr S_2$, and we deduce that $m_I(S_6) < 5$, as wanted. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

References

[Apo76] T. M. Apostol. *Introduction to analytic number theory*. Springer-Verlag, New York-Heidelberg, 1976. Undergraduate Texts in Mathematics.

[BBD17] A. Blokhuis, A. Brouwer, and B. De Weger. Binomial collisions and near collisions. *Integers*, 17:paper a64, 8, 2017.

[CC02]   P. J. Cameron and P. Cara. Independent generating sets and geometries for symmetric groups. *Journal of Algebra*, 258(2):641–650, 2002.

[Dix92] J. D. Dixon. Random sets which invariably generate the symmetric group. *Discrete Mathematics*, 105(1-3):25–39, 1992.

[dW97]   B. M. M. de Weger. Equal binomial coefficients: Some elementary considerations. *J. Number Theory*, 63(2):373–386, 1997.

[FG12]   J. Fulman and R. M. Guralnick. Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements. *Trans. Am. Math. Soc.*, 364(6):3023–3070, 2012.

[GAP19] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.10.2*, 2019.

[GG20]   D. Garzoni and N. Gill. On the number of conjugacy classes of a primitive permutation group with nonabelian socle. *arXiv preprint arXiv:2012.05547*, 2020.

[GL20]   D. Garzoni and A. Lucchini. Minimal invariable generating sets. *Journal of Pure and Applied Algebra*, 224(1):218–238, 2020.

[Kan07] D. M. Kane. Improved bounds on the number of ways of expressing t as a binomial coefficient. *Integers*, 7(1):paper a53, 7, 2007.

[KLS11] W. M. Kantor, A. Lubotzky, and A. Shalev. Invariable generation and the Chebotarev invariant of a finite group. *J. Algebra*, 348:302–314, 2011.

[LPS88] M. W. Liebeck, C. E. Praeger, and J. Saxl. On the O'Nan-Scott theorem for finite primitive permutation groups. *J. Aust. Math. Soc., Ser. A*, 44(3):389–396, 1988.

[LS96]   M. W. Liebeck and A. Shalev. Maximal subgroups of symmetric groups. *J. Comb. Theory, Ser. A*, 75(2):341–352, 1996.

[Luc13a] A. Lucchini. The largest size of a minimal generating set of a finite group. *Archiv der Mathematik*, 101(1):1–8, 2013.

[Luc13b] A. Lucchini. Minimal generating sets of maximal size in finite monolithic groups. *Archiv der Mathematik*, 101(5):401–410, 2013.

[Rob83] G. Robin. Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n. *Acta Arithmetica*, 42(4):367–389, 1983.

[Sin71] D. Singmaster. How often does an integer occur as a binomial coefficient? *Am. Math. Monthly*, 78:385–386, 1971.

[Whi00] J. Whiston. Maximal independent generating sets of the symmetric group. *J. Algebra*, 232(1):255–268, 2000.

DANIELE GARZONI, DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA", UNIVERSITÀ DEGLI STUDI DI PADOVA, PADOVA, ITALY
    Email address: daniele.garzoni@phd.unipd.it

NICK GILL, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTH WALES, TREFOREST CF37 1DL, U.K.
    Email address: nick.gill@southwales.ac.uk