MATHEMATICS OF COMPUTATION
Volume 78, Number 265, January 2009, Pages 327–344
S 0025-5718(08)02138-8
Article electronically published on May 16, 2008

ON NEWMAN POLYNOMIALS WHICH DIVIDE NO LITTLEWOOD POLYNOMIAL

ARTŪRAS DUBICKAS AND JONAS JANKAUSKAS

ABSTRACT. Recall that a polynomial $P(x) \in \mathbb{Z}[x]$ with coefficients $0, 1$ and constant term 1 is called a Newman polynomial, whereas a polynomial with coefficients $-1, 1$ is called a Littlewood polynomial. Is there an algebraic number α which is a root of some Newman polynomial but is not a root of any Littlewood polynomial? In other words (but not equivalently), is there a Newman polynomial which divides no Littlewood polynomial? In this paper, for each Newman polynomial P of degree at most 8, we find a Littlewood polynomial divisible by P. Moreover, it is shown that every trinomial $1+ux^a+vx^b$, where $a < b$ are positive integers and $u, v \in \{-1, 1\}$, so, in particular, every Newman trinomial $1 + x^a + x^b$, divides some Littlewood polynomial. Nevertheless, we prove that there exist Newman polynomials which divide no Littlewood polynomial, e.g., $x^9+x^6+x^2+x+1$. This example settles the problem 006:07 posed by the first named author at the 2006 West Coast Number Theory conference. It also shows that the sets of roots of Newman polynomials $V_{\mathcal{N}}$, Littlewood polynomials $V_{\mathcal{L}}$ and $\{-1, 0, 1\}$ polynomials V are distinct in the sense that between them there are only trivial relations $V_{\mathcal{N}} \subset V$ and $V_{\mathcal{L}} \subset V$. Moreover, $V \neq V_{\mathcal{L}} \cup V_{\mathcal{N}}$. The proofs of several main results (after some preparation) are computational.

1. INTRODUCTION

A polynomial $P(x) \in \mathbb{Z}[x]$ with coefficients $0, 1$ and constant term 1 is called a *Newman polynomial.* Polynomials P with coefficients $-1, 1$ are called *Littlewood polynomials.* Let $V_{\mathcal{N}}$ and $V_{\mathcal{L}}$ be the sets of roots of Newman and Littlewood polynomials, respectively. Let also V be the set of roots of polynomials P with coefficients in the set $\{-1, 0, 1\}$ and $P(0) \neq 0$. Throughout this paper, we write $H(P)$ for the height of the polynomial P, namely, the maximum modulus of its coefficients. The polynomial $P^*(x) = x^{\deg P} P(1/x)$ is called the *reciprocal polynomial* of P.

The sets $V_{\mathcal{N}}, V_{\mathcal{L}}$ and V have been investigated by several authors, e.g., [8], [9], [15]. It is well known that the set $V_{\mathcal{N}}$ is contained in the intersection of the annulus $1/\phi < |z| < \phi$ with $\Re(z) < 3/2$, where $\phi = (1 + \sqrt{5})/2$. A more precise bounding contour was given in [15], where it was also shown that the closure of this set $\overline{V_{\mathcal{N}}}$ is path-connected. The points of $\overline{V_{\mathcal{L}}}$ inside the unit circle are related to the vanishing points of power series with ± 1 coefficients. Beaucoup, Borwein, Boyd and Pinner studied the extremal zeros of such power series and their multiplicity in [2] and [3].

Clearly, every $\alpha \in V$ is an algebraic integer. Moreover, it is a unit, and it is not difficult to show that all such α are located in the annulus $1/2 < |z| < 2$. The converse

Received by the editor December 10, 2007 and, in revised from, January 14, 2008.
2000 *Mathematics Subject Classification.* Primary 11R09, 11Y16, 12D05.
Key words and phrases. Newman polynomial, Littlewood polynomial.

of this statement does not hold; namely, there are many units α that lie with their conjugates in the annulus $1/2 < |z| < 2$ but $\alpha \notin V$. For instance, the minimal polynomial $P(x) = x^4 + x^3 + 2x^2 - x + 1$ of the number $\theta = (-1 + i\sqrt{3})(1 + \sqrt{5})/4$ does not divide any polynomial with coefficients $\{-1, 0, 1\}$ (see [9]).

It is evident that $V_{\mathcal{N}} \subseteq V$ and $V_{\mathcal{L}} \subseteq V$. Moreover, $V_{\mathcal{N}}$ is a proper subset of V, because $V_{\mathcal{N}}$ contains no positive numbers, whereas, say, $1 \in V_{\mathcal{L}} \subseteq V$. In order to show that $V_{\mathcal{L}}$ is a proper subset of V it would be sufficient to prove that there is an $\alpha \in V_{\mathcal{N}}$ which is not in $V_{\mathcal{L}}$. This would imply that $V_{\mathcal{N}}$ is not a subset of $V_{\mathcal{L}}$, so that all three sets $V_{\mathcal{N}}$, $V_{\mathcal{L}}$ and V are distinct and both sets $V_{\mathcal{N}} \setminus V_{\mathcal{L}}$ and $V_{\mathcal{L}} \setminus V_{\mathcal{N}}$ are not empty.

For this, it suffices to show that there is an irreducible polynomial $P(x) \in \mathbb{Z}[x], P(0) \neq 0$, which divides some Newman polynomial but does not divide any Littlewood polynomial. However, it seems that the problem of finding such examples is non-trivial, so the first named author posed this question as an open problem 006:07 at the 2006 West Coast Number Theory conference (see `http://web.newsguy.com/bartgoddard/problems2006.pdf`). Below, we shall use a numerical algorithm (see Theorem 4) to determine whether a given polynomial $P(x) \in \mathbb{Z}[x]$ with at least one zero outside the unit circle divides some Littlewood polynomial or not. In particular, using this test, we will show that the irreducible Newman polynomial $x^9 + x^6 + x^2 + x + 1$ of degree 9 does not divide any Littlewood polynomial. In addition, it will be shown that there are no such Newman polynomials of degree at most 8.

Divisibility properties of polynomials with coefficients $\{-1, 0, 1\}$ have been studied on many occasions, since they have many applications to various diophantine problems. For example, the order of vanishing of such polynomials at 1 was studied in [1], and the multiplicity of cyclotomic and non-cyclotomic factors of such polynomials was studied in [7] and [14]. The paper [14] was partly motivated by a hope to establish an absolute upper bound B for the multiplicity of a non-cyclotomic factor P in the factorization of polynomials with coefficients $\{-1, 0, 1\}$. Such a bound would lead to the proof of Lehmer's conjecture on Mahler's measure. If the bound B exists, then $B \geqslant 4$. Recently, several new results on Lehmer's conjecture have been obtained in [5] and [6]. In [5], Lehmer's conjecture was confirmed for polynomials with odd coefficients, so, in particular, for Littlewood polynomials. See also [10] for better numerical estimates.

The above-mentioned papers contain some interesting examples which are in some sense "special cases" of our problem. For instance, in [5], it was observed that if $P(x) \in \mathbb{Z}[x]$ is not a product of cyclotomic polynomials Φ_m modulo 2 and P divides some Littlewood polynomial L, then the quotient $Q = L/P$ has Mahler's measure greater than 1. In other words, Q cannot be a product of cyclotomic polynomials. Similarly, from the result on the Mahler measure of Littlewood polynomials given in [6], it follows that if $1 < M(P) < (1 + \sqrt{5})/2$ and P divides a non-reciprocal Littlewood polynomial L, then L/P must have at least one non-cyclotomic factor. Otherwise, we have $M(L) = M(P) < (1 + \sqrt{5})/2$, where L is a non-reciprocal Littlewood polynomial, which is impossible by [6]. Mossinghoff [14] found Littlewood polynomials divisible by ℓ and $\{-1, 0, 1\}$ polynomials divisible by ℓ^3, where $\ell(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$ is Lehmer's polynomial.

This paper is organized as follows. The main results are given in Sections 2 and 3. In Section 4 we give an auxiliary result for polynomials over the finite field $\mathbb{F}_2$

with two elements. Section 5 contains the proofs of most of our theoretical results. We then develop some algorithms used in our computations (see Section 6). The details of the computations are provided in Section 7.

2. Main results

Note that the sets $V_{\mathcal{N}}$ and $V_{\mathcal{L}}$ have infinitely many common elements. For example, the root of unity $\zeta = e^{2\pi i/u}$, where $u \geqslant 2$, is a root of $x^{u-1} + \cdots + x + 1$. This is a Newman polynomial and a Littlewood polynomial. So every root of unity except for 1 belongs to $V_{\mathcal{N}} \cap V_{\mathcal{L}}$. Our next result implies that the structure of the set $V_{\mathcal{N}} \cap V_{\mathcal{L}}$ is non-trivial: every Newman trinomial divides some Littlewood polynomial. (A trinomial is a polynomial with three non-zero coefficients.) In fact, our statement is more general:

Theorem 1. *For each trinomial P with $\{-1, 0, 1\}$ coefficients and $P(0) \neq 0$, there exists a polynomial Q with coefficients $\{-1, 0, 1\}$ such that the product PQ is a Littlewood polynomial.*

Similar results for certain special quadrinomials will be given in Section 3. Our computations show that the roots of Newman polynomials of degree at most 8 also belong to $V_{\mathcal{N}} \cap V_{\mathcal{L}}$:

Theorem 2. *Every Newman polynomial of degree at most* 8 *divides some Littlewood polynomial.*

We also have the following:

Theorem 3. *Every Newman polynomial divides some integer polynomial with odd coefficients.*

The main purpose of this paper is to give some examples of algebraic numbers $\alpha \in V_{\mathcal{N}} \setminus V_{\mathcal{L}}$. We found several irreducible Newman polynomials not dividing any Littlewood polynomial. Some of them are given in Table 1. Polynomials given in rows $2, 4, 6, 8$ are reciprocal to polynomials given in rows $1, 3, 5, 7$, respectively.

Table 1. Some Newman polynomials of degree 9 not dividing any Littlewood polynomial.

	Polynomial $P(x)$
1.	$1 + x^4 + x^6 + x^7 + x^9$
2.	$1 + x^2 + x^3 + x^5 + x^9$
3.	$1 + x^3 + x^7 + x^8 + x^9$
4.	$1 + x + x^2 + x^6 + x^9$
5.	$1 + x + x^2 + x^4 + x^6 + x^9$
6.	$1 + x^3 + x^5 + x^7 + x^8 + x^9$
7.	$1 + x + x^4 + x^5 + x^6 + x^7 + x^9$
8.	$1 + x^2 + x^3 + x^4 + x^5 + x^8 + x^9$

All these polynomials were found using numerical tests based on the following statement:

Theorem 4. *Let $P(x) \in \mathbb{Z}[x]$ be a monic polynomial whose roots of modulus strictly greater than 1 are labelled $\alpha_1, \dots, \alpha_k$, where $k \geqslant 1$. Suppose that there exist a positive integer N and a real number $\delta \geqslant 0$ with the property that, for each of the 2^N vectors $\mathbf{b} = (b_1, \dots, b_N)$, where $b_1, \dots, b_N \in \{-1, 1\}$, there are two positive integers $n = n(\mathbf{b}) \leqslant N$ and $i = i(\mathbf{b}) \leqslant k$ such that*

$$(|\alpha_i| - 1)|\alpha_i^n + b_1\alpha_i^{n-1} + \cdots + b_n| \geqslant 1 + \delta.$$

Then P does not divide any Littlewood polynomial.

At first glance, the statement of the theorem may look somewhat strange, because one obtains the weakest inequality when $\delta = 0$. However, on several occasions below, we shall use the statement of the theorem with strictly positive δ. This is why we prefer to state the theorem in the above form.

Using the examples from Table 1 it is possible to construct infinitely many irreducible Newman polynomials not dividing any Littlewood polynomial. This shows that the set $V_{\mathcal{N}} \setminus V_{\mathcal{L}}$ is infinite. We will prove the following statement:

Theorem 5. *There exist infinitely many primitive irreducible Newman polynomials which do not divide any Littlewood polynomial.*

In this context, a polynomial $P(x) \in \mathbb{Z}[x]$ is called *primitive* if P cannot be written as $P(x) = G(x^k)$ with some integer $k \geqslant 2$ and some $G(x) \in \mathbb{Z}[x]$.

Take $P(x) = 1 + x^4 + x^6 + x^7 + x^9$. Since $P(x)$ does not divide any Littlewood polynomial, the polynomial $P(-x) = 1 + x^4 + x^6 - x^7 - x^9$ also does not divide any Littlewood polynomial. The polynomial $1 + x^4 + x^6 - x^7 - x^9$ has a positive root α, so it does not divide any Newman polynomial. This shows that $\alpha \in V$, but $\alpha \notin V_{\mathcal{L}} \cup V_{\mathcal{N}}$, so $V_{\mathcal{L}} \cup V_{\mathcal{N}}$ is strictly contained in V.

3. Other results

For each complex root α of the polynomial $P(x) \in \mathbb{R}[x]$, the complex conjugate $\overline{\alpha}$ is also a root of P. If P is a Newman (resp. Littlewood) polynomial, then its reciprocal P^* is also a Newman (resp. Littlewood) polynomial. Thus each of the sets $V_{\mathcal{L}}$, $V_{\mathcal{N}}$, $V_{\mathcal{N}} \cap V_{\mathcal{L}}$, $V_{\mathcal{N}} \setminus V_{\mathcal{L}}$, $V_{\mathcal{L}} \setminus V_{\mathcal{N}}$ maps into itself by the complex conjugation $z \mapsto \overline{z}$ and the inversion $z \mapsto 1/z$. In the next statement we consider the map $z \mapsto z^{1/k}$.

Lemma 6. *Let k be a positive integer. Then $P(x) \in \mathbb{Z}[x]$ divides some Littlewood polynomial if and only if $P(x^k)$ divides some Littlewood polynomial.*

By the same method as that in the proof of Theorem 1, one can show that certain quadrinomials also divide polynomials with small odd coefficients and sometimes even Littlewood polynomials.

Theorem 7. *Let P be a quadrinomial with coefficients in $\{-1, 0, 1\}$ such that $P(0) = 1$. Then there is a Newman polynomial Q such that all coefficients of the product PQ belong to the set $\{-3, -1, 1, 3\}$ and, moreover, to the set $\{1, 3\}$ if P itself is a Newman polynomial. Furthermore, if $a < b < c$ are positive integers and P is of one of the forms*

i) $1 + x^a - x^b - x^c$,

ii) $1 - x^a - x^b - x^c$, *where exactly one of the numbers a, b, c is odd,*

iii) $1 + x^a + x^b + x^c$, *where exactly one of the numbers a, b, c is even,*

iv) $1 + x^a + x^b - x^c$, *where all the exponents* a, b, c *are odd or, alternatively,* c *is even and precisely one of the numbers* a, b *is odd,*
then the quadrinomial P *divides some Littlewood polynomial* L*, and* L/P *is a polynomial with coefficients in* $\{-1, 0, 1\}$.

It would be of interest to find out whether this result can be extended to the full analogue of Theorem 1, namely, to all quadrinomials of height 1. If so, then this would imply that our example $x^9 + x^6 + x^2 + x + 1$ is minimal not only in terms of its degree (nine), but also in terms of the number of its non-zero coefficients (five).

Suppose that $P(x) \in \mathbb{Z}[x]$ divides some Littlewood polynomial L. One may ask which values can its degree $\deg L$ take. The answer is given in terms of factorization of L modulo 2.

Lemma 8. *Suppose that a polynomial* $P(x) \in \mathbb{Z}[x]$ *divides a Littlewood polynomial* L*. Let* $\widetilde{P}(x) \in \mathbb{F}_2[x]$ *be the reduction of* P *modulo* 2*. Then* $\deg L + 1$ *is a multiple of* $\deg_2 \widetilde{P}$*. (This quantity will be defined in Section* 4*.)*

In fact, the value of $\deg L$ grows exponentially with the degree of P. If, for instance, a monic polynomial P of degree 10 is a prime divisor of the cyclotomic polynomial Φ_{1023} in $\mathbb{F}_2[x]$, then $\deg_2 \widetilde{P} = 2^{10} - 1$. The degree of any Littlewood polynomial L divisible by P must be of the form $1023k - 1$, where $k \in \mathbb{N}$, so it is greater than or equal to 1022. One has thus to consider 2^{1022} different possibilities in trying to find a polynomial L of degree 1022 divisible by P. This simple example demonstrates the computational complexity of the problem.

One possible strategy is to search for a factor $Q(x) \in \mathbb{Z}[x]$ of small height, say, $H(Q) \leqslant 2$ such that the product PQ is a Littlewood polynomial. The following lemma implies that one can restrict oneself with only finitely many choices for Q. This will be used in Algorithm 14 below.

Lemma 9. *Suppose that a polynomial* $P(x) \in \mathbb{Z}[x]$ *of degree* $d \geqslant 1$ *divides a Littlewood polynomial* L*. Let* $h = H(L/P)$*. Then there exists a polynomial* $Q(x) = \sum_{j=0}^{n} b_j x^j \in \mathbb{Z}[x]$ *of degree*

$$n \leqslant (2h+1)^d + d - 2$$

and height $H(Q) \leqslant h$ *such that the product* PQ *is also a Littlewood polynomial. Moreover, the vector of coefficients* $(b_0, b_1, b_2, \ldots, b_{n-1}, b_n)$ *of* Q *contains no two identical blocks* $b_j, b_{j+1}, \ldots, b_{j+d-1}$ *of length* d*.*

Suppose that a Newman polynomial P does not divide any Littlewood polynomial. We shall construct infinitely many examples of such polynomials by perturbing the roots of P.

Theorem 10. *Suppose that* P *satisfies the conditions of Theorem* 4 *with some* $\delta > 0$*. Then there exists an* $\varepsilon > 0$ *which depends on* P *and* δ *only with the following property: if the polynomial* $P_1(x) \in \mathbb{Z}[x]$ *has some roots* $\beta_1, \ldots, \beta_k$*, each of modulus strictly greater than* 1 *such that* $|\alpha_j - \beta_j| < \varepsilon$ *for* $j = 1, \ldots, k$*, where* $\alpha_1, \ldots, \alpha_k$ *are the roots of* P *of modulus strictly greater than* 1*, then* P_1 *does not divide any Littlewood polynomial.*

Such approximations may be obtained from the sequence of polynomials of the form $x^n P(x) + R(x)$, where R is a Newman polynomial relatively prime to P and $n > \deg R$.

Theorem 11. *Suppose that the polynomial P satisfies the conditions of Theorem 4 with some $\delta > 0$. Then, for any $R(x) \in \mathbb{Z}[x]$, there exists a positive integer n_0 such that, for each $n \geqslant n_0$, the polynomial $x^n P(x) + R(x)$ does not divide any Littlewood polynomial.*

All polynomials given in Table 1 have at least two zeros outside the unit circle. It would be of interest to find out whether there exists an irreducible polynomial $P(x) \in \mathbb{Z}[x]$ with exactly one root outside the unit circle such that P divides some Newman polynomial but no Littlewood polynomial. In other words, does there exist a Pisot or a Salem number α such that $-\alpha$ is a root of some Newman polynomial but not a root of any Littlewod polynomial?

4. Auxiliary facts about polynomials from $\mathbb{F}_2[x]$

Every polynomial $f(x) \in \mathbb{F}_2[x]$ with $f(0) \neq 0$ modulo 2 may be written uniquely as a product

$$f(x) = (x+1)^m \prod_{j=1}^{r} \phi_j(x)^{m_j},$$

where $m \geqslant 0$ and $\phi_j(x) \in \mathbb{F}_2[x]$ are irreducible polynomials of degree greater than or equal to 2 and multiplicity $m_j \geqslant 1, j = 1, \dots, r$. The product is empty if $r = 0$. Every polynomial ϕ_j divides a unique cyclotomic polynomial Φ_{e_j} of odd index e_j. Let s be the least positive integer satisfying $2^s \geqslant \max\{m+1, m_1, \dots, m_r\}$. Define the number

$$\deg_2 f = 2^s \mathrm{lcm}(e_1, \dots, e_r).$$

Lemma 12. *If a polynomial $f(x) \in \mathbb{F}_2[x]$ divides the polynomial $h(x) = x^n + \cdots + x + 1$, then $n+1$ is divisible by the number $\deg_2 f$. Conversely, if $\deg_2 f$ divides $n+1$, then there exists a polynomial $g(x) \in \mathbb{F}_2[x]$ such that $f(x)g(x) = h(x)$.*

Proof. Write $h(x) = (x^{n+1}+1)/(x+1)$ in $\mathbb{F}_2[x]$. Let $n+1 = 2^l k$, where k is odd and $l \geqslant 0$. Then, in $\mathbb{F}_2[x]$, we have

$$h(x) = (x^k+1)^{2^l}/(x+1).$$

Let α be a root of the irreducible factor $\phi_j(x)$ of f. Note that the order of α in the multiplicative group of the field $\mathbb{F}_{2^{\deg \phi_j}}$ is e_j, so e_j divides k for every $j = 1, \dots, r$. The polynomial $x^k + 1$ has no multiple roots. Therefore the power 2^l is greater than or equal to the maximum of the numbers $m+1, m_1, \dots, m_r$. Hence $n+1$ must be divisible by 2^s and the least common multiple of the integers $e_1, \dots, e_r$. On the other hand, if we take $n = n_1 \deg_2 f - 1$, for some positive integer n_1, then $h(x)$ vanishes at all roots of $f(x)$ with required multiplicities. Thus $h(x)$ is divisible by $f(x)$, and $g(x) \in \mathbb{F}_2[x]$ is the quotient $h(x)/f(x)$. □

We shall give an example of the computation of $\deg_2 \widetilde{P}$. Consider the polynomial $P(x) = 1 + x^2 + x^5 + x^9 \in \mathbb{Z}[x]$. Reducing modulo 2, the polynomial splits over $\mathbb{F}_2$ into the following irreducible factors:

$$\widetilde{P}(x) = (x+1)^2(x^2+x+1)(x^5+x^4+x^3+x+1).$$

In this example, we have $m = 2$, $r = 2$, $m_1 = m_2 = 1$, $\phi_1(x) = x^2 + x + 1$ and $\phi_2(x) = x^5 + x^4 + x^3 + x + 1$. The polynomial ϕ_1 is the cyclotomic polynomial Φ_3. The polynomial ϕ_2 divides the cyclotomic polynomial Φ_{31}. Hence $e_1 = 3, e_2 = 2^5 - 1 = 31$ and $s = 2$. Thus $\deg_2 \widetilde{P} = 2^2 \mathrm{lcm}(3, 31) = 372$. Therefore, by Lemma 8,

any Littlewood polynomial L divisible by $1 + x^2 + x^5 + x^9$ must be of degree $\deg L = 372k - 1$, where $k = 1, 2, \ldots$.

Two of our statements are very simple corollaries of Lemma 12.

Proof of Lemma 8. The reduction of any Littlewood polynomial L modulo 2 is $\widetilde{L}(x) = x^{\deg L} + \cdots + x + 1$. Since $\widetilde{L}$ is divisible by $\widetilde{P}$, the result follows from Lemma 12. □

Proof of Theorem 3. Let P be a Newman polynomial of degree b. By Lemma 12, there exists a polynomial $\widetilde{Q}(x) = \sum_{j=0}^{n-b} \widetilde{q}_j x^j \in \mathbb{F}_2[x]$, satisfying $\widetilde{P}(x)\widetilde{Q}(x) = x^n + \cdots + x + 1$ in $\mathbb{F}_2[x]$. Set $Q(x) = \widetilde{Q}(x)$, where 0 and 1 are understood as positive integers rather than elements of $\mathbb{F}_2$. It follows that PQ has all odd coefficients. □

5. Proofs

Proof of Lemma 6. The proof of the lemma is similar to the proof of Proposition (iv) in [16]. If the polynomial $P(x) \in \mathbb{Z}[x]$ divides some Littlewood polynomial L, and Q is a Littlewood polynomial of degree $k-1$, then the product $L(x^k)Q(x)$ is a Littlewood polynomial divisible by $P(x^k)$. One can take, for instance, $Q(x) = 1 + x + \cdots + x^{k-1}$.

For the converse, suppose that $P(x^k)$ divides a Littlewood polynomial L. Rewrite $L(x)$ putting the powers x^i, x^j satisfying $i \equiv j \pmod k$ together:

$$L(x) = L_0(x^k) + xL_1(x^k) + \cdots + x^{k-1}L_{k-1}(x^k).$$

Note that each $L_j(x), j = 0, \ldots, k-1$, is either a Littlewood polynomial or zero. For each $0 \leqslant j \leqslant k-1$, there exist $Q_j, R_j \in \mathbb{Z}[x]$, such that $L_j = PQ_j + R_j$, where $\deg R_j < \deg P$. Since $P(x^k) | L(x)$, it follows that $P(x^k)$ divides $R(x) = R_0(x^k) + xR_1(x^k) + \cdots + x^{k-1}R_{k-1}(x^k)$. The degree of R is $\leqslant k(\deg P - 1) + k - 1$, so $\deg R < k \deg P$. Hence all the polynomials R_j must be zeros identically. This implies that all non-zero polynomials L_j are Littlewood polynomials divisible by P. (There must be at least one non-zero L_j, because L is non-zero.) □

Proof of Lemma 9. Let $P(x) = \sum_{j=0}^{d} a_j x^j$. Among all polynomials Q of height $H(Q) \leqslant h$ such that the product PQ is a Littlewood polynomial, there is a polynomial of minimal degree, say, $Q(x) = \sum_{j=0}^{n} b_j x^j$. Write $P(x)Q(x) = L(x)$, where all coefficients of L are ± 1.

We begin from the second part of the statement. Suppose that the vector of coefficients of the polynomial Q, $(b_0, b_1, \ldots, b_{n-1}, b_n)$, contains two identical blocks $b_r, b_{r+1}, \ldots, b_{r+d-1}$ and $b_s, b_{s+1}, \ldots, b_{s+d-1}$ of length d, where $r < s$. After removing $s - r$ coefficients $b_r, b_{r+1}, \ldots, b_{s-1}$ from this vector, we obtain the vector $(b_0, \ldots, b_{r-1}, b_s, \ldots, b_n)$. Define the polynomial $T(x) = \sum_{j=0}^{n-(s-r)} t_j x^j$ by

$$t_j = \begin{cases} b_j & \text{if } j < r, \\ b_{j+(s-r)} & \text{if } j \geqslant r. \end{cases}$$

Since $b_{r+j} = b_{s+j}$ for $j = 0, \ldots, d-1$, the first $r+d$ coefficients of T and Q coincide, $t_j = b_j, 0 \leqslant j \leqslant r+d-1$. Hence $Q(x) \equiv T(x) \pmod{x^{r+d}}$. Similarly, the last $n - s + 1$ coefficients of Q and T are equal. So, for their reciprocal polynomials, we have $Q^*(x) \equiv T^*(x) \pmod{x^{n-s+1}}$. It follows that $L(x) = P(x)Q(x) \equiv P(x)T(x) \pmod{x^{r+d}}$ and $L^*(x) = P^*(x)Q^*(x) \equiv P^*(x)T^*(x) \pmod{x^{n-s+1}}$. Hence the first $r + d$ and the last $n - s + 1$ coefficients of L and PT are the same. But PT

has precisely $n-s+r+d+1$ coefficients, so each of those coefficients must be ± 1. Hence PT is a Littlewood polynomial. It follows that $\deg T < \deg Q$, which is a contradiction with the minimality of $\deg Q$.

Now, we turn to the first part of the statement. Since the right-hand side of the inequality, $(2h+1)^d+d-2$, is greater than d for every $d \geqslant 1$, we may assume $n > d$. The number of blocks of length d in the vector of coefficients of Q is $n-d+2$. On the other hand, this number must be less than or equal to the total number of different possible blocks, otherwise two of them will be identical, which is already proved to be impossible. By choosing any element of the block from the set of $2h+1$ integers $\{-h, \dots, 0, \dots, h\}$, one obtains exactly $(2h+1)^d$ different blocks. This implies that $n-d+2 \leqslant (2h+1)^d$, as claimed. □

Proof of Theorem 1. Without loss of generality, we may assume that the constant coefficient of P is 1 (otherwise multiply P by -1). The trinomial P has one of the four forms

$$\text{(i) } 1-x^a+x^b, \qquad \text{(ii) } 1+x^a-x^b, \qquad \text{(iii) } 1-x^a-x^b, \qquad \text{(iv) } 1+x^a+x^b,$$

where $a < b$ are two positive integers.

Write $P(x) = 1+\varepsilon_a x^a + \varepsilon_b x^b$, where the coefficients $\varepsilon_a, \varepsilon_b \in \{-1, 1\}$. We first consider the cases (i)–(iii), when at least one of the coefficients $\varepsilon_a, \varepsilon_b$ is negative. The reduction of the polynomial P mod 2 is $\widetilde{P}(x) = 1+x^a+x^b$. By Lemma 12, there exists a polynomial $\widetilde{Q}(x) = \sum_{j=0}^{n-b} \widetilde{q}_j x^j \in \mathbb{F}_2[x]$, satisfying $\widetilde{P}(x)\widetilde{Q}(x) = x^n+\cdots+x+1$ in $\mathbb{F}_2[x]$ provided that $n+1$ is divisible by $\deg_2 \widetilde{P}$. Take the number $n = \deg_2 \widetilde{P} - 1$ to obtain the polynomial of the least possible degree. Define the polynomial $Q(x) = \sum_{j=0}^{n-b} q_j x^j \in \mathbb{Z}[x]$ by

$$q_j = \begin{cases} 0 & \text{if } \widetilde{q}_j = 0, \\ 1 & \text{if } \widetilde{q}_j = 1, \end{cases}$$

so that $\widetilde{Q}(x)$ is a reduction mod 2 of the polynomial $Q(x)$.

Writing $P(x)Q(x) = (1+\varepsilon_a x^a+\varepsilon_b x^b)\sum_{j=0}^{n-b} q_j x^j = L(x) = \sum_{j=0}^{n} l_j x^j$, we see that the coefficients $l_j \in \mathbb{Z}$, $j = 0, \dots, n$, are given by the formulae

$$l_j = \begin{cases} q_j & \text{for } 0 \leqslant j < a, \\ q_j + \varepsilon_a q_{j-a} & \text{for } a \leqslant j < b, \\ q_j + \varepsilon_a q_{j-a} + \varepsilon_b q_{j-b} & \text{for } b \leqslant j \leqslant n-b, \\ \varepsilon_a q_{j-a} + \varepsilon_b q_{j-b} & \text{for } n-b < j \leqslant n-b+a, \\ \varepsilon_b q_{j-b} & \text{for } n-b+a < j \leqslant n. \end{cases}$$

The third line is excluded in case $n < 2b$. Since $L(x) \equiv \widetilde{P}(x)\widetilde{Q}(x) \equiv x^n+\cdots+x+1 \pmod 2$, all the coefficients l_j are odd. There are at most three non-zero terms in the formulae for l_j, so $l_j \in \{-3, -1, 1, 3\}$. Note that $l_j = \pm 3$ may appear only in the third line when all three terms q_j, $\varepsilon_a q_{j-a}$ and $\varepsilon_b q_{j-b}$ are 1 or all three -1. This is impossible, because $q_j, q_{j-a}, q_{j-b} \in \{0, 1\}$ and at least one of $\varepsilon_a, \varepsilon_b$ is negative. Thus PQ is a Littlewood polynomial, where Q is a Newman polynomial.

Now consider the remaining case (iv), where $P(x) = 1+x^a+x^b$. Write $k = \gcd(a, b)$. Then $a = ka_1, b = kb_1$. At least one of the integers a_1, b_1 is odd. Note that $P(x) = P_1(x^k)$, where $P_1(x) = 1+x^{a_1}+x^{b_1}$. The polynomial $P_1(-x)$ has one of the forms (i), (ii) or (iii). It follows from the earlier part of the proof that

there exists a polynomial $Q_1(x)$ with coefficients 0 or 1, such that $P_1(-x)Q_1(x)$ is a Littlewood polynomial. Thus $P_1(x)Q_1(-x)$ is a Littlewood polynomial, so that

$$P_1(x^k)Q_1(-x^k)(1+x+\cdots+x^{k-1}) = P(x)Q_1(-x^k)(1+x+\cdots+x^{k-1})$$

is also a Littlewood polynomial. Clearly, in this case, the factor $Q_1(-x^k)(1+\cdots+x^{k-1})$ is a polynomial with $\{-1,0,1\}$ coefficients. □

Proof of Theorem 7. The proof is very similar to the proof of Theorem 1 for trinomials; thus we will omit the details. For a given quadrinomial P, there exists a $Q(x) \in \mathbb{Z}[x]$ with $0,1$ coefficients, such that $P(x)Q(x) \equiv x^n + \cdots + x + 1 \pmod 2$. In the formulae for the coefficients l_j of the polynomial $L = PQ$ there are at most four non-zero terms and all of the l_j must be odd, by the choice of Q. Hence $l_j \in \{-3,-1,1,3\}$. Moreover, $l_j \in \{1,3\}$ if all the coefficients of P are non-negative. This proves the first part of the theorem.

Suppose that exactly two coefficients of the quadrinomial P are 1 and the other two are -1. (For any quadrinomial P listed in (i)–(iv) either $P(x)$ or $P(-x)$ has this property.) The number $l_j = \pm 3$ may appear only in equations with three or four non-zero terms (see the formulae for the coefficients l_j). This is impossible, because two of all non-zero terms have opposite signs. Therefore, for any polynomial P as in (i)–(iv), $P(x)Q(x)$ or $P(x)Q(-x)$ must be a Littlewood polynomial. □

Proof of Theorem 4. Suppose that there is a Littlewood polynomial L which is divisible by P. Since, for any positive integer m, $L(x)(1+x^{\deg L+1}+\cdots+x^{m(\deg L+1)})$ is a Littlewood polynomial too, we can assume without loss of generality that $\deg L \geqslant N$. Write $L(x) = x^M + b_1x^{M-1} + \cdots + b_M$, where $b_j \in \{-1,1\}$ and $M \geqslant N$. By the assumption of the theorem, there exist positive integers $n \leqslant N$ and $i \leqslant k$ such that $(|\alpha_i|-1)|\alpha_i^n + b_1\alpha_i^{n-1} + \cdots + b_n| \geqslant 1+\delta$.

On the other hand, using the fact that L is divisible by P, we have $L(\alpha_i) = 0$. Hence $\alpha_i^n + b_1\alpha_i^{n-1} + \cdots + b_n = -(b_{n+1}\alpha_i^{-1} + \cdots + b_M\alpha_i^{n-M})$. Thus

$$\begin{aligned}|\alpha_i^n + b_1\alpha_i^{n-1} + \cdots + b_n| &= |b_{n+1}\alpha_i^{-1} + \cdots + b_M\alpha_i^{n-M}| \\ &\leqslant \sum_{j=1}^{n-M} |\alpha_i|^{-j} < \sum_{j=1}^{\infty} |\alpha_i|^{-j} = 1/(|\alpha_i|-1),\end{aligned}$$

giving $(|\alpha_i|-1)|\alpha_i^n + b_1\alpha_i^{n-1} + \cdots + b_n| < 1$, a contradiction. □

Proof of Theorem 10. By Theorem 4, for each of the 2^N vectors $\mathbf{b} = (b_1,\dots,b_N) \in \{-1,1\}^N$, there exist positive integers $n = n(\mathbf{b}) \leqslant N$ and $i = i(\mathbf{b}) \leqslant k$ such that the function

$$f_{\mathbf{b}}(z) = (|z|-1)|z^n + b_1z^{n-1} + \cdots + b_n|$$

is greater than $1+\delta$ at α_i, namely, $f_{\mathbf{b}}(\alpha_i) \geqslant 1+\delta$. By continuity of $f_{\mathbf{b}}(z)$, the inequality $f_{\mathbf{b}}(z) > 1$ holds for all z in the circle $|z-\alpha_i| < \varepsilon_{\mathbf{b}}$. Here, $\varepsilon_{\mathbf{b}} > 0$ depends on $\mathbf{b}$, α_i and δ only. Set

$$\varepsilon = \min_{\mathbf{b}\in\{-1,1\}^N} \varepsilon_{\mathbf{b}}.$$

Now if $|\alpha_i - \beta_i| < \varepsilon$, then $f_{\mathbf{b}}(\beta_i) > 1$. Hence the roots $\beta_j, |\beta_j| > 1, j = 1,\dots,k$, of P_1 satisfy the same conditions of Theorem 4 as the roots of P with the same numbers $i = i(\mathbf{b})$, $n = n(\mathbf{b})$ and the number $\delta = 0$. □

Proof of Theorem 11. There exists a real number $\rho > 1$ such that all the roots $\alpha_j, j = 1, \dots, k$, of the polynomial P outside the unit circle are of moduli strictly greater than ρ, i.e., $|\alpha_j| > \rho$. For any $\varepsilon > 0$, choose a sufficiently small positive number $r < \varepsilon$ such that, firstly, all the points of the set $S = \bigcup_{j=1}^{k} \{z : |z - \alpha_j| = r\}$ are of modulus $|z| > \rho$ and, secondly, the polynomial P does not vanish for any $z \in S$. Let $m = \inf_{z \in S} |P(z)|$, $M = \sup_{z \in S} |R(z)|$. Since S is a compact set, by the continuity of P, we have $m > 0$. Hence there exists a positive integer n_0 such that, for every $n > n_0$ and each $z \in S$, the inequality $|z^n P(z)| > \rho^n m > M \geqslant |R(z)|$ is satisfied. By Rouché's theorem, the polynomial $z^n P(z) + R(z)$ has the same number of zeros inside each circle $|z - \alpha_j| = r$ as the polynomial P. Now, choose $\varepsilon = \varepsilon(P, \delta)$ given by Theorem 10. For $n > n_0$, the polynomial $z^n P(z) + R(z)$ has k roots, say, $\beta_{n,1}, \dots, \beta_{n,k}$, satisfying $|\beta_{n,j}| > 1$ and $|\alpha_j - \beta_{n,j}| < \varepsilon$. By Theorem 10, $z^n P(z) + R(z)$ does not divide any Littlewood polynomial. □

Proof of Theorem 5. We first show that there exist infinitely many irreducible Newman polynomials which do not divide any Littlewood polynomial. Take some irreducible non-reciprocal polynomial P from Table 1. It does not divide any Littlewood polynomial. By Lemma 6, for any positive integer k, $P(x^k)$ also does not divide any Littlewood polynomial. Theorem 3 in the paper of Filaseta [11] asserts that the Newman polynomial $P(x^k)$ is irreducible, because $P(x)$ is irreducible and non-reciprocal.

In order to prove the stronger version asserting that there are infinitely many such primitive irreducible polynomials, let us consider the polynomial $P(x) = 1 + x^4 + x^6 + x^7 + x^9$ from Table 1. Numerical computations show that it satisfies the conditions of Theorem 11 with $\delta = 2$ (see Table 6 below). By Theorem 11, there exists an integer n_0 such that for every $n > n_0$ the polynomial $x^n P(x) + 1$ is a Newman polynomial not dividing any Littlewood polynomial.

We shall prove the existence of irreducible polynomials among $x^n P(x) + 1$ using standard techniques from the paper [12]. In particular, the direct consequence of Theorem 2 in [12] is that if $P_n(x) = x^n P(x) + 1$, where $n > 2 \deg P = 18$, is reducible, then it must have a common non-constant reciprocal factor with the reciprocal polynomial $P_n^*(x)$. If $\alpha \neq 0$ is a root of this common factor, then $\alpha^n P(\alpha) = -1$ and $\alpha^{-n} P(1/\alpha) = -1$. Multiplying the corresponding sides of these equalities, we obtain $P(\alpha)P(1/\alpha) - 1 = 0$. This implies that the minimal polynomial of α over $\mathbb{Q}$ must divide the polynomial $G(x) = x^9 P(x) P(1/x) - x^9$. The factorization of G in $\mathbb{Z}[x]$ is

$$(x+1)^2(x^2+1)(x^2-x+1)(x^{12}-x^{11}+x^{10}-x^9+2x^8-2x^7+3x^6-2x^5+2x^4-x^3+x^2-x+1).$$

If an irreducible polynomial divides two polynomials $x^m P(x)+1$ and $x^n P(x)+1$ for some positive integers $n > m$, then it must divide their difference $x^m P(x)(x^{n-m} - 1)$. Hence the above non-cyclotomic factor of degree 12 divides at most one polynomial of the sequence $P_n(x) = x^n P(x) + 1$, $n = 1, 2, \dots$. The roots of the cyclotomic factors are $\alpha = -1, \pm i, e^{\pm \pi i/3}$. It is easy to check that $P_n(-1) = (-1)^n + 1$, $P_n(\pm i) = (\pm i)^n + 1$, $P(e^{\pm \pi i/3}) = e^{\pm \pi n i/3} + 1$. For any positive integer $n = 4k$, we have $P_{4k}(\alpha) \neq 0$. Therefore $P_{4k}(x)$ is not divisible by any of the cyclotomic factors of $G(x)$. Hence the subsequence $x^{4k} P(x) + 1$, $k = 1, 2, \dots$, contains infinitely many irreducible polynomials. □

6. Algorithms and implementation

6.1. **Polynomials not dividing any Littlewood polynomial.** Using Theorem 4 one can test whether a given polynomial $P(x) \in \mathbb{Z}[x]$ divides some Littlewood polynomial. Of course, there is no guarantee at all that this will give the required result if such an N exists, but is very large, or if such an N does not exist. In both cases, it can still happen that P does not divide any Littlewood polynomial.

In practice, we choose a positive integer N (typical values are $N = 50, 70, 100$), a real number $\delta \geqslant 0$ ($\delta = 0, 1, 2$) and check if there exists at least one vector $\mathbf{b} \in \{-1, 1\}^N$ of length N for which the left-hand side of the inequality of Theorem 4, namely, the quantity $(|\alpha_j| - 1)|\alpha_j^n + b_1\alpha_j^{n-1} + \cdots + b_n|$ is less than $1 + \delta$ for every n, where $1 \leqslant n \leqslant N$, and each root α_j, $j = 1, \ldots, k$, of P is of modulus strictly greater than 1. This is accomplished by the recursive search through the binary tree of all vectors $\mathbf{b}$. If the program reports that the reached depth is less than $N + 1$, then such a vector $\mathbf{b}$ does not exist. The conditions of Theorem 4 are satisfied, so that P does not divide any Littlewood polynomial. A similar method was already used in computer graphics (see [15]).

Algorithm 13. *Numerical test checking whether $P(x) \in \mathbb{Z}[x]$ can divide some Littlewood polynomial.*

Input:	*An integer $N \geqslant 1$, a real number $\delta \geqslant 0$,*
	the set S of roots α of P lying in $\lvert z\rvert > 1$.
Output:	*Integer depth – reached depth. Initially it is* 0.
Other variables:	*vector* $\boldsymbol{b}$.
Method:	*Check the conditions of Theorem* 4.

Step 0: Set $n = 0$.

Step 1: Given n.

if $n >$ depth then set depth $= n$.

if depth $\leqslant N$ then do

for each $\alpha \in S$ test whether
$(|\alpha| - 1)|\alpha^n + b_1\alpha^{n-1} + \cdots + b_n| < 1 + \delta$.

if all inequalities hold then do
i) set $b_{n+1} = 1$ and invoke Step 1 on $n + 1$.
ii) set $b_{n+1} = -1$ and invoke Step 1 on $n + 1$.
end if.

end if.

We used the following method in order to reduce the amount of numerical calculations. Let $T_n(\alpha) = \alpha^n + b_1\alpha^{n-1} + \cdots + b_n$. The value $T_{n+1}(\alpha)$ can be found by the formulae $T_{n+1}(\alpha) = \alpha T_n(\alpha) + b_{n+1}$. Moreover, if $\alpha, \overline{\alpha}$ are two complex conjugate roots of P, then it suffices to evaluate the inequality only at one of them, say, at α with $\Im(\alpha) \geqslant 0$.

The most critical part of this program is the numerical evaluation of the inequality of Theorem 4. Any rounding error may cause an incorrect termination of the recursion. To overcome this difficulty we coded the algorithm in C++ using the C–XSC library for validated real and complex bounding interval arithmetics (see [13]). The details concerning the initial approximation and the computation of enclosing rectangles of roots α are given in Section 7. We store the enclosures of the numbers $\alpha, T_n(\alpha)$ using C–XSC data types `cinterval` or `l_cinterval`. In order to evaluate the left-hand side of the inequality, we compute its interval enclosure (data types `interval` and `l_interval`). Then the lower bound of this enclosure, given by `interval.Inf()`, is compared to the right-hand side of our inequality. It must be strictly smaller than $1+\delta$ for the inequality to hold. In addition, setting the variable δ to be a quite large non-zero number, say $\delta = 2$, helps to prevent any accidental rounding errors.

6.2. **Littlewood polynomials divisible by a given polynomial.** Given $P(x) \in \mathbb{Z}[x]$, we search for a polynomial $Q(x) \in \mathbb{Z}[x]$ of height $H(Q) \leqslant h$ such that the product PQ is a Littlewood polynomial. Let

$$P(x) = a_0 + a_1 x + \cdots + a_d x^d, \qquad Q(x) = b_0 + b_1 x + \cdots + b_n x^n.$$

Clearly, $P(0)Q(0) = \pm 1$; hence we may assume that $a_0 = b_0 = 1$ (otherwise, replace P, Q by $-P, -Q$, respectively). If such a Q exists, then, by Lemma 9, it is possible to find Q of degree at most $(2h+1)^d + d - 2$. We used the following approach.

Suppose that the first j coefficients $b_0, b_1, \ldots, b_{j-1}$, where $0 \leqslant j \leqslant n$, of Q are already known. The coefficient l_j of the product $P(x)Q(x) = \sum_{j=0}^{n+d} l_j x^j$ is given by the equality

$$l_j = b_j a_0 + b_{j-1} a_1 + \cdots + b_{\max\{0,j-d\}} a_{\min\{j,d\}}.$$

Since $a_0 = 1$, from this equation we find that

$$b_j = l_j - b_{j-1} a_1 - \cdots - b_{\max\{0,j-d\}} a_{\min\{j,d\}}.$$

The coefficient b_j depends on the previous coefficients $b_i, 0 \leqslant i \leqslant j-1$, and the value of the coefficient $l_j \in \{-1, 1\}$. We must consider only those choices for l_j which give $|b_j| \leqslant h$. Suppose that we have determined the correct value of the coefficient l_j and computed the number b_j. If $j = n$, we are done. If no, we proceed to compute the next coefficient b_{j+1}.

This approach leads to the algorithm which recursively iterates through all candidates for the polynomial Q by trying all possible values $l_j = -1$ and $l_j = 1$ and finding the coefficients b_j. The recursion terminates when the factor Q is found or when two identical blocks of coefficients of length d are detected in the vector of coefficients b_j computed in the current branch of the recursion. Two identical blocks will necessarily occur if $j > (2h+1)^d + d - 2$ (see the proof of Lemma 9); hence the depth of recursion is finite. This also prevents the algorithm from searching through non-optimal candidates for the factor Q with repeated blocks of coefficients. The search ends immediately when the polynomial Q is found. Otherwise, it continues until all possible candidates for Q are rejected.

Algorithm 14. *Determines whether $P(x) \in \mathbb{Z}[x]$ divides a Littlewood polynomial L with $H(L/P) \leqslant h$.*

Input: *A Newman polynomial $P(x) = a_0 + \cdots + a_d x^d \in \mathbb{Z}[x]$ of degree d.*
A positive integer h.

Output: *A polynomial $Q(x) = b_0 + \cdots + b_n x^n \in \mathbb{Z}[x]$ of height $\leqslant h$ such that PQ is a Littlewood polynomial.*
Prints "$H(Q) > h$" if such a Q does not exist.

Level 0: 1. Set $b_0 = 1$, FOUND = false.
2. Iterate to the level 1.
3. If (FOUND is false), then print "$H(Q) > h$".
4. Exit.

Level j: 1. If (FOUND is true) or two identical blocks of length d are detected in the vector of coefficients $(b_0, b_1, \ldots, b_{j-1})$ computed so far, return.

2. Check if $P(x)(b_0 + b_1 x + \cdots + b_{j-1}x^{j-1})$ is already a Littlewood polynomial:
a) if it is, set FOUND = true, print the coefficients of Q and return;

b) if it is not:
i) set $l_j = 1$, compute $b_j = l_j - b_{j-1}a_1 - \cdots - b_{\max\{0,j-d\}}a_{\min\{j,d\}}$; if $|b_j| \leqslant h$, iterate to the next level $(j+1)$;

ii) set $l_j = -1$, compute $b_j = l_j - b_{j-1}a_1 - \cdots - b_{\max\{0,j-d\}}a_{\min\{j,d\}}$; if $|b_j| \leqslant h$, iterate to the next level $(j+1)$.

3. Return to the previous level $(j-1)$.

We coded the Algorithm 14 in C++. The detection of repeating blocks and checking if the product $P(x)(b_0 + b_1 x + \cdots + b_{j-1}x^{j-1})$ is already a Littlewood polynomial are very important to the performance of the program. We shall describe our implementation.

Before the search is started, we create an array of integers `A[ ]` of size $(2h+1)^d$ and initially fill this array with zeros. To every block $B_s = b_s, b_{s+1}, \ldots, b_{s+d-1}$ of length d we assign a non-negative integer

$$c(B_s) = (b_s + h)(2h+1)^{d-1} + (b_{s+1} + h)(2h+1)^{d-2} + \cdots + (b_{s+d-1} + h)$$

which is the representation of block B_s in base $2h+1$. If B_s and B_{s+1} are two adjacent blocks in the vector of coefficients, then the number $c(B_{s+1})$ can be quickly computed from the identity

$$c(B_{s+1}) = c(B_s)(2h+1) + b_{s+d} + h \pmod{(2h+1)^d}.$$

For each new block B_{j-d} found at the recursion level $j \geqslant d$, we check if `A[`$c(B_{j-d})$`]`$= 1$ and then store the value 1 at `A[`$c(B_{j-d})$`]`. If `A[`$c(B_{j-d})$`]`$= 1$, the new block is identical to one of the blocks computed before.

In order to check if the product of the polynomials P and $Q(x) = b_0 + b_1 x + \cdots + b_{j-1}x^{j-1}$ is already a Littlewood polynomial, it suffices to check the last d coefficients $l_j, l_{j+1}, \ldots, l_{j+d-1}$ of the product PQ. Indeed, all the coefficients $b_0, b_1, \ldots, b_{j-1}$ in the course of the recursive search are computed in such a way that the first j coefficients $l_0, l_1, \ldots, l_{j-1}$ are -1 or 1. The values $l_j, l_{j+1}, \ldots, l_{j+d-1}$ depend only on the last d values $b_{j-d}, b_{j-d+1}, \ldots, b_{j-1}$. We call block $B = b_{j-d}, b_{j-d+1}, \ldots, b_{j-1}$ the *endblock,* if the last d coefficients of the product $P(x)(b_{j-d} + b_{j-d+1}x + \cdots + b_{j-1}x^{d-1})$ belong to the set $\{-1, 1\}$. After initialization of the array `A[ ]`, before the recursive search is started, we precompute all possible endblocks B and store the values -1 at `A[`$c(B)$`]`. When the block B_s with `A[`$c(B_s)$`]`$= -1$ is found, the polynomial $Q(x)$ is printed and the search algorithm is stopped.

We remark that another algorithm for computing Littlewood polynomials with prescribed factors is given by Mossinghoff in the paper [14]. His approach is quite different from ours.

7. Computations

All the computations described below were performed on the Linux desktop computer with the Intel Pentium 4 class 2.4 Ghz processor and 1 GB of RAM. We used the GNU C++ compiler v.4.1.2.

7.1. **Newman polynomials dividing Littlewood polynomials.** We ran the implementation of Algorithm 14 on the list of all Newman polynomials P of degree $\deg P \leqslant 8$. For each of the 255 polynomials P in the list, the program computed a polynomial $Q(x) \in \mathbb{Z}[x]$, $H(Q) \leqslant 2$, such that the product PQ is a Littlewood polynomial L. The total program running time was less than one second. For most polynomials P, there exists a factor Q of height 1. There are only four exceptional Newman polynomials P of degree eight with the property that $H(L/P) \geqslant 2$ for any Littlewood polynomial L divisible by P. They are given in Table 2. The degree and height of the factor Q are also given here, together with the recursion depth reached until all candidates for Q of height 1 were rejected.

Table 2. Four exceptional Newman polynomials of degree 8 with $H(L/P) \geqslant 2$.

	Polynomial $P(x)$	$H(Q)$	$\deg Q$	Recursion depth ($h = 1$)
1.	$1 + x + x^4 + x^6 + x^8$	2	208	135
2.	$1 + x^2 + x^4 + x^7 + x^8$	2	208	78
3.	$1 + x + x^2 + x^5 + x^6 + x^8$	2	47	20
4.	$1 + x^2 + x^3 + x^6 + x^7 + x^8$	2	47	48

Then we ran the program on the list of Newman polynomials of degree 9. As a result, we found that 220 of the 256 polynomials divide some Littlewood polynomial L with the height of the quotient $H(L/P) = 1$. The program running time was also less than one second. For instance, for the Newman quadrinomial $P(x) = 1 + x^2 + x^5 + x^9$, which was used as an example in Section 4, the program found a Littlewood polynomial L divisible by P. The coefficients of L are given in Table 3. Note that the degree 371 of the polynomial L is exactly as predicted by Lemma 8.

Then we used our program once again for $h = 2$. As a result, we found that 18 polynomials of degree nine of the remaining 36 divide Littlewood polynomials L

TABLE 3. The signs of the coefficients $l_0, l_1, \ldots, l_{371} \in \{-1, 1\}$ of the Littlewood polynomial $L(x) = \sum_{j=0}^{371} l_j x^j$ divisible by the polynomial $P(x) = 1 + x^2 + x^5 + x^9$.

+ + + + + + + − − + + − − + + − + + + + − − + + + + + + + + +
+ + + + + + + − + + − + + + + + + − + + + + + − − + − − + + − −
+ + + + + + + − − + + − − + − − − + + + − + − − + + + − + + −
+ + + − + + − + + − + + − + + + + − − + + − + + − + + − − + +
− + − + + − + + − + + − + + − + + − + − − + + + + + − − + + − +
− − + + + − + + + + + + + + + − + + − + + − − + − − + + − −
+ − + − + + + − + + + + + − − + − + + + − − + + + + + + − +
+ − + + + − − + + − + + + + + + + − + + − + + − + − − + + − + +
+ − − + + − − + − + + + − + − − + + + + + + + − + + − + + −
+ + + + + + − + + + − + + − + + − − + + − + + − − + − − + + + −
+ − − + + − + + + − + + + − + + + − − + + + − + + + + + + − + +
− − + + − + + + − + + + + + + − + + + − + + − − + − − + + + − −

with $H(L/P) = 2$. The computations were completed in 1.6 sec. We launched the program once more to check if any of the remaining 18 polynomials divide some Littlewood polynomial with $H(L/P) = 3$. The time required for the program to complete the computations increased to 15.3 sec. The program gave a negative answer to all 18 polynomials. For the polynomials $1 + x^2 + x^6 + x^7 + x^9$ and $1 + x + x^2 + x^5 + x^7 + x^8 + x^9$ the algorithm reached the recursion depths 4640 and 4648, respectively, before rejecting all possible candidates for Q of height at most 3. For the other 16 polynomials, the maximal depth of the iterations required was not greater than 373.

Naturally, the polynomials from the last list are very good candidates for Newman polynomials not dividing any Littlewood polynomial. At least this gave us a realistic hope that such polynomials do exist. So we tested them using Algorithm 13 (see the next subsection).

In addition, we experimented with some special polynomials of higher degrees. For instance, we computed the following factor Q of height 1 for the Lehmer polynomial ℓ of degree 10 given above:

$$Q(x) = 1 + x^2 - x^3 + x^4 + x^7 - x^8 + x^{10} + x^{12} - x^{13} + x^{16} - x^{17} + x^{18} - x^{20}.$$

The product ℓQ is a Littlewood polynomial of degree 30. See also [14] for other examples.

7.2. **Irreducible Newman polynomials not dividing any Littlewood polynomial.** We used the numerical solver program MPSolve [4], which is based on the GMP library [17], for the computations with extended precision. For every root $\alpha = \Re(\alpha) + i\Im(\alpha)$ with modulus $|\alpha| > 1$ and imaginary part $\Im(\alpha) \geqslant 0$ of a given Newman polynomial P, we calculated the approximations a and b of real and imaginary parts of α to 100 digits. We then chose a real number $\varepsilon > 0$ which is sufficiently large to compute correct open bounding intervals $R = (a - \varepsilon, a + \varepsilon)$ and $I = (b - \varepsilon, b + \varepsilon)$ for $\Re(\alpha), \Im(\alpha)$, so that $\Re(\alpha) \in R, \Im(\alpha) \in I$. The values of ε are provided bellow. This procedure was applied to every polynomial P tested by Algorithm 13.

We launched the initial test to check the conditions of Theorem 4 for the values $N = 100$, $\delta = 0$ on 18 polynomials of degree 9. We set the variable ε which controls the accuracy of bounding intervals to a relatively large value, namely, $\varepsilon = 10^{-14}$. This accuracy was consistent with the capacity of the data types `interval` and `cinterval` used by the `C-XSC` library. The recursion depths reached by the program and the corresponding times are summarized in Table 4.

TABLE 4. $N = 100, \delta = 0, \varepsilon = 10^{-14}$

$P(x)$	The depth of recursion	Time, sec.
1.	67	8.9
2.	50	2.3
3.	71	0.7
4.	35	0.4
5.	59	1.7
6.	101	0.4
7.	101	0.1
8.	49	1.9

The row number in the first column of the table corresponds to the number of the polynomial in Table 1. If the recursion depth reached is less than $N + 1$, then the corresponding polynomial is confirmed to be the polynomial which does not divide any Littlewood polynomial (see Section 6).

The initial test gave no information about the polynomials numbered 6 and 7. In contrast, their reciprocals, numbers 5 and 8, were identified as those which do not divide any Littlewood polynomial. To deal with these two examples (which obviously must be the polynomials which do not divide any Littlewood polynomial either), we rewrote the code of the program, replacing the data types `interval` and `cinterval` with multiprecision data types `l_interval` and `l_cinterval`. We then increased the precision of the bounding intervals to $\varepsilon = 10^{-30}$. The numerical test confirmed both polynomials as not dividing any Littlewood polynomial (see Table 5).

TABLE 5. $N = 100, \delta = 0, \varepsilon = 10^{-30}$

$P(x)$	The depth of recursion	Time, sec.
6.	81	24.2
7.	58	7.6

Then we tested whether some polynomials from Table 1 satisfy the conditions of Theorem 4 with strictly positive δ. We used the first version of the code due to a considerable increase in the time required by the program to complete the tests. The results for $\delta = 2$, which terminated up to $N = 100$, are given in Table 6.

It is important to note that Table 1 contains only those Newman polynomials of degree 9 for which numerical tests confirmed that both polynomial P and its reciprocal P^* do not divide any Littlewood polynomial. Moreover, in order to be absolutely sure, in each case, using the test based on Algorithm 13, we found that

TABLE 6. $N = 100, \delta = 2, \varepsilon = 10^{-14}$

$P(x)$	The depth of recursion	Time, sec.
1.	83	1662.0
2.	59	346.7
4.	49	140.3
5.	75	685.6
8.	67	629.5

at least one of the polynomials P and P^* has the required property with a quite large value of δ. See Table 6, where $\delta = 2$.

In each of the remaining 10 cases, the classification problem was not completely solved. All 10 remaining polynomials are listed in Table 7.

TABLE 7. Newman polynomials of degree 9 which are not confirmed to divide a Littlewood polynomial.

1.	$1 + x^2 + x^3 + x^7 + x^9$
2.	$1 + x^2 + x^6 + x^7 + x^9$
3.	$1 + x + x^3 + x^4 + x^7 + x^9$
4.	$1 + x^2 + x^5 + x^6 + x^8 + x^9$
5.	$1 + x + x^2 + x^3 + x^6 + x^7 + x^9$
6.	$1 + x^2 + x^3 + x^6 + x^7 + x^8 + x^9$
7.	$1 + x + x^2 + x^3 + x^5 + x^8 + x^9$
8.	$1 + x + x^4 + x^6 + x^7 + x^8 + x^9$
9.	$1 + x + x^2 + x^4 + x^7 + x^8 + x^9$
10.	$1 + x + x^2 + x^5 + x^7 + x^8 + x^9$

Naturally, one can hope that further searches performed using Algorithm 14 expecting quotients L/P of height $H(L/P) \geqslant 4$ or additional tests based on Algorithm 13 with increased recursion depths and more accurate bounding intervals for the roots of P will complete the classification of polynomials given in Table 7. However, as we said above, in principle, it is possible that P does not divide any Littlewood polynomial, but this cannot be established by Algorithm 13 applied to P or P^*.

ACKNOWLEDGEMENTS

We are grateful to a referee who carefully read both (theoretical and computational) parts of this paper and made many useful remarks. We also thank Paulius Drungilas for his initial work on Algorithm 14 and his computations concerning Newman polynomials of degree at most seven. This research was supported in part by the Lithuanian State Studies and Science Foundation.

REFERENCES

[1] F. Amoroso, *Polynomials with prescribed vanishing at roots of unity*, Boll. Un. Mat. Ital. B(7), **9** (1995), 1021–1024. MR1369388 (97a:11120)

[2] F. Beaucoup, P. Borwein, D .W. Boyd and C. Pinner, *Multiple roots of* $[-1, 1]$ *power series*, J. London Math. Soc. (2), **57** (1998), 135–147. MR1624809 (99c:30005)

[3] F. Beaucoup, P. Borwein, D .W. Boyd and C. Pinner, *Power series with restricted coefficients and a root on a given ray*, Math. Comp., **67** (1998), 715–736. MR1468939 (98k:30006)
[4] D. A. Bini and G. Fiorentino, *Numerical computation of polynomial roots v. 2.0*, FRISCO report (1998) (available online at `http://www.dm.unipi.it/cluster-pages/mpsolve/index.htm`).
[5] P. Borwein, E. Dobrowolski and M. J. Mossinghoff, *Lehmer's problem for polynomials with odd coefficients*, Ann. of Math. (2), **166** (2007), 347–366.
[6] P. Borwein, K. G. Hare and M. J. Mossinghoff, *The Mahler measure of polynomials with odd coefficients*, Bull. London Math. Soc., **36** (2004), 332–338. MR2038720 (2004m:11177)
[7] P. Borwein and M. J. Mossinghoff, *Polynomials with height* 1 *and prescribed vanishing at* 1, Exper. Math., **9** (2000), 425–433. MR1795875 (2001k:11036)
[8] P. Borwein and C. Pinner, *Polynomials with* $\{0, +1, -1\}$ *coefficients and a root close to a given point*. Canadian J. Math., **49** (1997), 887–915. MR1604114 (98m:11014)
[9] P. Drungilas and A. Dubickas, *Roots of polynomials of bounded height*, Rocky Mt. J. Math. (to appear).
[10] A. Dubickas and M. J. Mossinghoff, *Auxiliary polynomials for some problems regarding Mahler's measure,* Acta Arith., **119** (2005), 65–79. MR2163518 (2006e:11162)
[11] M. Filaseta, *On the factorization of polynomials with small Euclidean norm*, In: Number theory in progress (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, **1** (1999), 143–163. MR1689504 (2000c:11177)
[12] M. Filaseta and M. Matthews, Jr., *On the irreducibility of* 0*,* 1 *- polynomials of the form* $f(x)x^n + g(x)$, Colloq. Math., **99** (2004), 1–5. MR2084532 (2005g:11205)
[13] W. Hofschuster and W. Krämer, *C–XSC 2.0: A C++ Class Library for Extended Scientific Computing*, Numerical Software with Result Verification, Lecture Notes in Computer Science, **2991**, Springer-Verlag, Heidelberg, (2004) 15–35 (available online at `http://www.math.uni-wuppertal.de/~xsc/`).
[14] M. J. Mossinghoff, *Polynomials with restricted coefficients and prescribed noncyclotomic factors*, LMS J. Comput. Math., **3** (2003), 314–325. MR2051588 (2004m:11034)
[15] A. M. Odlyzko and B. Poonen, *Zeros of polynomials with* 0*,*1 *coefficients*, Enseign. Math., **39** (1993), 317–384. MR1252071 (95b:11026)
[16] A. Schinzel, *On the reduced length of a polynomial*, Funct. Approx., Comment. Math., **35** (2006), 271–306. MR2271619 (2007h:12001)
[17] GMP, *The GNU Multiple Precision Arithmetic Library* (available online at `http://swox.com/gmp/`).

Department of Mathematics and Informatics, Vilnius University, Naugarduko 24, Vilnius LT-03225, Lithuania -and- Institute of Mathematics and Informatics, Akademijos 4, Vilnius LT-08663, Lithuania
E-mail address: `arturas.dubickas@mif.vu.lt`

Department of Mathematics and Informatics, Vilnius University, Naugarduko 24, Vilnius LT-03225, Lithuania
E-mail address: `jonas.jankauskas@gmail.com`