Vilnius University

Properties of Polynomials of Small Height

Grintas Junevičius

DOCTORAL DISSERTATION
2025

Natural Sciences
Mathematics **N 001**

https://doi.org/10.15388/vu.thesis.728
https://orcid.org/0009-0003-6034-3398

VILNIUS UNIVERSITY

Grintas Junevičius

Properties of Polynomials of Small Height

DOCTORAL DISSERTATION

Natural Sciences,
Mathematics (N 001)

VILNIUS 2025

The dissertation was prepared between 2019 and 2024 at Vilnius University.

Academic Supervisor - Prof. Dr. Paulius Drungilas (Vilnius University, Natural Sciences, Mathematics – N 001).
Academic Consultant - Prof. Habil. Dr. Artūras Dubickas (Vilnius University, Natural Sciences, Mathematics – N 001).

Dissertation Defence Panel:
Chairman - Prof. Dr. Jonas Šiaulys (Vilnius University, Natural Sciences, Mathematics - N 001).
Members:
Prof. Habil. Dr. Artūras Dubickas (Vilnius University, Natural Sciences, Mathematics - N 001),
Prof. Habil. Dr. Antanas Laurinčikas (Vilnius University, Natural Sciences, Mathematics - N 001),
Prof. Dr. Alar Leibak (Tallinn University of Technology, Natural Sciences, Mathematics - N 001),
Prof. Dr. Jurgita Markevičiūtė (Vilnius University, Natural Sciences, Mathematics - N 001).

The dissertation shall be defended at a public meeting of the Dissertation Defence Panel at 15:00 on February 28, 2025, in room 201 of the Faculty of Mathematics and Informatics at Vilnius University. Address: Naugarduko str. 24, LT03225 Vilnius, Lithuania; phone: +37052193050; email: mif@mif.vu.lt.
The text of this dissertation is available at the Vilnius University library and on its website:
https://www.vu.lt/naujienos/ivykiu-kalendorius

https://doi.org/10.15388/vu.thesis.728
https://orcid.org/0009-0003-6034-3398

VILNIAUS UNIVERSITETAS

Grintas Junevičius

Mažo aukščio polinomų savybės

DAKTARO DISERTACIJA

Gamtos mokslai,
matematika (N 001)

VILNIUS 2025

Disertacija rengta 2019 – 2024 metais Vilniaus universitete.

Mokslinis vadovas - prof. dr. Paulius Drungilas (Vilniaus universitetas, gamtos mokslai, matematika – N 001).

Mokslinis konsultantas - prof. habil. dr. Artūras Dubickas (Vilniaus universitetas, gamtos mokslai, matematika – N 001).

Gynimo taryba:

Pirmininkas - prof. dr. Jonas Šiaulys (Vilniaus universitetas, gamtos mokslai, matematika - N 001).

Nariai:

prof. habil. dr. Artūras Dubickas (Vilniaus universitetas, gamtos mokslai, matematika - N 001),

prof. habil. dr. Antanas Laurinčikas (Vilniaus universitetas, gamtos mokslai, matematika - N 001),

prof. dr. Alar Leibak (Talino technikos universitetas, gamtos mokslai, matematika - N 001),

prof. dr. Jurgita Markevičiūtė (Vilniaus universitetas, gamtos mokslai, matematika - N 001).

Disertacija ginama viešame Gynimo tarybos posėdyje 2025m. vasario mėn. 28 d. 15:00 Vilniaus universiteto Matematikos ir informatikos fakultete, 201 auditorijoje. Adresas: Naugarduko g. 24, LT03225 Vilnius, Lietuva; tel. +37052193050; el. paštas mif@mif.vu.lt.

Disertaciją galima peržiūrėti Vilniaus universiteto bibliotekoje ir Vilniaus universiteto interneto svetainėje adresu:

https://www.vu.lt/naujienos/ivykiu-kalendorius

Contents

Notation

$\mathbb{Z}$	Set of integers
$\mathbb{N}$	Set of positive integers
$\mathbb{Q}$	Set of rational numbers
$\mathbb{R}$	Set of real numbers
$\mathbb{C}$	Set of complex numbers
$\mathcal{B}$	Set of Borwein polynomials (coefficients in $\{-1, 0, 1\}$)
$\mathcal{N}$	Set of Newman polynomials (coefficients in $\{0, 1\}$)
$\mathcal{L}$	Set of Littlewood polynomials (coefficients in $\{-1, 1\}$)
P, Q	Polynomials
j, k, l, m, n	Positive integers
z	A complex variable
x	A real variable
$\lfloor x \rfloor$	*Floor*: the largest integer $\leqslant x$, where $x \in \mathbb{R}$
$\lceil x \rceil$	*Ceiling*: the smallest integer $\geqslant x$, where $x \in \mathbb{R}$
$\text{lcm}(e_1, e_2, \ldots, e_n)$	The least common multiple of positive integers $e_1, e_2, \ldots, e_n$
$\gcd(e_1, e_2, \ldots, e_n)$	The greatest common divisor of positive integers $e_1, e_2, \ldots, e_n$
$\mathbb{F}_2$	Finite field with two elements
$N(P)$	The number of roots of polynomial P inside the unit circle $\lvert z \rvert = 1$
$U(P)$	The number of roots of polynomial P on the unit circle $\lvert z \rvert = 1$
$\phi_n(z)$	N-th cyclotomic polynomial
$\deg_2 p$	As defined in Section 2.2

Chapter 1

Introduction

The central subject of this dissertation is polynomials with bounded coefficients. A polynomial

$$P(z) = a_d z^d + a_{d-1} z^{d-1} + \cdots + a_1 z + a_0 \in \mathbb{Z}[z] \tag{1}$$

with a non-zero constant term a_0 is called a *Borwein polynomial*, if $a_j \in \{-1, 0, 1\}$ for each $0 \leqslant j \leqslant d$. In the first chapter, we present the main problems considered in this thesis and give an overview of related research and historical results. In the second chapter, we analyse two subsets of Borwein polynomials and look into their multiplicative properties and relations. The third chapter is dedicated to the problem of finding Borwein trinomials with special numbers as their roots.

1.1 Actuality

Understanding polynomial properties and their behaviour is crucial because they form the foundation of algebra and are essential in both theoretical and applied mathematics, as well as real-world problems in physics, engineering, and economics. Specifically, polynomials of small height often appear in Diophantine equations, approximation theory, control theory, algebraic geometry, and lattice-based cryptography. For example, in NTRU[1] encryption, a widely studied lattice-based cryptosystem, Borwein polynomials are used to create public and private keys [39, 38]. Many algorithms perform better with small-height polynomials because of the reduced complexity of the computa-

[1] Nth-degree Truncated Polynomial Ring Unit

tions.

Similarly, Pisot numbers (see the definition after Theorem 2.4 in Section 1.3) have applications across various mathematical disciplines due to their unique algebraic and analytical properties. Pisot numbers are closely related to problems in algebraic number theory and field theory, Diophantine approximation, dynamic systems, and fractal geometry.

1.2 Aims and problems

The aim of the dissertation is to understand the properties and behaviour of certain polynomials with restricted coefficients. In particular, we look at two subsets of Borwein polynomials – *Littlewood polynomials*, which have all coefficients from the set $\{-1, 1\}$ and *Newman polynomials* with all coefficients equal to 0 or 1. The problems considered are the following.

1. Let $\mathcal{D} \subset \mathbb{Z}$ be a finite set. Given a polynomial $P \in \mathbb{Z}[z]$, does there exist a non-zero polynomial with coefficients in $\mathcal{D}$ which is divisible by P?

2. Does there exist a Newman quadrinomial with no Littlewood multiple?

3. Which Littlewood polynomials possess Newman multiples?

4. Which Newman polynomials P have a Littlewood multiple of degree $\deg_2 \widetilde{P} - 1$? (For more details, see Section 2.2.)

5. Identify all Borwein trinomials that have complex Pisot numbers as roots.

1.3 Literature review and the main results

The study of polynomials with bounded coefficients and their root distributions has a long and rich history, with numerous contributions made over the years. The relationship between the coefficients' bounds and the distribution of the roots is particularly interesting. Results have shown that tighter bounds on the coefficients often lead to more constrained root locations [55]. This relationship has profound implications for the design and analysis of polynomials in various applications, such as diophantine equations and signal processing.

The first significant study in this area appears to be conducted by Bloch and Pólya [6] in 1934. Their work explored polynomials with coefficients restricted to {-1, 0, 1}, now known as Borwein polynomials (see, e.g., [21], [43]), and analysed the maximum number of real zeros in the open interval $0 < x < 1$.

Almost a century later, the interest in Borwein polynomials has not faded, we now have numerous results on the reducibility of Borwein polynomials (see, e.g., [30], [46], [49], [61], [43]), their root distribution (see, e.g.,[12], [47], [9], [45]), fractal-like geometry (see, e.g.,[10], [49], [12]), and other algebraic properties (see, e.g.,[48].

In the general case, Question 1 (see section 1.2) is difficult to tackle and has been answered only for specific cases, restricting both the digit set $\mathcal{D}$ and the set of polynomials P. In addition to using algebraic properties, one can approach this problem computationally. Drungilas, Jankauskas and Šiurys [21] implemented an algorithm which can answer this question provided the polynomial $P(z)$ has no roots on the unit circle $|z| = 1$ in the complex plane. They have obtained the complete classification of Borwein polynomials of degrees up to 9 and the digit sets $\mathcal{D} = \{0, 1\}$ and $\mathcal{D} = \{-1, 1\}$.

It seems that the first instance of such an algorithm appeared in the work of Frougny [31] on the digit representations of numbers in algebraic integer bases produced by finite automata. Lau [44] describes a slightly different version of this algorithm used to determine the discreteness property of Bernoulli measures. He answered Question 1 (see Section 1.2) for $\mathcal{D} = \{-1, 0, 1\}$ and the case where $P(z)$ is the minimal polynomial of a Pisot number. Subsequently, Hare and his coauthors [11, 37] used the same algorithm to compute the discrete spectra of Pisot numbers. Stankov [56] considered the spectra of non-Pisot algebraic integers. Akiyama, Thuswaldner and Zaïmi [3, Th. 3] treated Question 1 in the context of *height reducing problem* and devised an algorithm that is essentially similar to that of Frougny [31]. Thus, Question 1 has been fully answered for separable monic polynomials $P(z) \in \mathbb{Z}[z]$ with no roots on the unit circle. In contrast, the implementation developed in [21] is also capable of handling non-separable cases $P(z) \in \mathbb{Z}[z]$ (i.e., when $P(z) \in \mathbb{Z}[z]$ has multiple roots).

The implementation of the algorithm in [21] (see Section 2.4 for details) was used to answer Question 1 for all Borwein polynomials of degree up to 9 and the digit sets $\mathcal{D} = \{0, 1\}$ and $\mathcal{D} = \{-1, 1\}$. More precisely, for every Borwein polynomial of degree at most 9 it was determined whether it has a

Littlewood multiple and whether it divides some Newman polynomial. Moreover, for every Newman polynomial $P(z)$ of degree at most 11 it was checked whether $P(z)$ has a Littlewood multiple. The main result of this paper is the following.

Theorem A ([21]). *Every Borwein polynomial of degree at most 8 which divides some Newman polynomial divides some Littlewood polynomial as well.*

These computations extended the results previously obtained by Dubickas and Jankauskas [25], Borwein and Hare [11], and Hare and Mossinghoff [37].

We extend their calculations even further. We will use $\mathcal{B}$, $\mathcal{N}$, and $\mathcal{L}$ to denote all Borwein, Newman, and Littlewood polynomials, respectively. We say that a polynomial

$$P(z) = a_d z^d + a_{d-1} z^{d-1} + \cdots + a_1 z + a_0 \in \mathbb{Z}[z]$$

is a *trinomial* if it has only three non-zero coefficients a_j, for $0 \leqslant j \leqslant d$. Similarly, if the number of non-zero coefficients is four, $P(z)$ is called a *quadrinomial*.

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

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

Let $\mathcal{A} \subset \mathbb{Z}[z]$. We will use the notation $\mathcal{L}(\mathcal{A})$ to denote the set of polynomials $P(z) \in \mathcal{A}$ that divide some Littlewood polynomial. Similarly, let $\mathcal{N}(\mathcal{A})$ be the set of polynomials $P(z) \in \mathcal{A}$ that divide some Newman polynomial. In particular, the set $\mathcal{N}_d \backslash \mathcal{L}(\mathcal{N})$ consists of those Newman polynomials of degree d that do not divide any Littlewood polynomial, whereas the set $\mathcal{L}_{\leqslant d} \setminus \mathcal{N}(\mathcal{L})$ consists of those Littlewood polynomials of degree at most d that do not divide any Newman polynomial.

Clearly, non-constant polynomials $P(z)$ with all non-negative coefficients cannot have any positive real zeros $z \in [0, \infty)$. Since Newman polynomials

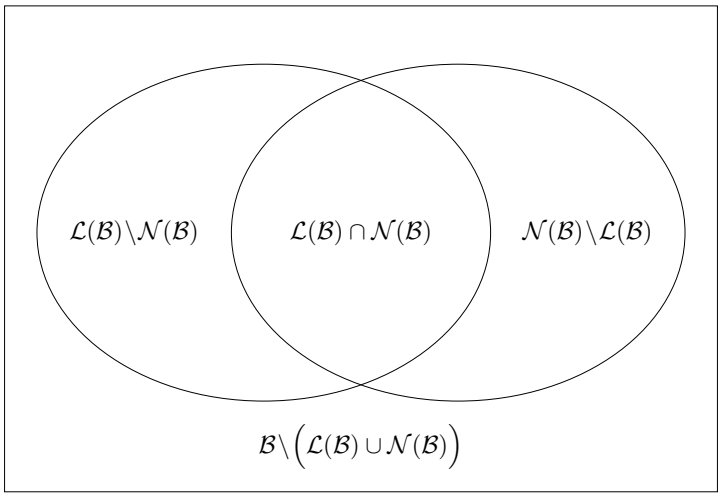


Figure 1.1: Decomposition of the set of Borwein polynomials.

are among such polynomials, it gives us a quick criterion to determine if a Littlewood polynomial has a Newman multiple: If a Littlewood polynomial has a positive real root, we can skip running the algorithm and state that the Newman multiple for it does not exist.

Our computations show that

Theorem 2.2. *Every quadrinomial $Q \in \mathcal{N}_{\leqslant 15}$, except possibly for those given in Table 2.1, divides some Littlewood polynomial. Moreover, every quadrinomial $Q \in \mathcal{N}_{\leqslant 14}$ possesses a Littlewood multiple of smallest possible degree $\deg_2 \widetilde{Q} - 1$ (this quantity is defined in Section 2.2 of Chapter 2).*

Quadrinomial $Q(z)$	$\deg_2 \widetilde{Q} - 1$
$z^{15} + z^{14} + z^{10} + 1$	10921
$z^{15} + z^{12} + z^{10} + 1$	32765
$z^{15} + z^{12} + z^{4} + 1$	31681
$z^{15} + z^{8} + z^{6} + 1$	32765

Table 2.1: Newman quadrinomials $Q \in \mathcal{N}_{\leqslant 15}$ which are not known to have Littlewood multiples (reciprocals omitted).

The second column in Table 2.1 indicates the smallest possible degree of a Littlewood multiple (if it exists) of $Q \in \mathcal{N}_{15}$. In particular, if the quadrinomial $z^{15} + z^8 + z^6 + 1$ divides a Littlewood polynomial $P(z)$, then $\deg P \geqslant 32765$.

Theorem 2.3. *Every polynomial $P(z) \in \mathcal{L}(\mathcal{N}_{\leqslant 10})$, except possibly for those given in Table 2.2, has a Littlewood multiple of smallest possible degree* $\deg_2 \widetilde{P} - 1$.

n	$P_n(z)$	$\deg_2 \widetilde{P_n} - 1$
1	$z^9 + z^8 + z^6 + z^5 + z^4 + z^3 + z + 1$	59
2	$z^{10} + z^9 + z^8 + z^3 + z^2 + 1$	1019
3	$z^{10} + z^9 + z^7 + z^6 + z^5 + 1$	1021

Table 2.2: Polynomials $P(z) \in \mathcal{L}(\mathcal{N}_{\leqslant 10})$ which are not known to have Littlewood multiples of degree $\deg_2 \widetilde{P} - 1$ (reciprocals omitted).

In [21] (see Proposition 18) it was proved that if $P(z)$ is a product of cyclotomic polynomials (with every root of $P(z)$ being a root of unity) and $P(1) \neq 0$ then $P(z)$ divides some Newman polynomial. Therefore Littlewood polynomials which are products of cyclotomic polynomials and do not vanish at $z = 1$ have Newman multiples too. Motivated by this result, we computed the sets $\mathcal{N}(\mathcal{L}_d)$ for small degrees d. By running the algorithm, described in Section 2.4, on every Littlewood polynomial $L(z) \in \mathcal{L}_{\leqslant 12}$, we calculated explicitly all non-trivial elements of the set $\mathcal{N}(\mathcal{L}_{\leqslant 12})$ (see Table 2.3).

Theorem 2.4. *There are exactly* 9 *monic Littlewood polynomials $P(z)$ of degree $\leqslant 12$ that possess Newman multiples and are not themselves the products of cyclotomic polynomials.*

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

Table 2.3: Monic non-trivial elements of $\mathcal{N}(\mathcal{L}_{\leqslant 12})$

In Chapter 2, we expand on our results and provide more details about the algorithm and computations.

To answer Question 5 from Section 1.2 we will first introduce the Pisot numbers. A real algebraic integer $\alpha > 1$ is called a *Pisot number* (after [27, 28]), if all the algebraic conjugates of α over the field of rational numbers $\mathbb{Q}$ (other than α itself) are of absolute value < 1. The minimal polynomial of a Pisot number is called a Pisot polynomial.

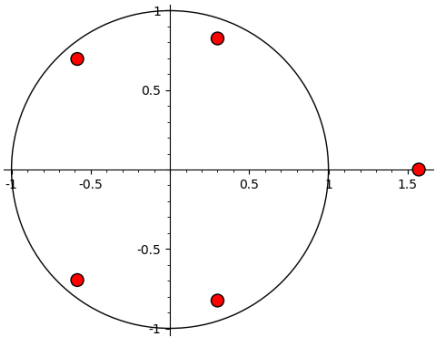


Figure 1.2: Roots of the Pisot polynomial $z^5 - z^4 - z^2 - 1$

Pisot numbers attract a lot of attention in the study of number expansions with algebraic number bases [2, 14], substitution tilings [1, 4, 5], integer sequences with special regard to linear recurrences [15, 17, 16], distributions of fractional parts of powers of real numbers [22, 23], and many other areas [24, 64].

Note that to find polynomials P that have Pisot numbers as roots, it is not necessary to identify all the roots of P. Instead, it is enough to understand how the polynomial roots are distributed in the complex plane in reference to the unit circle. To be exact, it suffices to show that P is divisible by an irreducible polynomial Q, which has exactly one real root greater than 1, and all other roots of absolute value less than 1. In other words, the problem can be formulated in terms of counting polynomial roots in certain regions.

Suppose $P(z)$ splits over the field of complex numbers $\mathbb{C}$ into

$$P(z) = a_n(z - \alpha_1)(z - \alpha_2)\cdots(z - \alpha_n),$$

where the complex zeros $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ of $P(z)$ are not necessarily distinct. The zero counting functions with respect to the unit circle are introduced

through the formulas

$$N(P) = \#\{j,\, 1 \leqslant j \leqslant n : |\alpha_j| < 1\}$$

and

$$U(P) = \#\{j,\, 1 \leqslant j \leqslant n : |\alpha_j| = 1\},$$

where the zeros are counted with the multiplicities.

For example, the Pisot polynomial $P(z) = z^5 - z^4 - z^2 - 1$ in Figure 1.2 has 4 roots inside the unit circle and none on its edge, therefore $N(P) = 4$ and $U(P) = 0$. Note that for Pisot polynomials P, the number $U(P)$ is always zero, and the number $N(P)$ is always one less than the degree of P.

In general, there is no known formula for $N(P)$ and $U(P)$ for arbitrary polynomials. However, some progress has been made for special cases. In [13], these numbers were identified for a subset of Littlewood polynomials:

Theorem B ([13]). *Let $n \geqslant k$ be positive integers with $\gcd(k, n+1) = d$. A polynomial $P(z) \in \{\pm 1\}[z]$ of degree n with one sign change (which occurs between terms z^k and z^{k-1}) has*

$$N(P) = \begin{cases} k & \text{if } n > 2k-1, \\ 0 & \text{if } n = 2k-1, \\ k-d & \text{if } n < 2k-1, \end{cases}$$

and

$$U(P) = \begin{cases} d-1 & \text{if } n \neq 2k-1, \\ n & \text{if } n = 2k-1, \end{cases}$$

roots inside and on the unit circle $|z| = 1$, respectively.

Later, in [35], Hare and Jankauskas focused on finding for which pairs of positive integers (k, n), there exist Newman and Littlewood polynomials of degree n with exactly k roots inside the unit circle $|z| = 1$ and no roots on its edge. The main result of their work is the following theorem about Newman polynomials:

Theorem C ([35]). *For any pair of integers (k, n) with $n \geqslant 7$ and $3 \leqslant k \leqslant n-3$, there exists a polynomial $P(z) \in \{0, 1\}[z]$ of degree n with $N(P) = k$ and $U(P) = 0$.*

For example, given a pair $(5, 8)$, their method can be used to construct a

Newman polynomial $P(z) = z^8 + z^7 + z^5 + z + 1$ of degree 8 with exactly 5 roots inside the unit circle and none on the edge (see Figure 1.3).

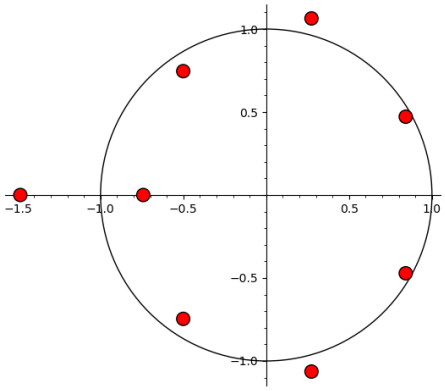


Figure 1.3: $P(z) = z^8 + z^7 + z^5 + z + 1$

Regarding trinomials, more than a century ago, a Latvian mathematician *Piers Bohl* proved the following theorem, which will be essential in proving our results in Section 3.4

Theorem D (Bohl's theorem, [8, 59])**.** *Let $P(z) = z^n + pz^m + q$ be a trinomial, where $p, q \in \mathbb{C}$ and m and n are coprime positive integers such that $n > m$. Assume that for a real number $v > 0$, there exists a triangle with edge lengths v^n, $|p|v^m$ and $|q|$. Let $\alpha = \angle(|p|v^m, |q|)$ and $\beta = \angle(v^n, |q|)$. Then the number of roots of $P(z)$ that reside in the open disc $|z| < v$ is given by the number of integers located in the open interval $(C_f - \delta_f, C_f + \delta_f)$, where*

$$C_f = \frac{n\,(\pi + \arg(p) - \arg(q)) - m\,(\pi - \arg(q))}{2\pi}$$

and

$$\delta_f = \frac{n\alpha + m\beta}{2\pi}.$$

By applying Bohl's theorem we have obtained explicit formulas for the number of roots of Borwein trinomials inside the unit circle.

Proposition 3.3. *Let $n > m$ be coprime positive integers. Then*

$$N(z^n + z^m + 1) = n - m - 1 - 2\left\lfloor \frac{n-2m}{3} \right\rfloor,$$
$$N(z^n + z^m - 1) = 2\left\lceil \frac{n+m}{6} \right\rceil - 1,$$
$$N(z^n - z^m + 1) = 2\left\lceil \frac{n+4m}{6} \right\rceil - m - 1,$$
$$N(z^n - z^m - 1) = n - 2\left\lfloor \frac{2n-m}{6} \right\rfloor - 1.$$

In Chapter 3 we also prove similar formulas for $U(P)$ and the number of roots outside the unit circle for all Borwein trinomials.

All (real) Pisot binomials, trinomials, and quadrinomials were identified in [26]. In a more recent literature, there has been a surge of interest in complex-base number expansions [34, 36, 41, 57]; in the distributions of the powers of algebraic numbers [62, 65] in the complex plane $\mathbb{C}$ with respect to the Gaussian lattice $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}, i^2 = -1\}$; in complex algebraic integers with special multiplicative properties [60, 63, 67, 66]. In these kinds of problems, the complex analogues of the Pisot numbers in $\mathbb{C}$ play the same pivotal role as the Pisot numbers in $\mathbb{R}$. Recall that an algebraic number $\beta \in \mathbb{C} \setminus \mathbb{R}$, $|\beta| > 1$ is called *a complex Pisot number*, if all of its algebraic conjugates $\beta' \notin \{\beta, \bar{\beta}\}$ satisfy $|\beta'| < 1$. The minimal polynomial of a complex Pisot number is called a complex Pisot polynomial. Note that for a complex Pisot polynomial P of degree n, we have $N(P) = n - 2$ and $U(P) = 0$.

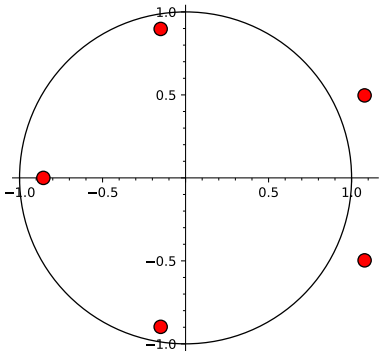


Figure 1.4: Roots of the complex Pisot polynomial $z^5 - z^4 + 1$

Complex Pisot numbers were first considered by Kelly and Samet [42,

53]. The smallest complex Pisot numbers were identified by Chamfy [19]; later, Garth [33, 32] significantly expanded Chamfy's list. Nonetheless, recent research raises the general interest in the spectra of complex Pisot numbers.

We are interested in complex Pisot numbers originating from the simplest possible polynomials, namely, Borwein trinomials of the form $z^n \pm z^m \pm 1$. For example, $z^5 - z^4 + 1$ is a Borwein trinomial. The main result of Chapter 3 is Theorem 3.1:

Theorem 3.1. *Any Borwein trinomial that has a complex Pisot number as its root is of the form $\pm P(\pm z)$, where $P(z)$ is one of the 17 polynomials listed in Table 3.1.*

$z^3 + z + 1$	$z^6 - z^2 + 1$
$z^3 - z^2 + 1$	$z^6 + z^4 + 1$
$z^4 + z + 1$	$z^6 + z^5 + 1$
$z^4 + z^2 - 1$	$z^7 + z^5 + 1$
$z^4 + z^3 + 1$	$z^7 - z^6 + 1$
$z^5 + z + 1$	$z^8 + z^6 - 1$
$z^5 - z^2 + 1$	$z^8 + z^7 + 1$
$z^5 + z^3 + 1$	$z^{10} + z^8 + 1$
$z^5 - z^4 + 1$	

Table 3.1: Representative Borwein trinomials that have a complex Pisot number as their root.

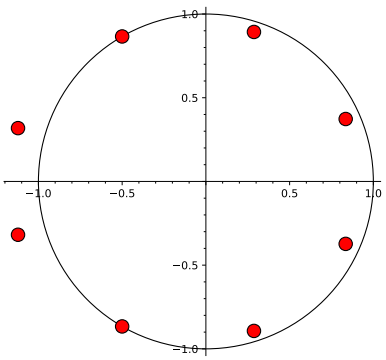


Figure 1.5: Roots of the Borwein trinomial $x^8 + x^7 + 1$

Chapter 3 contains proofs of our results as well as several corollaries that follow.

1.4 Methods

In Chapter 2 we use a computational approach employing an algorithm developed earlier to construct an oriented graph whose vertices represent polynomials and perform a search over it to find Littlewood and Newman multiples of Borwein polynomials. The results in Chapter 3 rely on classical methods of algebra and number theory.

1.5 Novelty

All of the findings presented in this thesis are new and original. Computations on the Littlewood and Newman multiples of Borwein polynomials expand and improve on the previous results of other authors. The results were published in peer-reviewed articles and presented at international conferences.

1.6 Approbation

The results of the dissertation were presented at the following conferences:

- International Conference on Probability Theory and Number Theory (2023, Palanga, Lithuania)
- The International Scientific Conference Dedicated to the 160th Anniversary of Prof. Dr. Hermann Minkowski (2024, Kaunas, Lithuania)
- Conference of the Lithuanian Mathematical Society (2024, Šiauliai, Lithuania)

1.7 Publications

The results of the dissertation are published in the following papers:

- P. Drungilas, J. Jankauskas, G. Junevičius, L. Klebonas, J. Šiurys, *On certain multiples of Littlewood and Newman polynomials*, Bull. Korean Math. Soc. 55(5) (2018) 1491-1501.
- P. Drungilas, J. Jankauskas, G. Junevičius, *On Complex Pisot Numbers That Are Roots of Borwein Trinomials*, Mathematics 12 (8) (2024), 1129.

1.8 Abstracts for conferences

- G. Junevičius. On Complex Pisot Numbers That are Roots of Borwein Trinomials. The international scientific conference dedicated to the 160th anniversary of Prof. Dr. Hermann Minkowski, June 20-22, 2024 Kaunas, Lithuania

- G. Junevičius. On Complex Pisot Numbers That are Roots of Borwein Trinomials. Conference of the Lithuanian Mathematical Society, June 27-28, 2024, Šiauliai, Lithuania. https://www.lmd2024.sa.vu.lt/wp-content/uploads/2024/06/LMD_65_tezes.pdf

Chapter 2

On certain multiples of Littlewood and Newman polynomials

2.1 Littlewood multiples of Newman quadrinomials

In [21, 25] the sets $\mathcal{L}(\mathcal{N}_d), \mathcal{N}_d \backslash \mathcal{L}(\mathcal{N})$ have been completely determined for $d \leqslant 11$. In particular, it was proved in [25] that every Newman polynomial of degree at most 8 divides some Littlewood polynomial, that is, $\mathcal{L}(\mathcal{N}_{\leqslant 8}) = \mathcal{N}_{\leqslant 8}$. On the other hand, $\#\mathcal{N}_9 \backslash \mathcal{L}(\mathcal{N}) = 18$, $\#\mathcal{N}_{10} \backslash \mathcal{L}(\mathcal{N}) = 36$ and $\#\mathcal{N}_{11} \backslash \mathcal{L}(\mathcal{N}) = 174$. It was also proved in [25] that every Borwein trinomial

$$z^b \pm z^a \pm 1, \quad 1 \leqslant a < b, \quad a, b \in \mathbb{Z}$$

(including Newman trinomials $z^b + z^a + 1$) has a Littlewood multiple, as well as certain Borwein quadrinomials $z^c \pm z^b \pm z^a \pm 1$ do. Therefore Dubickas and Jankauskas [25] asked whether there exist Borwein quadrinomials that do not divide any Littlewood polynomial. In [21], 20 such quadrinomials of degree $\leqslant 9$ were found. However, none of them is a Newman quadrinomial (each of them has coefficients -1 and 1). Therefore we raised the following question.

Question 2.1 ([21])**.** *Does there exist a Newman quadrinomial with no Littlewood multiple? Equivalently, does the set $\mathcal{N} \setminus \mathcal{L}(\mathcal{N})$ contain a quadrinomial?*

Our computations show that

Theorem 2.2. *Every quadrinomial $Q \in \mathcal{N}_{\leqslant 15}$, except possibly for those given in Table 2.1, divides some Littlewood polynomial. Moreover, every quadrinomial $Q \in \mathcal{N}_{\leqslant 14}$ possesses a Littlewood multiple of smallest possible degree $\deg_2 \widetilde{Q} - 1$ (this quantity will be defined in Section 2.2).*

Quadrinomial $Q(z)$	$\deg_2 \widetilde{Q} - 1$
$z^{15} + z^{14} + z^{10} + 1$	10921
$z^{15} + z^{12} + z^{10} + 1$	32765
$z^{15} + z^{12} + z^4 + 1$	31681
$z^{15} + z^8 + z^6 + 1$	32765

Table 2.1: Newman quadrinomials $Q \in \mathcal{N}_{\leqslant 15}$ which are not known to have Littlewood multiples (reciprocals omitted).

The second column in Table 2.1 indicates the smallest possible degree of a Littlewood multiple (if it exists) of $Q \in \mathcal{N}_{15}$. It was proved in [25] that if a polynomial $P(z) \in \mathbb{Z}[z]$ divides a Littlewood polynomial $L(z)$ then $\deg L \geqslant \deg_2 \widetilde{P} - 1$, where the number $\deg_2 \widetilde{P}$ is defined in Section 2.2. Figure 2.1 depicts the roots of polynomials from Table 2.1.

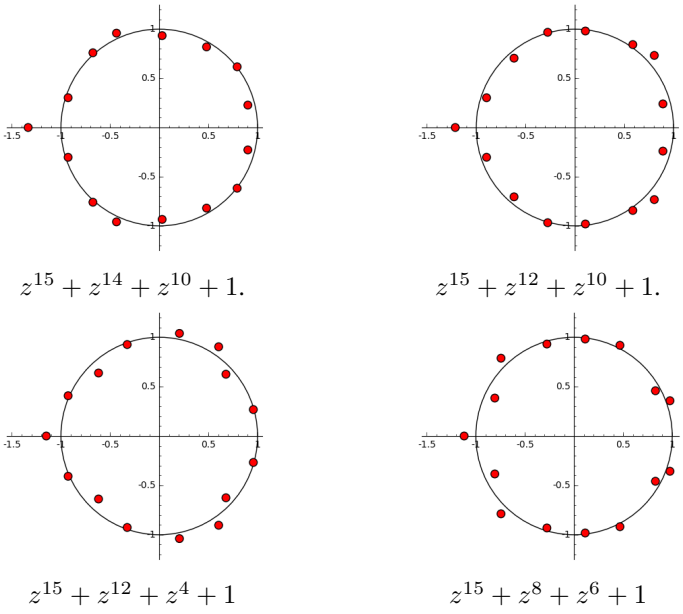


Figure 2.1: Complex roots of quadrinomials $Q(z)$ from Table 2.1.

2.2 Littlewood multiples of minimal degree

Let $\mathbb{F}_2$ be a finite field with two elements. Consider a polynomial $p(z) \in \mathbb{F}_2[z]$ with a non-zero constant term $p(0)$ in $\mathbb{F}_2$. Then $p(z)$ has a unique representation as a product

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

where $m \geqslant 0$ and $\phi_j(z) \in \mathbb{F}_2[z]$ are irreducible polynomials of degree greater than or equal to 2 and multiplicity $m_j \geqslant 1$, $j = 1, 2, \ldots, r$. The product is empty if $r = 0$. Every polynomial $\phi_j(z)$ divides a unique cyclotomic polynomial $\Phi_{e_j}(z)$ of odd index e_j (see, e.g., [25, Section 4]). Let s be the least positive integer satisfying $2^s \geqslant \max\{m+1, m_1, \ldots, m_r\}$. Following [25], we define the number

$$\deg_2 p = 2^s \cdot \operatorname{lcm}(e_1, \ldots, e_r).$$

Given a polynomial $P(z) \in \mathbb{Z}[z]$, denote by $\widetilde{P}(z) \in \mathbb{F}_2[z]$ its reduction modulo 2. In [25], it was shown that whenever $P(z) \in \mathbb{Z}[z]$ divides a Littlewood polynomial $L(z)$, then $\deg L = k \cdot \deg_2 \widetilde{P} - 1$ for some $k \in \{1, 2, \ldots\}$. Therefore $\deg L \geqslant \deg_2 \widetilde{P} - 1$. For example, $\deg_2 \widetilde{P} = 32766$ for the polynomial $P(z) = z^{15} + z^8 + z^6 + 1$ (see Table 2.1). Hence if this particular quadrinomial has a Littlewood multiple $L(z)$, then the $\deg(L) \geqslant 32765$. Another example is a quadrinomial $Q(z) = z^{15} + z^{10} + z^8 + 1$: we have computed a Littlewood multiple of $Q(z)$ of degree $\deg_2 \widetilde{Q} - 1 = 32765$. However, in general there might be more than one monic Littlewood multiple of minimal degree. Indeed, we found four distinct monic Littlewood multiples of $P(z) = z^{12} + z^{11} + z^{10} + 1$ of degree $\deg_2 \widetilde{P} - 1 = 1189$.

Our computations yield the following result.

Theorem 2.3. *Every polynomial $P(z) \in \mathcal{L}(\mathcal{N}_{\leqslant 10})$, except possibly for those given in Table 2.2, has a Littlewood multiple of the smallest possible degree* $\deg_2 \widetilde{P} - 1$.

The first polynomial in Table 2.2 is a product of cyclotomic polynomials:

$$P_1(z) = (z+1)^3 (z^2 - z + 1)(z^4 - z^3 + z^2 - z + 1).$$

The second and the third polynomials in Table 2.2 factor into irreducible poly-

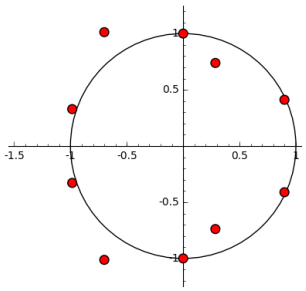
n	$P_n(z)$	$\deg_2 \widetilde{P_n} - 1$
1	$z^9 + z^8 + z^6 + z^5 + z^4 + z^3 + z + 1$	59
2	$z^{10} + z^9 + z^8 + z^3 + z^2 + 1$	1019
3	$z^{10} + z^9 + z^7 + z^6 + z^5 + 1$	1022

Table 2.2: Polynomials $P(z) \in \mathcal{L}(\mathcal{N}_{\leqslant 10})$ which are not known to have Littlewood multiples of degree $\deg_2 \widetilde{P} - 1$ (reciprocals omitted).

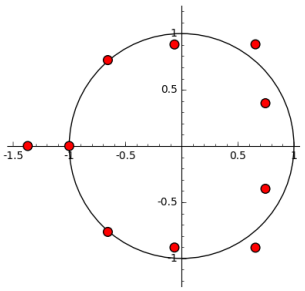
nomials as follows:

$$P_2(z) = (z^2 + 1)(z^8 + z^7 - z^5 + z^3 + 1),$$
$$P_3(z) = (z + 1)(z^9 + z^6 + z^4 - z^3 + z^2 - z + 1).$$

The roots of these two polynomials are depicted in Figure 2.2.



$z^{10} + z^9 + z^8 + z^3 + z^2 + 1$



$z^{10} + z^9 + z^7 + z^6 + z^5 + 1$

Figure 2.2: Complex roots of $P_2(z)$ and $P_3(z)$ from Table 2.2.

The corresponding result on Littlewood multiples of Newman quadrinomials was stated in Theorem 2.2 of Section 2.1.

2.3 Newman multiples of Littlewood polynomials

We already mentioned, that the sets $\mathcal{L}(\mathcal{N}_d)$ have been completely determined for $d \leqslant 11$. Also, it was proved in [21] (see Proposition 18) that if $P(z)$ is a product of cyclotomic polynomials and $P(1) \neq 0$ then $P(z)$ divides some Newman polynomial. Therefore Littlewood polynomials which are products of cyclotomic polynomials and do not vanish at $z = 1$ have Newman multiples too.

Motivated by this result, we considered the *complementary problem* of

computing the sets $\mathcal{N}(\mathcal{L}_d)$ for small degrees d. By running the algorithm, described in Section 2.4 on every Littlewood polynomial $L(z) \in \mathcal{L}_{12}$, we calculated explicitly all non-trivial elements of the set $\mathcal{N}(\mathcal{L}_{\leqslant 12})$.

Theorem 2.4. *There are exactly* 9 *monic Littlewood polynomials* $P(z)$ *of degree* $\leqslant 12$ *that possess Newman multiples and are not themselves the products of cyclotomic polynomials (see Table 2.3).*

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

Table 2.3: Monic non-trivial elements of $\mathcal{N}(\mathcal{L}_{\leqslant 12})$

This result contrasts very sharply with the fact that *most* Newman polynomials of small degree have Littlewood multiples. Roots of these 9 polynomials are depicted in Figure 2.3.

Recall that a real algebraic integer $\alpha > 1$ is called *Salem number* (see, e.g., [50, 52, 51]), if all other conjugates of α lie in the unit circle $|z| \leqslant 1$, with at least one conjugate on the unit circle $|z| = 1$. Similarly, an algebraic integer α is called a *negative Salem number* if $-\alpha$ is a Salem number. Finally, a *complex Salem number* (see, e.g., [62]) is a non-real algebraic integer α of modulus $|\alpha| > 1$ whose other conjugates, except for $\overline{\alpha}$, are of moduli $\leqslant 1$, with at least one conjugate of modulus $= 1$. Note that the non-cyclotomic parts (polynomials, obtained omitting their cyclotomic factors) of polynomials $P_1(z)$, $P_2(z)$ and $P_7(z)$ are minimal polynomials of negative Salem numbers, whereas the non-cyclotomic parts of polynomials $P_3(z)$, $P_4(z)$, $P_5(z)$ and $P_6(z)$ are minimal polynomials of complex Salem numbers. As a result we have the following corollary.

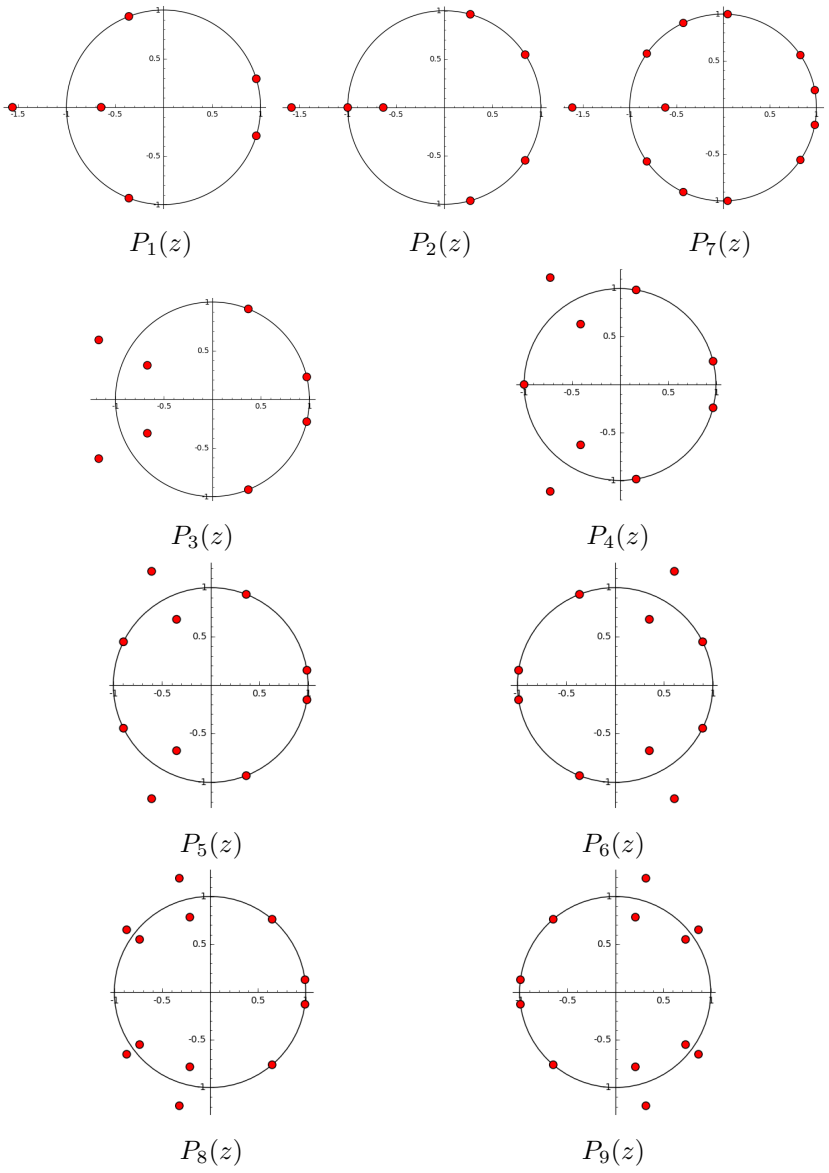


Figure 2.3: Roots of polynomials $P_k(z) \in \mathcal{N}(\mathcal{L}_{\leqslant 12})$ from Table 2.3

Corollary 2.1. *Every polynomial $P \in \mathcal{N}(\mathcal{L}_{\leqslant 12})$ that is not a product of cyclotomic polynomials, has a complex root on $|z| = 1$ which is not a root of unity.*

2.4 A short description of the algorithm

We start with the following definition.

Definition 2.5. *Let $P(z)$ be a non-constant polynomial with integer coefficients with no roots on the complex unit circle $|z| = 1$. Suppose that the factorization of P in $\mathbb{C}[z]$ is*

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

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

$$\begin{aligned} |R(\alpha_j)| &\leqslant \frac{B}{||\alpha_j| - 1|}, \\ |R'(\alpha_j)| &\leqslant \frac{1!B}{||\alpha_j| - 1|^2}, \\ &\ldots, \\ |R^{(e_j-1)}(\alpha_j)| &\leqslant \frac{(e_j - 1)!B}{||\alpha_j| - 1|^{e_j}}. \end{aligned} \tag{1}$$

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

Let $\mathcal{D} \subset \mathbb{Z}$ be a finite set and 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 $B = \max\{|b| : b \in \mathcal{D}\}$. Two vertices corresponding to polynomials R_i and R_j are connected by a directed edge from R_i to R_j, if $R_j \equiv z \cdot R_i + b \pmod{P}$ in $\mathbb{Z}[z]/(P)$ for some digit $b \in \mathcal{D}$.

It was proved in [3, 21, 31] that given a polynomial $P(z) \in \mathbb{Z}[z]$, which satisfies the conditions of Definition 2.5, the set $\mathcal{R}(P, B)$ is finite for every $B > 0$. Therefore the graph $\mathcal{G} = \mathcal{G}(P, \mathcal{D})$ is finite for such polynomials P.

We restate Theorem 18 from [21] without proof.

Theorem 2.6. *Let $P \in \mathbb{Z}[z]$ be a monic polynomial with no roots on the complex unit circle $|z| = 1$. Then P divides an integer polynomial*

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

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 $R(z) = a_n$ and ends at $R(z) = 0$. The length of the path is n, where n is the degree of Q.

Thus the polynomial Q with the coefficients in the set $\mathcal{D}$ can be found by running any path finding algorithm on $\mathcal{G} = \mathcal{G}(P, \mathcal{D})$.

A complex number with absolute value 1 is called a *unimodular number*. Note that every root of unity is a unimodular number. However, not every unimodular number is a root of unity, since $e^{ni} \neq 1$ for every positive integer n (here, as usual, $i^2 = -1$).

If a polynomial $P(z) \in \mathbb{Z}[z]$ has unimodular roots that are not roots of unity we exclude them when checking the inequalities (1) of Definition 2.5 and continue building the graph $\mathcal{G}(P, \mathcal{D})$. Even in cases where $\mathcal{G}(P, \mathcal{D})$ is infinite, the component that is accessible from $R_0 = a_n$ might be finite, or this component might be simple enough so an existing path from R_0 to $R = 0$ can be found within a reasonable time. Thus in practice, it is often the case that Question 1 (see Section 1.2) can still be answered for such polynomials.

For the reader's convenience, we include the pseudocode of the algorithm from [21]

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

Input: *a monic polynomial $P \in \mathbb{Z}[z]$,*
the digit set $\mathcal{D} \subset \mathbb{Z}$,
the leading coefficient $a \in \mathcal{D}$, $a \neq 0$.
Output: *a polynomial $Q \in \mathcal{D}[z]$ 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 indicating if the search is finished.
Method: *Depth-first search using Theorem 2.6.*

Step 0: set $\mathcal{V} = \varnothing$, $\mathcal{E} = \varnothing$
Step 1: add the polynomial $R = a$ into $\mathcal{V}$
Step 2: set *found* := False
Step 3: call **do_search**(a, *found*)
Step 4: if $found$ then print a
else print $\varnothing$
end if
Step 5: stop.

procedure **do_search**(local var $R \in \mathbb{Z}[z]$, var *found*):
local var $S \in \mathbb{Z}[z]$
if $R = 0$ then
set *found* := True
else
for each $d \in \mathcal{D}$ do
compute $S := z \cdot R + d \pmod P$.
if $S \notin \mathcal{V}$ and $S \in \mathcal{R}(P, B)$, where $B := \max\{|d| : d \in \mathcal{D}\}$ then
add S to $\mathcal{V}$
add d as an edge from R to S to $\mathcal{E}$
call **do_search**(S, *found*)
end if
if $found$ then
print digit d
break loop
end if
end do
end if
end proc

2.5 Computations

We implemented the algorithm described in Section 2.4 in C++ using Arb [40] library for arbitrary-precision floating-point ball arithmetic (see the Appendix) and ran it on the SGI Altix 4700 server at Vilnius University. OpenMP [7] was used for the multiprocessing.

For every $P \in \mathcal{L}_{\leqslant 12}$ we calculated whether it divides some Newman polynomial. In the same way, for every Newman quadrinomial $Q \in \mathcal{N}_{\leqslant 15}$, except for those given Table 2.1, we found a Littlewood multiple of Q. A slightly modified code was used to search for the smallest degree Littlewood multiples of Newman polynomials $P \in \mathcal{L}(\mathcal{N}_{10})$ and Newman quadrinomials $Q \in \mathcal{N}_{\leqslant 15}$ (see Section 2.2). We will briefly explain how these calculations were organized.

By Proposition 18, Section 4.1 of [21], one can omit cyclotomic factors of a polynomial $P(z) \in \mathbb{Z}[z]$ when searching for its Littlewood multiples: if $\Phi_n(z)$ is the n-th cyclotomic polynomial, then $\Phi_n P \in \mathcal{L}(\mathbb{Z}[z])$ if and only if $P \in \mathcal{L}(\mathbb{Z}[z])$. In particular, every polynomial that is a product of cyclotomic polynomials has a Littlewood multiple. For every quadrinomial $Q \in \mathcal{N}_{\leqslant 15}$ we omitted all of its cyclotomic factors and ran the algorithm to check whether Q has a Littlewood multiple. Similarly, we ran the algorithm for every polynomial $P \in \mathcal{L}(\mathcal{N}_{\leqslant 10})$. Only for polynomials given in Table 2.1 and Table 2.2 the computations did not terminate normally due to the limits on our server machine.

Similarly, one can omit cyclotomic factors, except for $\Phi_1(z) = z - 1$, when searching for Newman multiples: for $n > 1$, $\Phi_n P \in \mathcal{N}(\mathbb{Z}[z])$ if and only if $P \in \mathcal{N}(\mathbb{Z}[z])$. Also, real roots of Newman polynomials must be negative, therefore $P \in \mathcal{N}(\mathbb{Z}[z])$ implies that P has no positive real roots. We used SAGE [20] to filter out all such polynomials from $\mathcal{L}_{\leqslant 12}$ and then ran the algorithm on the non-cyclotomic parts of the remaining polynomials to check whether they have Newman multiples.

Some of the polynomials in sets $\mathcal{L}_{\leqslant 12}$ and $\mathcal{N}_{\leqslant 10}$ have unimodular roots that are not roots of unity. However, we succeeded in determining whether these polynomials belong to $\mathcal{L}(\mathcal{B})$ and $\mathcal{N}(\mathcal{B})$ (see Section 2.4 above).

Note that in the inequalities (1) of Section 2.4, one has the upper bound $B = \max\{|a| \mid a \in \mathcal{D}\} = 1$ in case of Littlewood and Newman multiples. To fasten the search, a new variable δ, $0 \leqslant \delta < 1$ was introduced, replacing the bound B 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. For polynomials in $\mathcal{N} \setminus \mathcal{L}(\mathcal{N})$ and $\mathcal{L} \setminus \mathcal{N}(\mathcal{L})$ the variable δ always reaches the value $\delta = 0$ in order to construct the full graph $\mathcal{G}(P, \mathcal{D})$.

All computations took approximately 49 hours of CPU time. The maximum recursion depth reached by the algorithm was $98\,936$. It took about 90 seconds of CPU time to run our algorithm to find the Littlewood multiple $L(z)$ of the polynomial $P(z) = z^{15} + z^{10} + z^8 + 1$ of smallest possible degree $\deg L = \deg_2 \widetilde{P} - 1 = 32\,765$; $283\,501$ vertices of the graph $\mathcal{G}(P, \{-1, 1\})$ were constructed. The maximal recursion depth reached for this polynomial was 471. On the other hand, it took 5960 seconds of CPU time to find a Littlewood multiple $L(z)$ of the polynomial $P(z) = z^{14} - z^{12} + z^3 + 1$ of smallest possible degree $\deg L = \deg_2 \widetilde{P} - 1 = 16\,381$; more than one million vertices of the graph $\mathcal{G}(P, \{-1, 1\})$ were constructed. For every polynomial in Table 2.1 and Table 2.2 it took 2 hours of CPU time before the computation was interrupted due to limitations of computational resources.

Chapter 3

On complex Pisot numbers that are roots of Borwein trinomials

3.1 Main results

Theorem 3.1. *Any Borwein trinomial that has a complex Pisot number as its root is of the form* $\pm P(\pm z)$*, where* $P(z)$ *is one of the* 17 *polynomials listed in Table 3.1.*

z^3+z+1	z^6-z^2+1
z^3-z^2+1	z^6+z^4+1
z^4+z+1	z^6+z^5+1
z^4+z^2-1	z^7+z^5+1
z^4+z^3+1	z^7-z^6+1
z^5+z+1	z^8+z^6-1
z^5-z^2+1	z^8+z^7+1
z^5+z^3+1	$z^{10}+z^8+1$
z^5-z^4+1	

Table 3.1: Representative Borwein trinomials which have a complex Pisot number as their root.

All the polynomials in Table 3.1 are irreducible, except for z^5+z+1, z^7+z^5+1, z^8+z^7+1 and $z^{10}+z^8+1$, which are all divisible by z^2+z+1. In comparison, all Borwein trinomials and quadrinomials that give a rise to real Pisot numbers were essentially identified in [26] (after taking into account the

irreducibly theorem by Ljunggren [29]). The proof of Theorem 3.1 is based on the following result.

Theorem 3.2. *Let $n > m$ be positive integers. All the Borwein trinomials $P(z) = z^n \pm z^m \pm 1$ with at most two roots inside the unit disc $|z| < 1$ are given in Table 3.2.*

$N(f) = 1$	$N(f) = 2$	$N(f) = 2$
$z^2 + z - 1$	$z^4 + z^2 - 1$	$z^3 + z^2 + 1$
$z^3 + z^2 - 1$	$z^4 - z^2 - 1$	$z^3 - z + 1$
$z^3 + z + 1$	$z^6 + z^4 - 1$	$z^4 + z^3 + 1$
$z^4 + z - 1$	$z^6 - z^4 - 1$	$z^4 + z + 1$
$z^5 + z - 1$	$z^6 + z^2 + 1$	$z^5 + z^4 + 1$
	$z^6 + z^2 - 1$	$z^5 - z^3 + 1$
	$z^8 + z^2 - 1$	$z^5 + z^2 + 1$
	$z^8 - z^2 - 1$	$z^5 - z + 1$
	$z^{10} + z^2 - 1$	$z^6 + z + 1$
	$z^{10} + z^2 + 1$	$z^7 + z^2 + 1$
		$z^7 - z + 1$
		$z^8 + z + 1$

Table 3.2: Representative Borwein trinomials with at most 2 zeros inside the open unit disk $|z| < 1$. Only one polynomial out of $\pm P(\pm z)$ is shown.

We also note that Borwein trinomials appear to have no multiple roots in $\mathbb{C}$ (see Proposition 3.7).

More generally, the number of zeros of a Borwein trinomial or a Borwein quadrinomial is interesting in the context of the distribution of zeros of polynomials with small coefficients [35]. For this, let us state the definition for the zero number $N(f)$ of a polynomial $f(z)$. First, recall $f(z)$ splits over the field of complex numbers $\mathbb{C}$ into

$$f(z) = a_n(z - \alpha_1)(z - \alpha_2)\cdots(z - \alpha_n),$$

where the complex zeros $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ of $f(z)$ are not necessarily distinct. The zero counting functions with respect to the unit circle are introduced through the formulas

$$N(f) = \#\{j,\, 1 \leqslant j \leqslant n : |\alpha_j| < 1\}$$

and

$$U(f) = \#\{j,\, 1 \leqslant j \leqslant n : |\alpha_j| = 1\},$$

where the zeros are counted with the multiplicities. The *reciprocal* polynomial $f^*(z)$ is defined by

$$f^*(z) = z^n f(1/z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n.$$

Note that

$$N(f^*) = \#\{j,\, 1 \leqslant j \leqslant n : |\alpha_j| > 1\}.$$

Hence, one always has that

$$N(f) + N(f^*) + U(f) = n.$$

We derive Theorem 3.2 from Proposition 3.3 which gives explicit formulas for $N(f)$ for any Borwein trinomial $f(z)$. Finally, Proposition 3.3 is derived from an old result of Bohl (see Theorem 3.6).

Previous work on smallest complex Pisot numbers [19, 33, 32] was based on the complicated computations of coefficients of Taylor-Maclaurin series of bounded analytic functions (Schur functions), a method pioneered by Dufresnoy and Pisot [28, 27]. Our new contribution to expanding the list of known complex Pisot numbers is based on Bohl's formula [8, 18]

Proposition 3.3. *Let $n > m$ be coprime positive integers. Then*

$$\begin{aligned}
N(z^n + z^m + 1) &= n - m - 1 - 2\left\lfloor \frac{n-2m}{3} \right\rfloor, \\
N(z^n + z^m - 1) &= 2\left\lceil \frac{n+m}{6} \right\rceil - 1, \\
N(z^n - z^m + 1) &= 2\left\lceil \frac{n+4m}{6} \right\rceil - m - 1, \\
N(z^n - z^m - 1) &= n - 2\left\lfloor \frac{2n-m}{6} \right\rfloor - 1.
\end{aligned}$$

3.2 Corollaries

The reciprocal polynomial $(z^n \pm z^m \pm 1)^*$ is of the form $\pm z^n \pm z^{n-m} + 1$. Therefore, Proposition 3.3 implies the following corollary.

Corollary 3.1. *Let $n > m$ be coprime positive integers. Then*

$$N\left((z^n + z^m + 1)^*\right) = 2\left\lceil \frac{n+m}{3} \right\rceil - m - 1,$$
$$N\left((z^n + z^m - 1)^*\right) = n - 2\left\lfloor \frac{n+m}{6} \right\rfloor - 1,$$
$$N\left((z^n - z^m + 1)^*\right) = 2\left\lceil \frac{5n-4m}{6} \right\rceil - n + m - 1,$$
$$N\left((z^n - z^m - 1)^*\right) = 2\left\lceil \frac{2n-m}{6} \right\rceil - 1.$$

Note that for $P(z) = z^n \pm z^m \pm 1$, $N(f^*)$ equals the number of roots of $P(z)$ which lie strictly outside the unit circle $|z| = 1$. Now, in view of Proposition 3.3, Corollary 3.1 and the formula

$$N(f) + N(f^*) + U(f) = n$$

we can determine the number of unimodular roots of $P(z)$.

Corollary 3.2. *Let $n > m$ be coprime positive integers. Then*

$$U(z^n + z^m + 1) = 2\left(1 - \left(\left\lceil \frac{n+m}{3} \right\rceil - \left\lfloor \frac{n+m}{3} \right\rfloor\right)\right),$$
$$U(z^n + z^m - 1) = 2\left(1 - \left(\left\lceil \frac{n+m}{6} \right\rceil - \left\lfloor \frac{n+m}{6} \right\rfloor\right)\right),$$
$$U(z^n - z^m + 1) = 2\left(1 - \left(\left\lceil \frac{n+4m}{6} \right\rceil - \left\lfloor \frac{n+4m}{6} \right\rfloor\right)\right),$$
$$U(z^n - z^m - 1) = 2\left(1 - \left(\left\lceil \frac{2n-m}{6} \right\rceil - \left\lfloor \frac{2n-m}{6} \right\rfloor\right)\right).$$

The following corollary has already been proved by Ljunggren (see Theorem 3 in [46]). Nevertheless, we give an alternative proof of this result.

Corollary 3.3. *Let $n > m$ be coprime positive integers.*

1. *The polynomial $P(z) = z^n + z^m + 1$ has a unimodular root if and only if $n + m$ is divisible by 3. Furthermore, if $n + m$ is divisible by 3, then $P(z) = (z^2+z+1)g(z)$, where the polynomial $g(z)$ has no unimodular roots.*

2. *The polynomial $P(z) = z^n + z^m - 1$ has a unimodular root if and only if $n + m$ is divisible by 6. Furthermore, if $n + m$ is divisible by 6, then*

$P(z) = (z^2 - z + 1)g(z)$, *where the polynomial* $g(z)$ *has no unimodular roots.*

3. *The polynomial* $P(z) = z^n - z^m + 1$ *has a unimodular root if and only if* $n + 4m$ *is divisible by 6. Furthermore, if* $n + 4m$ *is divisible by 6, then* $P(z) = (z^2 - z + 1)g(z)$, *where the polynomial* $g(z)$ *has no unimodular roots.*

4. *The polynomial* $P(z) = z^n - z^m - 1$ *has a unimodular root if and only if* $2n - m$ *is divisible by 6. Furthermore, if* $2n - m$ *is divisible by 6, then* $P(z) = (z^2 - z + 1)g(z)$, *where the polynomial* $g(z)$ *has no unimodular roots.*

Note that the polynomial $g(z)$ in this corollary is irreducible (see Theorem 3.4).

3.3 Irreducibility

Selmer [54] studied the irreducibility of trinomials $z^n \pm z \pm 1$. In particular, he proved that the trinomial $z^n - z - 1$ is irreducible for every positive integer $n > 1$. Tverberg [61] proved that a trinomial $z^n \pm z^m \pm 1$ is reducible if and only if it has a unimodular root. Ljunggren [46] extended this result to any quadrinomial $z^n \pm z^m \pm z^p \pm 1$.

Theorem 3.4 ([61] and Theorem 3 in [46])**.** *Let* $n > m$ *be positive integers. The trinomial* $P(z) = z^n \pm z^m \pm 1$ *is reducible over the rationals if and only if it has a unimodular root. If* $P(z)$ *has unimodular roots, these roots can be collected to give a rational factor of* $P(z)$*. The other factor of* $P(z)$ *is then irreducible.*

Note that for any polynomial $P(z)$ and any positive integer a, one has that $U(P(z^a)) = aU(P(z))$. So that $P(z^a)$ has a unimodular root if and only if $P(z)$ has a unimodular root. Combining this and Theorem 3.4, we obtain that for any positive integer a, the trinomial $z^n \pm z^m \pm 1$ is irreducible if and only if the trinomial $z^{na} \pm z^{ma} \pm 1$ is irreducible. Hence, considering the irreducibility of a trinomial $z^n \pm z^m \pm 1$, one can always assume that m and n are coprime.

The following corollary has already been proved by Ljunggren (see Theorem 3 in [46]). Nevertheless, we give an alternative proof of this result.

Corollary 3.4. *Let* $n > m$ *be positive integers and* $a = \gcd(n, m)$.

1. *The polynomial* $P(z) = z^n + z^m + 1$ *is reducible if and only if* $(n+m)/a$ *is divisible by 3. Furthermore, if* $(n+m)/a$ *is divisible by 3, then* $P(z)$ *has exactly* $2a$ *unimodular roots, which are the roots of* $z^{2a} + z^a + 1$ *and the quotient* $P(z)/(z^{2a} + z^a + 1)$ *is an irreducible polynomial.*

2. *The polynomial* $P(z) = z^n + z^m - 1$ *is reducible if and only if* $(n+m)/a$ *is divisible by 6. Furthermore, if* $(n+m)/a$ *is divisible by 6, then* $P(z)$ *has exactly* $2a$ *unimodular roots, which are the roots of* $z^{2a} - z^a + 1$ *and the quotient* $P(z)/(z^{2a} - z^a + 1)$ *is an irreducible polynomial.*

3. *The polynomial* $P(z) = z^n - z^m + 1$ *is reducible if and only if* $(n + 4m)/a$ *is divisible by 6. Furthermore, if* $(n + 4m)/a$ *is divisible by 6, then* $P(z)$ *has exactly* $2a$ *unimodular roots, which are the roots of* $z^{2a} - z^a + 1$ *and the quotient* $P(z)/(z^{2a} - z^a + 1)$ *is an irreducible polynomial.*

4. *The polynomial* $P(z) = z^n - z^m - 1$ *is reducible if and only if* $(2n - m)/a$ *is divisible by 6. Furthermore, if* $(2n-m)/a$ *is divisible by 6, then* $P(z)$ *has exactly* $2a$ *unimodular roots, which are the roots of* $z^{2a} - z^a + 1$ *and the quotient* $P(z)/(z^{2a} - z^a + 1)$ *is an irreducible polynomial.*

3.4 Proofs

Let x be a real number. Recall that $\lfloor x \rfloor$ denotes the largest rational integer which is less than or equal to x. Similarly, $\lceil x \rceil$ denotes the smallest rational integer which is greater than or equal to x. We will need the following basic properties of $\lfloor x \rfloor$ and $\lceil x \rceil$ which follow directly from the definitions of these functions.

Definition of $\lfloor x \rfloor$ and $\lceil x \rceil$ imply the following proposition.

Proposition 3.5. *The following statements are true.*

(i) For any real number x, $\lfloor x \rfloor \leqslant x \leqslant \lceil x \rceil$.

(ii) For any real number x *the equalities* $\lceil x \rceil = -\lfloor -x \rfloor$ *and* $\lfloor x \rfloor = -\lceil -x \rceil$ *hold.*

(iii) For any real numbers a *and* b, $a < b$, *the interval* $(a,\ b)$ *contains exactly* $\lceil b \rceil - \lfloor a \rfloor - 1$ *rational integers.*

The main tool in the proof of Theorem 3.2 is the following result due to Bohl: for modern formulation, see nice expository note [18] (also formulated as Theorem 3.2 in [59]).

Theorem 3.6 (Bohl's theorem, [8, 59])**.** *Let $P(z) = z^n + pz^m + q$ be a trinomial, where $p, q \in \mathbb{C}$ and m and n are coprime positive integers such that $n > m$. Assume that for a real number $v > 0$ there exists a triangle with edge lengths v^n, $|p|v^m$ and $|q|$. Let $\alpha = \angle(|p|v^m, |q|)$ and $\beta = \angle(v^n, |q|)$. Then the number of roots of $P(z)$ which lie in the open disc $|z| < v$ is given by the number of integers located in the open interval $(C_f - \delta_f, C_f + \delta_f)$, where*

$$C_f = \frac{n\left(\pi + \arg(p) - \arg(q)\right) - m\left(\pi - \arg(q)\right)}{2\pi}$$

and

$$\delta_f = \frac{n\alpha + m\beta}{2\pi}.$$

Note that if $P(z)$ is a polynomial such that $P(0) \neq 0$ and ℓ is a positive integer then $N(P(z^\ell)) = \ell N(P(z))$.

Proposition 3.7. *Let $n > m$ be positive integers and $a, b \in \{\pm 1\}$. Then the polynomial $z^n + az^m + b$ has no multiple roots in $\mathbb{C}$.*

Proof of Proposition 3.7. For a contradiction, assume that $z_0 \in \mathbb{C}$ is a multiple root of $P(z) = z^n + az^m + b$. Then $P(z_0) = f'(z_0) = 0$. Since $f'(z) = nz^{n-1} + amz^{m-1} = z^{m-1}(nz^{n-m} + am)$, we have that $z_0^{n-m} = -am/n$ and $|z_0|^{n-m} = m/n < 1$. Hence, $|z_0| < 1$. On the other hand, $f'(z_0) = 0$ implies that $z_0^n = -am/nz_0^m$. Substituting this into $P(z_0) = z_0^n + az_0^m + b = 0$ yields $-am/nz_0^m + az_0^m + b = 0$. Hence, $z_0^m = -bn/(a(n-m))$ and $|z_0|^m = n/(n-m) > 1$. Therefore, $|z_0| > 1$ which contradicts the previously obtained inequality $|z_0| < 1$. □

Proof of Proposition 3.3. We will apply Theorem 3.6 to the polynomial $P(z) = z^n + pz^m + q$, where $p = \pm 1$, $q = \pm 1$ and $v = 1$. Note that in Theorem 3.6 the triangle with edge lengths $v^n = 1$, $|p|v^m = 1$ and $|q| = 1$ is equilateral. Hence, $\alpha = \beta = \pi/3$ and $\delta_f = (n\alpha + m\beta)/(2\pi) = (n+m)/6$. By Theorem 3.6, $N(f)$ equals the number of integers located in the open interval $(C_f - \delta_f, C_f + \delta_f)$, where

$$C_f = \frac{n\left(\pi + \arg(p) - \arg(q)\right) - m\left(\pi - \arg(q)\right)}{2\pi}.$$

We will consider only the case $P(z) = z^n + z^m + 1$. The remaining formulas for $N(f)$ in Proposition 3.3 can be obtained completely analogously.

Let $P(z) = z^n + z^m + 1$. Then $p = q = 1$ and $\arg(p) = \arg(q) = 0$. Hence, $C_f = (n-m)/2$. By Theorem 3.6, $N(f)$ equals the number of integers located in the open interval $(C_f - \delta_f, C_f + \delta_f) = ((n-2m)/3,\ (2n-m)/3)$. Hence, in view of Proposition 3.5 (iii),

$$N(f) = \left\lceil \frac{2n-m}{3} \right\rceil - \left\lfloor \frac{n-2m}{3} \right\rfloor - 1.$$

Note that $(2n-m)/3 = n-m-(n-2m)/3$. Then, in view of Proposition 3.5 (ii),

$$\begin{aligned} N(f) &= \left\lceil n-m-\frac{n-2m}{3} \right\rceil - \left\lfloor \frac{n-2m}{3} \right\rfloor - 1 \\ &= n-m-1+\left\lceil -\frac{n-2m}{3} \right\rceil - \left\lfloor \frac{n-2m}{3} \right\rfloor = n-m-1-2\left\lfloor \frac{n-2m}{3} \right\rfloor. \end{aligned}$$

□

Proof of Corollary 3.2. We will consider only the case $P(z) = z^n + z^m + 1$. The remaining formulas for $U(f)$ can be obtained completely analogously.

Let $P(z) = z^n + z^m + 1$. By Proposition 3.3 and Corollary 3.1,

$$N(f) = n-m-1-2\left\lfloor \frac{n-2m}{3} \right\rfloor \quad \text{and} \quad N(f^*) = 2\left\lceil \frac{n+m}{3} \right\rceil - m - 1.$$

Hence, the formula $N(f) + N(f^*) + U(f) = n$ implies

$$\begin{aligned} U(f) &= n - N(f) - N(f^*) = n - \left(n-m-1-2\left\lfloor \frac{n-2m}{3} \right\rfloor \right) \\ &\quad - \left(2\left\lceil \frac{n+m}{3} \right\rceil - m - 1 \right) = 2m+2+2\left\lfloor \frac{n-2m}{3} \right\rfloor - 2\left\lceil \frac{n+m}{3} \right\rceil \\ &= 2m+2+2\left\lfloor \frac{n+m}{3} - m \right\rfloor - 2\left\lceil \frac{n+m}{3} \right\rceil \\ &= 2+2\left\lfloor \frac{n+m}{3} \right\rfloor - 2\left\lceil \frac{n+m}{3} \right\rceil \\ &= 2\left(1 - \left(\left\lceil \frac{n+m}{3} \right\rceil - \left\lfloor \frac{n+m}{3} \right\rfloor \right)\right). \end{aligned}$$

□

Proof of Corollary 3.3. The first part of every proposition follows directly from Corollary 3.2.

1. Assume that $n+m$ is divisible by 3. According to Corollary 3.2, the trinomial $P(z)=z^n+z^m+1$ has precisely two unimodular roots. It suffices to show that $\zeta=e^{\frac{2\pi i}{3}}$ is a root of $P(z)$ (indeed, if $P(\zeta)=0$ then $f\left(\bar{\zeta}\right)=\overline{P(\zeta)}=0$, so that ζ and $\bar{\zeta}=e^{-\frac{2\pi i}{3}}$ are the only unimodular roots of $P(z)$ and $z^2+z+1=(z-\zeta)(z-\bar{\zeta})$ divides $P(z)$). We have that $n+m=3t$ for some positive integer t. Also, ζ is a primitive 3rd root of unity, whose minimal polynomial is $z^2+z+1=(z-\zeta)(z-\bar{\zeta})$. Since $\zeta^3=1$, we have that

$$P(\zeta)=\zeta^n+\zeta^m+1=\zeta^{3t-m}+\zeta^m+1=\zeta^{-m}+\zeta^m+1=\zeta^{-m}\left(\zeta^{2m}+\zeta^m+1\right).$$

Note that m is not divisible by 3 since m and n are coprime and $n+m=3t$. Hence, ζ^m is also a primitive 3rd root of unity, and thus a root of z^2+z+1. Therefore, $P(\zeta)=\zeta^{-m}\left(\zeta^{2m}+\zeta^m+1\right)=0$.

2. Assume that $n+m$ is divisible by 6. According to Corollary 3.2, the trinomial $P(z)=z^n+z^m-1$ has precisely two unimodular roots. As in the proof of the first proposition, it suffices to show that $\zeta=e^{\frac{\pi i}{3}}$ is a root of $P(z)$. We have that $n+m=6t$ for some positive integer t. Also, ζ is a primitive 6th root of unity, whose minimal polynomial is $z^2-z+1=(z-\zeta)(z-\bar{\zeta})$. Since $\zeta^6=1$, we have that

$$P(\zeta)=\zeta^n+\zeta^m-1=\zeta^{6t-m}+\zeta^m-1=\zeta^{-m}+\zeta^m-1=\zeta^{-m}\left(\zeta^{2m}-\zeta^m+1\right).$$

Note that m is coprime to 6 since m and n are coprime and $n+m=6t$. Hence, ζ^m is also a primitive 6th root of unity, and thus a root of z^2-z+1. Therefore, $P(\zeta)=\zeta^{-m}\left(\zeta^{2m}-\zeta^m+1\right)=0$.

3. Assume that $n+4m$ is divisible by 6. According to Corollary 3.2, the trinomial $P(z)=z^n-z^m+1$ has precisely two unimodular roots. As in the proof of the first proposition, it suffices to show that $\zeta=e^{\frac{\pi i}{3}}$ is a root of $P(z)$. We have that $n+4m=6t$ for some positive integer t. Also, ζ is a primitive 6th root of unity, whose minimal polynomial is $z^2-z+1=(z-\zeta)(z-\bar{\zeta})$. Since $\zeta^6=1$, we have that

$$P(\zeta)=\zeta^n-\zeta^m+1=\zeta^{6t-4m}-\zeta^m+1=\zeta^{-4m}-\zeta^m+1=\zeta^{2m}-\zeta^m+1.$$

Note that m is coprime to 6 since m and n are coprime and $n+4m=6t$.

Hence, ζ^m is also a primitive 6th root of unity, and thus a root of $z^2 - z + 1$. Therefore, $P(\zeta) = \zeta^{2m} - \zeta^m + 1 = 0$.

4. This proposition follows from the second proposition by considering the reciprocal polynomial $-(z^n - z^m - 1)^* = z^n + z^{n-m} - 1$. □

Proof of Theorem 3.2. Let $n > m$ be positive integers. Suppose that $P(z) = z^n \pm z^m \pm 1$ is a Borwein trinomial such that $N(f) \leqslant 2$. Consider two possible cases: $\gcd(n, m) = 1$ and $\gcd(n, m) > 1$.

Case 1. We have that $\gcd(n, m) = 1$. We will apply Theorem 3.6 to the polynomial $P(z) = z^n + pz^m + q$, where $p = \pm 1$, $q = \pm 1$ and $v = 1$. Note that in Theorem 3.6 the triangle with edge lengths $v^n = 1$, $|p|v^m = 1$ and $|q| = 1$ is equilateral. Hence, $\alpha = \beta = \pi/3$ and $\delta_f = (n\alpha + m\beta)/(2\pi) = (n+m)/6$. By Theorem 3.6, $N(f)$ equals the number of integers located in the open interval $(C_f - \delta_f, C_f + \delta_f)$, where

$$C_f = \frac{n\,(\pi + \arg(p) - \arg(q)) - m\,(\pi - \arg(q))}{2\pi}.$$

Hence, by (iii) and (i) of Proposition 3.5, we have

$$\begin{aligned} N(f) = \lceil C_f + \delta_f \rceil - \lfloor C_f - \delta_f \rfloor - 1 &\geqslant (C_f + \delta_f) - \lfloor C_f - \delta_f \rfloor - 1 \\ &\geqslant (C_f + \delta_f) - (C_f - \delta_f) - 1 = 2\delta_f - 1 = \frac{n + m - 3}{3}. \end{aligned}$$

Recall that $N(f) \leqslant 2$. Thus $(n+m-3)/3 \leqslant 2$ which is equivalent to $n+m \leqslant 9$. So we are left to compute $N(f)$ for every polynomial $P(z) = z^n \pm z^m \pm 1$, where $n > m$, $\gcd(n, m) = 1$ and $n + m \leqslant 9$. In total there are 13 pairs (n, m), satisfying these conditions, namely,

$$\begin{gathered} (8,1),\ (7,2),\ (7,1),\ (6,1),\ (5,4),\ (5,3),\ (5,2),\ (5,1), \\ (4,3),\ (4,1),\ (3,2),\ (3,1),\ (2,1). \end{gathered}$$

Hence, there are exactly $4 \times 13 = 52$ polynomials $P(z) = z^n \pm z^m \pm 1$ to be considered. Applying Proposition 3.3 (one can use any mathematics software, e.g., SageMath [58]), we obtain that all such polynomials with $N(f) = 1$ and $N(f) = 2$ are given in the first and the third column of Table 3.2, respectively.

Case 2. We have that $\gcd(n, m) > 1$. Denote $a = \gcd(n, m)$. Then $n = an_1$ and $m = am_1$ for some coprime positive integers $n_1 > m_1$. Furthermore, $P(z) = z^n \pm z^m \pm 1 = g(z^a)$, where $g(z) = z^{n_1} \pm z^{m_1} \pm 1$ is a Borwein

trinomial. One has that $N(P(z)) = N(g(z^a)) = aN(g(z))$. This, in view of $a > 1$ and $N(f) \leqslant 2$, implies $a = 2$, $N(f) = 2$ and $N(g(z)) = 1$. We already determined all Borwein trinomials $g(z)$ with $N(g) = 1$ in Case 1 (see the first column in Table 3.2). Hence, $P(z) = g(z^2)$ for any polynomial $g(z)$ from the first column of Table 3.2. All such trinomials $P(z) = g(z^2)$ with $N(f) = 2$ are given in the second column of Table 3.2. □

Proof of Theorem 3.1. Let $P(z) = z^n \pm z^m \pm 1$ be a Borwein trinomial such that one of its roots, say β, is a complex Pisot number. Denote by $p(z)$ the minimal polynomial of β. Then $p(z)$ is irreducible and divides $P(z)$. By Theorem 3.4, every root (if any) of the quotient $P(z)/p(z)$ is a unimodular number (if $P(z)$ is irreducible, then $P(z) = p(z)$ and $P(z)/p(z) = 1$). Hence, both polynomials $P(z)$ and $p(z)$ have the same number of roots outside the unit circle $|z| > 1$, and this number equals 2 since $p(z)$ is the minimal polynomial of a complex Pisot number. Therefore, $N(f^*) = N(p^*) = 2$. Now we have that the Borwein trinomial $f^*(z)$ has exactly 2 roots inside the unit circle $|z| < 1$, namely β^{-1} and $\bar{\beta}^{-1}$. Recall that $\beta \in \mathbb{C}\backslash\mathbb{R}$. Thus, both roots of $f^*(z)$ inside the unit circle $|z| < 1$ are non-real numbers. On the other hand, Table 3.2 lists all Borwein trinomials $g(z)$ with $N(g) = 2$ on the second and third columns (see Theorem 3.2). One can easily check that all of these polynomials have two non-real roots inside the unit circle $|z| < 1$, except for polynomials z^4+z^2-1, $z^6 + z^4 - 1$, $z^6 + z^2 - 1$, $z^8 + z^2 - 1$ and $z^{10} + z^2 - 1$ which all have two real roots inside the unit circle $|z| < 1$. Hence, all the Borwein trinomials $P(z) = z^n \pm z^m \pm 1$, which have a complex Pisot number as a root, are given in Table 3.1. □

Chapter 4

Conclusions

The results of the dissertation lead us to the following conclusions.

1. Every Newman quadrinomial of degree $\leqslant 15$, except possibly for those listed in Table 2.1, has a Littlewood multiple.

2. Every Newman quadrinomial Q of degree $\leqslant 14$, possesses a Littlewood multiple of degree $\deg_2 \widetilde{Q} - 1$.

3. Every Newman polynomial N of degree $\leqslant 10$, except possibly for those, provided in table 2.2, has a Littlewood multiple of degree $\deg_2 \widetilde{N} - 1$.

4. There are exactly 9 monic Littlewood polynomials $P(z)$ of degree $\leqslant 12$ which are not products of cyclotomic polynomials and possess Newman multiples.

5. Any Borwein trinomial that has a complex Pisot number as its root is of the form $\pm P(\pm z)$, where $P(z)$ is one of the 17 polynomials listed in Table 3.1

Bibliography

[1] S. Akiyama. “Pisot number system and its dual tiling”. In: *Physics and theoretical computer science of NATO Secur. Sci. Ser. D Inf. Commun. Secur* 7 (Jan. 2007).

[2] S. Akiyama. “Pisot numbers and greedy algorithm”. English. In: *Number theory. Diophantine, computational and algebraic aspects. Proceedings of the international conference, Eger, Hungary, July 29–August 2, 1996*. Berlin: de Gruyter, 1998, pp. 9–21.

[3] S. Akiyama, J. M. Thuswaldner, and T. Zaïmi. “Comments on the height reducing property II”. In: *Indag. Math.* 26.1 (2015), pp. 28–39.

[4] S. Akiyama et al. “On the Pisot substitution conjecture”. English. In: *Mathematics of aperiodic order*. Basel: Birkhäuser/Springer, 2015, pp. 33–72.

[5] P. Arnoux and S. Ito. “Pisot substitutions and Rauzy fractals”. English. In: *Bull. Belg. Math. Soc. - Simon Stevin* 8.2 (2001), pp. 181–207.

[6] A. Bloch and G. Pólya. “On the Roots of Certain Algebraic Equations”. In: *Proceedings of the London Mathematical Society* 2.36 (1934), pp. 102–114.

[7] OpenMP Architecture Review Board. *OpenMP Application Program Interface Version 4.0*. 2013.

[8] P. Bohl. “Zur Theorie der trinomischen Gleichungen.” German. In: *Math. Ann.* 65 (1908), pp. 556–566.

[9] P. Borwein, T. Erdélyi, and G. Kós. “Littlewood-type problems on $[0, 1]$”. In: *Proc. London Math. Soc. (3)* 79.1 (1999), pp. 22–46.

[10] P. Borwein, T. Erdélyi, and F. Littmann. “Polynomials with coefficients from a finite set”. In: *Trans. Amer. Math. Soc.* 360.10 (2008), pp. 5145–5154.

[11] P. Borwein and K. G. Hare. “Some computations on the spectra of Pisot and Salem numbers”. In: *Math. Comp.* 71.238 (2002), pp. 767–780.

[12] P. Borwein and Ch. Pinner. “Polynomials with $\{0, +1, -1\}$ coefficients and a root close to a given point”. In: *Canad. J. Math.* 49.5 (1997), pp. 887–915.

[13] Peter Borwein et al. “On Littlewood polynomials with prescribed number of zeros inside the unit disk”. In: *Canad. J. Math.* 67.3 (2015), pp. 507–526.

[14] D. W. Boyd. “On beta expansions for Pisot numbers”. English. In: *Math. Comput.* 65.214 (1996), pp. 841–860.

[15] D. W. Boyd. “Pisot sequences which satisfy no linear recurrence”. English. In: *Acta Arith.* 32 (1976), pp. 89–98.

[16] D. W. Boyd. “Pisot sequences which satisfy no linear recurrence. II”. English. In: *Acta Arith.* 48 (1987), pp. 191–195.

[17] D. W. Boyd. “Some integer sequences related to Pisot sequences”. English. In: *Acta Arith.* 34 (1979), pp. 295–305.

[18] J. Čermák and L. Fedorková. “On a nearly forgotten polynomial result by P. Bohl”. English. In: *Am. Math. Mon.* 130.2 (2023), pp. 176–181.

[19] Ch. Chamfy. “Minimal value of the modulus for a closed set of algebraic indices”. French. In: *C. R. Acad. Sci., Paris* 244 (1957), pp. 1992–1994.

[20] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.6)*. 2017.

[21] P. Drungilas, J. Jankauskas, and J. Šiurys. “On Littlewood and Newman polynomial multiples of Borwein polynomials”. In: *Math. Comp.* 87.311 (2018), pp. 1523–1541.

[22] A. Dubickas. “A note on powers of Pisot numbers”. English. In: *Publ. Math. Debr.* 56.1-2 (2000), pp. 141–144.

[23] A. Dubickas. “Intervals without primes near elements of linear recurrence sequences”. English. In: *Int. J. Number Theory* 14.2 (2018), pp. 567–579.

[24] A. Dubickas. “Numbers expressible as a difference of two Pisot numbers”. In: *Acta Math. Hungar.* (2024).

[25] A. Dubickas and J. Jankauskas. “On Newman polynomials which divide no Littlewood polynomial”. In: *Math. Comp.* 78.265 (2009), pp. 327–344.

[26] A. Dubickas and J. Jankauskas. “On the fractional parts of powers of Pisot numbers of length at most 4”. English. In: *J. Number Theory* 144 (2014), pp. 325–339.

[27] J. Dufresnoy and Ch. Pisot. “Étude de certaines fonctions méromorphes bornées sur le cercle unité. Application à un ensemble fermé d’entiers algébriques”. French. In: *Ann. Sci. Éc. Norm. Supér. (3)* 72 (1955), pp. 69–92.

[28] J. Dufresnoy and Ch. Pisot. “Sur les dérivées successifs d’un ensemble fermé d’entiers algébriques”. French. In: *Bull. Sci. Math., II. Sér.* 77 (1953), pp. 129–136.

[29] M. Filaseta and I. Solan. “An extension of a theorem of Ljunggren”. English. In: *Math. Scand.* 84.1 (1999), pp. 5–10.

[30] C. Finch and L. Jones. “On the irreducibility of $\{-1, 0, 1\}$-quadrinomials”. In: *Integers* 6 (2006), A16, 4.

[31] C. Frougny. “Representations of numbers and finite automata”. In: *Math. Systems Theory* 25 (1992).

[32] D. Garth. “Complex Pisot numbers of small modulus.” English. In: *C. R., Math., Acad. Sci. Paris* 336.12 (2003), pp. 967–970.

[33] D. Garth. *Small limit points of sets of algebraic integers*. Thesis (Ph.D.)–Kansas State University. ProQuest LLC, Ann Arbor, MI, 2000, p. 156.

[34] M. Hama, M. Furukado, and Shunji Ito. “Complex Pisot numeration systems”. In: *Comment. Math. Univ. St. Pauli* 58.1 (2009), pp. 9–49.

[35] K. G. Hare and J. Jankauskas. “On Newman and Littlewood polynomials with a prescribed number of zeros inside the unit disk”. English. In: *Math. Comput.* 90.328 (2021), pp. 831–870.

[36] K. G. Hare, Z. Masáková, and T. Vávra. “On the spectra of Pisot-cyclotomic numbers”. In: *Lett. Math. Phys.* 108.7 (2018), pp. 1729–1756.

[37] K. G. Hare and M. J. Mossinghoff. “Negative Pisot and Salem numbers as roots of Newman polynomials”. In: *Rocky Mountain J. Math.* 44.1 (2014), pp. 113–138.

[38] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. *An introduction to mathematical cryptography*. Second. Undergraduate Texts in Mathematics. Springer, New York, 2014, pp. xviii+538.

[39] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. "NTRU: a ring-based public key cryptosystem". In: *Algorithmic number theory (Portland, OR, 1998)*. Vol. 1423. Lecture Notes in Comput. Sci. Springer, Berlin, 1998, pp. 267–288.

[40] F. Johansson. "Arb: a C library for ball arithmetic". In: *ACM Communications in Computer Algebra* 47.4 (2013), pp. 166–169.

[41] H. Kaneko and M. Kawashima. "The digit exchanges in the rotational beta expansions of algebraic numbers". English. In: *J. Number Theory* 241 (2022), pp. 430–449.

[42] J. B. Kelly. "A closed set of algebraic integers". English. In: *Am. J. Math.* 72 (1950), pp. 565–572.

[43] B. Koley and S.R. Arikatla. "Cyclotomic factors of Borwein polynomials". In: *Bull. Aust. Math. Soc.* 100.1 (2019), pp. 41–47.

[44] Ka-Sing Lau. "Dimension of a family of singular Bernoulli convolutions". In: *J. Funct. Anal.* 116 (1993), pp. 335–358.

[45] J. E. Littlewood. *Some Problems in Real and Complex Analysis*. Dover Publications, 1968.

[46] W. Ljunggren. "On the irreducibility of certain trinomials and quadrinomials". English. In: *Math. Scand.* 8 (1960), pp. 65–70.

[47] M. Mossinghoff, C. Pinner, and J. Vaaler. "Perturbing polynomials with all their roots on the unit circle". In: *Mathematics of Computation* (1998).

[48] D. J. Newman and J. S. Byrnes. "The L^4 norm of a polynomial with coefficients ± 1". In: *Amer. Math. Monthly* 97.1 (1990), pp. 42–45.

[49] A. M. Odlyzko and B. Poonen. "Zeros of polynomials with 0,1 coefficients". In: *Enseign. Math. (2)* 39.3–4 (1993), pp. 317–384.

[50] R. Salem. "A remarkable class of algebraic integers. Proof of a conjecture of Vijayaraghavan". English. In: *Duke Math. J.* 11 (1944), pp. 103–108.

[51] R. Salem. *Algebraic numbers and Fourier analysis*. English. Boston: D. C. Heath and Company. 66 p. (1963). Boston, Mass., 1963.

[52] R. Salem. “Power series with integral coefficients”. English. In: *Duke Math. J.* 12 (1945), pp. 153–172.

[53] P. A. Samet. “Algebraic integers with two conjugates outside the unit circle. II”. English. In: *Proc. Camb. Philos. Soc.* 50 (1954), p. 346.

[54] E. S. Selmer. “On the irreducibility of certain trinomials”. English. In: *Math. Scand.* 4 (1956), pp. 287–302.

[55] C. D. Sinclair and M. L. Yattselev. “Root statistics of random polynomials with bounded Mahler measure”. In: *Advances in Mathematics* (2015).

[56] D. Stankov. “On spectra of neither Pisot nor Salem algebraic integers”. In: *Monatsh. Math.* 159 (2010), pp. 115–131.

[57] P. Surer. “Representations for complex numbers with integer digits”. In: *Research in Number Theory* 6.4 (2020), p. 47.

[58] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.2)*. `https://www.sagemath.org`. 2023.

[59] T. Theobald and T. de Wolff. “Norms of roots of trinomials”. English. In: *Math. Ann.* 366.1-2 (2016), pp. 219–247.

[60] V. Todorčević. *Harmonic quasiconformal mappings and hyperbolic type metrics*. Springer, Cham, 2019, pp. xvii+163.

[61] H. Tverberg. “On the irreducibility of the trinomials $x^n \pm x^m \pm 1$”. English. In: *Math. Scand.* 8 (1960), pp. 121–126.

[62] T. Zaïmi. “On real parts of powers of complex Pisot numbers”. English. In: *Bull. Aust. Math. Soc.* 94.2 (2016), pp. 245–253.

[63] T. Zaïmi. “On Salem numbers which are Mahler measures of nonreciprocal 2-Pisot numbers”. English. In: *Publ. Math. Debr.* 98.3-4 (2021), pp. 467–474.

[64] T. Zaïmi. *On the distances between Pisot numbers generating the same number field*. 2024. arXiv: `2402.06182 [math.NT]`.

[65] T. Zaïmi. “On the distribution of powers of a Gaussian Pisot number”. English. In: *Indag. Math., New Ser.* 31.1 (2020), pp. 177–183.

[66] T. Zaïmi. “Quartic Salem numbers which are Mahler measures of nonreciprocal 2-Pisot numbers”. English. In: *J. Théor. Nombres Bordx.* 32.3 (2020), pp. 877–889.

[67] T. Zaïmi. “Salem numbers as Mahler measures of Gaussian Pisot numbers”. English. In: *Acta Arith.* 194.4 (2020), pp. 383–392.

Santrauka (Summary in Lithuanian)

Pagrindinis šios disertacijos objektas yra polinomai su aprėžtais koeficientais. Polinomas

$$P(z) = a_d z^d + a_{d-1} z^{d-1} + \cdots + a_1 z + a_0 \in \mathbb{Z}[z]$$

su nenuliniu koeficientu a_0 vadinamas *Borveino* (Borwein) polinomu, jei $a_j \in \{-1,\, 0, 1\}$ kiekvienam $0 \leqslant j \leqslant d$. Pirmajame skyriuje pristatome pagrindines šiame darbe nagrinėjamas problemas ir pateikiame susijusių tyrimų bei istorinių rezultatų apžvalgą. Antrajame skyriuje analizuojame du Borveino polinomų poaibius ir nagrinėjame jų dalumo savybes. Trečiasis skyrius skirtas Borveino trinomų, turinčių specialias šaknis, paieškai.

5.1 Aktualumas

Polinomų savybių supratimas yra labai svarbus, nes jie sudaro algebros pagrindą ir yra taikomi ne tik teorinėje bei taikomojoje matematikoje, bet ir fizikos, inžinerijos bei ekonomikos uždaviniuose. Ypač dažnai mažo aukščio polinomai figūruoja Diofantinėse lygtyse, aproksimacijos teorijoje, valdymo teorijoje, algebrinėje geometrijoje ir kriptografijoje. Pavyzdžiui, plačiai naudojamoje NTRU[1] šifravimo sistemoje, Borveino polinomai naudojami kuriant viešuosius ir privačiuosius raktus [39, 38]. Be to, daug algoritmų geriau veikia su mažo aukščio polinomais dėl mažesnio skaičiavimų sudėtingumo.

Pizo (Pisot) skaičiai (žr. apibrėžimą po 2.4 teoremos 5.3 skyrelyje) yra svarbūs įvairiose matematikos disciplinose dėl jų unikalių algebrinių ir analizinių savybių. Pizo skaičiai yra glaudžiai susiję su algebrinės skaičių teorijos,

[1] Nth-degree Truncated Polynomial Ring Unit

kūnų teorijos, Diofantinių aproksimacijų, dinaminių sistemų ir fraktalinės geometrijos uždaviniais.

5.2 Tikslas ir uždaviniai

Disertacijos tikslas yra suprasti tam tikrų polinomų su aprėžtais koeficientais savybes. Konkrečiai, nagrinėjame du Borveino polinomų poaibius - *Litlvudo* (Littlewood) polinomus, kurių visi koeficientai priklauso aibei $\{-1, 1\}$, ir *Niumeno* (Newman) polinomus, kurių kiekvienas koeficientas yra lygus 0 arba 1. Nagrinėjami tokie klausimai:

1. Tegul $\mathcal{D} \subset \mathbb{Z}$ yra baigtinė aibė, o P yra polinomas su sveikaisiais koeficientais. Ar egzistuoja toks nenulinis polinomas su koeficientais iš $\mathcal{D}$, kuris dalijasi iš P?
2. Ar egzistuoja Niumeno keturnomas, kuris neturi Litlvudo kartotinio?
3. Kurie Litlvudo polinomai turi Niumeno kartotinius?
4. Kurie Niumeno polinomai turi laipsnio $\deg_2 \widetilde{P} - 1$ Litlvudo kartotinį? (Žr. 2.2 skyrelį.)
5. Kiek yra Borveino trinomų, kurių bent viena šaknis yra kompleksinis Pizo skaičius?

5.3 Literatūros apžvalga ir pagrindiniai rezultatai

Yra žinoma, kad polinomo koeficientų aprėžtumas lemia glaudesnį to polinomo šaknų išsidėstymą kompleksinėje plokštumoje (žr., pavyzdžiui, [55]). Šis ryšys turi didelę reikšmę polinomų konstravimui ir analizei tokiose srityse kaip Diofantinės lygtys ir signalų apdorojimas.

Pirmą reikšmingą tyrimą šioje srityje atliko Bloch ir Pólya [6] 1934 m. Jie nagrinėjo polinomus, kurių kiekvienas koeficientas priklauso aibei {-1, 0, 1}; tokie polinomai dar vadinami Borveino polinomais (žr., pavyzdžiui, [21] ir [43]). Šiame darbe jie tyrinėjo kiek daugiausiai šaknų intervale $(0, 1)$ gali turėti Borveino polinomas.

Praėjus beveik šimtmečiui, susidomėjimas Borveino polinomais neišblėso. Šiandien turime daug rezultatų apie Borveino polinomų redukuojamumą (žr., pavyzdžiui, [30], [46], [49], [61], [43]), jų šaknų pasiskirstymą (žr., pavyz-

džiui, [12], [47], [9], [45]), fraktalinę geometriją (žr., pavyzdžiui, [10], [49], [12]) ir kitas algebrines savybes (žr., pavyzdžiui, [48]).

Bendruoju atveju, 1 klausimas (žr. 5.2 skyrelį) yra sudėtingas ir į jį buvo atsakyta tik specifiniais atvejais, smarkiai apribojant tiek skaitmenų aibę $\mathcal{D}$, tiek polinomus P. Be algebrinių savybių taikymo, šią problemą galima spręsti ir kompiuteriniais metodais. Drungilas, Jankauskas ir Šiurys [21] pasiūlė algoritmą, kuris gali atsakyti į šį klausimą, jei polinomas $P(z)$ neturi šaknų ant vienetinio apskritimo $|z| = 1$ kompleksinėje plokštumoje. Jie pilnai suklasifikavo Borveino polinomus, kurių laipsnis yra ne didesnis negu 9, skaitmenų aibėms $\mathcal{D} = \{0, 1\}$ ir $\mathcal{D} = \{-1, 1\}$.

Atrodo, kad pirmasis tokio algoritmo pavyzdys pasirodė Frougny darbe [31] apie skaičių, generuojamų baigtiniais automatais, išraiškas skaičiavimo sistemose, kurių bazė yra sveikasis algebrinis skaičius. Lau [44] pasiūlė šiek tiek kitokią šio algoritmo versiją, kuri buvo naudojama Bernulio matų diskretumo savybei nustatyti. Jis atsakė į 1 klausimą (žr. 5.2 skyrelį) tuo atveju, kai aibė $\mathcal{D} = \{-1, 0, 1\}$ ir $P(z)$ yra Pizo skaičiaus minimalusis polinomas. Vėliau, Hare su bendraautoriais [11, 37] panaudojo tą patį algoritmą skaičiuodami Pizo skaičių diskrečiuosius spektrus. Stankov [56] nagrinėjo algebrinių sveikųjų skaičių, kurie nėra Pizo skaičiai, spektrus. Akiyama, Thuswaldner ir Zaïmi [3, Th. 3] sprendė 1 uždavinį *aukščio mažinimo problemos* kontekste ir sukūrė algoritmą, kuris iš esmės yra panašus į tą, kurį pasiūlė Frougny [31]. Taigi, 1 klausimas buvo pilnai atsakytas polinomams $P(z) \in \mathbb{Z}[z]$, kurie neturi kartotinių šaknų, neturintiems šaknų ant vienetinio apskritimo ir kurių vyriausiasis koeficientas lygus 1. Kita vertus, algoritmo, sukurto [21], atveju polinomas $P(z) \in \mathbb{Z}[z]$ gali turėti kartotinių šaknų.

Sakysime, kad polinomas $P(z)$ turi Litlvudo kartotinį, jei jis dalija kokį nors Litlvudo polinomą. Panašiai, sakysime, kad polinomas turi Niumeno kartotinį, jei jis dalija kokį nors nenulinį Niumeno polinomą. Darbe [21] realizuoto algoritmo pagalba (žr. 2.4 skyrelį), į 1 klausimą buvo gautas atsakymas visiems Borveino polinomams, kurių laipsnis neviršija 9, ir skaitmenų aibėms $\mathcal{D} = \{0, 1\}$ ir $\mathcal{D} = \{-1, 1\}$. Tiksliau sakant, kiekvienam Borveino polinomui, kurio laipsnis ne didesnis kaip 9, buvo nustatyta, ar jis turi Litlvudo arba Niumeno kartotinį. Be to, kiekvienam Niumeno polinomui $P(z)$, kurio laipsnis ne didesnis kaip 11, buvo patikrinta, ar $P(z)$ turi Litlvudo kartotinį. Pagrindinis šio straipsnio rezultatas yra toks:

A teorema ([21])**.** *Kiekvienas Borveino polinomas, kurio laipsnis neviršija 8 ir kuris turi Niumeno kartotinį, taip pat turi ir Litlvudo kartotinį.*

Šie skaičiavimai pratęsė anksčiau Dubicko ir Jankausko [25], Borveino ir Hare [11], Hare ir Mossinghoff [37] gautus rezultatus.

Mums pavyko šiuos rezultatus išplėsti dar labiau. Pažymėkime $\mathcal{B}$, $\mathcal{N}$ ir $\mathcal{L}$ atitinkamai visų Borveino, Niumeno ir Litlvudo polinomų aibes. Sakome, kad polinomas

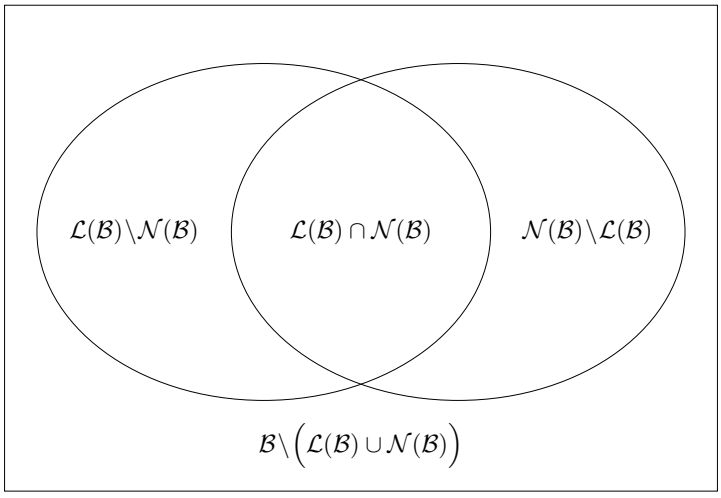
$$P(z) = a_d z^d + a_{d-1} z^{d-1} + \cdots + a_1 z + a_0 \in \mathbb{Z}[z]$$

yra *trinomas*, jei lygiai trys jo koeficientai a_j, $0 \leqslant j \leqslant d$ nėra lygūs nuliui. Atitinkamai, jei nenulinių koeficientų skaičius yra keturi, polinomas $P(z)$ yra vadinamas *keturnomu*.

Norėdami nagrinėti tik tam tikro laipsnio polinomus, naudosime indeksą d. Pavyzdžiui, aibė $\mathcal{N}_d$ sudaryta iš visų d-tojo laipsnio Niumeno polinomų. Panašiai, indeksas „$\leqslant d$“ reikš, kad aibę sudarančių polinomų laipsnis yra *ne daugiau* kaip d, t.y.,

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

Tarkime, $\mathcal{A} \subset \mathbb{Z}[z]$. $\mathcal{L}(\mathcal{A})$ žymime aibę polinomų $P(z) \in \mathcal{A}$, kurie dalijasi iš kurio nors Litlvudo polinomo. Atitinkamai, $\mathcal{N}(\mathcal{A})$ žymime aibę polinomų $P(z) \in \mathcal{A}$, kurie dalijasi iš kurio nors Niumeno polinomo.



5.1 pav.: Borveino polinomų aibės dekompozicija.

Pavyzdžiui, aibė $\mathcal{N}_d\setminus\mathcal{L}(\mathcal{N})$ sudaryta iš tų Niumeno polinomų, kurių laips-

nis yra d, ir kurie nedalija jokio Litlvudo polinomo, tuo tarpu aibė $\mathcal{L}_{\leqslant d} \setminus \mathcal{N}(\mathcal{L})$ sudaryta iš tų Litlvudo polinomų, kurių laipsnis yra ne didesnis nei d, ir kurie nedalija jokio Niumeno polinomo.

Akivaizdu, kad jei polinomo $P(z)$ visi koeficientai yra neneigiami, tai jis negali turėti teigiamų realiųjų šaknų. Taigi, jei koks nors Litlvudo polinomas turi šaknį, kuri yra teigiamas realusis skaičius, tuomet toks polinomas neturi Niumeno kartotinių.

Mūsų skaičiavimai rodo, kad

2.2 teorema. *Kiekvienas keturnomas $Q \in \mathcal{N}_{\leqslant 15}$, išskyrus galbūt tuos, kurie nurodyti 2.1 lentelėje, dalija tam tikrą Litlvudo polinomą. Be to, kiekvienas keturnomas $Q \in \mathcal{N}_{\leqslant 14}$ turi Litlvudo kartotinį, kurio laipsnis lygus $\deg_2 \widetilde{Q} - 1$ (ši reikšmė apibrėžta 2.2 skyrelyje).*

Keturnomas $Q(z)$	$\deg_2 \widetilde{Q} - 1$
$z^{15} + z^{14} + z^{10} + 1$	10921
$z^{15} + z^{12} + z^{10} + 1$	32765
$z^{15} + z^{12} + z^4 + 1$	31681
$z^{15} + z^8 + z^6 + 1$	32765

2.1 lentelė: Niumeno keturnomai $Q \in \mathcal{N}_{\leqslant 15}$, kuriems nežinoma, ar jie turi bent vieną Litlvudo kartotinį (simetriniai polinomai praleisti).

Darbe [21] buvo įrodyta, kad jei Niumeno keturnomas Q turi Litlvudo kartotinį L, tuomet $\deg L \geqslant \deg_2 \widetilde{Q} - 1$. Pavyzdžiui, jei keturnomas $z^{15} + z^8 + z^6 + 1$ dalija Litlvudo polinomą $P(z)$, tuomet $\deg P \geqslant 32765$ (žr. 2.1 lentelės antrąjį stulpelį).

2.3 teorema. *Kiekvienas polinomas $P(z) \in \mathcal{L}(\mathcal{N}_{\leqslant 10})$, išskyrus, galbūt tuos, kurie yra nurodyti 2.2 lentelėje, turi Litlvudo kartotinį, kurio laipsnis lygus $\deg_2 \widetilde{P} - 1$.*

n	$P_n(z)$	$\deg_2 \widetilde{P_n} - 1$
1	$z^9 + z^8 + z^6 + z^5 + z^4 + z^3 + z + 1$	59
2	$z^{10} + z^9 + z^8 + z^3 + z^2 + 1$	1019
3	$z^{10} + z^9 + z^7 + z^6 + z^5 + 1$	1021

2.2 lentelė: Polinomai $P(z) \in \mathcal{L}(\mathcal{N}_{\leqslant 10})$, kuriems nėra žinoma, ar jie dalija kokį nors Litlvudo polinomą (simetriniai polinomai praleisti).

Darbe [21] (žr. 18 teiginį) buvo įrodyta, kad jei $P(z) \in \mathbb{Z}[z]$ yra ciklotominių polinomų sandauga (kiekviena $P(z)$ šaknis yra šaknis iš vieneto) ir $P(1) \neq 0$, tada $P(z)$ turi Niumeno kartotinį. Todėl Litlvudo polinomai, kurie yra ciklotominių polinomų sandaugos ir skaičius $z = 1$ nėra jų šaknis, taip pat turi Niumeno kartotinius. Motyvuoti šio rezultato, suskaičiavome aibes $\mathcal{N}(\mathcal{L}_d)$ mažiems laipsniams d. Atlikę skaičiavimus pagal algoritmą, aprašytą 2.4 skyrelyje, kiekvienam Litlvudo polinomui $L(z) \in \mathcal{L}_{\leqslant 12}$, suskaičiavome visus netrivialius aibės $\mathcal{N}(\mathcal{L}_{\leqslant 12})$ elementus (žr. 2.3 lentelę).

2.4 teorema. *Yra lygiai devyni netrivialūs Litlvudo polinomai (jie nėra ciklotominių polinomų sandaugos), kurių laipsnis ne didesnis negu 12, vyriausiasis koeficientas lygus 1, ir kurie turi Niumeno kartotinius.*

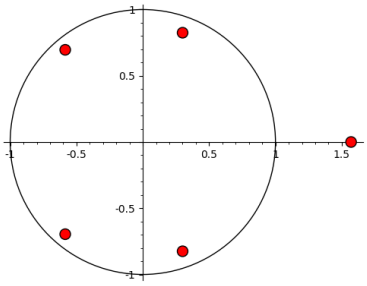
k	$P_k(z)$
1	$z^6 + z^5 - z^4 - z^3 - z^2 + z + 1$
2	$z^7 + z^6 - z^5 + z^4 + z^3 - z^2 + z + 1$
3	$z^8 + z^7 - z^6 - z^5 + z^4 - z^3 - z^2 + z + 1$
4	$z^9 + z^8 + z^7 - z^6 - z^5 - z^4 - z^3 + z^2 + z + 1$
5	$z^{10} - z^9 + z^8 + z^7 - z^6 + z^5 - z^4 + z^3 + z^2 - z + 1$
6	$z^{10} + z^9 + z^8 - z^7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

2.3 lentelė: Netrivialūs polinomai iš $\mathcal{N}(\mathcal{L}_{\leqslant 12})$, kurių vyriausiasis koeficientas lygus 1.

Išsamiau šie rezultatai aprašyti 2 skyriuje. Taip pat jame pateikta daugiau detalių apie algoritmą ir skaičiavimus.

Norėdami atsakyti į 5 klausimą (žr. 5.2 skyrelį), pirmiausia apibrėšime Pizo skaičius. Realusis sveikasis algebrinis skaičius $\alpha > 1$ yra vadinamas *Pizo skaičiumi* (žr., pavyzdžiui, [27, 28]), jei visi jo algebriniai jungtiniai skaičiai virš racionaliųjų skaičių kūno $\mathbb{Q}$ (išskyrus patį α) yra moduliu mažesni už 1. Pizo skaičiaus minimalusis polinomas vadinamas Pizo polinomu.

Pizo skaičiai sulaukia daug dėmesio tiriant skaičių skleidinius, kuriuose skleidinio bazė yra algebrinis skaičius (žr., pavyzdžiui, [2, 14]), plokštumos padengimo algoritmus (žr., pavyzdžiui, [1, 4, 5]), sveikųjų skaičių sekas susijusias su tiesinais rekurentiniais sąryšiais (žr., pavyzdžiui, [15, 17, 16]), realiųjų



5.2 pav.: Pizo polinomo $z^5 - z^4 - z^2 - 1$ šaknys.

skaičių laipsnių trupmeninių dalių pasiskirstymus (žr., pavyzdžiui, [22, 23]) ir daugelyje kitų sričių (žr., pavyzdžiui, [24, 64]).

Pastebėkime, kad norint rasti polinomą P, kurio bent viena šaknis yra Pizo skaičius, nebūtina rasti visų polinomo P šaknų. Pakanka suprasti, kaip polinomo šaknys pasiskirsčiusios kompleksinėje plokštumoje vienetinio apskritimo atvžvilgiu. T.y., užtenka parodyti, kad P dalijasi iš neredukuojamo polinomo Q, kuris turi tik vieną realiąją šaknį, didesnę už 1, ir kurio visos kitos šaknys yra moduliu mažesnės nei 1. Kitaip tariant, pakanka nustatyti polinomo šaknų skaičių tam tikrose kompleksinės plokštumos srityse.

Tarkime, kad polinomas $P(z)$ virš kompleksinių skaičių kūno $\mathbb{C}$ išsiskaido taip:

$$P(z) = a_n(z - \alpha_1)(z - \alpha_2)\cdots(z - \alpha_n),$$

čia skaičiai $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ nebūtinai yra skirtingi. Vienetinio apskritimo atžvilgiu, kompleksinėje plokštumoje $P(z)$ šaknis skaičiuojančias funkcijas žymėsime

$$N(P) = \#\{j,\, 1 \leqslant j \leqslant n : |\alpha_j| < 1\}$$

ir

$$U(P) = \#\{j,\, 1 \leqslant j \leqslant n : |\alpha_j| = 1\},$$

kur šaknys yra skaičiuojamos su kartotinumais.

Pavyzdžiui, Pizo polinomas $P(z) = z^5 - z^4 - z^2 - 1$ turi 4 šaknis vienetinio apskritimo viduje ir nė vienos ant šio apskritimo (žr. 5.2 pav.), todėl $N(P) = 4$ ir $U(P) = 0$. Iš tikrųjų, bet kuriam Pizo polinomui P teisingos lygybės $U(P) = 0$ ir $N(P) = \deg P - 1$.

Bendruoju atveju $N(P)$ ir $U(P)$ formulės nėra žinomos, tačiau specifiniams polinomams šios reikšmės jau buvo nagrinėtos. Pavyzdžiui, [13] buvo įrodyta tokia teorema Litlvudo polinomų poaibiui:

B teorema ([13]). *Tegul $n \geqslant k$ yra teigiami sveikieji skaičiai, DBD$(k, n+1) = d$. n-tojo laipsnio polinomui $P(z) \in \{\pm 1\}[z]$ su vienu ženklo pasikeitimu (kuris yra tarp narių z^k ir z^{k-1}) teisingos lygybės*

$$N(P) = \begin{cases} k & \text{jei } n > 2k-1, \\ 0 & \text{jei } n = 2k-1, \\ k-d & \text{jei } n < 2k-1, \end{cases}$$

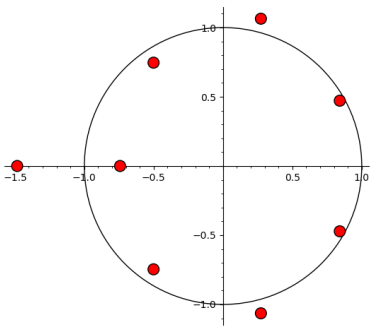
ir

$$U(P) = \begin{cases} d-1 & \text{jei } n \neq 2k-1, \\ n & \text{jei } n = 2k-1. \end{cases}$$

Vėliau, Hare ir Jankauskas [35] ieškojo natūraliųjų skaičių porų (k, n), kurioms egzistuoja n-tojo laipsnio Niumeno ir Litlvudo polinomai, turintys lygiai k šaknų vienetinio apskritimo $|z| = 1$ viduje ir nė vienos ant šio apskritimo. Pagrindinis jų gautas rezultatas apie Niumeno polinomus yra ši teorema:

C teorema ([35]). *Bet kokiai natūraliųjų skaičių porai (k, n), tenkinančiai nelygybes $n \geqslant 7$ ir $3 \leqslant k \leqslant n-3$, egzistuoja toks n-tojo laipsnio Niumeno polinomas P, kad $N(P) = k$ ir $U(P) = 0$.*

Pavyzdžiui, pasinaudoję jų metodu skaičių porai $(5, 8)$, galime rasti 8-ojo laipsnio Niumeno polinomą $P(z) = z^8 + z^7 + z^5 + z + 1$, kuris turi lygiai 5 šaknis vienetinio apskritimo viduje ir nė vienos šaknies ant to apskritimo (žr. 5.3 pav.).



5.3 pav.: $P(z) = z^8 + z^7 + z^5 + z + 1$

Prieš daugiau nei šimtmetį, latvių matematikas *Piers Bohl* įrodė štai tokią teoremą apie trinomus, kuri yra esminė įrodant mūsų rezultatus 3.4 skyrelyje.

D teorema (Bohl, [8, 59]). *Tegul $P(z) = z^n + pz^m + q$ yra trinomas, kur $p, q \in \mathbb{C}$, o m ir n yra tarpusavyje pirminiai natūralieji skaičiai ir $n > m > 0$. Tarkime, kad realiajam skaičiui $v > 0$ egzistuoja trikampis, kurio kraštinių ilgiai yra v^n, $|p|v^m$ ir $|q|$. Pažymėkime $\alpha = \angle(|p|v^m, |q|)$ ir $\beta = \angle(v^n, |q|)$. Tuomet polinomo $P(z)$ kompleksinių šaknų, priklausančių apskritimui $|z| < v$, skaičius lygus sveikųjų skaičių, priklausančių intervalui $(C_P - \delta_P, C_P + \delta_P)$, skaičiui; čia*

$$C_P = \frac{n\left(\pi + \arg(p) - \arg(q)\right) - m\left(\pi - \arg(q)\right)}{2\pi}$$

ir

$$\delta_P = \frac{n\alpha + m\beta}{2\pi}.$$

Pritaikę D teoremą, gavome paprastas formules, kurios leidžia nustatyti Borveino trinomų šaknų skaičių vienetinio apskritimo viduje.

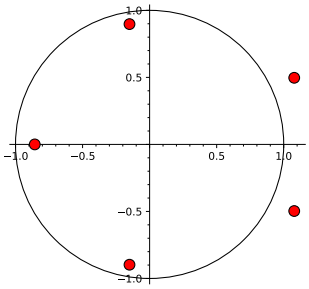
3.3 Teiginys. *Tegul $n > m$ yra tarpusavyje pirminiai sveikieji skaičiai. Tuomet*

$$\begin{aligned}
N(z^n + z^m + 1) &= n - m - 1 - 2\left\lfloor \frac{n-2m}{3} \right\rfloor, \\
N(z^n + z^m - 1) &= 2\left\lceil \frac{n+m}{6} \right\rceil - 1, \\
N(z^n - z^m + 1) &= 2\left\lceil \frac{n+4m}{6} \right\rceil - m - 1, \\
N(z^n - z^m - 1) &= n - 2\left\lfloor \frac{2n-m}{6} \right\rfloor - 1.
\end{aligned}$$

3 skyriuje taip pat įrodome analogiškas formules funkcijai $U(P)$ ir polinomo P šaknų skaičiui vienetinio apskritimo išorėje visiems Borveino trinomams.

Visi (realūs) Pizo binomai, trinomai ir keturnomai jau buvo surasti Dubicko ir Jankausko darbe [26]. Naujesnėje literatūroje didėja susidomėjimas skaičiavimo sistemomis, kurių pagrindas yra kompleksinis skaičius (žr., pavyzdžiui, [34, 36, 41, 57]); algebrinių skaičių laipsnių pasiskirstymu kompleksinėje plokštumoje Gauso gardelės $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\}$ atžvilgiu (žr., pavyzdžiui, [62, 65]); kompleksiniais algebriniais sveikaisiais skaičiais su tam tikromis daugybos savybėmis (žr., pavyzdžiui, [60, 63, 66, 67]). Šiose srityse kompleksiniai Pizo skaičių analogai kompleksinėje plokštumoje $\mathbb{C}$ vaidina tą pačią esminę rolę kaip ir Pizo skaičiai realiųjų skaičių

aibėje $\mathbb{R}$. Priminsime, kad sveikasis algebrinis skaičius $\beta \in \mathbb{C}\setminus\mathbb{R}$, $|\beta| > 1$, yra vadinamas *kompleksiniu Pizo skaičiumi*, jei visi jo algebriniai jungtiniai $\beta' \notin \{\beta, \bar{\beta}\}$ tenkina nelygybę $|\beta'| < 1$. Minimalus kompleksinio Pizo skaičiaus polinomas yra vadinamas kompleksiniu Pizo polinomu. Pastebėkime, kad n-tojo laipsnio kompleksiniam Pizo polinomui P teisingos lygybės $N(P) = n - 2$ ir $U(P) = 0$.



5.4 pav.: Kompleksinio Pizo polinomo $z^5 - z^4 + 1$ šaknys.

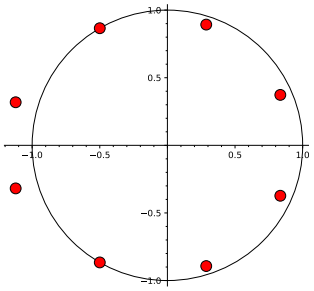
Kompleksinius Pizo skaičius pirmieji nagrinėjo Kelly ir Samet [42, 53]. Mažiausius kompleksinius Pizo skaičius nustatė Chamfy [19]; vėliau Garth [33, 32] gerokai išplėtė Chamfy gautą sąrašą. Naujausi tyrimai rodo didėjantį susidomėjimą kompleksinių Pizo skaičių spektru.

Mus domina kompleksiniai Pizo skaičiai, kurie yra pačių paprasčiausių polinomų – Borveino trinomų $z^n \pm z^m \pm 1$ – šaknys. Pagrindinis 3 skyriaus rezultatas yra tokia teorema:

3.1 teorema. *Jei kompleksinis Pizo skaičius yra Borveino trinomo šaknis, tai šis trinomas turi pavidalą $\pm P(\pm z)$, kur $P(z)$ yra vienas iš 17 polinomų, išvardintų 3.1 lentelėje.*

$z^3 - z^2 + 1$	$z^5 - z^4 + 1$	$z^7 - z^6 + 1$
$z^3 + z + 1$	$z^5 + z^3 + 1$	$z^7 + z^5 + 1$
$z^4 + z^2 - 1$	$z^5 + z + 1$	$z^8 + z^6 - 1$
$z^4 + z^3 + 1$	$z^6 - z^2 + 1$	$z^8 + z^7 + 1$
$z^4 + z + 1$	$z^6 + z^4 + 1$	$z^{10} + z^8 + 1$
$z^5 - z^2 + 1$	$z^6 + z^5 + 1$	

3.1 lentelė: Borveino trinomai, kurių bent viena šaknis yra kompleksinis Pizo skaičius (po vieną atstovą iš kiekvienos $\pm P(\pm z)$ šeimos).



5.5 pav.: Borveino trinomo $z^8 + z^7 + 1$ šaknys.

Rezultatų įrodymai bei keletas papildomų išvadų pateikiami 3 skyriuje.

5.4 Išvados

Disertacijos rezultatai leidžia padaryti šias išvadas:

1. Kiekvienas Niumeno keturnomas, kurio laipsnis neviršija 15, išskyrus, galbūt pateiktus 2.1 lentelėje, turi Litlvudo kartotinį.

2. Kiekvienas Niumeno keturnomas Q, kurio laipsnis yra ne didesnis nei 14, turi Litlvudo kartotinį, kurio laipsnis yra $\deg_2 \widetilde{Q} - 1$.

3. Kiekvienas Niumeno polinomas N, kurio laipsnis neviršija 10, išskyrus, galbūt pateiktus 2.2 lentelėje, turi laipsnio $\deg_2 \widetilde{N} - 1$ Litlvudo kartotinį.

4. Nustatyti visi Litlvudo polinomai, kurių laipsnis ne didesnis negu 12, ir kurie turi Niumeno kartotinius.

5. Nustatyti visi Borveino trinomai, kurių bent viena šaknis yra kompleksinis Pizo skaičius.

5.5 Naujumas

Visi rezultatai pateikti šioje disertacijoje yra nauji ir originalūs. Borveino polinomų kartotinių skaičiavimai Litlvudo ir Niumeno polinomų aibėse praplečia ir papildo ankstesnius, kitų autorių gautus rezultatus. Gauti rezultatai yra išspausdinti recenzuojamuose žurnaluose, bei buvo pristatyti tarptautinėse konferencijose.

5.6 Metodai

Antrame disertacijos skyriuje pateikti skaičiavimų rezultatai yra gauti pasitelkus Vilniaus Universiteto superkompiuterio resursus, bei anksčiau sukurtą algoritmą, kurio kodas yra parašytas *C* programavimo kalba. Algoritmas konstruoja orientuotą grafą, kurio viršūnės atitinka skirtingus Litlvudo arba Niumeno polinomus ir jame atlieka paiešką. Trečiame skyriuje pateikti rezultatai remiasi klasikiniais algebros ir skaičių teorijos metodais.

5.7 Aprobacija

Disertacijos rezultatai buvo pristatyti šiose mokslinėse konferencijose:

- Tarptautinė tikimybių teorijos ir skaičių teorijos konferencija (2023 m., Palanga, Lietuva)
- Tarptautinė mokslinė konferencija skirta prof. dr. Hermano Minkovskio (Hermann Minkowski) gimimo 160-ies metų jubiliejui (2024 m., Kaunas, Lietuva)
- Lietuvos matematikų draugijos konferencija (2024 m., Šiauliai, Lietuva)

5.8 Publikacijos

Disertacijos rezultatai yra paskelbti šiuose straipsniuose:

- P. Drungilas, J. Jankauskas, G. Junevičius, L. Klebonas, J. Šiurys, *On certain multiples of Littlewood and Newman polynomials*, Bull. Korean Math. Soc. 55(5) (2018) 1491-1501.
- P. Drungilas, J. Jankauskas, G. Junevičius, *On Complex Pisot Numbers That Are Roots of Borwein Trinomials*, Mathematics 12 (8) (2024), 1129.

5.9 Konferencijų tezės

- G. Junevičius. On Complex Pisot Numbers That are Roots of Borwein Trinomials. Tarptautinė mokslinė konferencija skirta prof. dr. Hermano Minkovskio (Hermann Minkowski) gimimo 160-ies metų jubiliejui, June 20-22, 2024, Kaunas, Lietuva

- G. Junevičius. On Complex Pisot Numbers That are Roots of Borwein Trinomials. Lietuvos matematikų draugijos konferencija, June 27-28, 2024, Šiauliai, Lietuva. https://www.lmd2024.sa.vu.lt/wp-content/uploads/2024/06/LMD_65_tezes.pdf

5.10 Trumpai apie autorių

Gimimo data ir vieta:
1994 m. balandžio 26 d., Kaunas, Lietuva.

Išsilavinimas:
2013 m. Vilniaus Salomėjos Nėries gimnazija, vidurinis išsilavinimas.
2017 m. Vilniaus universitetas. Matematika ir matematikos taikymai, bakalauro laipsnis (Cum Laude).
2019 m. Vilniaus universitetas. Matematika, magistro laipsnis.
2024 m. Vilniaus universitetas. Matematika, doktorantūros studijos.

Darbo patirtis:
2016 - 2018: IT pagalbos specialistas, Western Union.
2017 - 2018: Laborantas, VU MIF.
2018 - 2020: Duomenų mokslininkas, Nielsen.
2020 - 2021: Duomenų mokslininkas, Cybernews.
2021 - 2022: Duomenų mokslininkas, Revel Systems.
2022 - 2025: Vyr. duomenų platformos inžinierius, Revel Systems.

Appendix

Implementation of the algorithm used in Chapter 2

```
#include <iostream>
#include <fstream>
#include <sstream>
#include <typeinfo>
#include <cstring>
#include <string>
#include <vector>
#include <array>
#include <deque>
#include <map>
#include <unordered_set>
#include <omp.h>
#include <acb_poly.h>
#include <profiler.h>
#include <algorithm>
#include <random>
#include <chrono>

using namespace std;

#define memory_limit 10000
#define delta_upper 0
#define delta_lower -1
#define delta_step 1
#define level_begin 100000
#define level_end 100001
#define level_step 50
long precision = 64;

typedef struct Node {
    char *poly_str;
    short coeff;
    struct Node *parent;
    long level;
} Node;

void printNode(Node *node) {
    if (node != NULL) {
        cout << node->coeff << ", ";
        printNode(node->parent);
    }
}
void read_polynomial(string line, fmpz_poly_t polynomial) {
    long size;
    unsigned int i;
    string poly_str, token;
```

```
47      size_t pos = 0;
48      string delimeter = ", ";
49      vector<int> coeffs;
50      if (line[0] == '[') {
51          size = line.size();
52          poly_str = line.substr(1, size - 2);
53          i = 0;
54          while ((pos = poly_str.find(delimeter)) !=
            ↪  string::npos) {
55              token = poly_str.substr(0, pos);
56              coeffs.push_back(stoi(token));
57              poly_str.erase(0, pos + delimeter.length());
58          }
59          coeffs.push_back(stoi(poly_str));
60          for (i = 0; i < coeffs.size(); i++) {
61              fmpz_poly_set_coeff_si(polynomial, coeffs.size() -
                ↪  1 - i, coeffs[i]);
62          }
63          coeffs.clear();
64      }
65  }
66
67  void find_roots(acb_ptr roots, const fmpz_poly_t poly) {
68      acb_poly_t cpoly;
69      acb_poly_init(cpoly);
70      acb_poly_set_fmpz_poly(cpoly, poly, precision);
71      acb_poly_find_roots(roots, cpoly, NULL, 0, precision);
72  }
73
74  void trim_conjugates(acb_ptr roots_trim, acb_ptr roots, long
    ↪  deg, int &number_of_roots, int multiplicities[]) {
75      int i, j, k;
76      acb_t conjugate;
77      arb_t absolute_val;
78      k = 0;
79      arb_init(absolute_val);
80      acb_init(conjugate);
81      acb_set(roots_trim, roots);
82      for (j = 0; j < deg; j++) {
83          i = 0;
84          while (i < k) {
85              acb_conj(conjugate, roots_trim + i);
86              if (acb_overlaps(roots_trim + i, roots + j)) {
87                  multiplicities[i] += 1;
88                  break;
89              }
90              else if (acb_overlaps(conjugate, roots + j)) {
91                  break;
92              }
93              i++;
94          }
95          if (i == k) {
96              acb_abs(absolute_val, roots + j, precision);
97              arb_sub_ui(absolute_val, absolute_val, 1,
                ↪  precision);
98              arb_abs(absolute_val, absolute_val);
99              if (arb_is_positive(absolute_val)) {
100                 acb_set(roots_trim + k, roots + j);
101                 k++;
102             }
103             else {
104             }
105         }
106     }
107     number_of_roots = k;
108 }
```

```
109
110 bool bound_true(fmpz_poly_t S, acb_ptr roots, int H, double
    ↪  delta, int number_of_roots, int multiplicities[]) {
111     int i, j;
112     int factorial;
113     acb_t result;
114     arb_t eval;
115     arb_t multiplier;
116     acb_poly_t cS, dS;
117     arb_t bound;
118     arb_init(bound);
119     arb_set_d(bound, H - delta);
120     arb_abs(bound, bound);
121     acb_init(result);
122     arb_init(eval);
123     arb_init(multiplier);
124     acb_poly_init(cS);
125     acb_poly_init(dS);
126     acb_poly_set_fmpz_poly(cS, S, precision);
127     for (i = 0; i < number_of_roots; i++) {
128         acb_poly_evaluate(result, cS, roots + i, precision);
129         acb_abs(multiplier, roots + i, precision);
130         arb_sub_ui(multiplier, multiplier, 1, precision);
131         acb_mul_arb(result, result, multiplier, precision);
132         acb_abs(multiplier, result, precision);
133         arb_sub(multiplier, multiplier, bound, precision);
134         if (arb_is_positive(multiplier)) {
135             arb_clear(bound);
136             arb_clear(multiplier);
137             acb_clear(result);
138             acb_poly_clear(cS);
139             return false;
140         }
141         factorial = 1;
142         acb_poly_set_fmpz_poly(dS, S, precision);
143         for (j = 0; j < multiplicities[i]; j++) {
144             factorial = factorial * (j + 1);
145             arb_mul_ui(bound, bound, factorial, precision);
146             acb_poly_derivative(dS, dS, precision);
147             acb_poly_evaluate(result, dS, roots + i,
                ↪  precision);
148             acb_abs(eval, result, precision);
149             acb_abs(multiplier, roots + i, precision);
150             arb_sub_ui(multiplier, multiplier, 1, precision);
151             arb_abs(multiplier, multiplier);
152             arb_pow_ui(multiplier, multiplier, j + 2,
                ↪  precision);
153             arb_mul(eval, eval, multiplier, precision);
154             arb_sub(eval, eval, bound, precision);
155
156             if (arb_is_positive(eval)) {
157                 arb_clear(bound);
158                 arb_clear(multiplier);
159                 acb_clear(result);
160                 acb_poly_clear(cS);
161                 acb_poly_clear(dS);
162                 return false;
163             }
164         }
165     }
166     arb_clear(bound);
167     arb_clear(multiplier);
168     acb_clear(result);
169     acb_poly_clear(cS);
170     acb_poly_clear(dS);
171     return true;
```

```
172 }
173
174 template <size_t n>
175 int poly_search(deque<Node *> vertex, unordered_set<string>
    ↪ visited_vertex, fmpz_poly_t poly, array<int, n> Digits, int
    ↪ H, double delta, acb_ptr roots, int number_of_roots, long
    ↪ &size, long &max_level, double &memory, int L, int
    ↪ multiplicities[]) {
176     int i, delta0;
177     char *poly_str;
178     char *S_str;
179     bool condition;
180     fmpz_poly_t R, S, X, b;
181     long level;
182     Node *poly_node;
183     unordered_set<string>::iterator it;
184     Node *new_node;
185     ofstream results;
186     meminfo_t meminfo;
187     double start, end;
188     fmpz_poly_init(R);
189     fmpz_poly_init(X);
190     fmpz_poly_init(S);
191     fmpz_poly_init(b);
192     fmpz_poly_set_coeff_ui(X, 1, 1);
193     start = omp_get_wtime();
194     max_level = 0;
195     while (!vertex.empty()) {
196         poly_node = vertex.back();
197         poly_str = poly_node->poly_str;
198         fmpz_poly_set_str(R, poly_str);
199         if ((poly_node->level) > max_level) {
200             max_level = (poly_node->level);
201         }
202         level = poly_node->level;
203         delete[] poly_str;
204         vertex.pop_back();
205         if (fmpz_poly_is_zero(R)) {
206 #pragma omp critical(time)
207             {
208                 while (!vertex.empty()) {
209                     poly_node = vertex.back();
210                     poly_str = poly_node->poly_str;
211                     delete[] poly_str;
212                     delete poly_node;
213                     vertex.pop_back();
214                 }
215                 fmpz_poly_clear(R);
216                 fmpz_poly_clear(X);
217                 fmpz_poly_clear(S);
218                 fmpz_poly_clear(b);
219                 size = visited_vertex.size();
220                 visited_vertex.clear();
221             }
222             get_memory_usage(meminfo);
223             memory = meminfo->rss / 1024.0;
224             return 0;
225         }
226         else {
227             for (i = 0; i < n; i++) {
228                 fmpz_poly_set_coeff_si(b, 0, Digits[i]);
229                 fmpz_poly_mul(S, R, X);
230                 fmpz_poly_add(S, S, b);
231                 fmpz_poly_rem(S, S, poly);
232                 S_str = fmpz_poly_get_str(S);
```

```
                    condition = bound_true(S, roots, H, delta,
                    ↪  number_of_roots, multiplicities);
                    if (visited_vertex.count(S_str) == 0 and
                    ↪  condition) {
                        new_node = new Node();
                        new_node->poly_str = S_str;
                        new_node->coeff = Digits[i];
                        new_node->parent = poly_node;
                        new_node->level = level + 1;
                        if (level < L) {
                            vertex.push_back(new_node);
                        }
                        if (visited_vertex.size() < memory_limit) {
                            visited_vertex.insert(string(S_str));
                        }
                    }
                    else {
                        delete[] S_str;
                    }
                }
            }
            end = omp_get_wtime();
            if ((end - start) > 10) {
                cout << delta << endl;
                cout << max_level << endl;
                cout << visited_vertex.size() << endl;
                cout << vertex.size() << endl
                     << endl;
                get_memory_usage(meminfo);
                if (visited_vertex.size() > memory_limit) {
                    cout << "Out of Mem" << endl;
                    while (!vertex.empty()) {
                        poly_node = vertex.back();
                        poly_str = poly_node->poly_str;
                        delete[] poly_str;
                        delete poly_node;
                        vertex.pop_back();
                    }
                    fmpz_poly_clear(R);
                    fmpz_poly_clear(X);
                    fmpz_poly_clear(S);
                    fmpz_poly_clear(b);
                    size = visited_vertex.size();
                    visited_vertex.clear();
                    return 3;
                }
                start = omp_get_wtime();
            }
        }
        if (vertex.empty() and delta < 0.001) {
            fmpz_poly_clear(R);
            fmpz_poly_clear(X);
            fmpz_poly_clear(S);
            fmpz_poly_clear(b);
            size = visited_vertex.size();
            visited_vertex.clear();
            get_memory_usage(meminfo);
            memory = meminfo->rss / 1024.0;
            return 1;
        }
        fmpz_poly_clear(R);
        fmpz_poly_clear(X);
        fmpz_poly_clear(S);
        fmpz_poly_clear(b);
        visited_vertex.clear();
        return 3;
```

```
297 }
298
299 void print_results(int t, fmpz_poly_t poly, double delta, long
    ↪ max_level, long size, double tstart, double start, double
    ↪ end, double memory) {
300     ofstream results("results.csv", ios_base::app);
301     ostringstream line;
302     line << fmpz_poly_get_str(poly) << ";" <<
        ↪ fmpz_poly_degree(poly) << ";";
303     if (t == 0)
304         line << "True;";
305     else if (t == 1)
306         line << "False;";
307     else
308         line << "None;";
309     line << delta << ";" << size << ";" << end - tstart << ";"
        ↪ << end - start << ";" << max_level << ";" << memory;
310     if (results.is_open()) {
311         results << line.str() << endl;
312     }
313 }
314
315 void initialization(fmpz_poly_t poly) {
316     bool divide;
317     int H, i, t, number_of_roots, coeff, j;
318     const int leading_coeff = 1;
319     const int n = 2;
320     long deg, size, max_level = 0;
321     char *poly_str;
322     double delta, start, end, tstart, tend, memory;
323     array<int, n> Digits = {-1, 1};
324     deque<Node *> vertex;
325     unordered_set<string> visited_vertex;
326     Node *poly_node;
327     fmpz_poly_t R;
328     acb_ptr roots, roots_trim;
329     deg = poly->length - 1;
330     roots = _acb_vec_init(deg);
331     cout << "deg " << deg << endl;
332     int multiplicities[deg];
333     memset(multiplicities, 0, deg * sizeof(int));
334     find_roots(roots, poly);
335     roots_trim = _acb_vec_init(deg);
336     trim_conjugates(roots_trim, roots, deg, number_of_roots,
        ↪ multiplicities);
337     H = Digits[0];
338     for (i = 1; i < n; i++) {
339         if (H < abs(Digits[i])) {
340             H = abs(Digits[i]);
341         }
342     }
343     for (i = 0; i <= fmpz_poly_degree(poly); i++) {
344         coeff = fmpz_poly_get_coeff_si(poly, i);
345         divide = false;
346         for (j = 0; j < n; j++) {
347             if (coeff == Digits[j])
348             {
349                 divide = true;
350             }
351         }
352         if (divide == false) {
353             break;
354         }
355     }
356     if (divide) {
357         print_results(0, poly, 1, 0, 0, 0, 0, 0, 0);
```

```
358         }
359         else {
360             tstart = omp_get_wtime();
361             fmpz_poly_init(R);
362             for (i = delta_upper; i > delta_lower; i -= delta_step)
                ↪  {
363                 int L = 0;
364                 for (int L = level_begin; L < level_end; L +=
                    ↪  level_step) {
365                     delta = float(i) / 100;
366                     fmpz_poly_set_coeff_si(R, 0, leading_coeff);
367                     poly_str = fmpz_poly_get_str(R);
368                     cout << fmpz_poly_get_str(poly) << endl;
369                     cout << delta << endl;
370                     cout << L << endl;
371                     visited_vertex.insert(string(poly_str));
372                     poly_node = new Node();
373                     poly_node->poly_str = poly_str;
374                     poly_node->coeff = leading_coeff;
375                     poly_node->parent = NULL;
376                     poly_node->level = 0;
377                     vertex.push_back(poly_node);
378                     t = 5;
379                     start = omp_get_wtime();
380                     t = poly_search(vertex, visited_vertex, poly,
                        ↪  Digits, H, delta, roots_trim,
                        ↪  number_of_roots, size, max_level, memory,
                        ↪  L, multiplicities);
381                     end = omp_get_wtime();
382                     cout << max_level << endl;
383                     if (t < 3) {
384                         print_results(t, poly, delta, max_level,
                            ↪  size, tstart, start, end, memory);
385                         fmpz_poly_clear(R);
386                         visited_vertex.clear();
387                         vertex.clear();
388                         flint_cleanup();
389                         L = 1000000000;
390                         i = -1;
391                         break;
392                     }
393                     visited_vertex.clear();
394                     vertex.clear();
395                     flint_cleanup();
396                 }
397             }
398             tend = omp_get_wtime();
399             _acb_vec_clear(roots, deg);
400             _acb_vec_clear(roots_trim, deg);
401             cout << "total time " << tend - tstart << endl;
402         }
403     }
404
405     int main(int argc, char **argv) {
406         ifstream root_file("unsolved");
407         string line;
408         int num_of_poly = 0;
409         double start;
410         meminfo_t meminfo;
411         vector<string> poly_file;
412         fmpz_poly_t polynomial;
413         if (root_file.is_open()) {
414             while (getline(root_file, line)) {
415                 poly_file.push_back(line);
416                 num_of_poly++;
417             }
```

```
418         }
419         omp_set_num_threads(omp_get_num_procs());
420         start = omp_get_wtime();
421         int id;
422         int i;
423         if (root_file.is_open()) {
424     #pragma omp parallel for private(polynomial, id, i)
        ↪  schedule(dynamic, 1)
425             for (i = 0; i < num_of_poly; i++) {
426                 fmpz_poly_init(polynomial);
427                 read_polynomial(poly_file[i], polynomial);
428                 id = omp_get_thread_num();
429     #pragma omp critical
430                 {
431                     cout << "New polynomial" << endl;
432                     fmpz_poly_print(polynomial);
433                     cout << i << " " << id << endl;
434                 }
435                 initialization(polynomial);
436                 fmpz_poly_clear(polynomial);
437                 flint_cleanup();
438             }
439         }
440         get_memory_usage(meminfo);
441         cout << "Memory-----: " << (meminfo->rss / 1024.0) << " "
            ↪  << meminfo->hwm / 1024.0 << endl;
442         cout << "Elapsed time " << (omp_get_wtime() - start) <<
            ↪  endl;
443         return 0;
444     }
```

Acknowledgement

I want to express my deepest gratitude to my supervisor, Professor Paulius Drungilas, whose clarity of thought and ability to convey the beauty of abstract mathematics made him one of the most inspiring professors during my studies. His passion for teaching sparked my interest in algebra and number theory over a decade ago and provided continuous guidance throughout my academic journey to this day. I am also grateful to Professors Ramūnas Garunkštis, Artūras Dubickas, Antanas Laurinčikas, and Dr. Mindaugas Skujus, who played significant roles in fostering my fascination with mathematics and encouraging me to pursue a PhD.

I extend my heartfelt thanks to my co-authors, Dr. Jonas Šiurys, my coursemate Lukas Klebonas, and especially Assoc. Prof. Dr. Jonas Jankauskas, whose contributions were essential from suggesting research problems and proposing possible solutions to collaborating on our publications.

My journey in mathematics began with my high school teacher, Jurga Deveikytė, whose dedication to teaching and ability to engage her students revealed the beauty of mathematics to me. Without her guidance and encouragement, I might never have discovered my passion for the subject or reached this point in my academic journey. I am deeply grateful for her patience, encouragement, and guidance.

Finally, I am immensely thankful to my wife Neringa and daughter Ūla, whose unwavering support, patience, and love have been a constant source of strength and joy throughout this endeavor. Their presence has brightened even the most challenging days and made this journey worthwhile.

Publications by the Author

1st publication

On Certain Multiples of Littlewood and Newman Polynomials

P. Drungilas, J. Jankauskas, **G. Junevičius**, L. Klebonas, J. Šiurys

Bull. Korean Math. Soc. ***55(5)****(2018)*

Link to the publication:
https://doi.org/10.4134/BKMS.b170854

2nd publication

On Complex Pisot Numbers That Are Roots of Borwein Trinomials

P. Drungilas, J. Jankauskas, **G. Junevičius**

Mathematics, ***12 (8)****, (2024), 1129*

Link to the publication:
https://doi.org/10.3390/math12081129

NOTES

Vilniaus universiteto leidykla
Saulėtekio al. 9, III rūmai, LT-10222 Vilnius
El. p. info@leidykla.vu.lt, www.leidykla.vu.lt
bookshop.vu.lt, journald.vu.lt
Tiražas 25 egz.

NUO / SINCE 1579

Fragmentas iš Vilniaus universiteto auklėtinio Alberto Diblinskio (1601–1665) vieno geriausių XVII a. astronomijos veikalų *Centuria astronomica* (Vilnius, 1639), kuriame pateikta astronomijos pasiekimų apžvalga, remiantis stebėjimais teleskopu, atliktais kartu su kitu VU mokslininku, matematiku ir astronomu Osvaldu Krygeriu (apie 1598–1655).

VU biblioteka, BAV 47.10.21

Fragment from *Centuria astronomica* (Vilnius, 1639), one of the most well-known works on astronomy from the 17th c., written by Vilnius University graduate Albertas Diblinskis (1601–1665). It presents an overview of achievements in the field of astronomy, based on observations using a telescope together with another VU scientist, mathematician, and astronomer Osvaldas Krygeris (c. 1598–1655).

VU Library, BAV 47.10.21

bookshop.vu.lt journals.vu.lt

https://doi.org/10.15388/vu.thesis.728