

Pacific Journal of Mathematics

**DIVISIBILITY OF BINOMIAL COEFFICIENTS AND
GENERATION OF ALTERNATING GROUPS**

JOHN SHARESHIAN AND RUSS WOODROOFE

Volume 292 No. 1

January 2018

DIVISIBILITY OF BINOMIAL COEFFICIENTS AND GENERATION OF ALTERNATING GROUPS

JOHN SHARESHIAN AND RUSS WOODROOFE

We examine an elementary problem on prime divisibility of binomial coefficients. Our problem is motivated by several related questions on alternating groups.

1. Introduction

We will discuss several closely related problems. The first is an elementary problem concerning divisibility of binomial coefficients by primes. Consider the following condition that a positive integer n might satisfy:

- (1) There exist primes p and r such that if $1 \leq k \leq n-1$, then the binomial coefficient $\binom{n}{k}$ is divisible by at least one of p or r .

Question 1.1. *Does Condition (1) hold for all positive integers n ?*

We were led to ask Question 1.1 by a problem on the alternating groups. Indeed, we consider several related group-theoretic conditions on a positive integer n :

- (2) There exist primes p and r such that if $H < A_n$ is a proper subgroup, then the index $[A_n : H]$ is divisible by at least one of p or r .
- (2') There exist primes p and r such that if P is a Sylow p -subgroup and R a Sylow r -subgroup of A_n , then $\langle P, R \rangle = A_n$.
- (3) There exist a prime p and a conjugacy class D in A_n consisting of elements of prime power order, such that if P is a Sylow p -subgroup of A_n and $d \in D$, then $\langle P, d \rangle = A_n$.
- (4) There exist conjugacy classes C and D in A_n , both consisting of elements of prime power order, such that if $(c, d) \in C \times D$, then $\langle c, d \rangle = A_n$.
- (5) There exist conjugacy classes C and D in A_n , both consisting of elements of prime order, such that if $(c, d) \in C \times D$, then $\langle c, d \rangle = A_n$.

The first author was supported in part by NSF Grants DMS-0902142 and DMS-1202337.

MSC2010: 05A10, 05E15, 11B65, 20B30.

Keywords: alternating group, binomial coefficients, generation, prime density.

If we wish to specify one or both of the primes, then we may say that n satisfies Condition (1) with p , or that n satisfies Condition (1) with p and r . We'll use similar language for the other conditions.

Conditions (2) and (2') are equivalent, and each condition in the above list implies the previous condition. That is, for any positive integer n the following chain of implications holds, where the primes p and r may be held fixed.

$$(1-1) \quad (5) \Rightarrow (4) \Rightarrow (3) \Rightarrow (2') \iff (2) \Rightarrow (1).$$

See also Theorem 1.3 below.

All implications in (1-1) are completely trivial or immediate from the definition of a Sylow subgroup, with the exception of the implication $(2) \Rightarrow (1)$. This implication follows since A_n has subgroups of index $\binom{n}{k}$ for each $0 \leq k \leq n$. (The stabilizer in A_n of a k -subset of $[n]$ is such a subgroup.)

There are infinitely many positive integers n that do not satisfy Condition (5). However, the set of such integers is rather sparse, and likely very sparse. See Proposition 1.6 and Theorem 1.5 below. We are not aware of any integer n for which Conditions (1)–(4) fail to hold. In addition to Question 1.1, we will consider the following.

Questions 1.2–1.4. *Do Conditions (2)–(4) hold for all positive integers n ?*

1A. Motivations and related questions. Question 1.1 fits into a line of inquiry going back to Kummer [1852] on the distribution of binomial coefficients that are divisible by a given prime. The remaining conditions and questions arose from our work and that of others on generation of finite simple groups. Recall that the classification of finite simple groups tells us that every simple group is isomorphic to one of the following: an alternating group A_n with $n \geq 5$, a cyclic group of prime order, a group of Lie type, or one of twenty six sporadic groups. Conditions analogous to Conditions (2)–(5) are known or conjectured for sporadic and Lie type groups.

We became interested in these problems via Question 1.2. In [Sharesian and Woodroffe 2016], we define a group G to be *universally (p, r) -generated* if $G = \langle P, R \rangle$ for any Sylow p -subgroup P and Sylow r -subgroup R . (Compare with Condition (2')!) We say G is *universally $(2, *)$ -generated* if there is some prime p such that G is universally $(2, p)$ -generated. We showed the following.

Theorem 1.2 [Sharesian and Woodroffe 2016]. *If G is a finite simple group that is abelian, of Lie type, or sporadic, then G is universally $(2, *)$ -generated.*

We used Theorem 1.2, along with fixed-point theorems of Smith [1941] and Oliver [1975], to show that the order complex of the coset poset of any finite group is noncontractible.

In light of Theorem 1.2, it is natural to ask whether A_n is universally $(2, *)$ -generated for every n — that is, whether every n satisfies Condition (2) with 2. This

is not the case. The first failure of universal $(2, *)$ -generation is at $n = 7$. It may be easier to understand the second failure, at 15, since $n = 15$ does not even satisfy Condition (1) with 2. Question 1.2 naturally suggests itself. We will further discuss the case $p = 2$ below in Section 1C.

We found that similar conditions had been examined earlier. The general problem of generation by elements selected from fixed conjugacy classes has been more broadly studied under the name of “invariable generation”. See for example [Dixon 1992; Kantor et al. 2011; Detomi and Lucchini 2015; Eberhard et al. 2017]. Dolfi, Guralnick, Herzog and Praeger first asked Question 1.4 in [Dolfi et al. 2012, Section 6]. These authors conjecture that the analogue of Condition (5) holds for all but finitely many simple groups of Lie type, but point out that the corresponding statement for alternating groups occasionally fails.

Condition (3) interpolates naturally between Conditions (2) and (4). Although they do not ask Question 1.3, Damian and Lucchini [2007] show that an analogue of Condition (3) holds for many sporadic simple groups and groups of Lie type. Indeed, they show that many simple groups are generated by a Sylow 2-subgroup P together with any element of a certain conjugacy class consisting of elements of prime order.

1B. Results for arbitrary primes. Our first result adds an additional implication to the list in (1-1).

Theorem 1.3. *Let p and r be primes. If the positive integer n is not a prime power, then Conditions (1) and (2) are equivalent for n with p and r .*

The case where n is a prime power is not difficult.

Proposition 1.4. *If n is a power of the prime p , then*

- (A) *n satisfies Condition (3) with a Sylow 2-subgroup unless $n = 7$, and*
- (B) *n satisfies Condition (4) with p .*

In particular, it follows from Theorem 1.3 and Proposition 1.4 that Questions 1.1 and 1.2 are equivalent. We remark that the requirement $n \neq 7$ in Proposition 1.4(A) is necessary, as $n = 7$ satisfies Condition (1), but not Condition (2), with the prime 2.

While Questions 1.1–1.4 are still open, we have amassed a large collection of integers for which the answers are “yes”. The *asymptotic density* [Niven et al. 1991] of a set S of positive integers is defined to be

$$\liminf_{M \rightarrow \infty} \frac{|S \cap [M]|}{M}.$$

Dolfi, Guralnick, Herzog and Praeger [2012] remark that Condition (5) appears likely to hold with asymptotic density 1. We show the following:

Theorem 1.5. *Let α be the asymptotic density of the set of positive integers n that satisfy Condition (5), and let ρ denote the Dickman–de Bruijn function (see for example [Granville 2008]). We have*

- (A) $\alpha \geq 1 - \rho(20) > 1 - 10^{-28}$, and
- (B) *if either the Riemann hypothesis or the Cramér conjecture holds, then $\alpha = 1$.*

The authors also claim in [Dolfi et al. 2012] that Condition (5) fails for infinitely many values of n , and that the smallest n for which Condition (5) fails is 210. We will see that the first claim is true, but the second is not.

Proposition 1.6. *For any $a \geq 3$, the integer $n = 2^a$ fails to satisfy Condition (5).*

Theorem 1.5 suggests a positive answer to Questions 1.1–1.4 for all but a vanishingly sparse set of large integers. We have also examined many small integers with the aid of a computer, verifying the following.

Proposition 1.7. *Every $n \leq 1,000,000,000$ satisfies Condition (2).*

The key tool in the proofs of both Theorem 1.5 and Proposition 1.7 is the following sieve lemma.

Lemma 1.8 (sieve lemma). *Let $n \geq 9$ be an integer. Let p and r be primes, and let a and b be positive integers.*

- (A) *If n is not a prime power, p^a divides n , and $r^b < n < r^b + p^a$, then n satisfies Condition (2) with p and r .*
- (B) *If p divides n and $r + 2 < n < r + p$, then n satisfies Condition (5) with p and r .*

Theorem 1.5 follows from combining Lemma 1.8 with known results on prime gaps and smooth numbers. We also use Lemma 1.8 to do much of the work in verifying Proposition 1.7.

For those integers not handled by Lemma 1.8(A), Theorem 1.3 tells us that it suffices to check divisibility of binomial coefficients. In particular, we can avoid making any computations in large alternating groups. We do not know how to avoid such computations for Condition (4). The slow speed of these computations is the main obstacle to a computational verification of Condition (4) for those values of n not addressed by Lemma 1.8.

1C. Results for $p = 2$. We return now to the case where one of the primes in Condition (2) is 2. Theorem 1.2 suggests this case as being particularly worthy of attention, and Proposition 1.4 gives infinitely many values of n for which Condition (2) holds with 2.

However, there are also infinitely many positive integers n that do not even satisfy Condition (1) with 2. By a theorem of Kummer (see Lemma 3.1 below), if

$n = 2^a - 1$ for some positive integer a , then $\binom{n}{k}$ is odd for all $1 \leq k \leq n - 1$. (Indeed, a similar statement holds for any prime p . In the language of group-actions, this says that any Sylow p -subgroup of S_{p^a-1} stabilizes a set of every possible size k with $1 < k < p^a - 1$.) Kummer's theorem also implies that there is no prime dividing every nontrivial $\binom{n}{k}$ unless n is a prime power. There are infinitely many n of the form $2^a - 1$ that are not prime powers.

Using techniques similar to those for Proposition 1.7, we computationally verify the following.

Proposition 1.9. *About 86.7% of the positive integers $n \leq 1,000,000$ satisfy Condition (2) with 2.*

1D. Organization. We begin in Section 2 by giving necessary background on maximal subgroups of alternating groups. In Section 3 we state the well-known theorem of Kummer on prime divisibility of binomial coefficients, and prove an analogue on prime divisibility of the number of equipartitions of a set. We use these results in Section 4 to prove Theorem 1.3, Propositions 1.4 and 1.6, and Lemma 1.8. We also verify that Condition (4) holds for all small alternating groups. We apply Lemma 1.8 to prove Theorem 1.5 in Section 5. We describe our computational verification of Propositions 1.7 and 1.9 in Section 6.

2. Preliminaries

In this section we discuss necessary background on alternating and symmetric groups. Readers familiar with basic facts about permutation groups can safely skip this section.

In order to show that the index of every subgroup of the alternating group A_n is divisible by either p or r , it suffices to show the same for every maximal subgroup. The maximal subgroups of A_n are well-understood, as we now review. Additional background can be found in [Dixon and Mortimer 1996], see also [Liebeck et al. 1987].

We say that a subgroup $H \leq A_n$ is transitive or primitive if the action of H on $[n]$ satisfies the same property. That is, H is *transitive* if for every $i, j \in [n]$, there is some $\sigma \in H$ such that $i \cdot \sigma = j$. A transitive subgroup H is *imprimitive* if there is a proper partition π of $[n]$ into sets of size greater than one, such that the parts of π are permuted by the action of H . If H is transitive and not imprimitive, then it is *primitive*. Clearly, every subgroup is either intransitive, imprimitive, or primitive. We examine maximal subgroups of A_n according to this trichotomy.

An intransitive subgroup H is maximal in the (sub)poset of intransitive subgroups of A_n if and only if H is the stabilizer in A_n of some nonempty proper subset $X \subset [n]$. As A_n sits naturally in S_n , it is illuminating to also consider the stabilizer H^+ in S_n of X . Then $H = H^+ \cap A_n$. It is clear that $H^+ \cong S_{|X|} \times S_{n-|X|}$. If $|X| = k$, then it

follows either from this isomorphism or the orbit-stabilizer theorem that

$$[A_n : H] = [S_n : H^+] = \frac{n!}{k! \cdot (n-k)!} = \binom{n}{k}.$$

Every imprimitive subgroup of A_n stabilizes a partition of $[n]$. It follows easily that a subgroup H is maximal in the (sub)poset of imprimitive subgroups of A_n if and only if H is the stabilizer of a partition of $[n]$ into n/d parts of size d for some nontrivial proper divisor d of n . As in the intransitive case, we also consider the stabilizer H^+ of the same partition in the action by S_n . Then H^+ is isomorphic to the wreath product $S_d \wr S_{n/d}$. Since $H = H^+ \cap A_n$ (and $H^+ \not\leq A_n$), we see that

$$[A_n : H] = [S_n : H^+] = \frac{n!}{(d!)^{n/d} \cdot (n/d)!}.$$

By either the orbit-stabilizer theorem or an elementary counting argument, $[A_n : H]$ counts the number of partitions of $[n]$ into n/d equal-sized parts.

The index of a primitive proper subgroup of A_n is typically divisible by every prime smaller than n . See Theorem 4.1 and the discussion following for a precise statement.

3. Kummer's theorem and an analogue

3A. Kummer's theorem. We make considerable use of the following result of Kummer. The most useful case of the lemma for us will be that where $a = 1$. See also [Granville 1997] for an overview of related results.

Lemma 3.1 (Kummer's theorem [1852, pp. 115–116]). *Let k and n be integers with $0 \leq k \leq n$. If a is a positive integer, then p^a divides $\binom{n}{k}$ if and only if at least a carries are needed when adding k and $n - k$ in base p .*

3B. An analogue for the number of equipartitions. Lemma 3.1 completely describes the prime divisibility of indices of intransitive maximal subgroups of A_n . Lemma 3.2 below provides a weaker but similarly useful characterization regarding indices of imprimitive subgroups. Throughout this section, if d is a nontrivial proper divisor of the positive integer n , then we will write $I_{n,d}$ for the number of equipartitions of n into parts of size d . Thus,

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

Lemma 3.2. *Let n be a positive integer, d be a nontrivial proper divisor of n , and p be a prime. Then p divides $I_{n,d}$ if and only if*

- (1) *at least one carry is necessary when adding n/d copies of d in base p , and*
- (2) *d is not a power of p .*

Proof. It is straightforward to show by elementary arguments that

$$(3-1) \quad I_{n,d} = \frac{1}{(n/d)!} \cdot \prod_{j=1}^{n/d} \binom{jd}{d} = \prod_{j=1}^{n/d} \frac{1}{j} \binom{jd}{d} = \prod_{j=1}^{n/d} \binom{jd-1}{d-1}.$$

Our strategy is to use Lemma 3.1 to examine divisibility of the terms in these products.

Case 1 ($n/d < p$). In this case p does not divide $(n/d)!$, and the first condition of the hypothesis implies the second. From (3-1) we thus see that p divides $I_{n,d}$ if and only if p divides $\binom{jd}{d}$ for some $1 \leq j \leq n/d$. The claim for this case then follows from Lemma 3.1.

Case 2 ($n/d \geq p$). In this case a carry is always necessary when adding n/d copies of d , so we need only consider the second condition of the hypothesis.

If the base p expansion of d has at least 2 nonzero places, then there are at least 2 carries when adding d to $pd - d$, as the base p expansion of pd is obtained by shifting that of d to the left by one place. It follows that p^2 divides $\binom{pd}{d}$, hence that p divides $\binom{pd-1}{d-1} = \frac{1}{p} \binom{pd}{d}$. By (3-1), p divides $I_{n,d}$.

Otherwise, we have $d = kp^a$ for some $1 \leq k < p$. Then the base p expansion of $(jd - 1) - (d - 1) = (j - 1)kp^a$ vanishes below the a -th place. Also, the base p expansion of $d - 1$ is $(k - 1)p^a + \sum_{i=0}^{a-1} (p - 1)p^i$. As the latter vanishes above the a -th place, this place is the only possible location for a carry in adding $d - 1$ and $jd - 1$. If $k = 1$, then the a -th place of $d - 1$ is 0, so no carry occurs and for no j does p divide $\binom{jd-1}{d-1}$. If $k > 1$, then a carry occurs at the a -th place for values of j such that $(j - 1) \cdot k \equiv p - 1 \pmod{p}$. (Such a $j < n/d$ exists since $\mathbb{Z}/p\mathbb{Z}$ is a field.) \square

Remark 3.3. After submission of the paper, we became aware that a slightly different (from Lemma 3.2) characterization of prime divisibility of $I_{n,d}$ appears as [Thompson 1966, Lemma 2].

Corollary 3.4. *Let n and b be positive integers and r be a prime, such that $n/2 < r^b \leq n$. If d is a nontrivial proper divisor of n which is not a power of r , then r divides $I_{n,d}$.*

Proof. Since $r^b > n/2$, there is a 1 in the b -th place of the base r expansion of n . On the other hand, $d \leq n/2$. Hence, the base r expansion of d has a 0 in the b -th place. It follows that there is at least one carry when we sum n/d copies of d . Lemma 3.2 then gives that r divides $I_{n,d}$ unless d is a power of r . \square

One can indeed extract from (3-1) the highest power of p dividing $I_{n,d}$, but we will not need to do so.

4. Proofs of the sieve lemma and other tools

In this section we prove several results that we will use as tools in the sections that follow, including Theorem 1.3, Lemma 1.8, and Propositions 1.4 and 1.6.

4A. Proof of Theorem 1.3. Suppose n satisfies Condition (2) with p and r . As described in Section 2, the maximal intransitive subgroups of A_n are stabilizers of k -subsets of $[n]$, and have index $\binom{n}{k}$ in A_n . Hence, n also satisfies Condition (1) with p and r . See the discussion following (1-1).

Thus, in order to prove Theorem 1.3, it suffices to show that if n satisfies Condition (1) with p and r , then the index of every primitive or imprimitive maximal subgroup is divisible by at least one of p or r .

For the primitive case, we use the following version of a classic theorem of permutation group theory due to Jordan.

Theorem 4.1 [Jordan 1875; Dixon and Mortimer 1996, Section 3.3]. *Let $n \geq 9$ and let H be a primitive subgroup of A_n :*

- (1) *If $p \leq n - 3$ is a prime and H contains a p -cycle, then $H = A_n$.*
- (2) *If H contains the product of two transpositions, then $H = A_n$.*

The next lemma follows quickly.

Lemma 4.2. *Let p be a prime. If $n \geq 9$ and $p \leq n - 3$, then p divides the index of every primitive proper subgroup of A_n .*

Proof. If p is odd, then every Sylow p -subgroup of A_n contains a p -cycle. Similarly, every Sylow 2-subgroup of A_n contains an element that is the product of two transpositions. In either case, Theorem 4.1 gives that no primitive proper subgroup of A_n contains any Sylow p -subgroup of A_n . \square

Since Lemma 4.2 only applies when $n \geq 9$, we pause to handle the situation when $n < 9$. The only integer less than 9 that is not a prime power is 6, and the equivalence of Conditions (1) and (2) for $n = 6$ is obtained by direct inspection (see Table 1 below).

Now assume as above that $n \geq 9$ satisfies Condition (1) with p and r . Since n is not a prime power, we see from Lemma 3.1 that p and r must be distinct, hence one must be smaller than $n - 2$. As $n \geq 9$, it follows from Lemma 4.2 that the index of every primitive proper subgroup is divisible by at least one of p or r , as desired.

We now handle the imprimitive case, using Lemma 3.2. Let d be a divisor of n . We notice that if p divides $\binom{n}{d}$, then adding $n - d$ and d in base p requires a carry (by Lemma 3.1). It follows immediately from Lemma 3.2 that the index $n!/((d!)^{n/d} \cdot (n/d)!)$ of an imprimitive maximal subgroup is divisible by either p or r , except possibly if d is a power of p or r .

Suppose that d is a power of p , and that p^a is the highest power of p dividing n . Then Lemma 3.1 shows that $\binom{n}{p^a}$ is not divisible by p , hence it is divisible by r . Adding n/p^a copies of p^a in base r therefore requires a carry. Since $d \leq p^a$, adding n/d copies of d in base r will also require a carry. Therefore, $n!/((d!)^{n/d} \cdot (n/d)!)$ is divisible by r , as desired. The case where d is a power of r is handled similarly.

4B. Proof of Lemma 1.8(A). Kummer's theorem (Lemma 3.1) gives us the following.

Lemma 4.3. *Let n be a positive integer and let p and r be distinct primes. If there are positive integers a and b such that $p^a \mid n$ and $r^b < n < p^a + r^b$, then for $0 < k < n$ at least one of p, r divides $\binom{n}{k}$.*

Proof. Notice that since $p^a > n - r^b$, either $k < p^a$ or else $k > n - r^b$. We assume without loss of generality that $k \leq n/2$.

Let $k = \sum k_i p^i$ and $n = \sum n_i p^i$ respectively be the base p expansions of k and n . As $p^a \mid n$, therefore $n_i = 0$ for $i < a$. When $k < p^a$, then $k_j = 0$ for all $j \geq a$. Since $k \neq 0$, there is a carry when adding k and $n - k$ in base p . It follows from Lemma 3.1 that $p \mid \binom{n}{k}$.

When $k > n - r^b$, we notice that $k \leq n/2 < r^b$, and therefore both k and $n - k$ are between $n - r^b$ and r^b . In particular, the b -th place of the base r expansion of both k and $n - k$ has a 0. Since $n/2 < r^b < n$, the b -th place of the base r expansion of n has a 1. It follows that there is a carry when adding k and $n - k$, hence by Lemma 3.1 that $r \mid \binom{n}{k}$. \square

Lemma 1.8 follows from Lemma 4.3 and Theorem 1.3.

4C. Proof of Lemma 1.8(B). Let $x \in A_n$ have cycle type $p^{n/p}$, that is, let x be the product of n/p pairwise disjoint p -cycles. (Since $p \neq 2$, a p -cycle is an even permutation.) Let $y \in A_n$ be an r -cycle. We take C to be the conjugacy class containing x , and D to be the conjugacy class containing y . Since we chose (x, y) arbitrarily from $C \times D$, it is enough to show $\langle x, y \rangle = A_n$, that is, that $\langle x, y \rangle$ is not contained in a maximal subgroup of any of the three types discussed in Section 2.

Since $r < n - 2$, it is immediate from Theorem 4.1 that $\langle y \rangle$ is contained in no maximal primitive subgroup.

If p is a proper divisor of n , we see that $p \leq n/2$ and hence that $r > n - p \geq n/2$. It is then immediate by Corollary 3.4 that $\langle y \rangle$ is contained in no imprimitive maximal subgroup. Otherwise, if $n = p$, then A_n has no imprimitive maximal subgroups.

It remains to show that $\langle x, y \rangle$ is transitive in the natural action on $[n]$. Since y acts transitively on an r -set $Y \subseteq [n]$, it suffices to show that every $i \in [n]$ can be moved into Y by x . But i is permuted in a p -cycle by x , and since $r + p > n$, some element of this p -cycle must be in Y , as desired.

4D. Proof of Proposition 1.4. Direct inspection verifies the proposition for $n \leq 8$. See Table 1 below. We assume henceforth that $n \geq 9$.

We first verify part (B). By the Bertrand–Chebyshev theorem [Niven et al. 1991, Theorem 8.7] there is a prime r with $n/2 < r < n - 2$. We let x be any r -cycle, and notice that $\langle x \rangle$ is a Sylow r -subgroup. Then r divides the index of any imprimitive or primitive maximal subgroup by Corollary 3.4 and Lemma 4.2 respectively.

We now take y to be any n -cycle in the case where $n = p^a$ is odd, or the product of any two disjoint 2^{a-1} -cycles in the case where $n = 2^a$ is even. In the former case, $\langle y \rangle$ is transitive. In the latter case, as $r > 2^{a-1}$, we see that $\langle x, y \rangle$ is transitive. In either case, $\langle x, y \rangle$ is contained in no intransitive maximal subgroup, hence

$$\langle x, y \rangle = A_n.$$

Since conjugation fixes cycle type, part (B) follows.

It remains to verify (A). In the case where n is even, it follows from part (B). Otherwise, we take y to be any n -cycle. Then $\langle y \rangle$ is transitive, while Lemmas 3.2 and 4.2 give that no imprimitive or primitive maximal subgroup contains a Sylow 2-subgroup. It follows that

$$\langle y, P \rangle = A_n$$

for any Sylow 2-subgroup P , completing the proof of part (A).

4E. Proof of Proposition 1.6. Let C and D be as in Condition (5). We will find $(c, d) \in C \times D$ such that $\langle c, d \rangle \neq A_n$.

Since A_n is transitive, if D does not consist of derangements then we may find an element d of D fixing n . The same holds for C . If c and d both fix n , then $\langle c, d \rangle$ is intransitive, hence a proper subgroup of A_n . This reduces us to the situation where one conjugacy class (without loss of generality C) consists of derangements.

Since $n = 2^a$, derangements of prime order in A_n are fixed-point-free involutions. It is straightforward to verify that the fixed-point-free involutions of A_n form a single conjugacy class. Thus, C consists of all fixed-point-free involutions in A_n .

Since a Sylow 2-subgroup of A_n intersects every conjugacy class of involutions nontrivially, we see that D must consist of elements of odd prime order p . For any $d \in D$, every orbit of $\langle d \rangle$ is of size 1 or p . If $\langle d \rangle$ has more than two orbits, then let O_1 and O_2 be orbits. Now there is some $c \in C$ such that $O_1 \cup O_2$ is the union of the supports of 2-cycles in the disjoint cycle decomposition of c . The subgroup $\langle c, d \rangle$ is thus intransitive.

It remains only to consider the case where $\langle d \rangle$ has exactly two orbits. As $n = 2^a$, so d is a p -cycle fixing exactly one point. Now $n = p + 1$, and so by the Sylow theorems the subgroups of order p in A_n form a single conjugacy class. Thus, it suffices to find a proper subgroup of A_n that contains both a fixed-point-free involution c and an element d of order p .

n	maximal subgroup indices	Condition (4) conjugacy class representatives
5	5, 6, 10	(1 2 3), (1 2 3 4 5)
6	6, 10, 15	(1 2 3 4)(5 6), (1 2 3 4 5)
7	7, 15, 21, 35	(1 2 3 4 5), (1 2 3 4 5 6 7)
8	8, 15, 28, 35, 56	(1 2 3 4)(5 6 7 8), (1 2 3 4 5)

Table 1. Indices of maximal subgroups and generating conjugacy class representatives for A_n , $5 \leq n \leq 8$.

Consider the transitive action of $\mathrm{PSL}_2(p)$ on the set \mathcal{S} of 1-dimensional subspaces of \mathbb{F}_p^2 . Since $|\mathcal{S}| = n$ and $\mathrm{PSL}_2(p)$ is simple, we obtain from the group action a subgroup $H \cong \mathrm{PSL}_2(p)$ of A_n . Then $|H| = (p \cdot (p^2 - 1))/2$, and by the orbit-stabilizer theorem, the stabilizer of any point has order $(p \cdot (p - 1))/2 = p \cdot (2^{a-1} - 1)$. In particular, the subgroup H contains elements of order p and order 2, and no element of order 2 in H fixes any point.

Remark 4.4. Powers of 2 satisfy Condition (4) by Proposition 1.4.

4F. Very small alternating groups. As Lemma 1.8 does not apply when $n \leq 8$, we examine small n separately. The solvable alternating groups (where $n < 5$) all trivially satisfy Condition (5). For $5 \leq n \leq 8$, we present in Table 1 the indices of maximal subgroups of A_n , together with representatives for generating conjugacy classes as in Condition (4). This list is easy to produce either by GAP [2012], or else by hand (using well-known facts about primitive groups of small degree).

For $n = 5$ or 7, these representatives are of prime order, so 5 and 7 satisfy Condition (5). Proposition 1.6 tells us that 8 fails Condition (5), and a similar argument or GAP computation shows that 6 also fails Condition (5).

5. Asymptotic density

In this section, we use part (B) of Lemma 1.8 to prove Theorem 1.5.

Lemma 1.8 tells us that n satisfies Condition (5) unless both the largest prime divisor p of n and the largest prime r that is less than $n - 2$ are small relative to n . This allows us to apply known and conjectured results about prime gaps, which we combine with known results about numbers without large prime divisors (“smooth numbers”).

We will use the following notation:

- We will denote the k -th smallest prime number by p_k . For example, $p_1 = 2$ and $p_2 = 3$.
- For a real number $x > 2$, we will denote by $r(x)$ the largest prime that is no larger than x .

- For positive real numbers x, y , we will denote by $\Psi(x, y)$ the number of positive integers no larger than x which have no prime factor larger than y .

Our strategy is to show that if p is the largest prime divisor of n , then asymptotically $r(n) + p$ is frequently greater than n . We remark that $r(n) \geq n - 2$ only on a set of asymptotic density 0, so we may treat the $r + 2 < n$ condition of Lemma 1.8 as reading $r \leq n$ for the purpose of asymptotic density arguments.

We will require several tools from number theory, as we will describe below. See [Granville 2008] for further background on (5-2) and (5-3), and [Granville 1995] for background and history on (5-4) and (5-5).

5A. Proof of Theorem 1.5(A). Jia [1996] showed that, for any $\epsilon > 0$, there is a prime on the interval $[n, n + n^{1/20+\epsilon}]$ for all n excluding a set of asymptotic density 0. It follows by routine manipulation that

$$(5-1) \quad n - r(n) < n^{1/20} \quad \text{except on a set of asymptotic density 0.}$$

See [Harman 2007, Chapter 9] for further discussion of results of this type.

Dickman [1930] showed that

$$(5-2) \quad \lim_{x \rightarrow \infty} \frac{\Psi(x, x^{1/u})}{x} = \rho(u) \quad \text{for any fixed } u,$$

where ρ denotes the so-called *Dickman–de Bruijn function*, that is, the solution to the differential equation $u\rho'(u) + \rho(u - 1) = 0$.

By combining (5-1) and (5-2) with Lemma 1.8, we see that the desired asymptotic density α satisfies

$$\alpha \geq 1 - \rho(20),$$

as desired. Consulting the table of values for ρ in [Granville 2008, Table 2], we see that $\rho(20) \cong 2.462 \cdot 10^{-29} < 10^{-28}$.

5B. Proof of Theorem 1.5(B). Rankin [1938] showed that

$$(5-3) \quad \lim_{x \rightarrow \infty} \frac{\Psi(x, \log^b x)}{x} = 0, \quad \text{for any } b > 1.$$

Taking $b = 3$ in (5-3), we see that the set of integers n with no prime factor larger than $\log^3 n$ has asymptotic density 0.

The Cramér conjecture [1936, (4)] says that there is a constant C such that

$$(5-4) \quad p_{k+1} - p_k \leq C \log^2 p_k \quad \text{for all } k.$$

In the same paper, Cramér [1936, Theorem II] showed the Riemann hypothesis to imply that

$$(5-5) \quad \lim_{x \rightarrow \infty} \frac{1}{x} \cdot \sum_{\substack{p_k \leq x, \\ p_{k+1} - p_k \geq \log^3 p_k}} (p_{k+1} - p_k) = 0.$$

Thus, if either the Cramér conjecture or the Riemann hypothesis hold, then

$$(5-6) \quad n - r(n) \leq \log^3 r(n) \leq \log^3 n$$

except on a set of asymptotic density zero. Theorem 1.5(B) follows upon combining (5-3) with $b = 3$, (5-6), and Lemma 1.8.

6. Computational results

In this section we describe the verification by computer of Proposition 1.7.

Our program iterates through the integers, beginning with $n = 9$. We factor each integer into primes. If n is a prime power, then n satisfies Condition (3) and hence Condition (2) by Proposition 1.4. In this case, we store $n = r^b$ as the largest prime power known so far in the computation. Otherwise, we find the largest prime power p^a dividing n . The program then checks whether $p^a + r^b$ is greater than n , where r^b is the largest prime power found so far. If so, then n satisfies Condition (2) with p and r by Lemma 1.8. This sieving method succeeds for all but 14,638 of the integers in the interval from 9 to 1,000,000,000. For these remaining integers, the program checks directly which indices of intransitive and imprimitive subgroups are divisible by p (using Lemmas 3.1 and 3.2), and searches for a prime r dividing those that are not. This second method works for all but 22 of the remaining 14,638 integers. For these 22 integers we perform a similar search, using divisors of n other than p . See Table 2 for the results of this search.

Running this program out to $n = 1,000,000,000$ on a 2012 MacBook Pro with the GAP computer algebra system [GAP 2012] takes around 2 weeks. This computation verifies Proposition 1.7.

We approach checking which values of n satisfy Condition (2) with the prime 2 in a similar fashion. When we apply Lemma 1.8, we look for a pair $p^a + r^b > n > r^b$ (where $p^a | n$) as before, but now we require $2 \in \{p, r\}$. This technique gives a positive answer for about 45.7% of the first 1,000,000 integers $n \geq 9$. The remaining values of n require significantly more computation, and as a result we did not examine values of n beyond 1,000,000.

Running the program to check Condition (2) with the prime 2 out to $n = 1,000,000$ takes around a day on a 2012 MacBook Pro. This computation verifies Proposition 1.9. More precisely, 867,247 of the integers between 9 and 1,000,000 satisfy Condition (2) with 2. The histogram in Figure 6.1 shows the density of

n	p^a	Condition (2) prime pairs
$31,416 = 2^3 \cdot 3 \cdot 7 \cdot 11 \cdot 17$	17^1	(2, 7853)
$46,800 = 2^4 \cdot 3^2 \cdot 5^2 \cdot 13$	5^2	(2, 149)
$195,624 = 2^3 \cdot 3^2 \cdot 11 \cdot 13 \cdot 19$	19^1	(2, 3)
$5,504,490 = 2 \cdot 3^3 \cdot 5 \cdot 19 \cdot 29 \cdot 37$	37^1	(3, 5)
$7,458,780 = 2^2 \cdot 3 \cdot 5 \cdot 7^2 \cdot 43 \cdot 59$	59^1	(2, 276251)
$9,968,112 = 2^4 \cdot 3^2 \cdot 7 \cdot 11 \cdot 29 \cdot 31$	31^1	(2, 3)
$12,387,600 = 2^4 \cdot 3^3 \cdot 5^2 \cdot 31 \cdot 37$	37^1	(2, 3)
$105,666,600 = 2^3 \cdot 3 \cdot 5^2 \cdot 13 \cdot 19 \cdot 23 \cdot 31$	31^1	(2, 5)
$115,690,848 = 2^5 \cdot 3 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 41$	41^1	(2, 3)
$130,559,352 = 2^3 \cdot 3 \cdot 7 \cdot 11 \cdot 31 \cdot 43 \cdot 53$	53^1	(2, 112843)
$146,187,444 = 2^2 \cdot 3 \cdot 13 \cdot 19 \cdot 31 \cdot 37 \cdot 43$	43^1	(2, 31)
$225,613,050 = 2 \cdot 3 \cdot 5^2 \cdot 13 \cdot 37 \cdot 53 \cdot 59$	59^1	(2, 516277)
$275,172,996 = 2^2 \cdot 3 \cdot 7 \cdot 29 \cdot 37 \cdot 43 \cdot 71$	71^1	(2, 567367)
$282,429,840 = 2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 29 \cdot 31$	31^1	(2, 29)
$300,688,752 = 2^4 \cdot 3 \cdot 7 \cdot 13 \cdot 23 \cdot 41 \cdot 73$	73^1	(2, 11)
$539,509,620 = 2^2 \cdot 3 \cdot 5 \cdot 13 \cdot 17 \cdot 23 \cdot 29 \cdot 61$	61^1	(2, 1201)
$653,426,796 = 2^2 \cdot 3 \cdot 11 \cdot 19 \cdot 43 \cdot 73 \cdot 83$	83^1	(2, 73)
$696,595,536 = 2^4 \cdot 3^2 \cdot 7 \cdot 13 \cdot 17 \cdot 53 \cdot 59$	59^1	(2, 13)
$784,474,592 = 2^5 \cdot 11 \cdot 29 \cdot 31 \cdot 37 \cdot 67$	67^1	(2, 29)
$798,772,578 = 2 \cdot 3 \cdot 19 \cdot 29 \cdot 41 \cdot 71 \cdot 83$	83^1	(2, 563)
$815,224,800 = 2^5 \cdot 3 \cdot 5^2 \cdot 13 \cdot 17 \cdot 29 \cdot 53$	53^1	(2, 87013)
$851,716,320 = 2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 31 \cdot 37$	37^1	(2, 31)

Table 2. The values of $n \leq 1,000,000,000$ together with their maximal prime power divisors p^a , such that n does not satisfy Condition (2) with p . Each such n satisfies Condition (2) with either 2 or 3.

those n which do not satisfy Condition (2) with 2. We remark that this histogram appears to show that the failing values are concentrated towards the values of n slightly preceding integers that are divisible by a high power of 2.

Source code and output for all computer programs discussed in this section are available in the online supplement as ancillary files. They are also currently available from Woodroffe's web page. A list of the values of $n \leq 1,000,000$ such that n does not satisfy Condition (2) with the prime 2 can be found in the same places.

Acknowledgements

We thank Andrew Granville and Bob Guralnick for their thoughtful remarks. A comment by Ben Green led to a significant improvement in the bound given in Theorem 1.5(A).

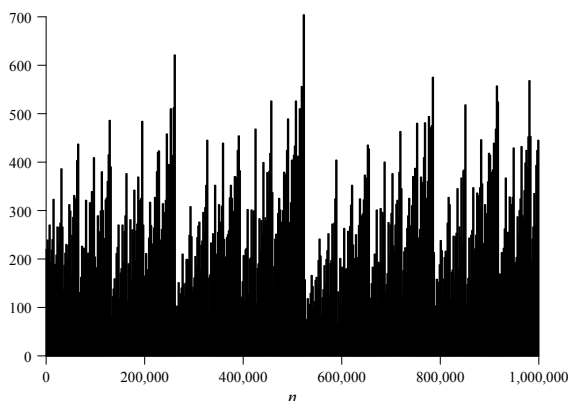


Figure 6.1. A histogram, for $n = 9$ to 1,000,000 in bins of size 2500, showing the density of integers that do not meet Condition (2) with the prime 2.

References

- [Cramér 1936] H. Cramér, “On the order of magnitude of the difference between consecutive prime numbers”, *Acta Arith.* **2**:1 (1936), 23–46. Zbl
- [Damian and Lucchini 2007] E. Damian and A. Lucchini, “The probabilistic zeta function of finite simple groups”, *J. Algebra* **313**:2 (2007), 957–971. MR Zbl
- [Detomi and Lucchini 2015] E. Detomi and A. Lucchini, “Invariable generation with elements of coprime prime-power orders”, *J. Algebra* **423** (2015), 683–701. MR Zbl
- [Dickman 1930] K. Dickman, “On the frequency of numbers containing prime factors of a certain relative magnitude”, *Ark. Mat. Astr. Fys.* **22A**:10 (1930), 1–14. JFM
- [Dixon 1992] J. D. Dixon, “Random sets which invariably generate the symmetric group”, *Discrete Math.* **105**:1–3 (1992), 25–39. MR Zbl
- [Dixon and Mortimer 1996] J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics **163**, Springer, New York, 1996. MR Zbl
- [Dolfi et al. 2012] S. Dolfi, R. M. Guralnick, M. Herzog, and C. E. Praeger, “A new solvability criterion for finite groups”, *J. Lond. Math. Soc.* (2) **85**:2 (2012), 269–281. MR Zbl
- [Eberhard et al. 2017] S. Eberhard, K. Ford, and B. Green, “Invariable generation of the symmetric group”, *Duke Math. J.* **166**:8 (2017), 1573–1590. MR Zbl
- [GAP 2012] “GAP – Groups, Algorithms, and Programming”, version 4.5.5, 2012, available at <http://www.gap-system.org/Releases/4.5.5.html>.
- [Granville 1995] A. Granville, “Harald Cramér and the distribution of prime numbers”, *Scand. Actuar. J.* **1** (1995), 12–28. MR Zbl
- [Granville 1997] A. Granville, “Arithmetic properties of binomial coefficients, I: Binomial coefficients modulo prime powers”, pp. 253–276 in *Organic mathematics* (Burnaby, BC, 1995), edited by J. Borwein et al., CMS Conf. Proc. **20**, American Mathematical Society, Providence, RI, 1997. MR Zbl
- [Granville 2008] A. Granville, “Smooth numbers: computational number theory and beyond”, pp. 267–323 in *Algorithmic number theory: lattices, number fields, curves and cryptography*, edited by

- J. P. Buhler and P. Stevenhagen, *Math. Sci. Res. Inst. Publ.* **44**, Cambridge Univ. Press, 2008. MR Zbl
- [Harman 2007] G. Harman, *Prime-detecting sieves*, London Mathematical Society Monographs Series **33**, Princeton Univ. Press, 2007. MR Zbl
- [Jia 1996] C. Jia, “Almost all short intervals containing prime numbers”, *Acta Arith.* **76**:1 (1996), 21–84. MR Zbl
- [Jordan 1875] C. Jordan, “Sur la limite du degré des groupes primitifs qui contiennent une substitution donnée”, *J. Reine Angew. Math.* **79** (1875), 248–258. MR JFM
- [Kantor et al. 2011] W. M. Kantor, A. Lubotzky, and A. Shalev, “Invariable generation and the Chebotarev invariant of a finite group”, *J. Algebra* **348** (2011), 302–314. MR Zbl
- [Kummer 1852] E. E. Kummer, “Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen”, *J. Reine Angew. Math.* **44** (1852), 93–146. MR Zbl
- [Liebeck et al. 1987] M. W. Liebeck, C. E. Praeger, and J. Saxl, “A classification of the maximal subgroups of the finite alternating and symmetric groups”, *J. Algebra* **111**:2 (1987), 365–383. MR Zbl
- [Niven et al. 1991] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An introduction to the theory of numbers*, 5th ed., Wiley, New York, 1991. MR Zbl
- [Oliver 1975] R. Oliver, “Fixed-point sets of group actions on finite acyclic complexes”, *Comment. Math. Helv.* **50** (1975), 155–177. MR Zbl
- [Rankin 1938] R. A. Rankin, “The difference between consecutive prime numbers”, *J. London Math. Soc.* **S1-13**:4 (1938), 242–247. MR Zbl
- [Shareshian and Woodroofe 2016] J. Shareshian and R. Woodroofe, “Order complexes of coset posets of finite groups are not contractible”, *Adv. Math.* **291** (2016), 758–773. MR Zbl
- [Smith 1941] P. Smith, “Fixed-point theorems for periodic transformations”, *Amer. J. Math.* **63** (1941), 1–8. MR Zbl
- [Thompson 1966] J. G. Thompson, “Hall subgroups of the symmetric groups”, *J. Combinatorial Theory* **1** (1966), 271–279. MR Zbl

Received July 25, 2016. Revised May 12, 2017.

JOHN SHARESHIAN
DEPARTMENT OF MATHEMATICS
WASHINGTON UNIVERSITY IN ST. LOUIS
ST. LOUIS, MO
UNITED STATES
shareshi@math.wustl.edu

RUSS WOODROOFE
DEPARTMENT OF MATHEMATICS & STATISTICS
MISSISSIPPI STATE UNIVERSITY
STARKVILLE, MS
UNITED STATES

and

UNIVERSITY OF PRIMORSKA
UP FAMNIT
KOPER, SLOVENIA
russ.woodroofe@famnit.upr.si

PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

msp.org/pjm

EDITORS

Don Blasius (Managing Editor)
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
blasius@math.ucla.edu

Paul Balmer
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
balmer@math.ucla.edu

Wee Teck Gan
Mathematics Department
National University of Singapore
Singapore 119076
matgwt@nus.edu.sg

Sorin Popa
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
popa@math.ucla.edu

Vyjayanthi Chari
Department of Mathematics
University of California
Riverside, CA 92521-0135
chari@math.ucr.edu

Kefeng Liu
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
liu@math.ucla.edu

Jie Qing
Department of Mathematics
University of California
Santa Cruz, CA 95064
qing@cats.ucsc.edu

Daryl Cooper
Department of Mathematics
University of California
Santa Barbara, CA 93106-3080
cooper@math.ucsb.edu

Jiang-Hua Lu
Department of Mathematics
The University of Hong Kong
Pokfulam Rd., Hong Kong
jhlu@maths.hku.hk

Paul Yang
Department of Mathematics
Princeton University
Princeton NJ 08544-1000
yang@math.princeton.edu

PRODUCTION

Silvio Levy, Scientific Editor, production@msp.org

SUPPORTING INSTITUTIONS

ACADEMIA SINICA, TAIPEI
CALIFORNIA INST. OF TECHNOLOGY
INST. DE MATEMÁTICA PURA E APLICADA
KEIO UNIVERSITY
MATH. SCIENCES RESEARCH INSTITUTE
NEW MEXICO STATE UNIV.
OREGON STATE UNIV.

STANFORD UNIVERSITY
UNIV. OF BRITISH COLUMBIA
UNIV. OF CALIFORNIA, BERKELEY
UNIV. OF CALIFORNIA, DAVIS
UNIV. OF CALIFORNIA, LOS ANGELES
UNIV. OF CALIFORNIA, RIVERSIDE
UNIV. OF CALIFORNIA, SAN DIEGO
UNIV. OF CALIF., SANTA BARBARA

UNIV. OF CALIF., SANTA CRUZ
UNIV. OF MONTANA
UNIV. OF OREGON
UNIV. OF SOUTHERN CALIFORNIA
UNIV. OF UTAH
UNIV. OF WASHINGTON
WASHINGTON STATE UNIVERSITY

These supporting institutions contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its contents or policies.


See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2018 is US \$475/year for the electronic version, and \$640/year for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and Web of Knowledge (Science Citation Index).

The Pacific Journal of Mathematics (ISSN 0030-8730) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2018 Mathematical Sciences Publishers

PACIFIC JOURNAL OF MATHEMATICS

Volume 292 No. 1 January 2018

New characterizations of linear Weingarten spacelike hypersurfaces in the de Sitter space	1
LUIS J. ALÍAS, HENRIQUE F. DE LIMA and FÁBIO R. DOS SANTOS	
Cellular structures using U_q -tilting modules	21
HENNING HAAHR ANDERSEN, CATHARINA STROPPEL and DANIEL TUBBENHAUER	
Meridional rank and bridge number for a class of links	61
MICHEL BOILEAU, YEONHEE JANG and RICHARD WEIDMANN	
Pointwise convergence of almost periodic Fourier series and associated series of dilates	81
CHRISTOPHE CUNY and MICHEL WEBER	
The poset of rational cones	103
JOSEPH GUBELADZE and MATEUSZ MICHAŁEK	
Dual mean Minkowski measures and the Grünbaum conjecture for affine diameters	117
QI GUO and GABOR TOTH	
Bordered Floer homology of $(2, 2n)$ -torus link complement	139
JAEPIIL LEE	
A Feynman–Kac formula for differential forms on manifolds with boundary and geometric applications	177
LEVI LOPES DE LIMA	
Ore’s theorem on cyclic subfactor planar algebras and beyond	203
SEBASTIEN PALCOUX	
Divisibility of binomial coefficients and generation of alternating groups	223
JOHN SHARESHIAN and RUSS WOODROOFE	
On rational points of certain affine hypersurfaces	239
ALEXANDER S. SIVATSKI	



0030-8730(201801)292:1;1-Z