

# ON THE ORDER OF LACUNARY SUMS OF BINOMIAL COEFFICIENTS

Tamás Lengyel<sup>1</sup>

*Department of Mathematics, Occidental College, 1600 Campus Road, Los Angeles, USA*  
lengyel@oxy.edu

*Received: 11/19/02, Accepted: 2/26/03, Published: 2/27/03*

## Abstract

In this paper we study the exact orders of lacunary sums of binomial coefficients. It is remarkable that the periodic patterns evolving from powers of 2 differ markedly from those of other prime powers. For the latter ones the pattern is transparent and is determined by the first term. For the former ones multisected generating functions are used to obtain the exact order or lower bounds on it.

## 1. Introduction

We set the lacunary sum of binomial coefficients

$$G_{n,l}(k) = \sum_{t=0}^{\lfloor k/n \rfloor} \binom{k}{l+nt} \quad (1)$$

and the associated generating function

$$g_{n,l}(x) = \sum_{k=0}^{\infty} G_{n,l}(k)x^k = \frac{x^l(1-x)^{n-l-1}}{(1-x)^n - x^n}$$

for any integer  $n \geq 1$  and  $l = 0, 1, \dots, n-1$ . These multisected sums arise in combinatorics, applied probability, the analysis of algorithms, and number theoretical settings (e.g., in [1], [2], [4], [11], [12]). Ramus [10] determined  $G_{n,l}(k)$  as an  $n$ -term trigonometric sum in 1834. Clearly, for  $n = 2$  we have  $G_{2,0}(k) = G_{2,1}(k) = 2^{k-1}$ ,  $k \geq 1$ ,  $g_{2,0}(x) = \frac{1-x}{1-2x}$ , and  $g_{2,1}(x) = \frac{x}{1-2x}$ . From now on we assume that  $n > 2$ .

The analysis of  $g_{n,l}(x)$  for a prime  $n$  is similar to that of [4] in which alternating binomial coefficient sums are studied and sharp lower bounds are found on the orders. In that

---

<sup>1</sup>The author wishes to express his gratitude to the Computer and Automation Institute of the Hungarian Academy of Sciences for its hospitality during this work.

analysis changing the value of  $l$  requires only slight modifications (cf. Theorem 3 [4]). Our case is more complicated in this respect. Other closely related binomial coefficient sums are studied in [8], and closed forms for  $g_{n,l}(x)$  and its alternating version are derived by Howard and Witt [6] for  $n = 3, 4, 5, 8$ , and  $10$ . The case  $n = 12$  appears in [12] in the context of some congruences.

Section 2 is devoted to the analysis of divisibility by  $p$  of  $G_{n,l}(k)$  for any prime  $n = p$  and prime power  $n = p^q, p > 2$ . We deal with the case in which  $n$  is a power of two in Section 3. Some related conjectures are mentioned in Section 4.

**2. The case of the gap size  $n = p^q, p > 2$**

In this section we prove that for a prime power  $n = p^q$  with  $p > 2$ ,  $\rho_p(G_{n,l}(k))$  is the same as the order of the first term, i.e.,  $\rho_p\binom{k}{l}$ . Therefore, the mod  $p^q$  periodicity of the binomial coefficients guarantees either a periodic increment or periodicity of  $\rho_p(G_{n,l}(cp+k))$  in  $c$  depending on whether  $k < l$  or not. We start with the case of  $q = 1$ .

**Theorem 1.** For any odd prime  $p$  and  $0 \leq l \leq p - 1$ , we have  $\rho_p(G_{p,l}(k)) = \rho_p\binom{k}{l}$ .

*Proof of Theorem 1.* The relevant coefficients of the denominator contributing to the recursion  $(1 - x)^p - x^p$  of  $g_{p,l}(x)$  are divisible by  $p$  except those of  $x^0$  and  $x^p$ . Also notice that  $G_{p,l}(k) = 0$  for  $k = 0, 1, \dots, l - 1$ , and  $\rho_p(G_{p,l}(k)) = 0$  for  $k = l, l + 1, \dots, p - 1$ . These facts imply the cases resulting in a  $p$ -adic order of 0 (cf. [8] and [9]).

For  $m \geq 1, 1 \leq l \leq p - 1, 0 \leq i \leq l - 1, 1 \leq c \leq p - 1, 0 \leq t \leq cp^{m-1} - 1$ , we observe that  $\rho_p\binom{cp^m+i}{l+pt} = m$  by carry counting due to Kummer (cf. [7]). We will rely on the fact that this holds for every  $t$  which enters the summation in (1).

Now we use a theorem which was independently derived by Anton, Stickelberger, and Hensel (see identity (2) in [5]) to determine  $\frac{1}{p^q}\binom{N}{M} \pmod{p}$  with  $p^q$  being the exact power of  $p$  dividing  $\binom{N}{M}$ .

**Theorem A.** Let  $N = (N_d, \dots, N_1, N_0)_p = N_0 + N_1p + \dots + N_dp^d$ ,  $M = M_0 + M_1p + \dots + M_dp^d$  and  $R = N - M = R_0 + R_1p + \dots + R_dp^d$  with  $0 \leq N_i, M_i, R_i \leq p - 1$  for each  $i$ , be the base  $p$  representations of  $N, M$ , and  $R = N - M$ , respectively. Then

$$(-1)^q \frac{1}{p^q} \binom{N}{M} \equiv \left( \frac{N_0!}{M_0!R_0!} \right) \left( \frac{N_1!}{M_1!R_1!} \right) \cdots \left( \frac{N_d!}{M_d!R_d!} \right) \pmod{p}. \tag{2}$$

We apply this with  $q = \rho_p\binom{cp^m+i}{l+pt} = m$  as noted above. To expand the right side of (1) by (2) for the case of the form  $k = cp^m + i$ , we group the various value ranges for  $t$  according to its  $p$ -ary digits  $t = (t_{m-1}, \dots, t_0)_p$ . With  $t_{m-1} : 0 \leq t_{m-1} \leq c - 1, t_j : 0 \leq$

$t_j \leq p - 1, j = 0, 1, \dots, m - 2$ , we rewrite

$$\sum_{\substack{0 \leq t_{m-1} \leq c-1 \\ 0 \leq t_j \leq p-1, j=0,1,\dots,m-2}} \left( \frac{c!}{t_{m-1}!(c-1-t_{m-1})!} \right) \left( \prod_{0 \leq j \leq m-2} \left( \frac{0!}{t_j!(p-1-t_j)!} \right) \right) \left( \frac{i!}{l!(p+i-l)!} \right) \equiv \frac{c!i!}{l!(p+i-l)!} \left( \sum_{0 \leq t_{m-1} \leq c-1} \frac{1}{t_{m-1}!(c-1-t_{m-1})!} \right) \times \left( \sum_{0 \leq t_0 \leq p-1} \frac{1}{t_0!(p-1-t_0)!} \right) \cdots \left( \sum_{0 \leq t_{m-2} \leq p-1} \frac{1}{t_{m-2}!(p-1-t_{m-2})!} \right) \pmod p. \tag{3}$$

Note that  $T_d = \sum_{i=0}^{d-1} \frac{1}{i!(d-1-i)!} = \frac{1}{(d-1)!} \sum_{i=0}^{d-1} \binom{d-1}{i} = \frac{2^{d-1}}{(d-1)!} \not\equiv 0 \pmod p$ , for  $d \leq p$ . We use this with  $d = c$  and  $p$ . (In the latter case we obtain  $T_p \equiv -1 \pmod n$  by Euler's and Wilson's Theorems.) This guarantees that the expression in (3) is not a multiple of  $p$ . In fact, we get that

$$G_{p,l}(cp^m + i) \equiv -c2^{c-1}i!a_{i,l}p^q \pmod{p^{q+1}}$$

with  $a_{i,l} \equiv (l!(p+i-l)!)^{p-2} \pmod p$  being the mod  $p$  multiplicative inverse of  $l!(p+i-l)!$ .

In general, if  $k \geq p, i \equiv k \pmod p, 0 \leq i \leq l-1$ , and  $\rho_p(k-i) = m$  then the proof can be easily modified by using  $T_d \not\equiv 0 \pmod p$  with  $d \equiv \frac{k-i}{p^m} \pmod p$  so that  $0 < d < p$ , and with  $d = p$ , to yield  $\rho_p(G_{p,l}(k)) = \rho_p\left(\binom{k}{l}\right) = m$ . Note, however, that if  $k-i > p^{m+1}$  then some terms  $\binom{k}{l+pt}$  will be divisible by  $p^{m+1}$ .

The case of  $k \geq p, i \equiv k \pmod p, l \leq i \leq p-1$ , is taken care of by the observation for cases resulting in a  $p$ -adic order of 0 made at the beginning of the proof.  $\square$

We can generalize Theorem 1 for prime powers.

**Theorem 2.** For any prime power  $n = p^q, 0 \leq l \leq n - 1$ , we have  $\rho_p(G_{n,l}(k)) = \rho_p\left(\binom{k}{l}\right)$ .

The proof is similar to that of the Theorem 1 and is based on the fact that the coefficients of  $(1-x)^n - x^n$  are divisible by  $p$  except those of  $x^0$  and  $x^n$ .

### 3. Gap size of $2^m$

This case is quite involved. In fact, first we prove a theorem for alternating sums. Later we discuss the divisibility behavior for the non-alternating sum  $G_{2^m,0}(k)$  by applying multisection techniques to its generating function. Recall that we are interested only in cases with  $m \geq 2$ .

We note that Gessel [3] studies generalized Dedekind sums, including  $\sum_{j=0}^{2^m-1} (1 + \omega^j)^k$  with  $\omega = \cos(2\pi/2^m) + i \sin(2\pi/2^m)$  being a primitive  $2^m$ th root of unity. Of course, the

above sum is  $2^m G_{2^m,0}(k)$  in disguise (cf. [2], [10], or [11]) but the analysis in [3] does not seem to help in determining the 2-adic order of  $G_{2^m,0}(k)$ . In [13] we proved

**Theorem B.** For  $k \geq 2$ , we have

$$\rho_2(G_{4,0}(k)) = \begin{cases} \lfloor k/2 \rfloor - 1, & \text{if } k \equiv 0, 1, 3 \pmod{4} \\ k - 2, & \text{if } k \equiv 2 \pmod{4} \end{cases} \quad (4)$$

and

$$\rho_2(G_{4,l}(2k + 1)) = k - 1, l = 0, 1, 2, 3, k \geq 1.$$

We generalize this theorem. The main results of this section are summarized in the following theorem.

**Theorem 3.** For  $k, c \geq 1$ , we have

$$\rho_2(G_{2^m,0}(k)) \geq \lceil \frac{k}{2^{m-1}} \rceil - 2, \quad (5)$$

$$\rho_2(G_{2^m,0}((2c - 1)2^{m-1})) = 4c - 4, \quad (6)$$

$$\rho_2(G_{2^m,0}(c2^m)) = 2c - 1, \quad (7)$$

and

$$\rho_2(G_{2^m,2^{m-1}}(c2^m)) = 2c - 1. \quad (8)$$

For  $l = 0, 1, \dots, 2^m - 1, c \geq 2$ , we have

$$\rho_2(G_{2^m,l}(c2^{m-1} - 1)) = c - 2. \quad (9)$$

**Corollary 4.** If inequality (5) holds with equality for some value  $k$  then

$$\rho_2(G_{2^m,0}(k + 2^{2(m-1)})) = \rho_2(G_{2^m,0}(k)) + 2^{m-1}. \quad (10)$$

Note that (5) is sharpened by (7), and (10) also holds for even multiples of  $2^{m-1}$  while (6) shows that for odd multiples the growth rate is doubled. The corollary and identity (6) reveal the differences in the periodic nature of  $\rho_2(G_{2^m,0}(k))$ . We note that  $\rho_2(G_{2^m,0}(k)) \geq \lfloor k/2^{m-1} \rfloor - 1$  also holds true in agreement with (4) but we prefer to use (5).

In order to prove Theorem 3, we set

$$S_{2^m}(k) = \sum_t \binom{k}{2^m t} (-1)^t,$$

for the lacunary alternating binomial coefficient sum with generating function

$$\sum_{k=0}^{\infty} S_{2^m}(k)x^k = \frac{(1-x)^{2^m-1}}{(1-x)^{2^m} + x^{2^m}}, \quad (11)$$

and prove

**Theorem 5.** For  $k, c \geq 1$ , we have

$$\rho_2(S_{2^m}(k)) \geq \frac{k}{2^m} - 1, \tag{12}$$

$$\rho_2(S_{2^m}(k)) = \frac{k}{2^m} \text{ if } 2^{m+1} | k, \quad \text{i.e.,} \quad \rho_2(S_{2^m}(c2^{m+1})) = 2c, \tag{13}$$

and

$$\rho_2(S_{2^m}((2c - 1)2^m)) = \infty.$$

*Proof of Theorem 5.* We note that

$$S_{2^m}((2c - 1)2^m) = 0, \tag{14}$$

for  $\binom{(2c-1)2^m}{2^m t}(-1)^t + \binom{(2c-1)2^m}{(2c-1)2^m - 2^m t}(-1)^{(2c-1)-t} = 0$ ,  $0 \leq t \leq c - 1$ , which yields the last part of the theorem.

We prove the other statements by induction on  $k$ . We will need the first  $2^{m+1}$  values of  $S_{2^m}(l)$  as starting values for the order  $2^{m+1}$  linear recurrence (15) below. The values are obvious for  $k : 1 \leq k \leq 2^m$ . For  $0 < i < 2^m$ ,  $S_{2^m}(2^{m+1} - i) = \binom{2^{m+1}-i}{0} - \binom{2^{m+1}-i}{2^m}$  is even confirming  $\rho_2(S_{2^m}(2^{m+1} - i)) \geq 1 - \frac{i}{2^m} = \frac{2^{m+1}-i}{2^m} - 1$ . By Theorem 1 in [5], which is an extension of identity (2), we have that for  $m \geq 1 : \rho_2(S_{2^m}(2^{m+1})) = 2$ . In fact,

$$\frac{1}{2} \binom{2^{m+1}}{2^m} \equiv 3 \pmod{2^3}$$

which yields  $S_{2^m}(2^{m+1}) \equiv 1 - 6 + 1 \pmod{8}$ .<sup>2</sup>

Now we prove the inductive statements. Identity (11) suggests a recurrence of order  $2^m$ . For  $k > 2^m$ ,

$$S_{2^m}(k + 2^m) = \left( \sum_{i=1}^{2^m-1} (-1)^{i+1} \binom{2^m}{i} S_{2^m}(k + 2^m - i) \right) - 2S_{2^m}(k).$$

This implies (12). In fact, for  $1 \leq i \leq 2^m - 1$  we have  $\rho_2(\binom{2^m}{i} S_{2^m}(k + 2^m - i)) \geq m - \rho_2(i) + \frac{k+2^m-i}{2^m} - 1 \geq \frac{k}{2^m} + \frac{1}{2}$ , with the unique minimum taken at  $i = 2^{m-1}$ , and  $\rho_2(2S_{2^m}(k)) \geq 1 + \frac{k}{2^m} - 1 = \frac{k}{2^m}$ .

To prove (13) we multiply both the numerator and denominator in (11) by  $(1 - x)^{2^m} + x^{2^m}$ . This results in the order  $2^{m+1}$  recurrence

$$S_{2^m}(k + 2^{m+1}) = \left( \sum_{i=1}^{2^{m+1}-1} c_i S_{2^m}(k + 2^{m+1} - i) \right) - 4S_{2^m}(k), \tag{15}$$

---

<sup>2</sup>Note that in general, for every  $N \geq 1$  there exists an  $m_0 = m_0(N)$  so that for all  $m \geq m_0 : \frac{1}{2} \binom{2^{m+1}}{2^m} \pmod{2^N}$  is the same.

for  $k > 2^{m+1}$ . It is fairly easy to see that  $\rho_2(c_i) \geq 3$  except for  $\rho_2(c_{2^{m-2}}) = 2$ . Provided that  $2^{m+1}|k$ , we get that  $\rho_2(c_i S_{2^m}(k + 2^{m+1} - i)) \geq 3 + \frac{k+2^{m+1}-i}{2^m} - 1 > 2 + \frac{k}{2^m}$  except for  $i = 2^{m-2}$  when the lower bound still exceeds  $2 + \frac{k}{2^m}$  and for the last term whose contribution is only  $\rho_2(4S_{2^m}(k)) = 2 + \frac{k}{2^m}$ .  $\square$

Now we turn back to the original problem and first prove

**Lemma 6.**

$$G_{2^m,0}(k) = \frac{2^k}{2^m} + \frac{1}{2^m} \sum_{q=1}^{m-1} 2^q S_{2^q}(k). \tag{16}$$

*Proof of Lemma 6.* We use the corresponding generating functions of  $G_{2^m}(k)$  and  $S_{2^q}(k), 0 < q \leq m$ . Note that  $S_{2^m}(0) = 1$ . For  $m \geq 1$ , we set  $A_m(x) = \frac{1}{2^{m-1}} \frac{1-x}{1-2x} + \sum_{q=1}^{m-1} \frac{(1-x)^{2^q-1}}{(1-x)^{2^q} + x^{2^q}} \frac{2^q}{2^m}$ , and observe that  $A_{m+1}(x) = \frac{1}{2} A_m(x) + \frac{1}{2} \frac{(1-x)^{2^m-1}}{(1-x)^{2^m} + x^{2^m}}$ . Now identity (16) follows by a simple inductive proof that  $A_m(x) = g_{2^m,0}(x)$  for  $m \geq 1$ .  $\square$

We are ready to proceed with the

*Proof of Theorem 3.* If  $k < 2^m$  then  $G_{2^m,0}(k) = 1$  holds in accordance with the assertions. Otherwise, we can rely on the summation in (16) to estimate or determine  $\rho_2(G_{2^m,0}(k))$ .

First we prove (5) without the ‘‘ceiling’’ function, i.e., in the form  $\rho_2(G_{2^m,0}(k)) \geq \frac{k}{2^{m-1}} - 2$ . For  $k \geq 2^m$ , we observe that the terms of (16) are divisible by various powers of 2. The exponent of the term with index  $q$  is at least  $q - m + \frac{k}{2^q} - 1$  whose unique minimum is  $\frac{k}{2^{m-1}} - 2$  taken at  $q = m - 1$ , proving (5).

For the proof of (6) with  $k = (2c - 1)2^{m-1}$ , we need only consider the term with index  $q = m - 2$  in (16). (In fact the last term, with index  $q = m - 1$ , is 0 by (14).) To see this we observe that for  $k > 2^{m+1}$  and  $q \leq m - 1$ :  $1 < \frac{k}{2^{m+1}} < \frac{k}{2^m} \leq \frac{k}{2^{q+1}}$ . This means that if  $2^{m-1}|k$  then for the 2-adic order of the terms with indices  $q$  and  $q + 1$  we have  $q - m + \frac{k}{2^q} > q + 1 - m + \frac{k}{2^{q+1}}$  by (13). In other words, the terms on the right side of identity (16) contribute smaller and smaller exponents of 2 as  $q$  increases. (For example, to get  $\rho_2(G_{16}(24)) = 4$  we need only  $\rho_2(\frac{2^{m-2}}{2^m} S_{2^{m-2}}(24)) = 2 - 4 + \frac{24}{4} = 4$  since  $m = 4$  and  $8|24$ .) We immediately obtain  $\rho_2(G_{2^m,0}((2c - 1)2^{m-1})) = m - 2 - m + \rho_2(S_{2^{m-2}}((2c - 1)2^{m-1})) = 4c - 4$ . A similar analysis yields (7), for only the last term matters in (16) if  $k = c2^m$ . This leads to the 2-adic order  $(m - 1) - m + k/2^{m-1} = 2c - 1$  by identity (13).

Now we turn to (9). Since by binomial identities  $G_{2^m,0}(c2^m - 1) = G_{2^m,2^{m-1}}(c2^m - 1)$ , and their sum is  $G_{2^m,0}(c2^m)$ , it follows from identity (7) that  $\rho_2(G_{2^m,l}(c2^m - 1)) = 2c - 2$ , if  $l = 0$  or  $2^m - 1$ . This works for all cases if  $m = 2$  (see [13]) but does not seem to work for other values of  $l$  if  $m > 2$  so we opt for a different approach below. On the other hand, identity (8) can be derived from (9) since  $G_{2^m,2^{m-1}-1}(c2^m - 1) = G_{2^m,2^{m-1}}(c2^m - 1)$ , and their sum is  $G_{2^m,2^{m-1}}(c2^m)$ .

It turns out that (9) requires  $2^{m-1}$ -section of  $g_{2^m,l}(x)$ . It can be derived by multiplying

(cf. [4], [8]) both the numerator and denominator of  $g_{2^m,l}(x)$  by  $\prod_{j=1}^{2^{m-1}-1} D(\omega^j x)$  with  $D(x) = (1-x)^{2^m} - x^{2^m} = \sum_{j=0}^{2^m-1} \binom{2^m}{j} (-1)^j x^j$  with  $\omega$  being a  $2^{m-1}$ th primitive root of unity. We expand the new denominator  $D^*(x)$  symbolically:

$$D^*(x) = \prod_{j=0}^{2^{m-1}-1} D(\omega^j x) = 1 - c_{2^m-1} x^{2^m-1} - \dots - c_{(2^{m-1})2^m-1} x^{(2^m-1)2^m-1} \tag{17}$$

which is a polynomial in  $x^{2^{m-1}}$  since  $D^*(\omega^j x) = D^*(x), 0 \leq j < 2^{m-1}$ . Any combination of  $2^{m-1}$  factors contributing  $x^{k2^{m-1}}$  to the expansion can be characterized by the number,  $i_j$ , of polynomial factors in which the term with  $x^j$  is selected. By binomial expansion and ignoring the factors of  $\omega$ , the contribution of any term with the characterization  $(i_0, i_1, \dots, i_{2^m-1})$  is a multiple of

$$\binom{2^m}{0}^{i_0} \binom{2^m}{1}^{i_1} \dots \binom{2^m}{2^m-1}^{i_{2^m-1}}. \tag{18}$$

We determine the exponent in the power of 2 which divides this quantity in terms of  $(i_0, i_1, \dots, i_{2^m-1})$ . Here we need a finer analysis than that of Lemmas 1 and 2 of [8] which is accomplished by the following two lemmas.

**Lemma 7.** We have  $\rho_2(c_{k2^{m-1}}) \geq k$ , for  $k : 1 \leq k \leq 2^m - 1$ . Equality holds if and only if  $k = 2^{m-1}$ .

**Lemma 8.** With  $y_c = G_{2^m,l}(c2^{m-1} - 1)$  we have  $\rho_2(y_c) = c - 2$ , for  $c = 2, \dots, 2^m$ .

We get the recurrence  $y_{c+1} = \sum_{k=1}^{2^m-1} c_{k2^{m-1}} y_{c+1-k}$  by (17). It follows that

$$\rho_2(c_{k2^{m-1}} y_{c+1-k}) \geq k + (c + 1 - k - 2) = c - 1$$

by Lemmas 7 and 8, with equality holding for the index  $k = 2^{m-1}$  only. This guarantees the statement of identity (9),  $\rho_2(y_{c+1}) = c - 1$ . Hence, the proof of Theorem 3 is now complete.  $\square$

*Proof of Lemma 7.* Indeed, in (18) for the terms contributing to  $x^{k2^{m-1}}$  we get that  $i_0 + i_1 + \dots + i_{2^m-1} = 2^{m-1}$  and  $0i_0 + 1i_1 + \dots + (2^m - 1)i_{2^m-1} = k2^{m-1}$  since each of the  $2^{m-1}$  factors has exactly one contributing term. With  $C = i_{2^m-1}$ , we have that  $k2^{m-1}$  is  $C2^{m-1}$  plus the other at most  $2^{m-1} - C$  terms  $ji_j, j \neq 2^m-1$ . Thus,  $(k - C)2^{m-1} \leq (2^{m-1} - C)(2^m - 1)$ . This yields that  $k \leq \frac{2^{m-1}-C}{2^{m-1}}(2^m - 1) + C \leq 2^m - 1 - C + \frac{C}{2^{m-1}}$  leading to  $k \leq 2^m - C$  since  $C \leq 2^{m-1}$  and equality holding if and only if  $C = k = 2^{m-1}$ . In order to determine  $\rho_2(c_{k2^{m-1}})$  we count the contribution of the corresponding factors in (18) to the exponent of 2 and get that  $\rho_2(c_{k2^{m-1}}) \geq 1 \cdot C + 2 \cdot (2^{m-1} - C) = 2^m - C \geq k$ . Equality holds in  $\rho_2(c_{k2^{m-1}}) = k$  if and only if  $k = C = 2^{m-1}$ . For example, for  $m = 3$ , we get  $\rho_2(c_{4k}) \geq k$  and equality holds if and only if  $k = 0$  or  $k = C = 4$ ; in fact, we have that the exponents are 0, 3, 3, 6, 4, 7, 8, 12, in the order of  $k = 0, 1, 2, 3, 4, 5, 6, 7$ .  $\square$

*Proof of Lemma 8.* We apply an argument similar to that used for proving Lemma 2 of [8]. Recall that by the  $2^{m-1}$ -section used in (17),  $g_{2^m,l}(x)$  can be written with numerator  $x^l(1-x)^{2^m-l-1} \frac{D^*(x)}{D(x)}$  and denominator  $D^*(x)$ . (In the above proof we have just discussed the divisibility properties of the coefficients of the latter.) Let us focus now on the numerator. To get the coefficient of  $x^{c2^{m-1}-1}$ , i.e.,  $y_c, c \geq 2$ , we take

$$[x^u]x^l(1-x)^{2^m-l-1} = \begin{cases} \binom{2^m-l-1}{u-l}(-1)^{u-l}, & \text{if } u : l \leq u < 2^m, \\ 0, & \text{if } u : 0 \leq u < l, \end{cases} \tag{19}$$

and

$$[x^{c2^{m-1}-1-u}]D^*(x)/D(x) \tag{20}$$

with  $0 \leq u < 2^m$  and the usual notation. We will see shortly that the only interesting cases are  $u = i2^{m-1} - 1, i = 1, 2$ . Note that the right hand side of (19) is  $\pm 1$  if  $i = 2$ .

We observe that  $\rho_2(\binom{2^m}{j}), 1 \leq j \leq 2^m - 1$ , is smallest for  $j = 2^{m-1}$ . So to keep the 2-adic order small in (18) we try to maximize  $i_0$  and then  $C = i_{2^{m-1}}$ . We now prove that  $C$  is either  $c - 1$  or  $c - 2$ . In fact, as we dropped  $D(x)$  from (17),  $\sum_{j=0}^{2^m-1} i_j = 2^{m-1} - 1$  and  $\sum_{j=0}^{2^m-1} j i_j = c2^{m-1} - 1 - u \geq C2^{m-1}$  yield  $(c - C)2^{m-1} \geq u + 1$ . To avoid adding extra factors of 2 in (18), we take  $i_0 = 2^{m-1} - 1 - C$  implying  $u = (c - C)2^{m-1} - 1$ . Note that  $1 \leq 1 + u \leq 2^m$ ; therefore,  $C + 1 \leq c \leq C + 2$ .

If  $C = c - 1$  then the contribution is  $2^{c-1}$  from (20), while if  $C = c - 2$  then the contribution is  $2^{c-2}$  since in this case  $u = 2^m - 1$  and there is no contribution from (19). This gives  $\rho_2(y_c) = c - 2$  for  $c \geq 2$ . □

**Remark.** We note that identity (16) can be generalized. Let  $q'$  be the smallest integer  $q$  so that  $2^q > l$ . We set  $S_{2^m,l}(k) = \sum_t \binom{k}{l+2^m t} (-1)^t, 0 \leq l < 2^m$ , and prove that

$$G_{2^m,l}(k) = \frac{1}{2^{m-q'}} G_{2^{q'},l}(k) + \frac{1}{2^m} \sum_{q=q'}^{m-1} 2^q S_{2^q,l}(k).$$

In fact, for  $m \geq q'$  we set  $A_{m,l}(x) = \frac{1}{2^{m-q'}} \frac{x^l(1-x)^{2^{q'}-l-1}}{(1-x)^{2^{q'}} - x^{2^{q'}}} + \sum_{q=q'}^{m-1} \frac{x^l(1-x)^{2^q-l-1}}{(1-x)^{2^q} + x^{2^q}} \frac{2^q}{2^m}$  and observe that  $A_{m+1,l}(x) = \frac{1}{2} A_{m,l}(x) + \frac{1}{2} \frac{x^l(1-x)^{2^m-l-1}}{(1-x)^{2^m} + x^{2^m}}$  and  $A_{m,l}(x) = g_{2^m,l}(x)$  by induction on  $m$ . The previous proof with  $l = 0$  suggests that it might be possible to utilize the above identity and information on  $\rho_2(S_{2^m,l}(k))$  to obtain lower bounds on  $\rho_2(G_{2^m,l}(k))$  or even its value. Numerical evidence, however, suggests that this job might be more complicated.

Identity (7) is generalized by

**Theorem 9.** For  $c \geq 1$  and  $0 \leq l \leq 2^{m-1} - 1$ , we have  $\rho_2(G_{2^m,l}(c2^m + l)) = \rho_2(G_{2^m,0}(c2^m)) = 2c - 1$ .

The proof parallels that of identity (9) and is based on the  $2^m$ -section of  $g_{2^m,l}(x)$  and lemmas similar to Lemmas 7 and 8. The details are left to the reader. If  $l \equiv$



$2^{m-1} \pmod{2^m}$  then numerical evidence suggests that the pattern apparently changes to  $\rho_2(G_{2^m, 2^{m-1}}((2c-1)2^{m-1})) = 4c - 4$ . Similarly,  $\rho_2(G_{2^m, 0}(k)) = \rho_2(G_{2^m, 2^{m-1}}(k))$  seems to be true, in agreement with (7) and (8), if  $k$  is sufficiently large.

Finally we present the

*Proof of Corollary 4.* The proof is based on the combination of (5) and Lemma 7. We have  $G_{2^m, 0}(k + 2^{2(m-1)}) = c_{2^{m-1}}G_{2^m, 0}(k + 2^{2(m-1)} - 2^{m-1}) + c_{2^m}G_{2^m, 0}(k + 2^{2(m-1)} - 2^m) + \dots + c_{2^{2(m-1)}}G_{2^m, 0}(k) + \dots + c_{(2^m-1)2^{m-1}}G_{2^m, 0}(k + 2^{2(m-1)} - (2^m - 1)2^{m-1})$  by (17). Taking the 2-adic orders we get that  $\rho_2(G_{2^m, 0}(k + 2^{2(m-1)}))$  is at least as large as  $j + 1 + \lceil \frac{k + 2^{2(m-1)} - j2^{m-1}}{2^{m-1}} \rceil - 2$ ,  $1 \leq j \leq 2^m - 1$ , except for  $j = 2^{m-1}$  where the unique minimum is taken by Lemma 7, (5) and the assumption on  $k$ . In fact, the minimum is  $2^{m-1} + \rho_2(G_{2^m, 0}(k)) = 2^{m-1} + \lceil \frac{k}{2^{m-1}} \rceil - 2$  guaranteeing that equality in (5) will also hold for  $k + 2^{2(m-1)}$ .  $\square$

#### 4. Related questions

We propose three conjectures. Numerical evidence suggests

**Conjecture 1.** Assertion (5) holds with equality with  $2^{m-2}$  exceptions at and immediately following odd multiples of  $2^{m-1}$ . (Even multiples of  $2^{m-1}$  are taken care of by (7).)

This means that (5) gives the exact order in about 75% of the cases. It seems interesting to investigate the periodic increment of  $\rho_2(G_{2^m, 0}(k))$  similar to (10) but for all  $k \not\equiv 2^{m-1} \pmod{2^m}$ . We believe that this “limited scope” period is  $2^m$  rather than  $2^{2(m-1)}$ .

**Conjecture 2.**  $\rho_2(G_{2^m, 0}(k + c2^m)) = \rho_2(G_{2^m, 0}(k)) + 2c$ , for all sufficiently large  $k$  with  $k \not\equiv 2^{m-1} \pmod{2^m}$ .

For example, if  $m = 2$  then  $\rho_2(G_{4, 0}(k + 4c)) = \rho_2(G_{4, 0}(k)) + 2c$ , for  $k \geq 3$  and  $k \not\equiv 2 \pmod{4}$ . For  $l > 0$ ,  $\rho_2(G_{2^m, l}(k))$  seems to have a larger set of positions excluded from the period. Typically,  $k \equiv 0, 1, \dots, l - 1 \pmod{2^m}$  are all excluded. We also propose

**Conjecture 3.**  $\rho_2(G_{2^{m+s}, 0}(2^s k)) = \rho_2(G_{2^m, 0}(k))$  for  $s \geq 1$ .

This evidently holds if  $2^{m-1} | k$  by (6) and (7), or if  $k \leq 2^m$ . This latter observation proves that Conjecture 3 follows from Conjecture 2 by induction on  $k$ . In fact, repeated use of Conjecture 2 implies that if  $\rho_2(G_{2^{m+1}, 0}(2k)) = \rho_2(G_{2^m, 0}(k))$  then

$$\rho_2(G_{2^m, 0}(k + c2^m)) = \rho_2(G_{2^m, 0}(k)) + 2c = \rho_2(G_{2^{m+1}, 0}(2k)) + 2c = \rho_2(G_{2^{m+1}, 0}(2k + c2^{m+1})).$$

## Acknowledgments

I wish to thank Greg Tollisen for making many helpful suggestions and comments that improved the presentation of this paper.

## References

- [1] D. S. Clark, On some abstract properties of binomial coefficients, *Amer. Math. Monthly* **89**(1982), 433-443.
- [2] L. Comtet, *Advanced Combinatorics*, D. Reidel, Dordrecht, 1974
- [3] I. M. Gessel, Generating functions and generalized Dedekind Sums, The Wilf Festschrift, *Electronic Journal of Combinatorics* **4**(1997), #R11
- [4] I. M. Gessel and T. Lengyel, On the order of Stirling numbers and alternating binomial coefficient sums, *The Fibonacci Quarterly* **39**(2001), 444–454.
- [5] A. Granville, Binomial coefficients modulo prime powers, in preparation at <http://www.math.uga.edu:80/~andrew> in Binomial/index.html or Postscript/binomial.ps
- [6] F. T. Howard and R. Witt, Lacunary sums of binomial coefficients. *Applications of Fibonacci Numbers*, Vol 7: 185–195. Kluwer Academic Publishers, 1998.
- [7] D. E. Knuth and H. S. Wilf, The power of a prime that divides a generalized binomial coefficient. *J. Reine Angew. Math.* **396**(1989), 212–219.
- [8] T. Lengyel, Difference equations and divisibility properties of sequences, *Journal of Difference Equations and Applications* **8**(2002), 741–753.
- [9] N. S. Mendelsohn, Congruence relationships for integral recurrences, *Can. Math. Bull.* **5**(1962), 281–284.
- [10] Chr. Ramus, Solution générale d'un problème d'analyse combinatoire, *J. Reine Angew. Math.* **11**(1834), 353-355.
- [11] J. Riordan, *An Introduction to Combinatorial Analysis*, Wiley, New York, 1958
- [12] Z.-W. Sun, On the sum  $\sum_{k \equiv r \pmod m} \binom{n}{k}$  and related congruences, *Israel J. Math.* **128**(2002), 135–156.
- [13] G. P. Tollisen and T. Lengyel, Averaging around the circle, manuscript, 2002.