



DIVISIBILITY AND ARITHMETIC PROPERTIES OF A CLASS OF SPARSE POLYNOMIALS

Karl Dilcher

*Department of Mathematics and Statistics, Dalhousie University, Halifax,
Nova Scotia, Canada
dilcher@mathstat.dal.ca*

Maciej Ulas

*Jagiellonian University, Faculty of Mathematics and Computer Science, Institute
of Mathematics, Kraków, Poland
maciej.ulas@uj.edu.pl*

Received: 8/25/20, Revised: 9/19/21, Accepted: 12/29/21, Published: 1/7/22

Abstract

We investigate algebraic and arithmetic properties of a class of sequences of sparse polynomials that have binomial coefficients both as exponents and as coefficients. In addition to divisibility and irreducibility results we also consider rational roots. This leads to the study of an infinite class of integer sequences which have interesting properties and satisfy linear recurrence relations.

1. Introduction

The sequence of sparse polynomials defined by

$$f_n(z) := \sum_{j=0}^n \binom{n}{j} z^{j(j-1)/2} \quad (1)$$

arises naturally from a graph theoretic question related to the expected number of independent sets of a graph [2]. Various properties, including asymptotics, zero distribution, and arithmetic properties, can be found in [1], [2], [3], and [9]. More recently, in [4], we extended the polynomials in (1) by introducing the class of polynomials

$$f_{m,n}(z) := \sum_{j=0}^n \binom{n}{j} z^{\binom{j}{m}}, \quad (2)$$

where we typically fix the integer parameter $m \geq 1$ and consider the sequence $(f_{m,n}(z))_n$; obviously $f_{2,n}(z) = f_n(z)$. Since $f_{1,n}(z) = (1+z)^n$, we usually assume

that $m \geq 2$. It is also clear from (2) that $f_{m,n}(z) = 2^n$ when $n \leq m - 1$, and that for all $m \geq 1$ we have

$$f_{m,m}(z) = z + 2^m - 1, \quad f_{m,m+1}(z) = z^{m+1} + (m + 1)z + (2^{m+1} - m - 2), \quad (3)$$

and we have the special values

$$f_{m,n}(0) = \sum_{j=0}^{m-1} \binom{n}{j}, \quad f_{m,n}(1) = 2^n. \quad (4)$$

In [4] we investigated various analytic properties of the polynomials $f_{m,n}(z)$, especially monotonicity and log-concavity, connections between the polynomials and their derivatives, and the distribution of their real and complex zeros. Some of the properties were obtained for a more general class of polynomials.

It is the purpose of the present paper to study arithmetic and algebraic properties of the polynomials $f_{m,n}(z)$, especially divisibility and irreducibility, and number theoretic properties of special values of $f_{m,n}(z)$. We begin, in Section 2, by considering the sequence of special values $(f_{m,n}(-1))_n$; the results in that section will be useful also in later sections. In Section 3 we investigate divisibility properties of the polynomials, and Section 4 is devoted to the related concept of rational roots. In Section 5 we deal with further properties of the sequence $(f_{m,n}(-1))_n$ in the special case $m = 2^k$. Finally, in Section 6, we prove some irreducibility results.

2. Monotonicity Properties

We define the usual difference operator Δ on a sequence (a_n) by $\Delta a_n = a_{n+1} - a_n$, and the operator Δ^r of order $r \geq 0$ is defined recursively by $\Delta^{r+1} = \Delta \circ \Delta^r$, with $\Delta^0 a_n = a_n$. A sequence of real numbers is called *absolutely monotonic* if for all integers $r, n \geq 0$ we have $\Delta^r a_n \geq 0$. It is well-known that

$$\Delta^r a_n = \sum_{k=0}^r (-1)^k \binom{r}{k} a_{n+r-k}, \quad (5)$$

which is easy to see by induction. This also means that if $a_n = f(n)$, where f is a polynomial of degree d , then for $r > d$ we have $\Delta^r a_n = 0$ for all $n \geq 0$.

In [4] we obtained the following as a consequence of a more general result; see also Lemma 3 below.

Proposition 1. *For any integer $m \geq 1$ and real $z > 0$, the sequence $(f_{m,n}(z))_{n \geq 0}$ is absolutely monotonic.*

This gives rise to the question whether there are real numbers $z < 0$ and integers $m \geq 2$ such that $(f_{m,n}(z))_{n \geq 0}$ is also an absolutely monotonic sequence. Computations suggest that in general this is not the case. However, we have the following surprising result.

Proposition 2. *Let m be a positive integer.*

- (1) *If m is odd, then the sequence $(f_{m,n}(-1))_{n \geq 1}$ is absolutely monotonic.*
- (2) *If m is even, then $(f_{m,n}(-1))_{n \geq 1}$ is not absolutely monotonic.*

See Table 1 for an illustration of this result. In spite of the negative nature of part (2), much more can be said about the sequence $(f_{m,n}(-1))_{n \geq 1}$ for both even and odd m ; this will be done in Section 4.

For the proof of Proposition 2 and for other results in this paper we require some parity properties of binomial coefficients. We first quote a special case of a well-known congruence of Lucas.

Lemma 1. *Suppose that the integers $0 \leq m \leq k$ are given in binary expansion as $k = a_h \cdot 2^h + \dots + a_1 \cdot 2 + a_0$ and $m = b_h \cdot 2^h + \dots + b_1 \cdot 2 + b_0$. Then*

$$\binom{k}{m} \equiv \binom{a_h}{b_h} \cdots \binom{a_1}{b_1} \binom{a_0}{b_0} \pmod{2}. \tag{6}$$

n	$f_{2,n}(-1)$	$f_{3,n}(-1)$	$f_{4,n}(-1)$	$f_{5,n}(-1)$	$f_{6,n}(-1)$
1	2	2	2	2	2
2	2	4	4	4	4
3	0	6	8	8	8
4	-4	8	14	16	16
5	-8	12	20	30	32
6	-8	24	20	52	62
7	0	56	0	84	112
8	16	128	-68	128	184
9	32	272	-232	188	272
10	32	544	-560	280	364
11	0	1056	-1120	464	464
12	-64	2048	-1912	928	664

Table 1: $f_{m,n}(-1)$ for $2 \leq m \leq 6$ and $1 \leq n \leq 12$.

For the general case, valid for any prime base and modulus p in place of 2, see, e.g., [7] where a proof is also given. The next lemma is related to “the geometry of binomial coefficients”; see, e.g., [19] or [20] for some fractal-like images of Pascal’s triangle modulo 2, along with other related properties. We cannot claim that the following properties are new, but we provide proofs for the sake of completeness.

Lemma 2. *Let the positive integers m and ν be such that $2^{\nu-1} \leq m < 2^\nu$. Then*

- (1) the sequence $\left(\binom{m+k}{m} \pmod{2}\right)_{k \geq 0}$ is periodic with period 2^ν , but not with period 2^μ , $\mu < \nu$;
- (2) when m is odd, then $\binom{k}{m}$ and $\binom{k+1}{m}$ cannot both be odd, for any $k \geq 0$;
- (3) when m is even, there is always an integer k , $2^\nu \leq k < 2^{\nu+1}$, such that $\binom{k}{m}$ and $\binom{k+1}{m}$ are both odd.

Proof. (1) Suppose that m has the binary representation as in Lemma 1, with $b_h = 1$. Then $h = \nu - 1$, and the residue modulo 2 in (6) does not change if we add multiples of 2^ν to k since we may take $b_{h+1} = b_{h+2} = \dots = 0$.

To prove the second statement, we note that

$$\binom{m}{m} = 1, \quad \text{while} \quad \binom{m+2^{\nu-1}}{m} \equiv 0 \pmod{2},$$

so that we cannot have periodicity modulo $2^{\nu-1}$ or any smaller power of 2. This last congruence comes from the fact that $m = 2^{\nu-1} + b_{\nu-2}2^{\nu-2} + \dots$, which implies $m + 2^{\nu-1} = 2^\nu + b_{\nu-2}2^{\nu-2} + \dots$; hence the binomial coefficient in (6) corresponding to $2^{\nu-1}$ is $\binom{0}{1} = 0$.

(2) If m is odd, then $b_0 = 1$ in (6). Since one of $k, k + 1$ is even, the corresponding a_0 is 0, which means that the right-hand side of (6) is zero, that is, at least one of $\binom{k}{m}, \binom{k+1}{m}$ is even.

(3) We take $k = m + 2^\nu$. Then by part (1), $\binom{k}{m} = \binom{m}{m} = 1$ and $\binom{k+1}{m} = \binom{m+1}{m} = m + 1$, both of which are odd since m is even. □

The next lemma is also needed for the proof of Proposition 2, as well as for Proposition 4 later in this paper. It is actually a special case of Proposition 3.1 in [4], but for the sake of completeness we repeat the proof here. We also note that by (5), this lemma immediately implies Proposition 1.

Lemma 3. *For all integers $m \geq 2$ and $r, n \geq 0$ we have*

$$\sum_{\nu=0}^r (-1)^\nu \binom{r}{\nu} f_{m, n+r-\nu}(z) = \sum_{j=0}^n \binom{n}{j} z^{\binom{j+r}{m}}. \tag{7}$$

Proof. Using the definition (2), we rewrite the left-hand side of (7) as

$$\sum_{\nu=0}^r (-1)^\nu \binom{r}{\nu} \sum_{j=0}^{n+r-\nu} \binom{n+r-\nu}{j} z^{\binom{j}{m}} = \sum_{j=0}^{n+r} \left(\sum_{\nu=0}^r (-1)^\nu \binom{r}{\nu} \binom{n+r-\nu}{j} \right) z^{\binom{j}{m}}, \tag{8}$$

where we have extended the range of j by adding zero-terms. Now we observe that, by (5), the inner sum on the right of (8) is just $\Delta^r \binom{n}{j}$, and $\binom{n}{j}$ is a polynomial in n of degree j . Hence, by the remark following (5), this sum is 0 for $j < r$. When

$j \geq r$, this inner sum has the known evaluation $\binom{n}{j-r}$; see, e.g., [10, Eq. (3.49)]. So, altogether the left-hand side of (7), with (8), becomes

$$\sum_{j=r}^{n+r} \binom{n}{j-r} z^{\binom{j}{m}} = \sum_{j=0}^n \binom{n}{j} z^{\binom{r+j}{m}},$$

which was to be shown. □

Proof of Proposition 2. We have seen at the beginning of this section that a sequence (a_n) is absolutely monotonic if and only if the right-hand side of (5) is non-negative for all $r, n \geq 0$. In view of (7), we denote

$$S_m(n, r) := \sum_{k=0}^n \binom{n}{k} (-1)^{\binom{k+r}{m}}. \tag{9}$$

We need to show that for all $n \geq 1$ and $r \geq 0$, we have $S_m(n, r) \geq 0$ if and only if m is odd. For this purpose we show that these sums satisfy a “triangular” recurrence relation. Indeed, by manipulating the right-hand side of (9), we get

$$\begin{aligned} S_m(n, r) + S_m(n, r + 1) &= \sum_{k=0}^n \binom{n}{k} (-1)^{\binom{k+r}{m}} + \sum_{k=1}^{n+1} \binom{n}{k-1} (-1)^{\binom{k+r}{m}} \\ &= \sum_{k=0}^{n+1} \left(\binom{n}{k} + \binom{n}{k-1} \right) (-1)^{\binom{k+r}{m}} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} (-1)^{\binom{k+r}{m}}, \end{aligned}$$

where we have used the well-known Pascal triangle relation. Thus we have shown

$$S_m(n, r) + S_m(n, r + 1) = S_m(n + 1, r). \tag{10}$$

We first observed the relation (10) by fixing small integers $m \geq 2$ and constructing tables for sufficient ranges of n and r , using the computer algebra package Maple. The above proof was then routine.

It is clear that the sequence $(S_m(0, r))_{r \geq 0}$ has only -1 and 1 as terms. First, when m is odd, then by Lemma 2(2), no two terms -1 can occur as neighbours. By (10) this means that the sequence $(S_m(1, r))_{r \geq 0}$ consists only of the terms 0 and 2 . It now follows by induction, with (10) as induction step, that for any $n \geq 1$ we have $S_m(n, r) \geq 0$ for all $r \geq 0$. This proves part (1) of the Proposition.

If m is even, then by Lemma 2(3) there are two consecutive odd binomial coefficients $\binom{k}{m}, \binom{k+1}{m}$. However, by (6) not all $\binom{j}{m}$ can be odd; hence, keeping periodicity in mind, there must be a triple of consecutive binomial coefficients, the first of which is even, followed by two odd ones. This, in turn, means that there is

an integer $r \geq 1$ such that $S_m(0, r) = 1$ and $S_m(0, r + 1) = S_m(0, r + 2) = -1$. The recurrence (10) then implies that $S_m(1, r) = 0$ and $S_m(1, r + 1) = -2$, and applying (10) again, we have $S_m(2, r) = -2$. This shows that the sequence $(f_{m,n}(-1))_{n \geq 1}$ is not absolutely monotonic. \square

We conclude this section with an easy consequence of the identity (7). The second part of the following corollary will be used later, in Section 4.

Corollary 1. *Let $m \geq 2$ and $\nu \geq 2$ be integers such that $2^{\nu-1} \leq m < 2^\nu$. Then the sequence $(f_{m,n}(-1))_{n \geq 0}$ satisfies*

$$\Delta^{2^\nu} f_{m,n}(-1) = f_{m,n}(-1). \tag{11}$$

If $m = 2^k$ for some integer $k \geq 1$, then in addition to (11) we have

$$\Delta^{2^k} f_{2^k,n}(-1) = -f_{2^k,n}(-1). \tag{12}$$

Proof. We set $r = 2^\nu$ and $z = -1$ in (7). Then with (5) we have

$$\Delta^{2^\nu} f_{m,n}(-1) = \sum_{j=0}^n \binom{n}{j} (-1)^{\binom{2^\nu+j}{m}} = \sum_{j=0}^n \binom{n}{j} (-1)^{\binom{j}{m}} = f_{m,n}(-1),$$

where we have used the fact that, by Lemma 6(1), the binomial coefficient $\binom{j}{m}$ is periodic modulo 2 with period 2^ν .

For (12), we use again (7) with $z = -1$, and this time with $r = m = 2^k$, obtaining

$$\Delta^{2^k} f_{2^k,n}(-1) = \sum_{j=0}^n \binom{n}{j} (-1)^{\binom{2^k+j}{2^k}}. \tag{13}$$

Now, by Lucas's congruence (6) we have

$$\binom{j}{2^k} \equiv \begin{cases} 0 \pmod{2}, & 0 \leq j \leq 2^k - 1, \\ 1 \pmod{2}, & 2^k \leq j \leq 2^{k+1} - 1. \end{cases} \tag{14}$$

This, along with periodicity with period 2^{k+1} (see Lemma 2), means that

$$\binom{j + 2^k}{2^k} \equiv \binom{j}{2^k} + 1 \pmod{2},$$

which in turn shows that the right-hand side of (13) is $-f_{2^k,n}(-1)$. This completes the proof. \square

3. Divisibility Properties

In [3] it was shown that for any integer $k \geq 1$, the polynomial $f_{2,2k+1}(z)$ is divisible by $z^k + 1$. This gives rise to the question of whether there are similar divisibility results for polynomials $f_{m,n}(z)$ with other parameters m . Computations indicate that this is indeed the case when m is a power of 2, with certain additional restrictions. In fact, we have the following result.

Proposition 3. *Let $\mu \geq 1$ be a fixed integer, and suppose that the integer $k \geq 1$ is not divisible by any odd prime $p < 2^\mu$. Then*

$$z^k + 1 \text{ divides } f_{2^\mu, (k+1)2^{\mu-1}}(z).$$

For the proof of this result we require the following two lemmas.

Lemma 4. *For any integer $\mu \geq 1$, the exact power of 2 in $2^\mu!$ is $2^\mu - 1$.*

Proof. Among various possible proofs, it is probably easiest to use the well-known formula for the largest power of a prime in a factorial (see, e.g., [14, p. 182]), which in this case gives the exponent of 2 as

$$\sum_{i \geq 1} \left\lfloor \frac{2^\mu}{2^i} \right\rfloor = 2^{\mu-1} + 2^{\mu-2} + \dots + 2 + 1 = 2^\mu - 1,$$

as claimed. □

Lemma 5. *Let $\mu \geq 1$ be given. Then for any integer $j \geq 1$, the exact power of 2 that divides*

$$\prod_{r=j}^{j+2^\mu-1} r \sum_{s=j}^{j+2^\mu-1} \frac{1}{s} \text{ is } 2^\mu - \mu - 1, \tag{15}$$

independent of j .

Proof. It is clear that among any 2^μ consecutive integers, for instance those from j to $j + 2^\mu - 1$, we have that

$$\begin{aligned} 2^{\mu-1} \text{ of them are } &\equiv 1 \pmod{2}, \\ 2^{\mu-2} \text{ of them are } &\equiv 2 \pmod{2^2}, \\ &\vdots \\ \text{two of them are } &\equiv 2^{\mu-2} \pmod{2^{\mu-1}}, \\ \text{one of them is } &\equiv 2^{\mu-1} \pmod{2^\mu}, \text{ and} \\ \text{one of them is } &\text{divisible by } 2^\mu. \end{aligned}$$

Comparing consecutive congruences, we see that the integers satisfying them have to be distinct. Their total number is $2^{\mu-1} + 2^{\mu-2} + \dots + 1 + 1 = 2^\mu$, and thus they form a partition of all the 2^μ integers.

In (15), consider the term where s equals the one integer in the given range that is divisible by 2^μ ; then the exact power of 2 in the product of all integers r , $j \leq r \leq j + 2^\mu - 1$, without this s , is

$$2^{\mu-2} \cdot 1 + 2^{\mu-3} \cdot 2 + \dots + 2 \cdot (\mu - 2) + 1 \cdot (\mu - 1).$$

This sums to $2^\mu - \mu - 1$, which is easy to see, for instance by induction. All the other $2^\mu - 1$ products in the expression (15) are divisible by higher powers of 2. This proves the statement of the lemma. \square

Proof of Proposition 3. We use the basic idea of the proof of Proposition 2.1 in [3], which is actually our case $\mu = 1$. Using the definition (2), we have

$$\begin{aligned} f_{2^\mu, 2^\mu k + 2^\mu - 1}(z) &= \sum_{j=0}^{2^\mu k + 2^\mu - 1} \binom{2^\mu k + 2^\mu - 1}{j} z^{\binom{j}{2^\mu}} \\ &= \sum_{j=0}^{2^{\mu-1} k + 2^{\mu-1} - 1} \binom{2^\mu k + 2^\mu - 1}{j} \left(z^{\binom{j}{2^\mu}} + z^{\binom{2^\mu k + 2^\mu - 1 - j}{2^\mu}} \right) \\ &= \sum_{j=0}^{2^{\mu-1} k + 2^{\mu-1} - 1} \binom{2^\mu k + 2^\mu - 1}{j} z^{\binom{j}{2^\mu}} (1 + z^{b_\mu(k, j)}), \end{aligned} \tag{16}$$

where

$$b_\mu(k, j) := \binom{2^\mu k + 2^\mu - 1 - j}{2^\mu} - \binom{j}{2^\mu}. \tag{17}$$

We claim that if k is not divisible by an odd prime $p < 2^\mu$, then for all integers j with $0 \leq j \leq 2^{\mu-1} k + 2^{\mu-1} - 1$, the integer $b_\mu(k, j)$ is k times an odd integer. But this would mean that

$$1 + z^k \mid 1 + z^{b_\mu(k, j)}, \quad 0 \leq j \leq 2^{\mu-1} k + 2^{\mu-1} - 1;$$

this, with (16), would prove the proposition.

It remains to prove our claim. We rewrite (17) as

$$\begin{aligned} b_\mu(k, j) &= \frac{1}{2^{\mu!}} \left(\prod_{r=0}^{2^\mu-1} (2^\mu k - j + r) - \prod_{r=0}^{2^\mu-1} (j - r) \right) \\ &= \frac{1}{2^{\mu!}} \left(-2^\mu k \prod_{r=0}^{2^\mu-1} (j - r) \sum_{s=0}^{2^\mu-1} \frac{1}{j - s} + \dots \right), \end{aligned} \tag{18}$$

where the dots indicate multiples of $(2^\mu k)^\nu$, $\nu \geq 2$. The second line of (18) is obtained from the first line by setting $x := 2^\mu k$ and expanding the first product as a polynomial in x . Then the constant coefficient is cancelled, the coefficient of x is shown in the second line, and the rest is represented by the dots.

Now by Lemma 5, the exact power of 2 that divides the expression in parentheses on the right of (18), excluding the factor k , is $\mu + 2^\mu - \mu - 1$. Meanwhile, by Lemma 4, the exact power of 2 dividing the denominator $2^\mu!$ is also $2^\mu - 1$.

Finally we note that if k is not divisible by any odd prime $p < 2^\mu$, then there cannot be any cancellation with the denominator $2^\mu!$. This means that the integer $b_\mu(k, j)$ is divisible by k , and as we saw in the previous paragraph, the quotient is an odd integer. This completes the proof. \square

We can easily obtain the following consequence from Proposition 3.

Corollary 2. *Let $\mu \geq 1$ be a fixed integer, and suppose that the integer $k \geq 1$ is not divisible by any odd prime $p < 2^\mu$. Then*

$$f_{2^\mu, n}(z) \equiv 0 \pmod{z^k + 1}$$

for infinitely many integers n .

Proof. Since $z^k + 1$ divides $z^{k(2j+1)} + 1$ for any integer $j \geq 0$, by Proposition 3 we see that

$$f_{2^\mu, n}(z) \equiv 0 \pmod{z^k + 1} \quad \text{for } n = (k(2j + 1) + 1)2^\mu - 1.$$

There are clearly infinitely many $j \geq 0$ such that $2j + 1$ is not divisible by an odd prime $p < 2^\mu$; for instance, let j run through all the multiples of the product of all such primes. This proves the corollary. \square

Example 1. Corollary 2 shows that $z^k + 1$ divides $f_{4, n}(z)$ for infinitely many n when k is not a multiple of 3. Similarly, $z^k + 1$ divides $f_{8, n}(z)$ for infinitely many n when k is not divisible by 3, 5, or 7.

Example 2. On the other hand, for any $\mu \geq 1$ and any $j \geq 0$, we have

$$f_{2^\mu, n}(z) \equiv 0 \pmod{z^{2^j} + 1}$$

for infinitely many n . When $j = 0$, we can actually show more:

Corollary 3. *Given an integer $\mu \geq 1$, we have*

$$f_{2^\mu, n}(z) \equiv 0 \pmod{z + 1} \quad \text{for } n = k \cdot 2^{\mu+1} - 1, \quad k = 0, 1, 2, \dots \quad (19)$$

Proof. By the definition (2) we have

$$f_{2^\mu, n}(-1) = \sum_{j=0}^n \binom{n}{j} (-1)^{b(j)}, \quad b(j) := \binom{j}{2^\mu}. \tag{20}$$

Now, by (14) we have, modulo 2,

$$b(j) \equiv \begin{cases} 0, & \text{when } 0 \leq j \leq 2^\mu - 1, \\ 1, & \text{when } 2^\mu \leq j \leq 2^{\mu+1} - 1, \end{cases}$$

and by Lemma 2(1), this pattern continues with period $2^{\mu+1}$. In particular, since $n = k \cdot 2^{\mu+1} - 1$, this means that $b(j)$ and $b(n - j)$ have different parities, and thus

$$(-1)^{b(j)} + (-1)^{b(n-j)} = 0. \quad j = 0, 1, \dots, n.$$

This, in turn, means that by (20) we have

$$\begin{aligned} f_{2^\mu, n}(-1) &= \sum_{j=0}^{\frac{n-1}{2}} \binom{n}{j} (-1)^{b(j)} + \sum_{j=0}^{\frac{n-1}{2}} \binom{n}{n-j} (-1)^{b(n-j)} \\ &= \sum_{j=0}^{\frac{n-1}{2}} \binom{n}{j} \left((-1)^{b(j)} + (-1)^{b(n-j)} \right) = 0, \end{aligned}$$

which completes the proof. □

We note that Corollary 2 does not mean that we have no divisibility in the exceptional cases. In fact, based on calculations we propose the following

Conjecture 1. Let $\mu \geq 1$ be an integer. Then for any integer $k \geq 1$ there are infinitely many n such that $f_{2^\mu, n}(z) \equiv 0 \pmod{z^k + 1}$.

4. Rational Roots

The existence of rational roots is obviously another divisibility property. In the case of our polynomials $f_{m, n}(z)$ this question presents some interesting challenges; we therefore devote a separate section to it. We begin with a lemma which shows that we only need to consider one specific candidate.

Lemma 6. *Let $m \geq 2$ be an integer. The only possible rational root of $f_{m, n}(z)$ is $z_1 = -1$, with the exception of the root $1 - 2^m$ of $f_{m, m}(z)$.*

Proof. It is obvious from the first identity in (3) that $1 - 2^m$ is the only root of $f_{m, m}(z)$. When $n < m$ then by the definition (2), $f_{m, n}(z)$ is a positive integer. We therefore assume that $n \geq m + 1$.

In this case the polynomial $f_{m,n}(z)$ has leading coefficient 1, and therefore any rational root is an integer dividing $f_{m,n}(0)$. Furthermore, this divisor has to be negative since $f_{m,n}(z)$ has only nonnegative coefficients. Suppose that $-g$ is such an integer solution, and for now we assume that $g \geq 2$. Then with (2) we obtain

$$\begin{aligned} |f_{m,n}(-g)| &\geq g^{\binom{n}{m}} - \sum_{j=0}^{n-1} \binom{n}{j} g^{\binom{j}{m}} \geq g^{\binom{n}{m}} - g^{\binom{n-1}{m}}(2^n - 1) \\ &> g^{\binom{n-1}{m}} \left(g^{\binom{n}{m} - \binom{n-1}{m}} - 2^n \right) = g^{\binom{n-1}{m}} \left(g^{\binom{n-1}{m-1}} - 2^n \right). \end{aligned}$$

Since we assumed that $g \geq 2$, we then have

$$|f_{m,n}(-g)| > 2^{\binom{n-1}{m-1}} \left(2^{\binom{n-1}{m-1}} - 2^n \right). \tag{21}$$

Now for $n \geq m + 2$ and $m \geq 3$ we have

$$\binom{n-1}{m-1} \geq \binom{n-1}{2} > n \quad \text{for } n \geq 5,$$

where the second inequality is easy to verify, and the few cases with $n \leq 4$ are easy to check by computation. Finally, when $n = m + 1$, the second identity in (3) shows that we only need to consider $z = -2$, and only when m is even, in which case we have $f_{m,m+1}(-2) = -3m - 4$.

The case $m = 2$ needs to be treated separately. In a similar way as in the general case, but separating one more term from (2), we have

$$\begin{aligned} |f_{2,n}(-g)| &\geq g^{\binom{n}{2}} - n \cdot g^{\binom{n-1}{2}} - g^{\binom{n-2}{2}}(2^n - n - 1) \\ &> g^{\binom{n-2}{2}} \left(g^{\binom{n}{2} - \binom{n-2}{2}} - n \cdot g^{\binom{n-1}{2} - \binom{n-2}{2}} - 2^n \right) \\ &= g^{\binom{n-2}{2}} \left(g^{2n-3} - n \cdot g^{n-2} - 2^n \right) \geq 2^{\binom{n-2}{2}} \left(2^{2n-3} - n \cdot 2^{n-2} - 2^n \right) \\ &= 2^{\binom{n-2}{2}} 2^{n-2} \left(2^{n-1} - n - 4 \right) \geq 0 \end{aligned}$$

for $n \geq 4$. Together with (21) we have therefore shown that, when $n \neq m$, the only possible rational root is $z_1 = -1$, which concludes the proof of the lemma. \square

Lemma 6 shows that for a fixed $m \geq 2$ it suffices to consider the sequence $(f_{m,n}(-1))_n$. By Proposition 2 we know that, when m is odd, nothing more needs to be shown. However, since the next result is of independent interest, we also include the case where m is odd.

To motivate the following result, we consider the entries in Table 1. Computations indicate that the sequence $(f_{2,n}(-1))$ satisfies the recurrence relation $f_{2,n} = 2 f_{2,n-1} - 2 f_{2,n-2}$, where for simplicity we have deleted the argument -1 ,

i.e., we put $f_{m,n} := f_{m,n}(-1)$. Further, the recurrences for $3 \leq m \leq 6$ and n sufficiently large, appear to be

$$\begin{aligned} f_{3,n} &= 4 f_{3,n-1} - 6 f_{3,n-2} + 4 f_{3,n-3}, \\ f_{4,n} &= 4 f_{4,n-1} - 6 f_{4,n-2} + 4 f_{4,n-3} - 2 f_{4,n-4}, \\ f_{5,n} &= 6 f_{5,n-1} - 14 f_{5,n-2} + 16 f_{5,n-3} - 10 f_{5,n-4} + 4 f_{5,n-5} \\ f_{6,n} &= 8 f_{6,n-1} - 28 f_{6,n-2} + 56 f_{6,n-3} - 70 f_{6,n-4} + 56 f_{6,n-5} \\ &\quad - 28 f_{6,n-6} + 8 f_{6,n-7}. \end{aligned}$$

If $p_m(x)$ denotes the corresponding characteristic polynomial, then we have, along with their factorizations,

$$\begin{aligned} p_2(x) &= x^2 - 2x + 2, \\ p_3(x) &= x^3 - 4x^2 + 6x - 4 = (x^2 - 2x + 2)(x - 2), \\ p_4(x) &= x^4 - 4x^3 + 6x^2 - 4x + 2, \\ p_5(x) &= x^5 - 6x^4 + 14x^3 - 16x^2 + 10x - 4 = (x^4 - 4x^3 + 6x^2 - 4x + 2)(x - 2), \\ p_6(x) &= x^7 - 8x^6 + 28x^5 - 56x^4 + 70x^3 - 56x^2 + 28x - 8 \\ &= (x^4 - 4x^3 + 6x^2 - 4x + 2)(x^2 - 2x + 2)(x - 2). \end{aligned}$$

To explain all this, we define the polynomials

$$g_0(x) := x - 2, \tag{22}$$

$$g_k(x) := (x - 1)^{2^k} + 1 \quad (k \geq 1). \tag{23}$$

By expanding the right-hand side of (23) with the binomial theorem and using, for instance, the congruence (6), we see that $g_k(x)$ is a 2-Eisenstein polynomial for any $k \geq 0$, by which we mean that it satisfies Eisenstein’s criterion with the prime $p = 2$; the polynomial is therefore irreducible over the rationals. There is also a close connection with cyclotomic polynomials; indeed, we can write

$$g_k(x) = \Phi_{2^{k+1}}(x - 1) \quad (k \geq 1), \tag{24}$$

and $g_0(x) = \Phi_1(x - 1)$, where $\Phi_n(x)$ is the n th cyclotomic polynomial. This provides another proof of the fact that all $g_k(x)$ are irreducible.

We are now ready to state the following result.

Proposition 4. *Let $p_m(x)$ be the characteristic polynomial of $(f_{m,n}(-1))_{n \geq 1}$, and let $m = 2^{k_r} + \dots + 2^{k_1}$, $k_r > \dots > k_1 \geq 0$, be the binary representation of $m \geq 2$. Then we have:*

- (1) *If $m = 2^k$, then $p_m(x) = g_k(x)$;*
- (2) *If m is even and not a power of 2, then $p_m(x) = g_{k_r}(x) \cdots g_{k_1}(x)g_0(x)$.*

(3) If m is odd, then $p_m(x) = g_{k_r}(x) \cdots g_{k_1}(x)$.

Example. For $m = 2, 3, \dots, 6$, we immediately obtain $p_2(x) = g_1(x)$ and

$$p_3(x) = g_1(x)g_0(x), p_4(x) = g_2(x), p_5(x) = g_2(x)g_0(x), p_6(x) = g_2(x)g_1(x)g_0(x),$$

which is consistent with the polynomials listed above, before (22).

Proof of Proposition 4. (1) By (12) we have

$$\sum_{\nu=0}^{2^k} (-1)^\nu \binom{2^k}{\nu} f_{2^k, n+2^k-\nu}(-1) = -f_{2^k, n}(-1).$$

This is therefore the recurrence relation for which $g_k(x)$ is the characteristic polynomial, which proves part (1).

(2) We fix an even m , not a power of 2, and denote

$$p_m^0(x) := g_{k_r}(x) \cdots g_{k_1}(x), \quad \text{so that} \quad p_m(x) = p_m^0(x) \cdot (x - 2). \tag{25}$$

Next we denote $A_m := \{k_1, \dots, k_r\}$, and for a subset $A \subseteq A_m$ we define

$$e(A) := \sum_{j \in A} 2^j,$$

so that in particular we have $e(\emptyset) = 0$ and $e(A_m) = m$. Then by (25),

$$p_m^0(x) = \prod_{j \in A_m} \left((x - 1)^{2^j} + 1 \right) = \sum_{A \subseteq A_m} (x - 1)^{e(A)}, \tag{26}$$

and with $g_0(x) = ((x - 1) - 1)$,

$$p_m(x) = \sum_{A \subseteq A_m} \left((x - 1)^{e(A)+1} - (x - 1)^{e(A)} \right). \tag{27}$$

Next we expand the terms in (27) binomially and replace x^j by $f_{m, j+n}(-1)$. Then we use (7) with $z = -1$ and $r = e(A)$, resp. $r = e(A) + 1$, for all $A \subseteq A_m$, and the right-hand side of (27) becomes

$$\begin{aligned} S_m(n) &:= \sum_{A \subseteq A_m} \left(\sum_{j=0}^n \binom{n}{j} (-1)^{\binom{j+e(A)+1}{m}} - \sum_{j=0}^n \binom{n}{j} (-1)^{\binom{j+e(A)}{m}} \right) \\ &= \sum_{j=0}^n \binom{n}{j} \sum_{A \subseteq A_m} \left((-1)^{\binom{j+e(A)+1}{m}} - (-1)^{\binom{j+e(A)}{m}} \right). \end{aligned} \tag{28}$$

We are done if we can show that $S_m(n) = 0$ for all $n \geq 1$, since then $p_m(x)$ is indeed the characteristic polynomial for the sequence $(f_{m, n}(-1))_{n \geq 1}$.

To simplify the right-most term in (28) we denote, for any integer $r \geq 0$,

$$\binom{r}{m}^* \equiv \binom{r}{m} \pmod{2}, \quad \binom{r}{m}^* \in \{0, 1\}.$$

Since obviously $(-1)^a = 1 - 2a$ for $a \in \{0, 1\}$, we have

$$(-1)^{\binom{r}{m}} = 1 - 2\binom{r}{m}^* \quad (r = 0, 1, 2, \dots),$$

and with (28) we get

$$S_m(n) = 2 \sum_{j=0}^n \binom{n}{j} \sum_{A \subseteq A_m} \left(\binom{j+e(A)}{m}^* - \binom{j+e(A)+1}{m}^* \right). \quad (29)$$

We recall that, by Lemma 6(1), for a fixed m with $2^{\nu-1} < m < 2^\nu$, the sequence $\binom{r}{m}^*$ is periodic with period 2^ν . Since $m = 2^{k_1} + \dots + 2^{k_r}$, by Lucas's congruence (6) we have $\binom{j+e(A)}{m}^* = 0$ unless all powers $2^{k_1}, \dots, 2^{k_r}$ occur in the binary expansion of $j + e(A)$. For each j there is exactly one $A \subseteq A_m$ for which this is the case. Indeed, let $B_j \subseteq A_m$ be the possibly empty subset containing all $i \in A_m$ for which 2^i occurs in the binary expansion of j ; then $A = A_m \setminus B_j$. Similarly, for $j + e(A) + 1$ we have the unique set $A = A_m \setminus B_{j+1}$ for which the second binomial coefficient is 1. These two values “1” cancel, and thus the inner sum in (29) vanishes for each j . Hence $S_m(n) = 0$ for all $n \geq 1$, which proves part (2).

(3) When m is odd, the situation is similar to part (2), but with some important differences. While in $p_m(x)$ we no longer consider the additional factor $g_0(x)$, we now have $k_1 = 0$, and so $g_{k_1}(x) = x - 2 = (x - 1) - 1$. Therefore we consider

$$p_m(x) = g_{k_r}(x) \cdots g_{k_2}(x) \cdot (x - 2),$$

and with $A'_m := \{k_2, \dots, k_r\}$ we have, as in (27),

$$p_m(x) = \sum_{A \subseteq A'_m} \left((x - 1)^{e(A)+1} - (x - 1)^{e(A)} \right),$$

where, by definition, $e(A)$ is always even. Then (29) holds as before, with A'_m in place of A_m .

To finish the proof, we use the same argument as in part (2) and note that (since $e(A)$ is even) for each odd j there is exactly one $A \subseteq A'_m$ such that $\binom{j+e(A)}{m}^* = 1$, while $\binom{j+e(A)+1}{m}^* = 0$ for all $A \subseteq A'_m$. Conversely, when j is even, there is exactly one $A \subseteq A'_m$ such that $\binom{j+e(A)+1}{m}^* = 1$, while $\binom{j+e(A)}{m}^* = 0$ for all $A \subseteq A'_m$.

This implies that the inner sum in (29) is $(-1)^{j+1}$, and therefore, by the binomial theorem, we have again $S_m(n) = 0$ for all $n \geq 1$. This completes part (3) of the proposition. \square

We are now ready to prove the main result of this section.

Proposition 5. *Let $m \geq 2$ be an integer.*

- (a) $f_{m,m}(z)$ has the root $z_0 = 1 - 2^m$.
- (b) When m is odd and $n \geq 1$, then $f_{m,n}(z)$ has no other rational roots.
- (c) When m is even but not a power of 2, then $f_{m,n}(z)$ has no other rational roots except, possibly, $z_1 = -1$ for finitely many n .
- (d) When $m = 2^k$, $k \geq 1$, then $f_{m,2^j m-1}(-1) = 0$ for all $j = 1, 2, \dots$, and there are at most finitely many other n for which $f_{m,n}(z)$ has a rational root.

Proof. Statement (a) is obvious from the first identity in (3). By Lemma 6, the only other possible rational root is $z_1 = -1$. When m is odd, we use Proposition 2(1) which implies that the sequence $(f_{m,n}(-1))_{n \geq 1}$ is increasing. But for $n \leq m - 1$ these are positive constants, and also $f_{m,m}(-1) = 2^m - 2 > 0$; thus $f_{m,n}(-1) > 0$ for all $n \geq 1$, which proves part (b).

When m is even and not a power of 2, we use Proposition 4(2). Since the polynomials $g_k(x)$, $k \geq 0$, are distinct and irreducible, the characteristic polynomials $p_m(x)$ all have simple roots, one of which is $x_0 = 2$. From (23) we can explicitly determine all roots of $g_k(x)$ for $k \geq 1$, namely

$$1 + \exp\left(\pm \frac{2j + 1}{2^k} \pi i\right), \quad j = 0, 1, \dots, 2^{k-1} - 1, \tag{30}$$

and from this it is not difficult to see that the respective moduli are

$$2 \cdot \cos\left(\frac{2j + 1}{2^{k+1}} \pi\right) < 2.$$

It follows from a well-known fact in the theory of linear recurrence relations (see, e.g., [6, p. 4] or [13]) that in this case, where $p_m(x)$ has only simple roots $x_0 = 2, x_1, \dots, x_m$, we can write

$$f_{m,n}(-1) = a_0 2^n + a_1 x_1^n + \dots + a_m x_m^n. \tag{31}$$

The coefficients a_0, a_1, \dots, a_m are constants that could be determined by solving a suitable linear system, using $m + 1$ terms of the sequence. Since $x_0 = 2$ is the unique root of $p_m(x)$ with largest absolute value, it can be shown by way of the method of Darboux (see, e.g., [15, p. 310]), together with the theory of generating functions of linear recurrences (see, e.g., [13]), that $f_{m,n}(-1) = O(2^n)$, and thus $a_0 \neq 0$. Alternatively, an explicit expression of a_0 can be found in (41) in the next section. Now, since $|x_j| < 2$ for all $j = 1, \dots, m$, we have $f_{m,n}(-1) \neq 0$ if n is sufficiently large. This proves part (c).

Finally, the first statement of part (d) is just a restatement of Corollary 3, while the second statement follows from Corollary 6 in the next section. □

Remark 1. (1) From (30) it is also not difficult to see that the arguments of the pair of roots belonging to j are $\pm(2j+1)2^{-k-1}\pi$. So, in particular, the two complex conjugate roots of $g_k(x)$ with largest modulus are

$$2 \cdot \cos\left(\frac{\pi}{2^{k+1}}\right) \cdot \exp\left(\pm \frac{\pi i}{2^{k+1}}\right), \quad \text{modulus } \beta_k := 2 \cdot \cos\left(\frac{\pi}{2^{k+1}}\right). \quad (32)$$

This means that the modulus of the largest roots gets very close to 2 very quickly, as k grows. For instance, the largest roots of $g_4(x)$ have modulus $2 \cos(\pi/32) \simeq 1.99037$.

This fact, together with (31), explains why the sequence $(f_{m,n}(-1))_n$ displays a rather irregular behavior for some even m . Here is a summary of our computations for even m , $1 \leq m \leq 128$ and $1 \leq n \leq 5000$:

- (a) $f_{12,n}(-1) < 0$ for $24 \leq n \leq 29$, and positive elsewhere.
- (b) $f_{24,n}(-1) < 0$ for $48 \leq n \leq 62$ and $115 \leq n \leq 123$, and positive elsewhere.
- (c) For $m = 40, 48, 56, 72, 80, 96$, and 112 , $f_{m,n}(-1)$ also has intervals of negative values, not all beginning with $n = 2m$.
- (d) The values $f_{20,n}(-1)$ are all positive, but $f_{20,44}(-1) < f_{20,42}(-1)$. Apart from (a)–(c) and $m = 2^k$, this is the only case for which monotonicity fails.
- (e) For all other even m that are not a power of 2, the sequence $(f_{m,n}(-1))_{n \geq 1}$ is positive and strictly increasing.

All these computations were done with Maple.

5. More on the Sequence $f_{2^k,n}(-1)$

We have seen in several places in Sections 3 and 4 that the case $m = 2^k$ is quite exceptional. We therefore devote this separate section to investigating the sequence $f_{2^k,n} = f_{2^k,n}(-1)$ in greater detail, where $k \geq 1$ is considered fixed. We recall that the sequence $(f_{2^k,n})_{n \geq 0}$ is a linear recurrence sequence with constant coefficients and with characteristic polynomial $g_k(x)$, as defined in (23). We begin by obtaining the ordinary generating function of this sequence.

Proposition 6. *Let $k \geq 1$ be an integer. Then*

$$\sum_{n=0}^{\infty} f_{2^k,n} x^n = \frac{1}{2x-1} \cdot \frac{x^{2^k} - (x-1)^{2^k}}{x^{2^k} + (x-1)^{2^k}}, \quad |x| < \frac{1}{\beta_k}, \quad (33)$$

where $\beta_k = 2 \cos(\pi/2^{k+1})$.

Proof. Using the definition (2) and changing the order of summation, we obtain

$$S_k(x) := \sum_{n=0}^{\infty} f_{2^k, n} x^n = \sum_{j=0}^{\infty} (-1)^{\binom{j}{2^k}} \sum_{n=j}^{\infty} \binom{n}{j} x^n.$$

By absolute convergence for sufficiently small x this is allowable. Upon shifting the summation and using a well-known series evaluation (see, e.g., [10, Eq. (1.3)]), the inner sum becomes

$$x^j \sum_{n=0}^{\infty} \binom{n+j}{j} x^n = \frac{x^j}{(1-x)^{j+1}}, \quad |x| < 1,$$

which gives

$$S_k(x) = \sum_{j=0}^{\infty} (-1)^{\binom{j}{2^k}} \frac{x^j}{(1-x)^{j+1}}. \tag{34}$$

The binomial coefficient in the exponent has already been evaluated in (14), and using periodicity with period 2^{k+1} (see again Lemma 2), the series in (34) becomes

$$\begin{aligned} S_k(x) &= \sum_{j=0}^{2^k-1} \sum_{\ell=0}^{\infty} \left(\frac{x^{j+\ell 2^{k+1}}}{(1-x)^{j+1+\ell 2^{k+1}}} - \frac{x^{j+2^k+\ell 2^{k+1}}}{(1-x)^{j+1+2^k+\ell 2^{k+1}}} \right) \\ &= \sum_{j=0}^{2^k-1} \frac{x^j}{(1-x)^{j+1}} \left(1 - \frac{x^{2^k}}{(1-x)^{2^k}} \right) \sum_{\ell=0}^{\infty} \frac{x^{\ell 2^{k+1}}}{(1-x)^{\ell 2^{k+1}}}. \end{aligned} \tag{35}$$

Now the finite sum in this last line evaluates as

$$\frac{1}{1-x} \cdot \frac{1 - \left(\frac{x}{1-x}\right)^{2^k}}{1 - \frac{x}{1-x}} = \frac{1}{1-2x} \cdot \frac{(1-x)^{2^k} - x^{2^k}}{(1-x)^{2^k}}, \tag{36}$$

while the infinite series in the same line has sum

$$\frac{1}{1 - (x/(1-x))^{2^{k+1}}} = \frac{(1-x)^{2^{k+1}}}{(1-x)^{2^{k+1}} - x^{2^{k+1}}}, \quad |x| < \frac{1}{2}. \tag{37}$$

We substitute (36) and (37) into (35); then we get (33) after some straightforward manipulations which include the polynomial factorization

$$(1-x)^{2^{k+1}} - x^{2^{k+1}} = \left((1-x)^{2^k} - x^{2^k} \right) \left((1-x)^{2^k} + x^{2^k} \right)$$

Finally we note that $x = 1/2$ is a removable singularity of the right-hand side of (33). By analytic continuation, the identity (33) then holds for all $x \in \mathbb{C}$ with $|x| < 1/\beta_k$ since, by (32), $1/\beta_k$ is the smallest modulus of the roots of

$$x^{2^k} + (x-1)^{2^k} = x^{2^k} g_k\left(\frac{1}{x}\right).$$

This completes the proof of the proposition. □

As an application of (33) we set $x = \frac{1}{2}$, which still lies inside the circle of convergence. Then after some easy manipulations (e.g., using L'Hospital's Rule on the right-hand side of (33)), we get the following somewhat surprising series evaluations.

Corollary 4. *For any integer $k \geq 1$, we have*

$$\sum_{n=0}^{\infty} f_{2^k, n} \cdot \left(\frac{1}{2}\right)^n = 2^k.$$

The next result gives an explicit formula for all $f_{2^k, n}$; it can also be seen as a refinement of Corollary 3.

Proposition 7. *For any integers $k \geq 1$ and $n \geq 0$ we have*

$$f_{2^k, n} = 2^{1-k} \sum_{j=1}^{2^{k-1}} \frac{(2 \cos(\frac{2j-1}{2^{k+1}}\pi))^n}{\sin(\frac{2j-1}{2^{k+1}}\pi)} \cdot \sin\left((n+1)\frac{2j-1}{2^{k+1}}\pi\right). \tag{38}$$

Before proving this result, we give the two smallest cases as illustrations. For this, we have used some well-known special values for sine and cosine.

Corollary 5. *For all integers $n \geq 0$ we have*

$$\begin{aligned} f_{2, n} &= (\sqrt{2})^{n+1} \sin\left(\frac{n+1}{4}\pi\right), \\ f_{4, n} &= \frac{1}{\sqrt{2}}(2 + \sqrt{2})^{\frac{n+1}{2}} \sin\left(\frac{n+1}{8}\pi\right) + \frac{1}{\sqrt{2}}(2 - \sqrt{2})^{\frac{n+1}{2}} \sin\left(\frac{3(n+1)}{8}\pi\right). \end{aligned}$$

Proof of Proposition 7. By the theory of linear recurrence relations (see, e.g., [6, p. 4] or [13]), and since the characteristic polynomial $g_k(x)$ has only simple roots, we have

$$f_{2^k, n} = \sum_{j=1}^{2^k} a_j^{(k)} \cdot (x_j^{(k)})^n, \tag{39}$$

where $a_j^{(k)}$, $j = 1, 2, \dots, 2^k$, are constant coefficients, and $x_j^{(k)}$, $j = 1, 2, \dots, 2^k$, are the roots of $g_k(x)$. As we saw in (31) and in Remark 1(1), we have

$$x_j^{(k)} = 1 + \exp\left(\frac{2j-1}{2^k}\pi i\right) = 2 \cos\left(\frac{2j-1}{2^{k+1}}\pi\right) \exp\left(\frac{2j-1}{2^{k+1}}\pi i\right). \tag{40}$$

To determine the coefficients $a_j^{(k)}$, we use (39) together with (36), to set up a linear system of 2^k equations for $n = 0, 1, \dots, 2^k - 1$ (the matrix of this system is a Vandermonde matrix). We did this for some small k and found, conjecturally, that

$$a_j^{(k)} = \frac{2^{1-k}}{1 - \exp\left(-\frac{2j-1}{2^k}\pi i\right)} = \frac{-i \cdot x_j^{(k)}}{2^k \sin\left(\frac{2j-1}{2^k}\pi\right)}. \tag{41}$$

Pairing the product of (40) and (41) for each j with that of $2^k + 1 - j$, $j = 1, 2, \dots, 2^{k-1}$, we obtain (38) from (39). In order to prove this in general, it remains to show that for each $k \geq 1$, the right-hand side of (38) equals 2^n for all $n = 0, 1, \dots, 2^k - 1$, or equivalently

$$\sum_{j=1}^{2^{k-1}} \frac{\sin((n+1)\alpha_j)}{\sin(\alpha_j)} \cos^n(\alpha_j) = 2^{k-1}, \quad \alpha_j := \frac{2j-1}{2^{k+1}}\pi. \tag{42}$$

This identity actually holds in greater generality. We are going to use Chebyshev polynomials of the second kind, $U_n(x)$, defined by

$$U_n(\cos \theta) = \frac{\sin((n+1)\theta)}{\sin \theta}$$

(see, e.g., [18, Eq. (1.23)]), and we will show that

$$\sum_{j=1}^m U_n(\cos(\frac{2j-1}{4m}\pi)) \cos^n(\frac{2j-1}{4m}\pi) = m, \quad 0 \leq n \leq 2m-1. \tag{43}$$

Then (42) immediately follows from (43), with $m = 2^{k-1}$.

When $n = 0$, then (43) is trivially true. To prove (43) for $n \geq 1$, we use the well-known explicit formula

$$U_n(x) = \sum_{\nu=0}^{\lfloor n/2 \rfloor} (-1)^\nu \binom{n-\nu}{\nu} (2x)^{n-2\nu} \quad (n \geq 1);$$

see, e.g., [18, p. 39]. Substituting this into (43) and changing the order of summation, we see that (43) holds if we can show that

$$\sum_{\nu=0}^{\lfloor n/2 \rfloor} (-1)^\nu \binom{n-\nu}{\nu} 2^{n-2\nu} \sum_{j=1}^m \cos^{2n-2\nu}(\frac{2j-1}{4m}\pi) = m. \tag{44}$$

The inner sum in (44) is easy to reduce to a known sum; indeed, if we rewrite it as

$$\sum_{j=1}^{2m} \cos^{2n-2\nu}(\frac{j}{4m}\pi) - \sum_{j=1}^m \cos^{2n-2\nu}(\frac{2j}{4m}\pi),$$

we can use the identity 4.4.2.11 in [16, p. 640] twice, obtaining

$$\sum_{j=1}^m \cos^{2n-2\nu}(\frac{2j-1}{4m}\pi) = \frac{4m}{2^{2n-2\nu+1}} \binom{2n-2\nu}{n-\nu} - \frac{2m}{2^{2n-2\nu+1}} \binom{2n-2\nu}{n-\nu}$$

(valid for $n - \nu < 2m$), so that the left-hand side of (44) becomes

$$\frac{m}{2^n} \sum_{\nu=0}^{\lfloor n/2 \rfloor} (-1)^\nu \binom{n-\nu}{\nu} \binom{2n-2\nu}{n-\nu} = \frac{m}{2^n} \sum_{\nu=0}^{\lfloor n/2 \rfloor} (-1)^\nu \binom{n}{\nu} \binom{2n-2\nu}{n},$$

where it is easy to check that the two products of binomial coefficients are identical. Finally, the sum on the right has the known evaluation 2^n ; see, e.g., [10, Eq. (3.117)]. Thus we have shown that (44) holds, which completes the proof. \square

The following result is our main application of Proposition 7; in fact, it was already used in the proof of Proposition 5(d).

Corollary 6. *Let $k \geq 1$ and $1 \leq r \leq 2^{k+1} - 1$ be fixed integers. Then for all $\nu \geq 2^{3k-1}/\pi^2$ we have*

$$(-1)^\nu f_{2^k, n} > 0, \quad \text{where } n = \nu \cdot 2^{k+1} + r - 1.$$

Proof. For $k = 1$ and $n = 4\nu + r - 1$ we have by Corollary 5,

$$f_{2, n} = (\sqrt{2})^{n+1} \sin\left(\frac{4\nu+r}{4}\pi\right) = (-1)^\nu (\sqrt{2})^{4\nu+r} \sin\left(\frac{r\pi}{4}\right),$$

and since $1 \leq r \leq 3$, the sine term on the right is positive. Hence the statement is true for $k = 1$ and all $\nu \geq 0$.

Now let $k \geq 2$. We are going to use (38), and first note that

$$\begin{aligned} \sin\left((n+1)\frac{2j-1}{2^{k+1}}\pi\right) &= \sin\left(\nu(2j-1)\pi + \frac{r(2j-1)}{2^{k+1}}\pi\right) \\ &= (-1)^\nu \sin\left(\frac{r(2j-1)}{2^{k+1}}\pi\right), \end{aligned}$$

so that

$$f_{2^k, n} = 2^{n+1-k} (-1)^\nu \sum_{j=1}^{2^{k-1}} \cos^n\left(\frac{2j-1}{2^{k+1}}\pi\right) \cdot \frac{\sin\left(\frac{r(2j-1)}{2^{k+1}}\pi\right)}{\sin\left(\frac{2j-1}{2^{k+1}}\pi\right)}, \quad (45)$$

with $n = \nu \cdot 2^{k+1} + r - 1$. Now let S_n be the sum on the right of (45). We now use the fact that $|\sin(r\alpha)/\sin(\alpha)| \leq r$ for any $\alpha \in \mathbb{R}$ and integer $r \geq 1$. This can be seen, for instance, by combining the identities (1.23) and (1.24) in [18, pp. 7–8]. Then we have the estimate

$$\begin{aligned} S_n &\geq \cos^n\left(\frac{\pi}{2^{k+1}}\right) - \sum_{j=2}^{2^{k-1}} \cos^n\left(\frac{3\pi}{2^{k+1}}\right) \cdot r \\ &\geq \cos^n\left(\frac{\pi}{2^{k+1}}\right) - \cos^n\left(\frac{3\pi}{2^{k+1}}\right) (2^{k-1} - 1)(2^{k+1} - 1) \\ &> \cos^n\left(\frac{3\pi}{2^{k+1}}\right) \left(\left(\frac{\cos(\pi/2^{k+1})}{\cos(3\pi/2^{k+1})}\right)^n - 2^{2k}\right). \end{aligned} \quad (46)$$

We now estimate the quotient of cosines in this last expression. For ease of notation we set $\alpha := \pi/2^{k+1}$, and first note that $\alpha \leq \frac{\pi}{8} < \frac{4}{5}$ for $k \geq 2$. By the Maclaurin expansion for cosine we have

$$\cos \alpha > 1 - \frac{1}{2}\alpha^2 \quad \text{and} \quad \cos(3\alpha) < 1 - \frac{1}{2}(3\alpha)^2 + \frac{1}{24}(3\alpha)^4.$$

So we get

$$\frac{\cos(\alpha)}{\cos(3\alpha)} > \frac{1 - \frac{1}{2}\alpha^2}{1 - \frac{1}{2}(3\alpha)^2 + \frac{1}{24}(3\alpha)^4} > 1 + 4\alpha^2,$$

where it is straightforward to verify that the right inequality holds for $0 < \alpha < \frac{4}{5}$. Thus, using $n = \nu \cdot 2^{k+1} + r - 1$,

$$\left(\frac{\cos(\alpha)}{\cos(3\alpha)}\right)^n > \left(1 + 4 \cdot \frac{\pi^2}{2^{2k+2}}\right)^n > 1 + \nu \cdot 2^{k+1} \cdot 4 \cdot \frac{\pi^2}{2^{2k+2}} > \frac{\nu\pi^2}{2^{k-1}}.$$

Hence, by (46) we have $S_n > 0$ when $\nu\pi^2 \geq 2^{3k-1}$, and with (45) this completes the proof. \square

It is clear from this proof that the lower bound for ν could be somewhat improved, but also, we conjecture that the statement of Corollary 6 holds for all $\nu \geq 0$. By numerical computation we checked that our conjecture is true for $k \leq 5$. In fact, at the end of this section we propose a stronger conjecture.

As another consequence of Proposition 7 we obtain a proof of the observation that in each sequence $(f_{2^k, n})_{n \geq 0}$, any two terms that immediately precede a zero term are identical; see also Table 1. A second, related, identity can be obtained in a similar way. We recall that $f_{2^k, \nu \cdot 2^{k+1} - 1} = 0$ for all integers $k, \nu \geq 1$, a fact that is also obvious from (38).

Corollary 7. *For all integers $k, \nu \geq 1$ we have*

$$\begin{aligned} f_{2^k, \nu \cdot 2^{k+1} - 2} &= f_{2^k, \nu \cdot 2^{k+1} - 3}, \\ f_{2^k, (2\nu - 1)2^{k+1} - 1} &= 2f_{2^k, (2\nu - 1)2^{k+1} - 2}. \end{aligned}$$

Proof. To obtain the first identity we show that, in fact, for a fixed $k \geq 1$ the corresponding summands on the right of (38) have the same values for each $j = 1, 2, \dots, 2^{k-1}$. This is equivalent to

$$2 \cos(\alpha_j) \sin((\nu \cdot 2^{k+1} - 1)\alpha_j) = \sin((\nu \cdot 2^{k+1} - 2)\alpha_j), \quad \alpha_j := \frac{2j - 1}{2^{k+1}}\pi.$$

But this identity is easy to verify by way of some elementary trigonometric identities. The second identity can be obtained in an analogous way. \square

It follows from the definition (2) that $f_{2^k, n} = 2^n$ for $0 \leq n \leq 2^k - 1$. We can extend this as follows. This is also related to Corollary 6 with $\nu = 1$.

Proposition 8. *Let $k \geq 2$ be an integer. Then the sequence $(f_{2^k, n})_{n \geq 0}$ is positive and nondecreasing for $0 \leq n \leq 2^{k+1} - 2$.*

Proof. For $0 \leq n \leq 2^k - 1$, the statement is clear by the remark just before the proposition. For $2^k \leq n \leq 2^{k+1} - 2$, we use (14), obtaining

$$f_{2^k,n} = \sum_{j=0}^n \binom{n}{j} (-1)^{\binom{j}{2^k}} = \sum_{j=0}^{2^k-1} \binom{n}{j} - \sum_{j=2^k}^n \binom{n}{j}. \tag{47}$$

For n in the given range, we see that each negative binomial coefficient on the right is canceled by its positive counterpart, with at least one positive term remaining. This proves the positivity claim.

Next, by the left equality of (47), or by (7) with $r = 1$ and $z = -1$, we have

$$f_{2^k,n+1} - f_{2^k,n} = \sum_{j=0}^n \binom{n}{j} (-1)^{\binom{j+1}{2^k}} = \sum_{j=0}^{2^k-2} \binom{n}{j} - \sum_{j=2^k-1}^n \binom{n}{j}, \tag{48}$$

where we have used (14) again. We now argue just as in the first part of this proof. When n is such that $2^k - 1 \leq n \leq 2^{k+1} - 4$, then each negative binomial coefficient is canceled by its positive counterpart, with at least one positive term remaining. Hence $f_{2^k,n}$ is strictly increasing for $n \leq 2^{k+1} - 3$. Finally, the right-hand side of (48) vanishes for $n = 2^{k+1} - 3$; this also follows from Corollary 6. \square

Computations indicate that the behavior of the sequence $(f_{2^k,n})_{n \geq 0}$ proved in Proposition 8 holds for each interval between the zeros that occur at all $n = (\nu + 1) \cdot 2^{k+1} - 1$, $\nu = 0, 1, 2, \dots$

Conjecture 2. Let $k \geq 1$ and $\nu \geq 0$ be integers. If $\nu \cdot 2^{k+1} \leq n \leq (\nu + 1) \cdot 2^{k+1} - 2$, then $(-1)^\nu f_{2^k,n} > 0$, and the sequence $((-1)^\nu f_{2^k,n})_n$ is strictly increasing in this interval, with the exception of the final two terms which are equal.

Further supporting evidence for this conjecture is given by Corollaries 6 and 7, where the former shows that the alternating sign structure is true, at least for sufficiently large ν , depending on k .

6. Some Irreducibility Results

Computations with Maple suggest that, apart from the factors $z^k + 1$ exhibited in the previous section, and the rational roots in Proposition 3.7(a), all other polynomials $f_{m,n}(z)$ are irreducible. While we are unable to prove this in general, we have the following result. For the remainder of this paper, “irreducible” will mean irreducible over \mathbb{Q} .

Proposition 9. *Let p be an odd prime, d an integer with $1 \leq d \leq p - 1$, and suppose that*

$$\sum_{k=1}^d \frac{(-1)^{k-1}}{k} \not\equiv 0 \pmod{p}. \tag{49}$$

Then for every $n = j(p - 1)p$, where $j = 1, 2, \dots$ and $p \nmid j$, the polynomial $f_{n-d,n}(z)$ is p -Eisenstein and thus irreducible. If, furthermore, $p \equiv \pm 1 \pmod{8}$, then the conclusion holds for all $n = j(p - 1)p/2$, with j as above.

Proof. By (2) we have

$$f_{n-d,n}(z) = z^{\binom{n}{n-d}} + \binom{n}{1} z^{\binom{n-1}{n-d}} + \dots + \binom{n}{d} z + \sum_{k=0}^{n-d-1} \binom{n}{k}. \tag{50}$$

We now consider

$$\binom{n}{r} = \frac{n(n-1)\dots(n-r+1)}{r!}, \quad 1 \leq r \leq d \leq p-1.$$

If n is a multiple of p , we see that there is no cancellation, and thus $p \mid \binom{n}{r}$. Therefore, to prove that $f_{n-d,n}(z)$ is p -Eisenstein, it remains to show that

$$p \parallel \sum_{k=0}^{n-d-1} \binom{n}{k}, \tag{51}$$

that is, p but not p^2 divides the sum on the right. To do so, we note that

$$\sum_{k=0}^{n-d-1} \binom{n}{k} = 2^n - 1 - \binom{n}{1} - \dots - \binom{n}{d}. \tag{52}$$

First, by Fermat’s little theorem, we have for $n = j(p - 1)p$,

$$2^n = (2^{p-1})^{jp} = (1 + \nu p)^{jp} = 1 + jp\nu p + O(p^2) \equiv 1 \pmod{p^2}. \tag{53}$$

If $p \equiv \pm 1 \pmod{8}$, then 2 is a quadratic residue modulo p , and by Euler’s criterion we have $2^{(p-1)/2} \equiv 1 \pmod{p}$. Then, just as in (53), we get

$$2^n \equiv 1 \pmod{p^2} \quad \text{for } n = j(p - 1)p/2. \tag{54}$$

Next, when $n = sp$, $p \nmid s$, then for $1 \leq k \leq d$ we have

$$\begin{aligned} \binom{n}{k} &= \frac{sp}{k!} (sp - 1)(sp - 2) \dots (sp - k + 1) \\ &\equiv \frac{sp}{k!} (-1)^{k-1} (k - 1)! = sp \frac{(-1)^{k-1}}{k} \pmod{p^2}. \end{aligned}$$

This, together with (52) and with (53), resp. (54), shows that

$$\sum_{k=0}^{n-d-1} \binom{n}{k} \equiv -sp \sum_{k=1}^d \frac{(-1)^{k-1}}{k} \pmod{p^2}.$$

Hence (49) implies (51), and the proof is complete. □

Example. Let $d = 3$ and $p = 5$. Then $j = 1$ gives $n = 20$, and

$$f_{17,20}(z) = z^{1140} + 20 z^{171} + 190 z^{18} + 1140 z + 1\,047\,225.$$

As we can see, 5^2 divides the constant coefficients, so this polynomial is not 5-Eisenstein. And indeed, we have $1 - \frac{1}{2} + \frac{1}{3} = \frac{5}{6}$, so (49) does not hold.

On the other hand, $p = 7$ does satisfy this condition, and since $7 \equiv -1 \pmod{8}$, Proposition 9 applies to $n = 21$. In fact, it is easily seen that

$$f_{18,21}(z) = z^{1330} + 21 z^{190} + 210 z^{19} + 1330 z + 2\,095\,590$$

is indeed 7-Eisenstein. Finally, we note that, although $f_{17,20}(z)$ does not satisfy the Eisenstein criterion, one can verify by computer algebra (in our case, using Maple) that it is irreducible.

In the cases $d = 1$ and $d = 2$, the condition (49) becomes irrelevant, and we can state the following corollary,

Corollary 8. *Let p be an odd prime, and let $n = j(p - 1)p$, resp. $n = j(p - 1)p/2$ when $p \equiv \pm 1 \pmod{8}$, where $j = 1, 2, \dots$ and $p \nmid j$. Then $f_{n-1,n}(z)$ and $f_{n-2,n}(z)$ are irreducible.*

The next corollary has an unexpected connection with Wieferich primes, which are closely related to Fermat quotients. For an odd prime p and an integer $a \geq 2$ with $p \nmid a$, the *Fermat quotient to base a* is defined by

$$q_p(a) := \frac{a^{p-1} - 1}{p}.$$

Fermat’s little theorem implies that this is an integer. A prime p that satisfies $q_p(2) \equiv 0 \pmod{p}$ is called a *Wieferich prime*. These primes played an important role in the classical theory of Fermat’s last theorem; see, e.g., [17]. Only two such primes are known, namely $p = 1093$ and $p = 3511$. The latest published search [5] for Wieferich primes went up to 6.7×10^{15} , while the current record stands at 6×10^{17} ; see [8]. It is not known whether there are infinitely many Wieferich primes, or even whether there are infinitely many non-Wieferich primes; see [11].

Corollary 9. *Let p be an odd non-Wieferich prime, and let $d = p - 1$, $d = (p - 1)/2$, or $d = \lfloor p/3 \rfloor$. Then $f_{n-d,n}(z)$ is irreducible for all $n = j(p - 1)p$, resp. $n = j(p - 1)p/2$ when $p \equiv \pm 1 \pmod{8}$, where $j = 1, 2, \dots$ and $p \nmid j$.*

Proof. To apply Proposition 9, it remains to verify (49). First we note that

$$\sum_{k=1}^d \frac{(-1)^{k-1}}{k} = \sum_{k=1}^d \frac{1}{k} - \sum_{k=1}^{\lfloor d/2 \rfloor} \frac{1}{k}. \tag{55}$$

We now recall the classical congruences

$$\sum_{k=1}^{p-1} \frac{1}{k} \equiv 0 \pmod{p}, \quad \sum_{k=1}^{(p-1)/2} \frac{1}{k} \equiv -2q_p(2) \pmod{p}, \tag{56}$$

$$\sum_{k=1}^{\lfloor p/3 \rfloor} \frac{1}{k} \equiv -\frac{3}{2}q_p(3) \pmod{p}, \quad \sum_{k=1}^{\lfloor p/4 \rfloor} \frac{1}{k} \equiv -3q_p(2) \pmod{p}, \tag{57}$$

$$\sum_{k=1}^{\lfloor p/6 \rfloor} \frac{1}{k} \equiv -2q_p(2) - \frac{3}{2}q_p(3) \pmod{p}. \tag{58}$$

All these congruences have well-known extensions modulo p^2 and p^3 . The left congruence in (56) follows from the fact that $\{1, 1/2, \dots, 1/(p-1)\}$ forms a reduced residue system modulo p , the sum of which is divisible by p . The right-hand congruence in (56) goes back to Eisenstein in 1850. All are special cases of congruences in [12]; see also [17, p. 155]. Combining them with (55), we see that

$$\begin{aligned} \sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} &\equiv 2q_p(2) \pmod{p}, & \sum_{k=1}^{(p-1)/2} \frac{(-1)^{k-1}}{k} &\equiv q_p(2) \pmod{p}, \\ \sum_{k=1}^{\lfloor p/3 \rfloor} \frac{(-1)^{k-1}}{k} &\equiv 2q_p(2) \pmod{p}. \end{aligned}$$

These cannot vanish modulo p unless p is a Wieferich prime. □

Acknowledgments. We would like to thank the anonymous referee for numerous suggestions which helped improve this paper. Research of the first author was supported in part by the Natural Sciences and Engineering Research Council of Canada, Grant # 145628481. Research of the second author was supported by a grant of the Polish National Science Centre, Poland, no. UMO-2019/34/E/ST1/00094

References

[1] J. I. Brown, K. Dilcher, and D. V. Manna, Series representations of theta functions in terms of a sequence of polynomials, *Fibonacci Quart.* **50** (2012), 5–10.

- [2] J. I. Brown, K. Dilcher, and D. V. Manna, On the roots of expected independence polynomials, *J. Graph Theory* **73** (2013), no. 3, 322–326.
- [3] J. I. Brown, K. Dilcher, and D. V. Manna, On a sequence of sparse binomial-type polynomials, *J. Math. Anal. Appl.* **398** (2013), 128–137.
- [4] K. Dilcher and M. Ulas, Some properties of a class of sparse polynomials, *J. Math. Anal. Appl.* **505** (2022), no. 1, Paper No. 125449, 18 pp.
- [5] F. G. Dorais and D. Klyve, A Wieferich prime search up to 6.7×10^{15} , *J. Integer Seq.* **14** (2011), no. 9, Article 11.9.2, 14 pp.
- [6] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward, *Recurrence Sequences*, American Mathematical Society, Providence, Rhode Island, 2003.
- [7] N. J. Fine, Binomial coefficients modulo a prime, *Amer. Math. Monthly* **54** (1947), 589–592.
- [8] R. Fischer, Tables of (prime) numbers. Fermat quotients. Web resource, available at http://www.fermatquotient.com/FermatQuotienten/FermQ_Sort.txt. (Accessed September 7, 2021).
- [9] W. Gawronski and T. Neuschel, On a conjecture on sparse binomial-type polynomials by Brown, Dilcher and Manna, *Anal. Appl. (Singap.)* **12**, (2014), no. 5, 511–522.
- [10] H. W. Gould, *Combinatorial Identities*, revised ed., Gould Publications, Morgantown, W. Va., 1972.
- [11] H. Graves and M. Ram Murty, The abc conjecture and non-Wieferich primes in arithmetic progressions, *J. Number Theory* **133** (2013), no. 6, 1809–1813.
- [12] E. Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, *Ann. of Math. Oxford Ser.* **39** (1938), 350–360.
- [13] C. Levesque, On m th order linear recurrences, *Fibonacci Quart.* **23** (1985), no. 4, 290–293.
- [14] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., Wiley, 1991.
- [15] F. W. J. Olver, *Asymptotics and Special Functions*. Academic Press, New York-London, 1974.
- [16] A. P. Prudnikov, Yu. A. Brychkov, and O. I. Marichev, *Integrals and Series. Vol. 1. Elementary Functions*. Translated from the Russian and with a preface by N. M. Queen. Gordon & Breach Science Publishers, New York, 1986. (Russian original: *Integraly i ryady. Elementarnye funktsii*. Nauka, Moscow, 1981.)
- [17] P. Ribenboim, *13 Lectures on Fermat’s Last Theorem*. Springer-Verlag, New York-Heidelberg, 1979.
- [18] T. J. Rivlin, *The Chebyshev polynomials*, 2nd ed., Wiley-Interscience, 1990.
- [19] M. Sved, Divisibility with visibility, *Math. Intelligencer* **10** (1988), no. 2, 56–64.
- [20] S. Wolfram, Geometry of binomial coefficients, *Amer. Math. Monthly* **91** (1984), no. 9, 566–571.