

Article

Automata and Arithmetics in Canonical Number Systems

Tamás Herendi [†]  and Viktória Padányi ^{*,†}

Department of Computer Science, Faculty of Informatics, University of Debrecen, Kassai str. 26, 4028 Debrecen, Hungary; herendi.tamas@inf.unideb.hu

* Correspondence: padanyi.viktoria@inf.unideb.hu

[†] These authors contributed equally to this work.

Abstract: In this paper, we discuss canonical number systems (CNSs), which are generalizations of positional number systems to polynomials over the integers. We defined the information quantity of a polynomial $A \in \mathbb{Z}[x]$ relative to the base of the CNS and proved that it has a strong relation with the length of the representation in the number system. Based on this result, we showed that for every CNS polynomial P , there exists a finite transducer automaton executing the addition operation of polynomials in canonical representation of base P . Finally, we observed the size—i.e., the number of states—of such automata.

Keywords: canonical number system; finite transducer automata; algorithms for arithmetics

1. Introduction

In their first appearance, canonical number systems (CNSs) were natural generalizations of the positional numeral systems of rational integers to algebraic integers. D. E. Knuth, in his famous book [1] (Ch. 4), studied the history of the radix representation of integers. He described various canonical number systems, and he proved that the complex number $-1 + i$ is a possible base of the number system representing Gaussian integers. His result was further generalized by I. Kátai and J. Szabó. In [2], they proved the existence of other bases, but still in the set of Gaussian integers. Later, I. Kátai and B. Kovács in [3], B. Kovács in [4], and B. Kovács and A. Pethő in [5] and [6] extended the concept of canonical number systems for the ring of algebraic integers and they proved their existence in some particular cases. In [7], A. Pethő first used the notion, and S. Akiyama and A. Pethő in [8] continued the development of results of CNSs over polynomials. A. Pethő and P. Varga in [9] dealt with canonical number systems over Euclidean domains.

In [4], a simple condition is given for the construction of CNSs, but in general, they are not easy to find. A. Kovács [10] presented a complete description of binary canonical number systems of degrees not greater than 8. Later, P. Burcsi and A. Kovács [11] extended the results for CNSs of degrees 9, 10, and 11.

The arithmetic in a canonical number system is similar to that of rational integers within the classical digit representation. However, calculating the digits requires a more complex reduction operation.

P. J. Grabner, P. Kirschenhofer, and H. Prodinger in [12] introduced the concept of counting automata (increasing by 1) for Gaussian integers, which was generalized to quadratic number fields by J. M. Thuswardner [13]. J. Allouche, K. Scheicher, and R. F. Tichy in [14] proved the existence of addition and multiplication by a constant in algebraic number fields. K. Scheicher and J. M. Thuswaldner in [15] introduced a fractal approach for the detailed analysis of counting automata.



Academic Editor: Ming-Feng Ge

Received: 17 December 2024

Revised: 13 February 2025

Accepted: 18 February 2025

Published: 20 February 2025

Citation: Herendi, T.; Padanyi, V. Automata and Arithmetics in Canonical Number Systems.

Algorithms **2025**, *18*, 122.

<https://doi.org/10.3390/a18030122>

Copyright: © 2025 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license

(<https://creativecommons.org/licenses/by/4.0/>).

Transducers were extensively studied by S. Eilenberg in Automata, Languages and Machines [16], and further developed by W. Kuich and A. Salomaa in Semirings, Automata, Languages [17].

In the present paper, we prove that for every CNS polynomial, an automaton can be constructed to perform digit-wise addition (Theorem 5). This relies on several assertions, which are detailed in Section 2. We implement a program for the calculation of addition automata in binary CNSs and summarize our experiments in Section 4.

The rest of the paper is organized as follows.

In Section 2, we introduce the concepts and key results related to canonical number systems. We also define a useful measure for the information quantity of a polynomial and outline its fundamental properties. One of the main results of the section is Theorem 3, which establishes a general bound on geometric sums of complex numbers α with modulus greater than 1, under the condition that α is not a positive real number. The proof of this statement requires some further lemmas concerning the behavior of geometric sums, which we address in the subsequent paragraphs. Using these lemmas, we present an algorithm, which is designed to calculate a reasonably small constant appearing in Theorem 3. In the last part of the section, we prove Theorem 4, which discusses the relationship between the length of a polynomial A in canonical representation and the information quantity of A . The constants referenced in this theorem are derived using Theorem 3, and thus can be calculated by an algorithm explained after the theorem.

In Section 3, we define the concept of finite transducer automata. In Theorem 5, we show that for every canonical number system, there exists a transducer automaton executing the addition operation for polynomials in canonical representation. The proof is constructive, and the automaton produced is minimal (Theorem 6). Using arguments from the previous results, in Theorem 7, we show that there is no finite transducer automaton capable of performing multiplication in canonical number systems.

In the final section, we present our experimental results regarding the construction of minimal addition automata in particular canonical number systems.

2. Definitions and Results Related to Canonical Number Systems

Definition 1. Let $P \in \mathbb{Z}[x]$ be a monic polynomial, $R = \mathbb{Z}[x]/P\mathbb{Z}[x]$ be the corresponding quotient ring, and let $\varphi : \mathbb{Z}[x] \rightarrow R$ be the homomorphism $\varphi(A) = A \bmod P$. Furthermore, let $m > 1$, $\mathcal{N} = \{n_1, \dots, n_m\} \subseteq \mathbb{Z}$, and let $\mathcal{N}[x] \subseteq \mathbb{Z}[x]$ be the set of polynomials with all coefficients from $\mathcal{N}$. The pair $(P, \mathcal{N})$ is called a number system, if for any $A \in \mathbb{Z}[x]$ there exists a unique $B \in \mathcal{N}[x]$, such that $\varphi(A) = \varphi(B)$.

The number system is called canonical, and $P(x)$ is called a CNS polynomial if $\mathcal{N} = \{0, 1, \dots, m-1\}$.

The length of the representation of A by P is $L(A) = L(A, P) = \deg(B) + 1$.

Example 1. Let us consider the number system corresponding to the base-3 system.

The base-3 numeration system is, in fact, isomorphic to the polynomial system based on $P(x) = x - 3$ since the unique root of $x - 3$ is 3. In other words, the isomorphism arises because when we substitute $x = 3$ into any polynomial, we recover the standard evaluation in base-3.

Let us illustrate this with the constant 16 as an example:

(a) In the classical base-3 system, the representation of 16 is obtained by dividing 16 by 3 repeatedly:

1. $16 \div 3 = 5$ with remainder $16 - 5 \cdot 3 = 1 \Rightarrow$ units digit is 1.
2. $5 \div 3 = 1$ with remainder $5 - 1 \cdot 3 = 2 \Rightarrow$ next digit is 2.
3. $1 \div 3 = 0$ with remainder $1 - 0 \cdot 3 = 1 \Rightarrow$ highest digit is 1.

So we obtain the digits 1, 2, 1, i.e., $16 = 121_3$.

(b) In the polynomial system with base $x - 3$, we essentially perform the same 'division with remainder' process, but in the context of polynomials. Here, the constant 16 must be represented by a polynomial $B(x) = a_2x^2 + a_1x + a_0$ (with $a_i \in \{0, 1, 2\}$) such that $B(3) = 16$. Analogously to the integer numeration system, we repeatedly divide 16 by $x - 3$.

1. To find the last digit, we execute the 'integer' division $16 \div (x - 3)$. Actually, we solve the equation $16 = q \cdot (x - 3) + s \cdot x + r$, where $r \in \{0, 1, 2\}$. The only solution is $q = -5$, $s = 5$ and $r = 1$. Hence, the last digit is 1, and we should represent $5x$ in the system.
2. For the second digit, we solve $5 = q \cdot (x - 3) + s \cdot x + r$, with $r \in \{0, 1, 2\}$. The only solution is $q = -1$, $s = 1$, and $r = 2$.
3. Finally, we should solve $1 = q \cdot (x - 3) + s \cdot x + r$, with $r \in \{0, 1, 2\}$. The only solution is $q = 0$, $s = 0$, and $r = 1$. Since $s = 0$, thus there is no more carry in the computation, so the algorithm terminates.

Thus, the polynomial representation of 16 is $x^2 + 2x + 1$, exactly as in the classical base-3 system.

Remark 1. Note that the system in Example 1 is not a number system in the general sense of Definition 2 since negative integers cannot be represented.

Example 2. Now, consider the base system (-3) number, which corresponds to the polynomial $P(x) = x + 3$. This system has the same digits $\mathcal{N} = \{0, 1, 2\}$, just like the base-3 system. We may observe that in the system with base (-3) , we can represent all integers, both negative and non-negative.

Express 16 once more in this numeration system:

(a) Again, we execute repeated division by -3 :

1. $16 \div -3 = -5$ with remainder $16 - (-5) \cdot (-3) = 1 \Rightarrow$ units digit is 1.
2. $-5 \div -3 = 2$ with remainder $5 - 2 \cdot (-3) = 1 \Rightarrow$ next digit is 1.
3. $2 \div -3 = 0$ with remainder $2 - 0 \cdot 3 = 2 \Rightarrow$ highest digit is 2.

So we obtain the digits 2, 1, 1, i.e., $16 = 211_{-3}$.

(b) In the polynomial system with base $x + 3$, we execute similar steps to those in the previous example. Here, the constant 16 must be represented by a polynomial $B(x) = a_2x^2 + a_1x + a_0$ (with $a_i \in \{0, 1, 2\}$) such that $B(-3) = 16$.

1. To find the last digit, we solve the equation $16 = q \cdot (x + 3) + s \cdot x + r$, where $r \in \{0, 1, 2\}$. The only solution is $q = 5$, $s = -5$ and $r = 1$. Hence, the last digit is 1, and we should represent $-5x$ in the system.
2. For the second digit, we solve $-5 = q \cdot (x + 3) + s \cdot x + r$, with $r \in \{0, 1, 2\}$. The only solution is $q = -2$, $s = 2$, and $r = 1$.
3. Finally, we should solve $2 = q \cdot (x + 3) + s \cdot x + r$, with $r \in \{0, 1, 2\}$. The only solution is $q = 0$, $s = 0$, and $r = 2$. Since $s = 0$, thus there is no more carry in the computation, so the algorithm terminates.

Thus, the polynomial representation of 16 is $2x^2 + x + 1$.

Remark 2. The system in Example 2 is indeed a valid number system since it can represent both positive and negative integers. For instance, $-1 = 12_{-3}$.

Remark 3. If $(P, \mathcal{N})$ is a number system, then the reduced homomorphism $\varphi : \mathcal{N}[x] \rightarrow R$ is an isomorphism.

B. Kovács in [4] proved that if the coefficients of P are increasing, then there exists a corresponding canonical number system. We reformulate it in the following theorem.

Theorem 1. Let $P \in \mathbb{Z}[x]$ be a monic polynomial with $\deg(P) = d$, and $P(x) = p_d x^d + \dots + p_0$ be such that $1 = p_d \leq p_{d-1} \leq \dots \leq p_0$ with $2 \leq p_0$. If P is not divisible by a cyclotomic polynomial, then P is a CNS polynomial.

Example 3. Let $P(x) = x^2 + x + 3$ and let α be one of its roots. By Theorem 1, $(P, \{0, 1, 2\})$ is a canonical number system. The corresponding numeration system of $\mathbb{Z}[\alpha]$ has the base α , with digits $\{0, 1, 2\}$. This polynomial defines a number system over the algebraic integers, extending the idea of canonical number systems to the algebraic integers $\mathbb{Z}[\alpha]$.

Now, we consider the only case when calculating the digits in the polynomial number system. Again, we want to express 16 in this system.

1. To find the last digit, we solve the equation $16 = q \cdot (x^2 + x + 3) + s \cdot x + r$, where $r \in \{0, 1, 2\}$. The only solution is $q = 5$, $s = -5x - 5$, and $r = 1$. Hence, the last digit is 1, and we should represent $-5x^2 - 5x$ in the system.
2. For the second digit, we solve $-5x - 5 = q \cdot (x^2 + x + 3) + s \cdot x + r$, with $r \in \{0, 1, 2\}$. The only solution is $q = -2$, $s = 2x - 3$, and $r = 1$.
3. Next, we should solve $2x - 3 = q \cdot (x^2 + x + 3) + s \cdot x + r$, with $r \in \{0, 1, 2\}$. The only solution is $q = -1$, $s = x + 3$, and $r = 0$. This yields that the next digit is 0.
4. Now, we should solve $x + 3 = q \cdot (x^2 + x + 3) + s \cdot x + r$, with $r \in \{0, 1, 2\}$. The only solution is $q = 1$, $s = -x$, and $r = 0$. Hence, the next digit is again 0.
5. Then, we solve $-x = q \cdot (x^2 + x + 3) + s \cdot x + r$, with $r \in \{0, 1, 2\}$. The only solution is $q = 0$, $s = -1$, and $r = 0$. The next digit is again 0.
6. In the next step we solve $-1 = q \cdot (x^2 + x + 3) + s \cdot x + r$, with $r \in \{0, 1, 2\}$. The only solution is $q = -1$, $s = x + 1$, and $r = 2$. The next digit is 2.
7. Now, we solve $x + 1 = q \cdot (x^2 + x + 3) + s \cdot x + r$, with $r \in \{0, 1, 2\}$. The only solution is $q = 0$, $s = 1$, and $r = 1$. The next digit is 1.
8. Finally, we should solve $1 = q \cdot (x^2 + x + 3) + s \cdot x + r$, with $r \in \{0, 1, 2\}$. The only solution is $q = 0$, $s = 0$, and $r = 1$. Hence, the first digit is again 1, and the algorithm terminates.

The iterations of the algorithm are displayed in Table 1. Column N refers to the remaining value we should represent in the system, while q , s , and r are as in the description.

Table 1. steps for decomposing the number 16 in the number system $(x^2 + x + 3, \{0, 1, 2\})$.

Iter.	N	q	s	r
1	16	5	$-5x - 5$	1
2	$-5x - 5$	-2	$2x - 3$	1
3	$2x - 3$	-1	$x + 3$	0
4	$x + 3$	1	$-x$	0
5	$-x$	0	-1	0
6	-1	-1	$x + 1$	2
7	$x + 1$	0	1	1
8	1	0	0	1

We obtain that the representation of 16 in the number system $(x^2 + x + 3, \{0, 1, 2\})$ is $11\ 200\ 011_{(x^2+x+3)}$. Similarly, as before, if we set $B(x) = x^7 + x^6 + 2x^5 + x + 1$, then $B(\alpha) = 16$.

The above example illustrates how numbers in this algebraic number system can be expressed as polynomials, extending the classical notion of number systems into the realm of algebraic integers.

A. Pethő in [7] and later Akiyama et al. [18] have stated a necessary condition for CNS polynomials.

Theorem 2. If $P(x)$ is a CNS polynomial, then all roots of $P(x)$ lie outside the closed unit circle and all real roots of $P(x)$ are less than -1 .

Now, we define the information quantity of a polynomial. Later, at the end of this section, we will show the relation between the information quantity and the length of the canonical representation of a polynomial in Theorem 4. In Section 3, we will use this definition in Theorem 5 for the proof of the existence of addition automata in canonical number systems.

Definition 2. Let $P(x)$ be a CNS polynomial of degree d , $\alpha_1, \dots, \alpha_d$ be the (not necessarily different) roots of P , and let $A(x) \in \mathbb{Z}[x]$. We define the relative information quantity of A as

$$\mathbb{I}(A) = \mathbb{I}_P(A) = \max_{\substack{1 \leq i \leq d \\ A(\alpha_i) \neq 0}} \frac{\log |A(\alpha_i)|}{\log |\alpha_i|}.$$

In the special case of A is divisible by P , we set $\mathbb{I}(A) = 0$.

Example 4. Let $P(x) = x^4 + 2$. In the paper of A. Kovács [10], it is proven that P is a CNS polynomial. The roots of P are

$$\frac{2^{\frac{3}{4}}}{2} + I \frac{2^{\frac{3}{4}}}{2}, \quad \frac{2^{\frac{3}{4}}}{2} - I \frac{2^{\frac{3}{4}}}{2}, \quad -\frac{2^{\frac{3}{4}}}{2} - I \frac{2^{\frac{3}{4}}}{2}, \quad -\frac{2^{\frac{3}{4}}}{2} + I \frac{2^{\frac{3}{4}}}{2},$$

where I is the imaginary unit. The modulus of the roots are identical and equal to $\left| \frac{2^{\frac{3}{4}}}{2} + I \frac{2^{\frac{3}{4}}}{2} \right| = 2^{\frac{1}{4}}$.

Based on the properties of the logarithm, any base of the logarithm provides the same value for the relative information quantity; thus, for the sake of simplicity, let $\log$ be the base-2 logarithm. Then, $\log \left| \frac{2^{\frac{3}{4}}}{2} + I \frac{2^{\frac{3}{4}}}{2} \right| = \frac{1}{4}$ (and the same is true for all the roots).

- (a) Let $A(x) = x^3 + x + 1$. Substituting the four roots to A and calculating the base-2 logarithm of the absolute value of $A(\alpha)$, according to the order of the roots, we obtain the approximate values

$$1.0923, 1.0923, 1.2851, 1.2851.$$

Then, we obtain

$$\mathbb{I}(A) = \frac{1.2851}{1/4} \approx 5.1406.$$

- (b) Let $A(x) = x^4 + x + 1$. As before, execute the same operations. We obtain the logarithms of the absolute values of the substituted roots as

$$-0.2246, -0.2246, 1.0171, 1.0171,$$

whence

$$\mathbb{I}(A) = \frac{1.0171}{1/4} \approx 4.0684.$$

- (c) Let $A(x) = x^5 + x + 1$. Then, one can see that for $\mathbb{I}(A)$, we obtain get exactly the same value as in case (b).

The equality of case b) and c) can be seen if we notice that if α is one of the roots of P , then $\alpha^4 = -2$, whence in case b), $A(\alpha) = \alpha - 1$, while in case c) $A(\alpha) = -2 \cdot \alpha + \alpha - 1 = -\alpha + 1$.

Lemma 1. Let $P(x)$ be a CNS polynomial and $A(x), B(x) \in \mathbb{Z}[x]$. Then,

- (i) $0 \leq \mathbb{I}(A)$;
- (ii) If $\varphi(A) = \varphi(B)$, then $\mathbb{I}(A) = \mathbb{I}(B)$;
- (iii) $\mathbb{I}(A + B) \leq \max\{\mathbb{I}(A), \mathbb{I}(B)\} + \mathbb{I}(2)$;
- (iv) $\mathbb{I}(A \cdot B) \leq \mathbb{I}(A) + \mathbb{I}(B)$;
- (v) $\mathbb{I}(x \cdot A) = \mathbb{I}(A) + 1$;
- (vi) $\mathbb{I}(A^n) = n\mathbb{I}(A)$.

Proof.

(i) Let P' be an irreducible divisor of P of degree d' , and for the sake of simplicity, assume that $\alpha_1, \dots, \alpha_{d'}$ are the roots of P' . Assume that A is not divisible by P' .

Since P is a CNS polynomial, by Theorem 2, $|\alpha| > 1$ for any root of P and hence for any root of P' as well.

P' is irreducible and does not divide A , thus the roots of P' are not roots of A , whence $A(\alpha_i) \neq 0$ for all $i = 1, \dots, d'$.

By definition $P \in \mathbb{Z}[x]$, consequently, $P' \in \mathbb{Z}[x]$, whence $\alpha_1, \dots, \alpha_{d'}$ are algebraic integers. Since $A \in \mathbb{Z}[x]$, the values $A(\alpha_1), \dots, A(\alpha_{d'})$ are algebraic integers as well.

The roots $\alpha_1, \dots, \alpha_{d'}$ form a complete set of algebraic conjugates over $\mathbb{Q}$, which means that the set $A(\alpha_1), \dots, A(\alpha_{d'})$ is also a complete set of algebraic conjugates over $\mathbb{Q}$ with each value appearing in the same number. This implies that

$$\prod_{1 \leq i \leq d'} A(\alpha_i) \in \mathbb{Q}. \quad (1)$$

The product of algebraic integers is an algebraic integer, hence, together with Equation (1),

$$0 \neq \prod_{1 \leq i \leq d'} A(\alpha_i)$$

is a rational integer. If $|A(\alpha_i)| < 1$ for all $1 \leq i \leq d'$, then

$$1 > \prod_{1 \leq i \leq d'} |A(\alpha_i)|,$$

which is a contradiction, whence at least one of the roots α of P' is such that $|A(\alpha)| \geq 1$.

For this α , we have

$$0 \leq \frac{\log|A(\alpha)|}{\log|\alpha|},$$

whence by definition $0 \leq \mathbb{I}(A)$.

(ii) If $\varphi(A) = \varphi(B)$, then $A(x) \equiv B(x) \pmod{P(x)}$, i.e., $A(x) = Q(x)P(x) + B(x)$ with some $Q \in \mathbb{Z}[x]$. This yields that $A(\alpha) = B(\alpha)$ for any root of P , which implies $\mathbb{I}(A) = \mathbb{I}(B)$.

(iii) Let α be a root of P . In the general case, when we do not assume that $\varphi(A) = \varphi(B)$, we cannot state $A(\alpha) = B(\alpha)$. For the sake of simplicity, assume that $|A(\alpha)| \geq |B(\alpha)|$. Then, $\log(|A(\alpha) + B(\alpha)|) \leq \log(|A(\alpha)| + |B(\alpha)|) \leq \log(2|A(\alpha)|) = \log(2) + \log(|A(\alpha)|)$, which implies the statement.

(iv)–(vi) These statements can be proven by similar arguments using the additive property of the logarithm.

□

Theorem 3. Let $\alpha \in \mathbb{C}$ with $1 < |\alpha|$, and assume that α is not a positive real number. Then, there exists a constant $c < 1$ depending only on α such that for every $0 < N \in \mathbb{Z}$, and for any sequence $a_0, a_1, \dots$ of integers satisfying $0 \leq a_i \leq N$ for all $i = 0, 1, \dots$, we have

$$\left| \sum_{i=0}^{k-1} a_i \alpha^i \right| \leq cN \frac{|\alpha|^k}{|\alpha| - 1}, \quad (2)$$

for any $1 < k \in \mathbb{Z}$.

Remark 4. In Theorem 3, we assume that $2 \leq k$, thus a natural lower bound on c can be obtained from inequality (2) if we set $k = 2$. Then, we have

$$|\alpha + 1| \leq c \frac{|\alpha|^2}{|\alpha| - 1},$$

which implies

$$|\alpha + 1| \frac{|\alpha| - 1}{|\alpha|^2} \leq c.$$

To present this lower bound in a more expressive form, we multiply the left-hand side by $\frac{|\alpha| + 1}{|\alpha| + 1}$. Then, we obtain

$$\begin{aligned} \frac{|\alpha + 1|}{|\alpha| + 1} \cdot \frac{(|\alpha| + 1)(|\alpha| - 1)}{|\alpha|^2} &= \\ \frac{|\alpha + 1|}{|\alpha| + 1} \cdot \frac{|\alpha|^2 - 1}{|\alpha|^2} &= \\ \frac{|\alpha + 1|}{|\alpha| + 1} \cdot \left(1 - \frac{1}{|\alpha|^2} \right) &\leq c. \end{aligned} \quad (3)$$

Since α is not a positive real number, thus $|\alpha + 1| < |\alpha| + 1$, whence the left-hand side of inequality (3) is a product of two positive numbers both less than 1. This means that there is an infimum of the possible values of c .

The proof of Theorem 3 is presented later in this section, and based on the proof, we will construct an algorithm to find a proper c close to the above-mentioned infimum.

Remark 5. We consider three cases illustrating inequality (2).

(i) (This case is excluded from Theorem 3)

If α is a positive real number, then

$$\frac{1}{\alpha^k} \sum_{i=0}^{k-1} \alpha^i = \frac{1}{\alpha^k} \frac{\alpha^k - 1}{\alpha - 1} = \frac{1}{\alpha - 1} - \frac{1}{\alpha^k(\alpha - 1)},$$

where the last term of the right side approximates 0 as k increases and hence,

$$\frac{1}{\alpha - 1} - \frac{1}{\alpha^k(\alpha - 1)} > c \frac{1}{\alpha - 1},$$

for any $c < 1$, if k is big enough. If $a_0 = a_1 = \dots = a_{k-1} = N$, then inequality (2) cannot hold for suitably large k 's.

(ii) In the opposite extremal case, when α is a negative real number, the left-hand side of inequality (2) is maximal if we sum up the members with the same sign only.

To estimate this maximum, set $b_{k-1} = b_{k-3} = \dots = N$, $b_{k-2} = b_{k-4} = \dots = 0$ and let $j = (k + 1) \bmod 2$ (i.e., $j = 0$, if k is odd and $j = 1$, if k is even). Furthermore, denote by $\lfloor x \rfloor$ the integer part of x and set $c = \frac{|\alpha|}{|\alpha| + 1} < 1$.

Because of the alternating sign of the powers of α , we have

$$\begin{aligned} \left| \sum_{i=0}^{k-1} a_i \alpha^i \right| &\leq \left| \sum_{i=0}^{k-1} b_i \alpha^i \right| \leq |\alpha|^j \left| \sum_{i=0}^{\lfloor \frac{k-1}{2} \rfloor} N \alpha^{2i} \right| = |\alpha|^j N \frac{|\alpha|^{2 \cdot (\lfloor \frac{k-1}{2} \rfloor + 1)} - 1}{|\alpha|^2 - 1} \leq \\ &\leq |\alpha|^j N \frac{|\alpha|^{2 \cdot (\lfloor \frac{k-1}{2} \rfloor + 1)}}{|\alpha|^2 - 1} = N \frac{|\alpha|^{k+1}}{(|\alpha| - 1)(|\alpha| + 1)} = cN \frac{|\alpha|^k}{|\alpha| - 1}. \end{aligned}$$

- (iii) For the third case, when α is a nonreal complex number, we need some geometric considerations. In Figure 1, we can see an example of the first four powers of a particular complex number. Since $|\alpha| > 1$, the modulus of the powers of α are increasing, and the arguments of the powers are integer multiples of the argument of α (denoted by $\arg(\alpha)$).

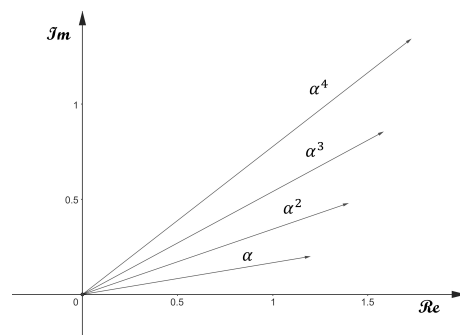


Figure 1. Powers of a complex number .

If $\frac{\arg(\alpha)}{\pi} \in \mathbb{Q}$, then the sequence $\arg(\alpha^0), \arg(\alpha^1), \arg(\alpha^2), \arg(\alpha^3), \dots$ is periodic, otherwise, it is uniformly distributed in the interval $[0, 2\pi[$ and if $\arg(\alpha^n) = \arg(\alpha^k)$ then $n = k$. It also implies that in the nonperiodic case, $\arg(\alpha^n) = 0$ only if $n = 0$; in other words, $\alpha^n \in \mathbb{R}$ if and only if $n = 0$.

For the proof of Theorem 3, we study first the maximum of the left-hand side of inequality (2). One immediate thing we find is that if the left-hand side is maximal, then the coefficient of the largest power in the sum cannot be 0, and if a coefficient is nonzero, then it should be N (i.e., maximal itself). The latter means that to prove the general statement, it is enough to deal with geometric sums with 0, 1 coefficients and multiply this by N at the end.

We may geometrically depict the theorem as in Figure 2. Then, the statement can be interpreted as $\frac{r}{R} < c$ with some constant $c < 1$, depending only on α .

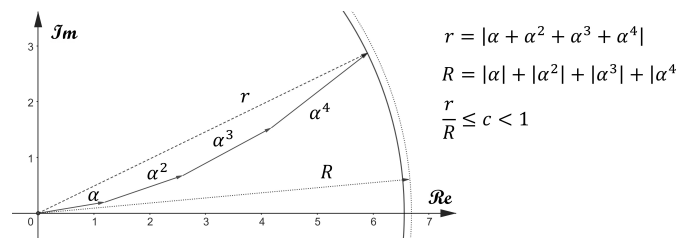


Figure 2. Sum of powers.

We will also use the observation that if we denote by M_n and M_k the maximum of $\left| \sum_{i=0}^{n-1} a_i \alpha^i \right|$

and $\left| \sum_{i=0}^{k-1} a_i \alpha^i \right|$, respectively, then $\frac{M_k}{M_n} \approx |\alpha|^{k-n}$.

Finally, the following property plays the most important role in proving the existence of the above-mentioned constant $c < 1$. Assume we have an arbitrary finite set of nonzero complex

numbers $A = \{\alpha_1, \dots, \alpha_n\}$. Let $B \subseteq A$, such that $\left| \sum_{\alpha \in B} \alpha \right|$ is maximal, and let $\mu = \sum_{\alpha \in B} \alpha$. Let e be the line with normal vector μ , i.e., $e = \left\{ \beta \mid |\arg(\beta) - \arg(\mu)| = \frac{\pi}{2} \right\}$. Then, B consist of those elements of A that lie on the same side of e as μ , i.e., $\alpha \in B$ if and only if $|\arg(\alpha) - \arg(\mu)| < \frac{\pi}{2}$. (see Figure 3. In the figure, μ is the sum of the complex numbers represented by solid lines.)

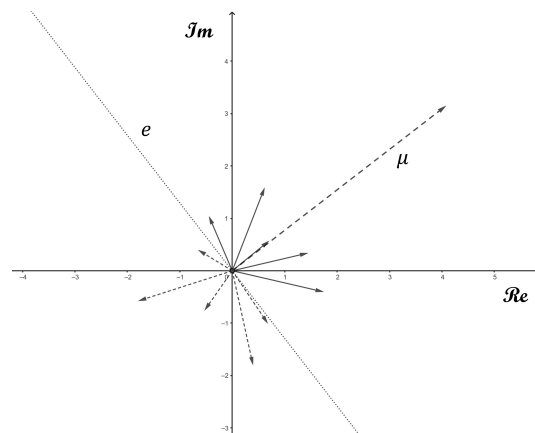


Figure 3. Maximum of subsum. (1) μ is the sum of numbers (vectors) with solid lines. (2) e is perpendicular to μ .

Before we turn to the proof of Theorem 3, we prove some lemmas, according to our observations of case (iii) of Remark 5.

First, we show that if we want to have a maximal value of the left-hand side of inequality (2), then the most significant power of α cannot vanish.

Lemma 2. Let $\alpha \in \mathbb{C}$, with $1 < |\alpha|$, $1 < N \in \mathbb{Z}$, let $0 \leq a_0, a_1, \dots, a_{n-1} \leq N$ be fixed integers, and

$$M = \max \left\{ \left| \sum_{i=0}^{n-1} b_i \cdot \alpha^i \right| : 0 \leq b_0, b_1, \dots, b_{n-1} \leq N, \text{ integers} \right\}.$$

If

$$\left| \sum_{i=0}^{n-1} a_i \cdot \alpha^i \right| = M,$$

then $a_{n-1} \neq 0$.

Proof. Contrary, if $a_{n-1} = 0$, then

$$M = \left| \sum_{i=0}^{n-2} a_i \cdot \alpha^i \right| < |\alpha| \cdot \left| \sum_{i=0}^{n-2} a_i \cdot \alpha^i \right| = \left| \sum_{i=1}^{n-1} a_{i-1} \cdot \alpha^i \right| \leq M,$$

which is a contradiction. $\square$

In the next lemma and the following corollary, we prove that if M_r and M_n denote the possible maximum of the modulus of different length geometric sums, then $\frac{M_r}{M_n}$ is nearly proportional to $\frac{|\alpha^r|}{|\alpha^n|}$. In Lemma 2, we show this property when $r < n$, and in Corollary 1, we extend it for values greater than n .

Lemma 3. Let $\alpha \in \mathbb{C}$, with $1 < |\alpha|$, $1 < N \in \mathbb{Z}$, $0 < r < n$ be integers, and

$$M_n = \max \left\{ \left| \sum_{i=0}^{n-1} b_i \cdot \alpha^i \right| : 0 \leq b_0, b_1, \dots, b_{n-1} \leq N, \text{integers} \right\}$$

$$M_r = \max \left\{ \left| \sum_{i=0}^{r-1} b_i \cdot \alpha^i \right| : 0 \leq b_0, b_1, \dots, b_{r-1} \leq N, \text{integers} \right\}$$

Then, $|\alpha|^{n-r} \cdot M_r \leq M_n$.

Proof. Let $0 \leq a_0, a_1, \dots, a_{r-1} \leq N$ be integers, with

$$\left| \sum_{i=0}^{r-1} a_i \cdot \alpha^i \right| = M_r.$$

Then,

$$|\alpha|^{n-r} \cdot M_r = \left| \alpha^{n-r} \cdot \sum_{i=0}^{r-1} a_i \cdot \alpha^i \right| = \left| \sum_{i=0}^{r-1} a_i \cdot \alpha^{n-r+i} \right| = \left| \sum_{j=n-r}^{n-1} a_{j-n+r} \cdot \alpha^j \right| \leq M_n.$$

□

Corollary 1. With the notations of Lemma 2, let $1 < k, n$, with $k = q \cdot n + r$, where $0 \leq r < n$, and $0 \leq a_0, \dots, a_{k-1} \leq N$ are integers. Then

$$\left| \sum_{i=0}^{k-1} a_i \cdot \alpha^i \right| \leq M \frac{|\alpha|^k}{|\alpha|^n - 1}.$$

Proof. Assume first that $k < n$. Then, by Lemma 3,

$$\left| \sum_{i=0}^{k-1} a_i \cdot \alpha^i \right| \leq M \frac{1}{|\alpha|^{n-k}} < M \frac{|\alpha|^k}{|\alpha|^n - 1}.$$

Now, let $k \geq n$. If $0 < r$, then by Lemma 3,

$$\begin{aligned} \left| \sum_{i=0}^{k-1} a_i \cdot \alpha^i \right| &\leq \left| \sum_{i=0}^{r-1} a_i \cdot \alpha^i \right| + \sum_{j=0}^{q-1} |\alpha|^{j \cdot n + r} \left| \sum_{i=0}^{n-1} a_{j \cdot n + r + i} \cdot \alpha^i \right| \\ &\leq |\alpha|^{r-n} M + |\alpha|^r \sum_{j=0}^{q-1} |\alpha|^{j \cdot n} M \\ &= M \cdot \left(|\alpha|^{r-n} + |\alpha|^r \frac{|\alpha|^{q \cdot n} - 1}{|\alpha|^n - 1} \right) \\ &= M \cdot \left(\frac{|\alpha|^{r-n} \cdot (|\alpha|^n - 1)}{|\alpha|^n - 1} + \frac{|\alpha|^{q \cdot n + r} - |\alpha|^r}{|\alpha|^n - 1} \right) \\ &= M \frac{|\alpha|^r - |\alpha|^{r-n} + |\alpha|^{q \cdot n + r} - |\alpha|^r}{|\alpha|^n - 1} \\ &= M \frac{|\alpha|^k - |\alpha|^{r-n}}{|\alpha|^n - 1} \leq M \frac{|\alpha|^k}{|\alpha|^n - 1}. \end{aligned}$$

If $r = 0$, then the proof is similar but even simpler. □

In Lemma 4, we show that the left-hand side of inequality (2) is maximal if the nonvanishing coefficients are maximal.

Lemma 4. Let $\alpha \in \mathbb{C}$, with $1 < |\alpha|$, $1 < N \in \mathbb{Z}$, let $0 \leq a_0, a_1, \dots, a_{n-1} \leq N$ be integers, and

$$M = \max \left\{ \left| \sum_{i=0}^{n-1} b_i \cdot \alpha^i \right| : 0 \leq b_0, b_1, \dots, b_{n-1} \leq N, \text{ integers} \right\}.$$

If $\left| \sum_{i=0}^{n-1} a_i \cdot \alpha^i \right| = M$, then $a_0, a_1, \dots, a_{n-1} \in \{0, N\}$.

Proof. Let $0 \leq j < n$ be such that $a_j \neq 0$, and $\mu = \sum_{i=0}^{n-1} a_i \cdot \alpha^i$. Since $M = |\mu|$, thus $|\mu - \alpha^j| \leq |\mu|$. Denote by $\bar{x}$ the complex conjugate of x . Then,

$$\mu \bar{\mu} - (\mu \bar{\alpha}^j + \bar{\mu} \alpha^j) + \alpha^j \bar{\alpha}^j = (\mu - \alpha^j)(\bar{\mu} - \bar{\alpha}^j) = |\mu - \alpha^j|^2 \leq |\mu|^2 = \mu \bar{\mu},$$

whence

$$-(\mu \bar{\alpha}^j + \bar{\mu} \alpha^j) + \alpha^j \bar{\alpha}^j \leq 0,$$

which implies

$$0 < \alpha^j \bar{\alpha}^j \leq \mu \bar{\alpha}^j + \bar{\mu} \alpha^j. \quad (4)$$

Assume that $a_j < N$. By the maximality of M , $|\mu + \alpha^j| \leq M$. Conversely, $M^2 \geq |\mu + \alpha^j|^2 = (\mu + \alpha^j)(\bar{\mu} + \bar{\alpha}^j) = \mu \bar{\mu} + \alpha^j \bar{\alpha}^j + \mu \bar{\alpha}^j + \bar{\mu} \alpha^j > \mu \bar{\mu} = |\mu|^2 = M^2$, which is a contradiction. $\square$

We may summarize the previous results in the following corollary.

Corollary 2. With the notations of Lemma 2, there exist $a_0, a_1, \dots, a_{n-1} \in \{0, 1\}$ such that

$$N \left| \sum_{i=0}^{n-1} a_i \cdot \alpha^i \right| = M,$$

where $a_{n-1} = 1$.

Now, we turn to the proof of our last observation of case *iii*) of Remark 5. Namely, if the left-hand side of inequality (2) is maximal, then the coefficient of the i^{th} power in this maximal modulus sum μ is nonvanishing if and only if α^i and μ lie on the same side of the normal line e of μ . This property can be expressed by the relation $|\arg(\mu) - \arg(\alpha^i)| < \frac{\pi}{2}$.

If we would like to represent this geometric property algebraically, we should observe that if β and γ are nonzero complex numbers, then $|\arg(\beta) - \arg(\gamma)| < \frac{\pi}{2}$ if and only if $\operatorname{Re}\left(\frac{\beta}{\gamma}\right) > 0$, or with another expression, $\frac{\beta}{\gamma} + \frac{\bar{\beta}}{\bar{\gamma}} > 0$. Here, $\operatorname{Re}(\beta)$ is the real part of β .

Lemma 5. Let $\alpha \in \mathbb{C}$, with $1 < |\alpha|$, $1 < N \in \mathbb{Z}$, and

$$M = \max \left\{ \left| \sum_{i=0}^{n-1} b_i \cdot \alpha^i \right| : 0 \leq b_0, b_1, \dots, b_{n-1} \leq N, \text{ integers} \right\}.$$

Furthermore, let the coefficients $a_0, a_1, \dots, a_{n-1} \in \{0, 1\}$ be chosen such that

$$N \left| \sum_{i=0}^{n-1} a_i \cdot \alpha^i \right| = M, \text{ and let } \mu = \sum_{i=0}^{n-1} a_i \cdot \alpha^i.$$

Then, $a_j = 1$ if and only if $\frac{\mu}{\alpha^j} + \frac{\bar{\mu}}{\bar{\alpha}^j} > 0$.

Proof. Assume first, that $a_j = 1$. Then, $|\mu - \alpha^j| \leq |\mu|$, whence by (4),

$$\frac{\mu}{\alpha^j} + \frac{\bar{\mu}}{\bar{\alpha}^j} = \frac{\mu \bar{\alpha}^j + \bar{\mu} \alpha^j}{\alpha^j \bar{\alpha}^j} \geq 1.$$

Now, let $a_j \neq 1$. Since a_j can only be either 0 or 1, this means that $a_j = 0$. Then, $|\mu + \alpha^j| \leq |\mu|$, whence $0 < \alpha^j \bar{\alpha}^j \leq -(\mu \bar{\alpha}^j + \bar{\mu} \alpha^j)$, and

$$\frac{\mu}{\alpha^j} + \frac{\bar{\mu}}{\bar{\alpha}^j} = \frac{\mu \bar{\alpha}^j + \bar{\mu} \alpha^j}{\alpha^j \bar{\alpha}^j} \leq -1.$$

□

Remark 6. By the proof of Lemma 5, there is no $0 \leq j < n$ for which $\frac{\mu}{\alpha^j} + \frac{\bar{\mu}}{\bar{\alpha}^j} = 0$. In other words, if μ is the maximal modulus subsum, then there is no power of α , which is perpendicular to μ .

Let $\beta, \gamma \in \mathbb{C} \setminus \{0\}$ such that $\arg(\beta) \neq \arg(\gamma)$. The two numbers determine two complementary sectors of the complex plane between β and γ , and counterwise (see Figure 4).

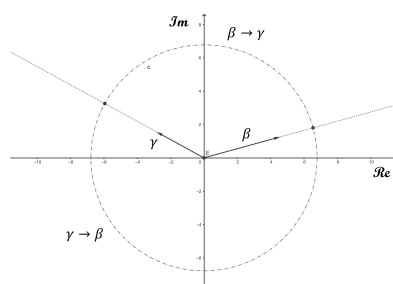


Figure 4. Sectors of the complex plane.

Corollary 3 states that if the left-hand side of inequality (2) is the maximal modulus sum μ , then there exist two different powers α^k and α^j such that all powers which are included in μ lie in the same sector defined by α^k and α^j , while the powers which are not included in μ lie in the other sector.

Corollary 3. With the notations of Lemma 2, let $a_0, a_1, \dots, a_{n-1} \in \{0, 1\}$ such that

$$N \left| \sum_{i=0}^{n-1} a_i \cdot \alpha^i \right| = M, \quad \mu = \sum_{i=0}^{n-1} a_i \cdot \alpha^i,$$

and denote by $\Im(\beta)$ be the imaginary part of $\beta \in \mathbb{C}$. Then, there exist $0 \leq j, k < n$ such that $a_i = 1$ if and only if $\Im\left(\frac{\alpha^i}{\alpha^j}\right) \geq 0$ and $\Im\left(\frac{\alpha^i}{\alpha^k}\right) \leq 0$, for all $0 \leq i < n$.

Proof. Let $\preceq$ be the binary relation on $\mathbb{C} \setminus \{0\}$, where $x \preceq y$ if and only if $\Im\left(\frac{y}{x}\right) \geq 0$. According to the notation of Figure 4, this means that $x \preceq y$ if and only if y lies in the sector $x \rightarrow -x$. Then, for any $\beta \in \mathbb{C} \setminus \{0\}$, the relation $\preceq$ is transitive on the set

$$\mathbb{C}_\beta = \left\{ \gamma : 0 \leq \frac{\beta}{\gamma} + \frac{\bar{\beta}}{\bar{\gamma}}, \text{ and } \gamma \in \mathbb{C} \setminus \{0\} \right\}.$$

Let $C_\mu = \left\{ \alpha^i : 0 \leq \frac{\mu}{\alpha^i} + \frac{\bar{\mu}}{\bar{\alpha}^i}, 0 \leq i < n \right\} \subseteq \mathbb{C}_\mu$. Clearly, $a_i = 1$ if and only if $\alpha^i \in C_\mu$. Since C_μ is a finite set, by the transitivity property, there exists not necessarily unique $0 \leq j, k < n$ such that $\alpha^j \preceq \gamma \preceq \alpha^k$ for all $\gamma \in C_\mu$. If $a_i = 0$, then $\alpha^i \notin C_\mu$, and either $\alpha^i \prec \alpha^j$ or $\alpha^k \prec \alpha^i$. $\square$

Now, we have collected everything necessary to prove Theorem 3.

Proof of Theorem 3. Let $0 < n$ be a sufficiently large integer, and according to the notation of Lemma 2, let

$$N \left| \sum_{i=0}^{n-1} a_i \cdot \alpha^i \right| = M, \text{ and } \mu = \sum_{i=0}^{n-1} a_i \cdot \alpha^i.$$

Let

$$c = \frac{|\mu|(|\alpha| - 1)}{|\alpha|^n - 1}. \quad (5)$$

Since α is not a positive real number, by Lemma 5, at least for one i , the coefficient $a_i \neq 1$, whence $c < 1$. By Corollary 1,

$$\left| \sum_{i=0}^{k-1} b_i \cdot \alpha^i \right| \leq M \frac{|\alpha|^k}{|\alpha|^n - 1} = Nc \frac{|\alpha|^n - 1}{|\alpha| - 1} \frac{|\alpha|^k}{|\alpha|^n - 1} = cN \frac{|\alpha|^k}{|\alpha| - 1}.$$

$\square$

The following corollary is an asymptotic extension of Theorem 3.

Corollary 4. Let $\alpha \in \mathbb{C}$ with $1 < |\alpha|$, and assume that α is not a positive real number. Let $0 < N \in \mathbb{Z}$ and

$$M_n = \max \left\{ \left| \sum_{i=0}^{n-1} b_i \cdot \alpha^i \right| : 0 \leq b_0, b_1, \dots, b_{n-1} \leq N, \text{ integers} \right\},$$

for all $0 < n \in \mathbb{Z}$. Then, there exists $c < 1$ depending only on α such that

$$\lim_{n \rightarrow \infty} \frac{M_n}{|\alpha|^n} = \frac{cN}{|\alpha| - 1}.$$

Proof. By Theorem 3,

$$\frac{M_n}{|\alpha|^n} \leq \frac{c_1 N}{|\alpha| - 1},$$

for all $0 < n \in \mathbb{Z}$ with some $c_1 < 1$ depending only on α . By Lemma 3, $|\alpha| M_{n-1} \leq M_n$. Hence, the sequence $\frac{M_n}{|\alpha|^n}$ is an increasing bounded sequence, which implies the corollary. $\square$

As is explained in Remark 4, there is an exact lower bound on the possible values of the constant c in Theorem 3. Based on the previous results, we can construct a fast algorithm to find a good approximation of the value of this constant. First, we slightly modify the definition of the relation introduced in the proof of Corollary 1.

Definition 3. Let $\preceq$ be the binary relation on $\mathbb{C} \setminus \{0\}$, where $x \preceq y$ if and only if either $y = c \cdot x$ with some $1 \leq c \in \mathbb{R}$ or $\Im\left(\frac{y}{x}\right) > 0$.

Remark 7. If $x, y \in \mathbb{C} \setminus \{0\}$, then $x \preceq y$ means that either $\arg(x) \leq \arg(y) < \arg(x) + \pi$ or $\arg(x) \leq \arg(y) + 2\pi < \arg(x) + \pi$. If $\arg(x) = \arg(y)$, then $|x| \leq |y|$.

Remark 8. This $\preceq$ is a total ordering on any open half-plane (the boundary line is excluded from the plane).

Choose a sufficiently large n and let

$$C_1 = \left\{ \alpha^i : 0 \leq \alpha^i + \bar{\alpha}^i, 0 \leq i < n \right\}, \text{ and}$$

$$C_{-1} = \left\{ \alpha^i : 0 > \alpha^i + \bar{\alpha}^i, 0 \leq i < n \right\}.$$

Sort C_1 and C_{-1} by $\preceq$ and glue them at both ends. Then, we obtain a cyclically sorted set $\beta_0, \dots, \beta_{n-1}$ of $\alpha^0, \dots, \alpha^{n-1}$, where the next of β_{n-1} is $\beta_n = \beta_0$. The property that $\beta_0, \dots, \beta_{n-1}$ is sorted means that for a given β_i the β_{i+1} is such that $0 \leq \arg(\beta_{i+1}) - \arg(\beta_i)$ is the smallest possible, i.e., the β_i 's are in increasing order by their argument. (If they have the same argument, then they are sorted by their modulus.)

If we want to have better constants, then we have to find an n such that $\Im m(\alpha^n)$ is as small as it is possible.

To find c , we can use Algorithm 1 with $O(n)$ operations on complex numbers.

The idea of the algorithm is the following:

- (1) In the outer while loop for a given i , we compute the sum of the consecutive β 's which are contained in the open half-plane started from β_i . Let us denote this subsum by μ_i . By Lemma 5, the maximal modulus subsum of the set of β 's will be one of $\mu_0, \dots, \mu_{n-1}$.
- (2) In the inner while loop, we rotate the half plane, and compute μ_{i+1} from μ_i by accumulating new β 's at the end and eliminating β_i from the front.

Algorithm 1: Calculating a proper constant c of Theorem 3

```

Data:  $\beta_0, \dots, \beta_{n-1}$  // Input:  $\alpha^i$  sorted according to  $\preceq$ 
Result:  $c$  // Output: an approximation of the constant in Theorem 3
max  $\leftarrow 0$  // max: the largest modulus subsum of  $\beta$ 's
 $\mu \leftarrow 0$  //  $\mu$ : the sum of  $\beta$ 's in a given half-plane
 $i \leftarrow 0, j \leftarrow 0$ 
while  $i < n$  do // Calculating  $\mu$  in the half-plane starting from  $\beta_i$ 
    while  $\Im m\left(\frac{\beta_j}{\beta_i}\right) > 0$  do // rotating the half-plane
         $\mu \leftarrow \mu + \beta_j$  // New  $\beta$ 's in the front are added to  $\mu$ 
         $j \leftarrow j + 1 \bmod n$ 
        if max  $< |\mu|$  then // max is replaced by the new largest  $\mu$ 
            max  $\leftarrow |\mu|$ 
        end
    end
     $\mu \leftarrow \mu - \beta_i$  // Exceeded  $\beta_i$  at the end is eliminated from  $\mu$ 
     $i \leftarrow i + 1$ 
end
 $c \leftarrow \max \cdot \frac{|\alpha| - 1}{|\alpha|^n - 1}$  //  $c$ : the constant defined in Equation (5)
return  $c$ 

```

In the following theorem, we prove a relation between the relative information quantity described in Definition 2 and the length of a polynomial in a CNS representation explained in Definition 1. For the calculations of the constants c_1, c_2 , we use estimates on geometric sums of complex numbers, where Theorem 3 plays an important role. Theorem 4 will be

used in Section 3 for the proof of the existence of an addition automaton in a canonical number system.

Theorem 4. Let $P(x) = x^d + p_{d-1}x^{d-1} + \dots + p_0$ be a CNS polynomial. Then, there exist effectively computable constants c_1, c_2 such that

$$\mathbb{I}(A) - c_1 \leq L(A) \leq \mathbb{I}(A) + c_2 \quad (6)$$

holds for every $A(x) \in \mathbb{Z}[x]$.

Proof. The proof is based on the idea of [6]. The new theorem is a more generalized form of the previous result, and its proof introduces a refined method for calculating the constants c_1 and c_2 . This refinement allows for more precise constants compared to earlier approaches.

Specifically, we have extended the theorem by B. Kovács and A. Pethő, offering a new method for calculating these constants with greater accuracy. The key contribution of this work is the development of an improved algorithm for determining c_1 and c_2 , leading to more exact results in the context of canonical number systems.

Let $(P, \mathcal{N})$ be a CNS, with $N = |\mathcal{N}|$ and $A(x) \in \mathbb{Z}[x]$ with canonical representation

$$B(x) = b_{L-1}x^{L-1} + \dots + b_0 \in \mathcal{N}[x],$$

where $L = L(A) = L(B) = \deg(B) + 1$. Then, $\varphi(A) = \varphi(B)$, which means $\mathbb{I}(A) = \mathbb{I}(B)$. Assume that α is a root of $P(x)$. Then, by Theorem 3,

$$\begin{aligned} |B(\alpha)| &= |b_{L-1}\alpha^{L-1} + b_{L-2}\alpha^{L-2} + \dots + b_0| \\ &\leq c \cdot (N-1) \frac{|\alpha|^L}{|\alpha| - 1} < c \cdot N \frac{|\alpha|^L}{|\alpha| - 1}, \end{aligned}$$

where $0 < c < 1$ depends only on α .

By Theorem 2, $0 < |\alpha| - 1$ validates the last inequality and makes it possible to take the logarithm of both sides. Then, we obtain

$$\log(|B(\alpha)|) < \log(c) + \log(N) + L \log(|\alpha|) - \log(|\alpha| - 1).$$

Again by Theorem 2, we may have

$$\begin{aligned} \frac{\log(|B(\alpha)|)}{\log(|\alpha|)} &< L + \frac{\log(c) + \log(N) - \log(|\alpha| - 1)}{\log(|\alpha|)} \quad \text{and} \\ \frac{\log(|B(\alpha)|)}{\log(|\alpha|)} - \frac{\log(c) + \log(N) - \log(|\alpha| - 1)}{\log(|\alpha|)} &< L, \end{aligned}$$

which can be effectively bounded from below by some c_1 :

$$\frac{\log(|B(\alpha)|)}{\log(|\alpha|)} - c_1 < L.$$

Taking the maximum on all roots of P , we obtain the first inequality of (6).

$$\mathbb{I}(A) - c_1 \leq L(A).$$

For the proof of the second inequality, set $k = \lceil \mathbb{I}(A) \rceil$, which denotes the upper integer part of $\mathbb{I}(A)$, and let $B(x) = x^k B_1(x) + B_0(x)$, where $B_0, B_1 \in \mathcal{N}[x]$ and $\deg(B_0) < k$. Assume that α is a root of P . Then,

$$B_1(\alpha) = \frac{B(\alpha) - B_0(\alpha)}{\alpha^k} \quad \text{and}$$

$$\begin{aligned} |B_1(\alpha)| &\leq \frac{|B(\alpha)|}{|\alpha|^k} + \frac{|B_0(\alpha)|}{|\alpha|^k} \\ &< \frac{|B(\alpha)|}{|\alpha|^k} + N \frac{|\alpha|^k - 1}{|\alpha|^k(|\alpha| - 1)} \\ &< \frac{|B(\alpha)|}{|\alpha|^k} + \frac{N}{|\alpha| - 1}. \end{aligned}$$

The fraction $\frac{c_\alpha \cdot N}{|\alpha| - 1}$ can be bounded by an effectively computable constant depending only on P , and by the definition of k , $\frac{|B(\alpha)|}{|\alpha|^k} = \frac{|A(\alpha)|}{|\alpha|^k} \leq 1$. Hence, $|B_1(\alpha)| \leq c$ where c is a constant depending only on P . Since there exist only finitely many polynomials $A' \in \mathbb{Z}[x]$ with $\deg(A') < d$ satisfying $A'(\alpha) < c$ and these polynomials are effectively computable, we can determine

$$c'_\alpha = \max \left\{ \deg(B') : B' \in \mathcal{N}[x], \varphi(B') = \varphi(A'), \deg(A') < d, A'(\alpha) < c \right\} + 1.$$

Let $c_2 = 1 + \max_{1 \leq i \leq d} c'_{\alpha_i}$. Then

$$L(A) = \deg(B) + 1 = k + \deg(B_1) + 1 \leq k + c'_\alpha \leq \mathbb{I}(A) + c_2.$$

□

3. Automata and Canonical Number Systems

As we have seen before, adding and multiplying by a constant are implementable with automata in CNSs. In this section, we prove that an automaton exists that executes the digit-wise addition. The existence of such an automaton is not obvious since the length of the sum of two algebraic integers represented in the canonical number system may have a shorter length than the summands'.

Definition 4. The 6-tuple $\mathcal{A} = (k, S, X, Y, s, \delta)$ is called a finite transducer automaton with k input tape if

$k \in \mathbb{Z}^+$;

S is a finite, non-empty set of states;

X is a finite set of at least two elements (the input alphabet);

Y is a finite set of at least two elements (the output alphabet);

$s \in S$ is the initial state;

$\delta : S \times X^k \longrightarrow S \times Y$ is a unique mapping.

Remark 9. We follow the convention for extending the transducer automaton to operate on words of the input alphabet and having the result as a word of the output alphabet.

In the following, if $\bar{a} = (a_0 \dots a_{n-1}) \in \mathcal{N}^*$ is a finite word, then we will use the notation $Q_a(x) = a_{n-1}x^{n-1} + \dots + a_0$ for the corresponding polynomial.

Theorem 5. Let $(P, \mathcal{N})$ be a CNS. Then, there exists a finite transducer automaton $\mathcal{A}$ with two input tapes, such that $\bar{c} = \mathcal{A}(\bar{a}, \bar{b})$ for all $\bar{a}, \bar{b}, \bar{c} \in \mathcal{N}^*$ if $\varphi(Q_c) = \varphi(Q_a + Q_b)$.

Remark 10. In Theorem 5, we assume that the length of the words $\bar{a}, \bar{b}, \bar{c}$ are equal. If not, we extend them with the necessary amount of 0s on the right.

Remark 11. In [19], there is a similar result, but the proof there is not constructive. Furthermore, based on our proof, we can state the minimality of our construction, as it is done in Theorem 6.

Proof of Theorem 5. We prove the statement by constructing the addition automaton $\mathcal{A} = (2, S, X, Y, s, \delta)$, where $X = Y = \mathcal{N}$. We will define $S \subseteq \mathcal{N}[x]$ and δ in an appropriate way, and we will prove that S is finite. Assume that $N = |\mathcal{N}|$.

Let S be the smallest set such that

1. $0 \in S$;
2. if $A \in S$, $B \in \mathcal{N}[x]$, $b \in \mathcal{N}$, and $0 \leq a < 2N - 1$ such that $\varphi(xB(x) + b) = \varphi(A(x) + a)$ then $B \in S$.

We define the transition function $\delta : S \times \mathcal{N}^2 \rightarrow S \times \mathcal{N}$ by $\delta(A, a_1, a_2) = (B, b)$, if $\varphi(xB(x) + b) = \varphi(A(x) + a_1 + a_2)$.

Let $\bar{a}, \bar{b} \in \mathcal{N}^*$, $A_0 = 0$, and $Q_0 = Q_a + Q_b$. If $0 \leq i$, let A_{i+1} be defined by $\delta(A_i, a_i, b_i) = (A_{i+1}, c_i)$, and $Q_{i+1}(x) = Q_i(x) + (c_i - a_i - b_i)x^i$. By the definition of δ , we have

$$\varphi(Q_{i+1}(x) + A_{i+1}(x)x^{i+1}) = \varphi(Q_i(x) + A_i(x)x^i) = \varphi(Q_a + Q_b),$$

for all $0 \leq i$.

Let $n = 1 + \max\{\deg(Q_a), \deg(Q_b)\}$ and $k = 1 + \deg(A_i)$. Then, $\deg(Q_n) < n$, $Q_c = Q_{n+k} = Q_n + A_n x^n \in \mathcal{N}[x]$, and $\varphi(Q_c) = \varphi(Q_a + Q_b)$.

Hence, by Theorem 4, and by Lemma 1(iii),

$$\begin{aligned} n + k &= \deg(Q_c) + 1 = L(Q_c) \\ &\leq \mathbb{I}(Q_c) + C_2 \\ &\leq \max\{\mathbb{I}(Q_a), \mathbb{I}(Q_b)\} + \mathbb{I}(2) + C_2 \\ &= n + \mathbb{I}(2) + C_2, \end{aligned}$$

where C_2 is the constant c_2 in Theorem 4.

This yields that

$$\deg(A_i) < k \leq \mathbb{I}(2) + C_2.$$

Since S is defined to be the smallest set satisfying (1) and (2), every $A \in S$ may appear as the last carry A_n . Thus, for all $A \in S \subseteq \mathcal{N}[x]$, $\deg(A) < \mathbb{I}(2) + C_2$, which implies that S is finite. $\square$

Remark 12. Observe now the properties of the states defined in the proof of Theorem 5. Let $A(x) = a_k x^k + a_{k-1} x^{k-1} + \dots + a_0$, where $a_k \neq 0$ and $A(x) \in S$. Assume that the automaton is in state A , and there are no more digits arriving from the input. Then, by the definition of the transition function δ , the output of the automaton starting from this state is the sequence $a_0 a_1 \dots a_k$. This means that different states represent different tail releases of the output, i.e., if the automaton is state $B \neq A$, then the output without input is different to $a_0 a_1 \dots a_k$.

Theorem 6. The addition automaton, constructed in the proof of Theorem 5, is minimal.

Proof. In the definition of $\mathcal{A}$ in the proof of the previous theorem, S is the smallest possible set satisfying the given properties. This means that for any $A \in S$, there exist proper inputs $\bar{a}, \bar{b}$ such that $\mathcal{A}(\bar{a}, \bar{b})$ terminates in state A .

Let $S = \{A_1, A_2, \dots, A_n\}$ and $\bar{a}_1, \bar{a}_2, \dots, \bar{a}_n, \bar{b}_1, \bar{b}_2, \dots, \bar{b}_n$ are such that $\mathcal{A}(\bar{a}_i, \bar{b}_i)$ terminates in state A_i for all $i \in \{1, \dots, n\}$.

Assume that there exists an automaton $\mathcal{A}'$, which executes the same addition as $\mathcal{A}$, but $|S'| < |S|$, i.e., $\mathcal{A}'$ has strictly fewer states. Then, by the pigeonhole principle, there exist $1 \leq i < j \leq n$ such that $\mathcal{A}'(\bar{a}_i, \bar{b}_i)$ and $\mathcal{A}'(\bar{a}_j, \bar{b}_j)$ terminates in the same states. By Remark 12, automaton $\mathcal{A}$ continues with different tail releases from the states A_i and A_j , but $\mathcal{A}'$ continues in the same way if there are no more input digits. This is a contradiction because we assumed that $\mathcal{A}$ and $\mathcal{A}'$ execute the same operation. Hence, the assumption of the existence of $\mathcal{A}'$ is wrong. $\square$

Although we can not be sure there is no linear time algorithm for multiplication, we have the following.

Theorem 7. Let $(P, \mathcal{N})$ be a CNS. Then, there are no finite transducer automaton S with two input tapes, such that $\bar{c} = S(\bar{a}, \bar{b})$ for all $\bar{a}, \bar{b}, \bar{c} \in \mathcal{N}^*$ if $\varphi(Q_c) = \varphi(Q_a \cdot Q_b)$.

Proof. On the contrary, assume that $\mathcal{A} = (2, S, \mathcal{N}, \mathcal{N}, s, \delta)$ executes the multiplication, and $N = |\mathcal{N}|$.

Let $\bar{a}, \bar{c} \in \mathcal{N}^*$ satisfying $\varphi(Q_c) = \varphi(Q_a^2)$. Then by Lemma 1(vi), and by Theorem 4,

$$\begin{aligned} \deg(Q_c) &= L(Q_c) - 1 \geq \mathbb{I}(Q_c) - C_1 - 1 = 2\mathbb{I}(Q_a) - C_1 - 1 \\ &\geq 2(L(Q_a) - C_2) - C_1 = 2\deg(Q_a) - 2C_2 - C_1 + 1. \end{aligned}$$

Set $n = 1 + \deg(Q_a)$, and $Q_i = c_i x^i + \dots + c_0$ for all $0 \leq i$. (If $\deg(Q_c) < i$, then $Q_i = Q_c$.) Since the automaton executes the multiplication, there exist $s_0, s_1, \dots \in S$ such that $s_0 = s$, and $\delta(s_i, a_i, a_i) = (s_{i+1}, c_i)$, for all $0 \leq i$.

If $n \leq i$, then $a_i = 0$, and $Q_{c,n}(x) = \frac{Q_c(x) - Q_n(x)}{x^n}$ is determined purely by s_n . Since $\deg(Q_{c,n}) \geq n - 2C_2 - c_1 + 1$, there are infinitely many different $Q_{c,n}$, whence there are infinitely many different corresponding states. However, this is a contradiction since we assumed that $\mathcal{A}$ is a finite automaton. $\square$

4. Estimation of the Number of States of an Addition Automaton

In this section, we show an example of how to execute addition and how to construct the addition automaton based on the addition algorithm in a given polynomial CNS. We also provide the result of an experiment where we determined the addition automata for different CNSs.

4.1. Example of the Computation in the Number System $(x^2 + x + 2, \{0, 1\})$

Let $x^2 + x + 2$ be the base polynomial and $\{0, 1\}$ is the digit set. By Theorem 1, we know that this is a CNS.

Let $\gamma_1 = 110101$ and $\gamma_2 = 101111$ be 6-bit long binary ‘numbers’ in the above CNS, and let $\gamma = \gamma_1 + \gamma_2$. The calculation of the digits of γ is similar to the usual binary arithmetic, but the carry propagation is a bit more advanced. In the classical binary system, we use the fact that $1(-2)_2 = 1 \cdot 2^1 + (-2) \cdot 2^0 = 0$ (i.e., we use the $x - 2$ polynomial as the base). In the present system, according to this observation, $112_{x^2+x+2} = 0$.

The addition process works as follows:

1. Initialization

The two numbers, γ_1 and γ_2 , are digit-wise added without any further computations. The result is $\gamma' = 211212$.

2. Reduction

Starting from the least significant digit on the right, we reduce the augmented digits, which are not in the digit set $\{0, 1\}$. In this CNS, this is the only value 2. However, as in the classical binary systems, we have to take into account the possible carries, arriving from lower digits. How can we calculate this carry?

In the case of the last digit, we assume that there is no carry; more precisely, the value of the carry is 0. To eliminate the last digit 2, we should subtract 112 . The result is $(-1)(-1)0$, which is split into two parts: the calculated digit at the given position and the carry for the next position. In our case, the digit is 0, while the carry is $(-1)(-1)$. For the next digit, we add the carry arriving from the right to the value given at the position: $1 + (-1)(-1) = (-1)0$. Since 0 is a valid digit, we do not need any further operation at this position. The carry for the next position is (-1) .

The next augmented digit is 2. Adding the carry, we obtain $2 + (-1) = 1$, so the next calculated digit is 1, and the carry is 0.

We continue the iteration until γ' is completely processed and the carry becomes 0.

The algorithm described above can be visualized by Table 2.

Table 2. Computation in the binary number system.

γ'					2	1	1	2	1	2
$\mathfrak{C}$	0	1	10	$-1-1$	0	0	0	-1	$-1-1$	0
$\mathfrak{C} + \gamma'$		1	10	$-1-1$	2	1	1	1	-10	2
mod		0	0	$+(112)$	$-(112)$	0	0	0	0	$-(112)$
γ''	0	1	10	101	$-1-10$	1	1	1	-10	$-1-10$
γ		1	0	1	0	1	1	1	0	0

Based on the algorithm for calculating the sum, we may construct the corresponding addition automaton. The states of the automaton are the possible carries during the computation. We start from the carry 0 and calculate the transition according to the possible inputs (augmented digit). The value of the transition is a pair $(\mathfrak{C}, d)$, where $\mathfrak{C}$ is the next carry and d is the output digit. The new carries are added to the automaton, and until we have unexplained transitions, we continue the construction of the automaton.

The process generates the transition function of the automaton, as illustrated in Table 3.

Table 3. State transition table.

	State	0	$-1-1$	10	-1	1	11	-10	$-1-2$
Input	0	(0, 0)	(10, 1)	(1, 0)	(11, 1)	(0, 1)	(1, 1)	(-1 , 0)	(10, 0)
	1	(0, 1)	(-1 , 0)	(1, 1)	(0, 0)	($-1-1$, 0)	(-10 , 0)	(-1 , 1)	(10, 1)
	2	($-1-1$, 0)	(-1 , 1)	(10, 0)	(0, 1)	($-1-1$, 1)	(-10 , 1)	($-1-2$, 0)	(-1 , 0)

The values of the cells in the table contain pairs: the next state (carry) and the output (digit), according to the present state (carry) and the input (augmented digit). If a new unexplored carry appears in the transition value, then a new column is added to the table. We continue to fill out the table until no new carry appears. By Theorem 5, the algorithm will terminate in finitely many steps.

4.2. Analysis of Binary Polynomial CNS's

As we have observed before, the states of the addition automaton may represent the possible carries. According to construction, these are polynomials in $\mathcal{N}[x]$. Since the degrees of the state polynomials are bounded by the constant $c = \mathbb{I}(2) + c_2$ of Theorem 4, we may state the following simple result.

Theorem 8. *Let $(P, \mathcal{N})$ be a CNS, and $\mathcal{A}$ be the minimal automaton implementing the addition. Then, the number of states of $\mathcal{A}$ is bounded by $|\mathcal{N}|^c$.*

We have made an experiment on the construction of addition automata for different CNS polynomials. We determined and counted the number of states for binary Kovács-type CNS polynomials of different degrees. (i.e., the coefficients of P have the property $1 = p_d \leq p_{d-1} \leq \dots \leq p_0 = 2$.) A. Kovács in [10] listed the canonical polynomials of binary number systems until degree 8. According to this result, we know, for instance, that the only binary CNS polynomials of degree 3 satisfying the conditions of Theorem 1, are $x^3 + 2$, $x^3 + x^2 + x + 2$, and $x^3 + 2x^2 + 2x + 2$. Using the construction of the proof of Theorem 5, we implemented a computer program to calculate the addition automaton for a given CNS polynomial. We determined all different CNS polynomials of degrees from 3 to 10 in the form given in Theorem 1, and constructed the corresponding addition automaton. We collected the size of these automata, which are expressed by the number of states. The results are summarized in Table 4. The table contains the size (number of states) of the smallest and largest automata for different degree CNS polynomials.

Table 4. Number of states of addition automata.

Deg	Min. NoS	Max. NoS
3	62	125
4	239	1195
5	1185	13,037
6	6248	155,765
7	33,387	2,041,141
8	185,695	27,270,180
9	1,074,944	370,005,950
10	6,419,041	$\geq 380,278,058$

As we advanced to higher degree CNS polynomials, the experiment ran into memory limitations. When we computed the transition function of the automaton in question, we had to store the states and the effect of the input digits. To save some space, we did not care about the output, and we just represented the state transitions. Since the number of states was increasing exponentially with the degree of the CNS polynomials, even for degree 10, we ran out of memory during the tests. The experiment was executed on a computer with an Intel Core i9-9900K CPU on 3.60GHz equipped with 64 GB of RAM. The running time did not limit the computation since it took only some hours.

5. Conclusions

The presented research demonstrates the feasibility of constructing finite transducer automata for digit-wise addition of polynomials in canonical number systems (Theorem 5). The constructive proof provided also establishes that the resulting automata are minimal (Theorem 6). The proof of Theorem 5 is based on the relation between the length of a

polynomial A in canonical representation and the information quantity of A (Theorem 4), as well as on the additive property of the information quantity (Lemma 1(iii)). For practical applications, it is reasonable to compute the constants appearing in Theorem 4 with a reasonably good approximation of the possible minimum values. To achieve this, we developed Algorithm 1, which is based on an improved upper bound for geometric sums (Theorem 3).

The study also exposed a fundamental limitation: as is proven in Theorem 7, no finite transducer automaton can be created for the multiplication of polynomials in canonical representation. At present, we do not know whether an algorithm exists that can execute the multiplication of n digit numbers (or analogously degree n polynomials) in $O(n)$ time; however, based on the above result, we cannot do this with constant memory usage.

Author Contributions: The authors T.H. and V.P. equally contributed to every component of the research, writing, reviewing and management of the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially supported by the project TKP2021-NKTA of the University of Debrecen, Hungary. Project no. TKP2021-NKTA-34 has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund, financed under the TKP2021-NKTA funding scheme. The APC was funded by the University of Debrecen.

Data Availability Statement: There were no new data created, and there were no particular data used during the research.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

- Knuth, D.E. *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*; Addison-Wesley: Boston, MA, USA, 1981.
- Kátai, I.; Szabó, J. Canonical number-systems for complex integers. *Acta Sci. Math.* **1975**, *37*, 255–260.
- Kátai, I.; Kovács, B. Canonical number systems in algebraic number fields. *Acta Math. Hung.* **1981**, *37*, 159–164.
- Kovács, B. Integral domains with canonical number systems. *Publ. Math.* **1989**, *36*, 153–156.
- Kovács, B.; Pethő, A. Number systems in integral domains, especially in orders of algebraic number fields. *Acta Sci. Math.* **1991**, *55*, 287–299.
- Kovács, B.; Pethő, A. On a representation of algebraic integers. *Stud. Sci. Math. Hung.* **1992**, *27*, 169–172.
- Pethő, A. On a polynomial transformation and its application to the construction of a public key cryptosystem. In *Computational Number Theory: Proceedings of the Colloquium on Computational Number Theory held at Kossuth Lajos University, Debrecen, Hungary, 4–9 September 1989*; Pethő, A., Pohst, M.E., Williams, H.C., Zimmer, H.G., Eds.; De Gruyter: Berlin, Germany; New York, NY, USA, 1991; pp. 31–44.
- S. Akiyama.; Pethő, A. On a canonical number systems. *Theor. Computer. Sci.* **2002**, *270*, 921–933.
- Pethő, A.; Varga, P. Canonical number systems over imaginary quadratic Euclidean domains. *Colloq. Math.* **2016**, *146*, 1–22.
- Kovács, A. Generalized binary number systems. *Ann. Univ. Sci. Budapest, Sect. Comp* **2001**, *20*, 195–206.
- Burcsi, P.; Kovács, A. Exhaustive search methods for CNS polynomials. *Monatshefte Math.* **2008**, *155*, 421–430.
- Grabner, P.J.; Kirschenhofer, P.; Prodinger, H. The sum-of-digits function for complex bases. *J. Lond. Math. Soc.* **1998**, *57*, 20–40.
- Thuswaldner, J.M. Elementary properties of the sum of digits function in quadratic number fields. In *Applications of Fibonacci Numbers*; Et Al Bergum, G.E., Eds.; Kluwer Academic Publisher: Alphen aan den Rijn, The Netherlands, 1998; Volume 7, 405–414.
- Allouche, J.; Scheicher, K.; Tichy, R.F. Regular Maps in Generalized Number Systems. *Math. Slovaca* **2000**, *50*, 41–58.
- Scheicher, K.; Thuswaldner, J.M. Canonical Number Systems, Counting Automata Furthermore, Fractals. *Math. Proc. Camb. Philos. Soc.* **2007**, *133*, 163–182.
- Samuel, E. *Automata, Languages, and Machines*; Academic Press: New York, NY, USA, 1974.
- Kuich, W.; Salomaa, A. *Semirings, Automata, Languages*; Springer: Berlin/Heidelberg, Germany, 1986.

18. Akiyama, S.; Borbély, T.; Brunotte, H.; Pethő, A.; Thuswaldner, J.M. On a generalization of the radix representation—A survey. *Fields Inst. Commun.* **2004**, *41*, 19–27.
19. Berthé, V.; Rigo, M. (Eds.) *Combinatorics, Automata and Number Theory*; Cambridge University Press: Cambridge, UK, 2015.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.