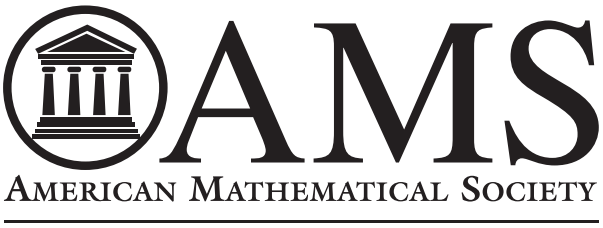


P. Drungilas, J. Jankauskas, J. Šiurys

On Littlewood and Newman polynomial multiples of Borwein polynomials

Mathematics of Computation

DOI: 10.1090/mcom/3258

Accepted Manuscript

ON LITTLEWOOD AND NEWMAN POLYNOMIAL MULTIPLES OF BORWEIN POLYNOMIALS

P. DRUNGILAS, J. JANKAUSKAS, J. ŠIURYS

Abstract. A Newman polynomial has all the coefficients in $\{0,1\}$ and constant term 1, whereas a Littlewood polynomial has all coefficients in $\{-1,1\}$. We call $P(X) \in \mathbb{Z}[X]$ a *Borwein* polynomial if all its coefficients belong to $\{-1,0,1\}$ and $P(0) \neq 0$. By exploiting an algorithm which decides whether a given monic integer polynomial with no roots on the unit circle $|z| = 1$ has a non-zero multiple in $\mathbb{Z}[X]$ with coefficients in a finite set $\mathcal{D} \subset \mathbb{Z}$, for every Borwein polynomial of degree at most 9 we determine whether it divides any Littlewood or Newman polynomial. In particular, we show that every Borwein polynomial of degree at most 8 which divides some Newman polynomial divides some Littlewood polynomial as well. In addition to this, for every Newman polynomial of degree at most 11, we check whether it has a Littlewood multiple, extending the previous results of Borwein, Hare, Mossinghoff, Dubickas and Jankauskas.

1. Introduction

Let $d \in \mathbb{N}$ and let $P(X)$ be a polynomial

$$P(X) = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0 \tag{1.1}$$

in one variable X with integer coefficients $a_j \in \mathbb{Z}$. To avoid trivialities, we consider only polynomials with non-zero leading and constant terms $a_d \cdot a_0 \neq 0$. In such case, both $P(X)$ and its reciprocal polynomial $P^*(X) := X^d P(1/X)$ are of the same degree d. If $P(X)$ has only three non-zero coefficients a_j, for $0 \leq j \leq d$, then it is called *a trinomial*. Similarly, if the number of non-zero coefficients is four, $P(X)$ is called *a quadrinomial*.

The polynomial $P(X)$ in (1.1) is called a *Littlewood* polynomial, if $a_j \in \{-1,1\}$ for each $0 \leq j \leq d$. For instance, $P(X) = X^4 + X^3 - X^2 + X - 1$ is a Littlewood polynomial. The set of all Littlewood polynomials is denoted by $\mathcal{L}$. Similarly, a polynomial $P(X)$ is called *a Newman polynomial*, if all coefficients $a_j \in \{0,1\}$ and $P(0) = 1$. For instance, $P(X) = X^3 + X + 1$

2010 *Mathematics Subject Classification.* 11R09, 11Y16, 12D05, 11R06.

Key words and phrases. Borwein polynomial, Littlewood polynomial, Newman polynomial, Pisot number, Salem Number, Mahler measure, polynomials of small height.

The first author is supported by the Research Council of Lithuania grant MIP-049/2014. The second author is supported by project P27050 *Fractals and Words: Topological, Dynamical, and Combinatorial Aspects* funded by the Austrian Science Fund (FWF).

is a Newman polynomial. The subset of $\mathbb{Z}[X]$ of all Newman polynomials is denoted by $\mathcal{N}$. Finally, we call an integer polynomial $P(X)$ in (1.1) with all coefficients $a_j \in \{-1, 0, 1\}$ and a nonzero constant term $P(0)$ *a Borwein polynomial*[1]. $P(X) = X^5 - X^2 + 1$ is an example of a Borwein polynomial. The set of all Borwein polynomials is denoted by $\mathcal{B}$. One has trivial set relations $\mathcal{N} \subset \mathcal{B}$, $\mathcal{L} \subset \mathcal{B}$.

We say that a polynomial $P(X)$ has a Littlewood multiple if it divides some polynomial in the set $\mathcal{L}$. In the similar way, we say that $P(X)$ has a Newman multiple, or a Borwein multiple if $P(X)$ divides some polynomial in $\mathcal{N}$ or in $\mathcal{B}$, respectively. When we need to restrict our attention only to polynomials of fixed degree, we use the subscript d in $\mathcal{N}_d$, $\mathcal{L}_d$ and $\mathcal{B}_d$ to denote the sets of Newman, Littlewood and Borwein polynomials of degree d, respectively. Similarly, we use the subscript "$\leq d$" to indicate the sets of polynomials of degree *at most* d, that is

$$\mathcal{N}_{\leq d} = \bigcup_{j=0}^{d} \mathcal{N}_j, \qquad \mathcal{L}_{\leq d} = \bigcup_{j=0}^{d} \mathcal{L}_j, \qquad \mathcal{B}_{\leq d} = \bigcup_{j=0}^{d} \mathcal{B}_j.$$

Clearly, non-constant polynomials $P(X)$ with all non-negative coefficients cannot have any positive real zeros $X \in [0, \infty)$. Newman polynomials are among such polynomials. To denote the subsets of Littlewood or Borwein polynomials with no real positive zeros, we append the " $-$ " superscript, for instance, $\mathcal{L}^-$, $\mathcal{B}^-$, $\mathcal{L}_d^-$, $\mathcal{B}_d^-$ and $\mathcal{L}_{\leq d}^-$, $\mathcal{B}_{\leq d}^-$.

Let $\mathcal{A} \subset \mathbb{Z}[X]$. We will employ the notation $\mathcal{L}(\mathcal{A})$ to denote the set of polynomials $P(X) \in \mathcal{A}$ which divide some Littlewood polynomial. Similarly, denote by $\mathcal{N}(\mathcal{A})$ the set of polynomials $P(X) \in \mathcal{A}$ which divide some Newman polynomial. In particular, the set $\mathcal{B}_d \setminus \mathcal{L}(\mathcal{B})$ consists of those Borwein polynomials of degree d that do not divide any Littlewood polynomial, whereas the set $\mathcal{N}(\mathcal{B}_d) \setminus \mathcal{L}(\mathcal{B})$ consists of those Borwein polynomials of degree d that divide some Newman polynomial but do not divide any Littlewood polynomial.

Let $\mathcal{D} \subset \mathbb{Z}$ be a finite set. We call $\mathcal{D}$ a *digit set*. Central to our work is a further development (see Section 3) of an algorithm that can answer the following question.

Question 1. *Given a monic polynomial $P \in \mathbb{Z}[X]$ which has no roots on the unit circle $|z| = 1$ in the complex plane, does there exist a nonzero polynomial with coefficients in $\mathcal{D}$ which is divisible by P?*

[1]This nomenclature in honor of P. Borwein for his work on polynomials of this type was proposed by C. Smyth during the 2015 workshop *The Geometry, Algebra and Analysis of Algebraic numbers* in Banff, Alberta (personal communication).

The first instance of such an algorithm that we are aware of appeared in the work of Lau [13]. It was confined to the case when $P(X)$ is a minimal polynomial of a Pisot number. Subsequent computations were done by Borwein and Hare [4], Hare and Mossinghoff [9]. It was used for the computation of the discrete spectra of Pisot numbers. In a special case where the set $\mathcal{D} = \{-q, \ldots, -1, 0, 1, \ldots, q\}$ (here q is a positive integer) the fact that $P(X)$ has a non-zero multiple $Q(X)$ with coefficients in $\mathcal{D}$ is equivalent to the fact that the number 0 has a non-trivial representation in the difference set of the spectra generated by the root α of $P(X)$ with digits $\{0, 1, \ldots, q\}$. Stankov [22] extended the algorithm to non-Pisot algebraic integers with no conjugates on the unit circle. Akiyama, Thuswaldner and Zaïmi [2, Theorem 3] show that there exists automata that can determine the minimal height polynomial with integer coefficients for a given algebraic number provided it has no algebraic conjugates on $|z| = 1$ in the complex plane. Thus the algorithm of Akiyama, Thuswaldner and Zaïmi [2] answers Question 1 for irreducible monic polynomials $P(X) \in \mathbb{Z}[X]$ with no roots on the unit circle. One contribution of our paper is a further development of this algorithm to allow $P(X)$ to have repeated roots (i.e., when $P(X)$ is not separable). This should open the way to answering questions regarding the multiplicity of the divisors of polynomials with restricted coefficients (see, e.g., Example 9 in Section 4). We do not know if the condition that $P(X)$ has no roots with $|z| = 1$ can be dropped or not; it seems to be essential to the proof that the search terminates. In some cases this condition can be circumvented (see Subsection 4.1 on cyclotomic factors and the last note at the end of Section 3). Other approaches to search for Newman and Littlewood multiples of $P(X)$ in the literature are: the application of LLL [4]; the factorization of Littlewood polynomials of large degrees [15]; the search for multipliers of bounded height [7]. These approaches do not allow to identify polynomials $P(X)$ that have no such multiple.

We implement our algorithm to answer this question for all Borwein polynomials of degree up to 9 and the digit sets $\mathcal{D} = \{0, 1\}$ and $\mathcal{D} = \{-1, 1\}$. In other words, for every Borwein polynomial of degree at most 9 we decide whether it has a Littlewood multiple and whether it divides some Newman polynomial. Moreover, for every Newman polynomial $P(X)$ of degree at most 11 we determine whether $P(X) \in \mathcal{L}(\mathcal{N})$. These computations allow us to extend the results previously obtained by Dubickas and Jankauskas [7], Borwein and Hare [4], Hare and Mossinghoff [9] (see Section 2.1 and Section 4).

This paper is organized as follows. The main results are given in Section 2.1. In Section 4 we describe our computations. The algorithm, along with the proofs of auxiliary results, are given in Section 3.

2. Main results

2.1. **Relations between sets $\mathcal{B}$, $\mathcal{L}(\mathcal{B})$ and $\mathcal{N}(\mathcal{B})$.** The set $\mathcal{B}$ of Borwein polynomials can be partitioned into the following four subsets.

$\mathcal{L}(\mathcal{B})\setminus\mathcal{N}(\mathcal{B})$	– the set of Borwein polynomials that have Littlewood multiples and don't have Newman multiples;
$\mathcal{N}(\mathcal{B})\setminus\mathcal{L}(\mathcal{B})$	– the set of Borwein polynomials that have Newman multiples and don't have Littlewood multiples;
$\mathcal{L}(\mathcal{B})\cap\mathcal{N}(\mathcal{B})$	– the set of Borwein polynomials that have Littlewood and Newman multiples;
$\mathcal{B}\setminus(\mathcal{L}(\mathcal{B})\cup\mathcal{N}(\mathcal{B}))$	– the set of Borwein polynomials that divide no Littlewood and no Newman polynomial.

We implemented Algorithm 1 (see Section 4) and ran it to determine whether $P(X)\in\mathcal{L}(\mathcal{B})$ and whether $P(X)\in\mathcal{N}(\mathcal{B})$ for all Borwein polynomials $P(X)$ of degree at most 9. Thus we have completed the classification of polynomials from $\mathcal{B}_{\le 9}$ started by Dubickas and Jankauskas [7]. In particular, we calculated the numbers

$$\#\left(\mathcal{L}(\mathcal{B}_d)\setminus\mathcal{N}(\mathcal{B})\right),\ \ \#\left(\mathcal{N}(\mathcal{B}_d)\setminus\mathcal{L}(\mathcal{B})\right)\ \text{ and }\ \#\left(\mathcal{L}(\mathcal{B}_d)\cap\mathcal{N}(\mathcal{B}_d)\right)$$

for every $d\in\{1,2,\dots,9\}$ that are provided in Table 1. As a result we obtain the following statement (see the third column in Table 1).

Theorem 2. *Every Borwein polynomial of degree at most* 8 *which divides some Newman polynomial divides some Littlewood polynomial as well.*

Theorem 2 is a generalization of Theorem 2 in [7] where it is proved that every Newman polynomial of degree at most 8 divides some Littlewood polynomial.

Table 1

d	$\#\left(\mathcal{L}(\mathcal{B}_d)\setminus\mathcal{N}(\mathcal{B})\right)$	$\#\left(\mathcal{N}(\mathcal{B}_d)\setminus\mathcal{L}(\mathcal{B})\right)$	$\#\left(\mathcal{L}(\mathcal{B}_d)\cap\mathcal{N}(\mathcal{B}_d)\right)$
1	2	0	2
2	6	0	6
3	24	0	12
4	72	0	32
5	224	0	68
6	612	0	164
7	1518	0	342
8	3610	0	822
9	8564	60	1596

By the inclusion-exclusion principle, one obtains the following equalities

$$\begin{aligned}
\#\mathcal{B}_d\backslash\mathcal{L}(\mathcal{B}) &= \#\mathcal{B}_d - \#\left(\mathcal{L}(\mathcal{B}_d)\backslash\mathcal{N}(\mathcal{B})\right) - \#\left(\mathcal{L}(\mathcal{B}_d)\cap\mathcal{N}(\mathcal{B}_d)\right),\\
\#\mathcal{B}_d\backslash\mathcal{N}(\mathcal{B}) &= \#\mathcal{B}_d - \#\left(\mathcal{N}(\mathcal{B}_d)\backslash\mathcal{L}(\mathcal{B})\right) - \#\left(\mathcal{L}(\mathcal{B}_d)\cap\mathcal{N}(\mathcal{B}_d)\right),\\
\#\mathcal{B}_d\backslash(\mathcal{L}(\mathcal{B})\cup\mathcal{N}(\mathcal{B})) &= \#\mathcal{B}_d - \#\left(\mathcal{L}(\mathcal{B}_d)\backslash\mathcal{N}(\mathcal{B})\right)\\
&\qquad - \#\left(\mathcal{N}(\mathcal{B}_d)\backslash\mathcal{L}(\mathcal{B})\right) - \#\left(\mathcal{L}(\mathcal{B}_d)\cap\mathcal{N}(\mathcal{B}_d)\right),
\end{aligned}$$

which are valid for all positive integers d. These numbers, for $d \in \{1, 2, \ldots, 9\}$, are given in Table 2.

TABLE 2

d	$\#\left(\mathcal{B}_d\backslash\mathcal{L}(\mathcal{B})\right)$	$\#\left(\mathcal{B}_d\backslash\mathcal{N}(\mathcal{B})\right)$	$\#\left(\mathcal{B}_d\backslash(\mathcal{L}(\mathcal{B})\cup\mathcal{N}(\mathcal{B}))\right)$
1	0	2	0
2	0	6	0
3	0	24	0
4	4	76	4
5	32	256	32
6	196	808	196
7	1056	2574	1056
8	4316	7926	4316
9	16084	24588	16024

For example, there are exactly 196 Borwein polynomials of degree 6 which have no Littlewood multiple.

2.2. **Borwein polynomials that do not divide any Littlewood polynomial.** Recall that a real algebraic integer $\alpha > 1$ is called a *Pisot number* after [18], if all the algebraic conjugates of α over $\mathbb{Q}$ (other than α itself) are of modulus $|z| < 1$. Similarly, a real algebraic integer $\alpha > 1$ is called a *Salem number* (see, e.g., [19, 20, 21]), if all other conjugates of α lie in the unit circle $|z| \leq 1$ with at least one conjugate on the unit circle $|z| = 1$.

In their computation of the discrete spectra of Pisot numbers, Borwein and Hare [4] found the first examples of Borwein polynomials $P(X)$ that provably divide no Littlewood polynomial. All these polynomials are of degree $d = 9$ or $d = 10$ and they are minimal polynomials of Pisot numbers, see Table 3. So the sets $\mathcal{B}_9\backslash\mathcal{L}(\mathcal{B})$ and $\mathcal{B}_{10}\backslash\mathcal{L}(\mathcal{B})$ are non-empty.

In the present paper, we find the least degree Borwein polynomials with no Littlewood multiple.

Proposition 3. *The smallest degree Borwein polynomial which does not divide any Littlewood polynomial is* $p(X) = X^4 + X^3 - X + 1$. *Moreover,*

$$\mathcal{B}_{\leq 4}\backslash\mathcal{L}(\mathcal{B}) = \{\pm p(X), \pm p^*(X)\}.$$

TABLE 3. Minimal polynomials of Pisot numbers that divide no Littlewood polynomial found by Borwein and Hare.

#	Polynomial $P(X) \in \mathcal{B}$	Pisot number
1	$X^{10} - X^8 - X^7 - X^6 - X^5 + 1$	$1.954062236\ldots$
2	$X^9 - X^8 - X^7 - X^6 - X^5 - X^4 + 1$	$1.963515789\ldots$
3	$X^9 - X^8 - X^7 - X^6 - X^5 - X^4 - X^3 - X - 1$	$1.992483962\ldots$
4	$X^9 - X^8 - X^7 - X^6 - X^5 - X^4 - X^3 - X^2 - 1$	$1.994016415\ldots$

A systematic investigation of the sets $\mathcal{L}(\mathcal{B}) \cap \mathcal{N}(\mathcal{B})$ and $\mathcal{N}(\mathcal{B}) \setminus \mathcal{L}(\mathcal{B})$ was started by Dubickas and Jankauskas in [7]. They found that each $P(X) \in \mathcal{N}_{\le 8}$ has a Littlewood multiple, so that $\mathcal{L}(\mathcal{N}_{\le 8}) = \mathcal{N}_{\le 8}$. First known polynomials $P(X) \in \mathcal{N}_9$ that do not divide any polynomial in $\mathcal{L}$ were also identified in [7]. They are equal to one of the polynomials no. 1, 3, 5, 9 of Table 4 or their reciprocals. Moreover, all the possible candidates of $P(X) \in \mathcal{N}_9$ with no Littlewood multiple were identified (see Table 7 in [7]) but not fully resolved.

TABLE 4. The complete set $\mathcal{N}_9 \setminus \mathcal{L}(\mathcal{N})$ (reciprocals omitted).

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

Our recent computations confirm that none of these candidates divides any Littlewood polynomial. They are listed as polynomials no. 2, 4, 6, 7, 8 (or their reciprocals) in Table 4. Hence, the sets $\mathcal{L}(\mathcal{N}_9)$ and $\mathcal{N}_9 \setminus \mathcal{L}(\mathcal{N})$ are now completely determined. In particular, $\#\mathcal{N}_9 \setminus \mathcal{L}(\mathcal{N}) = 18$. The complete list of Newman polynomials of degree 9 that have no Littlewood multiple is provided in Table 4 (with reciprocals omitted) .

In this paper, we have been able to extend the classification of the polynomials from the set $\mathcal{N}_9$ to larger degrees. As it is not practical to provide the full lists here, we just indicate that the sets $\mathcal{L}(\mathcal{N}_d)$, $\mathcal{N}_d \setminus \mathcal{L}(\mathcal{N})$ have been completely determined for $d = 10$ and $d = 11$. In particular, our computations show that $\#\mathcal{N}_{10} \setminus \mathcal{L}(\mathcal{N}) = 36$ and $\#\mathcal{N}_{11} \setminus \mathcal{L}(\mathcal{N}) = 174$.

Using the polynomial $P(X)$ no.3 from Table 4, Dubickas and Jankauskas [7] proved that for all sufficiently large positive integers n the polynomial $x^n P(X) + 1$ does not divide any Littlewood polynomial. This implies that the set $\mathcal{N}_d \backslash \mathcal{L}(\mathcal{N})$ is non-empty for all sufficiently large d. In addition to this, they proved that every Borwein polynomial with three non-zero terms

$$X^b \pm X^a \pm 1, \quad 1 \le a < b, \quad a, b \in \mathbb{Z}$$

(including Newman trinomials $X^b + X^a + 1$) has a Littlewood multiple, as well as some types of Borwein quadrinomials $X^c \pm X^b \pm X^a \pm 1$ do. These results show that set $\mathcal{L}(\mathcal{B}) \cap \mathcal{N}(\mathcal{B})$ has a non-trivial structure.

Dubickas and Jankauskas [7] asked whether there exists a Borwein quadrinomial that does not divide any Littlewood polynomial. Our computations imply that there are exactly 20 such quadrinomials of degree ≤ 9. They are given in Table 5 (we only list quadrinomials with positive leading coefficient).

TABLE 5. Monic quadrinomials in $\mathcal{B}_{\le 9} \backslash \mathcal{L}(\mathcal{B})$ (reciprocals omitted).

$X^4 + X^3 - X + 1$	$X^6 - X^5 - X - 1$	$X^8 - X^5 + X^3 + 1$
$X^8 + X^7 - X + 1$	$X^8 + X^6 - X^2 + 1$	

Since every Borwein trinomial divides some Littlewood polynomial (see [7, Theorem 1]), we have the following result (see also Table 5).

Corollary 4. *The least positive integer k for which there exists a Borwein polynomial with k nonzero terms that divides no Littlewood polynomial is $k = 4$.*

Our computations also show that each quadrinomial in $\mathcal{N}_{\le 11}$ divides some Littlewood polynomial. Therefore the following question is of interest.

Question 5. *Does there exist a Newman quadrinomial with no Littlewood multiple? Equivalently, does the set $\mathcal{N} \backslash \mathcal{L}(\mathcal{N})$ contain a quadrinomial?*

If such quadrinomial exists, it must be of degree ≥ 12.

2.3. **Borwein polynomials that do not divide any Newman polynomial.** Recall that a Newman polynomial has no nonnegative real roots. However, not every polynomial $P(X) \in \mathcal{B}^-$ divides a Newman polynomial. Our computations show that

Proposition 6. *The smallest degree Borwein polynomial without nonnegative real roots and no Newman multiple is $p(X) = X^3 + X^2 - X + 1$, and $\mathcal{B}^-_{\le 3} \backslash \mathcal{N}(\mathcal{B}) = \{\pm p(X), \pm p^*(X)\}$.*

Recall that the *Mahler measure* of a polynomial

$$p(X) = \sum_{i=k}^{n} a_k X^k = a_n \prod_{k=1}^{n} (X - \alpha_k) \in \mathbb{C}[X]$$

is defined by $M(p) = |a_n| \prod_{k=1}^{n} \max\{1, |\alpha_k|\}$.

Hare and Mossinghoff [9] considered the following problem: does there exist a real number $\sigma > 1$ such that if $f(X) \in \mathbb{Z}[X]$ has no nonnegative real roots and $M(f) < \sigma$, then $f(X)$ divides some Newman polynomial $F(X)$? Based on the results of Dufresnoy and Pisot[8], Amara [3] and Boyd [5, 6] they proved that every negative Pisot number which has no positive real algebraic conjugate and is larger than $-\tau$, where $\tau = (1+\sqrt{5})/2 \approx 1.61803$ is the golden ratio, is a root of some Newman polynomial. They also proved that certain negative Salem numbers greater than $-\tau$ are roots of Newman polynomials. Moreover, they have constructed a number of polynomials that have Mahler measure less than τ, have no positive real roots and yet do not divide any Newman polynomial. The smallest Mahler measure in their list is approximately 1.556 attained by the polynomial $X^6 - X^5 - X^3 + X^2 + 1$. We found that among Borwein polynomials of degree at most 9 there are exactly 16 polynomials which extend this list and have Mahler measure less than 1.556. They are given in Table 6 (we omit their reciprocal polynomials).

TABLE 6. Polynomials in $\mathcal{B}^{-}_{\leq 9} \backslash \mathcal{N}(\mathcal{B})$ of small Mahler measure.

Polynomial $P(X) \in \mathcal{B}^{-}_{\leq 9} \backslash \mathcal{N}(\mathcal{B})$	Mahler measure
$X^9 + X^8 + X^7 - X^5 - X^4 - X^3 + 1$	1.436632261
$X^9 + X^8 - X^3 - X^2 + 1$	1.483444878
$X^9 - X^7 - X^5 + X^3 + X + 1$	1.489581321
$X^8 - X^7 - X^4 + X^3 + 1$	1.489581321
$X^8 + X^7 - X^3 - X^2 + 1$	1.518690904
$X^8 + X^7 + X^6 - X^4 - X^3 - X^2 + 1$	1.536566472
$X^9 - X^8 - X^6 + X^5 + 1$	1.536913983
$X^9 + X^5 - X^3 - X^2 + 1$	1.550687063

Note that the third polynomial in Table 6 factors as $(X+1) \cdot (X^8 - X^7 - X^4 + X^3 + 1)$ and the second factor is the fourth polynomial of the table. All the other polynomials in this table are irreducible over $\mathbb{Z}$.

2.4. **Examples with special factors.** The following example demonstrates that if two polynomials have Littlewood multiples, their product does not necessarily have one.

Example 7. *Borwein polynomials* $p(x) = X^4 + X^3 + 1$ *and* $q(x) = X^5 - X^4 + X^3 - X + 1$ *belong to* $\mathcal{L}(\mathcal{B})$. *However, their product* $p(x)q(x)$ *has no Littlewood multiple. Consequently, the Newman multiple of* $p(x)q(x)$

$$P(X) = X^{11} + X^{10} + X^9 + X^8 + X^7 + X^5 + X^4 + X^3 + 1 =$$
$$= (X^2 + X + 1)(X^4 + X^3 + 1)(X^5 - X^4 + X^3 - X + 1)$$

also has no Littlewood multiple.

Moreover, $p(X) \in \mathcal{N}(\mathcal{B})$ does not imply that always $p(X)p^*(X) \in \mathcal{N}(\mathcal{B})$, as can be seen from Example 8.

Example 8. *Let $p(X) = X^3 - X + 1$ be the minimal polynomial of the largest negative Pisot number $-\theta \approx -1.32472$. Both $p(X)$ and its reciprocal $p^*(X) = X^3 - X^2 + 1$ have Newman multiples $P(X) = X^5 + X^4 + 1$ and $P^*(X) = X^5 + X + 1$, respectively. However, the product*

$$p(X)p^*(X) = X^6 - X^5 - X^4 + 3X^3 - X^2 - X + 1$$

has no Newman multiple. In contrast, $p(X)p^*(X)$ divides the Borwein polynomial

$$\begin{aligned} Q(X) &= (X^2 + X + 1)(X^3 - X + 1)(X^3 - X^2 + 1) = \\ &= X^8 - X^6 + X^5 + X^4 + X^3 - X^2 + 1 \end{aligned}$$

that, in turn, has its own Littlewood multiple.

The last example in this subsection illustrates the ability of Algorithm 1 to work with polynomials $P(X)$ with repeated noncyclotomic roots.

Example 9. *The polynomial $p(X) = X^3 - X + 1$ has a Newman multiple (see Example 8). However, its square $p(X)^2$ does not.*

The square $p(X)^2$ divides a Littlewood polynomial $L(X)$ of degree 195 *from Table 7, while the cube $p(X)^3$ has no Littlewood multiple at all.*

These two facts imply that the Borwein multiple

$$P(X) = (X^2 + X + 1)p(X)^2 = X^8 + X^7 - X^6 + X^4 + X^3 - X + 1$$

of $p^2(X)$ divides no Newman polynomial, but $P(X)$ has a Littlewood multiple, namely the polynomial $L(X)\Phi_3(X^{196})$, where $\Phi_3(X) = X^2 + X + 1$.

TABLE 7. Coefficients $l_0, l_1, \ldots, l_{195} \in \{-1, 1\}$ of the Littlewood multiple $L(X) = \sum_{j=0}^{195} l_j X^{195-j}$ of $p(X) = (X^3 - X + 1)^2$.

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

2.5. **Irreducible non-cyclotomic polynomials with some unimodular roots.** In the context of the work of Borwein and Hare [4], Stankov [22] on the spectra of Salem numbers and the work of Hare and Mossinghoff [9] on Salem numbers that are roots of Newman polynomials, we also investigated the subset $\mathcal{U}_{\leq 9}^{irr}$ of monic irreducible non-cyclotomic Borwein polynomials of

degree at most 9 with at least one unimodular root. The set $\mathcal{U}_{\leq 9}^{irr}$ contains exactly 52 polynomials. It can be partitioned into 3 disjoint subsets

$$\mathcal{U}_{\leq 9}^{irr} = \mathcal{U}_{\leq 9}^{1} \cup \mathcal{U}_{\leq 9}^{2} \cup \mathcal{U}_{\leq 9}^{spor},$$

where:

- $\mathcal{U}_{\leq 9}^{1}$ consists of 28 minimal polynomials of Salem numbers (*Salem polynomials*) or minimal polynomials of negative Salem numbers (α is a negative Salem number if $-\alpha$ is a Salem number). Salem polynomials are given in Table 8; negative–Salem polynomials can be obtained by substitution $X \mapsto -X$. All $P(X)$ from Table 8 belong to the set $\mathcal{L}(\mathcal{B})\backslash\mathcal{N}(\mathcal{B})$.
- $\mathcal{U}_{\leq 9}^{2}$ consists of 19 minimal polynomials of complex Salem numbers. $P(X) \in \mathcal{U}_{\leq 9}^{irr}$ is a complex Salem polynomial if exactly four of its roots, $\{z, \overline{z}, z^{-1}, \overline{z}^{-1}\}$ do not lie on the unit circle. These polynomials $P(X)$ are shown in Table 9, where $P(-X)$ are omitted. All but one (no. 4) polynomials from Table 9 belong to $\mathcal{L}(\mathcal{B})$. Only polynomials no. 5, 6 and 8 of Table 9 belong to $\mathcal{N}(\mathcal{B})$.
- $\mathcal{U}_{\leq 9}^{spor}$ contains remaining 5 'sporadic' cases from $\mathcal{U}_{\leq 9}^{irr}$; these polynomials are listed in Table 10; $P(-X)$ are omitted. Polynomial no.1 has 2 unimodular roots; no. 2 and 3 have 4 unimodular roots each. All polynomials from Table 10 belong to $\mathcal{L}(\mathcal{B})\backslash\mathcal{N}(\mathcal{B})$.

TABLE 8. Salem polynomials from $\mathcal{U}_{\leq 9}^{1}$.

$P(X) \in \mathcal{B}_{\leq 9}$	$P(-X) \in \mathcal{N}(\mathcal{B})$
$X^4 - X^3 - X^2 - X + 1$	*no*
$X^6 - X^5 - X^4 - X^3 - X^2 - X + 1$	*no*
$X^6 - X^5 - X^4 - X^2 - X + 1$	*no*
$X^6 - X^5 - X^4 + X^3 - X^2 - X + 1$	*yes*
$X^6 - X^5 - X^3 - X + 1$	*yes*
$X^6 - X^4 - X^3 - X^2 + 1$	*yes*
$X^8 - X^7 - X^6 - X^5 - X^3 - X^2 - X + 1$	*no*
$X^8 - X^7 - X^6 - X^4 - X^2 - X + 1$	*no*
$X^8 - X^7 - X^6 - X^2 - X + 1$	*no*
$X^8 - X^7 - X^6 + X^4 - X^2 - X + 1$	*yes*
$X^8 - X^7 - X^5 - X^4 - X^3 - X + 1$	*no*
$X^8 - X^7 - X^5 + X^4 - X^3 - X + 1$	*yes*
$X^8 - X^6 - X^5 - X^3 - X^2 + 1$	*yes*
$X^8 - X^5 - X^4 - X^3 + 1$	*yes*

We end Section 2.5 by exhibiting a few notable examples of $P(X) \in \mathcal{U}_{\leq 9}^{irr}$.

TABLE 9. Complex Salem polynomials $\mathcal{U}^2_{\leq 9}$; $P(-X)$ omitted

#	$P(X) \in \mathcal{B}_{\leq 9}$	$P(-X) \in \mathcal{N}(\mathcal{B})$
1	$X^6 - X^5 + X^4 + X^3 + X^2 - X + 1$	*no*
2	$X^8 - X^7 - X^6 + X^5 + X^4 + X^3 - X^2 - X + 1$	*yes*
3	$X^8 - X^7 + X^5 + X^3 - X + 1$	*yes*
4	$X^8 - X^7 + X^5 + X^4 + X^3 - X + 1$	*no*
5	$X^8 - X^7 + X^6 - X^4 + X^2 - X + 1$	*yes*
6	$X^8 - X^7 + X^6 + X^4 + X^2 - X + 1$	*yes*
7	$X^8 - X^7 + X^6 + X^5 + X^4 + X^3 + X^2 - X + 1$	*no*
8	$X^8 + X^5 + X^4 + X^3 + 1$	*yes*
9	$X^8 + X^6 - X^4 + X^2 + 1$	*no*
10	$X^8 + X^6 + X^5 - X^4 + X^3 + X^2 + 1$	*no*

TABLE 10. Sporadic polynomials from $\mathcal{U}^{spor}_{\leq 9}$; $P(-X)$ omitted

$P(X) \in \mathcal{B}_{\leq 9}$	$P(-X) \in \mathcal{N}(\mathcal{B})$
$X^8 - X^7 + X^6 - X^5 - X^4 - X^3 + X^2 - X + 1$	*no*
$X^8 - X^7 - X^6 + X^5 - X^4 + X^3 - X^2 - X + 1$	*no*
$X^8 - X^6 - X^4 - X^2 + 1$	*no*

Example 10. *Complex Salem polynomials* $P(X) = X^8 - X^7 + X^6 - X^4 + X^2 - X + 1$ *and* $P(-X)$ *belong to* $\mathcal{L}(\mathcal{B}) \cap \mathcal{N}(\mathcal{B})$. *In contrast, complex Salem polynomials* $Q(X) = X^8 - X^7 + X^5 + X^4 + X^3 - X + 1$ *and* $Q(-X)$ *are in* $\mathcal{B} \setminus (\mathcal{L}(\mathcal{B}) \cup \mathcal{N}(\mathcal{B}))$. *Moreover,* $Q(X)$ *and* $Q(-X)$ *are the only polynomials from* $\mathcal{U}^{irr}_{\leq 9}$ *with no Littlewood multiple.*

Example 11. *Sporadic polynomials* $P(X) = X^8 - X^7 - X^6 + X^5 - X^4 + X^3 - X^2 - X + 1$ *and* $P(-X)$ *have 4 unimodular roots and 4 real roots. Sporadic polynomials* $Q(X) = X^8 - X^7 + X^6 - X^5 - X^4 - X^3 + X^2 - X + 1$ *and* $Q(-X)$ *have exactly 2 unimodular roots each. It is notable that* $\{P(\pm X), Q(\pm X)\} \subset \mathcal{L}(\mathcal{B}) \setminus \mathcal{N}(\mathcal{B})$.

3. The algorithm

We develop the algorithm to answer Question 1 for non-separable polynomials. In separable cases, it reduces to previous algorithms in [2, 13, 22].

Lemma 12. *Suppose that* $z \in \mathbb{C}$ *is a root of multiplicity* $m \geq 1$ *of the polynomial* $Q(X) = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0 \in \mathbb{C}[X]$ *of degree* $d \geq 1$, *and that* $|z| \neq 1$. *Let* $j \in \{1, \ldots, d\}$ *and* $R(X) = a_d X^j + a_{d-1} X^{j-1} + \cdots + a_{d-j}$. *Then, for each* $k \in \{0, 1, \ldots, m-1\}$, *the inequality*

$$|R^{(k)}(z)| \leq \frac{k! \cdot H(Q)}{||z|-1|^{k+1}} \tag{3.1}$$

holds.

Here $R^{(k)}$ denotes the kth derivative of the polynomial R, $R^{(0)} := R$, and $H(Q)$ stands for the height of the polynomial Q, namely,

$$H(Q) = \max\{|a_d|, |a_{d-1}|, \dots, |a_1|, |a_0|\}.$$

Proof of Lemma 12. First, assume that $|z| > 1$. Since z is a root of $Q(X)$ of multiplicity m, there exists a polynomial $T(X) \in \mathbb{C}[X]$ such that

$$a_d X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + a_0 = T(X) \cdot (X - z)^m.$$

One has

$$X^{d-j}\left(a_d X^j + a_{d-1}X^{j-1} + \cdots + a_{d-j}\right) + a_{d-j-1}X^{d-j-1} + \cdots + a_0 = T(X)\cdot(X-z)^m,$$

and so

$$R(X) = a_d X^j + a_{d-1}X^{j-1} + \cdots + a_{d-j} = -\tfrac{a_{d-j-1}}{X} - \cdots - \tfrac{a_0}{X^{d-j}} + \tfrac{T(X)\cdot(X-z)^m}{X^{d-j}}.$$

Now fix $k \in \{0, 1, \dots, m-1\}$. One can easily see that the kth derivative of the rational function $T(X) \cdot (X - z)^m / X^{d-j} \in \mathbb{C}(X)$ vanishes at $X = z$. Therefore

$$R^{(k)}(z) = \left(-\tfrac{a_{d-j-1}}{X} - \cdots - \tfrac{a_0}{X^{d-j}}\right)^{(k)}\Big|_{X=z} =$$

$$= (-1)^{k+1}\tfrac{k!\,a_{d-j-1}}{z^{k+1}} + (-1)^{k+1}\tfrac{(k+1)!\,a_{d-j-2}}{1!\,z^{k+2}} + \cdots + (-1)^{k+1}\tfrac{(d+k-j-1)!\,a_0}{(d-j-1)!\,z^{d+k-j}}.$$

From this we obtain

$$\begin{aligned}
|R^{(k)}(z)| &\le H(Q)\left(\tfrac{k!}{|z|^{k+1}} + \tfrac{(k+1)!}{1!\,|z|^{k+2}} + \cdots + \tfrac{(d+k-j-1)!}{(d-j-1)!\,|z|^{d+k-j}}\right) \\
&\le H(Q)\left(\tfrac{k!}{|z|^{k+1}} + \tfrac{(k+1)!}{1!\,|z|^{k+2}} + \cdots + \tfrac{(d+k-j-1)!}{(d-j-1)!\,|z|^{d+k-j}} + \cdots\right) \\
&= H(Q)\,(-1)^k\left(\tfrac{1}{X} + \tfrac{1}{X^2} + \cdots\right)^{(k)}\Big|_{X=|z|} \\
&= H(Q)\,(-1)^k\left(\tfrac{1}{X-1}\right)^{(k)}\Big|_{X=|z|} = \tfrac{k!H(Q)}{(|z|-1)^{k+1}}. \qquad (3.2)
\end{aligned}$$

Now assume that $|z| < 1$. If $k > j = \deg R$ then $R^{(k)}(X) \equiv 0$ and the inequality (3.1) obviously holds. Hence assume that $k \le j$. Then

$$R^{(k)}(z) = \left(a_d X^j + a_{d-1}X^{j-1} + \cdots + a_{d-j}\right)^{(k)}\Big|_{X=z} =$$

$$= \tfrac{j!}{(j-k)!}a_d z^{j-k} + \cdots + \tfrac{(k+1)!}{1!}a_{d-j+k+1}z + k!a_{d-j+k},$$

and therefore

$$\begin{aligned}|R^{(k)}(z)| &\le H(Q)\left(\tfrac{j!}{(j-k)!}|z|^{j-k}+\cdots+\tfrac{(k+1)!}{1!}|z|+k!\right)\\ &\le H(Q)\left(k!+\tfrac{(k+1)!}{1!}|z|+\cdots+\tfrac{j!}{(j-k)!}|z|^{j-k}+\cdots\right)\\ &= H(Q)\,(1+X+X^2+\cdots)^{(k)}\Big|_{X=|z|}\\ &= H(Q)\,\left(\tfrac{1}{1-X}\right)^{(k)}\Big|_{X=|z|}=\tfrac{k!H(Q)}{(1-|z|)^{k+1}}. \qquad (3.3)\end{aligned}$$

The inequality (3.1) follows from (3.2) and (3.3). □

Let $P \in \mathbb{Z}[X]$ be a monic polynomial (that is, the leading coefficient of P is equal to 1). Then one can divide any integer polynomial Q by P in $\mathbb{Z}[X]$: there exist unique integer quotient and remainder polynomials S and R, $\deg R < \deg P$, such that $Q = P \cdot S + R$. The first key observation: polynomials S and R have integer coefficients, provided that P is monic. The second key observation is as follows. For any complex number z which satisfies $P(z) = 0$, one has $Q(z) = R(z)$. This means that the values of the polynomial Q evaluated at any complex root of the divisor polynomial P coincide with the values of the remainder polynomial R evaluated at the same points. The reduction map $Q \mapsto Q \pmod P$ is a homomorphism of rings which maps the ring $\mathbb{Z}[X]$ to the quotient ring $\mathbb{Z}[X]/(P)$. The remainder polynomial R is a representative integer polynomial for the class in $\mathbb{Z}[X]/(P)$ to which Q belongs.

Definition 13. *Let $P(X)$ be a nonconstant polynomial with integer coefficients with no roots on the complex unit circle $|z| = 1$. Suppose that the factorization of P in $\mathbb{C}[X]$ is*

$$P(X) = a \cdot (X-\alpha_1)^{e_1}(X-\alpha_2)^{e_2}\cdots(X-\alpha_s)^{e_s},$$

where $\alpha_1, \alpha_2, \ldots, \alpha_s$ are distinct complex numbers and $e_j \ge 1$ for $j = 1, 2, \ldots, s$. Let B be arbitrary positive number. Define $\mathcal{R}(P, B)$ to be the set of all polynomials $R \in \mathbb{Z}[X]$, $\deg R < \deg P$, which, for each $j \in \{1, 2, \ldots, s\}$, satisfy the inequalities

$$|R(\alpha_j)| \le \tfrac{B}{||\alpha_j|-1|},\ |R'(\alpha_j)| \le \tfrac{1!B}{||\alpha_j|-1|^2}, \cdots, |R^{(e_j-1)}(\alpha_j)| \le \tfrac{(e_j-1)!B}{||\alpha_j|-1|^{e_j}}. \qquad (3.4)$$

Here $R^{(k)}$ denotes the kth derivative of the polynomial R, and $R^{(0)} := R$.

Lemma 14. *Let $P \in \mathbb{Z}[X]$ and $B \in \mathbb{R}$ be as in Definition 13. Then $\mathcal{R}(P, B)$ is a finite set.*

Proof. Write $R(X) = r_{d-1}X^{d-1} + \cdots + r_1X + r_0$, where r_k, $0 \le k \le d-1$ are unknown integers. Denote by $R^{(n)}(X)$ the nth derivative of the polynomial

$R(X)$. Consider the following equalities obtained by substituting $X = \alpha_j$ into $R^{(n)}(X)$, for $j = 1, 2, \dots, s$:

$$
\begin{aligned}
r_0 + r_1\alpha_j + \ r_2\alpha_j^2 + \ & \dots \ + \ r_{d-1}\alpha_j^{d-1} = R(\alpha_j), \\
r_1 \ + 2r_2\alpha_j + \ & \dots \ + (d-1)r_{d-1}\alpha_j^{d-2} = R'(\alpha_j), \\
& \dots \ \dots \ \dots \\
& (e_j-1)!r_{e_j-1} + \dots + \tfrac{(d-1)!}{(d-e_j)!}r_{d-1}\alpha_j^{d-e_j} = R^{(e_j-1)}(\alpha_j).
\end{aligned} \tag{3.5}
$$

Write it in the matrix form $A\mathbf{x} = \mathbf{y}$, where

$$
\mathbf{x} = (r_0, r_1, \dots, r_{d-1})^t, \quad \mathbf{y} = \left(R(\alpha_1), R'(\alpha_1), \dots, R^{(e_s-1)}(\alpha_s)\right)^t
$$

and the system matrix A is the confluent Vandermonde matrix which consists of row-blocks ($j = 1, 2, \dots, s$)

$$
\begin{array}{ccccccc}
1 & \alpha_j & \alpha_j^2 & \cdots & & & \alpha_j^{d-1} \\
0 & 1 & 2\alpha_j & \cdots & & & (d-1)\alpha_j^{d-2} \\
0 & 0 & 2 & \cdots & & & (d-1)(d-2)\alpha_j^{d-3} \\
 & & \cdots & \cdots & & & \cdots \\
0 & 0 & \cdots & (e_j-1)! & e_j!\alpha_j & \cdots & \frac{(d-1)!}{(d-e_j)!}\alpha_j^{d-e_j}
\end{array}
$$

(each row in this block, except for the first one, is the derivative in α_j of the previous row). Denote by $D(\alpha_1^{e_1}, \alpha_2^{e_2}, \dots, \alpha_s^{e_s})$ the determinant of the confluent Vandermonde matrix A. It is well-known (see, for instance, [1, Chapter VI], [10, Chapter 6], [12] and [14]) that

$$
D(\alpha_1^{e_1}, \alpha_2^{e_2}, \dots, \alpha_s^{e_s}) = \prod_{i<j}(\alpha_j - \alpha_i)^{e_i e_j} \prod_{k=1}^{s}(e_k - 1)!!,
$$

where $n!!$ stands for the product $n!(n-1)! \cdots 2!\, 1!$. In particular, $\det(A) \neq 0$, since $\alpha_1, \alpha_2, \dots, \alpha_s$ are distinct complex numbers. So the inverse matrix A^{-1} exists and $\mathbf{x} = A^{-1}\mathbf{y}$. By Cramer's formula,

$$
r_k = \tfrac{1}{\det(A)}\left(R(\alpha_1)A_{1\,k+1} + \dots + R^{(e_1-1)}(\alpha_1)A_{e_1\,k+1} + \dots + R^{(e_s-1)}(\alpha_s)A_{d\,k+1}\right),
$$

for $k = 0, 1, \dots, d-1$, where A_{lm}, $1 \le l, m \le d$ are the cofactors of the matrix A.

Now, let B be arbitrary positive number and assume that $R \in \mathcal{R}(P, B)$. Then in view of (3.4) we have

$$
|r_k| \le \tfrac{B}{|\det(A)|}\left(\tfrac{|A_{1\,k+1}|}{||\alpha_1|-1|} + \dots + \tfrac{(e_1-1)!|A_{e_1\,k+1}|}{||\alpha_1|-1|^{e_1}} + \dots + \tfrac{(e_s-1)!|A_{d\,k+1}|}{||\alpha_s|-1|^{e_s}}\right),
$$

for $k = 0, 1, \dots, d-1$. Therefore the number of solutions $\mathbf{x} \in \mathbb{Z}^d$ to (3.5), satisfying the condition (3.4), is finite, i.e., the set $\mathcal{R}(P, B)$ is finite. □

We now define a certain graph which is associated to the set of remainder polynomials and the digit set $\mathcal{D}$.

Definition 15. *Let $\mathcal{G} = \mathcal{G}(P, \mathcal{D})$ be a directed graph whose vertices represent all the distinct polynomials $R \in \mathcal{R}(P, B) \cup \mathcal{D}$, where $B = \max\{|b| : b \in \mathcal{D}\}$. We connect the vertices which represent two remainder polynomials R_i and R_j, by an edge which points from R_i to R_j, if $R_j \equiv X \cdot R_i + b \pmod P$ in $\mathbb{Z}[X]/(P)$ for some digit $b \in \mathcal{D}$.*

Here is the main theorem of this section.

Theorem 16. *Let $P \in \mathbb{Z}[X]$ be a monic polynomial with no roots on the complex unit circle $|z| = 1$. Then P divides an integer polynomial*

$$Q(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{C}[X]$$

with all the coefficients $a_j \in \mathcal{D}$ and the leading coefficient $a_n \in \mathcal{D}$, if and only if the graph $\mathcal{G} = \mathcal{G}(P, \mathcal{D})$ contains a path which starts at the remainder polynomial $R(X) = a_n$ and ends at $R(X) = 0$. The length of the path is n, where n is the degree of Q.

Proof. Let us first prove the necessity. Assume that P divides Q, that is, $Q(X) \equiv 0 \pmod P$. Define the polynomials

$$\begin{aligned}
Q_0(X) &= a_n, \\
Q_1(X) &= a_n X + a_{n-1}, \\
Q_2(X) &= a_n X^2 + a_{n-1} X + a_{n-2}, \\
&\cdots \\
Q_n(X) &= a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0.
\end{aligned}$$

Let R_j be the remainder of Q_j modulo P. Suppose that the factorization of P in $\mathbb{C}[X]$ is

$$P(X) = a \cdot (X - \alpha_1)^{e_1} (X - \alpha_2)^{e_2} \cdots (X - \alpha_s)^{e_s},$$

where $\alpha_1, \alpha_2, \ldots, \alpha_s$ are distinct complex numbers and $e_j \geq 1$ for $j = 1, 2, \ldots, s$. By Lemma 12, each polynomial Q_i, $i = 1, 2, \ldots, n$, satisfies the inequalities

$$|Q_i(\alpha_j)| \leq \tfrac{H(Q)}{||\alpha_j|-1|}, \ |Q_i'(\alpha_j)| \leq \tfrac{1!H(Q)}{||\alpha_j|-1|^2}, \cdots, |Q_i^{(e_j-1)}(\alpha_j)| \leq \tfrac{(e_j-1)!H(Q)}{||\alpha_j|-1|^{e_j}}, \tag{3.6}$$

for $j = 1, 2, \ldots, s$. Moreover, for each $j \in \{1, 2, \ldots, s\}$ and each $i \in \{1, 2, \ldots, n\}$, $R_i^{(k)}(\alpha_j) = Q_i^{(k)}(\alpha_j)$, $0 \leq k \leq e_j - 1$, since $R_i \equiv Q_i \pmod P$. Therefore, in view of (3.6), R_i all belong to the set $\mathcal{R}(P, B)$, where $B = H(Q)$. Reducing modulo P the equality $Q_i = X \cdot Q_{i-1} + a_{n-i}$ with $a_{n-i} \in \mathcal{D}$ yields $R_i \equiv X \cdot R_{i-1} + a_{n-i} \pmod P$. Hence, there exists an edge in the graph $\mathcal{G}$ which connects R_{i-1} to R_i. Since $Q_n(X) = Q(X) \equiv 0 \pmod P$, one has $R_n = 0$. Consequently, there exists a path in $\mathcal{G}$ which joins $R_0 = a_n$ to the reminder polynomial $R_n = 0$.

Conversely, assume that there exists a path of length n which connects the $n + 1$ vertices $R_0, R_1, \ldots, R_n$ with $R_0 = a_n$ and $R_n = 0$. By the definition

of the graph $\mathcal{G}$, there exist coefficients $a_i \in \mathcal{D}$, $i = 1, \ldots, n$, such that $R_i \equiv X \cdot R_{i-1} + a_{n-i} \pmod{P}$. Recursively define the polynomials $Q_0 := R_0 = a_n$, $Q_i := X \cdot Q_{i-1} + a_{n-i}$ for $i = 1, 2, \ldots, n$. By the definition, $Q_i \equiv R_i \pmod{P}$. Then the polynomial $Q(X) := Q_n(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ has all the coefficients $a_i \in \mathcal{D}$, and $Q_n(X)$ is divisible by P in $\mathbb{Z}[X]$. □

By Lemma 14, the graph $\mathcal{G} = \mathcal{G}(P, \mathcal{D})$ is finite. Thus, the polynomial Q with the coefficients in the set $\mathcal{D}$ may be found by running any path finding algorithm on $\mathcal{G}$. For performance reasons, depth-first search was used.

Algorithm 1. *Determines whether $P \in \mathbb{Z}[X]$ has a multiple $Q \in \mathcal{D}[X]$ with leading coefficient $a \in \mathcal{D}$.*

Input: *a monic polynomial $P \in \mathbb{Z}[X]$, the finite digit set $\mathcal{D} \subset \mathbb{Z}$, the leading coefficient $a \in \mathcal{D}$, $a \neq 0$.*
Output: *a polynomial $Q \in \mathcal{D}[X]$ or $\varnothing$, if such Q does not exist*
Variables: *the set $\mathcal{V}$ of visited vertices of the directed graph $\mathcal{G} = \mathcal{G}(P, \mathcal{D})$, the set $\mathcal{E}$ of edges that join vertices of $\mathcal{V}$, found - boolean variable.*
Method: *Depth-first search using Theorem 16.*

```
Step 1: set V = {a}, E = ∅
Step 2: set found := False
Step 3: call do_search(a, found)
Step 4: if found then print a
          else print ∅
        end if
Step 5: stop.
procedure do_search(local var R ∈ Z[X], global var found):
    local var S ∈ Z[X]
    if R = 0 then
        set found := True
    else
        for each d ∈ D do
            compute S := X · R + d (mod P).
            if S ∉ V and S ∈ R(P, B), where B := max{|d| : d ∈ D} then
                add S to V
                add d as an edge from R to S to E
                call do_search(S, found)
            end if
            if found then
                print digit d
                break loop
            end if
        end do
    end if
end proc
```

Note. If a polynomial $P(X) \in \mathbb{Z}[X]$ has unimodular roots we can exclude them from (3.4) and try to build the graph $\mathcal{G}(P, \mathcal{D})$. If the resulting graph is finite then we can still answer Question 1 for such polynomials.

4. Computations

Assume that $p(X)$ is a nonzero polynomial with integer coefficients and recall that *the content* of $p(X)$ is the greatest common divisor of all of its coefficients. Suppose we have a factorization $p(X) = a \cdot C(X)N(X)$, where $a \in \mathbb{Z}$, $C(X), N(X) \in \mathbb{Z}[X]$, the polynomial $C(X)$ is a product of cyclotomic polynomials, whereas the polynomial $N(X)$ has no cyclotomic divisors, the content of $N(X)$ equals 1 and the leading coefficient of $N(X)$ is a positive integer. Then $N(X)$ is called *the noncyclotomic part of* $p(X)$ and the polynomial $C(X)$ is called the *cyclotomic part of* $p(X)$. Note that the noncyclotomic part of a polynomial is uniquely determined.

The set $\mathcal{B}_{\le 9}$ is the union of the following disjoint subsets (see Table 11):

- $\mathcal{C}$ – the set of polynomials from $\mathcal{B}_{\le 9}$ which are products of cyclotomic polynomials;
- $\mathcal{F}^1$ – the set of polynomials from $\mathcal{B}_{\le 9}$ whose noncyclotomic part is an irreducible nonconstant polynomial;
- $\mathcal{F}^2$ – the set of polynomials from $\mathcal{B}_{\le 9}$ whose noncyclotomic part is the product of two distinct monic irreducible nonconstant polynomials;
- $\mathcal{M}$ – the set of polynomials from $\mathcal{B}_{\le 9}$ whose noncyclotomic part is the square of a monic irreducible nonconstant polynomial.

The same classification of the elements of $\mathcal{B}_d$ is also valid for degrees $d = 10$ and 11, but no longer holds for $\mathcal{B}_{12}$. The numbers (computed with SAGE [23]) $\#\mathcal{B}_d$, $\#\mathcal{C}_d$, $\#\mathcal{F}^1_d$, $\#\mathcal{F}^2_d$, $\#\mathcal{M}_d$, for $d \in \{1, 2, \ldots, 9\}$, are given in Table 11. (Recall that $\mathcal{A}_d$ denotes the set of polynomials from $\mathcal{A}$ of degree d.) In particular, $\#\mathcal{B}_{\le 9} = 39364$.

Table 11. Partition of the set $\mathcal{B}_{\le 9}$.

d	$\#\mathcal{B}_d$	$\#\mathcal{C}_d$	$\#\mathcal{F}^1_d$	$\#\mathcal{F}^2_d$	$\#\mathcal{M}_d$
1	4	4	0	0	0
2	12	8	4	0	0
3	36	12	24	0	0
4	108	20	88	0	0
5	324	32	292	0	0
6	972	48	892	32	0
7	2916	68	2784	64	0
8	8748	96	8352	292	8
9	26244	136	25228	880	0

We implemented Algorithm 1 in C using library Arb [11] for arbitrary-precision floating-point ball arithmetic and ran it on the SGI Altix 4700 server at Vilnius University. We used OpenMP [17] for an implementation of multiprocessing. For every Borwein polynomial $p(X)$ of degree at most 9 we calculated whether it divides some Littlewood polynomial as well as whether $p(X)$ divides some Newman polynomial. Moreover, for every Newman polynomial of degree at most 11 we calculated whether it has a Littlewood multiple. We will briefly explain how these calculations were organized.

First, note that in view of Proposition 18 a polynomial $P(X) \in \mathbb{Z}[X]$ divides some Littlewood polynomial if and only if its noncyclotomic part divides some Littlewood polynomial. Similarly, if $P(1) \neq 0$ then $P(X)$ has a Newman multiple if and only if its noncyclotomic part has a Newman multiple. (Note that Newman polynomials do not have nonnegative real roots.) Therefore when considering the statements $P(X) \in \mathcal{L}(\mathcal{B})$ and $P(X) \in \mathcal{N}(\mathcal{B})$ we can omit the cyclotomic part of the polynomial $P(X)$. Also, by Proposition 18, if $P(X) \in \mathcal{C}$ then $P(X)$ divides some Littlewood polynomial; $P(X) \in \mathcal{C}$ divides some Newman polynomial if and only if $P(1) \neq 0$.

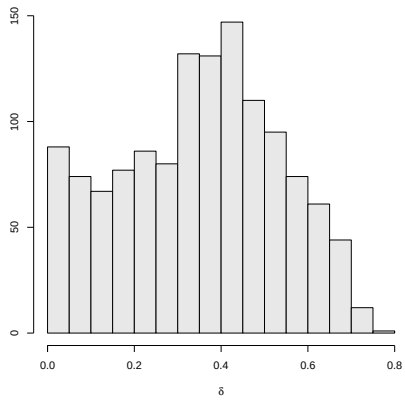
For each noncyclotomic irreducible factor of polynomials from $\mathcal{B}_{\leq 9}$ we ran our algorithm and calculated whether it had a Littlewood multiple and whether it had a Newman multiple. This allowed us to easily verify the statements $P(X) \in \mathcal{L}(\mathcal{B})$ and $P(X) \in \mathcal{N}(\mathcal{B})$ for polynomials $P(X) \in \mathcal{F}^1$. Further, when considering the statement $P(X) \in \mathcal{L}(\mathcal{B})$ we omitted those polynomials $P(X)$ from $\mathcal{F}^2$ and $\mathcal{M}$ which had a noncyclotomic irreducible factor that does not divide any Littlewood polynomial. The procedure for calculating Newman multiples was the same. Finally, we ran our algorithm for noncyclotomic parts of the remaining polynomials from $\mathcal{F}^2$ and $\mathcal{M}$.

We used the following fact to decide that a polynomial has no Newman multiple. Odlyzko and Poonen [16] proved that roots of Newman polynomials are contained in the annulus $1/\tau < |z| < \tau$, where $\tau = (1+\sqrt{5})/2 \approx 1.61803$ is the golden ratio. There are exactly 376 Borwein polynomials of degree at most 9 that have unimodular roots which are not roots of unity. For every such polynomial we ran Algorithm 1 and omitted unimodular roots when checking the condition (3.4) (see the note after Algorithm 1). We succeeded in deciding whether these polynomials belong to $\mathcal{L}(\mathcal{B})$ and $\mathcal{N}(\mathcal{B})$.

Note that $B = \max\{|a| \mid a \in \mathcal{D}\} = 1$ in case of Littlewood and Newman multiples. We introduced a new variable $0 \leq \delta < 1$ to hasten the search for polynomials in $\mathcal{L}(\mathcal{B}_{\leq 9})$ and $\mathcal{N}(\mathcal{B}_{\leq 9})$, see Figure 1. For a given δ we replaced B in the inequalities (3.4) of Section 3 by $B - \delta$. This eliminates some of the vertices in the original graph $\mathcal{G}(P, \mathcal{D})$. We start with the initial value $\delta = 0.95$. If a Littlewood (or Newman) multiple is found then we are done. Otherwise we decrease δ by 0.05 and try again. Note that for polynomials in

$\mathcal{B}\backslash\mathcal{L}(\mathcal{B})$ and $\mathcal{B}\backslash\mathcal{N}(\mathcal{B})$ the variable δ always reaches the value $\delta = 0$ in order to construct the full graph $\mathcal{G}(P, \mathcal{D})$.

FIGURE 1. Distribution of noncyclotomic factors $F(X)$ of polynomials from $\mathcal{B}_{\leq 9}$ such that $F(X) \in \mathcal{L}(\mathbb{Z}[X])$.



The above mentioned computations took approximately 296 hours of CPU time. The maximum recursion depth reached when searching for Littlewood multiples was 57 767, whereas for Newman multiples it was 825. For instance, it took approximately 119 minutes of CPU time to run our algorithm to decide that the polynomial $X^9 + X^8 - X^7 - X^5 + X^3 + X^2 - 1$ has no Littlewood multiple. The graph $\mathcal{G}(P, \mathcal{D})$, constructed for this polynomial, contained 1 428 848 vertices. The maximal recursion depth reached for this polynomial was 471. On the other hand, it took 92 minutes of CPU time to find a Littlewood multiple for the polynomial $X^9 - X^8 + X^7 + X^6 - X^5 + X^4 - X^3 + X - 11$. The graph $\mathcal{G}(P, \mathcal{D})$, constructed for this polynomial, contained 9 372 425 vertices and the maximal recursion depth was 43554.

4.1. **Omitting cyclotomic factors.** Given a set X of numbers denote by $-X$ the set $\{-x \mid x \in X\}$.

Lemma 17. *Let $\Phi_n(X)$ be the n-th cyclotomic polynomial. If a positive integer t is not divisible by n then $\Phi_n(X)$ divides the polynomial $X^{(n-1)t} + X^{(n-2)t} + \cdots + X^t + 1$.*

Proof. By applying formula $X^m - 1 = \prod_{d|m} \Phi_d(X)$, which is valid for every positive integer m, we obtain that $X^t - 1$ is not divisible by $\Phi_n(X)$, because t is not a multiple of n. Hence $\Phi_n(X)$ and $X^t - 1$ are coprime, since $\Phi_n(X)$ is irreducible.

Obviously, $X^n - 1$ divides $X^{nt} - 1$, and therefore $\Phi_n(X)$ divides $X^{nt} - 1$. On the other hand, $X^{nt} - 1$ factors as

$$X^{nt} - 1 = (X^t - 1)(X^{(n-1)t} + X^{(n-2)t} + \cdots + X^t + 1).$$

Since $\Phi_n(X)$ is coprime to X^t-1, we obtain that $\Phi_n(X)$ divides the polynomial $X^{(n-1)t}+X^{(n-2)t}+\cdots+X^t+1$. □

The following proposition shows that under certain conditions, we can omit its cyclotomic divisors $\Phi_n(X)$, $n>1$ from polynomial $P(X)$ in Problem 1.

Proposition 18. *Let $\mathcal{D}\subset\mathbb{Z}$ be nonempty set. Suppose that $\mathcal{D}$ satisfies at least one of the two conditions: $0\in\mathcal{D}$ or $\mathcal{D}=-\mathcal{D}$. If $P\in\mathbb{Z}[X]$ divides some nonzero polynomial with coefficients from $\mathcal{D}$, then for every positive integer $n>1$, the product $P(X)\Phi_n(X)$, where $\Phi_n(X)$ is the n-th cyclotomic polynomial, also divides some nonzero polynomial with coefficients from $\mathcal{D}$.*

In case $\mathcal{D}=-\mathcal{D}$, this is also true for $n=1$: $P(X)(X-1)$ has a non-zero multiple with coefficients from $\mathcal{D}$.

Proof. Suppose that there exists a nonzero polynomial $R\in\mathbb{Z}[X]$ whose all the coefficients are in $\mathcal{D}$ and which is a multiple of P. Let d be the degree of R. Assume that $0\in\mathcal{D}$ and choose an integer $t\geq d+1$, which is not divisible by n (e.g., $t=dn+1$). Then all the coefficients of the polynomial

$$R(X)(X^{(n-1)t}+X^{(n-2)t}+\cdots+X^t+1) \tag{4.1}$$

lie in $\mathcal{D}$. Moreover, this polynomial is divisible by the product $P\Phi_n$, since P divides R and, by Lemma 17, $X^{(n-1)t}+X^{(n-2)t}+\cdots+X^t+1$ is a multiple of $\Phi_n(X)$. This completes the proof of the proposition in the case when $0\in\mathcal{D}$.

Assume that $\mathcal{D}=-\mathcal{D}$. If n divides $d+1$ then, obviously, X^n-1 divides $X^{d+1}-1$, and therefore $X^{d+1}-1$ is a multiple of Φ_n. Since $\mathcal{D}=-\mathcal{D}$, all the coefficients of the polynomial $R(X)(X^{d+1}-1)$ lie in $\mathcal{D}$ and we are done in this case. If $d+1$ is not a multiple of n then, by Lemma 17, $\Phi_n(X)$ divides the polynomial $X^{(n-1)(d+1)}+X^{(n-2)(d+1)}+\cdots+X^{d+1}+1$. Finally, note that all the coefficients of the polynomial (4.1) lie in $\mathcal{D}$ and this polynomial is divisible by the product $P\Phi_n$.

As for the second part of the Proposition, note that if $\mathcal{D}=-\mathcal{D}$ then the polynomial $R(X)(X^{d+1}-1)$ is divisible by $P(X)(X-1)$ and all of its coefficients belong to $\mathcal{D}$. □

References

[1] A.C. Aitken, *Determinants and matrices,* 9th ed. Interscience Pub., New York, 1956.

[2] S. Akiyama, J. M. Thuswaldner, T. Zaïmi, *Comments on the height reducing property II*, Indag. Math. **26** (1) (2015), 28–39.

[3] M. Amara, *Ensembles fermés de nombres algébriques*, Ann. Sci. Ecole Norm. Sup. **83** (3) (1966), 215–270.

[4] P. Borwein, K. G. Hare, *Some computations on the spectra of Pisot and Salem numbers*, Math. Comp. **71** (238) (2002), 767–780.

[5] D. W. Boyd, *Pisot and Salem numbers in intervals of the real line*, Math. Comp. **32** (144) (1978), 1244–1260.

[6] D. W. Boyd, *Pisot numbers in a neighbourhood of a limit point, I*, J. Number Theory **21** (1) (1985), 17–43.
[7] A. Dubickas, J. Jankauskas, *On Newman polynomials that divide no Littlewood polynomial*, Math. Comp., **78** (265) (2009), 327–344.
[8] J. Dufresnoy, Ch. Pisot, *Étude de certaines fonctions méromorphes bornées sur le cercle unité. Application à un ensemble fermé d'entiers algébriques*, Annales scientifiques de l'É.N.S. 3^e série, **72** (1) (1955), 69–92.
[9] K. G. Hare, M. J. Mossinghoff, *Negative Pisot and Salem numbers as roots of Newman polynomials*, Rocky Mountain J. Math. **44** (1) (2014), 113–138.
[10] R.A. Horn, C.R. Johnson, *Topics in matrix analysis,* 1st pbk edition with corr., Cambridge: Cambridge University Press, 1994.
[11] F. Johansson, *Arb: a C library for ball arithmetic*, ACM Communications in Computer Algebra **47** (4) (2013), 166-169, `http://fredrikj.net/arb/`.
[12] D. Kalman, *The generalized Vandermonde matrix,* Math. Mag. **57** (1984) 15–21.
[13] Ka-Sing Lau, *Dimension of a family of singular Bernoulli convolutions*, J. Funct. Anal. **116** (1993), 335–358.
[14] C. Méray, *Sur un déterminant dont celui de Vandermonde n'est qu'un cas particulier,* Rev. math. spéc. **9** (1899), 217–219.
[15] M. Mossinghoff, *Polynomials with restricted coefficients and prescribed noncyclotomic factors,* LMS J. Comput. Math. **6** (2003), 314–325.
[16] A. M. Odlyzko, B. Poonen, *Zeros of polynomials with 0,1 coefficients*, Enseign. Math., (2) **39**, (1993) no.3–4, 317–384.
[17] OpenMP Architecture Review Board, OpenMP Application Program Interface Version 4.0, 2013, `http://www.openmp.org/mp-documents/OpenMP4.0.0.pdf`
[18] C. Pisot, *La répartition modulo* 1 *et les nombres algébriques*, Ann. Scuola Norm. Super. Pisa **7** (2) (1938), 205–248.
[19] R. Salem, *A remarkable class of algebraic integers. Proof of a conjecture of Vijayaraghavan.*, Duke Math. J. **11**, (1944). 103–108.
[20] R. Salem, *Power series with integral coefficients*, Duke Math. J. **12**, (1945). 153–172.
[21] R. Salem, *Algebraic numbers and Fourier analysis*, D. C. Heath and Co., Boston, Mass., 1963.
[22] D. Stankov, *On spectra of neither Pisot nor Salem algebraic integers*, Monatsh. Math. **159** (2010), 115–131.
[23] W. A. Stein et al., *Sage Mathematics Software (Version 7.2)*, The Sage Development Team, 2016, http://www.sagemath.org.

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

Mathematik und Statistik, Montanuniversität Leoben, Franz Josef Strasse 18, A-8700 Leoben, Austria
E-mail address: `jonas.jankauskas@gmail.com`

Department of Mathematics and Informatics, Vilnius University, Naugarduko 24, Vilnius LT-03225, Lithuania
E-mail address: `jonas.siurys@mif.vu.lt`