Bull. Aust. Math. Soc. **83** (2011), 138–157
doi:10.1017/S0004972710001723

ON COMMON DIVISORS OF MULTINOMIAL COEFFICIENTS

GEORGE M. BERGMAN

(Received 20 March 2010)

Abstract

Erdős and Szekeres ['Some number theoretic problems on binomial coefficients', *Aust. Math. Soc. Gaz.* **5** (1978), 97–99] showed that for any four positive integers satisfying $m_1 + m_2 = n_1 + n_2$, the two binomial coefficients $(m_1 + m_2)!/m_1!m_2!$ and $(n_1 + n_2)!/n_1!n_2!$ have a common divisor greater than 1. The analogous statement for k-element families of k-nomial coefficients ($k > 1$) was conjectured in 1997 by David Wasserman.

Erdős and Szekeres remark that if m_1, m_2, n_1, n_2 as above are all greater than 1, there is probably a lower bound on the common divisor in question which goes to infinity as a function of $m_1 + m_2$. Such a bound is obtained in Section 2.

The remainder of this paper is devoted to proving results that narrow the class of possible counterexamples to Wasserman's conjecture.

2010 *Mathematics subject classification*: primary 11B65; secondary 11A41, 11A63, 20B30.

Keywords and phrases: common divisors of multinomial coefficients.

In the above Abstract I have worded Erdős and Szekeres's result so as to make clear the intended generalization to k-nomial coefficients. In the next two sections, however, I formulate it essentially as they do in [2].

I have 'trimmed the fat' from an earlier, lengthier version of this paper. The material removed can be found in [1].

I am indebted to Pace Nielsen for a number of valuable corrections and comments.

1. Background: the result of Erdős and Szekeres

We begin with two quick proofs of Erdős and Szekeres's result, one roughly as in [2], the other group-theoretic.

THEOREM 1 (Erdős and Szekeres [2]). *Suppose that i, j, N are integers with $0 < i \leq j \leq N/2$. Then $\binom{N}{i}$ and $\binom{N}{j}$ have a common divisor greater than* 1.

Any updates, errata or related references, learned of after publication of this paper will be recorded at http://math.berkeley.edu/~gbergman/papers/.

PROOF FOLLOWING [2]. Note that

$$\binom{N}{i}\binom{N-i}{j-i} = \binom{N}{j}\binom{j}{i}. \tag{1}$$

Now if the first factors on the two sides of the above equation were relatively prime, the second factor on each side would have to be divisible by, and hence at least as large as, the first factor on the other side. In particular, we would have $\binom{j}{i} \geq \binom{N}{i}$. Multiplying both sides by $i!$, this would say that

$$j(j-1)\cdots(j-i+1) \geq N(N-1)\cdots(N-i+1),$$

which is clearly false. □

GROUP-THEORETIC PROOF. Let X denote the set of decompositions (A, B) of $\{1, \ldots, N\}$ into a set A of i elements and a complementary set B of $N - i$ elements, and Y the set of decompositions (C, D) of the same set into complementary sets of j and $N - j$ elements. The permutation group S_N acts transitively on each of these sets, which have cardinalities $\binom{N}{i}$ and $\binom{N}{j}$, respectively.

Consider the product action of S_N on $X \times Y$. Each orbit must have cardinality divisible by both $\mathrm{card}(X)$ and $\mathrm{card}(Y)$, hence if these were relatively prime, every orbit would have cardinality at least $\mathrm{card}(X \times Y)$, so there could be only one orbit. But in fact, the orbits correspond to the possible choices of cardinalities for $A \cap C$, $B \cap C$, $A \cap D$ and $B \cap D$, and these can be chosen in different ways; for example, so that $A \subseteq C$ or so that $A \subseteq D$, so there are at least two orbits. □

2. Lower bounds

The above two proofs are not as different as they look: the value (1) is the trinomial coefficient $N!/i!(j-i)!(N-j)!$, which counts the orbit of $X \times Y$ consisting of decompositions with $A \subseteq C$. (The right-hand side of (1) essentially says 'break $\{1, \ldots, N\}$ into C and D, then choose A within C', while the left-hand side says 'break $\{1, \ldots, N\}$ into A and B, then choose $C - A$ within B'.)

Note that in the first proof above, the ratio of the numbers we compared,

$$N(N-1)\cdots(N-i+1)$$

and $j(j-1)\cdots(j-i+1)$, can be written $(N/j)((N-1)/(j-1))\cdots((N-i+1)/(j-i+1)) \geq 2^i$. As noted in [2], this implies that $\binom{N}{i}$ and $\binom{N}{j}$ have a common divisor greater than or equal to 2^i. This estimate goes to infinity with i, but gives no information on how the greatest common divisor of these numbers behaves as a function of N for i fixed; indeed, it is observed in [2] that when $i = 1$, that greatest common divisor is 2 in infinitely many cases. Let us now show, however, as Erdős and Szekeres suspected, that when

$$i > 1, \tag{2}$$

https://doi.org/10.1017/S0004972710001723 Published online by Cambridge University Press

that greatest common divisor goes to infinity with N. To this end, we shall bring in the other orbits of our action of S_N.

Fixing N, i and j, we find that for each orbit of pairs of decompositions $\{1, \ldots, N\} = A \sqcup B = C \sqcup D$, the integer $h = \mathrm{card}(A \cap D)$ is an invariant of the orbit, uniquely determining the orbit, and that this invariant can take on any value satisfying $0 \leq h \leq i$. The cardinality of the orbit associated with h is given by the 4-nomial coefficient

$$\binom{N}{i}\binom{i}{h}\binom{N-i}{j-i+h} = Q_h = \binom{N}{j}\binom{j}{i-h}\binom{N-j}{h}. \tag{3}$$

By (3), each of these values Q_h must be divisible by the integer

$$L = \mathrm{lcm}\left(\binom{N}{i}, \binom{N}{j}\right). \tag{4}$$

Our idea is that as h varies from 0 to i, Q_h should vary in a 'nice' fashion; but if the above value L were too large, the big gaps between the available values would make this impossible. Let us try out this idea on Q_0, Q_1 and Q_2. Since multinomial coefficients are multiplicative in nature, let us subtract the product of the first and last of these from the square of the middle one, after multiplying these products by integer factors ($2i$ and $i-1$ respectively) that compensate for the different denominators of the binomial coefficients in question. Expanding the Q_h by the right-hand expression in (3), we can say that L^2 divides

$$\begin{aligned}
&(i-1)Q_1^2 - 2iQ_0Q_2 \\
&\quad = \binom{N}{j}^2 \left((i-1)\binom{j}{i-1}^2\binom{N-j}{1}^2\right. \\
&\qquad\quad \left. - 2i\binom{j}{i}\binom{j}{i-2}\binom{N-j}{0}\binom{N-j}{2}\right) \\
&\quad = \binom{N}{j}^2\binom{j}{i-2}^2\left((i-1)\left(\frac{j-i+2}{i-1}\right)^2\left(\frac{N-j}{1}\right)^2\right. \\
&\qquad\quad \left. - 2i\,\frac{(j-i+2)(j-i+1)}{i(i-1)}\,\frac{(N-j)(N-j-1)}{2\cdot 1}\right) \\
&\quad = \frac{(j-i+2)(N-j)}{i-1}\binom{N}{j}^2\binom{j}{i-2}^2 \\
&\qquad\quad \times ((j-i+2)(N-j) - (j-i+1)(N-j-1)) \\
&\quad = \frac{(j-i+2)(N-j)}{i-1}\binom{N}{j}^2\binom{j}{i-2}^2(N-i+1).
\end{aligned} \tag{5}$$

Since the above expression is positive, it gives an upper bound on L^2. Moreover, the cancellation, at the last step, of the degree-two terms in the final parenthesis gives the goal we were aiming for: the above upper bound is of smaller magnitude than the values we started with. We now make some estimates to get a simpler expression. Note that $j-i+2 \leq j \leq N/2$, $N-j < N$, $\binom{j}{i-2} \leq \binom{N}{i-2}/2^{i-2}$ (cf. the second paragraph of this section), and $N-i+1 < N$. Hence (5) gives

$$L^2 < \frac{N^3}{2^{2i-3}(i-1)} \binom{N}{j}^2 \binom{N}{i-2}^2. \tag{6}$$

Now the greatest common divisor of $\binom{N}{i}$ and $\binom{N}{j}$ is their product divided by L. When we divide their product by the square root of the right-hand side of (6), the factors $\binom{N}{j}$ cancel, while $\binom{N}{i}$ in the product and $\binom{N}{i-2}$ in the bound on L almost cancel, with quotient $(N-i+2)(N-i+1)/i(i-1)$. So the greatest common divisor is at least

$$\frac{(N-i+2)(N-i+1)}{i(i-1)} \left(\frac{2^{2i-3}(i-1)}{N^3} \right)^{1/2}. \tag{7}$$

Bounding $N-i+2$ and $N-i+1$ below by $N/2$, we get the final bound of the following theorem.

THEOREM 2. *Suppose that i, j, N are integers with $2 \leq i \leq j \leq N/2$. Then the greatest common divisor of $\binom{N}{i}$ and $\binom{N}{j}$ is bounded below by (7); hence by*

$$N^{1/2} 2^{i-7/2} / i(i-1)^{1/2}. \tag{8}$$

□

For each i, (8) goes to infinity as a function of N; clearly it can also be weakened to a bound that goes to infinity in N independent of i.

Can one get still better bounds if one assumes that $i > 2$? Our calculation above was based on the idea that $Q_0 Q_1^{-2} Q_2$ should be well behaved; note that the exponents in that expression are the binomial coefficients 1, 2, 1 taken with alternating signs; so for $i \geq 3$, the expression $Q_0 Q_1^{-3} Q_2^3 Q_3^{-1}$ might be still better behaved, suggesting that one look at the difference between appropriate integer multiples of $Q_0 Q_2^3$ and $Q_1^3 Q_2$. But in fact, the higher powers of L and N that would be involved in the analog of (6) seems to negate the advantage coming from the larger number of terms which cancel in that difference. On the other hand, for $i \geq 4$, an appropriate linear combination of $Q_0 Q_4$, $Q_1 Q_3$ and Q_2^2 might yield an improved estimate without suffering from this disadvantage. I leave these questions to others to investigate.

(We remark that the focus of [2] was not the question answered above, but the value of the largest prime dividing both $\binom{N}{i}$ and $\binom{N}{j}$.)

3. Wasserman's conjecture on multinomial coefficients

Before examining the conjectured generalization of Theorem 1, let us set up notation and language for multinomial coefficients, and record some immediate properties thereof.

https://doi.org/10.1017/S0004972710001723 Published online by Cambridge University Press

DEFINITION 3. If $a_1, \dots, a_k$ are nonnegative integers, we define

$$\mathrm{ch}(a_1, \dots, a_k) = (a_1 + \cdots + a_k)!/a_1! \cdots a_k! \tag{9}$$

(modeled on the reading 'n-choose-m' for binomial coefficients). Thus, $\mathrm{ch}(a_1, \dots, a_k)$ counts the ways of partitioning a set of cardinality $a_1 + \cdots + a_k$ into a list of subsets, of respective cardinalities $a_1, \dots, a_k$.

We shall call an integer (9) a k-nomial coefficient of *weight* $a_1 + \cdots + a_k$. It will be called a *proper* k-nomial coefficient if none of the a_i is zero.

A k-nomial coefficient will also be called a *multinomial* coefficient of *nomiality* k.

(The more usual notation for multinomial coefficients is $\binom{a_1+\cdots+a_k}{a_1,\dots,a_k}$; but $\mathrm{ch}(a_1, \dots, a_k)$ is visually simpler.)

We note three straightforward identities. First, 'monomial' coefficients are trivial:

$$\mathrm{ch}(n) = 1. \tag{10}$$

Second, the operator ch is commutative, that is, invariant under permutation of its arguments:

$$\mathrm{ch}(a_1, \dots, a_k) = \mathrm{ch}(a_{\pi(1)}, \dots, a_{\pi(k)}) \quad \text{for } \pi \in S_k. \tag{11}$$

Finally, given any *string of strings* of nonnegative integers, $a_1, \dots, a_{j_1}; \dots; a_{j_{k-1}+1}, \dots, a_{j_k}$, we have the associativity-like relation

$$\begin{aligned}\mathrm{ch}(a_1, \dots, a_{j_k}) = \mathrm{ch}(a_1 + \cdots + a_{j_1},\ \dots, a_{j_{k-1}+1} + \cdots + a_{j_k})\\ \cdot\, \mathrm{ch}(a_1, \dots, a_{j_1}) \cdot \dots \cdot \mathrm{ch}(a_{j_{k-1}+1}, \dots, a_{j_k}).\end{aligned} \tag{12}$$

In particular, (12) tells us that a multinomial coefficient is a multiple of any multinomial coefficient (generally of smaller nomiality) obtained from it by collecting and summing certain of its arguments.

In the language introduced above, Erdős and Szekeres's result says that any two proper binomial coefficients of equal weight N have a common divisor greater than 1. This implies the same conclusion for two proper k-nomial coefficients of equal weight N, for any $k \geq 2$, since (12) implies that these are multiples of two proper binomial coefficients of weight N. But a stronger statement would be the following.

CONJECTURE 4 (David Wasserman, personal communication, 1997; cf. [4, p. 131]). For every $k > 1$, every family of k proper k-nomial coefficients of equal weight N has a common divisor greater than 1.

Note the need for the condition $k > 1$: by (10), the corresponding statement with $k = 1$ is false.

It is not clear whether one can somehow adapt the methods of the preceding sections to prove this conjecture. Even looking at the case $k = 3$, one finds that the set of orbits into which the product of three orbits of 3-fold partitions of $\{1, \dots, N\}$ decomposes is an unwieldy structure, in which the single index 'h' that parametrized

https://doi.org/10.1017/S0004972710001723 Published online by Cambridge University Press

the orbits in a product of two orbits of 2-fold partitions is replaced by 20 parameters (computation sketched in [1, Section 1]). Moreover, to get divisors common to a threesome of trinomial coefficients by studying the set of their common multiples, one would presumably have to apply the inclusion–exclusion principle, for which one would need *upper* bounds on their *pairwise* common divisors.

In the remaining sections we will take a more pedestrian approach, and obtain results narrowing the class of cases where one might look for counterexamples to the above conjecture.

4. A lemma of Kummer

A basic tool in studying divisibility properties of multinomial coefficients is the next result, proved by Kummer for binomial coefficients, that is, for $k = 2$. That proof generalizes without difficulty to arbitrary k. (The result appears in [6] as the third-from-last display on page 116. The symbol $\Pi(n)$ there denotes what is now written $n!$.)

LEMMA 5 (After Kummer [6]; cf. [5]). *Let $a_1, \ldots, a_k$ be natural numbers, and p a prime. Then the power to which p divides* $\mathrm{ch}(a_1, \ldots, a_k)$ *is equal to the number of 'carries' that must be performed when the sum $a_1 + \cdots + a_k$ is computed in base p.*

In particular, $\mathrm{ch}(a_1, \ldots, a_k)$ *is relatively prime to p if and only if that sum can be computed 'without carrying', that is, if and only if, for each i, the sum of the coefficients of p^i in the base-p expressions for $a_1, \ldots, a_k$ is less than p (and hence gives the coefficient of p^i in the base-p expression for $a_1 + \cdots + a_k$).* □

REMARKS. In the classical case $k = 2$, the meaning of the 'number of carries' is clear: it is the number of values of i for which the coefficient of p^i in the expression for $a_1 + a_2$ is not the sum of the corresponding coefficients from a_1 and a_2, possibly augmented by a 1 carried from the next-lower column, but rather, the result of subtracting p from that sum. In the case of k summands $a_1, \ldots, a_k$, we could define the number of carries recursively in terms of two-term addition, as the sum of the number of 'carries' that occur in adding a_2 to a_1, the number that occur in adding a_3 to that sum, and so on. Or we could consider the computation of $a_1 + \cdots + a_k$ to be performed all at once, by a process of successively adding up, for each i, the coefficients of p^i in the k summands, together with any value carried from lower digits, writing the result as $s_i p + t_i$ with $0 \leq t_i < p$, taking t_i to be the coefficient of p^i in the sum, and 'carrying' s_i into the next column. We would then consider this step of the calculation to contribute s_i to our tally of the number of 'carries'. Since turning a coefficient p of p^i into a coefficient 1 of p^{i+1} reduces the sum of the digits by $p - 1$, the number of carries under either description can be evaluated by summing the digits in the base-p expressions for $a_1, \ldots, a_k$, subtracting from their total the sum of the digits of $a_1 + \cdots + a_k$, and dividing by $p - 1$.

However, we will not need the exact value of the number of carries, but only to know when it is zero, and for this, the easy criterion in the second paragraph of the above lemma suffices.

https://doi.org/10.1017/S0004972710001723 Published online by Cambridge University Press

In discussing Conjecture 4, the following language will be useful.

DEFINITION 6. Given a positive integer N and a prime p, we will call a decomposition of N as a sum of positive integers $N = a_1 + \cdots + a_k$ *p-acceptable* if $\mathrm{ch}(a_1, \ldots, a_k)$ is not divisible by p; equivalently, if, for each i, the ith digit of the base-p expression for N is the sum of the ith digits of the base-p expressions for $a_1, \ldots, a_k$.

This language reflects the point of view of someone trying to find a counterexample to the conjecture: such a counterexample for given k and N would require a set of k decompositions of N into k positive summands, such that for every prime p, at least one of these decompositions is p-acceptable. And, indeed, in obtaining our results supporting the conjecture, we shall in general put ourselves in the position of trying to find such a counterexample, and discover obstructions to getting p-acceptability for all p.

Note that by the last criterion in Definition 6, we have the following result.

If an integer N has digit-sum less than k when written to the prime base p, then every proper k-nomial coefficient of weight N is divisible by p. (13)

For $k = 3$, the condition of digit-sum less than k to base p means that N can be written p^e or $p^e + p^{e'}$. Examining the first 100 positive integers, one finds that 75 of them can be so written for some prime p, and so cannot be the weight of a counterexample to Wasserman's conjecture for that k. The remaining 25 are

$$\begin{gathered}15, 21, 35, 39, 45, 51, 52, 55, 57, 63, 69, 70, 75, 76,\\ 77, 78, 85, 87, 88, 91, 92, 93, 95, 99, 100.\end{gathered} \tag{14}$$

My early pursuit of this problem involved case-by-case elimination of these values. In [1, Section 3] I reproduce the *ad hoc* arguments for one of the less easily eliminated cases, $N = 78$. Below, however, we shall give general arguments that exclude all values in a much larger range.

Let us note one other immediate consequence of the final criterion of Definition 6.

If $N = a_1 + \cdots + a_k$ is a 2-acceptable decomposition of a positive integer, then the powers of 2 dividing $a_1, \ldots, a_k$ are distinct. (15)

5. Preview of results on Wasserman's conjecture for $k = 3$

Suppose that we are given a positive integer N, and wish to know whether it is a counterexample to Conjecture 4 for $k = 3$; that is, whether there exist three decompositions of N as sums of three positive integers, such that for every prime p, one of those decompositions is p-acceptable.

If so, then one of those decompositions must have a summand quite close to N. Namely, if $p_{\max}^d$ is the largest prime power less than or equal to N, then a decomposition that is $p_{\max}$-acceptable must include a summand greater than or equal

https://doi.org/10.1017/S0004972710001723 Published online by Cambridge University Press

to $p_{\max}^d$ (since on adding the summands in that decomposition in base $p_{\max}$, the digit in the $p_{\max}^d$ column of N cannot arise by carrying). Let us write that decomposition as

$$N = (N - i - j) + i + j, \tag{16}$$

where $N - i - j \geq p_{\max}^d$, so that i and j are small. Note that the corresponding trinomial coefficient

$$\mathrm{ch}(N - i - j, i, j) = N(N-1) \cdots (N - i - j + 1)/i!j! \tag{17}$$

is not divisible by any prime *not* dividing one of $N, N-1, \ldots, N-i-j+1$; so primes not dividing any of those integers can be ignored in studying the conditions that must be satisfied by the other two decompositions of N. On the other hand, $\mathrm{ch}(N-i-j, i, j)$ *will* tend to be divisible by the primes that divide one of N, $N-1$, $\ldots$, $N-i-j+1$: that can only fail if the relatively small denominator $i!j!$ in (17) cancels all occurrences of those primes in the numerator.

The further study of this situation bifurcates into two cases: if i and j are as small as possible, namely, both equal to 1, then in deducing conditions that must be satisfied by the other two decompositions, we have the advantage of knowing that no primes are cancelled by the denominator $i!j!$ in (17); on the other hand, the only primes we have to work with are those dividing $N(N-1)$. We shall study this situation in the next section, and show that there can be no such example with $N < 1726$, or, if N is even, with $N < 6910$.

In Section 7 we study the reverse situation, where $i + j > 2$. Here the use of the primes dividing $N(N-1)(N-2)$ will prove significantly stronger than the use of primes dividing $N(N-1)$, but the cancellation of factors by the denominator $i!j!$ will take its toll. That problem is not serious for low values of $i + j$: we will find that there can be no counterexamples with $2 < i + j < 11$. Thus, in any counterexample falling under this case we must have $N - p_{\max}^d \geq 11$. Looking individually at the first few N satisfying that inequality, and applying *ad hoc* considerations to these, we shall show that there are no counterexamples with $N < 785$.

What about the primes dividing $(N-3) \cdots (N-i-j+1)$? For any particular N, these can be useful in excluding possible counterexamples; but the general methods of Section 7 below cannot make use of them. Perhaps some reader will succeed in doing so.

6. The case $i = j = 1$

The proposition below gives the first of the two results previewed above, and a little more. In the proof, and the remainder of this paper, by ‘the prime power factors of N’ we shall mean the factors occurring in the decomposition of N into positive powers of *distinct* primes. (So in this usage, 4 is among the ‘prime power factors’ of 12, but 2 is not.)

https://doi.org/10.1017/S0004972710001723 Published online by Cambridge University Press

Proposition 7. *Suppose that N is a positive integer having decompositions with positive integer summands,*

$$N = (N-2) + 1 + 1, \quad N = a_1 + a_2 + a_3, \quad N = b_1 + b_2 + b_3, \tag{18}$$

such that

$$\textit{for every prime } p\textit{, at least one of the decompositions of (18) is } p\textit{-acceptable.} \tag{19}$$

Then $N \geq 1726 = 2^6 \cdot 3^3 - 2$.
If N is even, then in fact $N \geq 6910 = 2^8 \cdot 3^3 - 2$.
In either case, $N - 1$ is divisible by at least three distinct primes.

Proof. From the discussion in the last section, we see that for every prime p dividing N or $N-1$, one of the last two decompositions of (18) must be p-acceptable. Thus, if N is divisible by p^d, then looking at the last d digits of the base-p expression of N in the light of Definition 6, we see that p^d must divide all three summands in one of those two decompositions; that is, either all three of a_1, a_2, a_3 or all three of b_1, b_2, b_3. Hence, $N^3 \mid a_1a_2a_3b_1b_2b_3$. In the same way, we see that each prime power factor of $N-1$ must either divide two of a_1, a_2, a_3 or two of b_1, b_2, b_3, hence $(N-1)^2 \mid a_1a_2a_3b_1b_2b_3$. Since N and $N-1$ are relatively prime, this gives

$$N^3(N-1)^2 \mid a_1a_2a_3b_1b_2b_3. \tag{20}$$

On the other hand, it is easy to verify that for any positive real number, the decomposition into three nonnegative summands having the largest product is the one in which each summand is one third of the total; so $a_1a_2a_3 \leq (N/3)(N/3)(N/3)$; and likewise for the b_i:

$$a_1a_2a_3 \leq N^3/3^3, \quad b_1b_2b_3 \leq N^3/3^3. \tag{21}$$

At this point, we could combine (20) and (21) to get a lower bound on N. But let us first strengthen each of (20) and (21) a little, using some special considerations involving the prime 2. That prime necessarily divides $N(N-1)$; assume without loss of generality that $a_1 + a_2 + a_3$ is 2-acceptable. Then by (15), the powers of 2 dividing a_1, a_2 and a_3 are distinct. If $2|N$, occurring, say, to the dth power, this means that $a_1a_2a_3$ must be divisible not merely by the factor $2^d2^d2^d = 2^{3d}$ implicit in our derivation of (20), but by $2^d2^{d+1}2^{d+2} = 2^{3d+3}$. If, rather $2 \mid N-1$, again, say, to the dth power, we can merely say that a_1, a_2 and a_3 include, along with one odd term, terms divisible by 2^d and 2^{d+1}, giving a divisor 2^{2d+1} in place of the 2^{2d} implicit in (20). Thus, we can improve (20) to

$$2N^3(N-1)^2 \mid a_1a_2a_3b_1b_2b_3, \quad \text{and if } N \text{ is even, } 8N^3(N-1)^2 \mid a_1a_2a_3b_1b_2b_3. \tag{22}$$

To improve (21), on the other hand, consider three real numbers

$$r_1 \geq r_2 \geq r_3 \tag{23}$$

https://doi.org/10.1017/S0004972710001723 Published online by Cambridge University Press

(which we shall assume given with specified base-2 expressions, so that, for example, 1.000 . . . and 0.111 . . . are, for the purposes of this discussion, distinct), subject to the condition that

$$\text{there is no need to carry when } r_1, r_2, r_3 \text{ are added in base 2;} \tag{24}$$

and suppose that we want to know how large the number

$$r_1 r_2 r_3/(r_1 + r_2 + r_3)^3 \tag{25}$$

(regarded as a real number, without distinguishing between alternative base-2 expansions if these exist) can be. Note that if, in one of the r_i, we change a base-2 digit 1, other than the highest such digit, to 0, that is, subtract 2^d for appropriate d, and simultaneously, for some $j > i$ (see (23)), add 2^d to r_j (change the corresponding digit, which was 0 by (24), to 1), then, proportionately, the decrease in r_i will be less than the increase in r_j. From this it is easy to deduce that for fixed $r_1 + r_2 + r_3$, we will get the largest possible value for (25) by letting r_1 contain only the leftmost digit 1 of that sum, r_2 only the next 1, and r_3 everything else. (To make this argument rigorous, we have to know that (25) assumes a largest value. We can show this by regarding the set of 3-tuples of strings of 1s and 0s, with a specified number of these to the left of the decimal point and the rest to the right, and with $r_1 \geq 1$ and no two members of our 3-tuple having 1s in the same position, as a compact topological space under the product topology. We can then interpret (25) as a continuous real-valued function on that space, and conclude that it attains a maximum.)

More subtly, I claim that if some digit of $r_1 + r_2 + r_3$ after the leading 1 is 0, then the value (25) will be increased on replacing that digit by 1 in r_3, and hence in $r_1 + r_2 + r_3$. This can be deduced using the fact that the partial derivative of (25) with respect to r_3 is positive, together with some *ad hoc* considerations in the case where the digit in question has value greater than r_2. Since (25) is invariant under multiplication of all r_i by a common power of 2 ('shifting the decimal point'), it is not hard to deduce that it is maximized when r_1, r_2 and r_3 have base-2 expansions 1_2, 0.1_2 and $0.0111\ldots_2$. In that case, its value is $(1 \cdot 1/2 \cdot 1/2)/(1 + 1/2 + 1/2)^3 = 2^{-5}$. Thus we can improve the first inequality of (21) to

$$a_1 a_2 a_3 \leq N^3/2^5. \tag{26}$$

(We cannot similarly improve the second inequality, since the decomposition $b_1 + b_2 + b_3$ need not be 2-acceptable, that is, need not satisfy the analog of (24).)

If we now combine (21), so improved, with the first assertion of (22), we get

$$2N^3(N-1)^2 \leq (N^3/2^5)(N^3/3^3). \tag{27}$$

So

$$(N-1)^2 \leq N^3/(2^6 \cdot 3^3), \quad \text{so}$$
$$N^3/(N-1)^2 \geq 2^6 \cdot 3^3.$$

https://doi.org/10.1017/S0004972710001723 Published online by Cambridge University Press

Expanding the left-hand side in powers of $N-1$, we get $(N-1)+3$, plus terms whose sum becomes less than 1 as soon as $N \geq 5$. Since the above inequality certainly cannot be satisfied by any integer N with $1 < N < 5$, we can discard those terms, getting

$$N+2 \geq 2^6 \cdot 3^3.$$

This gives the first assertion of the proposition. When N is even, we use the second inequality of (22) in place of the first, getting the second assertion.

To prove the final assertion, suppose that $N-1$ were the product of two prime powers. (For brevity, we consider this to include the case where $N-1$ is itself a prime power, putting in a dummy second prime power 1.) Then each of these would divide either two summands in the decomposition $N = a_1 + a_2 + a_3$, or two summands in the decomposition $N = b_1 + b_2 + b_3$. If they each divided two summands in the same decomposition, then they would both divide at least one of those summands, making that summand greater than or equal to $N-1$, which is impossible if the three terms of the decomposition are to sum to N. So instead, one prime power divisor of $N-1$, which we shall write r, must divide two terms of $a_1 + a_2 + a_3$, and the other, which we shall write s, must divide two terms of $b_1 + b_2 + b_3$. Moreover, since every prime power dividing N divides either all of a_1, a_2, a_3 or all of b_1, b_2, b_3, we can write $N = tu$ where t divides all of the former and u divides all of the latter. Now since $a_1 + a_2 + a_3$ has all terms divisible by t and at least two divisible by r, and sums to N, we have $N > 2rt$; and similarly, we have $N > 2su$. Multiplying, we get $N^2 > 4rstu = 4N(N-1)$, which is impossible. □

REMARK. If one tries to extend the argument of the above paragraph to the case where $N-1$ is a product of three prime powers, one discovers one case which there is no obvious way to exclude: one of our given decompositions, say $N = a_1 + a_2 + a_3$, might be p-acceptable for all three of those primes, with one prime power factor dividing a_1 and a_2, another dividing a_1 and a_3, and the third dividing a_2 and a_3. The product t of the prime power factors of N that divide all of a_1, a_2, a_3 could then be nontrivial, though it would have to be smaller than each of the three prime power factors of $N-1$.

7. The case $i + j > 2$

Let us now consider a possible counterexample to Conjecture 4 for $k = 3$ of the contrary sort, where the member of our triad of decompositions involving a summand greater than or equal to $p_{\max}^d$,

$$N = (N-i-j) + i + j, \tag{28}$$

has at least one of the remaining summands, i and j, greater than 1. We will find it most convenient to begin by assuming that we are given only the other two decompositions in our triad,

$$N = a_1 + a_2 + a_3, \qquad N = b_1 + b_2 + b_3, \tag{29}$$

https://doi.org/10.1017/S0004972710001723 Published online by Cambridge University Press

and develop results on such a pair of decompositions, from which we will subsequently obtain constraints on the decomposition (28).

The primes dividing $N(N-1)(N-2)$ that will eventually have to be taken care of by the decomposition (28) are given a name in the following definition.

DEFINITION 8. Given two decompositions (29) of an integer N into positive integer summands, we shall call a prime p *relevant* (with respect to (29)) if it divides $N(N-1)(N-2)$, but neither of the decompositions (29) is p-acceptable.

If p is a relevant prime, and p^d $(d>0)$ a prime power factor (in the sense defined at the beginning of the preceding section) of any of N, $N-1$ or $N-2$, we will call p^d a *relevant prime power*.

To measure the impact of the relevant primes in the estimates to be made, we define

$$\begin{aligned} C = \text{ the product of:}& \\ &\text{all relevant prime power factors of } N-2,\\ &\text{the squares of all relevant prime power factors of } N-1,\\ &\text{and the cubes of all relevant prime power factors of } N. \end{aligned} \tag{30}$$

(Note that if 2 is a relevant prime and N is even, then the computation of C will involve both the power of 2 dividing $N-2$, and the cube of the power of 2 dividing N.)

The next result, using ideas similar to those of the preceding section, shows that C must be fairly large.

LEMMA 9. *In the situation of (29) and (30), one always has*

$$C > 3^6(1-4N^{-1}). \tag{31}$$

(In particular if $N \geq 12$, then $C > 486$, and if $N \geq 81$, then $C > 693$.) If, moreover, 2 *is not a relevant prime (with respect to (29)), then*

$$C > 3^3 \cdot 2^6(1-4N^{-1}). \tag{32}$$

PROOF. Let us write C_i for the product of the relevant prime powers dividing $N-i$ $(i=0,\,1,\,2)$. Then we see (from the definition of p-acceptability) that each prime power dividing N/C_0 will either divide all of a_1, a_2, a_3 or all of b_1, b_2, b_3, each prime power dividing $(N-1)/C_1$ will either divide two of a_1, a_2, a_3 or two of b_1, b_2, b_3, and each prime power dividing $(N-2)/C_2$ will either divide at least one of a_1, a_2, a_3 or at least one of b_1, b_2, b_3. Hence $a_1a_2a_3b_1b_2b_3$ will be divisible by $(N-2)/C_2$, by $(N-1)^2/C_1^2$, and by N^3/C_0^3. Moreover, the only prime that can divide more than one of three successive integers is 2, so $a_1a_2a_3b_1b_2b_3$ will be divisible by the product of these integers, $N^3(N-1)^2(N-2)/C$, possibly adjusted by an appropriate power of 2.

That adjustment will not be needed if 2 is a relevant prime, since in that case, by definition of the C_i, those remove all divisors 2 from our expression. It also will

https://doi.org/10.1017/S0004972710001723 Published online by Cambridge University Press

not come in if N is odd, since then only one of $N-2$, $N-1$, N, namely $N-1$, is divisible by 2. So in both of those cases we have

$$N^3(N-1)^2(N-2)/C \mid a_1a_2a_3b_1b_2b_3. \tag{33}$$

Combining this with (21), we get, in these cases

$$N^3(N-1)^2(N-2)/C \leq N^6/3^6, \tag{34}$$

that is,

$$C \geq 3^6(1-N^{-1})^2(1-2N^{-1}). \tag{35}$$

(We cannot improve (21) using (26) in this calculation: the argument that previously allowed us to do so only applies if 2 is not a relevant prime.) When we expand the product of the last two factors in (35), we see that the N^{-2} term has coefficient $+5$ and the N^{-3} term coefficient -2, so their sum is positive for all $N \geq 1$, and we may drop those terms, getting (31) under these conditions; in particular, whenever 2 is a relevant prime.

We now consider the case where 2 is not a relevant prime. Suppose that the decomposition $a_1+a_2+a_3$ is 2-acceptable. Then we can, as in the proof of Proposition 7, replace the first inequality of (21) by (26), and so improve our upper bound on $a_1a_2a_3b_1b_2b_3$ from $N^6/3^6$ to $N^6/3^3 \cdot 2^5$.

Now if N is odd, we have noted that we still have (34); moreover, as in the proof of Proposition 7, we can use (15) to put a factor of 2 on the left-hand side of that inequality (since if $N-1$ is divisible by 2^d, then $a_1a_2a_3$ will be divisible by 2^d2^{d+1}). Combining this with the modification of the right-hand side indicated in the preceding paragraph, we get (32) for such N.

When N is even, we must analyze more closely the relation between the powers of 2 dividing $N^3(N-1)^2(N-2)$ and $a_1a_2a_3$. Exactly one of N and $N-2$ will be divisible by 2^d for some $d>1$. Assume first that $2^d \mid N$. Then the power of 2 dividing $N^3(N-1)^2(N-2)$ is $2^{3d}\cdot 2^0 \cdot 2^1 = 2^{3d+1}$, while the power dividing $a_1a_2a_3$ will be at least $2^d \cdot 2^{d+1} \cdot 2^{d+2} = 2^{3d+3}$, giving *two* extra powers of 2, and hence an inequality that is in fact stronger than (32). If, rather, $2^d \mid N-2$, then the power of 2 dividing $N^3(N-1)^2(N-2)$ will be $2^3 \cdot 2^0 \cdot 2^d = 2^{d+3}$, while the power dividing $a_1a_2a_3$ will be at least $2^1 \cdot 2^d \cdot 2^{d+1} = 2^{2d+2} \geq 2^{d+4}$, which provides a single extra factor of 2, and so again gives (32). □

We now apply the above to a possible counterexample to Conjecture 4.

PROPOSITION 10. *Suppose that a positive integer N admits three decompositions, which we will write as (28) and (29), such that, for every prime p dividing $N(N-1)(N-2)$, at least one of these decompositions is p-acceptable. Then we cannot have* $2<i+j<11$.

https://doi.org/10.1017/S0004972710001723 Published online by Cambridge University Press

PROOF. Below, 'relevant' will mean relevant with respect to (29). We claim first that

$$\begin{aligned}&\text{if } p^d \text{ is a relevant prime power, then there is no carrying when}\\ &\quad N-i-j,\ i \text{ and } j \text{ are added in base } p,\\ &\quad \text{and the remainders on dividing } i \text{ and } j \text{ by } p^d \text{ sum to at most } 2.\end{aligned} \tag{36}$$

Indeed, the first assertion follows from our hypothesis, which implies that the decomposition (28) is p-acceptable for every relevant prime p. Combining this with the fact that a relevant prime power p^d is by definition a divisor of N, $N-1$ or $N-2$, hence that $N \equiv 0, 1 \text{ or } 2 \pmod{p^d}$, we get the second assertion.

Let us now, by way of contradiction,

$$\text{assume that } 2 < i+j < 11. \tag{37}$$

Then i and j, though positive, are not both 1; so for p as in (36), we see from the second assertion thereof that one of i or j must be greater than or equal to p^d. Thus,

$$\text{if } p^d \text{ is a relevant prime power, } i+j \geq p^d+1. \tag{38}$$

This and the upper bound of (37) limit the possible relevant prime powers to

$$2, 3, 4, 5, 7, 8, 9. \tag{39}$$

Now the hypotheses of the proposition cannot be satisfied for any $N \leq 14$. Indeed, for each such value, N or $N-1$ is a prime power p^d, hence N has digit-sum less than or equal to 2 to base p, so for such p there can be no p-acceptable decomposition of N (cf. (13), (14)). Hence we may assume that $N > 14$, and so use the bound

$$C > 486 \tag{40}$$

of Lemma 9.

Let us now consider a relevant prime power p_0^d dividing N itself. In that case, (36) implies that p_0^d must divide both i and j, so (37) limits us to $p_0^d = 2, 3, 4, 5$. Of these values, 4 is excluded, since the condition that there be no carrying when i and j are added in base $p=2$ shows that if i, j are divisible by 4, one of them is divisible by 8, making their sum at least 12; we are left with $p_0^d = 2, 3, 5$. If $p_0^d = 3$ or 5, then the first statement of (36), together with the divisibility of i and j by p_0^d, and (37), force $i = j = p_0$. But this has the consequence that there can be no relevant prime (whether dividing N, $N-1$ or $N-2$) *other* than p_0: indeed, for these choices of i and j, each of the other prime powers in the list (39) is eliminated by at least one of the conditions of (36). This gives $C = p_0^3 \leq 125$, contradicting (40). Likewise, if $p_0^d = 2$, then the combination of the first condition of (36) and our bound on $i+j$ excludes all possibilities but $\{i, j\} = \{2, 4\}$ and $\{2, 8\}$. Neither of these choices is consistent with (36) holding for any of our odd prime powers. So in this case $C \leq 8 \cdot 2^3 = 64$, again contradicting (40). These contradictions show that no relevant primes divide N.

https://doi.org/10.1017/S0004972710001723 Published online by Cambridge University Press

Knowing this, let us again look through the possible relevant primes. If 7 is relevant, then by (36) and (37), the unordered pair $\{i, j\}$ must be one of $\{7, 1\}$, $\{7, 2\}$ or $\{8, 1\}$. Applying (36) to the other prime powers in (39), we see that for $\{i, j\} = \{7, 1\}$, the only other relevant prime power could be a 3, in which case the final digit of N to base 3 would be 2, so that 3 would divide $N - 2$, making $C \leq 3 \cdot 7^2 = 147$. For $\{i, j\} = \{7, 2\}$, there are no other possible relevant prime powers; and for $\{i, j\} = \{8, 1\}$, we could at most have an 8 dividing $N - 1$, which, since 7 would divide $N - 2$, gives $C \leq 7 \cdot 8^2 = 448$; in each case contradicting (40). If 5 is relevant, the possibilities for $\{i, j\}$ are $\{5, 1\}$, $\{5, 2\}$, $\{6, 1\}$ and $\{5, 5\}$. Looking at the cases where i and/or j is 5, we see that the only other possible relevant prime power consistent with (36) is 2, which could divide $N - 1$ in the one case $\{5, 2\}$, giving $C \leq 2^2 \cdot 5^2 = 100$; while in the case $\{6, 1\}$, we get 2 and 3 as possible relevant prime power factors of $N - 1$, which, together with 5 dividing $N - 2$, would give $C \leq 5 \cdot 2^2 \cdot 3^2 = 180$; again each case contradicts (40). So at most 2 and 3 can be relevant primes. If 9 were a relevant prime power, then by (37) we could only have $\{i, j\} = \{9, 1\}$, so 2 would not be relevant, and C would be at most $9^2 = 81$. Likewise, if 8 were a relevant prime power, then we could only have $\{i, j\} = \{8, 1\}$, or $\{8, 2\}$, so 3 would not be relevant, and C would be at most $8^2 = 64$. So the relevant prime powers are at most 3 and 4, each occurring in the expression for C to at most the second power, giving $C \leq 144$, and yielding the same contradiction. □

We remark that the argument just given cannot be extended to exclude $i + j = 11$. Indeed, for N of the form $180M + 11$, consider the decomposition

$$N = 180M + 10 + 1. \tag{41}$$

I claim that for infinitely many values of M, the above decomposition of N is 2-, 3- and 5-acceptable, with $2 \cdot 5 \mid N - 1$ and $3^2 \mid N - 2$. Indeed, we see that the conditions for 2-, 3- and 5-acceptability of (41) are that the base-2 expansion of $180M$ have 2^3-digit 0, that its base-3 expansion have 3^2 digit 0 or 1, and that its base-5 expansion have 5^1 digit 0, 1 or 2; so these are satisfied $(1/2)(2/3)(3/5) = 1/5$ of the time. (The first few values satisfying these conditions are $M = 5, 12, 17$.) Thus, if we combine (41) with two other decompositions (29) of N, the latter need not be 2-, 3- or 5-acceptable, so we can get $C = 2^2 \cdot 3^2 \cdot 5^2 = 900$, which no longer contradicts (31). (Here 2 *is* a relevant prime, so we cannot use the stronger conclusion (32).) I suspect that as we take still larger values of $i + j$, we can get arbitrarily large C.

However, the bound of Proposition 10 is enough to eliminate a large range of values of N, as we shall now show.

8. There are no counterexamples with $k = 3$, $N < 785$

Propositions 7 and 10 together show us that in looking for counterexamples to Conjecture 4 with $k = 3$ and $N < 1726$, it suffices to check values of N which exceed by at least 11 the largest prime power less than or equal to N. In particular, N must lie in a gap of length at least 12 between successive prime powers. A search through a list of primes shows 17 gaps of length greater than or equal to 12 with the lower prime less than 1000, their lengths ranging from 12 to 20. Several of these are thrown out of the picture when we bring higher prime powers into consideration. (The length-14 gap between 113 and 127 is interrupted by 121 and 125, the one between 953 and 967 by $31^2 = 961$, and the length-12 gaps between 509 and 521, and between 619 and 631, by $2^9 = 512$ and $5^4 = 625$, respectively.) A couple of other gaps are shortened from greater lengths down to length 12 in this way (the one between 523 and 541 by $23^2 = 529$, and the one between 839 and 853 by $29^2 = 841$). The surviving gaps, with those of length greater than 12 shown in bold face, are

$$\begin{aligned}(199, 211), (211, 223), (\mathbf{293}, \mathbf{307}), (\mathbf{317}, \mathbf{331}), (467, 479),\\ (529, 541), (661, 673), (\mathbf{773}, \mathbf{787}), (797, 809),\\ (841, 853), (\mathbf{863}, \mathbf{877}), (\mathbf{887}, \mathbf{907}), (997, 1009).\end{aligned} \tag{42}$$

Since most of these gaps have length 12, a large fraction of the values of N that this list informs us are not covered by Proposition 10 are of the form $N = p_{\max}^d + 11$. Many such cases, including all in the above list, can be eliminated using the following result.

LEMMA 11. *Suppose that (28) and (29) are decompositions of N such that, for every prime p dividing $N(N-1)(N-2)$, at least one of these decompositions is p-acceptable. Suppose, moreover, that in (28), i and j are relatively prime to one another, and $N - i - j$ is relatively prime to $i + j - 1$. Then no divisor of N or $N - 1$ is a relevant prime; hence $C \mid N - 2$.*

PROOF. Any relevant prime p dividing N would have to divide all of $N - i - j$, i and j, which is excluded by the relative primality of the last two of these, while a relevant prime p dividing $N - 1$ must divide two of $N - i - j$, i and j, with the remaining one being $\equiv 1 \pmod p$. Each choice of which two terms are $\equiv 0$ modulo p and which is $\equiv 1$ is excluded by one or the other of our relative primality hypotheses. □

Now if $N = p_{\max}^d + 11 < 1009$ is a counterexample to Conjecture 4, with $p_{\max}$-admissible decomposition (28), then Propositions 7 and 10 exclude all possible values for $i + j$ other than 11. Since $i + j = 11$ is prime, i and j must be relatively prime; if, moreover, $p_{\max}^d$ is not a power of 2 or 5 (as indeed none of the first members of the pairs in (42) are), it must be relatively prime to $i + j - 1 = 10$. So Lemma 11 tells us that in these cases, $C | N - 2$, so $C \leq 1009 - 2$. Lemma 11 also shows that $2 \mid N(N-1)$ is not a relevant prime, so (32) says that $C > 1728 \cdot (1 - 4 \cdot 200^{-1}) > 1693$ (since the values of N arising from (42) are all greater than 200), contradicting the preceding inequality, and eliminating these cases.

The values of $N < 1009$ not eliminated by this argument are those that exceed by at least 12 the greatest prime power less than or equal to them. From (42), these are

$$305, 306; 329, 330; 785, 786; 875, 876; \text{ and } 899, \ldots, 906 \text{ (8 terms).} \tag{43}$$

https://doi.org/10.1017/S0004972710001723 Published online by Cambridge University Press

Feeling that case-by-case elimination of possible N is not a way I want to continue to pursue this problem, I have only checked the first four of these. By looking at the primes dividing N, $N-1$ and $N-2$ in these cases, it is not hard to find properties that exclude each of these values of N. This is done in the proposition below. Let us start with a definition and two lemmas that formalize a kind of observation that we will use. (Note that the 'digit-sum greater than or equal to k' condition in the next definition is simply the necessary and sufficient condition for there to be *any* p-acceptable decompositions of N.)

DEFINITION 12. If k and N are positive integers, and p a prime such that the base-p expression for N has digit-sum greater than or equal to k, then by the *p-threshold* for N (with respect to k) we shall mean the greatest integer m occurring in any p-acceptable expression for N as a sum of k positive integers.

From the characterization of p-acceptable decompositions at the end of Definition 6, we immediately get the first of the two criteria below.

LEMMA 13. *For $k=3$, and N and p as in Definition 12, the p-threshold for N is $N-p^{e_1}-p^{e_2}$, where p^{e_1} is the largest power of p dividing N, and p^{e_2} is the largest power of p dividing $N-p^{e_1}$. (For general k, one has the corresponding description with $k-1$ successive subtractions.)*

LEMMA 14. *Let N be a positive integer, and $p^d_{\max}$ the largest prime power less than or equal to N. Suppose that for some prime $p_0 \neq p_{\max}$ and not dividing N, the base-p_0 expression for N has digit-sum less than or equal to 5, and that for all primes p dividing N, and also for $p=p_0$, the p-threshold for N with respect to $k=3$ is less than $p^d_{\max}$. Then N is not a counterexample to Conjecture 4 for $k=3$.*

PROOF. Suppose that N were a counterexample, with decompositions (28), (29), where the first is $p_{\max}$-acceptable. By our hypothesis on p-thresholds, neither p_0 nor any of the primes dividing N can be relevant primes; so for each of these, one of the decompositions of (29) must be p-acceptable. Let $a_0+a_1+a_2$ be the p_0-acceptable decomposition.

Since in base p_0, N has digit-sum less than 6, at least one of a_0, a_1, a_2 must have digit-sum less than 2, that is, must be a power of p_0. This term will be relatively prime to all the primes dividing N, so for each of those primes p, the p-acceptable decomposition must be $b_0+b_1+b_2$. This makes each of b_1, b_2, b_3 a multiple of N, contradicting the assumption that they sum to N. □

We can now verify the result we have been aiming for.

PROPOSITION 15. *There are no counterexamples to Conjecture 4 for $k=3$ with $N<785$.*

PROOF. Examining (43), we see that we must check $N=305$, 306, 329 and 330. From (42) we see that for the first two of these, $p^d_{\max}=293$, while for the last two it is 317.

https://doi.org/10.1017/S0004972710001723 Published online by Cambridge University Press

The case 306 is excluded by (13), since its base-17 expansion is 110_{17}, while 305 is excluded by Lemma 14 with $p_0 = 2$.

The case 329, which has base-2 expression 101001001_2, would likewise be excluded by that lemma with $p_0 = 2$, except that its 2-threshold is 320, which is not less than 317. However, in the proof of that lemma, the condition that the p_0-threshold of N be less than $p_{\max}^d$ is used only to rule out the possibility that p_0 is a relevant prime. Now if 2 were a relevant prime, then since $i + j \leq N - p_{\max} = 329 - 317 = 12$, we see from the above base-2 expression that $i + j$ would have to be $8 + 1 = 9$, which is greater than 2 and less than 11, contradicting Proposition 10.

To handle 330, note that again $p_{\max} = 317$, and that now $330 = 101001010_2$. Here we will use an argument similar to that of Lemma 14, but with the roles of N and $N - 1$ reversed. Essentially the same reasoning as in the preceding case shows that 2 cannot be a relevant prime. Moreover, since the base-2 expression for N has digit-sum 4, any 2-acceptable decomposition of N must have two terms that are powers of 2; hence such a decomposition cannot be p-acceptable for any $p \mid N - 1$. Looking at the prime factorization of $N - 1 = 329 = 47 \cdot 7$, we see that 47 has threshold less than 317, while if 7 were relevant we would have $i + j = 7 + 1$, which is again greater than 2 and less than 11. So any three decompositions of 330 comprising a counterexample to Conjecture 4 must consist of a $p_{\max}$-acceptable decomposition, a 2-acceptable decomposition, and a decomposition acceptable for both factors of $N - 1$. This forces at least one summand in the last of these decompositions to be divisible by the product of those factors, $N - 1$, making it too large. □

9. Quick counterexamples to some plausible strengthenings of Conjecture 4

It is natural to ask whether Conjecture 4 is the 'right' statement, or whether some stronger statement might hold. For instance, for $k > 2$, might the number of proper k-nomial coefficients that are guaranteed to have a common divisor grow faster than k?

An example showing that *four* proper *trinomial* coefficients of the same weight need not have a common divisor is given by the following four decompositions of 159:

$$157 + 1 + 1, \quad 144 + 12 + 3, \quad 53 + 53 + 53, \quad 79 + 79 + 1. \tag{44}$$

(The only primes not handled by the first decomposition are the divisors of $159 = 53 \cdot 3$ and $158 = 79 \cdot 2$. Of these, 2 and 3 are handled by the second decomposition, and the remaining two primes by the last two.)

Might the importance of the condition that our multinomial coefficients be proper and of nomiality k simply be to ensure that all their arguments are less than or equal to $N - k + 1$? If so, we would expect binomial coefficients with all arguments strictly greater than 1 to behave as well as is conjectured for trinomial coefficients. A counterexample is given by the following three decompositions of 46:

$$44 + 2, \quad 36 + 10, \quad 23 + 23. \tag{45}$$

https://doi.org/10.1017/S0004972710001723 Published online by Cambridge University Press

Finally, might it be possible to replace the assumption of k multinomial coefficients, of equal weight and common nomiality k, with that of a finite family of multinomial coefficients of equal weight but possibly varying nomialities, such that the sum of the reciprocals of those nomialities is less than or equal to 1? Here a counterexample is given by the following three decompositions of 65:

$$64+1, \quad 25+25+5+5+5, \quad 13+13+13+13+13, \tag{46}$$

where the reciprocals of the nomialities sum to $1/2+1/5+1/5=9/10<1$. (If one wants the sum to be exactly 1, one can replace any two terms of the second decomposition by their sum, and similarly in the third decomposition.)

In [1, Section 4], it is shown that, assuming the truth of Schinzel's conjecture on prime values assumed by polynomials with integer coefficients [7], all these counterexamples belong to infinite families.

10. Where do we go from here?

A proof of Conjecture 4, even for $k=3$, may well require an approach entirely different from that of Sections 5–8 above. On the other hand, if it is false, and we want to find a counterexample, or if, on the contrary, the approach of this paper can somehow be extended to a proof, our results indicate a bifurcation of the problem into two cases, the one where the decomposition with largest summand has the other two summands i and j both 1, and the case where i and j sum to at least 11. (Thought: might one get additional mileage by subdividing the latter case according to whether *one* of i and j equals 1?)

In the case $i+j>2$, we have made use of primes dividing $N(N-1)(N-2)$; but I suspect that these are not enough—that we must in some way also use the facts that for every prime p dividing $(N-3)\cdots(N-i-j+1)$, one of our decompositions is p-acceptable. A suggestion as to how this might be attempted is sketched in [1, Section 5].

I have not tried a computer search for counterexamples. Someone skilled at such searches might use the results proved in this paper to limit the cases (both the values of N and the triads of decompositions thereof) to be checked. (The reference in [4, p. 131] to 'fairly extensive computer evidence' was a misunderstanding; all the computations Wasserman and I did were by hand. See [1, Section 3] for an example.)

Some additional restrictions limiting the decompositions of N that would have to be checked in such searches are noted in [1, Section 6]. The idea is that in the proof of Proposition 7 above, if instead of the estimate $a_1a_2a_3 \le N^3/3^3$, we use $a_1a_2a_3 \le a_1N^2/2^2$, we get, instead of a lower bound on N, a lower bound on a_1 independent of N, while if we do the same in the proof of Lemma 9 we get, instead of a bound on C independent of N, a bound on a_1C that grows linearly in N. The bounds in question say that when $i=j=1$, all a_i and b_i are greater than or equal to 216, while when $i+j>1$, all a_iC and b_iC are greater than or equal to $108(N-4)$; in each case with strengthenings under additional assumptions.

https://doi.org/10.1017/S0004972710001723 Published online by Cambridge University Press

Turning to general k, we remark that the equality of the degrees of the two sides of (34) is special to $k = 3$. For large k, the degree of the left-hand side of the analogous inequality grows as $k^2/2$, while that of the right-hand side grows as k^2; so the methods we have been using for $k = 3$ are not likely to extend to larger k. Conjecture 4 might in fact be too strong; perhaps the largest k' such that every family of k' proper k-nomial coefficients has a common divisor satisfies $k' \approx k/\sqrt{2}$ when k is large, rather than $k' = k$.

The hope for a proof of Conjecture 4 (or some variant) in the spirit of the group-theoretic proof of Theorem 1 is appealing. Sticking with $k = 3$ for simplicity, let us ask the following question.

QUESTION 16. Suppose that G is a group, and X, Y, Z are finite transitive G-sets, such that

$$\gcd(\mathrm{card}(X), \mathrm{card}(Y), \mathrm{card}(Z)) = 1,$$

but such that none of the G-sets $X \times Y$, $Y \times Z$, $Z \times X$ is transitive (so that no two of $\mathrm{card}(X)$, $\mathrm{card}(Y)$, $\mathrm{card}(Z)$ are relatively prime). What, if anything, can one conclude about the orbit structure of the G-set $X \times Y \times Z$?

On the other hand, other interpretations of multinomial coefficients might be useful in attacking Conjecture 4. One result of that sort, conjectured by F. Dyson, and proved by several others ([3] and papers cited there) describes $\mathrm{ch}(a_1, \ldots, a_k)$ as the constant term of the Laurent polynomial $\prod_{i \neq j} (1 - x_j/x_i)^{a_i}$ in indeterminates $x_1, \ldots, x_n$.

References

[1] G. M. Bergman, ‘Addenda to “On common divisors of multinomial coefficients” ’, unpublished note, March 2010, 9 pp., readable at http://math.berkeley.edu/∼gbergman/papers/unpub/.

[2] P. Erdős and G. Szekeres, ‘Some number theoretic problems on binomial coefficients’, *Aust. Math. Soc. Gaz.* **5** (1978), 97–99, readable at www.math-inst.hu/∼p_erdos/1978-46.pdf.

[3] I. J. Good, ‘Short proof of a conjecture by Dyson’, *J. Math. Phys.* **11** (1970), 1884 (In the second display in this telegraphic note, the final equation $i = j$ is, as far as I can see, meaningless, and should be ignored.)

[4] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd edn (Springer, New York, 2004).

[5] A. Granville, ‘Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers’, in: *Organic Mathematics (Burnaby, BC, 1995)*, CMS Conference Proceedings, 20 (American Mathematical Society, Providence, RI, 1997), pp. 253–276.

[6] E. E. Kummer, ‘Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen’, *J. reine angew. Math.* **44** (1852), 93–146, readable at www.digizeitschriften.de/no_cache/en/home/, and in the author’s *Collected Papers,* Springer, Berlin–New York, 1975.

[7] A. Schinzel and W. Sierpiński, ‘Sur certaines hypothèses concernant les nombres premiers’, *Acta Arith.* **4** (1958), 185–208; erratum at **5** (1958), 259.

GEORGE M. BERGMAN, Department of Mathematics, University of California,
Berkeley, CA 94720-3840, USA
e-mail: gbergman@math.berkeley.edu

https://doi.org/10.1017/S0004972710001723 Published online by Cambridge University Press