

# Covering The Symmetric Groups With Proper Subgroups

Attila Maróti

Department of Mathematics, University of Southern California  
Los Angeles, CA 90089-1113, U.S.A.

15th of October 2004

## Abstract

Let  $G$  be a group that is a set-theoretic union of finitely many proper subgroups. Cohn defined  $\sigma(G)$  to be the least integer  $m$  such that  $G$  is the union of  $m$  proper subgroups. Tomkinson showed that  $\sigma(G)$  can never be 7, and that it is always of the form  $q + 1$  ( $q$  a prime power) for solvable groups  $G$ . In this paper we give exact or asymptotic formulas for  $\sigma(S_n)$ . In particular, we show that  $\sigma(S_n) \leq 2^{n-1}$ , while for alternating groups we find  $\sigma(A_n) \geq 2^{n-2}$  unless  $n = 7$  or  $9$ . An application of this result is also given.

## 1 Introduction

Let  $G$  be a group that is a set-theoretic union of finitely many proper subgroups. Cohn [5] defined the function  $\sigma(G)$  to be the least integer  $m$  such that  $G$  is the union of  $m$  of its proper subgroups. (A result of Neumann [18] states that if  $G$  is the union of  $m$  proper subgroups where  $m$  is finite and small as possible, then the intersection of these subgroups is a subgroup of finite index in  $G$ . Hence in investigating  $\sigma$  we may assume that  $G$  is finite.) It is an easy exercise that  $\sigma(G)$  can never be 2; it is at least 3. Groups that are the union of three proper subgroups, as  $C_2 \times C_2$  is for example, are investigated in the papers [23], [11], and [3]. Moreover,  $\sigma(G)$  can be 4, 5, and 6 too, as the examples,  $C_3 \times C_3$ ,  $A_4$ , and  $C_5 \times C_5$  show. However, Tomkinson [24] proved that there is no group  $G$  with  $\sigma(G) = 7$ . Cohn [5] showed that for any prime power  $p^a$  there exists a solvable group  $G$  with  $\sigma(G) = p^a + 1$ . In fact, Tomkinson [24] established that  $\sigma(G) - 1$  is always a prime power for solvable groups  $G$ . He also pointed out that it would be of interest to investigate  $\sigma$  for families of simple groups. Indeed, the situation for nonsolvable groups seems

to be totally different. Bryce, Fedri, Serena [4] investigated certain nonsolvable 2-by-2 matrix groups over finite fields,  $((P)G(S)L(2, q))$  and obtained the formula  $\frac{1}{2}q(q+1)$  for even prime powers  $q \geq 4$ , and the formula  $\frac{1}{2}q(q+1) + 1$  for odd prime powers  $q \geq 5$ . Moreover, Lucido [14] found that  $\sigma(Sz(q)) = \frac{1}{2}q^2(q^2 + 1)$  where  $q = 2^{2m+1}$ . There are partial results due to Bryce and Serena for determining  $\sigma((P)G(S)L(n, q))$ .

In this paper the following is established.

**Theorem 1.1.** *Let  $n > 3$ , and let  $S_n$  and  $A_n$  be the symmetric and the alternating group respectively on  $n$  letters.*

(1) *We have  $\sigma(S_n) = 2^{n-1}$  if  $n$  is odd unless  $n = 9$ , and  $\sigma(S_n) \leq 2^{n-2}$  if  $n$  is even.*

(2) *If  $n \neq 7, 9$ , then  $\sigma(A_n) \geq 2^{n-2}$  with equality if and only if  $n$  is even but not divisible by 4.*

In the following sections we will prove more than what is stated in Theorem 1.1. We will obtain exact or asymptotic formulas in all (infinite) cases (possibly) except for  $\sigma(A_p)$  where  $p$  is a prime of the form  $(q^k - 1)/(q - 1)$  where  $q$  is a prime power and  $k$  is a positive integer.

For the groups  $S_9$ ,  $S_{12}$ ,  $A_7$ , and  $A_9$  we only prove  $172 \leq \sigma(S_9) \leq 256$ ,  $\sigma(S_{12}) \leq 761$ ,  $\sigma(A_7) \leq 31$ , and  $\sigma(A_9) \geq 80$ . Notice that the numbers 761 and 31 are primes not of the form  $q + 1$  where  $q$  is a prime power. We prove that  $\sigma(G)$  can indeed be such a prime.

**Proposition 1.1.** *For the smallest Mathieu group we have  $\sigma(M_{11}) = 23$ .*

This result was also proved (independently) by Holmes in [12]. In her paper many interesting results are found about sporadic simple groups. It is proved that  $\sigma(M_{22}) = 771$ ,  $\sigma(M_{23}) = 41079$ ,  $\sigma(O'N) = 36450855$ ,  $\sigma(Ly) = 112845655268156$ ,  $5165 \leq \sigma(J_1) \leq 5415$ , and that  $24541 \leq \sigma(McL) \leq 24553$ .

At this point we note that Tomkinson [24] conjectured that  $\sigma(G)$  can never be 11 nor 13.

In Section 6 we investigate the relationship between some of the known infinite series of  $\sigma$ .

The commuting graph  $\Gamma$  of a group  $G$  is as follows. Let the vertices of  $\Gamma$  be the elements of  $G$  and two vertices  $g, h$  of  $\Gamma$  are joined by an edge if and only if  $g$  and  $h$  commute as elements of  $G$ . (The commuting graph is used to measure how abelian the group is. See [8], and [21].) Several people have studied  $\alpha(G)$ , the maximal cardinality of an empty subgraph of  $\Gamma$  and  $\beta(G)$ , the minimal cardinality

of a covering of the vertices of  $\Gamma$  by complete subgraphs. (See the papers [8], [16], and [20].) Brown investigated the relationship between the numbers  $\alpha_n = \alpha(S_n)$  and  $\beta_n = \beta(S_n)$ . In [1] it is shown that these numbers are surprisingly close to each other, though for  $n \geq 15$ , they are never equal [2].

As an application of Theorem 1.1, we prove that if we add ‘more’ edges to the commuting graph of the symmetric group, then the corresponding numbers will be equal in infinitely many cases. Let  $G$  be a group. Define a graph  $\Gamma'$  on the elements of  $G$  with the property that two group elements are joined by an edge if and only if they generate a proper subgroup of  $G$ . Similarly as for the commuting graph, we may define  $\alpha'(G)$  and  $\beta'(G)$  for our new graph,  $\Gamma'$ . Put  $\alpha'_n = \alpha'(S_n)$  and  $\beta'_n = \beta'(S_n)$ . The theorem can now be stated.

**Theorem 1.2.** *There is a subset  $S$  of density 1 in the set of all primes, so that  $\alpha'_n = \beta'_n$  holds for all  $n \in S$ .*

The equality  $\alpha'_n = \beta'_n$  is valid for very small values of  $n$  also. Does it hold for all  $n$ ?

We note that the problem of covering groups by subgroups has found interest for many years. The first reference the author is aware of is the 1926 work of Scorza [23]. Probably Neumann [18], [19] was the first to study the number of (abelian) subgroups needed to cover a (not necessarily finite) group  $G$  in relation to the index of the center of  $G$ . For a survey of this area see [22]. On the other hand, for an extensive account of work in (packing and) covering groups with (isomorphic) subgroups (or of subgroups of a specified order) the reader is referred to [13].

## 2 Preliminaries

Let  $G$  be  $S_n$  or  $A_n$ , the symmetric or the alternating group on  $n$  letters. Let  $\Pi$  be a set of permutations of  $G$ . Define  $\sigma(\Pi)$  to be the least integer  $m$  such that  $\Pi$  is the subset of the set-theoretic union of  $m$  proper subgroups of  $G$ . It is straightforward that  $\sigma(\Pi) \leq \sigma(G)$ . We will say that a set  $\mathcal{H} = \{H_1, \dots, H_m\}$  of  $m$  proper subgroups of  $G$  is *definitely unbeatable* on  $\Pi$  if  $\Pi \subseteq \bigcup_{i=1}^m H_i$ ; if  $\Pi \cap H_i \cap H_j = \emptyset$  for all  $i \neq j$ ; and if  $|S \cap \Pi| \leq |H_i \cap \Pi|$  holds whenever  $1 \leq i \leq m$  and when  $S \notin \mathcal{H}$  is a proper subgroup of  $G$ . If  $\mathcal{H}$  is definitely unbeatable on  $\Pi$ , then  $|\mathcal{H}| = \sigma(\Pi) \leq \sigma(G)$ .

We will call a permutation an  $(i, n - i)$ -cycle if it is a product of two disjoint cycles one of length  $i$  and one of length  $n - i$ , and will call a permutation an  $(i, j, n - i - j)$ -cycle if it is a product of three

disjoint cycles one of length  $i$ , one of length  $j$ , and one of length  $n - i - j$ .

We will use the list of primitive permutation groups of [7] and the result of [15] stating that a primitive permutation group of degree  $n$  not containing  $A_n$  has order at most  $e^n$ . Sometimes the computer package [9] is also used for computations in symmetric and alternating groups of small degree.

### 3 Symmetric groups

First, let us consider the case where the degree of the symmetric group is odd.

**Theorem 3.1.** *If  $n > 1$  is odd, then  $\sigma(S_n) = 2^{n-1}$  unless  $n = 9$ .*

*Proof.* The set-theoretic union of  $A_n$  and all maximal intransitive subgroups of  $S_n$  is  $S_n$ . This gives

$$\sigma(S_n) \leq 1 + \frac{1}{2} \cdot \sum_{i=1}^{n-1} \binom{n}{i} = 1 + \frac{1}{2}(2^n - 2) = 2^{n-1}.$$

The upper bound is known to be exact for  $n = 3$  and  $n = 5$  from [5], so assume that  $n \geq 7$ . Now let  $\Pi$  be the set of all permutations of  $S_n$ , which are the products of at most two disjoint cycles. It is sufficient to prove  $\sigma(\Pi) \geq 2^{n-1}$ .

For  $n \geq 11$  the latter inequality is the direct consequence of the fact that the set consisting of  $A_n$  and of all maximal intransitive subgroups of  $S_n$  is definitely unbeatable on  $\Pi$ . This is proved in two steps.

**Claim 3.1.** *Let  $H_1$  and  $H_2$  be  $A_n$  or a maximal intransitive subgroup of  $S_n$ . If  $H_1 \neq H_2$ , then  $\Pi \cap H_1 \cap H_2 = \emptyset$ .*

*Proof.* Indeed,  $A_n \cap \Pi$  is the set of all  $n$ -cycles, while  $S_\Delta \times S_{\bar{n} \setminus \Delta} \cap \Pi$  is the set of all permutations of the form  $\pi = \delta \cdot \bar{\delta}$  with  $\delta$  a  $|\Delta|$ -cycle from  $S_\Delta$  and  $\bar{\delta}$  a  $|\bar{n} \setminus \Delta|$ -cycle from  $S_{\bar{n} \setminus \Delta}$ , where  $\bar{n}$  denotes the set of  $n$  letters on which  $S_n$  acts and where  $\Delta$  is a nontrivial proper subset of  $\bar{n}$ . □

**Claim 3.2.** *Suppose that  $n \geq 11$  is odd. Let  $H$  be  $A_n$  or a maximal intransitive subgroup of  $S_n$ , and let  $S$  be any subgroup of  $S_n$  different from  $A_n$  and different from any maximal intransitive subgroup. Then  $|S \cap \Pi| \leq |H \cap \Pi|$ .*

*Proof.* It can be assumed that  $S$  is maximal in  $S_n$ . First let  $n \geq 17$ . If  $S$  is primitive, then  $|S \cap \Pi| \leq |S| \leq e^n$  follows from [15], while we have  $e^n \leq ((n-1)/2)! \cdot ((n-3)/2)! \leq |H \cap \Pi|$ . If  $S$  is imprimitive, then  $|S \cap \Pi| \leq |S| \leq (n/p)!^p \cdot p! \leq ((n-1)/2)! \cdot ((n-3)/2)! \leq |H \cap \Pi|$  holds, where  $p$  is the smallest prime divisor of  $n$ . If  $n = 11$  or  $13$ , then  $S$  is primitive and  $|S| < ((n-1)/2)! \cdot ((n-3)/2)!$  is checked easily by [7] or [15]. If  $n = 15$ , then by [7],  $S$  is conjugate to a maximal imprimitive group with five blocks of imprimitivity, to a maximal imprimitive group with three blocks of imprimitivity, or to  $S_6$  acting on the set of distinct pairs of points. In the first and the third case we have  $|S| \leq 3!^5 \cdot 5! < 6! \cdot 7! \leq |H \cap \Pi|$ . Let  $S$  be a maximal imprimitive subgroup of  $S_{15}$  with three blocks of imprimitivity. Now in  $S \cap \Pi$  the number of 15-, (5, 10)-, (3, 12), and (6, 9)-cycles are  $(5!^3 \cdot 3!)/15$ ,  $72 \cdot 5!^2/5$ ,  $5!^3/2$ , and  $5!^3/3$ , respectively. All together we get  $|S \cap \Pi| = 2338560 < 6! \cdot 7!$ . □

The remaining cases,  $n = 7, 9$ , are dealt separately.

Let  $n = 7$ . We have  $\sigma(\Pi) \leq 64$ . We will show that  $\sigma(\Pi) \geq 64$ . Let  $\mathcal{L}$  be a set of  $\sigma(S_7)$  maximal subgroups of  $S_7$  covering  $S_7$ . Since there is exactly one maximal subgroup (an intransitive one) containing a given (3, 4)- or a given (2, 5)-cycle, all  $\binom{7}{3} + \binom{7}{2} = 56$  maximal intransitive groups which do not stabilize any point are contained in  $\mathcal{L}$ . The group  $A_7$  is also contained in  $\mathcal{L}$ . For if it would not, then the subset of all 7-cycles of  $\Pi$  (having  $6!$  elements) could only be covered by  $5!$  maximal primitive groups each conjugate to  $AGL(1, 7)$ . So we would get  $\sigma(\Pi) \geq 56 + 5!$ , which contradicts  $\sigma(\Pi) \leq 64$ . We claim that  $\mathcal{L}$  contains all 7 one-point stabilizers as well, hence  $\sigma(\Pi) \geq 56 + 1 + 7 = 64$  would follow. To see this, consider the (1, 6)-cycles of  $\Pi$ . A maximal subgroup of  $S_7$  containing such permutations is either a stabilizer of a point, or is conjugate to the primitive affine group,  $AGL(1, 7)$ . Suppose that  $\mathcal{L}$  does not contain the stabilizer of the point  $\alpha$ . Then the 6-cycles of  $S_{\bar{n} \setminus \{\alpha\}}$  are covered with at least 60 primitive affine groups, which gives the contradiction  $\sigma(\Pi) \geq 56 + 60$ .

Let  $n = 9$ . We have  $\sigma(\Pi) \leq 256$ . Partition  $\Pi$  into three sets. Let  $\Pi_1$  be the set of (4, 5)-cycles of  $S_9$ , let  $\Pi_2$  be the set of (3, 6)-cycles of  $S_9$ , and let  $\Pi_3 = \Pi \setminus (\Pi_1 \cup \Pi_2)$ . We will show that  $\sigma(\Pi) \geq \sigma(\Pi_1 \cup \Pi_3) = 172$ . There is no subgroup intersecting both  $\Pi_1$  and  $\Pi_3$ , so we have  $\sigma(\Pi_1 \cup \Pi_3) = \sigma(\Pi_1) + \sigma(\Pi_3)$ . Since there is exactly one maximal subgroup - a group conjugate to  $S_4 \times S_5$  - containing a given (4, 5)-cycle, we have  $\sigma(\Pi_1) = 126$ . Now the set  $\mathcal{H}$  of subgroups  $A_9$  with all maximal intransitive subgroups of  $S_9$  isomorphic to  $S_1 \times S_8$

or  $S_2 \times S_7$  is definitely unbeatable on  $\Pi_3$ , since these subgroups cover  $\Pi_3$  in a disjoint way, and  $|S \cap \Pi_3| \leq 6! \leq |H \cap \Pi_3|$  holds for all subgroups  $S \notin \mathcal{H}$ ,  $H \in \mathcal{H}$  of  $S_9$ . □

If  $n > 2$  is even, then  $\sigma(S_n)$  is asymptotically equal to the index of the largest transitive subgroup of  $S_n$ , that is to  $\frac{1}{2} \binom{n}{n/2}$ . However, we prove more than that.

**Theorem 3.2.** *If  $n > 2$  is even, then  $\sigma(S_n) \sim \frac{1}{2} \binom{n}{n/2}$ . More precisely, for any  $\epsilon > 0$  there exists  $N$  such that if  $n > N$ , then*

$$\frac{1}{2} \binom{n}{n/2} + \left(\frac{1}{2} - \epsilon\right) \sum_{i=0}^{\lfloor n/3 \rfloor} \binom{n}{i} < \sigma(S_n) \leq \frac{1}{2} \binom{n}{n/2} + \sum_{i=0}^{\lfloor n/3 \rfloor} \binom{n}{i}.$$

Note that the term  $\sum_{i=0}^{\lfloor n/3 \rfloor} \binom{n}{i}$  is considerably smaller than  $\frac{1}{2} \binom{n}{n/2}$  for large values of  $n$ .

*Proof.* The set-theoretic union of all maximal imprimitive subgroups conjugate to  $S_{n/2} wr S_2$ , all maximal intransitive subgroups conjugate to some  $S_i \times S_{n-i}$  with  $i \leq \lfloor n/3 \rfloor$ , and  $A_n$  is  $S_n$ . This gives

$$\sigma(S_n) \leq \frac{1}{2} \binom{n}{n/2} + \sum_{i=0}^{\lfloor n/3 \rfloor} \binom{n}{i}.$$

Let  $\Pi_0$  be the set of all  $n$ -cycles of  $S_n$ . For each  $(n-2)/4 < i < \lfloor n/3 \rfloor$  with  $i$  odd, let  $\Pi_i$  be the set of all  $(i, i+1, n-2i-1)$ -cycles of  $S_n$ . Moreover, let  $\mathcal{H}_0$  be the set of all maximal imprimitive subgroups of  $S_n$  conjugate to  $S_{n/2} wr S_2$ . For each  $i > 0$  with  $\Pi_i$  defined above, let  $\mathcal{H}_i$  be the set of all maximal intransitive subgroups of  $S_n$  conjugate to  $S_i \times S_{n-i}$ . The following two claims are to show that if  $n$  is sufficiently large, then  $\mathcal{H}_0$  is definitely unbeatable on  $\Pi_0$ , and for each  $i > 0$  the set  $\mathcal{H}_i$  is definitely unbeatable on  $\Pi_i$ .

**Claim 3.3.** *With the notations above we have the following.*

- (i)  $\Pi_0 \subseteq \bigcup_{H \in \mathcal{H}_0} H$ ;
- (ii)  $\Pi_i \subseteq \bigcup_{H \in \mathcal{H}_i} H$  for all  $i > 0$ ;
- (iii) If  $H_1, H_2 \in \mathcal{H}_0$  and  $H_1 \neq H_2$  then  $\Pi_0 \cap H_1 \cap H_2 = \emptyset$ ;
- (iv) For all  $i$  if  $H_1, H_2 \in \mathcal{H}_i$  and  $H_1 \neq H_2$ , then  $\Pi_i \cap H_1 \cap H_2 = \emptyset$ .

*Proof.* All statements are checked easily. □

**Claim 3.4.** *Let  $n \geq 14$  and let  $S$  be a maximal subgroup of  $S_n$ . Then*

(i)  $|S \cap \Pi_0| < |H \cap \Pi_0|$  for all  $S \notin \mathcal{H}_0, H \in \mathcal{H}_0$ ;

(ii)  $|S \cap \Pi_i| < |H \cap \Pi_i|$  for all  $i$  and all  $S \notin \mathcal{H}_i, H \in \mathcal{H}_i$ .

*Proof.*

(i) If  $S$  is primitive, then

$$|S \cap \Pi_0| \leq |S| < e^n < \frac{(n/2)!^2 \cdot 2}{n} = |H \cap \Pi_0|$$

follows. If  $S$  is imprimitive, then

$$|S \cap \Pi_0| \leq |S| \leq (n/d)!^d \cdot d! < \frac{(n/2)!^2 \cdot 2}{n} = |H \cap \Pi_0|,$$

where  $d$  is the smallest divisor of  $n$  greater than 2. If  $S$  is intransitive, then  $S \cap \Pi_0 = \emptyset$ .

(ii) Fix an index  $i$ . If  $S$  is primitive, then

$$|S \cap \Pi_i| \leq |S| < e^n < \frac{([n/3] - 2)! \cdot (n - [n/3] + 1)!}{[n/3] \cdot (n - 2[n/3] + 1)} \leq |H \cap \Pi_i|$$

follows. If  $S$  is imprimitive, then

$$|S \cap \Pi_i| \leq |S| < (n/d)!^d \cdot d! < \frac{([n/3] - 2)! \cdot (n - [n/3] + 1)!}{[n/3] \cdot (n - 2[n/3] + 1)} \leq |H \cap \Pi_i|,$$

where  $d$  is the smallest divisor of  $n$  greater than 2. Let  $S$  be intransitive. If  $S$  is contained in a group conjugate to  $S_{i+1} \times S_{n-i-1}$ , then

$$\frac{|S \cap \Pi_i|}{|H \cap \Pi_i|} = \frac{(i+1)! \cdot (n-i-1)!}{i! \cdot (n-i)!} < 1.$$

If  $S$  is contained in a group conjugate to  $S_{n-2i-1} \times S_{2i+1}$ , then

$$\frac{|S \cap \Pi_i|}{|H \cap \Pi_i|} = \frac{(n-2i-1)! \cdot (2i+1)!}{i! \cdot (n-i)!} = \frac{\binom{n}{i}}{\binom{n}{2i+1}} < 1.$$

Finally, if  $S$  is contained neither in a group conjugate to  $S_{i+1} \times S_{n-i-1}$ , nor in a group conjugate to  $S_{n-2i-1} \times S_{2i+1}$ , then  $S \cap \Pi_i = \emptyset$ .  $\square$

Now let  $\Pi = \Pi_0 \cup \bigcup_i \Pi_i$ . Let  $\mathcal{H}$  be a set of  $\sigma(\Pi)$  maximal subgroups of  $S_n$  covering  $\Pi$ .

**Claim 3.5.** *With the notations above, we have  $\mathcal{H} = \mathcal{H}_0 \cup \bigcup_i \mathcal{H}_i$  whenever  $n \geq 14$ .*

*Proof.* Let  $\mathcal{H}'$  be the set of all intransitive groups in  $\mathcal{H}$  together with all maximal imprimitive subgroups of  $\mathcal{H}$  conjugate to  $S_{n/2}wrS_2$ . For each  $S \in \mathcal{H}'$ , there exists a unique  $j$  such that  $S \cap \Pi_j \neq \emptyset$ . Moreover, for all  $i$  and all  $S \in \mathcal{H}'$ ,  $H_i \in \mathcal{H}_i$ , we have  $|S \cap \Pi_i| \leq |H_i \cap \Pi_i|$ . This means that the union of all subgroups in  $\mathcal{H}'$  does not contain at least

$$(|\mathcal{H}_0 \cup \bigcup_i \mathcal{H}_i| - |\mathcal{H}'|) \cdot \min\left\{\frac{(n/2)!^2 \cdot 2}{n}, \frac{([n/3] - 2)! \cdot (n - [n/3] + 1)!}{[n/3] \cdot (n - 2[n/3] + 1)}\right\}$$

elements of  $\Pi$ . If this expression is 0, then by Claims 3.3 and 3.4 we are finished. Otherwise, these elements can be covered by at most  $|\mathcal{H}_0 \cup \bigcup_i \mathcal{H}_i| - |\mathcal{H}'|$  transitive groups neither of which is conjugate to  $S_{n/2}wrS_2$ . But this is impossible since

$$\max\{e^n, (n/d)!^d \cdot d!\} < \min\left\{\frac{(n/2)!^2 \cdot 2}{n}, \frac{([n/3] - 2)! \cdot (n - [n/3] + 1)!}{[n/3] \cdot (n - 2[n/3] + 1)}\right\},$$

where  $d$  is the smallest divisor of  $n$  with  $d$  greater than 2. □

The following claim nearly finishes the proof of the theorem.

**Claim 3.6.** *If  $n \geq 14$ , then*

$$\frac{1}{2} \binom{n}{n/2} + \sum_{\substack{(n-2)/4 < i < [n/3] \\ i \text{ odd}}} \binom{n}{i} = \sigma(\Pi) < \sigma(S_n) \leq \frac{1}{2} \binom{n}{n/2} + \sum_{i=0}^{[n/3]} \binom{n}{i}.$$

*Proof.* The first equality is a consequence of Claim 3.5.  $\sigma(\Pi) < \sigma(S_n)$  follows from the fact that  $\sigma(\Pi) \neq \sigma(S_n)$ , since the union of all subgroups of  $\mathcal{H}_0 \cup \bigcup_i \mathcal{H}_i$  does not contain all even permutations. The upper bound was already established. □

Finally, we need to show that for any fixed  $0 < \epsilon < 1/2$ , there exists an integer  $N$ , so that

$$\left(\frac{1}{2} - \epsilon\right) \sum_{i=0}^{[n/3]} \binom{n}{i} < \sum_{\substack{(n-2)/4 < i < [n/3] \\ i \text{ odd}}} \binom{n}{i}$$

holds whenever  $n > N$ . Indeed, for a fixed real number  $0 < \epsilon < 1/2$ , a suitable  $N$  is an integer with the property that whenever  $n > N$ ,



then both

$$\sum_{(n-2)/4 < i < [n/3]} \binom{n}{i} \leq (2 + 2\epsilon) \sum_{\substack{(n-2)/4 < i < [n/3] \\ i \text{ odd}}} \binom{n}{i}$$

and

$$\sum_{0 \leq i \leq (n-2)/4} \binom{n}{i} \leq 2\epsilon \sum_{\substack{(n-2)/4 < i < [n/3] \\ i \text{ odd}}} \binom{n}{i}$$

hold.

□

By Theorems 3.1 and 3.2, to complete the proof of part (1) of Theorem 1.1, we only need to show  $\sigma(S_n) \leq 2^{n-2}$  for  $4 \leq n \leq 12$  and  $n$  even, since if  $n \geq 14$  we have

$$\frac{1}{2} \binom{n}{n/2} + \sum_{i=0}^{[n/3]} \binom{n}{i} < 2^{n-2}.$$

If  $n = 4$ , then  $\sigma(S_4) \leq 4$ , since  $S_4$  is the union of  $A_4$  and the three Sylow 2-subgroups of  $S_4$ . For  $n = 6$ , we have  $\sigma(S_6) \leq 16$ , since  $S_6$  is the union of all imprimitive subgroups conjugate to  $S_3wrS_2$  and all intransitive subgroups conjugate to  $S_1 \times S_5$ . If  $n = 8$ , then  $S_8$  is the union of all imprimitive subgroups conjugate to  $S_4wrS_2$ , all intransitive subgroups conjugate to  $S_2 \times S_6$  and  $A_8$ , hence  $\sigma(S_8) \leq 64$ . For  $n = 10$  we have  $\sigma(S_{10}) \leq 256$ , since  $S_{10}$  is the union of all imprimitive subgroups conjugate to  $S_5wrS_2$ , all intransitive subgroups conjugate to  $S_1 \times S_9$  and all intransitive subgroups conjugate to  $S_3 \times S_7$ . Finally,  $\sigma(S_{12}) \leq 761$ , since  $S_{12}$  may be written as the union of all imprimitive subgroups conjugate to  $S_6wrS_2$ , all intransitive subgroups conjugate to  $S_1 \times S_{11}$ ,  $S_2 \times S_{10}$ , or  $S_3 \times S_9$ , and  $A_{12}$ .

## 4 Alternating groups

**Theorem 4.1.** *Let  $n > 2$  be even. If  $n$  is not divisible by 4, then  $\sigma(A_n) = 2^{n-2}$ . While if  $n$  is divisible by 4, then*

$$\binom{(3n/4) - 1}{(n/4) - 1} \leq \sigma(A_n) - 2^{n-2} \leq \frac{1}{2} \binom{n}{n/2},$$

that is  $\sigma(A_n) \sim 2^{n-2}$ .

*Proof.* The set-theoretic union of all maximal imprimitive subgroups of  $A_n$  conjugate to  $(S_{n/2}wrS_2) \cap A_n$ , and all maximal intransitive subgroups of  $A_n$  conjugate to some  $(S_i \times S_{n-i}) \cap A_n$  with  $1 \leq i \leq (n/2) - 1$  odd is  $A_n$ . This gives

$$\sigma(A_n) \leq \frac{1}{2} \binom{n}{n/2} + \sum_{\substack{i=1 \\ i \text{ odd}}}^{(n/2)-1} \binom{n}{i}.$$

The right-hand-side of the former inequality is equal to  $2^{n-2}$  if  $n$  is not divisible by 4, and is  $\frac{1}{2} \binom{n}{n/2} + 2^{n-2}$  if  $n$  is divisible by 4.

First suppose that  $n$  is not divisible by 4. We have  $\sigma(A_n) \leq 2^{n-2}$ . It is proved below that this estimate is exact. The upper bound is known to be exact for  $n = 6$  by [4], so assume that  $n \geq 10$ . Now let  $\Pi$  be the set of all permutations of  $A_n$  which are the product of exactly two disjoint cycles of odd lengths. We will show that the set  $\mathcal{H}$  of all maximal imprimitive subgroups of  $A_n$  conjugate to  $(S_{n/2}wrS_2) \cap A_n$ , and all maximal intransitive subgroups of  $A_n$  conjugate to some  $(S_i \times S_{n-i}) \cap A_n$  with  $1 \leq i \leq (n/2) - 1$  odd is definitely unbeatable on  $\Pi$  if  $n \geq 10$ , that is  $\sigma(\Pi) \geq 2^{n-2}$  for  $n \geq 10$  and not divisible by 4.

**Claim 4.1.** *Let  $\mathcal{H}$  be as above. If  $n \geq 10$  is not divisible by 4, then*

- (i)  $\Pi \subseteq \bigcup_{H \in \mathcal{H}} H$ ;
- (ii) If  $H_1, H_2 \in \mathcal{H}$  and  $H_1 \neq H_2$ , then  $\Pi \cap H_1 \cap H_2 = \emptyset$ ;
- (iii)  $|S \cap \Pi| \leq |H \cap \Pi|$  for all  $S \notin \mathcal{H}$ ,  $H \in \mathcal{H}$ .

*Proof.*

(i) This was established above.

(ii) This is checked easily.

(iii) First suppose that  $n \geq 14$ . Let  $H \cong (S_k \times S_{n-k}) \cap A_n$  for some  $k$ , and let  $d$  be the smallest divisor of  $n$  greater than 2. If  $S$  is transitive, then

$$|S \cap \Pi| \leq |S| \leq \max\left\{e^n, \frac{(n/d)!^d \cdot d!}{2}\right\} \leq (k-1)! \cdot (n-k-1)! = |H \cap \Pi|$$

holds. If  $S$  is intransitive, then it is either a subgroup of a subgroup in  $\mathcal{H}$ , or  $S \cap \Pi = \emptyset$ . Now let  $n = 10$ . For any maximal subgroup  $S \notin \mathcal{H}$ , the set  $S \cap \Pi$  is either empty, or it contains only  $(5, 5)$ -cycles. In the latter case,  $S$  is either permutation isomorphic to  $(S_2wrS_5) \cap A_{10}$ , or is a proper primitive subgroup of  $A_{10}$ . There are 96 Sylow 5-subgroups in  $(S_2wrS_5) \cap A_{10}$ , and there are at most 36

Sylow 5-subgroups (all of order 5) in a proper primitive subgroup of  $A_{10}$ , hence  $|S \cap \Pi| \leq 384$ . On the other hand, we have  $|H \cap \Pi| \geq 576$  whenever  $H \in \mathcal{H}$ . □

Now let  $n$  be divisible by 4. We have  $\sigma(A_n) \leq 2^{n-2} + \frac{1}{2} \binom{n}{n/2}$ . It is proved below that

$$2^{n-2} + \binom{(3n/4) - 1}{(n/4) - 1} \leq \sigma(A_n).$$

This bound is certainly sharp for  $n = 4$ , since  $\sigma(A_4) = 5$  by [5]. So assume that  $n \geq 8$ . Let  $\Pi_1$  be the set of all permutations of  $A_n$  which are the product of exactly two disjoint cycles of odd lengths. Moreover, let  $\Sigma$  be an arbitrary subset of  $(n/4) + 1$  letters, and let  $\Pi_2$  be the set of all permutations of  $A_n$  which are the product of exactly two disjoint cycles of equal lengths with one cycle moving all letters of  $\Sigma$ . Finally, let  $\Pi = \Pi_1 \cup \Pi_2$ . We will show that the set  $\mathcal{H}$  of all maximal imprimitive subgroups of  $A_n$  conjugate to  $(S_{n/2}wrS_2) \cap A_n$  and intersecting  $\Pi$  nontrivially, and all maximal intransitive subgroups of  $A_n$  conjugate to some  $(S_i \times S_{n-i}) \cap A_n$  with  $1 \leq i \leq \frac{n}{2} - 1$  odd is definitely unbeatable on  $\Pi$  if  $n$  is divisible by 4 and greater than 12. That is  $\sigma(\Pi) \geq 2^{n-2} + \binom{(3n/4)-1}{(n/4)-1}$  for  $n$  divisible by 4 and greater than 12.

**Claim 4.2.** *If  $n$  is divisible by 4, then*

- (i)  $\Pi \subseteq \bigcup_{H \in \mathcal{H}} H$ ;
- (ii) If  $H_1, H_2 \in \mathcal{H}$  and  $H_1 \neq H_2$ , then  $\Pi \cap H_1 \cap H_2 = \emptyset$ ;
- (iii) If  $n \geq 16$ , then  $|S \cap \Pi| \leq |H \cap \Pi|$  for all  $S \notin \mathcal{H}$ ,  $H \in \mathcal{H}$ .

*Proof.*

- (i) This was established above.
- (ii) This is checked easily.
- (iii) If  $n \geq 14$ , then the argument of the proof of Claim 3.4 may be applied. □

Let  $n = 8$ . Any  $(3, 5)$ -cycle is contained in only one maximal subgroup, in a group permutation isomorphic to  $(S_3 \times S_5) \cap A_8$ . So if  $\mathcal{L}$  is a set of  $\sigma(A_8)$  maximal subgroups covering  $A_8$ , then  $\mathcal{L}$  must contain all 56 maximal subgroups permutation isomorphic to  $(S_3 \times S_5) \cap A_8$ . Now consider a given  $(1, 7)$ -cycle. This is contained in either a maximal affine permutation group, or in a one-point

stabilizer of  $A_8$ . It is checked easily that if  $\mathcal{L}$  does not contain all of the 15 maximal affine permutation groups, then the  $(1, 7)$ -cycles can only be covered with all one-point stabilizers. Conversely, it can also be checked that if  $\mathcal{L}$  does not contain all the one-point stabilizers, then it must contain all 15 maximal affine subgroups. In the latter case we have  $\sigma(A_8) \geq 56 + 15 > 69$ , where 69 is the lower bound for  $n = 8$ . For the first case, consider a given  $(2, 6)$ -cycle. This is contained in either a maximal imprimitive group with two or four blocks of imprimitivity, or in a maximal intransitive group permutation isomorphic to  $(S_2 \times S_6) \cap A_8$ . It can be checked easily that in all of these groups the number of  $(2, 6)$ -cycles is at most 192, while the number of  $(2, 6)$ -cycles in  $A_8$  is exactly 3360. This implies that  $\sigma(A_8) \geq 56 + 8 + 17 > 69$ .

Finally, let  $n = 12$ . We have to show that  $\sigma(A_{12}) \geq 1052$ . For  $i = 1, 3$ , and  $5$ , let  $\Pi_i$  be the set of all  $(i, 12 - i)$ -cycles (of  $A_{12}$ ), and let  $\mathcal{L}_i$  be the set of all maximal intransitive subgroups of  $A_{12}$  permutation isomorphic to  $(S_i \times S_{12-i}) \cap A_{12}$ . It is easy to see that  $\mathcal{L}_i$  is definitely unbeatable on  $\Pi_i$  for each  $i$ . (Note that a proper primitive subgroup of  $A_{12}$  contains no  $(3, 9)$ - or  $(5, 7)$ -cycle, and has order at most 95040.) Moreover, all maximal subgroups of  $A_{12}$  intersect at most one of the sets  $\Pi_i$ . This means that  $\sigma(\Pi) = \binom{12}{1} + \binom{12}{3} + \binom{12}{5} = 1024$  where  $\Pi = \Pi_1 \cup \Pi_2 \cup \Pi_3$ . Now let  $\mathcal{L}$  be a set of  $\sigma(A_{12})$  maximal subgroups covering  $A_{12}$ . Since no maximal subgroup different from the subgroups in  $\mathcal{L}_5$  intersects  $\Pi_5$ , we have  $\mathcal{L}_5 \subseteq \mathcal{L}$ . We may suppose that  $\mathcal{L}_1 \subseteq \mathcal{L}$ . For if  $\mathcal{L}$  does not contain  $k > 0$  subgroups of  $\mathcal{L}_1$ , then  $\Pi$  is covered by at least  $1024 - k + (10! \cdot k)/95040 > 1052$  subgroups. We may also assume that  $\mathcal{L}_3 \subseteq \mathcal{L}$ . For suppose that  $\mathcal{L}$  does not contain a subgroup  $H$  of  $\mathcal{L}_3$ . Then  $H \cap \Pi_3$  is covered by subgroups permutation isomorphic to  $(S_4 wr S_3) \cap A_{12}$  or  $(S_3 wr S_4) \cap A_{12}$ . Since such a group can cover at most 288 permutations of  $H \cap \Pi_3$ , a covering of  $H \cap \Pi_3$  must contain at least  $(2! \cdot 8!)/288 = 280$  subgroups. Hence  $|\mathcal{L}| \geq 1024 - \binom{12}{3} + 280 > 1052$ . So we may suppose that all maximal subgroups permutation isomorphic to  $(S_i \times S_{12-i}) \cap A_{12}$  are contained in  $\mathcal{L}$  for  $i = 1, 3$ , and  $5$ . Suppose that  $A_{12}$  acts on the set  $\{1, \dots, 12\}$ . Let  $\Delta$  be the set of all  $(6, 6)$ -cycles of  $A_{12}$  such that the letters 1, 2, 3, and 4 are in the same 6-cycle. The set  $\Delta$  is the disjoint union of the subgroups of a certain set,  $\mathcal{K}$  consisting of  $\binom{8}{2}$  maximal subgroups each permutation isomorphic to  $(S_6 wr S_2) \cap A_{12}$ . We will show that  $\mathcal{K}$  is definitely unbeatable on  $\Delta$ . Indeed, any element of  $\mathcal{K}$  covers 14400 permutations of  $\Delta$ , while an imprimitive maximal subgroup of  $A_{12}$  cannot cover more, a primitive group not isomorphic to  $M_{12}$  has order less than 14400, and finally, the number

of  $(6, 6)$ -cycles contained by the primitive group  $M_{12}$  is only 7920. Since no subgroup in  $\mathcal{L}_i$  intersects  $\Delta$  nontrivially when  $i = 1, 3,$  or  $5,$  we readily see that  $\mathcal{L} \geq 1024 + \binom{8}{2} = 1052.$

□

Now we turn to the case when  $n$  is odd. The possibilities of  $n$  being prime and  $n = 9$  are treated separately.

**Theorem 4.2.** *If  $n > 9$  is odd and not a prime, then*

$$h \leq \sigma(A_n) \leq h + \sum_{i=1}^{\lfloor n/3 \rfloor} \binom{n}{i}$$

where  $h$  denotes the index of the largest transitive proper subgroup of  $A_n.$  In particular,  $\sigma(A_n) \sim h$  and  $\sigma(A_n) > 2^{n-2}.$

*Proof.* Let  $d$  be the smallest prime divisor of  $n,$  and let  $\mathcal{L}$  be the set of all maximal imprimitive subgroups of  $A_n$  conjugate to  $(S_{n/d} \text{wr} S_d) \cap A_n.$  Notice that  $|\mathcal{L}| = h.$  All subgroups permutation isomorphic to  $(S_i \text{wr} S_{n-i}) \cap A_n$  for some  $1 \leq i \leq \lfloor n/3 \rfloor$  together with all subgroups of  $\mathcal{L}$  cover  $A_n.$  This yields the upper bound for  $\sigma(A_n).$  To verify the lower bound, it is sufficient to show that  $\mathcal{L}$  is definitely unbeatable on the set  $\Pi$  of all  $n$ -cycles of  $A_n.$  It is easy to see that the subgroups of  $\mathcal{L}$  cover  $\Pi$  disjointly with each group covering exactly  $h/n$  different  $n$ -cycles. If  $S$  is an imprimitive maximal subgroup of  $A_n$  of index  $k$  intersecting  $\Pi$  nontrivially, then  $|S \cap \Pi| \leq k/n \leq h/n.$  Finally, if  $S$  is a proper primitive subgroup of  $A_n,$  then  $|S| \leq e^n < h/n$  follows for  $n \geq 21,$  and we have  $|S| < h/n$  for  $n = 15.$  (Note that intransitive groups intersect  $\Pi$  trivially.)

□

**Theorem 4.3.** *Let  $n > 3$  be a prime. If  $n$  is not equal to 7, then  $\sigma(A_n) > 2^{n-2},$  and  $\sigma(A_7) \leq 31.$*

*Proof.* First let  $n > 11.$  The alternating group,  $A_n$  contains  $(n-2)!$  Sylow  $n$ -subgroups, while a proper transitive subgroup,  $H$  of  $A_n$  contains at most  $|H|/n.$  Hence the set of  $n$ -cycles of  $A_n$  cannot be covered by less than  $n!/(|G| \cdot (n-1))$  subgroups where  $G$  is a proper transitive group of  $A_n$  of largest possible order. It is sufficient to show that  $2^{n-2} < n!/(|G| \cdot (n-1)),$  that is  $|G| < n!/((n-1) \cdot 2^{n-2}).$  Since  $n$  is prime,  $G$  is primitive. For  $n > 17,$  we have  $|G| < e^n < n!/((n-1) \cdot 2^{n-2}),$  while if  $n = 13,$  then  $|G| \leq 5616 < 13!/(12 \cdot 2^{11})$  holds. Now let  $n = 11.$  Then the number of 11-subgroups contained by  $A_{11}$  is  $9!,$  while a proper primitive subgroup contains at most 144. Hence a covering of  $A_{11}$  has at least  $9!/144 > 2^9$  elements.

Let  $n = 7$ . We will show that  $A_7$  can be covered by at most 31 subgroups. Suppose that  $A_7$  acts on the set  $\Omega$  of size 7. Let  $\alpha \in \Omega$ . Let  $\mathcal{L}$  be the set of all subgroups conjugate to a copy of  $PSL(3, 2)$ , all intransitive subgroups conjugate to  $(S_2 \times S_5) \cap A_7$  satisfying the property that the 2-element orbit does not contain  $\alpha$ , and the stabilizer of  $\alpha$  in  $A_7$ . Notice that  $|\mathcal{L}| = 31$ , and that the subgroups of  $\mathcal{L}$  cover all permutations of the group  $A_7$ . Finally, if  $n = 5$ , then  $\sigma(A_5) = 10$  by [5].

□

**Theorem 4.4.** *If  $p > 23$  is a prime not of the form  $(q^k - 1)/(q - 1)$  where  $q$  is a prime power and  $k$  is an integer, then*

$$(p - 2)! \leq \sigma(A_p) \leq (p - 2)! + \sum_{i=1}^{\lfloor p/3 \rfloor} \binom{p}{i}.$$

*Proof.* By [10], there are only two conjugacy classes of maximal transitive subgroups of  $A_p$ . Both conjugacy classes consist of subgroups isomorphic to the unique subgroup of  $AGL(1, p)$  of index 2. Let this set, the set of all maximal transitive subgroups of  $A_p$  be denoted by  $\mathcal{L}$ . Since  $\mathcal{L}$  is definitely unbeatable on the set of  $p$ -cycles and  $|\mathcal{L}| = (n - 2)!$ , the lower bound for  $\sigma(A_p)$  follows. The upper bound is a consequence of the proof of Theorem 4.2.

□

Later, in Lemma 7.1, we will show that there are infinitely many primes of this kind, so  $(p - 2)!$  is actually an asymptotic estimate for  $\sigma(A_p)$  for such primes,  $p$ .

Now let  $n = 9$ . Among all transitive subgroups of  $A_9$ , the primitive group  $P\Gamma L(2, 8)$  contains the most 9-cycles; it contains exactly 3024. Since the number of 9-cycles in  $A_9$  is  $8!$ , at least  $8!/3024 = 80$  subgroups are needed to cover all 9-cycles. This gives  $\sigma(A_9) \geq 80$ .

## 5 A Mathieu group

In this section we prove Proposition 1.1. We first show that  $\sigma(M_{11}) \leq 23$ .

**Claim 5.1.** *The Mathieu group,  $M_{11}$  is the set-theoretic union of all 11 one-point stabilizers of its action on 11 letters and of all 12 one-point stabilizers of its action on 12 letters. In particular,  $\sigma(M_{11}) \leq 23$ .*

*Proof.* By [6], the permutation character of the action of  $M_{11}$  on 11 letters is  $1_{M_{11}} + \chi_2$ , and the permutation character of the action of  $M_{11}$  on 12 letters is  $1_{M_{11}} + \chi_5$  where  $\chi_2, \chi_5$  are the irreducible characters of  $M_{11}$  indicated in the character table of  $M_{11}$  found in [6]. The character table also shows that for arbitrary  $g \in M_{11}$  we cannot have  $(1_{M_{11}} + \chi_2)(g) = 0$  and  $(1_{M_{11}} + \chi_5)(g) = 0$ . □

To prove  $\sigma(M_{11}) \geq 23$  it is enough to consider only maximal subgroups whose union is  $M_{11}$ .

**Claim 5.2.**

(i) *The only maximal subgroups of  $M_{11}$  containing an element of order 11 are the one-point stabilizers of  $M_{11}$  on 12 letters.*

(ii) *Moreover, let  $\mathcal{L}$  be a set of maximal subgroups whose union is  $M_{11}$ . Then  $\mathcal{L}$  contains all the one-point stabilizers of  $M_{11}$  of its action on 12 letters. In particular,  $\sigma(M_{11}) \geq 12$ .*

*Proof.*

(i) Let  $G$  be a maximal subgroup of  $M_{11} \leq S_{11}$  containing a permutation of order 11. Then  $G$  is transitive and so primitive. A primitive permutation group of degree 11 contained in  $M_{11}$  is either a one-point stabilizer of  $M_{11}$  of its action on 12 letters, or is affine of order 55. Assume that  $G \leq M_{11}$  is affine of order 55 generated by the elements  $g_1$  and  $g_2$  of order 5 and 11, respectively. Represent  $M_{11}$  on 12 points. Now  $G \leq M_{11} \leq S_{12}$  must be intransitive, since  $12 \nmid 55$ . This can only be if  $g_1$  and  $g_2$  fixes the same point. Thus  $G$  is contained in a one-point stabilizer of  $M_{11} \leq S_{12}$ .

(ii) Represent  $M_{11}$  on 12 letters. For any letter  $\alpha$ , there exists a permutation  $g$  of  $M_{11}$  of order 11 fixing  $\alpha$ . By (i), the only maximal subgroup of  $M_{11}$  containing  $g$  is the one-point stabilizer of  $\alpha$ . □

We recall the following fact from [6].

**Claim 5.3.** *A maximal subgroup of  $M_{11}$  different from a one-point stabilizer of  $M_{11}$  of its action on 11 letters and different from a one-point stabilizer of  $M_{11}$  of its action on 12 letters has order at most 144.*

By the character table of  $M_{11}$  in [6], we see that the set  $\Pi$  of group elements  $g$  satisfying  $(1_{M_{11}} + \chi_2)(g) = 1$  and  $(1_{M_{11}} + \chi_5)(g) = 0$  is exactly the set of 1980 elements of order 8 in  $M_{11}$ . By Claim 5.3, the set of 11 copies of  $M_{10}$  is definitely unbeatable on  $\Pi$ . This, together with Claim 5.2, implies  $\sigma(M_{11}) \geq 23$ . By Claim 5.1, we now obtain  $\sigma(M_{11}) = 23$  which proves Proposition 1.1.

## 6 On some infinite series of $\sigma$

We start with a theorem which was conjectured by Ramanujan in 1913 and was confirmed by Nagell [17] in 1960.

**Theorem 6.1** (Nagell, [17]). *The only solutions to the Diophantine equation  $x^2 + 7 = 2^n$  are  $(n, x) = (3, 1), (4, 3), (5, 5), (7, 11)$  and  $(15, 181)$ .*

This is used to prove

**Theorem 6.2.** *Any positive integer is a member of at most one of the following infinite series.*

- (1)  $\mathcal{A} = \{2^n\}_{n=5}^\infty$ ;
- (2)  $\mathcal{B}_p = \{\frac{1}{2}p^n(p^n + 1) + 1\}_{n=1}^\infty$  where  $p$  is an odd prime;
- (3)  $\mathcal{C} = \{\frac{1}{2}2^n(2^n + 1)\}_{n=2}^\infty$ .

*Proof.* Suppose that  $2^n = \frac{1}{2}p^k(p^k + 1) + 1$  where  $n \geq 5$ ,  $k \geq 1$  and  $p$  is an odd prime. After multiplying both sides of the equation by 8, we obtain  $2^{n+3} = (2p^k + 1)^2 + 7$ . By Theorem 6.1, we get a contradiction. Suppose that  $2^n = 2^{k-1}(2^k + 1)$  where  $n \geq 5$  and  $k \geq 2$ . Notice that the right-hand-side of this equation is divisible by an odd prime, while the left-hand-side is not. Finally, no positive integer is an element of both  $\mathcal{B}_p$  and  $\mathcal{C}$  for any odd prime  $p$ , since the function  $\frac{1}{2}x(x + 1)$  is strictly increasing on the set of positive integers by a difference of at least 2 whenever  $x > 2$ . □

## 7 An application

We will show that  $\alpha'_n = \beta'_n$  for  $n$  a prime greater than 23 and not of the form  $(q^k - 1)/(q - 1)$  where  $q$  is a prime power and  $k$  is an integer. But before we do this, we prove

**Lemma 7.1.** *The set of primes not of the form  $(q^k - 1)/(q - 1)$  where  $q$  is a prime power and  $k$  is an integer has density 1 in the set of all primes.*

*Proof.* The Prime Number Theorem states that there are asymptotically  $x/\ln x$  primes less than  $x$ . Now let us count the primes less than  $x$  which are of the form  $(q^k - 1)/(q - 1)$  for some prime power  $q$  and some positive integer  $k$ . If  $k = 2$ , then  $q$  has to be a power of 2, and so there are at most  $\log_2 x$  such primes. For each  $k \geq 3$ , there are at most  $\sqrt{x}$  such primes. Since  $k$  cannot exceed  $\log_2 x$ ,



there are at most  $(\sqrt{x} + 1) \log_2 x$  such primes in total. We conclude that the sequence

$$\frac{x/\ln x - (\sqrt{x} + 1) \log_2 x}{x/\ln x}$$

tends to 1 as  $x$  goes to infinity. □

Now we turn to the proof of Theorem 1.2. Let  $p$  be a prime greater than 23 and satisfying the condition of Lemma 7.1. By part (1) of Theorem 1.1, we see that  $2^{p-1} = \sigma(S_p) \geq \beta'_p \geq \alpha'_p$ . Hence it is sufficient to show that  $2^{p-1} \leq \alpha'_p$ . Suppose that  $S_p$  is acting naturally on a set  $\Omega$  of size  $p$ . For each  $1 < i \leq (p-1)/2$  and each subset of  $\Omega$  of size  $i$ , say  $\Delta$ , choose an  $(i, p-i)$ -cycle of  $S_p$  such that all elements of  $\Delta$  are moved by the cycle of length  $i$ . Let the set of all permutations so obtained be  $\Pi_0$ . Now choose an arbitrary  $n$ -cycle, say  $g$ . This permutation is contained in a unique copy of  $AGL(1, p)$ , say in  $G$ . Since any  $(1, p-1)$ -cycle is contained in at most  $\varphi(p-1) \cdot p(p-1)$  distinct copies of  $AGL(1, p)$  where  $\varphi(p-1)$  denotes the Euler function of the integer  $p-1$ , and since  $(p-2)! - 1 > \varphi(p-1) \cdot p^2(p-1)$ , it follows that for each  $\omega \in \Omega$  we may choose a  $(1, p-1)$ -cycle,  $g_\omega$  fixing  $\omega$  and not contained in  $G$  such that if  $\omega \neq \omega'$  are distinct elements of  $\Omega$ , then there is no subgroup of  $S_p$  isomorphic to  $AGL(1, p)$  containing both  $g_\omega$  and  $g_{\omega'}$ . Now let  $\Pi$  be the set consisting of all elements of  $\Pi_0$  together with  $g$  and all  $g_\omega$  with  $\omega \in \Omega$ . Notice that  $|\Pi| = 2^{p-1}$ . Now it is easy to see that any two distinct permutations of  $\Pi$  generate a transitive subgroup of  $S_p$  contained neither in  $A_p$  nor in any conjugate of  $AGL(1, p)$ . So by [10], it follows that any two distinct elements of  $\Pi$  generate  $S_p$ . Hence we have  $2^{p-1} \leq \alpha'_p$ , which completes the proof of Theorem 1.2.

### Acknowledgements

Thanks are due to L. Pyber who introduced me to this subject, and to Á. Pintér who kindly pointed out Theorem 6.1. I am also very grateful to L. Serena and the referee for many valuable remarks. This work was started at the University of Szeged in Hungary, continued at the University of Birmingham in England, and completed at the University of Southern California in the United States. The author was partially supported by the Hungarian National Foundation for Scientific Research Grant TO34878, by the School of Mathematics and Statistics at the University of Birmingham in England, and by NSF Grant DMS 0140578.

## References

- [1] Brown, R. Minimal covers of  $S_n$  by abelian subgroups and maximal subsets of pairwise noncommuting elements. *J. Combin. Theory Ser. A* **49**, (1988), no. 2, 294-307.
- [2] Brown, R. Minimal covers of  $S_n$  by abelian subgroups and maximal subsets of pairwise noncommuting elements. II. *J. Combin. Theory Ser. A* **56**, (1991), no. 2, 285-289.
- [3] Bruckheimer, M; Bryan, A. C; Muir, A. Groups which are the union of three subgroups. *Amer. Math. Monthly* **77**, (1970), 52-57.
- [4] Bryce, R. A; Fedri, V; Serena, L. Subgroup coverings of some linear groups. *Bull. Austral Math. Soc.* **60**, (1999), no. 2, 227-238.
- [5] Cohn, J. H. E. On  $n$ -sum groups. *Math. Scand.* **75**, (1994), no. 1, 44-58.
- [6] Conway, J. H; Curtis, R. T; Norton, S. P; Parker, R. A; Wilson, R. A. Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. *Oxford University Press*, Eynsham, (1985).
- [7] Dixon, J. D; Mortimer, B. The primitive permutation groups of degree less than 1000. *Math. Proc. Cambridge Philos. Soc.* **103** (1988), no. 2, 213–238.
- [8] Erdős, P; Straus, E. G. How abelian is a finite group? *Linear and Multilinear Algebra* **3**, (1975/76), no. 4, 307-312.
- [9] The GAP Group, GAP — Groups, Algorithms, Programming, Version 4.2; Aachen, St Andrews, (1999). (<http://www-gap.dcs.st-and.ac.uk/gap>).
- [10] Guralnick, R. M. Subgroups of prime power index in a simple group. *J. Algebra* **81**, (1983), 304-311.
- [11] Haber, S; Rosenfeld, A. Groups as unions of proper subgroups. *Amer. Math. Monthly* **66**, (1959), 491-494.
- [12] Holmes, P. E. Subgroup coverings of some sporadic groups, preprint.
- [13] Jungnickel, D; Storme, L. Packing and covering groups with subgroups. *J. Algebra* **239**, (2001), no. 1, 191-214.

- [14] Lucido, M. S. On the covers of finite groups. *Groups St. Andrews 2001* Vol. II, 395-399, London Math. Soc. Lecture Note Ser., **305**, Cambridge Univ. Press, Cambridge, 2003.
- [15] Maróti, A. On the orders of primitive groups. *J. Algebra* **258** (2002), no. 2, 631-640.
- [16] Mason, D. R. On coverings of a finite group by abelian subgroups. *Math. Proc. Cambridge Philos. Soc.* **83**, (1978), no. 2, 205-209.
- [17] Nagell, T. The Diophantine equation  $x^2 + 7 = 2^n$ . *Ark. Math.* **4**, (1960), 185-187.
- [18] Neumann, B. H. Groups covered by finitely many cosets. *Publ. Math. Debrecen* **3**, (1954), 227-242.
- [19] Neumann, B. H. Groups covered by permutable subsets. *J. London Math. Soc.* **29**, (1954), 236-248.
- [20] Pyber, L. The number of pairwise noncommuting elements and the index of the centre in a finite group. *J. London Math. Soc.* (2) **35**, (1987), no. 2, 287-295.
- [21] Pyber, L. How abelian is a finite group? The mathematics of Paul Erdős, I, 372-384, *Algorithms Combin.* **13**, Springer, Berlin, 1997.
- [22] Serena, L. On finite covers of groups by subgroups. *Advances in group theory* 2002, 173-190, Aracne, Rome, 2003.
- [23] Scorza, G. I gruppi che possono pensarsi come somma di tre loro sottogruppi. *Boll. Un. Mat. Ital.* **5**, (1926), 216-218.
- [24] Tomkinson, M. J. Groups as the union of proper subgroups. *Math. Scand.* **81**, (1997), 191-198.