On the indices of maximal subgroups and the normal primary coverings of finite groups

J. Group Theory **22** (2019), 1015–1034
DOI 10.1515/jgth-2018-0212

On the indices of maximal subgroups and the normal primary coverings of finite groups

Francesco Fumagalli

Communicated by Andrea Lucchini

Abstract. We define and study two arithmetic functions γ_0 and η, having domain the set of all finite groups whose orders are not prime powers. Namely, if G is such a group, we call $\gamma_0(G)$ the *normal primary covering number* of G; this is defined as the smallest positive integer k such that the set of primary elements of G is covered by k conjugacy classes of proper (pairwise non-conjugate) subgroups of G. Also we set $\eta(G)$, the *indices covering number* of G, to be the smallest positive integer h such that G has h proper subgroups having coprime indices. This second function is an upper bound for γ_0, and it is much friendlier. The study of these functions for arbitrary finite groups reduces immediately to the non-abelian simple ones. We therefore apply CFSG to obtain bounds and interesting properties for γ_0 and η. Open questions on these functions are reformulated in pure number-theoretical terms and lead to problems concerning the distributions and the representations of prime numbers.

Introduction

A finite non-trivial group G can never be the set-theoretic union of all the conjugates of a fixed proper subgroup H. For the question of whether there are elements outside $\bigcup_{g \in G} H^g$ possessing some interesting group theoretical properties, a significant answer is given in [9, Theorem 1]. The authors prove that, for any $H < G$, there always exists an element of prime power order which does not lie in $\bigcup_{g \in G} H^g$. An equivalent statement is that every non-trivial finite transitive permutation group has a derangement (i.e., an element acting fixed-point-free) of prime power order. This result – which relies on the Classification of Finite Simple Groups – permits the authors to prove that there is no global field extension $\mathbb{L} \supseteq \mathbb{K}$ such that the reduced Brauer group $B(\mathbb{L}/\mathbb{K})$ is finite, a theorem of significant importance in algebraic number theory.

In this paper, given a finite group G, whose order is not a prime power, we let G_0 be the set of primary elements of G (we recall that a primary element of a group is an element having prime power order) and, along the lines of [2–5, 7], define a *normal primary covering for G* to be any collection of complete conjugacy classes of subgroups of G whose union contains G_0. The *normal primary covering number of* G is by definition the cardinality of a minimal normal primary covering, namely, the smallest natural number $\gamma_0(G)$ such that

$$G_0 \subseteq \bigcup_{i=1}^{\gamma_0(G)} \bigcup_{g \in G} H_i^g$$

for some proper – pairwise non-conjugate – subgroups H_i of G.

Theorem 1 in [9] can therefore be reformulated by saying that $\gamma_0(G) \geq 2$.

We are interested in bounding the function γ_0. For this, we define a second function on the set of finite groups G, whose orders are not prime powers, by setting $\eta(G)$ to be the smallest number of proper subgroups of G having coprime indices. We call $\eta(G)$ the *indices covering number of* G. Note that $\eta(G)$ is always an upper bound for $\gamma_0(G)$. It happens that this second function is much friendlier than γ_0. Most of the paper is addressed to the study of η, which immediately reduces to the case of finite non-abelian simple groups (Proposition 1). We therefore make use of the Classification theorem.

If, following the number-theoretic literature (for instance, [20]), we denote with $\omega(n)$ the number of distinct prime divisors of n; our results on alternating groups can be summarized in the following theorem.

Theorem A. *If A_n is the alternating group of degree $n \geq 5$, then*

(1) $\eta(A_n) \leq \omega(n) + 1$ *(Lemma* 2*),*

(2) $\eta(A_n) = 2$ *if and only if n is a prime power (Theorem* 1*),*

(3) $\liminf_{\omega(n)\to\infty} \eta(A_n) = 3$ *(Theorem* 2*).*

For groups of Lie type, we manage to prove the following (Theorems 3 and 4):

Theorem B. *If G is a simple group of Lie type of rank n, then $\eta(G)$ is bounded above by a linear function in $\omega(n)$. In particular, if G is an exceptional group, $\eta(G)$ is uniformly bounded.*

Tables 1, 2 and 3 provide upper bounds (which may be close to best possible) for the classical, the exceptional and the sporadic simple groups, respectively.

The last part of the paper is devoted to normal primary coverings and the related function γ_0. In particular, we show that γ_0 and η are in general different functions (Proposition 6).

The paper leaves open the following questions.

Question A. Do there exist positive constants C and D such that, for every finite group G (whose order is not a prime power), $\gamma_0(G) \leq C$ and $\eta(G) \leq D$?

Of course, if η is uniformly bounded, then so is γ_0. Our analysis allows us to reduce the above question (relative to the case of alternating groups) to problems concerning distributions and representations of prime numbers. In particular, Question A for the function η and when G is alternating, can be restated in the following purely number-theoretical form.

Question B. Given a positive integer n, let $\eta(n)$ be the smallest number such that

$$\gcd\left\{\binom{n}{m_1},\dots,\binom{n}{m_{\eta(n)}}\right\} = 1 \quad \text{if } n \text{ is odd},$$

$$\gcd\left\{\binom{n}{m_1},\dots,\binom{n}{m_{\eta(n)}},\frac{1}{2}\binom{n}{n/2}\right\} = 1 \quad \text{if } n \text{ is even},$$

for some $1 \le m_i < n/2$ for every i. Is it true that $\limsup \eta(n) < +\infty$?

1 Some basic results for the function $\eta(G)$

As stated in the introduction, for every finite group G whose order is not a prime power, we define the *indices covering number of* G, $\eta(G)$, to be the smallest number of proper subgroups of G having coprime indices, i.e., $\eta(G) = k$ if and only if there are k (and not fewer) proper subgroups of G, say, $H_0, H_1, \dots, H_{k-1}$, with the property

$$\gcd(|G:H_0|, |G:H_1|, \dots, |G:H_{k-1}|) = 1. \tag{CI}$$

The following lemma collects some elementary properties. We recall that, following the number-theoretic literature [20], we set $\omega(n)$ for the number of distinct prime divisors of a positive integer n. The proof of the lemma is left to the reader.

Lemma 1. *Let G be a finite group whose order is not a prime power. Then the following holds.*

(1) $\eta(G) \le \omega(|G|)$.

(2) *$\eta(G)$ can always be realized by taking a collection of maximal subgroups H_i of G (for $i = 0, 1, \dots, \eta(G) - 1$).*

(3) *If $\eta(G) = 2$, then $G = H_0 H_1$ (Poincaré lemma).*

(4) *If N is a proper normal subgroup of G, then $\eta(G) \le \eta(G/N)$, and if G/N is a p-group, for some prime p, then $\eta(G) = 2$.*

The following proposition is easy but crucial.

Proposition 1. *Let G be a finite group whose order is not a prime power. Then $\eta(G) = 2$ if $G' \ne G$. In particular, if G is a soluble group or an almost simple group which is not simple, then $\eta(G) = 2$.*

Proof. By Lemma 1 (4) with $N = G'$, it is enough to show that the result holds for G a finite abelian group of non-prime power order. In this case, choose a prime p dividing $|G|$, and take as H_0 a (maximal) subgroup containing the Sylow p-subgroup P of G and as H_1 a maximal one containing the complement of P in G. □

In virtue of Proposition 1, the study of the function η takes its interest only for perfect groups and, in particular, it immediately reduces to the case of finite non-abelian simple groups. However, the following remark shows that there are perfect groups G having $\eta(G) < \eta(G/N)$, for every proper non-trivial normal subgroup N.

Remark 1. Let $G = A_6 \times \mathrm{PSL}_2(13)$. By looking at the list of maximal subgroups (for instance, in [6]), it is immediate to see that $\eta(A_6) = \eta(\mathrm{PSL}_2(13)) = 3$. However, G has maximal subgroups isomorphic to $A_6 \times A_4$ and $A_5 \times \mathrm{PSL}_2(13)$, and therefore $\eta(G) = 2$.

From now on, we assume that G is a finite non-abelian simple group. We separately treat the various cases according to CFSG.

2 The case of alternating groups

Let A_n be the alternating group of degree $n \geq 5$ that is acting on the natural set $\{1, 2, \dots, n\}$. We start with this simple lemma.

Lemma 2. $\eta(A_n) \leq \omega(n) + 1$.

Proof. Take $H_0 = \mathrm{Stab}_{A_n}(1)$ to be the stabilizer of point 1. Then $H_0 \simeq A_{n-1}$ has index n in A_n. For every prime p_i dividing n, let H_i be a maximal subgroup containing a Sylow p_i-subgroup of A_n. Then the collection of subgroups

$$\mathcal{H} = \{H_0, H_1, \dots, H_{\omega(n)}\}$$

has property (CI), and therefore $\eta(A_n) \leq \omega(n) + 1$. □

Lemma 2 in particular implies $\eta(A_n) = 2$ whenever n is a prime power. We will prove that the converse of this statement holds (see Theorem 1).

From now on, assume that the degree n is not a prime power.

Moreover, we make the following important assumption. We always include a one-point stabilizer (as subgroup H_0) in a list of maximal subgroups of A_n whose cardinality is at least $\eta(A_n) + 1$, meaning that if $\eta(A_n) = k$ and there is a list $\mathcal{H} = \{H_1, H_2, \dots, H_k\}$ of maximal subgroups of coprime indices and not containing the stabilizer of a single point, then we consider the extended list $\widehat{\mathcal{H}} = \mathcal{H} \cup \{H_0\}$. The family $\widehat{\mathcal{H}}$ still has property (CI). The advantage of this choice is evident: the computation of $\eta(A_n)$ is reduced to finding which maximal subgroups of A_n contain Sylow p-subgroups for the various primes p that divide n.

The maximal subgroups of A_n split in three different classes, according to their action on $\{1, 2, \dots, n\}$: intransitive subgroups, imprimitive and primitive ones.

The primitive maximal subgroups are unnecessary for the computation of the indices covering number; this is a consequence of the following famous result of C. Jordan.

Lemma 3. *No proper primitive subgroup of A_n contains p-cycles for primes p, where $p \leq n - 3$. In particular, no primitive maximal subgroup of A_n contains a Sylow p-subgroup for p a proper divisor of n.*

Proof. We refer to [24, Theorem 13.9]. □

Before considering in detail the other cases of maximal subgroups of A_n, we introduce some more notation.

Given two natural numbers n and $b \geq 2$, if

$$n = n_0 + n_1 b + n_2 b^2 + \cdots + n_k b^k$$

is the expansion of n in base b, we write

$$[n]_b = (n_0, n_1, \dots, n_k).$$

Also, if m and d are other positive numbers, we write

$$\begin{aligned} [n]_b \leq [m]_b \qquad & \text{if } n_i \leq m_i, \\ [n]_b = d \cdot [m]_b \quad & \text{if } n_i = d \cdot m_i \end{aligned}$$

for all $i = 0, 1, \dots, \max\{\lfloor \log_p(n) \rfloor, \lfloor \log_p(m) \rfloor\}$. We recall also that if p is a prime, the p-adic value of $n!$, namely, the exponent of the p-part of $n!$, is usually denoted by $v_p(n!)$ and is given by

$$v_p(n!) = \sum_{i \geq 1} \lfloor n/p^i \rfloor \tag{2.1}$$

and, equivalently, if $[n]_p = (n_0, n_1, \dots, n_k)$, then

$$v_p(n!) = \sum_{i=1}^{k} n_i \cdot \frac{p^i - 1}{p - 1} \tag{2.2}$$

(see, for instance, [20, Theorem 1.12] or [8, Example 2.6.8]).

Consider now the case of intransitive maximal subgroups of A_n. Any such subgroup is the setwise stabilizer of a set of cardinality m, for some $1 \le m < n/2$, being therefore isomorphic to $(S_m \times S_{n-m}) \cap A_n$ and having index $\binom{n}{m}$. For convenience, we choose a prototype of these subgroups by letting X_m be the stabilizer of the set $\{1, 2, \dots, m\}$ in A_n.

The next lemma says exactly when a maximal intransitive subgroup contains a Sylow p-subgroup of A_n, for some prime number p which divides n. This is basically a result of Ernst Kummer [15, pp. 115–116]. See also [21, Lemma 3.1] and [11] for an overview.

Lemma 4. *Let $1 \le m < n/2$ and p a prime number, $p \le n$. The following conditions are equivalent.*

(1) *p does not divide $\binom{n}{m}$;*

(2) *X_m contains a Sylow p-subgroup of A_n;*

(3) *any p-element of A_n lies in a conjugate of X_m;*

(4) $[m]_p \le [n]_p$.

Proof. Since $|A_n : X_m| = |S_n : S_m \times S_{n-m}| = \binom{n}{m}$, we prove the analogous statement for the groups $S_m \times S_{n-m} \le S_n$ instead of $X_m \le A_n$.

The implications (1) $\Rightarrow$ (2) $\Rightarrow$ (3) are trivial consequences of Sylow theorems. We prove (3) $\Rightarrow$ (4). Write the p-adic expansions of n and m respectively as

$$[n]_p = (n_0, n_1, \dots, n_l) \quad \text{and} \quad [m]_p = (m_0, m_1, \dots, m_l),$$

where $l = \lfloor \log_p n \rfloor$ and $m_i = 0$ for $i = \lfloor \log_p m \rfloor + 1, \dots, l$. The group S_n contains p-elements whose cycle type consists of exactly n_i cycles of length p^i, for $i = 1, 2, \dots, l$. By (3), let g be such an element of X_m. The set $\{1, 2, \dots, m\}$ being the union of $\langle g \rangle$-orbits, we have $m_i \le n_i$ for every $i = 0, 1, \dots, \lfloor \log_p(n) \rfloor$, i.e., $[m]_p \le [n]_p$.

Finally, assuming (4), from formula (2.2), it is straightforward to see that

$$v_p(n!) = v_p(m!) + v_p((n-m)!),$$

which is equivalent to (1). □

Corollary 1. *If any of the conditions* (1)–(4) *of Lemma* 4 *is verified, then the p-part of n divides both m and $n - m$.*

We consider now the case of imprimitive maximal subgroups. Any such subgroup of A_n is the stabilizer of a partition of $\{1, 2, \dots, n\}$ into equal-sized subsets, and therefore it is isomorphic to the wreath product $(S_d \wr S_{n/d}) \cap A_n$, for some proper non-trivial divisor d of n, its index in A_n being

$$\frac{n!}{(d!)^{n/d} \cdot (n/d)!} =: I_{n,d}.$$

As before, for convenience, we set W_d to be the stabilizer in A_n of the partition

$$\big\{\{1,2,\ldots,d\},\{d+1,d+2,\ldots,2d\},\ldots,\{n-d+1,n-d+2,\ldots,n\}\big\}.$$

We prove the analogous result of Lemma 4, which already appeared in [23, Lemma 2] (see also [21, Lemma 3.2]).

Lemma 5. *Let d be a proper non-trivial divisor of n. Then $p \nmid I_{n,d}$, i.e., the imprimitive maximal subgroup W_d contains a Sylow p-subgroup of A_n if and only if one of the following is satisfied:*

(i) *either d is a p-power, or*

(ii) *$n/d < p$ and $[n]_p = n/d \cdot [d]_p$.*

Proof. For convenience, we set $l = n/d$. Since $I_{n,d} = |S_n : S_d \wr S_l|$, we prove the lemma by considering the subgroup $H_d := S_d \wr S_l$ of S_n, instead of W_d in A_n.

We first assume that H_d contains a p-Sylow subgroup of S_n, equivalently that $v_p(n!) = l \cdot v_p(d!) + v_p(l!)$.

As $d > 1$, p divides $\frac{n!}{l!}$, and therefore $v_p(n!) > v_p(l!)$, showing that $v_p(d!) > 0$, i.e., $d \geq p$. We write

$$[n]_p = (n_0, n_1, \ldots, n_u),$$
$$[d]_p = (d_0, d_1, \ldots, d_h),$$
$$[l]_p = (l_0, l_1, \ldots, l_k).$$

Note that $u = \lfloor \log_p n \rfloor$ is either $h+k$ or $h+k+1$. If $u = h+k+1$, the group S_n contains cycles of length p^{h+k+1}. Note that none of these p-elements belong to H_d since, as $p^{h+k+1} > d$, the support of such an element must meet at least p^{k+1} blocks, which do not exist. Thus $u = h+k$. Assume now that $k \geq 1$, equivalently that $l \geq p$. Consider a cycle of length p^{h+k} that lies in H_d. Such an element would cyclically permute p^k blocks, and its support must be a union of complete blocks; this shows that d divides p^{h+k}, i.e., condition (i) holds. Now let $k = 0$, and show (ii), i.e., $n_i = l \cdot d_i$ for any $i = 0, 1, \ldots, u$. Arguing by contradiction, we set r to be the largest integer for which $n_r > l \cdot d_r$ (of course, $n_u \geq l \cdot d_u$). The full symmetric group S_n contains p-elements which are products, for i running from r to u, of n_i disjoint cycles of length p^i each. However, for similar reasons as before, such an element cannot stay in H_d, which contradicts the fact that H_d contains a Sylow p-subgroup. Therefore, we proved

$$n_i \leq l \cdot d_i \quad \text{for every } i = 0, 1, \ldots, u. \tag{2.3}$$

But then $n_u = l \cdot d_u$ and, from this and equation (2.3), it is then straightforward to prove $n_i = l \cdot d_i$ for every $i = 0, 1, \ldots, u$.

Conversely, first assume condition (i), and let $d = p^r$, so that the p-adic expansions of n and $l = n/d$ are, respectively,

$$[n]_p = (0, \ldots, 0, n_r, \ldots, n_u)$$
$$[l]_p = (n_r, \ldots, n_u),$$

where the first line starts with r zeros, n being divisible by p^r.

We have

$$\begin{aligned} l \cdot v_p(d!) + v_p(l!) &= \frac{n}{d} \cdot \frac{p^r - 1}{p - 1} + \sum_{i=0}^{u-r} n_{r+i} \frac{p^i - 1}{p - 1} \\ &= \sum_{i=0}^{u-r} n_{r+i} p^i \cdot \frac{p^r - 1}{p - 1} + \sum_{i=0}^{u-r} n_{r+i} \frac{p^i - 1}{p - 1} \\ &= \sum_{i=0}^{u-r} n_{r+i} \left(p^i \frac{p^r - 1}{p - 1} + \frac{p^i - 1}{p - 1} \right) \\ &= \sum_{i=0}^{u-r} n_{r+i} \left(\frac{p^{r+i} - 1}{p - 1} \right) = v_p(n!). \end{aligned}$$

Now assume (ii), and write $[d]_p = (d_0, \ldots, d_h)$ and $[n]_p = (l d_0, \ldots, l d_h)$. Thus

$$l \cdot v_p(d!) + v_p(l!) = l \cdot \sum_{i \geq 1} d_i \frac{p^i - 1}{p - 1} = \sum_{i \geq 1} l \cdot d_i \frac{p^i - 1}{p - 1} = v_p(n!),$$

which completes the proof. □

Lemma 5 has these easy but important consequences.

Corollary 2. *Let d be a non-trivial proper divisor of n.*

(1) *If d is a p-power, then W_d contains Sylow p-subgroups of A_n, but not Sylow q-subgroups for any other prime $q \neq p$ dividing n.*

(2) *If W_d contains a Sylow p_1-subgroup, with p_1 the smallest prime divisor of n, then d is a p_1-power and W_d does not contain any other Sylow p-subgroup for $p \neq p_1$ dividing n.*

Proof. (1) Let $d = p^r$, and let q be a different prime dividing n. Then q divides n/d, forcing $n/d \geq q$. By the previous lemma, W_d cannot contain a Sylow q-subgroup of A_n.

(2) If d is not a power of p_1 and W_d contains a Sylow p_1-subgroup of A_n, by Lemma 5, we have $n/d < p_1$, which is a contradiction since p_1 is the smallest prime divisor of n. □

Proposition 2. *Let n be different from a prime power. If n is odd, the maximal intransitive subgroups of A_n are enough to produce a set of (maximal) subgroups of A_n realizing $\eta(A_n)$. If n is even, there always exists a set of (maximal) subgroups realizing $\eta(A_n)$ consisting either entirely of intransitive subgroups or of intransitive subgroups and the subgroup $W_{n/2}$.*

Proof. Let $\mathcal{H}$ be a collection of maximal subgroups realizing $\eta(A_n)$. Assume that $\mathcal{H}$ contains some primitive maximal subgroup R. By Lemma 3, the only prime divisors of $|A_n|$ that do not divide the index of R are greater than or equal to $n-2$. Since n is not a prime power, we may replace this subgroup R with the intransitive subgroup X_1 in $\mathcal{H}$.

Assume now that $\mathcal{H}$ contains some imprimitive maximal subgroup W_d, for some proper non-trivial divisor d of n. By Lemma 5, if d is not a prime power, the only primes r not dividing $I_{n,d}$ are those for which $n/d < r$ and $[n]_r = n/d[d]_r$. Note that this implies $[d]_r \leq [n]_r$, and so, by Lemma 4, these primes r do not divide $\binom{n}{d}$. As long as $n \neq 2d$, we may therefore substitute W_d with X_d in $\mathcal{H}$. Suppose now that d is a prime power, say, $d = p^a$. If $p^{a+1} \mid n$, then note that, in virtue of Lemma 5, the primes r not dividing $I_{n,d}$ also do not divide $I_{n,dp}$; therefore, the subgroup W_{dp} may take the place of W_d in $\mathcal{H}$. Without loss of generality, we assume therefore that p^{a+1} does not divide n. Of course, W_d contains Sylow p-subgroups and possibly Sylow r-subgroups for those primes r such that $n/d < r$ and $[n]_r = n/d[d]_r$. As before, by Lemma 4, neither p nor any of these r's divide $\binom{n}{d}$, and again if $n \neq 2d$, the subgroup X_d can substitute W_d in the list $\mathcal{H}$. □

Example 1 below shows that, in some situations, the presence of $W_{n/2}$ is necessary for $\mathcal{H}$ to realize $\eta(A_n)$.

We can now prove the already anticipated characterization of alternating groups having indices covering number equal to two.

Theorem 1. *Let $n \geq 5$. Then $\eta(A_n) = 2$ if and only if n is a prime power.*

Proof. One implication is obvious from the remark after Lemma 2.

Let us assume that $\eta(A_n) = 2$ and prove that n is a prime power. A direct inspection of the Atlas [6] shows that $\eta(A_6) = \eta(A_{10}) = 3$; therefore, we assume $n \geq 12$. Let A and B be two proper subgroups of coprime indices; in particular, we have $A_n = AB$. According to [16, Theorem D] up to changing A with B, we have $A \simeq X_m$ and that B is m-homogeneous (i.e., transitive on the set of m-subsets of $\{1, 2, \ldots, n\}$), for some $1 \leq m \leq 5$. By [8, Theorem 9.4B], if $m \geq 2$, then either B is 2-transitive or $m = 2$ and $ASL_1(q) \leq B \leq A\Gamma L_1(q)$, with $n = q \equiv 3 \pmod 4$, acting in the usual permutation representation on the field of q elements. Since, in the latter case, we clearly have that n is a prime power, we assume that B is 2-transitive and therefore primitive. Now B contains a Sylow p-subgroup of A_n for any p dividing $\binom{n}{m}$, the index of A. Let p_1 be the smallest of these primes. If $n - p_1 \geq 3$, we reach a contradiction by Lemma 3. Therefore, $n - p_1 \leq 2$, and the only possible situations arise when $n = 7$, $p_1 = 5$ and $m = 3$ or 4, which is not the case as $n \geq 12$. Therefore, $m = 1$, $A \simeq X_1$, and B is a transitive subgroup whose index is coprime with n. By Lemma 3, B is not primitive. Then B is a transitive imprimitive subgroup isomorphic to W_d, for some proper non-trivial divisor d of n. By Corollary 2, n is a prime power. □

In Lemma 2, we proved $\eta(A_n) \leq \omega(n) + 1$. The following theorem shows that the difference between $\eta(A_n)$ and $\omega(n)$ can be arbitrarily big.

Theorem 2. $\liminf_{\omega(n)\to\infty} \eta(A_n) = 3$.

We need a preliminary lemma in number theory.

Lemma 6. *Let $m = p_1 p_2 \ldots p_k$ be the product of k distinct prime numbers p_i. For every $i = 1, \ldots, k$, let a_i be the p_i-adic value of $m!$, and choose any prime number q which is congruent to* 1 *modulo $p_1^{a_1} \ldots p_k^{a_k}$. Then*

$$\binom{mq}{m} \equiv 1 \pmod{p_i} \quad \text{for every } i = 1, \ldots, k.$$

Proof. Let p be any prime from the set $\{p_i\}_{i=1}^k$. By applying Lucas' theorem (see, for instance, [11]) we have

$$\binom{mq}{m} \equiv \prod_{j=0}^{h} \binom{(mq)_j}{m_j} \pmod{p},$$

where

$$[m]_p = (m_0, m_1, \ldots, m_h),$$
$$[mq]_p = \big((mq)_0, (mq)_1, \ldots, (mq)_h\big).$$

By our choice of q, we have $mq \equiv m \pmod{p_1^{a_1} \dots p_k^{a_k}}$ and $(mq)_j = m_j$ for every $j = 0, 1, \dots, \lfloor \log_p m \rfloor$, while $(mq)_j \geq m_j = 0$ for $j = \lfloor \log_p m \rfloor + 1, \dots, h$. This implies $\binom{(mq)_j}{m_j} = 1$ for all j, and so $\binom{mq}{m} \equiv 1 \pmod{p}$. □

Proof of Theorem 2. Let m and q be chosen as in the previous lemma, and let $n = mq$. Of course, $\omega(n) = k + 1 \to \infty$ when $k \to \infty$.

By Lemma 6, the maximal subgroups X_m of A_{mq} contain Sylow p-subgroups for every prime p different from q that divides n. Therefore, the family

$$\mathcal{H} = \{X_1, X_m, Q\},$$

where Q is any Sylow q-subgroup of A_n, is made of subgroups of coprime indices, proving that $\eta(A_n) \leq 3$. Finally, Theorem 1 completes the proof. □

Question A stated in the introduction, for the function η and the case of alternating groups becomes:

Question A′. Is $\limsup_{\omega(n)\to\infty} \eta(A_n)$ always finite?

Our analysis permits the following reformulation in terms of pure number theory.

Question B. Given a positive integer n, let $\eta(n)$ be the smallest number such that

$$\gcd\left\{\binom{n}{m_1}, \dots, \binom{n}{m_{\eta(n)}}\right\} = 1 \quad \text{if } n \text{ is odd,}$$

$$\gcd\left\{\binom{n}{m_1}, \dots, \binom{n}{m_{\eta(n)}}, \frac{1}{2}\binom{n}{n/2}\right\} = 1 \quad \text{if } n \text{ is even,}$$

where $1 \leq m_i < n/2$ for every i. Is it true that $\limsup \eta(n) < +\infty$?

This seems to be quite a hard problem since it deals with the distributions and the representations (in different bases) of prime numbers. We made some computations with a program, considering values of n that are products of the first k distinct primes, up to $k = 10$ (and so $n \leq 6\,469\,693\,230$). Our data suggest that it might be $\eta(A_n) \geq \lfloor k/2 \rfloor - 1$, but more evidence should be gathered.

The following example shows a particular situation when n is even.

Example 1. Consider $n = 826\,610 = 2 \cdot 5 \cdot 131 \cdot 631$ and $d = n/2$. Then we have

$$\begin{aligned} 826\,610 &= 2 \cdot 5 + 4 \cdot 5^2 + 2 \cdot 5^3 + 2 \cdot 5^4 + 4 \cdot 5^5 2 \cdot 5^6 + 2 \cdot 5^8 \\ &= 22 \cdot 131 + 48 \cdot 131^2 \\ &= 48 \cdot 631 + 2 \cdot 631^2. \end{aligned}$$

Therefore, by Lemma 5, $W_{n/2}$ contains Sylow p-subgroups for $p = 5, 131, 631$. The collection

$$\mathcal{H} = \{X_1, W_{n/2}, H_2\},$$

where H_2 is a maximal subgroup containing Sylow 2-subgroups, satisfies condition (CI). By Theorem 1, we have $\eta(A_n) = 3$.

Example 1 also suggests the following:

Question C. Are there infinitely many odd primes p_i for which the subgroup $W_{n/2}$ of A_n, for $n = 2p_1 p_2 \dots p_k$, contains Sylow p_i-subgroups *for all* $i = 1, \dots, k$?

Equivalently,

Question C′. Are there infinitely many odd primes p_i for which the number $\frac{1}{2}\binom{n}{n/2}$, for $n = 2p_1 p_2 \dots p_k$, is coprime with every p_i?

Note that a positive answer to the above questions will provide a different proof of Theorem 2.

3 Other finite simple groups

3.1 Classical groups of Lie type

We assume now that G is a finite simple classical group. We adopt the notation of [12] and, by [12, Proposition 2.9.1], we let G be one of the following groups:

- $\mathrm{PSL}_n(q)$ for $n \geq 2$ and $q \geq 7$ when $n = 2$,
- $\mathrm{PSp}_n(q)$ for $n \geq 2$ even and $q \geq 3$,
- $\mathrm{PSU}_n(q)$ for $n \geq 3$, $q \geq 9$ a square,
- $\mathrm{P}\Omega_n(q)$ for $n \geq 7$ odd and $q \geq 3$ odd,
- $\mathrm{P}\Omega_n^+(q)$ for $n \geq 4$ even,
- $\mathrm{P}\Omega_n^-(q)$ for $n \geq 4$ even.

Proposition 3. *Assume that G is a finite simple classical group. Then Table* 1 *provides upper bounds for $\eta(G)$. In particular, we always have $\eta(G) \leq 4 + 2\omega(n)$.*

Proof. The proof is based on a direct inspection of the indices of the maximal subgroups of the simple classical groups. The basic references are [12] when $n \geq 13$, and [1] otherwise. Here we limit our exposition to $n \geq 13$ and treat in detail only

G	$\eta(G) \leq$	d
$\mathrm{PSL}_n(q)$	$2 + \omega(d) + \omega(n)$	$\gcd(n, q-1)$
$\mathrm{PSp}_n(q)$	$4 + \omega(n/2)$	
$\mathrm{PSU}_n(q)$	$4 + \omega(d) + \omega(n)$	$\gcd(n, q+1)$
$\mathrm{P}\Omega_n(q)$	3	
$\mathrm{P}\Omega_n^+(q)$	$4 + \omega(d) + \omega(n/2)$	$\gcd(4, q^n - 1)$
$\mathrm{P}\Omega_n^-(q)$	$4 + \omega(n/2)$	

Table 1. Upper bounds for $\eta(G)$ when G is a simple classical group.

the case $G = \mathrm{PSL}_n(q)$; for the other groups, we just exhibit a list $\mathcal{H}$ of subgroups having property (CI) and whose cardinality realizes the upper bound given in Table 1. When $n \leq 12$, better bounds (and, in some cases, explicit computations) can be found, according to the specific parameters of G.

Case $G = \mathrm{PSL}_n(q)$. The only maximal subgroups of G containing Sylow p-subgroups, for p being the characteristic of the underlying field, are the maximal parabolic subgroups, namely, the conjugates of the various P_i, for $i = 1, \dots, n$. We take P_1 to be the stabilizer of a 1-dimensional subspace so that

$$|G : P_1| = \frac{q^n - 1}{q - 1}.$$

Now, for every odd prime p dividing n, we set R_p to be a maximal subgroup of Aschbacher's class $\mathcal{C}_3$ associated to the field extension $\mathbb{F}_{q^p}$ of $\mathbb{F}_q$. For the structure of R_p, as well as its order and properties, we refer the reader to [12, Proposition 4.3.6], (or [10, 19]). Such a group R_p contains Sylow t-subgroups for the various primes t such that p divides the order of $q \pmod t$, i.e., t dividing $q^p - 1$. Therefore, by taking all the R_p, for the primes $p \mid n$, we can cover every prime dividing $(q^n - 1)/(q - 1)$ and not dividing $q - 1$. In particular, we have

$$\gcd(|G : P_1|, |G : R_p| : p \mid n) \text{ divides } \gcd\left(\frac{q^n - 1}{q - 1}, q - 1\right).$$

Note that every odd prime s, dividing both $(q^n - 1)/(q - 1)$ and $q - 1$, is necessarily a divisor of n and so of $d = \gcd(n, q - 1)$. In general, a Sylow s-subgroup Q_s is not contained in any of the R_p above (it does if and only if $s^2 \nmid q - 1$) and, for this reason, we need to add at most $\omega(d)$ more subgroups (the Sylow s-subgroups for s dividing d). Finally, if necessary, we need to add to our list (a maximal subgroup containing) a Sylow 2-subgroup Q_2. Then

$$\mathcal{H} = \{P_1, R_p, Q_s, Q_2 : p \mid n,\ s \mid d\}.$$

Case $G = \mathrm{PSp}_n(q)$. A list of subgroups having coprime indices is

$$\mathcal{H} = \{P_1, A, B, Q_2, R_p, Q_s, Q_2 : p \mid (n/2)\},$$

where

- P_1 is the stabilizer of a point [12, Proposition 4.1.19],
- A and B are given by

$$A \simeq \begin{cases} \frac{q-1}{2}.\mathrm{PGL}_{n/2}(q).2 \in \mathcal{C}_2 & \text{if } q \text{ is odd [12, Proposition 4.2.5]},\\ O_n^+(q) \in \mathcal{C}_8 & \text{if } q \text{ is even [12, Proposition 4.8.6]}, \end{cases}$$

$$B \simeq \begin{cases} O_n^+(q) \in \mathcal{C}_8 & \text{if } q, n/2 \text{ are even [12, Proposition 4.8.6]},\\ O_n^-(q) \in \mathcal{C}_8 & \text{if } q \text{ is even and } n/2 \text{ is odd}\\ & \text{[12, Proposition 4.8.6]},\\ \frac{q+1}{2}.\mathrm{PGU}_{n/2}(q).2 \in \mathcal{C}_3 & \text{if } q \text{ is odd [12, Proposition 4.3.7]}, \end{cases}$$

- Q_2 is a Sylow 2-subgroup,
- R_p, for $p \mid (n/2)$, are maximal subgroups of class $\mathcal{C}_3$ [12, Proposition 4.3.10], each containing Sylow t-subgroups for primes t such that the order of $q^2 \pmod t$ is divisible by p.

Case $G = \mathrm{PSU}_n(q)$. The bound in Table 1 is reached by considering the following list of subgroups having coprime indices:

$$\mathcal{H} = \{P_1, S_1, W, Q_2, R_p, Q_s : 2 \neq p \mid n,\ s \mid d\},$$

where

- P_1 is the stabilizer of an isotropic point [12, Proposition 4.1.18],
- S_1 the stabilizer of a non-isotropic point [12, Proposition 4.1.4],
- $W \simeq \mathrm{PSp}_n(q).\frac{(2,q-1)(q+1,n/2)}{d} \in \mathcal{C}_5$ when n is even [12, Proposition 4.5.6],
- Q_2 is a Sylow 2-subgroup and Q_s a Sylow s-subgroup, for $s \mid d$,
- R_p, for odd primes $p \mid n$, is a maximal subgroup of class $\mathcal{C}_3$ (see [12, Proposition 4.3.6]), each containing Sylow t-subgroups of G for the primes t such that the order of $q \pmod t$ is divisible by the prime p.

Case $G = \mathrm{P}\Omega_n(q)$, *$nq$ odd.* A collection of three maximal subgroups having (CI) is

$$\mathcal{H} = \{P_1, H^+, H^-\},$$

where

- P_1 is the stabilizer of an isotropic point,
- $H^+ \simeq \Omega^+_{n-1}(q).2$ is the stabilizer of a "plus" point [12, Proposition 4.1.16],
- $H^- \simeq \Omega^-_{n-1}(q).2$ is the stabilizer of a "minus" point [12, Proposition 4.1.16].

Case $G = \mathrm{P}\Omega^+_n(q)$. We may take

$$\mathcal{H} = \{P_1, H, U, R_2, R_p, Q_2, Q_s : 2 \neq p \mid (n/2),\ 2 \neq s \mid d\},$$

where

- $P_1 \in \mathcal{C}_1$ is the stabilizer of an isotropic point [12, Proposition 4.1.20],
- H is given by

$$H \simeq \begin{cases} \mathrm{Sp}_{n-2}(q) \in \mathcal{C}_1 & \text{if } q \text{ is even [12, Proposition 4.1.7],} \\ \Omega_{n-1}(q).a \in \mathcal{C}_1 & \text{if } q \text{ is odd [12, Proposition 4.1.6],} \end{cases}$$

  where $a \in \{1, 2\}$,
- $U \in \mathcal{C}_3$ (see [12, Proposition 4.3.18]) containing Sylow t-subgroups for

$$2 \neq t \mid (q+1) \quad \text{when} \quad 4 \mid n,$$

- $R_2 \in \mathcal{C}_3$ when $n/2 \geq 4$ and n is even [12, Proposition 4.3.14],
- $R_p \in \mathcal{C}_3$, for $2 \neq p \mid (n/2)$, when $n/2$ is not a prime [12, Proposition 4.3.14], otherwise $P_{n/2} \in \mathcal{C}_1$ if $n/2$ is an odd prime [12, Proposition 4.1.20],
- Q_2 and Q_s are respectively Sylow 2- and s-subgroups, for odd primes $s \mid d$.

Case $G = \mathrm{P}\Omega^-_n(q)$. Here we take

$$\mathcal{H} = \{P_1, H, R_p, R, Q_2 : p \mid (n/2)\},$$

where

- $P_1\mathcal{C}_1$ is the stabilizer of an isotropic point,
- H is given by

$$H \simeq \begin{cases} \Omega_{n-1}(q).2 \in \mathcal{C}_1 & \text{if } q \text{ is even [12, Proposition 4.1.6],} \\ \Omega_{n-1}(q).a \in \mathcal{C}_1 & \text{if } q \text{ is odd [12, Proposition 4.1.6],} \end{cases}$$

  where $a \in \{1, 2\}$,
- $R \simeq \frac{q+1}{(q+1,4)}.\mathrm{U}_r(q).[(q+1, r)] \in \mathcal{C}_3$ when $n/2$ is odd [12, Proposition 4.2.18],

- R_p, for primes $p \mid n/2$, are maximal subgroups of class $\mathcal{C}_3$ (see [12, Proposition 4.2.16]) containing Sylow t-subgroups of G for those odd primes t such that the order of $q \pmod t$ is divisible by p,
- Q_2 a Sylow 2-subgroup. □

We conclude the case of classical groups by noting that, contrary to what happens for alternating groups (Theorem 1), there exist classical simple groups having indices covering number two, without having maximal subgroups of prime power index. One example is the group $\mathrm{PSL}_4(5)$.

3.2 Groups of exceptional type

Let G be an exceptional simple group, namely, one of the following groups:

$$\begin{array}{llll} & & {}^2B_2(q) & \text{with } q = 2^{2m+1} \geq 8, \\ G_2(q) & \text{with } q \geq 3, & {}^2G_2(q) & \text{with } q = 3^{2m+1} \geq 27, \\ F_4(q) & \text{with } q \geq 3, & {}^2F_4(q) & \text{with } q = 2^{2m+1} \geq 8, \end{array}$$

${}^3D_4(q)$, $E_6(q)$, ${}^2E_6(q)$, $E_7(q)$ and $E_8(q)$. Note that we need not treat ${}^2B_2(2)$ (which is solvable), $G_2(2) \simeq \mathrm{PSU}_3(3).2$, ${}^2G_2(3) \simeq \mathrm{PSL}_2(8).3$ and ${}^2F_4(2)'$, which will be treated in Section 3.3.

Proposition 4. *For every finite exceptional simple group of Lie type G, we have $\eta(G) \leq 20$.*

Proof. Let p be a prime dividing $|G|$. If p is different from the characteristic of G and p does not divide $2|W|$, where W is the Weyl subgroup associated to G, then every Sylow p-subgroup of G lies in a Sylow d-torus, for a unique d, for which the cyclotomic value $\Phi_d(q)$ divides $|G|$ (see [19, Theorem 25.14]). Since exceptional groups have bounded rank, the number of such d is bounded and therefore so are the values of $\eta(G)$.

Table 2 provides reasonably good bounds for $\eta(G)$ when G is one of the simple groups of exceptional type. These results have been obtained by analyzing the indices of the maximal subgroups of G; these have been classified in the papers [13, 14, 17, 18, 22]. □

3.3 The case of sporadic groups

Table 3 provides the exact values of $\eta(G)$, for (almost all) the sporadic simple groups G and the Tits group ${}^2F_4(2)'$. Indeed, for the groups Fi_{24}', B and M, we

G	$\eta(G) \leq$	G	$\eta(G) \leq$
${}^2B_2(q)$	3	${}^3D_4(q)$	5
$G_2(q)$	3	$E_6(q)$	7
${}^2G_2(q)$	4	${}^2E_6(q)$	6
$F_4(q)$	4	$E_7(q)$	6
${}^2F_4(q)$	6	$E_8(q)$	14

Table 2. Upper bounds for $\eta(G)$ when G is an exceptional group.

G	$\eta(G)$	$\omega(\lvert G\rvert)$	G	$\eta(G)$	$\omega(\lvert G\rvert)$	G	$\eta(G)$	$\omega(\lvert G\rvert)$
M_{11}	2	4	Co_3	4	6	B	≤ 5	11
M_{12}	3	4	Co_2	3	6	M	≤ 10	15
M_{22}	3	5	Co_1	5	7	J_1	3	6
M_{23}	2	6	He	3	5	O'N	5	7
M_{24}	2	6	Fi_{22}	3	6	J_3	4	5
J_2	3	4	Fi_{23}	4	8	Ly	4	8
Suz	3	6	Fi'_{24}	≤ 5	9	Ru	4	6
HS	3	5	HN	5	6	J_4	5	10
McL	3	5	Th	5	7	${}^2F_4(2)'$	3	4

Table 3. A comparison between $\eta(G)$ and $\omega(|G|)$ for sporadic groups and the Tits group.

furnish an upper bound (which we think is probably the exact value of $\eta(G)$), as the list of maximal subgroups of these groups is still incomplete. These results have been obtained by a direct inspection in [6] of the maximal subgroups of G.

4 Normal primary coverings and the function $\gamma_0(G)$

Given a finite group G, let G_0 be the set of its primary elements, namely,

$$G_0 = \{g \in G \mid |g| \text{ is a prime power}\}.$$

Definition 1. A *normal primary covering* for G is a collection of conjugacy classes of subgroups of G whose union contains G_0.

If G is a finite group which is not a cyclic p-group, we define $\gamma_0(G)$ to be the cardinality of a smallest normal primary covering for G, i.e., the smallest natural integer such that

$$G_0 \subseteq \bigcup_{i=1}^{\gamma_0(G)} \bigcup_{g \in G} H_i^g,$$

for some proper (pairwise non-conjugate) subgroups H_i of G.

This definition is suggested by the analogous function $\gamma(G)$ (defined in [3]) as the smallest positive number of conjugacy classes of subgroups that covers all of G.

The following lemma collects some basic facts about the function γ_0.

Proposition 5. *Let G be a finite group. Then the following holds.*

(1) *If G is a non-cyclic p-group, then $\gamma_0(G) = \gamma(G) = p + 1$.*

(2) *If G is not a p-group, then $2 \leq \gamma_0(G) \leq \eta(G)$.*

Proof. (1) This is trivial from the definitions of the functions γ_0 and γ.

(2) The fact that $\gamma_0(G) \leq \eta(G)$ is immediate from the definitions of the two functions. The fact that $\gamma_0(G) \geq 2$ is [9, Theorem 1], and it depends on CFSG. □

Lemma 7. *Let p be a prime divisor of n. Then any p-element of A_n acting fixed-point-freely on $\{1, 2, \ldots, n\}$ lies in a conjugate of the subgroup $W_{n/p}$.*

Proof. Let p be odd (the proof for $p = 2$ is just a slight modification). Write $n = rp$, and let τ be a p-element that has no fixed points. Assume that τ is the disjoint product of cycles c_i, for $i = 1, 2, \ldots, h$, and that each c_i has order p^{α_i} so that it can be written as $c_i = (a_1^i, a_2^i, \ldots, a_{p^{\alpha_i}}^i)$. Since τ acts fixed-point-freely, we necessarily have $n = \sum_{i=1}^h p^{\alpha_i}$, thus $r = \sum_{i=1}^h p^{\alpha_i - 1}$. Now, for every $j = 0, 1, \ldots, p-1$, we set

$$\Delta_j := \{a_s^i \mid i = 1, \ldots, h,\ s \equiv j \pmod{p}\}.$$

Note that $|\Delta_j| = \sum_{i=i}^h p^{\alpha_i - 1} = r$ for every j and that τ stabilizes the partition $\{\Delta_0, \Delta_1, \ldots, \Delta_{p-1}\}$. Since A_n acts transitively on the set of partitions of r-size blocks, τ lies in a conjugate of W_r. □

Proposition 6. *If $n \geq 5$ and n is either p^k or $p^r q$, with $p \neq q$, then $\gamma_0(A_n) = 2$. In particular, γ_0 and η are different arithmetic functions.*

Proof. The case $n = p^k$ is trivial by Proposition 5 (2) and Theorem 1.

Let $n = p^r q$. We construct a normal primary covering of cardinality 2 by taking the subgroups X_1 and W_{p^r}. Indeed, any given primary element of A_n with no fixed point is either a p-element or a q-element. In any case, it lies in a conjugate of W_{p^r} by Lemma 5 and Lemma 7.

When p and q are different primes we have $\gamma_0(A_{p^r q}) = 2$ and $\eta(A_{p^r q}) = 3$. □

Bibliography

[1] J. N. Bray, D. F. Holt and C. M. Roney-Dougal, *The Maximal Subgroups of the Low-dimensional Finite Classical Groups*, London Math. Soc. Lecture Note Ser. 407, Cambridge University, Cambridge, 2013.

[2] J. R. Britnell and A. Maróti, Normal coverings of linear groups, *Algebra Number Theory* **7** (2013), no. 9, 2085–2102.

[3] D. Bubboloni and C. E. Praeger, Normal coverings of finite symmetric and alternating groups, *J. Combin. Theory Ser. A* **118** (2011), no. 7, 2000–2024.

[4] D. Bubboloni, C. E. Praeger and P. Spiga, Normal coverings and pairwise generation of finite alternating and symmetric groups, *J. Algebra* **390** (2013), 199–215.

[5] D. Bubboloni, C. E. Praeger and P. Spiga, Conjectures on the normal covering number of the finite symmetric and alternating groups, *Int. J. Group Theory* **3** (2014), no. 2, 57–75.

[6] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of Finite Groups*, Oxford University, Eynsham, 1985.

[7] E. Crestani and A. Lucchini, Normal coverings of solvable groups, *Arch. Math. (Basel)* **98** (2012), no. 1, 13–18.

[8] J. D. Dixon and B. Mortimer, *Permutation Groups*, Grad. Texts in Math. 163, Springer, New York, 1996.

[9] B. Fein, W. M. Kantor and M. Schacher, Relative Brauer groups. II, *J. Reine Angew. Math.* **328** (1981), 39–57.

[10] D. Gorenstein, R. Lyons and R. Solomon, *The Classification of the Finite Simple Groups. Number 3. Part I. Chapter A. Almost Simple K-groups*, Math. Surveys Monogr. 40, American Mathematical Society, Providence, 1998.

[11] A. Granville, Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers, in: *Organic Mathematics* (Burnaby 1995), CMS Conf. Proc. 20, American Mathematical Society, Providence (1997), 253–276.

[12] P. Kleidman and M. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Ser. 129, Cambridge University, Cambridge, 1990.

[13] P. B. Kleidman, The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, the Ree groups ${}^2G_2(q)$, and their automorphism groups, *J. Algebra* **117** (1988), no. 1, 30–71.

[14] P. B. Kleidman, The maximal subgroups of the Steinberg triality groups ${}^3D_4(q)$ and of their automorphism groups, *J. Algebra* **115** (1988), no. 1, 182–199.

[15] E. E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, *J. Reine Angew. Math.* **44** (1852), 93–146.

[16] M. W. Liebeck, C. E. Praeger and J. Saxl, The maximal factorizations of the finite simple groups and their automorphism groups, *Mem. Amer. Math. Soc.* **86** (1990), no. 432, 1–151.

[17] M. W. Liebeck, J. Saxl and G. M. Seitz, Subgroups of maximal rank in finite exceptional groups of Lie type, *Proc. Lond. Math. Soc. (3)* **65** (1992), no. 2, 297–325.

[18] G. Malle, The maximal subgroups of ${}^2F_4(q^2)$, *J. Algebra* **139** (1991), no. 1, 52–69.

[19] G. Malle and D. Testerman, *Linear Algebraic Groups and Finite Groups of Lie Type*, Cambridge Stud. Adv. Math. 133, Cambridge University, Cambridge, 2011.

[20] M. B. Nathanson, *Elementary Methods in Number Theory*, Grad. Texts in Math. 195, Springer, New York, 2000.

[21] J. Shareshian and R. Woodroofe, Divisibility of binomial coefficients and generation of alternating groups, *Pacific J. Math.* **292** (2018), no. 1, 223–238.

[22] M. Suzuki, On a class of doubly transitive groups, *Ann. of Math. (2)* **75** (1962), 105–145.

[23] J. G. Thompson, Hall subgroups of the symmetric groups, *J. Combin. Theory* **1** (1966), 271–279.

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

Received November 19, 2018; revised March 14, 2019.

Author information

Francesco Fumagalli, Dipartimento di Matematica e Informatica "Ulisse Dini", Università degli Studi di Firenze, viale Morgagni 67/A, 50134 Firenze, Italy.
E-mail: `francesco.fumagalli@unifi.it`