CHAPTER 7

# *Numeration systems*

## Contents



## 7.0. Introduction

This chapter deals with positional numeration systems. Numbers are seen as finite or infinite words over an alphabet of digits. A *numeration system* is defined by a couple composed of a base or a sequence of numbers, and of an alphabet of digits. In this chapter we study the representation of natural numbers, of real numbers and of complex numbers. We will present several generalizations of the usual notion of numeration system, which lead to interesting problems.

Properties of words representing numbers are well studied in number theory: the concepts of period, digit frequency, normality give way to important results.

Cantor sets can be defined by digital expansions.

In computer arithmetic, it is recognized that algorithmic possibilities depend on the representation of numbers. For instance, addition of two integers represented in the usual binary system, with digits 0 and 1, takes a time proportional to the size of the data. But if these numbers are represented with signed digits 0, 1, and $-1$, then addition can be realized in parallel in a time independent of the size of the data.

Since numbers are words, finite state automata are relevant tools to describe sets of number representations, and also to characterize the complexity of arithmetic operations. For instance, addition in the usual binary system is a function computable by a finite automaton, but multiplication is not.

Usual numeration systems, such that the binary and the decimal ones, are described in the first section. In fact, these systems are a particular case of all the various generalizations that will be presented in the next sections.

The second section is devoted to the study of the so-called beta-expansions, introduced by Rényi, see Notes. It consists in taking for base a real number $\beta > 1$. When $\beta$ is actually an integer, we get the standard representation. When $\beta$ is not an integer, a number may have several different $\beta$-representations. A particular $\beta$-representation, playing an important role, is obtained by a greedy algorithm, and is called the $\beta$-expansion; it is the greatest in the lexicographic order. The set of $\beta$-expansions of numbers of $[0, 1[$ is shift-invariant, and its closure, called the $\beta$-shift, is a symbolic dynamical system. We give several results on these topics. We do not cover the whole field, which is very lively and still growing. It has interesting connections with number theory and symbolic dynamics.

In the third section we consider the representation of integers with respect to a sequence of integers, which can be seen as a generalization of the notion of base. The most popular example is the one of Fibonacci numbers. Every positive integer can be represented in such a system with digits 0 and 1. This field is closely related to the theory of beta-expansions.

The last section is devoted to complex numbers. Representing complex numbers as strings of digits allows to handle them without separating real and imaginary part. We show that every complex number has a representation in base $-n \pm i$, where $n$ is an integer $\geq 1$, with digits in $\{0, \ldots, n^2\}$. This numeration system enjoys properties similar to those of the standard $\beta$-ary system.

For notations concerning automata and words the reader may want to consult Chapter 1.

## 7.1. Standard representation of numbers

In this section we will study standard numeration systems, where the base is a natural number. We will represent first the natural numbers, and then the nonnegative real numbers. The notation introduced in this section will be used in the other sections.

### 7.1.1. Representation of integers

Let $\beta \geq 2$ be an integer called the *base*. The (usual) *$\beta$-ary representation* of an integer $N \geq 0$ is a finite word $d_k \cdots d_0$ over the digit alphabet $A = \{0, \ldots, \beta-1\}$, and such that

$$N = \sum_{i=0}^{k} d_i \beta^i.$$

Such a representation is unique, with the condition that $d_k \neq 0$. This representation is called *normal*, and is denoted by

$$\langle N \rangle_\beta = d_k \cdots d_0$$

most significant digit first.

The set of all the representations of the positive integers is equal to $A^*$.

Let us consider the addition of two integers represented in the $\beta$-ary system. Let $d_k \cdots d_0$ and $c_k \cdots c_0$ be two $\beta$-ary representations of respectively $N$ and $M$. It is not a restriction to suppose that the two representations have the same length, since the shortest one can be padded to the left by enough zeroes. Let us form a new word $a_k \cdots a_0$, with $a_i = d_i + c_i$ for $0 \leq i \leq k$. Obviously, $\sum_{i=0}^{k} a_i \beta^i = N + M$, but the $a_i$'s belong to the set $\{0, \ldots, 2(\beta - 1)\}$. So the word $a_k \cdots a_0$ has to be transformed into an equivalent one (*i.e.* having the same numerical value) belonging to $A^*$.

More generally, let $C$ be a finite alphabet of integers, which can be positive or negative. The *numerical value* in base $\beta$ on $C^*$ is the function

$$\pi_\beta : C^* \longrightarrow \mathbb{Z}$$

which maps a word $w = c_n \cdots c_0$ of $C^*$ onto $\sum_{i=0}^{n} c_i \beta^i$. The *normalization* on $C^*$ is the partial function

$$\nu_C : C^* \longrightarrow A^*$$

that maps a word $w = c_n \cdots c_0$ of $C^*$ such that $N = \pi_\beta(w)$ is nonnegative onto its normal representation $\langle N \rangle_\beta$. Our aim is to prove that the normalization is computable by a finite transducer. We first prove a lemma.

Lemma 7.1.1. *Let $C$ be an alphabet containing $A$. There exists a right subsequential transducer that maps a word $w$ of $C^*$ such that $N = \pi_\beta(w) \geq 0$ onto a word $v$ belonging to $A^*$ and such that $\pi_\beta(v) = N$.*

*Proof.* Let $m = \max\{|c - a| \mid c \in C, a \in A\}$, and let $\gamma = m/(\beta - 1)$. First observe that, for $s \in \mathbb{Z}$ and $c \in C$, by the Euclidean division there exist unique $a \in A$ and $s' \in \mathbb{Z}$ such that $s + c = \beta s' + a$. Furthermore, if $|s| < \gamma$, then $|s'| \leq (|s| + |c - a|)/\beta < (\gamma + m)/\beta = \gamma$.

Consider the subsequential finite transducer $(\mathcal{A}, \omega)$ over $C^* \times A^*$, where $\mathcal{A} = (Q, E, 0)$ is defined as follows. The set $Q = \{s \in \mathbb{Z} \mid |s| < \gamma\}$ is the set of possible carries, the set of edges is

$$E = \{s \xrightarrow{c/a} s' \mid s + c = \beta s' + a\}.$$

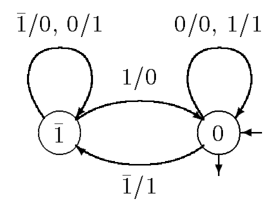


**Figure 7.1.** Right subsequential transducer realizing the conversion in base 2 from $\{\bar{1}, 0, 1\}$ onto $\{0, 1\}$

Observe that the edges are "letter-to-letter". The terminal function is defined by $\omega(s) = \langle s \rangle_\beta$ for $s \in Q$ such that $\pi_\beta(s) \geq 0$.

Now let $w = c_n \cdots c_0 \in C^*$ and $N = \sum_{i=0}^{n} c_i \beta^i$. Setting $s_0 = 0$, there is a unique path

$$s_0 \xrightarrow{c_0/a_0} s_1 \xrightarrow{c_1/a_1} s_2 \xrightarrow{c_2/a_2} \cdots \xrightarrow{c_{n-1}/a_{n-1}} s_n \xrightarrow{c_n/a_n} s_{n+1}.$$

By construction $N = a_0 + a_1\beta + \cdots + a_n\beta^n + s_{n+1}\beta^{n+1}$, hence the word $v = \omega(s_{n+1}) a_n \cdots a_0$ has the same numerical value in base $\beta$ as $w$.

Remark that $v$ is equal to the normal representation of $N$ if and only if it does not begin with zeroes. ■

Example 7.1.2. Figure 7.1 gives the right subsequential transducer realizing the conversion in base 2 from the alphabet $\{-1, 0, 1\}$ onto $\{0, 1\}$. The signed digit $(-1)$ is denoted by $\bar{1}$.

The two following results are a direct consequence of Lemma 7.1.1.

Proposition 7.1.3. *In base $\beta$, for every alphabet $C$ of positive integers containing $A$, the normalization restricted to the domain $C^* \setminus 0C^*$ is a right subsequential function.*

Removing the zeroes at the beginning of a word can be realized by a left sequential transducer, so the following property holds true for any alphabet.

Proposition 7.1.4. *In base $\beta$, for every alphabet $C$ containing $A$, the normalization on $C^*$ is computable by a finite transducer.*

Corollary 7.1.5. *In base $\beta$, addition and subtraction (with possibly zeroes ahead) are right subsequential functions.*

*Proof.* Take in Lemma 7.1.1 $C = \{0, \ldots, 2(\beta - 1)\}$ for addition, and $C = \{-(\beta - 1), \ldots, \beta - 1\}$ for subtraction. ■

One proves easily that multiplication by a fixed integer is a right subsequential function, and that division by a fixed integer is a left subsequential function, see the Problems Section. On the other hand, the following result shows that the power of functions computable by finite transducers is quite reduced.

PROPOSITION 7.1.6. *In base $\beta$, multiplication is not computable by a finite transducer.*

*Proof.* It is enough to show that the squaring function $\psi : A^* \longrightarrow A^*$ which maps $\langle N\rangle_\beta$ onto $\langle N^2\rangle_\beta$ is not computable by a finite transducer. Take for instance $\beta = 2$, and consider $\langle 2^n - 1\rangle_2 = 1^n$. Then $\psi(1^n) = \langle 2^{2n} - 2^{n+1} + 1\rangle_2 = 1^{n-1}0^n1$. Thus the image by $\psi$ of the set $\{1^n \mid n \geq 1\}$ which is recognizable by a finite automaton, is the set $\{1^{n-1}0^n1 \mid n \geq 1\}$ which is not recognizable, thus $\psi$ cannot be computed by a finite transducer. ∎

### 7.1.2. Representation of real numbers

Let $\beta \geq 2$ be an integer and set $A = \{0, \ldots, \beta - 1\}$. A *$\beta$-ary representation* of a nonnegative real number $x$ is an infinite sequence $(x_i)_{i\leq k}$ of $A^{\mathbb{N}}$ such that

$$x = \sum_{i\leq k} x_i\beta^i.$$

This representation is unique, and said to be *normal* if it does not end by $(\beta - 1)^\omega$, and if $x_k \neq 0$ when $x \geq 1$. It is traditionally denoted by

$$\langle x\rangle_\beta = x_k \cdots x_0 \cdot x_{-1}x_{-2} \cdots$$

If $x < 1$, then there exists some $i \geq 0$ such that $x < 1/\beta^i$. We then put $x_{-1}, \ldots, x_{-i+1} = 0$. The set of $\beta$-ary expansions of numbers $\geq 1$ is equal to $(A \setminus 0)(A^{\mathbb{N}} \setminus A^*(\beta - 1)^\omega)$, the one of numbers of $[0, 1]$ is $A^{\mathbb{N}} \setminus A^*(\beta - 1)^\omega$. The set $A^{\mathbb{N}}$ is the set of all $\beta$-ary representations (not necessarily normal).

The word $x_k \cdots x_0$ is the *integer part* of $x$ and the infinite word $x_{-1}x_{-2} \cdots$ is the *fractional part* of $x$. Note that the natural numbers are exactly those having a zero fractional part (compare with the representation of complex numbers in 7.4.1).

If $\langle x\rangle_\beta = x_k \cdots x_0 \cdot x_{-1}x_{-2} \cdots$, then $x/\beta^{k+1} < 1$, and by shifting we obtain that

$$\langle x/\beta^{k+1}\rangle_\beta = \cdot x_k \cdots x_0x_{-1}x_{-2} \cdots$$

thus from now on we consider only numbers from the interval $[0, 1]$. When $x \in [0, 1]$, we will change our notation for indices and denote $\langle x\rangle_\beta = (x_i)_{i\geq 1}$.

Let $C$ be a finite alphabet of integers, which can be positive or negative. The *numerical value* in base $\beta$ on $C^{\mathbb{N}}$ is the function

$$\pi_\beta : C^{\mathbb{N}} \longrightarrow \mathbb{R}$$

which maps a word $w = (c_i)_{i\geq 1}$ of $C^{\mathbb{N}}$ onto $\sum_{i\geq 1} c_i\beta^{-i}$. The *normalization* on $C^{\mathbb{N}}$ is the partial function

$$\nu_C : C^{\mathbb{N}} \longrightarrow A^{\mathbb{N}}$$

that maps a word $w = (c_i)_{i\geq 1}$ such that $x = \pi_\beta(w)$ belongs to $[0,1]$ onto its $\beta$-ary expansion $\langle x\rangle_\beta \in A^{\mathbb{N}} \setminus A^*(\beta-1)^\omega$.

Proposition 7.1.7. *For every alphabet $C$ containing $A$, the normalization on $C^{\mathbb{N}}$ is computable by a finite transducer.*

*Proof.* First we construct a finite transducer $\mathcal{B}$ where edges are the reverse of the edges of the transducer $\mathcal{A}$ defined in the proof of Lemma 7.1.1. Let $\mathcal{B} = (Q, F, 0, Q)$ with set of edges

$$F = \{t \xrightarrow{c/a} s \mid s \xrightarrow{c/a} t \in E\}.$$

Every state is terminal.

Let

$$s_0 \xrightarrow{c_1/a_1} s_1 \xrightarrow{c_2/a_2} s_2 \xrightarrow{c_3/a_3} \cdots \xrightarrow{c_n/a_n} s_n$$

be a path in $\mathcal{B}$ starting in $s_0 = 0$. Then

$$\frac{c_1}{\beta} + \cdots + \frac{c_n}{\beta^n} = \frac{a_1}{\beta} + \cdots + \frac{a_n}{\beta^n} - \frac{s_n}{\beta^n}.$$

Since $\mathcal{A}$ is sequential, the automaton $\mathcal{B}$ is unambiguous, that is, given an input word $(c_i)_{i\geq 1} \in C^{\mathbb{N}}$, there is a unique infinite path in $\mathcal{B}$ starting in 0 and labelled by $(c_i, a_i)_{i\geq 1}$ in $(C\times A)^{\mathbb{N}}$, and such that $\sum_{i\geq 1} c_i\beta^i = \sum_{i\geq 1} a_i\beta^i$, because for each $n$, $|s_n| < \gamma$.

To end the proof it remains to show that the function which, given a word in $A^{\mathbb{N}}$, transforms it into an equivalent word not ending by $(\beta-1)^\omega$, is computable by a finite transducer, and this is clear from the fact that $A^{\mathbb{N}} \times (A^{\mathbb{N}} \setminus A^*(\beta-1)^\omega)$ is a rational subset of $A^{\mathbb{N}} \times A^{\mathbb{N}}$ (see Chapter 1). ∎

Corollary 7.1.8. *Addition/subtraction, multiplication/division by a fixed integer of real numbers in base $\beta$ are computable by a finite transducer.*

Example 7.1.9. Figure 7.2 gives the finite transducer realizing non normalized addition (meaning that the result can end by the improper suffix $1^\omega$) of real numbers on the interval $[0,1]$ in base 2.

## 7.2. Beta-expansions

We now consider numeration systems where the base is a real number $\beta > 1$. Representations of real numbers in such systems were introduced by Rényi under the name of *$\beta$-expansions*. They arise from the orbits of a piecewise-monotone transformation of the unit interval $T_\beta : x \mapsto \beta x \pmod 1$, see below. Such transformations were extensively studied in ergodic theory and symbolic dynamics.

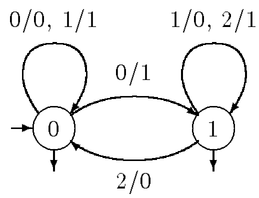


**Figure 7.2.** Finite transducer realizing non normalized addition of real numbers in base 2

### 7.2.1. Definitions

Let the base $\beta > 1$ be a real number. Let $x$ be a real number in the interval $[0, 1]$. A *representation in base* $\beta$ (or a $\beta$-representation) of $x$ is an infinite word $(x_i)_{i\geq 1}$ such that

$$x = \sum_{i\geq 1} x_i \beta^{-i}.$$

A particular $\beta$-representation — called the $\beta$*-expansion* — can be computed by the "greedy algorithm" : denote by $\lfloor y \rfloor$ and $\{y\}$ the integer part and the fractional part of a number $y$. Set $r_0 = x$ and let for $i \geq 1$, $x_i = \lfloor \beta r_{i-1} \rfloor$, $r_i = \{\beta r_{i-1}\}$. Then $x = \sum_{i\geq 1} x_i \beta^{-i}$.

The $\beta$-expansion of $x$ will be denoted by $d_\beta(x)$.

An equivalent definition is obtained by using the $\beta$*-transformation* of the unit interval which is the mapping

$$T_\beta : x \mapsto \beta x \,(\mathrm{mod}\ 1).$$

Then $d_\beta(x) = (x_i)_{i\geq 1}$ if and only if $x_i = \lfloor \beta T_\beta^{i-1}(x) \rfloor$.

Let $x$ be any real number greater than 1. There exists $k \in \mathbb{N}$ such that $\beta^k \leq x < \beta^{k+1}$. Hence $0 \leq x/\beta^{k+1} < 1$, thus it is enough to represent numbers from the interval $[0, 1]$, since by shifting we will get the representation of any positive real number.

Example 7.2.1. Let $\beta = (1 + \sqrt{5})/2$ be the golden ratio. For $x = 3 - \sqrt{5}$ we have $d_\beta(x) = 10010^\omega$.

If $\beta$ is not an integer, the digits $x_i$ obtained by the greedy algorithm are elements of the alphabet $A = \{0, \cdots, \lfloor \beta \rfloor\}$, called the *canonical alphabet*.

When $\beta$ is an integer, the $\beta$-expansion of a number $x$ of $[0, 1[$ is exactly the standard $\beta$-ary expansion, *i.e.* $d_\beta(x) = \langle x \rangle_\beta$, and the digits $x_i$ belong to $\{0, \cdots, \beta - 1\}$. However, for $x = 1$ there is a difference: $\langle 1 \rangle_\beta = 1\cdot$ but $d_\beta(1) = \cdot\beta$ . As we shall see later, the $\beta$-expansion of 1 plays a key role in this theory.

Another characterization of a $\beta$-expansion is the following one.

LEMMA 7.2.2. *An infinite sequence of nonnegative integers $(x_i)_{i\geq 1}$ is the $\beta$-expansion of a real number $x$ of $[0,1[$ (resp. of 1) if and only if for every $i \geq 1$ (resp. $i \geq 2$), $x_i\beta^{-i} + x_{i+1}\beta^{-i-1} + \cdots < \beta^{-i+1}$.*

*Proof.* Let $0 \leq x < 1$ and let $d_\beta(x) = (x_i)_{i\geq 1}$. By construction, for $i \geq 1$, $r_{i-1} = x_i/\beta + x_{i-1}/\beta^2 + \cdots < 1$, thus the result follows. ∎

A real number may have several $\beta$-representations. However, the $\beta$-expansion, obtained by the greedy algorithm, is characterized by the following property.

PROPOSITION 7.2.3. *The $\beta$-expansion of a real number $x$ of $[0,1]$ is the greatest of all the $\beta$-representations of $x$ with respect to the lexicographic order.*

*Proof.* Let $d_\beta(x) = (x_i)_{i\geq 1}$ and let $(s_i)_{i\geq 1}$ be another $\beta$-representation of $x$. Suppose that $(x_i)_{i\geq 1} < (s_i)_{i\geq 1}$, then there exists $k \geq 1$ such that $x_k < s_k$ and $x_1 \cdots x_{k-1} = s_1 \cdots s_{k-1}$. From $\sum_{i\geq k} x_i\beta^{-i} = \sum_{i\geq k} s_i\beta^{-i}$ one gets $\sum_{i\geq k+1} x_i\beta^{-i} \geq \beta^{-k} + \sum_{i\geq k+1} s_i\beta^{-i}$, which is impossible since by Lemma 7.2.2 $\sum_{i\geq k+1} x_i\beta^{-i} < \beta^{-k}$. ∎

EXAMPLE 7.2.1 (*continued*). Let $\beta$ be the golden ratio. The $\beta$-expansion of $x = 3 - \sqrt{5}$ is equal to $10010^\omega$. Different $\beta$-representations of $x$ are $01110^\omega$, or $100(01)^\omega$ for instance.

As in the usual numeration systems, the order between real numbers is given by the lexicographic order on $\beta$-expansions.

PROPOSITION 7.2.4. *Let $x$ and $y$ be two real numbers from $[0,1]$. Then $x < y$ if and only if $d_\beta(x) < d_\beta(y)$.*

*Proof.* Let $d_\beta(x) = (x_i)_{i\geq 1}$ and let $d_\beta(y) = (y_i)_{i\geq 1}$, and suppose that $d_\beta(x) < d_\beta(y)$. There exists $k \geq 1$ such that $x_k < y_k$ and $x_1 \cdots x_{k-1} = y_1 \cdots y_{k-1}$. Hence $x \leq y_1\beta^{-1} + \cdots + y_{k-1}\beta^{-k+1} + (y_k - 1)\beta^{-k} + x_{k+1}\beta^{-k-1} + x_{k+2}\beta^{-k-2} + \cdots < y$ since $x_{k+1}\beta^{-k-1} + x_{k+2}\beta^{-k-2} + \cdots < \beta^{-k}$. The converse is immediate. ∎

If a representation ends in infinitely many zeros, like $v0^\omega$, the ending zeros are omitted and the representation is said to be *finite*. Remark that the $\beta$-expansion of $x \in [0,1]$ is finite if and only if $T_\beta^i(x) = 0$ for some $i$, and it is eventually periodic if and only if the set $\{T_\beta^i(x) \mid i \geq 1\}$ is finite. Numbers $\beta$ such that $d_\beta(1)$ is eventually periodic are called *$\beta$-numbers* and those such that $d_\beta(1)$ is finite are called *simple* $\beta$-numbers.

REMARK 7.2.5. The $\beta$-expansion of 1 is never purely periodic.

Indeed, suppose that $d_\beta(1)$ is purely periodic, $d_\beta(1) = (a_1 \cdots a_n)^\omega$, with $n$ minimal, $a_i \in A$. Then $1 = a_1\beta^{-1} + \cdots + a_n\beta^{-n} + \beta^{-n}$, which means that $a_1 \cdots a_{n-1}(a_n + 1)$ is a $\beta$-representation of 1, and $a_1 \cdots a_{n-1}(a_n + 1) > d_\beta(1)$, which is impossible.

EXAMPLE 7.2.6. 1. Let $\beta$ be the golden ratio $(1+\sqrt{5})/2$. The expansion of 1 is finite, equal to $d_\beta(1) = 11$.
2. Let $\beta = (3+\sqrt{5})/2$. The expansion of 1 is eventually periodic, equal to $d_\beta(1) = 21^\omega$.
3. Let $\beta = 3/2$. Then $d_\beta(1) = 101000001\cdots$. We shall see later that it is aperiodic.

### 7.2.2. The $\beta$-shift

Recall that the set $A^{\mathbb{N}}$ is endowed with the lexicographic order, the product topology, and the (one-sided) shift $\sigma$, defined by $\sigma((x_i)_{i\geq 1}) = (x_{i+1})_{i\geq 1}$. Denote by $D_\beta$ the set of $\beta$-expansions of numbers of $[0,1[$. It is a shift-invariant subset of $A^{\mathbb{N}}$. The *$\beta$-shift* $S_\beta$ is the closure of $D_\beta$ and it is a subshift of $A^{\mathbb{N}}$. When $\beta$ is an integer, $S_\beta$ is the full $\beta$-shift $A^{\mathbb{N}}$.

The greedy algorithm computing the $\beta$-expansion can be rephrased as follows.

LEMMA 7.2.7. *The identity*

$$d_\beta \circ T_\beta = \sigma \circ d_\beta$$

*holds on the interval* $[0,1]$.

*Proof.* Let $x \in [0,1]$, and let $d_\beta(x) = (x_i)_{i\geq 1}$. Then $T_\beta(x) = \sum_{i\geq 1} x_i \beta^{-i}$, and the result follows. ∎

In the case where the $\beta$-expansion of 1 is finite, there is a special representation playing an important role. Let us introduce the following notation. Let $d_\beta(1) = (t_i)_{i\geq 1}$ and set $d^*_\beta(1) = d_\beta(1)$ if $d_\beta(1)$ is infinite and $d^*_\beta(1) = (t_1\cdots t_{m-1}(t_m-1))^\omega$ if $d_\beta(1) = t_1\cdots t_{m-1}t_m$ is finite.

When $\beta$ is an integer, $\beta$-representations ending by the infinite word $d^*_\beta(1)$ are the "improper" representations.

EXAMPLE 7.2.8. Let $\beta = 2$, then $d_\beta(1) = 2$ and $d^*_\beta(1) = 1^\omega$.
For $\beta = (1+\sqrt{5})/2$, $d_\beta(1) = 11$ and $d^*_\beta(1) = (10)^\omega$.

The set $D_\beta$ is characterized by the expansion of 1, as shown by the following result below. Notice that the sets of finite factors of $D_\beta$ and of $S_\beta$ are the same, and that $d^*_\beta(1)$ is the supremum of $S_\beta$, but that, in case $d_\beta(1)$ is finite, $d_\beta(1)$ is not an element of $S_\beta$.

THEOREM 7.2.9. *Let $\beta > 1$ be a real number, and let $s$ be an infinite sequence of nonnegative integers. The sequence $s$ belongs to $D_\beta$ if and only if for all $p \geq 0$*

$$\sigma^p(s) < d^*_\beta(1)$$

*and $s$ belongs to $S_\beta$ if and only if for all $p \geq 0$*

$$\sigma^p(s) \leq d^*_\beta(1).$$

*Proof.* First suppose that $s = (s_i)_{i\geq 1}$ belongs to $D_\beta$, then there exists $x$ in $[0,1[$ such that $s = d_\beta(x)$. By Lemma 7.2.7, for every $p \geq 0$, $\sigma^p \circ d_\beta(x) = d_\beta \circ T_\beta^p(x)$. Since $T_\beta^p(x) < 1$ and $d_\beta$ is a strictly increasing function (Proposition 7.2.4), $\sigma^p \circ d_\beta(x) = \sigma^p(s) < d_\beta(1)$.
In the case where $d_\beta(1) = t_1 \cdots t_m$ is finite, suppose there exists a $p \geq 0$ such that $\sigma^p(s) \geq d_\beta^*(1)$. Since $\sigma^p(s) < d_\beta(1)$, we get $s_{p+1} = t_1, \ldots, s_{p+m-1} = t_{m-1}$, $s_{p+m} = t_m - 1$. Iterating this process, we see that $\sigma^p(s) = d_\beta^*(1)$, which does not belong to $D_\beta$, a contradiction.

Conversely, let $d_\beta^*(1) = (d_i)_{i\geq 1}$ and suppose that for all $p \geq 0$, $\sigma^p(s) < d_\beta^*(1)$. By induction, let us show that for all $r \geq 1$, for all $i \geq 0$,

$$s_{p+1} \cdots s_{p+r} < d_{i+1} \cdots d_{i+r} \Rightarrow \frac{s_{p+1}}{\beta} + \cdots + \frac{s_{p+r}}{\beta^r} < \frac{d_{i+1}}{\beta} + \cdots + \frac{d_{i+r}}{\beta^r}.$$

This is obviously satisfied for $r = 1$.
Suppose that $s_{p+1} \cdots s_{p+r+1} < d_{i+1} \cdots d_{i+r+1}$.
First assume that $s_{p+1} = d_{i+1}$, then $s_{p+2} \cdots s_{p+r+1} < d_{i+2} \cdots d_{i+r+1}$. By induction hypothesis,

$$\frac{s_{p+2}}{\beta^2} + \cdots + \frac{s_{p+r+1}}{\beta^{r+1}} < \frac{d_{i+2}}{\beta^2} + \cdots + \frac{d_{i+r+1}}{\beta^{r+1}}$$

and the result follows.
Next, suppose that $s_{p+1} < d_{i+1}$. Since for all $p \geq 0$, $\sigma^p(s) < d_\beta^*(1)$ then $s_{p+2} \cdots s_{p+r+1} \leq d_1 \cdots d_r$, thus

$$\frac{s_{p+1}}{\beta} + \cdots + \frac{s_{p+r+1}}{\beta^{r+1}} \leq \frac{d_{i+1} - 1}{\beta} + \frac{d_1}{\beta^2} + \cdots + \frac{d_r}{\beta^{r+1}} < \frac{d_{i+1}}{\beta}$$

since $d_1/\beta^2 + \cdots + d_r/\beta^{r+1} < 1/\beta$.

Thus for all $p \geq 0$, for all $i \geq 0$,

$$\sum_{r\geq 1} s_{p+r}\beta^{-r} \leq \sum_{r\geq 1} d_{i+r}\beta^{-r}.$$

In particular for $i = 1$, $\sum_{r\geq 1} s_{p+r}\beta^{-r} \leq \sum_{r\geq 1} d_{r+1}\beta^{-r} < 1$ if $\beta$ is not an integer, and the result follows by Lemma 7.2.2.

If $\beta$ is an integer then $d_\beta^*(1) = (\beta - 1)^\omega$. If for all $p \geq 0$, $\sigma^p(s) < d_\beta^*(1)$, then every letter of $s$ is smaller than or equal to $\beta - 1$ and $s$ does not end by $(\beta - 1)^\omega$, therefore $s$ belongs to $D_\beta$.

For the $\beta$-shift, we have the following situation. A sequence $s$ belongs to $\overline{D_\beta}$ if and only if for each $n \geq 1$ there exists a word $v^{(n)}$ of $D_\beta$ such that $s_1 \cdots s_n$ is a prefix of $v^{(n)}$. Hence, $s$ belongs to $S_\beta$ if and only if for every $p \geq 0$, for every $n \geq 1$, $\sigma^p(s_1 \cdots s_n 0^\omega) < d_\beta^*(1)$, or equivalently if $\sigma^p(s) \leq d_\beta^*(1)$. ∎

From this result follows the following characterization : a sequence is the $\beta$-expansion of 1 for a certain number $\beta$ if and only if it is greater than all its shifted sequences.

Corollary 7.2.10. *Let $s = (s_i)_{i\geq 1}$ be a sequence of nonnegative integers with $s_1 \geq 1$ and for $i \geq 2$, $s_i \leq s_1$, and which is different from $10^\omega$. Then there exists a unique real number $\beta > 0$ such that $\sum_{i\geq 1} s_i\beta^{-i} = 1$. Furthermore, $s$ is the $\beta$-expansion of 1 if and only if for every $n \geq 1$, $\sigma^n(s) < s$.*

*Proof.* Let $f$ be the formal series defined by $f(z) = \sum_{i\geq 1} s_i z^i$, and denote by $\rho$ its radius of convergence. Since $0 \leq s_i \leq s_1$, we get $\rho \geq 1/(s_1+1)$. Since for $0 < z < \rho$ the function $f$ is continuous and increasing, and since $f(0) = 0$ and $f(z) > 1$ for $z$ sufficient close to $\rho$, it follows that the equation $f(z) = 1$ has a unique solution. If $\beta > 1$ exists such that $f(1/\beta) = 1$, we get that $s_1/\beta \leq f(1/\beta) \leq s_1/(\beta - 1)$, thus $\beta$ must be between $s_1$ and $s_1 + 1$. On the other hand, $f(1/(s_1 + 1)) \leq s_1/s_1 = 1$. If $s_1 \geq 2$, $f(1/s_1) \geq 1$. If $s_1 = 1$ and if the $s_i$'s are eventually 0, then $f(1/s_1) \geq 1$, otherwise $\lim_{z\to 1} f(z) = +\infty$. Thus in any case there exists a real $\beta \in [s_1, s_1 + 1]$ such that $f(1/\beta) = 1$.

Now we make the following hypothesis (H) : for all $n \geq 1$, $\sigma^n(s) < s$. Suppose that the $\beta$-expansion of 1 is $d_\beta(1) = t \neq s$. Since $s$ is a $\beta$-representation of 1, $s < t$. Hence, for each $n \geq 1$, $\sigma^n(s) < s < d_\beta(1)$. If $d_\beta(1)$ is infinite, by Theorem 7.2.9, $s$ belongs to $D_\beta$, a contradiction.

If $d_\beta(1)$ is finite, say $d_\beta(1) = t_1 \cdots t_m$, either $s < d^*_\beta(1)$, and as above we get that $s$ is in $D_\beta$, or $d^*_\beta(1) \leq s < d_\beta(1)$. In fact, $s$ cannot be purely periodic because of hypothesis (H), thus it is different from $d^*_\beta(1)$. Thus $s$ is necessarily of the form $(t_1 \cdots t_{m-1}(t_m - 1))^k t_1 \cdots t_m$ for some $k \geq 1$. So $s_{km+1} = t_1, \ldots, s_{km+m} = t_m$, and $\sigma^{km}(s) > s$ because $s_m = t_m - 1$, contradicting hypothesis (H). Hence the $\beta$-expansion of 1 is $s$.

Conversely, suppose that $s = d_\beta(1)$ for some $\beta > 1$. From Theorem 7.2.9, for every $n \geq 1$, $\sigma^n(s) < d^*_\beta(1)$. If $d_\beta(1)$ is infinite, $d_\beta(1) = d^*_\beta(1)$. If $d_\beta(1)$ is finite, $d^*_\beta(1) < d_\beta(1)$. ∎

Let us recall some definitions on symbolic dynamical systems or subshifts (see Chapter 1 Section ??). Let $S \subseteq A^{\mathbb{N}}$ be a subshift, and let $I(S) = A^+ \setminus F(S)$ be the set of factors avoided by $S$. Denote by $X(S)$ the set of words of $I(S)$ which have no proper factor in $I(S)$. The subshift $S$ is of *finite type* iff the set $X(S)$ is finite. The subshift $S$ is *sofic* iff $X(S)$ is a rational set. It is equivalent to say that $F(S)$ is recognized by a finite automaton. The subshift $S$ is said to be *coded* if there exists a prefix code $Y \subset A^*$ such that $F(S) = F(Y^*)$, or equivalently if $S$ is the closure of $Y^\omega$.

To the $\beta$-shift a prefix code $Y = Y_\beta$ is associated as follows. It is the set of words which, for each length, are strictly smaller than the prefix of $d_\beta(1)$ of same length, more precisely: if $d_\beta(1) = (t_i)_{i\geq 1}$ is infinite, set $Y = \{t_1 \cdots t_{n-1}a \mid 0 \leq a < t_n,\ n \geq 1\}$, with the convention that if $n = 1$, $t_1 \cdots t_{n-1} = \varepsilon$. If $d_\beta(1) = t_1 \cdots t_m$, let $Y = \{t_1 \cdots t_{n-1}a \mid 0 \leq a < t_n,\ 1 \leq n \leq m\}$.

Proposition 7.2.11. *The $\beta$-shift $S_\beta$ is coded by the code $Y$.*

*Proof.* First if $d_\beta(1) = (t_i)_{i\geq 1}$ is infinite, let us show that $D_\beta = Y^\omega$. Let $s \in D_\beta$.

By Theorem 7.2.9, $s < d_\beta(1)$, thus can be written as $s = t_1 \cdots t_{n_1-1} a_{n_1} v_1$, with $a_{n_1} < t_{n_1}$ and $v_1 < d_\beta(1)$. Iterating this process, we see that $s \in Y^\omega$. Conversely, let $s = u_1 u_2 \cdots \in Y^\omega$, with $u_i = t_1 \cdots t_{n_i-1} a_{n_i}$, $a_{n_i} < t_{n_i}$. Then $s < d_\beta(1)$. For each $p \geq 0$, $\sigma^p(s)$ begins with a word of the form $t_{j_p} t_{j_p+1} \cdots t_{j_p+r-1} b_{j_p+r}$ with $b_{j_p+r} < t_{j_p+r}$, thus $\sigma^p(s) < \sigma^{j_p-1}(d_\beta(1)) < d_\beta(1)$.

Next, if $d_\beta(1) = t_1 \cdots t_m$, is finite, we claim that $Y^\omega = S_\beta$. First, let $s \in S_\beta$. By Theorem 7.2.9, $s \leq d_\beta^*(1)$, thus $s = t_1 \cdots t_{n_1-1} a_{n_1} v_1$, with $n_1 \leq m$, $a_{n_1} < t_{n_1}$ and $v_1 \leq d_\beta^*(1)$. Iterating the process we get $s \in S_\beta$. Conversely, let $s \in Y^\omega$, $s = u_1 u_2 \cdots$ with $u_i = t_1 \cdots t_{n_i-1} a_{n_i}$, $n_i \leq m$. As above, one gets that, for each $p \geq 0$, $\sigma^p(s) < d_\beta^*(1)$. ∎

We now compute the topological entropy of the $\beta$-shift

$$h(S_\beta) = -\log(\rho_{F(S_\beta)})$$

(see **??** for definitions and notations). In the case where the $\beta$-shift is sofic, by Theorem **??** the entropy $h(S_\beta)$ can be shown to be equal to $\log \beta$. We show below that the same result holds true for any kind of $\beta$-shift.

Proposition 7.2.12. *The topological entropy of the $\beta$-shift is equal to $\log \beta$.*

*Proof.* For $n \geq 1$, the number of words of length $n$ of $Y$ is clearly equal to $t_n$, thus the generating series of $Y$ is equal to

$$f_Y(z) = \sum_{n \geq 1} t_n z^n.$$

By Corollary 7.2.10, $\beta^{-1}$ is the unique positive solution of $f_Y(z) = 1$. Since $Y$ is a code, by Lemma **??** $\rho_{Y^*} = \beta^{-1}$. It is thus enough to show that $\rho_{Y^*} = \rho_{F(S_\beta)}$.

Let $p_n$ be the number of factors of length $n$ of the elements of $S_\beta$ and let

$$f_{F(S_\beta)} = \sum_{n \geq 0} p_n z^n.$$

Let $c_n$ be the number of words of length $n$ of $Y^*$, and let

$$f_{F(Y^*)} = \sum_{n \geq 0} c_n z^n.$$

Since any word of $Y^*$ is in $F(S_\beta)$, we have $c_n \leq p_n$. On the other hand, let $w$ be a word of length $n$ in $F(S_\beta)$. By Proposition 7.2.11, $w$ can be uniquely written as $w = u_i t_1 \cdots t_i$, where $u_i \in Y^*$, $|u_i| = n - i$, and $0 \leq i \leq n$. Thus $p_n = c_n + \cdots + c_0$. Hence the series $f_{F(S_\beta)}$ and $f_{Y^*}$ have the same radius of convergence, and the result is proved. ∎

We now show that the nature of the subshift as a symbolic dynamical system is entirely determined by the $\beta$-expansion of 1.

THEOREM 7.2.13. *The $\beta$-shift $S_\beta$ is sofic if and only if $d_\beta(1)$ is eventually periodic.*

*Proof.* Suppose that $d_\beta(1)$ is infinite eventually periodic

$$d_\beta(1) = t_1 \cdots t_N (t_{N+1} \cdots t_{N+p})^\omega$$

with $N$ and $p$ minimal. We use the classical construction of minimal finite automata by right congruent classes (see Chapter 1). Let $F(D_\beta)$ be the set of finite factors of $D_\beta$. We construct an automaton $\mathcal{A}_\beta$ with $N+p$ states $q_1, \ldots,$ $q_{N+p}$, where $q_i$, $i \geq 2$, represents the right class $[t_1 \cdots t_{i-1}]_{F(D_\beta)}$ and $q_1$ stands for $[\varepsilon]_{F(D_\beta)}$. For each $i$, $1 \leq i < N+p$, there is an edge labelled $t_i$ from $q_i$ to $q_{i+1}$. There is an edge labelled $t_{N+p}$ from $q_{N+p}$ to $q_{N+1}$. For $1 \leq i \leq N+p$, there are edges labelled by $0, 1, \ldots, t_i - 1$ from $q_i$ to $q_1$. Let $q_1$ be the only initial state, and all states be terminal. That $F(D_\beta)$ is precisely the set recognized by the automaton $\mathcal{A}_\beta$ follows from Theorem 7.2.9. Remark that, when the $\beta$-expansion of 1 happens to be finite, say $d_\beta(1) = t_1 \cdots t_m$, the same construction applies with $N = m$, $p = 0$ and all edges from $q_m$ (labelled by $0, 1, \ldots, t_m - 1$) leading to $q_1$.

Suppose now that $d_\beta(1) = (t_i)_{i \geq 1}$ is not eventually periodic nor finite. There exists an infinite sequence of indexes $i_1 < i_2 < i_3 < \cdots$ such that the sequences $t_{i_k} t_{i_k+1} t_{i_k+2} \cdots$ be all different for all $k \geq 1$. Thus for all pairs $(i_j, i_\ell)$, $j, \ell \geq 1$, there exists $p \geq 0$ such that, for instance, $t_{i_j+p} < t_{i_\ell+p}$ and $t_{i_j} \cdots t_{i_j+p-1} = t_{i_\ell} \cdots t_{i_\ell+p-1} = w$ (with the convention that, when $p = 0$, $w = \varepsilon$). We have that $t_1 \cdots t_{i_j-1} w t_{i_j+p} \in F(D_\beta)$, $t_1 \cdots t_{i_\ell-1} w t_{i_\ell+p} \in F(D_\beta)$, $t_1 \cdots t_{i_\ell-1} w t_{i_j+p} \in F(D_\beta)$, but $t_1 \cdots t_{i_j-1} w t_{i_\ell+p}$ does not belong to $F(D_\beta)$. Hence $t_1 \cdots t_{i_j}$ and $t_1 \cdots t_{i_\ell}$ are not right congruent modulo $F(D_\beta)$. The number of right congruence classes is thus infinite, and $F(D_\beta)$ is not recognizable by a finite automaton.

■

EXAMPLE 7.2.14. For $\beta = (3+\sqrt{5})/2$, $d_\beta(1) = 21^\omega$, and the $\beta$-shift is sofic.

We have a similar result when the $\beta$-expansion of 1 is finite.

THEOREM 7.2.15. *The $\beta$-shift $S_\beta$ is of finite type if and only if $d_\beta(1)$ is finite.*

*Proof.* Let us suppose that $d_\beta(1) = t_1 \cdots t_m$ is finite and let

$$Z = \bigcup_{2 \leq i \leq m-1} \{u \in A^i \mid u > t_1 \cdots t_i\} \cup \{u \in A^m \mid u \geq t_1 \cdots t_m\}.$$

Clearly $Z \subseteq A^+ \setminus F(S_\beta)$. The set $X(S_\beta)$ of words forbidden in $S_\beta$ which are minimal for the factor order is a subset of $Z$. Since $Z$ is finite, $X(S_\beta)$ is finite, and thus $S_\beta$ is of finite type.

Conversely, suppose that the $\beta$-shift is of finite type. It is thus sofic, and by Theorem 7.2.13, $d_\beta(1)$ is eventually periodic. Suppose that $d_\beta(1)$ is not finite, $d_\beta(1) = t_1 \cdots t_N(t_{N+1} \cdots t_{N+p})^\omega$ with $N \geq 1$ and $p \geq 1$ minimal, and $t_{N+1} \cdots t_{N+p} \neq 0^p$. Let

$$\begin{aligned} Z = \{\, & t_1 \cdots t_{j-1}(t_j + h_j) \mid 2 \leq j \leq N,\ 1 \leq h_j \leq t_1 - t_j \} \\ \cup \{\, & t_1 \cdots t_N(t_{N+1} \cdots t_{N+p})^k t_{N+1} \cdots t_{N+j-1}(t_{N+j} + h_{N+j}) \\ & \mid k \geq 0,\ 1 \leq j \leq p,\ 1 \leq h_{N+j} \leq t_1 - t_{N+j} \}. \end{aligned}$$

Clearly $Z \subseteq A^+ \setminus F(S_\beta)$.
*Case 1.* Suppose there exists $1 \leq j \leq p$ such that $t_j > t_{N+j}$ and $t_1 = t_{N+1}, \ldots, t_{j-1} = t_{N+j-1}$. For $k \geq 0$ fixed, let $w^{(k)} = t_1 \cdots t_N(t_{N+1} \cdots t_{N+p})^k t_1 \cdots t_j \in Z$. We have $t_1 \cdots t_N(t_{N+1} \cdots t_{N+p})^k t_{N+1} \cdots t_{N+j-1} \in F(S_\beta)$. On the other hand, for $n \geq 2$, $t_n \cdots t_N(t_{N+1} \cdots t_{N+p})^k$ is strictly smaller in the lexicographic order than the prefix of $d_\beta(1)$ of same length (the inequality is strict, since the $t_i$'s are not all equal for $1 \leq i \leq N+p$), thus $t_n \cdots t_N(t_{N+1} \cdots t_{N+p})^k\ t_1 \cdots t_j \in F(S_\beta)$. Hence any strict factor of $w^{(k)}$ is in $F(S_\beta)$. Therefore for any $k \geq 0$, $w^{(k)} \in X(S_\beta)$, and $X(S_\beta)$ is thus infinite: the $\beta$-shift is not of finite type.
*Case 2.* No such $j$ exists, then $d_\beta(1) = (t_1 \cdots t_N)^\omega$, which is impossible by Remark 7.2.5. ■

Example 7.2.16. For $\beta = (1+\sqrt{5})/2$, the $\beta$-shift is of finite type, it is the golden mean shift described in Example ??.

### 7.2.3. Classes of numbers

Recall that an *algebraic integer* is a root of a monic polynomial with integral coefficients. An algebraic integer $\beta > 1$ is called a *Pisot number* if all its Galois conjugates have modulus less than one. It is a *Salem number* if all its conjugates have modulus $\leq 1$ and at least one conjugate has modulus one. It is a *Perron number* if all its conjugates have modulus less than $\beta$.

Example 7.2.17. 1. Every integer is a Pisot number. The golden ratio $(1+\sqrt{5})/2$ and its square $(3+\sqrt{5})/2$ are Pisot numbers, with minimal polynomial respectively $X^2 - X - 1$ and $X^2 - 3X + 1$.
2. A rational number which is not an integer is never an algebraic integer.
3. $(5+\sqrt{5})/2$ is a Perron number which is neither Pisot nor Salem.

The most important result linking $\beta$-shifts and numbers is the following one.

Theorem 7.2.18. *If $\beta$ is a Pisot number then the $\beta$-shift $S_\beta$ is sofic.*

This result is a consequence of a more general result on $\beta$-expansions of numbers of the field $\mathbb{Q}(\beta)$ when $\beta$ is a Pisot number. It is a partial generalization of the well known fact that, when $\beta$ is an integer, numbers having an eventually periodic $\beta$-expansion are the rational numbers of $[0,1]$ (see Problems Section).

Proposition 7.2.19. *If $\beta$ is a Pisot number then every number of $\mathbb{Q}(\beta) \cap [0,1]$ has an eventually periodic $\beta$-expansion.*

*Proof.* Let $P(X) = X^d - a_1X^{d-1} - \cdots - a_d$ be the minimal polynomial of $\beta = \beta_1$ and denote by $\beta_2, \ldots, \beta_d$ the conjugates of $\beta$. Let $x$ be arbitrarily fixed in $\mathbb{Q}(\beta) \cap [0,1]$. It can be expressed as

$$x = q^{-1} \sum_{i=0}^{d-1} p_i \beta^i$$

with $q$ and $p_i$ in $\mathbb{Z}$, $q > 0$ as small as possible in order to have uniqueness.

Let $(x_k)_{k \geq 1}$ be the $\beta$-expansion of $x$, and denote by

$$r_n = r_n^{(1)} = r_n(x) = \frac{x_{n+1}}{\beta} + \frac{x_{n+2}}{\beta^2} + \cdots = \beta^n (x - \sum_{k=1}^{n} x_k \beta^{-k}) = T_\beta^n(x) < 1.$$

For $2 \leq j \leq d$, let

$$r_n^{(j)} = r_n^{(j)}(x) = \beta_j^n (q^{-1} \sum_{i=0}^{d-1} p_i \beta_j^i - \sum_{k=1}^{n} x_k \beta_j^{-k}).$$

Let $\eta = \max_{2 \leq j \leq d} |\beta_j| < 1$ since $\beta$ is a Pisot number. Since $x_k \leq \lfloor \beta \rfloor$ we get

$$|r_n^{(j)}| \leq q^{-1} \sum_{i=0}^{d-1} |p_i| \eta^{n+i} + \lfloor \beta \rfloor \sum_{k=0}^{n-1} \eta^k$$

and, since $\eta < 1$, $\max_{1 \leq j \leq d} \sup_n |r_n^{(j)}| < +\infty$.

We need a technical result. Set $R_n = (r_n^{(1)}, \cdots, r_n^{(d)})$ and let $B$ be the matrix $B = (\beta_j^{-i})_{1 \leq i,j \leq d}$.

LEMMA 7.2.20. *Let $x = q^{-1} \sum_{i=0}^{d-1} p_i \beta^i$. For every $n \geq 0$, there exists a unique $d$-uple $Z_n = (z_n^{(1)}, \cdots, z_n^{(d)})$ in $\mathbb{Z}^d$ such that $R_n = q^{-1} Z_n B$.*

*Proof.* By induction on $n$. First, $r_1 = r_1^{(1)} = \beta x - x_1$, thus

$$r_1 = q^{-1} (\sum_{i=0}^{d-1} p_i \beta^{i+1} - q x_1) = q^{-1} (\frac{z_1^{(1)}}{\beta} + \cdots + \frac{z_1^{(d)}}{\beta^d})$$

using the fact that $\beta^d = a_1 \beta^{d-1} + \cdots + a_d$, $a_j \in \mathbb{Z}$. Now, $r_{n+1} = r_{n+1}^{(1)} = \beta r_n - x_{n+1}$, hence

$$r_{n+1} = q^{-1} (z_n^{(1)} + \frac{z_n^{(2)}}{\beta} + \cdots + \frac{z_n^{(d)}}{\beta^{d-1}} - q x_{n+1}) = q^{-1} (\frac{z_{n+1}^{(1)}}{\beta} + \cdots + \frac{z_{n+1}^{(d)}}{\beta^d})$$

since $z_n^{(1)} - q x_{n+1} \in \mathbb{Z}$.

Thus

$$r_n = r_n^{(1)} = \beta^n (q^{-1} \sum_{i=0}^{d-1} p_i \beta^i - \sum_{k=1}^{n} x_k \beta^{-k}) = q^{-1} \sum_{k=1}^{d} z_n^{(k)} \beta^{-k}.$$

Since the latter equation has integral coefficients and is satisfied by $\beta$, it is also satisfied by each conjugate $\beta_j$, $2 \le j \le d$,

$$r_n^{(j)} = \beta_j^n (q^{-1} \sum_{i=0}^{d-1} p_i \beta_j^i - \sum_{k=1}^{n} x_k \beta_j^{-k}) = q^{-1} \sum_{k=1}^{d} z_n^{(k)} \beta_j^{-k}. \qquad \blacksquare$$

We resume the proof of Proposition 7.2.19. Let $V_n = qR_n$. The $(V_n)_{n \ge 1}$ have bounded norm, since $\max_{1 \le j \le d} \sup_n |r_n^{(j)}| < +\infty$. As the matrix $B$ is invertible, for every $n \ge 1$,

$$||Z_n|| = ||(z_n^{(1)}, \cdots, z_n^{(d)})|| = \max_{1 \le j \le d} |z_n^{(j)}| < +\infty$$

so there exist $p$ and $m \ge 1$ such that $Z_{m+p} = Z_m$, hence $r_{m+p} = r_m$ and the $\beta$-expansion of $x$ is eventually periodic. $\blacksquare$

On the other hand, there is a gap between Pisot and Perron numbers as shown be the following result.

Proposition 7.2.21. *If $S_\beta$ is sofic then $\beta$ is a Perron number.*

*Proof.* With the automaton $\mathcal{A}_\beta$ defined in the proof of Theorem 7.2.13 one associates a matrix $M = M_\beta$ by taking for $M[i,j]$ the number of edges from state $q_i$ to state $q_j$, that is, if $d_\beta(1) = t_1 \cdots t_N (t_{N+1} \cdots t_{N+p})^\omega$,

$$\begin{aligned} M[i,1] &= t_i \\ M[i,i+1] &= 1 \text{ for } i \ne N+p \\ M[N+p, N+1] &= 1 \end{aligned}$$

and other entries are equal to 0.
*Claim* 1. The matrix $M$ is primitive: $M^{N+p} > 0$, since $M^{N+p}[i,j]$ is equal to the number of paths of length $N+p$ from $q_i$ to $q_j$ in the strongly connected automaton $\mathcal{A}_\beta$.
*Claim* 2. The characteristic polynomial of $M$ is equal to

$$K(X) = X^{N+p} - \sum_{i=1}^{N+p} t_i X^{N+p-i} - X^N + \sum_{i=1}^{N} t_i X^{N-i}$$

and $\beta$ is one of its roots: it can be checked by a straightforward computation.

When $d_\beta(1) = t_1 \cdots t_m$ is finite, the matrix associated with the automaton is simpler, it is the companion matrix of the polynomial $K(X) = X^m - t_1 X^{m-1} - \cdots - t_m$, which is primitive, since $M^m > 0$.

Since $\beta > 1$ is an eigenvalue of a primitive matrix, by the theorem of Perron-Frobenius, $\beta$ is strictly greater in modulus than its algebraic conjugates. $\blacksquare$

Thus when $\beta$ is a non-integral rational number (for instance 3/2), the $\beta$-shift $S_\beta$ cannot be sofic.

EXAMPLE 7.2.22. There are Perron numbers which are neither Pisot nor Salem numbers and such that the $\beta$-shift is of finite type: for instance the root $\beta \sim 3.616$ of $X^4 - 3X^3 - 2X^2 - 3$ satisfies $d_\beta(1) = 3203$, and $\beta$ has a conjugate $\gamma \sim -1.096$.

REMARK 7.2.23. If $\beta$ is a Perron number with a real conjugate $> 1$, then $d_\beta(1)$ cannot be eventually periodic.

In fact, suppose that $d_\beta(1) = t_1 \cdots t_N(t_{N+1} \cdots t_{N+p})^\omega$, and that $\beta$ has a conjugate $\gamma > 1$. Since $\beta$ is a zero of the polynomial $K(X)$ of $\mathbb{Z}[X]$, $\gamma$ is also a zero of this polynomial. Thus $d_\gamma(1) = d_\beta(1)$, and by Corollary 7.2.10, $\gamma = \beta$.
For instance the quadratic Perron number $\beta = (5 + \sqrt{5})/2$ has a real conjugate $> 1$, and thus $S_\beta$ is not sofic.

## 7.3. $U$-representations

We now consider another generalization of the notion of numeration system, which only allow to represent the natural numbers. The base is replaced by an infinite sequence of integers. The basic example is the well-known Fibonacci numeration system.

### 7.3.1. Definitions

Let $U = (u_n)_{n \geq 0}$ be a strictly increasing sequence of integers with $u_0 = 1$. A *representation in the system $U$* — or a *$U$-representation* — of a nonnegative integer $N$ is a finite sequence of integers $(d_i)_{k \geq i \geq 0}$ such that

$$N = \sum_{i=0}^{k} d_i u_i.$$

Such a representation will be written $d_k \cdots d_0$, most significant digit first.

Among all possible $U$-representations of a given nonnegative integer $N$ one is distinguished and called the *normal $U$-representation* of $N$ : it is sometimes called the *greedy* representation, since it can be obtained by the following greedy algorithm : given integers $m$ and $p$ let us denote by $q(m, p)$ and $r(m, p)$ the quotient and the remainder of the Euclidean division of $m$ by $p$. Let $k \geq 0$ such that $u_k \leq N < u_{k+1}$ and let $d_k = q(N, u_k)$ and $r_k = r(N, u_k)$, and, for $i = k-1$, $\ldots$, 0, $d_i = q(r_{i+1}, u_i)$ and $r_i = r(r_{i+1}, u_i)$. Then $N = d_k u_k + \cdots + d_0 u_0$. The normal $U$-representation of $N$ is denoted by $\langle N \rangle_U$.

By convention the normal representation of 0 is the empty word $\varepsilon$. Under the hypothesis that the ratio $u_{n+1}/u_n$ is bounded by a constant as $n$ tends to infinity, the integers of the normal $U$-representation of any integer $N$ are bounded and contained in a *canonical* finite alphabet $A$ associated with $U$.

EXAMPLE 7.3.1. Let $U = \{2^n \mid n \geq 0\}$. The normal $U$-representation of an integer is nothing else than its 2-ary standard expansion.

Example 7.3.2. Let $F = (F_n)_{n \geq 0}$ be the sequence of Fibonacci numbers (see Example ??). The canonical alphabet is equal to $A = \{0, 1\}$. The normal $F$-representation of the number 15 is 100010, another representation is 11010.

An equivalent definition of the notion of normal $U$-representation is the following one.

Lemma 7.3.3. *The word $d_k \cdots d_0$, where each $d_i$, for $k \geq i \geq 0$, is a nonnegative integer and $d_k \neq 0$, is the normal $U$-representation of some integer if and only if for each $i$, $d_i u_i + \cdots + d_0 u_0 < u_{i+1}$.*

*Proof.* If $d_k \cdots d_0$ is obtained by the greedy algorithm, $r_{i+1} = d_i u_i + \cdots + d_0 u_0 < u_{i+1}$ by construction. ∎

As for $\beta$-expansions, the $U$-representation obtained by the greedy algorithm is the greatest one for some order we define now. Let $v$ and $w$ be two words. We say that $v < w$ if $|v| < |w|$ or if $|v| = |w|$ and there exist letters $a < b$ such that $v = uav'$ and $w = ubw'$. This order is sometimes called "radix order" or "genealogic order", or even "lexicographic order" in the literature, although the definition is slightly different from the usual definition of lexicographic order on finite words (see Chapter 1).

Proposition 7.3.4. *The normal $U$-representation of an integer is the greatest in the radix order of all the $U$-representations of that integer.*

*Proof.* Let $d = d_k \cdots d_0$ be the normal $U$-representation of $N$, and let $w = w_j \cdots w_0$ be another representation. Since $u_k \leq N < u_{k+1}$, $k \geq j$. If $k > j$, then $d > w$. If $k = j$, suppose $d < w$. Thus there exists $i$, $k \geq i \geq 0$ such that $d_i < w_i$ and $d_k \cdots d_{i+1} = w_k \cdots w_{i+1}$. Hence $d_i u_i + \cdots + d_0 u_0 = w_i u_i + \cdots + w_0 u_0$, but $d_i u_i + \cdots + d_0 u_0 \leq (w_i - 1)u_i + d_{i-1} u_{i-1} + \cdots + d_0 u_0$, so $u_i + w_{i-1} u_{i-1} + \cdots + w_0 u_0 \leq d_{i-1} u_{i-1} + \cdots + d_0 u_0 < u_i$ since $d$ is normal, which is absurd. ∎

The order between natural numbers is given by their radix order between their normal $U$-representations.

Proposition 7.3.5. *Let $M$ and $N$ be two nonnegative integers, then $M < N$ if and only if $\langle M \rangle_U < \langle N \rangle_U$.*

*Proof.* Let $v = v_k \cdots v_0 = \langle M \rangle_U$ with $u_k \leq M < u_{k+1}$, and $w = w_j \cdots w_0 = \langle N \rangle_U$ with $u_j \leq N < u_{j+1}$, and suppose that $v < w$. Then $k \leq j$. If $k < j$, $u_{k+1} \leq u_j$, and $M < N$. If $k = j$, there exists $i$ such that $v_i < w_i$ and $v_k \cdots v_{i+1} = w_k \cdots w_{i+1}$. Hence

$$\begin{aligned} M &= v_k u_k + \cdots + v_0 u_0 \\ &\leq w_k u_k + \cdots + w_{i+1} u_{i+1} + (w_i - 1)u_i + v_{i-1} u_{i-1} + \cdots + v_0 u_0 \\ &< w_k u_k + \cdots + w_{i+1} u_{i+1} + w_i u_i \leq N \end{aligned}$$

since $v_{i-1} u_{i-1} + \cdots + v_0 u_0 < u_i$ by Lemma 7.3.3, thus $M < N$. ∎

### 7.3.2. The set of normal $U$-representations

The set of normal $U$-representations of all the nonnegative integers is denoted by $L(U)$.

Example 7.3.2 (*continued*). Let $F$ be the sequence of Fibonacci numbers. The set $L(F)$ is the set of words without the factor 11, and not beginning with a 0,

$$L(F) = 1\{0,1\}^* \setminus \{0,1\}^* 11 \{0,1\}^* \cup \varepsilon.$$

First the analogue of Theorem 7.2.9 is the following result.

Proposition 7.3.6. *The set $L(U)$ is the set of words over $A$ such that each suffix of length $n$ is less in the radix order than $\langle u_n - 1\rangle_U$.*

*Proof.* Let $v = v_k \cdots v_0$ be in $L(U)$, and $0 \leq n \leq k+1$. By Lemma 7.3.3 $v_{n-1}u_{n-1} + \cdots + v_0 u_0 \leq u_n - 1$, and by Proposition 7.3.5, $v_{n-1} \cdots v_0 \leq \langle u_n - 1\rangle_U$. The converse is immediate. ∎

An important case is when $L(U)$ is recognizable by a finite automaton, as it is the case for usual numeration systems. We first give a necessary condition.

Recall that a formal series with coefficients in $\mathbb{N}$ is said to be $\mathbb{N}$-*rational* if it belongs to the smallest class containing polynomial with coefficients in $\mathbb{N}$, and closed under addition, multiplication and star operation, where $F^*$ is the series $1 + F + F^2 + F^n + \cdots = 1/(1-F)$, $F$ being a series such that $F(0) = 0$. A $\mathbb{N}$-rational series is necessarily $\mathbb{Z}$-rational, and thus can be written $P(X)/Q(X)$, with $P(X)$ and $Q(X)$ in $\mathbb{Z}[X]$, and $Q(0) = 1$. Therefore the sequence of coefficients of a $\mathbb{N}$-rational series satisfies a linear recurrent relation with coefficients in $\mathbb{Z}$. It is classical that, if $L$ is recognizable by a finite automaton, then the series $f_L(X) = \sum_{n\geq 0} \ell_n X^n$, where $\ell_n$ denotes the number of words of length $n$ in $L$, is $\mathbb{N}$-rational (see Berstel and Reutenauer 1988).

Proposition 7.3.7. *If the set $L(U)$ is recognizable by a finite automaton, then the series $U(X) = \sum_{n\geq 0} u_n X^n$ is $\mathbb{N}$-rational, and thus the sequence $U$ satisfies a linear recurrence with integral coefficients.*

*Proof.* Let $\ell_n$ be the number of words of length $n$ in $L(U)$. The series $f_{L(U)}(X) = \sum_{n\geq 0} \ell_n X^n$ is $\mathbb{N}$-rational. We have $u_n = \ell_n + \cdots + \ell_0$, because the number of words of length $\leq n$ in $L(U)$ is equal to the number of naturals smaller than $u_n$, whose normal representation has length $n+1$. Thus $U(X) = f_{L(U)}(X)/(1-X)$, and it is $\mathbb{N}$-rational. ∎

When the sequence $U$ satisfies a linear recurrence with integral coefficients, we say that $U$ defines a *linear numeration system*.

To determine sufficient conditions on the sequence $U$ for the set $L(U)$ to be recognizable by a finite automaton is a difficult question (see Problem 7.3.1). It is strongly related to the theory of $\beta$-expansions where $\beta$ is the dominant root of the characteristic polynomial of the linear recurrence of $U$. Nevertheless, there is a case where the set $L(U)$ and the factors of the $\beta$-shift coincide. This means that the dynamical systems generated by the $\beta$-expansions of real numbers and by normal $U$-representations of integers are the same.

It is obvious that if a word of the form $v0^n$ belongs to $L(U)$ then $v$ itself is a word of $L(U)$, but the converse is not true in general. We will say that a set $L \subset A$ is *right-extendable* if the following property holds

$$v \in L \Rightarrow v0 \in L.$$

THEOREM 7.3.8. *Let $U = (u_n)_{n\geq 0}$ be a strictly increasing sequence of integers, with $u_0 = 1$, and such that $\sup u_{n+1}/u_n < +\infty$, and let $A$ be the canonical alphabet. There exists a real number $\beta > 1$ such that $L(U) = F(D_\beta)$ if and only if $L(U)$ is right-extendable. In that case, if $d^*_\beta(1) = (d_i)_{i\geq 1}$, the sequence $U$ is determined by*

$$u_n = d_1 u_{n-1} + \cdots + d_n u_0 + 1.$$

*Proof.* Clearly, if $L(U) = F(D_\beta)$ for some $\beta > 1$, then $L(U)$ is right-extendable.

Conversely, suppose that $L(U)$ is right-extendable. For each $n$, denote

$$\langle u_n - 1\rangle_U = d_1^{(n)} \cdots d_n^{(n)}.$$

Since $L(U)$ is right-extendable, for each $k < n$, $d_1^{(k)} \cdots d_k^{(k)} 0^{n-k} \in L(U)$, and thus $d_1^{(k)} \cdots d_k^{(k)} \leq d_1^{(n)} \cdots d_k^{(n)}$. Therefore $d_1^{(k)} \cdots d_k^{(k)} = d_1^{(n)} \cdots d_k^{(n)}$ because $d_1^{(k)} \cdots d_k^{(k)}$ is the greatest word of length $k$ in the radix order.
Let $d_n = d_n^{(n)}$, then $d_n d_{n+1} \cdots \leq d_1 d_2 \cdots$. Let $d = (d_i)_{i\geq 1}$. If there exists $m$ such that $d = \sigma^m(d)$ then $d$ is periodic. Let $m$ be the smallest such index. In that case, put $t_1 = d_1, \ldots, t_{m-1} = d_{m-1}$, $t_m = d_m + 1$, $t_i = 0$ for $i > m$. In case $d$ is not periodic, put $t_i = d_i$ for every $i$. Then the sequence $(t_i)_{i\geq 1}$ satisfies $t_n t_{n+1} \cdots < t_1 t_2 \cdots$ for all $n \geq 2$, and thus by Corollary 7.2.10 there exists a unique $\beta > 1$ such that $d_\beta(1) = (t_i)_{i\geq 1}$.

Let us show that $L(U) = F(D_\beta)$. Recall that

$$D_\beta = \{s \mid \forall p \geq 0, \sigma^p(s) < d^*_\beta(1) = (d_i)_{i\geq 1}\}$$

hence

$$\begin{aligned} F(D_\beta) &= \{v = v_k \cdots v_0 \mid \forall n,\ 0 \leq n \leq k, v_{n-1} \cdots v_0 \leq d_1 \cdots d_n = \langle u_n - 1\rangle_U\} \\ &= L(U) \end{aligned}$$

by Proposition 7.3.6.

Now, since by definition $d_1 \cdots d_n = \langle u_n - 1\rangle_U$, we get

$$u_n = d_1 u_{n-1} + \cdots + d_n u_0 + 1. \qquad \blacksquare$$

The numeration systems satisfying Theorem 7.3.8 will be called *canonical* numeration systems associated with $\beta$, and denoted by $U_\beta$. Note that if $d_\beta(1)$ is eventually periodic, then $L(U_\beta)$ is recognizable by a finite automaton and $U_\beta$ satisfies a linear recurrent sequence.

EXAMPLE 7.3.2 (*continued*). The Fibonacci numeration system is the canonical numeration system associated with the golden ratio.

### 7.3.3. Normalization in a canonical linear numeration system

We first give general definitions, valid for any linear numeration system defined by a sequence $U$. The *numerical value* in the system $U$ of a representation $w = d_k \cdots d_0$ is equal to $\pi_U(w) = \sum_{i=0}^{k} d_i u_i$. Let $C$ be a finite alphabet of integers. The *normalization* in the system $U$ on $C^*$ is the partial function

$$\nu_C : C^* \longrightarrow A^*$$

that maps a word $w$ of $C^*$ such that $\pi_U(w)$ is nonnegative onto the normal $U$-representation of $\pi_U(w)$.

In the sequel, we assume that $U = U_\beta$ is the canonical numeration system associated with a number $\beta$ which is a Pisot number. Thus $U$ satisfies an equation of the form

$$u_n = a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_m u_{n-m}, \quad a_i \in \mathbb{Z}, \quad a_m \neq 0, \quad n \geq m.$$

In that case, the canonical alphabet $A$ associated with $U$ is $A = \{0, \ldots, K\}$ where $K < \max(u_{i+1}/u_i)$. The polynomial $P(X) = X^m - a_1 X^{m-1} - \cdots - a_m$ will be called the *characteristic polynomial* of $U$.

We also make the hypothesis that $P$ is exactly the minimal polynomial of $\beta$ (in general, $P$ is a multiple of the minimal polynomial).

Our aim is to prove the following result.

THEOREM 7.3.9. *Let $U = U_\beta$ be a canonical linear numeration system associated with a Pisot number $\beta$, and such that the characteristic polynomial of $U$ is equal to the minimal polynomial of $\beta$. Then, for every alphabet $C$ of nonnegative integers, the normalization on $C^*$ is computable by a finite transducer.*

The proof is in several steps. Let $C = \{0, \ldots, c\}$, $\widetilde{C} = \{-c, \ldots, c\}$, and let

$$Z(U, c) = \{d_k \cdots d_0 \mid d_i \in \widetilde{C}, \ \sum_{i=0}^{k} d_i u_i = 0\}$$

be the set of words on $\widetilde{C}$ having numerical value 0 in the system $U$. We first prove a general result.

PROPOSITION 7.3.10. *If $Z(U, c)$ and $L(U)$ are recognizable by a finite automaton then $\nu_C$ is a function computable by a finite transducer.*

*Proof.* Let $f = f_n \cdots f_0$ and $g = g_k \cdots g_0$ be two words of $C^*$, with for instance $n \geq k$. We denote by $f \ominus g$ the word of $\widetilde{C}^*$ equal to $f_n \cdots f_{k+1}(f_k - g_k) \cdots (f_0 - g_0)$. The graph of $\nu_C$ is equal to $\widehat{\nu_C} = \{(f, g) \in C^* \times A^* \mid g \in L(U), f \ominus g \in Z(U, c)\}$.

Let $R$ be the graph of $\ominus$ :

$$R = [(\cup_{a \in C}((a, \varepsilon), a))^* \cup (\cup_{a \in C}((\varepsilon, a), -a))^*][\cup_{a,b \in C}((a, b), a - b)]^*$$

$R$ is a rational subset of $(C^* \times C^*) \times \widetilde{C}^*$. Let us consider the set

$$R' = R \cap ((C^* \times L(U)) \times Z(U,c)) \subseteq (C^* \times A^*) \times \widetilde{C}^*.$$

Then $\widehat{\nu_C}$ is the projection of $R'$ on $C^* \times A^*$. As $L(U)$ and $Z(U,c)$ are rational by assumption, $(C^* \times L(U)) \times Z(U,c)$ is a recognizable subset of $(C^* \times A^*) \times \widetilde{C}^*$ as a Cartesian product of rational sets (see Berstel 1979). Since $R$ is rational, $R'$ is a rational subset of $(C^* \times A^*) \times \widetilde{C}^*$. So, $\widehat{\nu_C}$ being the projection of $R'$, $\widehat{\nu_C}$ is a rational subset of $C^* \times A^*$, that is, $\nu_C$ is computable by a finite transducer. ■

The core of the proof relies in the following result.

Proposition 7.3.11. *Let $U$ be a linear numeration system such that its characteristic polynomial is equal to the minimal polynomial of a Pisot number $\beta$. Then $Z(U,c)$ is recognizable by a finite automaton.*

*Proof.* Set $Z = Z(U,c)$ for short. We define on the set $H$ of prefixes of $Z$ the equivalence relation $\zeta$ as follows ($m$ is the degree of $P$)

$$f \,\zeta\, g \Leftrightarrow [\forall n,\ 0 \le n \le m-1,\ \pi_U(f0^n) = \pi_U(g0^n)].$$

Let $f \,\zeta\, g$. It is clear that the sequences $(\pi_U(f0^n))_{n\ge 0}$ and $(\pi_U(g0^n))_{n\ge 0}$ satisfy the same recurrence relation as $U$. Since they coincide on the first $m$ values, they are equal. Thus, for any $h \in \widetilde{C}$,

$$\begin{aligned} fh \in Z &\Leftrightarrow \pi_U(f0^{|h|}) + \pi_U(h) = 0 \\ &\Leftrightarrow \pi_U(g0^{|h|}) + \pi_U(h) = 0 \\ &\Leftrightarrow gh \in Z \end{aligned}$$

which means that $f$ and $g$ are right congruent modulo $Z$. If $f$ and $g$ are not in $H$, then $f \sim_Z g$ as well.

It remains to prove that $\zeta$ has finite index. This will be achieved by showing that there are only finitely many possible values of $\pi_U(f0^n)$ for $f \in H$ and for all $0 \le n \le m-1$. Recall that, if $\beta = \beta_1, \beta_2, \ldots, \beta_m$ are the roots of $P$, since $P$ is minimal they are all distinct, and there exist complex constants $\lambda_1 > 0$, $\lambda_2, \ldots, \lambda_m$ such that for all $n \in \mathbb{N}$

$$u_n = \sum_{i=1}^{m} \lambda_i \beta_i^n.$$

If $f = f_k \cdots f_0$, let $\pi_\beta(f) = f_k\beta^k + \cdots + f_1\beta + f_0$.
*Claim 1.* There exists $\eta$ such that for all $f \in \widetilde{C}$

$$|\pi_U(f) - \lambda_1 \pi_\beta(f)| < \eta.$$

We have

$$\begin{aligned}\pi_U(f) - \lambda_1 \pi_\beta(f) &= \sum_{j=0}^{k} f_j u_j - \lambda_1 \sum_{j=0}^{k} f_j \beta^j \\ &= \sum_{j=0}^{k} f_j (\sum_{i=1}^{m} \lambda_i \beta_i^j) - \lambda_1 \sum_{j=0}^{k} f_j \beta^j \\ &= \sum_{j=0}^{k} f_j (\sum_{i=2}^{m} \lambda_i \beta_i^j).\end{aligned}$$

Since $\beta$ is a Pisot number, $|\beta_i| < 1$ for $2 \leq i \leq m$ and

$$|\pi_U(f) - \lambda_1 \pi_\beta(f)| < c \sum_{i=2}^{m} |\lambda_i| \frac{1}{1 - |\beta_i|} = \eta.$$

*Claim 2.* There exists $\gamma$ such that for all $f \in H$, $|\pi_\beta(f)| < \gamma$.
Since $f \in H$ there exists $h \in \widetilde{C}$ such that $fh \in Z$. Thus

$$\begin{aligned}0 = \pi_U(f0^{|h|}) + \pi_U(h) &< \lambda_1 \pi_\beta(f0^{|h|}) + \lambda_1 \pi_\beta(h) + 2\eta \\ &< \lambda_1 \pi_\beta(f)\beta^{|h|} + \lambda_1(c+1)\beta^{|h|} + 2\eta\beta^{|h|}\end{aligned}$$

thus $\pi_\beta(f) > -c - 1 - 2\eta\lambda_1^{-1}$. Similarly $\pi_\beta(f) < c + 1 + 2\eta\lambda_1^{-1}$, hence $|\pi_\beta(f)| < c + 1 + 2\eta\lambda_1^{-1} = \gamma$.
*Claim 3.* There exists $\delta$ such that for all $f \in H$, for all $0 \leq n \leq m-1$

$$|\pi_U(f0^n)| < \delta.$$

We have

$$\begin{aligned}|\pi_U(f0^n)| &\leq |\pi_U(f0^n) - \lambda_1 \pi_\beta(f0^n)| + |\lambda_1 \pi_\beta(f0^n)| \\ &< \eta + |\lambda_1 \pi_\beta(f)|\beta^n \\ &< \eta + \lambda_1 \gamma \beta^n\end{aligned}$$

hence $|\pi_U(f0^n)| < \delta = \eta + \lambda_1 \gamma \beta^{m-1}$.

Thus there are only finitely many possible values of $\pi_U(f0^n)$ for $f \in H$ and for all $0 \leq n \leq m-1$, therefore $\zeta$ has finite index, and $Z(U,c)$ is rational. ∎

*Proof* of the theorem. Since $U$ is canonical for a Pisot number, $L(U)$ is recognizable by a finite automaton. The result follows from Proposition 7.3.10 and Proposition 7.3.11. ∎

Corollary 7.3.12. *Under the same hypothesis as in Theorem 7.3.9, addition of integers represented in the canonical linear numeration system $U_\beta$ is computable by a finite transducer.*

*Proof.* The canonical alphabet being $A = \{0, \ldots, K\}$, take $C = \{0, \ldots, 2K\}$ in Theorem 7.3.9. ∎

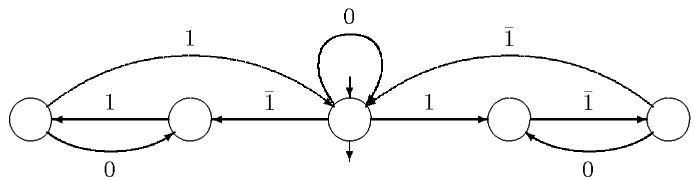


**Figure 7.3.** Automaton recognizing the set of words on $\{-1, 0, 1\}$ having value 0 in the Fibonacci numeration system

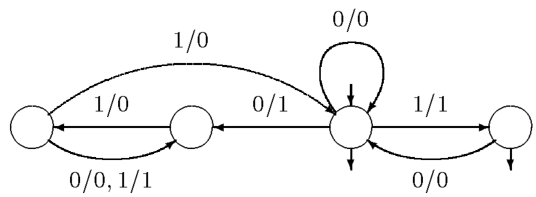


**Figure 7.4.** Normalization on $\{0, 1\}$ in the Fibonacci numeration system

Example 7.3.2 (*continued*). Let $F$ be the sequence of Fibonacci numbers. The characteristic polynomial of $F$ is $X^2 - X - 1$, and it is the minimal polynomial of the Pisot number $\beta = (1 + \sqrt{5})/2$. Figure 7.3 gives the automaton recognizing the set $Z(F, 1)$ of words on the alphabet $\{-1, 0, 1\}$ having numerical value 0 in the Fibonacci numeration system.

Figure 7.4 shows a finite transducer realizing the normalization on $\{0, 1\}$ in the Fibonacci numeration system. For simplicity, we assume that input and output words have the same length.

The result stated in Theorem 7.3.9 can be extended to the case where $U$ is not the canonical numeration system associated with a Pisot number $\beta$, but where the characteristic polynomial of $U$ is still equal to the minimal polynomial of $\beta$. There is a partial converse to this result, see Notes.

## 7.4. Representation of complex numbers

The usual method of representing real numbers by their decimal or binary expansions can be generalized to complex numbers. It is possible (see the Problem Section) to represent complex numbers with an integral base and complex digits, but we present here results when the base is some complex number.

### 7.4.1. Gaussian integers

In this section we focus on representing complex numbers using integral digits. The set of *Gaussian integers*, denoted by $\mathbb{Z}[i]$, is the set $\{a+bi \mid a,b \in \mathbb{Z}\}$. The base $\beta$ will be chosen as a Gaussian integer. It is quite natural to extend properties satisfied by integral base for real numbers, namely the fact that integers coincide with numbers having a zero fractional part. More precisely, given a base $\beta$ of modulus $> 1$ and an alphabet $A$ of digits that are Gaussian integers, we will say that $(\beta, A)$ is an *integral numeration system* for the field of complex numbers $\mathbb{C}$ if every Gaussian integer $z$ has a *unique integer* representation of the form $d_k \cdots d_0$ such that $z = \sum_{j=0}^{k} d_j \beta^j$, with $d_j \in A$. We shall see later that, in that case, every complex number has a representation.

We first show preliminary results. A set $A \subset \mathbb{Z}[i]$ is a *complete residue system* for $\mathbb{Z}[i]$ modulo $\beta$ if every element of $\mathbb{Z}[i]$ is congruent modulo $\beta$ to a unique element of $A$. The *norm* of a Gaussian integer $z = x + yi$ is $N(z) = x^2 + y^2$. The following result is well known in elementary number theory.

Theorem 7.4.1 (Gauss). *Let $\beta = a + bi$ be a non-zero Gaussian integer, and let $N$ be the norm of $\beta$. If $a$ and $b$ are coprime, then a complete residue system for $\mathbb{Z}[i]$ modulo $\beta$ is the set*

$$\{0, \ldots, N-1\}.$$

*If $\gcd(a,b) = \lambda$, a complete residue system for $\mathbb{Z}[i]$ modulo $\beta$ is the set*

$$\{p + iq \mid p = 0, 1, \ldots, (N/\lambda) - 1,\ q = 0, 1, \ldots, \lambda - 1\}.$$

We use it in the following circumstances.

Proposition 7.4.2. *Suppose that every Gaussian integer has an integer representation in $(\beta, A)$. Then this representation is unique if and only if $A$ is a complete residue system for $\mathbb{Z}[i]$ modulo $\beta$, that contains 0.*

*Proof.* Let us suppose that $A$ is a complete residue system containing 0, and let $d_k \cdots d_0$ and $c_p \cdots c_0$ be two representations of $z$ in $(\beta, A)$. One can suppose $d_0 \neq c_0$. Then $c_0 - d_0 = \beta(d_k\beta^{k-1} + \cdots + d_1 - c_p\beta^{p-1} - \cdots - c_1)$, thus $d_0$ and $c_0$ are congruent modulo $\beta$, and are elements of $A$, thus they are equal, which is absurd.

Conversely, suppose that every Gaussian integer $z$ has a unique representation of the form $d_k \cdots d_0$, with digits $d_j$ in $A$. Then $z$ is congruent to $d_0$ modulo $\beta$, thus the digit set $A$ must contain a complete residue system.

Now let $c$ and $d$ be two digits of $A$ that are congruent modulo $\beta$. Then $c - d = \beta q$ with $q$ in $\mathbb{Z}[i]$. Let $q_n \cdots q_0$ be the representation of $q$. Hence $c$ has two representations, $c$ itself and $q_n \cdots q_0 d$. ∎

If we require the digits to be natural numbers, the base must be a Gaussian integer $\beta = a + bi$ with $a$ and $b$ coprime, and the choice is drastically restricted.

THEOREM 7.4.3. *Let $\beta$ be a Gaussian integer of norm $N$, and let $A = \{0, \ldots, N-1\}$. Then $(\beta, A)$ is an integral numeration system for the complex numbers if and only if $\beta = -n \pm i$, for some $n \geq 1$.*

*Proof.* First let $\beta = a + bi$, $a$ and $b$ coprime, and let $A = \{0, \ldots, a^2 + b^2 - 1\}$. Suppose that $a > 0$. We shall show that the Gaussian integer $z = (1-a) + ib$ has no representation. Suppose in the contrary that $z$ has a representation $d_k \cdots d_0$. Let $y = z(1-\beta) = a^2 + b^2 - 2a + 1$. Since $a > 0$, $y$ belongs to $A$. But $y = d_0 + (d_1 - d_0)\beta + \cdots + (d_k - d_{k-1})\beta^k - d_k\beta^{k+1}$. Thus $y$ is congruent to $d_0$ modulo $\beta$, and so $y = d_0$. It follows that $d_1 - d_0 = 0, \ldots, d_k - d_{k-1} = 0$, $d_k = 0$, so for $0 \leq j \leq k$, $d_j = 0$. Thus $y = 0$ and $a = 1$, $b = 0$. But $\beta = 1$ is not the base of a numeration system.

If $a = 0$ and $b = \pm 1$, then $\beta = \pm i$ is not a base either. If $a = 0$ and $|b| \geq 2$, the digit set is $\{0, \cdots, b^2 - 1\}$. If $b > 0$ then $i$ has no integer representation, since $\langle i \rangle_\beta = 10 \cdot (b^2 - b)$. If $b < 0$, then $-i$ has no integer representation (see Exercise 7.4.2.)

Let now $a < 0$ and $b \neq \pm 1$. Suppose that a Gaussian integer $z$ has a representation $d_k \cdots d_0$. Then $\mathrm{Im} z = d_k \, \mathrm{Im}\beta^k + \cdots + d_1 \, \mathrm{Im}\beta$. Since $\mathrm{Im}\beta = b$ is a divisor of $\mathrm{Im}\beta^k$ for all $k$, $b$ divides $\mathrm{Im} z$. Take $z = i$. Since $b \neq \pm 1$, there is a contradiction.

Let now $\beta = -n + i$, $n \geq 1$, and thus $A = \{0, \ldots, n^2\}$. It remains to prove that any $z \in \mathbb{Z}[i]$ has an integer representation in $(\beta, A)$. Let $z = x + iy$, $x$ and $y$ in $\mathbb{Z}$. We have $z = c + d\beta$, with $d = y$ and $c = x + ny$. From the equality $\beta^2 + 2n\beta + n^2 + 1 = 0$, it is possible to write $z$ as $z = d_3\beta^3 + d_2\beta^2 + d_1\beta + d_0$ with $d_i \in \mathbb{N}$.

Let $z = d_k\beta^k + \cdots + d_0$, with $d_i \in \mathbb{N}$, and $k \geq 3$, and let $d = d_k \cdots d_0 \in \mathbb{N}^*$. Denote by $S$ the sum-of-digits function

$$\begin{aligned} S \,:\, \mathbb{C} \times \mathbb{N}^* &\longrightarrow \mathbb{N} \\ (z, d) &\longmapsto S(z, d) = d_k + \cdots + d_0. \end{aligned}$$

In the following we will use the fact that $n^2 + 1 = \beta^3 + (2n-1)\beta^2 + (n-1)^2\beta$, that is, $\langle n^2 + 1 \rangle_\beta$ is equal to the word $1(2n-1)(n-1)^2 0$, and that the sum of digits of these two representations is the same and equal to $n^2 + 1$. By the Euclidean division by $n^2 + 1$, $d_0 = r_0 + q_0(n^2 + 1)$ with $0 \leq r_0 \leq n^2$, thus $z = r_0 + (d_1 + q_0(n-1)^2)\beta + (d_2 + q_0(2n-1))\beta^2 + (d_3 + q_0)\beta^3 + d_4\beta^4 + \cdots + d_k\beta^k = d_0^{(1)} + \cdots + d_k^{(1)}\beta^k$. Clearly $S(z, d) = S(z, d^{(1)})$, where $d^{(1)} = d_k^{(1)} \cdots d_0^{(1)}$.

Let $z_1 = d_1^{(1)} + \cdots + d_k^{(1)}\beta^{k-1}$, then $S(z_1, d^{(1)}) \leq S(z, d)$, and the inequality is strict if and only if $r_0 \neq 0$. Repeating this process, we get $z = \beta z_1 + r_0$, $z_1 = \beta z_2 + r_1$, $\ldots$, $z_{j-1} = \beta z_j + r_{j-1}$, with for $0 \leq i \leq j-1$, $r_i \in A$, and $S(z, d) \geq S(z_1, d^{(1)}) \geq \cdots \geq S(z_{j-1}, d^{(j-1)})$.

Since the sequence $(S(z_j, d^{(j)}))_j$ of natural numbers is decreasing, there exists a $p$ such that, for every $m \geq 0$, $S(z_p, d^{(p)}) = S(z_{p+m}, d^{(p+m)})$, thus $\beta^m$ divides $z_p$ for every $m$, therefore $z_p = 0$. So we get

$$\langle z \rangle_\beta = r_{p-1} \cdots r_0.$$

Let now $\beta = -n - i$. Using the result for the conjugate $\bar\beta = -n + i$, we have

$$\langle \bar z \rangle_{\bar\beta} = r_{p-1} \cdots r_0$$

for every Gaussian integer $\bar z$. Hence

$$\langle z \rangle_{\beta} = r_{p-1} \cdots r_0$$

for every Gaussian integer $z$. ∎

From this result, one can deduce that every complex number is representable in this system.

THEOREM 7.4.4. *If $\beta = -n \pm i$, $n \geq 1$, and $A = \{0, \dots, n^2\}$, every complex number has a representation (not necessarily unique) in the numeration system $(\beta, A)$.*

*Proof.* Let $z = x + iy$, $x$ and $y$ in $\mathbb{R}$, be a fixed arbitrary complex number. For $k \geq 0$, let $\beta^k = u_k + iv_k$. Then

$$z = \frac{(x+iy)(u_k + iv_k)}{\beta^k} = \frac{p_k + iq_k}{\beta^k} + \frac{r_k + is_k}{\beta^k}$$

where $xu_k - yv_k = p_k + r_k$, $xv_k + yu_k = q_k + s_k$, with $p_k$ and $q_k$ in $\mathbb{Z}$, and $|r_k| < 1$, $|s_k| < 1$. Let

$$z_k = \frac{p_k + iq_k}{\beta^k}, \; y_k = \frac{r_k + is_k}{\beta^k}.$$

Since $y_k \to 0$ when $k \to \infty$, $\lim_{k\to\infty} z_k = z$. Since $p_k + iq_k$ is a Gaussian integer, by Theorem 7.4.3.

$$\langle p_k + iq_k \rangle_\beta = d^{(k)}_{t(k)} \cdots d^{(k)}_0.$$

Thus

$$z_k = d^{(k)}_{t(k)} \beta^{t(k)-k} + \cdots + d^{(k)}_0 \beta^{-k}.$$

So

$$\begin{aligned}
|d^{(k)}_{t(k)} \beta^{t(k)-k} + \cdots + d^{(k)}_k| &\leq |z_k| + \frac{d^{(k)}_{k-1}}{|\beta|} + \cdots + \frac{d^{(k)}_0}{|\beta|^k} \\
&\leq |z| + |y_k| + n^2\left(\frac{1}{|\beta|} + \frac{1}{|\beta|^2} + \cdots\right) \\
&\leq |z| + |y_k| + \frac{n^2}{|\beta| - 1} \leq c
\end{aligned}$$

where $c$ is a positive constant not depending on $k$.

Since the representation of a Gaussian integer is unique, and since $\mathbb{Z}[i]$ is a discrete lattice, *i.e.* is an additive subgroup such that any bounded part contains only a finite number of elements, $t(k) - k$ has an upper bound. Let $M$ be an integer such that $t(k) - k \leq M$. Then we can write $z_k$ on the form

$$z_k = a^{(k)}_M \beta^M + \cdots + a^{(k)}_0 + a^{(k)}_{-1}\beta^{-1} + a^{(k)}_{-2}\beta^{-2} + \cdots$$

**Figure 7.5.** Base $-1+i$ tile with fractal boundary

where $a_j^{(k)} \in A$ for $M \geq j$. Let $b_M \in A$ be an integer so that $a_M^{(k)} = b_M$ for infinitely many $k$'s. Let $D_M$ be the subset of those $k$'s such that $a_M^{(k)} = b_M$. Let $b_{M-1} \in A$ be an integer so that $a_{M-1}^{(k)} = b_{M-1}$ for infinitely many $k$'s in $D_M$, and let $D_{M-1}$ be the set of those $k$'s. Repeating this process a set sequence $(D_\ell)_{\ell \geq M}$ such that $D_M \supseteq D_{M-1} \supseteq \cdots$ and such that for all $k \in D_\ell$, $a_j^{(k)} = b_j$ for each $\ell \leq j \leq M$ is constructed. Let $k_1 < k_2 < \cdots$ be an infinite sequence such that $k_j \in D_{M-j+1}$ for $j \geq 1$. Since

$$z_{k_j} = b_M\beta^M + \cdots + b_{M-j+1}\beta^{M-j+1} + a_{M-j}^{(k_j)}\beta^{M-j} + a_{M-j-1}^{(k_j)}\beta^{M-j-1} + \cdots$$

we get $z_{k_j} \to \sum_{\ell \leq M} b_\ell \beta^\ell$ when $j \to \infty$. Since $\lim_{k\to\infty} z_k = z$, we have

$$\langle z \rangle_\beta = b_M \cdots b_0 \cdot b_{-1} b_{-2} \cdots \qquad \blacksquare$$

Example 7.4.5. On Figure 7.5 is shown the set obtained by considering complex numbers having a zero integer part and a fractional part of length less than a fixed bound in their $-1+i$-expansion. This set actually tiles the plane.

Let $C$ be a finite alphabet of Gaussian integers. The normalization on $C^*$ is the function

$$\begin{aligned} \nu_C : C^* &\longrightarrow A^* \\ c_k \cdots c_0 &\longmapsto \langle \textstyle\sum_{j=0}^{k} c_j \beta^j \rangle_\beta \end{aligned}$$

As for standard representations of integers (see Proposition 7.1.3), normalization is a right subsequential function, and in particular addition is right subsequential.

Proposition 7.4.6. *For any finite alphabet $C$ of Gaussian integers, the normalization in base $\beta = -n + i$ restricted to the set $C^* \setminus 0C^*$ is a right subsequential function.*

*Proof.* Let $m = \max\{|c-a| \mid c \in C, a \in A\}$, and let $\gamma = m/(|\beta|-1)$. First observe that, if $s \in \mathbb{Z}[i]$ and $c \in C$, there exist unique $a \in A$ and $s' \in \mathbb{Z}[i]$ such that $s + c = \beta s' + a$, because $A$ is a complete residue system mod $\beta$. Furthermore, if $|s| < \gamma$, then $|s'| \le (|s| + |c-a|)/|\beta| < (\gamma + m)/|\beta| = \gamma$.

Consider the subsequential finite transducer $(\mathcal{A}, \omega)$ over $C^* \times A^*$, where $\mathcal{A} = (Q, E, 0)$ is defined as follows. The set of states is $Q = \{s \in \mathbb{Z}[i] \mid |s| < \gamma\}$. Since $\mathbb{Z}[i]$ is a discrete lattice, $Q$ is finite.

$$E = \{s \xrightarrow{c/a} s' \mid s + c = \beta s' + a\}.$$

Observe that the edges are "letter-to-letter". The terminal function is defined by $\omega(s) = \langle s \rangle_\beta$. The transducer is subsequential because $A$ is a complete residue system.

Now let $c_k \cdots c_0 \in C^*$ and $z = \sum_{j=0}^{k} c_j \beta^j$. Setting $s_0 = 0$, there is a unique path

$$s_0 \xrightarrow{c_0/a_0} s_1 \xrightarrow{c_1/a_1} s_2 \xrightarrow{c_2/a_2} \cdots \xrightarrow{c_{k-1}/a_{k-1}} s_k \xrightarrow{c_k/a_k} s_{k+1}.$$

We get $z = a_0 + a_1\beta + \cdots + a_k\beta^k + s_{k+1}\beta^{k+1}$, and thus $\langle z \rangle_\beta = \omega(s_{k+1}) a_k \cdots a_0$. ∎

### 7.4.2. Representability of the complex plane

In general, the question of deciding whether, given a base $\beta$ and a set of digits $A$, every complex number is representable, is difficult. A sufficient condition is given by the following result.

THEOREM 7.4.7. *Let $\beta$ be a complex number of modulus greater than 1, and let $A$ be a finite set of complex numbers containing zero. If there exists a bounded neighborhood $V$ of zero such that $\beta V \subset V + A$, then every complex number $z$ has a representation of the form*

$$z = \sum_{j \le m} d_j \beta^j$$

*with $m$ in $\mathbb{Z}$ and digits $d_j$ in $A$.*

*Proof.* Let $z$ be in $\mathbb{C}$. There exists an integer $k \ge 0$ such that $\beta^{-k} z \in V$, thus it is enough to show that every element of $V$ is representable. Let $z$ be in $V$. A sequence $(z_j)_{j \ge 0}$ of elements of $V$ is constructed as follows. Let $z_0 = z$. As $\beta V \subset V + A$, if $z_j$ is in $V$, there exist $d_{j+1}$ in $A$ and $z_{j+1}$ in $V$ such that

$$z_{j+1} = \beta z_j - d_{j+1}.$$

Hence the sequence $(z_j)_{j \ge 0}$ is such that

$$z = d_1\beta^{-1} + \cdots + d_j\beta^{-j} + z_j\beta^{-j}$$

and since $V$ is bounded, by letting $j$ tend to infinity,

$$z = \sum_{j \ge 0} d_j \beta^{-j}.$$

∎

## Problems

*Section 7.1*

7.1.1 Prove that addition in the standard $\beta$-ary system is not left subsequential.

7.1.2 Give a right subsequential transducer realizing the multiplication by a fixed integer, and a left subsequential transducer realizing the division by a fixed integer in the standard $\beta$-ary system.

7.1.3 Prove the well-known fact that a number is rational if and only if its $\beta$-expansion in the standard $\beta$-ary system is eventually periodic.

7.1.4 Show that any real number can be represented without a sign using a negative base $\beta$, where $\beta$ is an integer $\leq -2$, and digit alphabet $\{0, \ldots, |\beta|-1\}$. Integers have a unique integer representation. Addition of integers is a right subsequential function.

7.1.5 Show that one can represent any real number without a sign using base 3, and digit alphabet $\{\bar{1}, 0, 1\}$. Integers have a unique integer representation. Addition of integers is a right subsequential function. Generalize this result to integral bases greater than 3.

*Section 7.2*

7.2.1 Show that the code $Y$ defined in the proof of Proposition 7.2.11 is finite if and only if $d_\beta(1)$ is finite, resp. is recognizable by a finite automaton if and only if $d_\beta(1)$ is eventually periodic.

7.2.2 If every rational number of $[0,1]$ has an eventually periodic $\beta$-expansion, then $\beta$ must be a Pisot or a Salem number. (See Schmidt 1980).

7.2.3 Normalization in base $\beta$. (See Frougny 1992, Berend and Frougny 1994).

1. Let $s = (s_i)_{i \geq 1}$ and denote by $\pi_\beta(s)$ the real number $\sum_{i \geq 1} s_i \beta^{-i}$. Let $C$ be a finite alphabet of integers. The canonical alphabet is $A = \{0, \ldots, \lfloor \beta \rfloor\}$. The *normalization function* on $C$

$$\nu_C : C^{\mathbb{N}} \longrightarrow A^{\mathbb{N}}$$

is the partial function which maps an infinite word $s$ over $C$, such that $0 \leq \pi_\beta(s) \leq 1$, onto the $\beta$-expansion of $\pi_\beta(s)$.

A transducer is said to be *letter-to-letter* if the edges are labelled by couples of letters.

Let $C = \{0, \ldots, c\}$, where $c$ is an integer $\geq 1$. Show that normalization $\nu_C$ is a function computable by a finite letter-to-letter transducer if and only if the set

$$Z(\beta, c) = \{s = (s_i)_{i \geq 0} \mid s_i \in \mathbb{Z},\ |s_i| \leq c,\ \sum_{i \geq 0} s_i \beta^{-i} = 0\}$$

is recognizable by a finite automaton.
2. Prove that the following conditions are equivalent:
(i) normalization $\nu_C : C^{\mathbb{N}} \longrightarrow A^{\mathbb{N}}$ is a function computable by a finite letter-to-letter transducer on any alphabet $C$ of nonnegative integers
(ii) $\nu_{A'} : A'^{\mathbb{N}} \longrightarrow A^{\mathbb{N}}$, where $A' = \{0, \ldots, \lfloor\beta\rfloor + 1\}$, is a function computable by a finite letter-to-letter transducer
(iii) $\beta$ is a Pisot number.

*Section 7.3*

**7.3.1 (See Hollander 1998) Let $U$ be a linear recurrent sequence of integers such that $\lim_{n\to\infty}(u_{n+1}/u_n) = \beta$ for real $\beta > 1$.
1. Prove that if $d_\beta(1)$ is not finite nor eventually periodic then $L(U)$ is not recognizable by a finite automaton.
2. If $d_\beta(1)$ is eventually periodic, $d_\beta(1) = t_1 \cdots t_N(t_{N+1} \cdots t_{N+p})^\omega$, set

$$B(X) = X^{N+p} - \sum_{i=1}^{N+p} t_i X^{N+p-i} - X^N + \sum_{i=1}^{N} t_i X^{N-i}.$$

Similarly, if $d_\beta(1)$ is finite, $d_\beta(1) = t_1 \cdots t_m$, set

$$B(X) = X^m - \sum_{i=1}^{m} t_i X^{m-i}.$$

Note that $B(X)$ is dependent on the choice of $N$ and $p$ (or $m$). Any such polynomial is called an *extended beta polynomial* for $\beta$. Prove that
(i) If $d_\beta(1)$ is eventually periodic, then $L(U)$ is recognizable by a finite automaton if and only if $U$ satisfies an extended beta polynomial for $\beta$.
(ii) If $d_\beta(1)$ is finite, then

- if $U$ satisfies an extended beta polynomial for $\beta$ then $L(U)$ is recognizable by a finite automaton
- if $L(U)$ is recognizable by a finite automaton then $U$ satisfies a polynomial of the form $(X^m - 1)B(X)$ where $B(X)$ is an extended polynomial for $\beta$ and $m$ is the length of $d_\beta(1)$.

*Section 7.4*

7.4.1 1. Show that every Gaussian integer can be uniquely represented using base 3 and digit set $A = \{\bar{1}, 0, 1\} + i\{\bar{1}, 0, 1\} = \{0, 1, -1, i, -i, 1+i, 1-i, -1+i, -1-i\}$. If each digit is written in the form

$$0 = \substack{0\\0},\ 1 = \substack{1\\0},\ -1 = \substack{\bar{1}\\0},\ i = \substack{0\\1},\ -i = \substack{0\\\bar{1}}$$

$$1+i = \substack{1\\1},\ 1-i = \substack{1\\\bar{1}},\ -1+i = \substack{\bar{1}\\1},\ -1-i = \substack{\bar{1}\\\bar{1}}$$

then for any representation the top row represents the real part and the bottom row is the imaginary part. Every complex number is representable.

2. Show that every complex number can be represented using base 2 and the same digit set $A$, but that the representation of a Gaussian integer is not unique.

7.4.2 Prove that every Gaussian integer has a unique representation of the form $d_k \cdots d_0 \cdot d_{-1}$ in base $\beta = \pm bi$, where $b$ is an integer $\geq 2$, and the digits $d_j$ are elements of $A = \{0, \ldots, b^2 - 1\}$. Every complex number is representable. (See Knuth 1988).

7.4.3 Show that every complex number can be represented using base 2 and digit set $A = \{0, 1, \zeta, \zeta^2, \zeta^3\}$, where $\zeta = \exp(2i\pi/4)$. These representations are called *polygonal* representations. (See Duprat, Herreros, and Kla 1993).

7.4.4 Let $\beta$ be a complex number of modulus $> 1$, and let $A$ be a finite digit set containing 0. Let $W$ be the set of fractional parts of complex numbers, $W = \{\sum_{j\geq 1} d_j \beta^{-j} \mid d_j \in A\}$.

1. Show that $W$ is the only compact subset of $\mathbb{C}$ such that $\beta W = W + A$.

2. Show that if the set $W$ is a neighborhood of zero, then every complex number has a representation with digits in $A$.

7.4.5 Let $\beta$ be a complex number of modulus $> 1$, and let $A$ be a finite digit set containing 0. An infinite sequence $(d_j)_{j\geq 1}$ of $A^{\mathbb{N}}$ is a *strictly proper* representation of a number $z = \sum_{j\geq 1} d_j \beta^{-j}$ if it is the greatest in the lexicographic order of all the representations of $z$ with digits in $A$. It is *weakly proper* if each finite truncation is strictly proper. Let $W = \{\sum_{j\geq 1} d_j \beta^{-j} \mid d_j \in A\}$. Show that, if $\beta$ is a complex Pisot number, the set of weakly proper representations of elements of $W$ is recognizable by a finite automaton. (See Thurston 1989, Kenyon 1992, Petronio 1994).

*7.4.6 Representation of algebraic number fields. (See Gilbert 1981, 1994, Kátai and Kovacs 1981).

Let $\beta$ be an algebraic integer of modulus $> 1$, and let $A$ be a finite set of elements of $\mathbb{Z}[\beta]$ containing zero. We say that $(\beta, A)$ is an *integral numeration system* for the field $\mathbb{Q}(\beta)$ if every element of $\mathbb{Z}[\beta]$ has a unique integer representation of the form $d_k \cdots d_0$ with $d_j$ in $A$.

1. Let $P(X) = X^m + p_{m-1}X^{m-1} + \cdots + p_0$ be the minimal polynomial of $\beta$. The *norm* of $\beta$ is $N(\beta) = |p_0|$. Show that a complete residue system of elements of $\mathbb{Z}[\beta]$ modulo $\beta$ is the set $\{0, \ldots, N(\beta) - 1\}$.

2. Suppose that every element of $\mathbb{Z}[\beta]$ has a representation in $(\beta, A)$. Prove that this representation is unique if and only if $A$ is a complete residue system for $\mathbb{Z}[\beta]$ modulo $\beta$, that contains zero.

3. Suppose that $(\beta, A)$ is an integral numeration system. Show that every element of the field $\mathbb{Q}(\beta)$ has a representation in $(\beta, A)$.

4. Show that $(\beta, A)$ is an integral numeration system if and only if $\beta$ and all its conjugates have moduli greater than 1 and there is no positive

integer $q$ for which

$$d_{q-1}\beta^{q-1} + \cdots + d_0 \equiv 0 \pmod{\beta^q - 1}$$

with $d_j$ in $A$ for $0 \le j \le q$.
5. Now suppose that $\beta$ is a quadratic algebraic integer, and let $A = \{0, \ldots, |p_0| - 1\}$. Prove that $(\beta, A)$ is an integral numeration system for $\mathbb{Q}(\beta)$ if and only if $p_0 \ge 2$ and $-1 \le p_1 \le p_0$.

## Notes

Concerning the representation of numbers in classical or less classical numeration systems, there is always something to learn in Knuth 1988. Representation in integral base with signed digits was popularized in computer arithmetic by Avizienis (1961) and can be found earlier in a work of Cauchy (1840).

We have not presented here $p$-adic numeration, nor the representation of real numbers by their continued fraction expansions (see Chapter 2 for this last topic).

The notion of beta-expansion is due to Rényi (1957). Its properties were essentially set up by Parry (1960), in particular Theorem 7.2.9. Coded systems were introduced by Blanchard and Hansel (1986). The result on the entropy of the $\beta$-shift is due to Ito and Takahashi (1974). The links between the $\beta$-expansion of 1 and the nature of the $\beta$-shift are exposed in Ito and Takahashi 1974 and in Bertrand-Mathis 1986. Connections with Pisot numbers are to be found in Bertrand 1977 and Schmidt 1980. It is also known that normalization in base $\beta$ is computable by a finite transducer on any alphabet if and only if $\beta$ is a Pisot number, see Problem 7.2.3. If $\beta$ is a Salem number of degree 4 then $d_\beta(1)$ is eventually periodic, see Boyd 1989. It is an open problem for degree $\ge 6$. Perron numbers are introduced in Lind 1984. There is a survey on the relations between beta-expansions and symbolic dynamics by Blanchard (1989). In Solomyak 1994 and in Flatto, Lagarias, and Poonen 1994 is proved the following property: if $d_\beta(1)$ is eventually periodic, then the algebraic conjugates of $\beta$ have modulus strictly less than the golden ratio. Beta-expansions also appear in the mathematical description of quasicrystals, see Gazeau 1995.

The representation of integers with respect to a sequence $U$ is introduced in Fraenkel 1985. The fact that, if $L(U)$ is recognizable by a finite automaton, then the sequence $U$ is linearly recurrent is due to Shallit (1994). We follow the proof of Loraud (1995). The converse problem is treated by Hollander 1998, see Problem 7.3.3. Canonical numeration systems associated with a number $\beta$ come from Bertrand-Mathis (1989). Normalization in linear numeration systems linked with Pisot numbers is studied in Frougny 1992, Frougny and Solomyak 1996, and with the use of congruential techniques, in Bruyère and Hansel 1997. Moreover, if the sequence $U$ has a characteristic polynomial which is the minimal polynomial of a Perron number which is not Pisot, then normalization cannot be computed by a finite transducer on every alphabet (Frougny and Solomyak 1996).

A famous result on sets of natural numbers recognized by finite automata is the theorem of Cobham (1969). Let $k$ be an integer $\geq 2$. A set $X$ of positive integers is said to be *$k$-recognizable* if the set of $k$-representations of numbers of $X$ is recognizable by a finite automaton. Two numbers $k$ and $l$ are said to be *multiplicatively independent* if there exist no positive integers $p$ and $q$ such that $k^p = l^q$. Cobham's Theorem then states: If $X$ is a set of integers which is both $k$-recognizable and $l$-recognizable in two multiplicatively independent bases $k$ and $l$, then $X$ is eventually periodic. There is a multidimensional version of Cobham's Theorem due to Semenov (1977). Original proofs of these two results are difficult, and several other proofs have been given, some of them using logic (see Michaux and Villemaire 1996). There are many works on generalizations of Cobham and Semenov theorems (see Fabre 1994, Bruyère and Hansel 1997, Point and Bruyère 1997, Fagnot 1997, Hansel 1998). In Durand 1998 there is a version of the Cobham theorem in terms of substitutions. We give now one result related to the concepts exposed in Section 7.3. Let $U$ be an increasing sequence of integers. A set $X$ of positive integers is $U$-recognizable if the set of normal $U$-representations of numbers of $X$ is recognizable by a finite automaton. Let $\beta$ and $\beta'$ be two multiplicatively independent Pisot numbers, and let $U$ and $U'$ be two linear numeration systems whose characteristic polynomial is the minimal polynomial of $\beta$ and $\beta'$ respectively. For every $n \geq 1$, if $X \subset \mathbb{N}^n$ is $U$- and $U'$-recognizable then $X$ is definable in $\langle \mathbb{N}, + \rangle$ (Bès 2000). When $n = 1$, the result says that $X$ is eventually periodic.

Theorem 7.4.3 on bases of the form $-n \pm i$, $n$ integer $\geq 1$ is due to Kátai and Szabó (1975). There is a more algorithmic proof, as well as results on the sum-of-digits function for base $\beta = -1+i$, in Grabner et al. 1998 Normalization in complex base is studied in Safer 1998. Theorem 7.4.7 appeared in Thurston 1989, as well as the result on complex Pisot bases presented in Problem 7.4.5. Representation of complex numbers in imaginary quadratic fields is studied in Kátai 1994. We have not discussed here beta-automatic sequences. Results on these topics can be found in Allouche et al. 1997, particularly for the case $\beta = -1 + i$.

The numeration in complex base is strongly related to fractals and tilings. Self-similar tilings of the plane in relation with complex Pisot bases are discussed in Thurston 1989, Kenyon 1992 and Petronio 1994. In Gilbert 1986, the fractal dimension of tiles obtained in some bases such as $-n+i$ is computed. A general survey has been written by Bandt (1991).

# Bibliography


Allouche, J.-P., Cateland, E., Gilbert, W., Peitgen, H.-O., Shallit, J., and Skordev, G. (1997). Automatic maps in exotic numeration systems, *Theory of Computing Systems*, *30*, 285–331.

Avizienis, A. (1961). Signed-digit number representations for fast parallel arithmetic, *IRE Transactions on electronic computers*, *10*, 389–400.

Bandt, C. (1991). Self-similar sets 5 : Integer matrices and fractal tilings of $\mathbb{R}^n$, *Proc. Amer. Math. Soc.*, *112*, 549–562.

Berend, D. and Frougny, Ch. (1994). Computability by finite automata and Pisot bases, *Math. Systems Theory*, *27*, 274–282.

Berstel, J. (1979). *Transductions and context-free languages.* Teubner.

Berstel, J. and Reutenauer, C. (1988). *Rational Series and Their Languages.* Springer-Verlag.

Bertrand, A. (1977). Développements en base de Pisot et répartition modulo 1, *C. R. Acad. Sci. Paris*, *285*, 419–421.

Bertrand-Mathis, A. (1986). Développement en base $\theta$, répartition modulo un de la suite $(x\theta^n)_{n\geq 0}$, langages codés et $\theta$-shift, *Bull. Soc. Math. France*, *114*, 271–323.

Bertrand-Mathis, A. (1989). Comment écrire les nombres entiers dans une base qui n'est pas entière, *Acta Math. Hung.*, *54*, 237–241.

Bès, A. (2000). An extension of the Cobham-Semenov theorem, *J. Symbolic Logic*, *65*, 201–211.

Blanchard, F. (1989). $\beta$-expansions and symbolic dynamics, *Theoret. Comput. Sci.*, *65*, 131–141.

Blanchard, F. and Hansel, G. (1986). Systèmes codés, *Theoret. Comput. Sci.*, *44*, 17–49.

Boyd, D. (1989). Salem numbers of degree four have periodic expansions, In de Coninck, J.-H. and Levesque, C. (Eds.), *Number Theory*, pp. 57–64. Walter de Gruyter.

Bruyère, V. and Hansel, G. (1997). Bertrand numeration systems and recognizability, *Theoret. Comput. Sci.*, *181*, 17–43.

Cauchy, A. (1840). Sur les moyens d'éviter les erreurs dans les calculs numériques, *Comptes Rendus de l'Académie des Sciences*, *11*, 789–798. Reprinted in A. Cauchy, Oeuvres complètes, 1ère série, Tome V, Gauthier-Villars, Paris, 1885, pp. 431–442.

Cobham, A. (1969). On the base-dependence of sets of numbers recognizable by finite automata, *Math. Systems Theory*, *3*, 186–192.

Duprat, J., Herreros, Y., and Kla, S. (1993). New complex representations of complex numbers and vectors, *IEEE Transactions on Computers*, *42*, 817–824.

Durand, F. (1998). A generalization of Cobham's theorem, *Theory of Computing Systems*, *32*, 169–185.

Fabre, S. (1994). Une généralisation du théorème de Cobham, *Acta Arithm.*, *67*, 197–208.

Fagnot, I. (1997). Sur les facteurs des mots automatiques, *Theoret. Comput. Sci.*, *172*, 67–89.

Flatto, L., Lagarias, J., and Poonen, B. (1994). The zeta function of the beta-transformation, *Ergod. Th. Dynam. Sys.*, *14*, 237–266.

Fraenkel, A.S. (1985). Systems of numeration, *Amer. Math. Monthly*, *92*, 105–114.

Frougny, Ch. (1992). Representation of numbers and finite automata, *Math. Systems Theory*, *25*, 37–60.

Frougny, Ch. and Solomyak, B. (1996). On representation of integers in linear numeration systems, In Pollicott, M. and Schmidt, K. (Eds.), *Ergodic theory of* $\mathbf{Z}^d$*-Actions*, No. 228 in London Mathematical Society Lecture Note Series, pp. 345–368. Cambridge University Press.

Gazeau, J.-P. (1995). Pisot-cyclotomic integers for quasilattice, In Moody, R. (Ed.), *The Mathematics of Long-Range Aperiodic Order*, No. 489 in NATO-ASI Series, pp. 175–198. Kluwer Academic Publishers.

Gilbert, W. (1981). Radix representations of quadratic fields, *J. Math. Anal. Appl.*, *83*, 264–274.

Gilbert, W. (1986). The fractal dimension of sets derived from complex bases, *Can. Math. Bul.*, *29*, 495–500.

Gilbert, W. (1994). Gaussian integers as bases for exotic number systems,. Unpublished manuscript.

Grabner, P., Kirschenhofer, P., and Prodinger, H. (1998). The sum-of-digits-function for complex bases, *J. London Math. Soc.*, *57*, 20–40.

Hansel, G. (1998). Systèmes de numération indépendants et syndéticité, *Theoret. Comput. Sci.*, *204*, 119–130.

Hollander, M. (1998). Greedy numeration systems and regularity, *Theory of Computing Systems*, *31*, 111–133.

Ito, S. and Takahashi, Y. (1974). Markov subshifts and realization of $\beta$-expansions, *J. Math. Soc. Japan*, *26*, 33–55.

Kátai, I. (1994). Number systems in imaginary quadratic fields, *Annales Univ. Sci. Budapest sect. Comp.*, *14*, 91–103.

Kátai, I. and Kovacs, B. (1981). Canonical number systems in imaginary quadratic fields, *Acta Math. Acad. Sci. Hung.*, *37*, 159–164.

Kátai, I. and Szabó, J. (1975). Canonical number systems, *Acta Sci. Math.*, *37*, 255–280.

Kenyon, R. (1992). Self-replicating tilings, In Walters, P. (Ed.), *Symbolic dynamics and its applications*, No. 135 in Contemporary Mathematics, pp. 239–263. A. M. S.

Knuth, D. (1988). *The Art of Computer Programming*, Vol. 2. Addison-Wesley. 2nd ed.

Lind, D. (1984). The entropies of topological Markov shifts and a related class of algebraic integers, *Ergod. Th. Dynam. Sys.*, *4*, 283–300.

Loraud, N. (1995). $\beta$-shift, systèmes de numération et automates, *Journal de Théorie de Nombres de Bordeaux*, *7*, 473–498.

Michaux, C. and Villemaire, R. (1996). Presburger arithmetic and recognizability of sets of natural numbers by automata: new proofs of Cobham's and Semenov's theorems, *Annals of Pure and Applied Logic*, *17*, 251–277.

Parry, W. (1960). On the $\beta$-expansions of real numbers, *Acta Math. Acad. Sci. Hung.*, *11*, 401–416.

Petronio, C. (1994). Thurston's solitaire tilings of the plane, *Rendiconti dell'Istituto di Matematica dell'Università di Trieste*, *26*, 247–248.

Point, F. and Bruyère, V. (1997). On the Cobham-Semenov theorem, *Theory of Computing Systems*, *30*, 197–220.

Rényi, A. (1957). Representations for real numbers and their ergodic properties, *Acta Math. Acad. Sci. Hung.*, *8*, 477–493.

Safer, T. (1998). Radix representations of algebraic number fields and finite automata, In *STACS '98*, No. 1373 in Lect. Notes Comp. Sci., pp. 356–365. Springer-Verlag.

Schmidt, K. (1980). On periodic expansions of Pisot numbers and Salem numbers, *Bull. London Math. Soc.*, *12*, 269–278.

Semenov, A. (1977). The Presburger nature of predicates that are regular in two number systems, *Siberian Math. J.*, *18*, 289–299.

Shallit, J. (1994). Numeration systems, linear recurrences, and regular sets, *Inform. Comput.*, *113*, 331–347.

Solomyak, B. (1994). Conjugates of beta-numbers and the zero-free domain for a class of analytic functions, *Proc. London Math. Soc.*, *68*, 477–498.

Thurston, W. (1989). Groups, tilings, and finite state automata, *AMS Colloquium Lecture Notes*.