Combinatorics, Automata and Number Theory

CANT

Edited by

Valérie Berthé

LIRMM - Univ. Montpelier II - CNRS UMR 5506
161 rue Ada, 34392 Montpellier Cedex 5, France

Michel Rigo

Université de Liège, Institut de Mathématiques
Grande Traverse 12 (B 37), B-4000 Liège, Belgium

2

Number representation and finite automata

Christiane Frougny

Univ. Paris 8 and
LIAFA, Univ. Paris 7 - CNRS UMR 7089
Case 7014, F-75205 Paris Cedex 13, France

Jacques Sakarovitch

LTCI, CNRS/ENST - UMR 5141
46, rue Barrault, F-75634 Paris Cedex 13, France.

Contents

2.1 Introduction

Numbers do exist — independently of the way we represent them, of the way we write them. And there are many ways to write them: integers as a finite sequence of digits once a base is fixed, rational numbers as a pair of integers or as an eventually periodic infinite sequence of digits, or reals as an infinite sequence of digits but also as a continued fraction, just to quote a few. *Operations on numbers* are defined — independently of the way they are computed. But when they are computed, they amount to be algorithms that work on the representations of numbers.

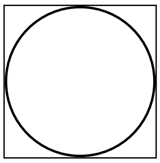


Fig. 2.1. Numbers do exist, a Greek view: $\frac{\pi}{4} = \frac{C}{P} = \frac{D}{S}$. Numbers are then *ratio* between measures (C = length of the circle, P = perimeter of the square, D = surface of the disk, S = surface of the square).

In this chapter, numbers will be represented by their expansion in a base, or more generally, with respect to a basis, hence by *words* over an alphabet of digits. The algorithms we shall consider are those that can be performed by finite state machines, that is, by the simplest machines one can think of. Natural questions then arise immediately. First, whether or not the whole set of expansions of all the positive integers, or the integers, or the real numbers (within an interval) is itself a set of finite, or infinite, words that is recognised by finite automata. Second, which operations on numbers can thus be defined by means of finite automata? how is this related to the chosen base? how, in a given base, may the choice of digits influence the way the operations can be computed? These are some of the questions that will be asked and, hopefully and to a certain extent, answered in this chapter.

It is not only these questions, repeated in every section, that will give this chapter its unity but also the methods with which we shall try to answer them. In every numeration system, defined by a base or a basis, we first consider a trivial infinite automaton — the *evaluator*, whose states are the values of the words it reads — from which we define immediately the *zero automaton* which recognises the words written on a signed digit alphabet and having value 0. From the zero automaton we then derive transducers, called *digit-conversion transducers*, that relate words with same values but written differently on the same or distinct alphabets of digits and, from these, transducers for the normalisation, the addition, *etc.* Whether all these latter transducers are finite or not depends on whether the zero automaton is finite or not and this question is analysed and solved by combinatorial and algebraic methods which depend on the base.

We begin with the classical — one could even say basic — case where the base is a positive integer. It will give us the opportunity to state a number of elementary properties which we nevertheless prove in detail for they will appear again in the other forthcoming parts. The zero automaton is easily seen to be finite, and thus so are finite the adder and the various normalisers. The same zero automaton is the socle on which we build the *local* adder for the Avizienis system, and the normaliser for the *non-adjacent forms* which yield representations of minimal weight.

The first and main non-classical case that will retain our attention is the one of numeration systems often called *non-standard*: a non-integer real β is chosen as a base and the (real) numbers are written in this base; a rather common example is when β is equal to the *Golden Ratio* φ. Such systems are also often called *beta-numeration* in the literature. In contrast with the integer-base case, numbers may have several distinct representations, even on the canonical alphabet, and the *expansion* of every number is computed by a *greedy* algorithm which produces the digits from left to right, that is, *most significant digit first.* The *arithmetic* properties of β, that is, which kind of algebraic integer it is, are put into correspondance with the properties of the system such as for instance the rationality† of the set of expansions. The main result in that direction is that the zero automaton is finite if, and only if, β is a *Pisot number* (Theorem 2.3.31).

Another property that is studied is the possibility of defining from β a sequence of integers that will be taken as a *basis* and that will thus yields a numeration system (for the positive integers), in the very same way as the *Fibonacci numeration system* is associated with the Golden Ratio. Although restricted to the integers, these systems happen to be more difficult to study than those defined by a real base, and the characterisation of those for which the set of expansions is rational is more intricate (Theorem 2.3.57).

Section 2.4 is devoted to *canonical numeration systems* in algebraic number fields. In these systems, every integer has a unique finite expansion, which is not computed by a greedy algorithm but by a right-to-left algorithm, that is, by an algorithm which computes the least significant digit first. The main open problem in this area is indeed to characterise such canonical numeration systems. A beautiful result is the characterisation

† We use 'rational set' as a synonym of 'regular set', see Section **??** and Section 2.6.1.

of Gaussian integers as a base of canonical numeration systems (Theorem 2.4.12).

The third and last kind of numeration systems which we consider is the one of systems with a base that is not an algebraic integer but a *rational number*. First the non-negative integers are given an expansion which is computed *from right to left*, as in the case of canonical numeration sytems. The set of all expansions is not a rational language anymore; it is a very intriguing set of words indeed, a situation which does not prevent the zero automaton to be still finite, and so is the digit-converter from any alphabet to the canonical one. The expansions of real numbers are not really 'computed' but defined *a priori* from the expansions of the integers. The matter of the statement is thus reversed and what is to be proved is not that we can compute the expansion of the real numbers but that every real number is given a representation (at least one) by this set brought from 'outside' (Theorem 2.5.23). This topic has been explored by the authors in a recent paper (Akiyama, Frougny, and Sakarovitch 2008) and is wide open to further research.

In Section 2.6 (before the Notes section) we have gathered definitions† and properties of finite automata and transducers that are not specific to the results on numeration systems but relevant to more or less classical parts of automata theory, and currently used in this chapter.

From this presentation, it appears that we are interested in the way numbers are written rather than in the definition of set of numbers *via* finite automata. And yet the latter has been the first encounter between finite automata theory and number representation, namely, Cobham's Theorem (we mention it only as it stands in the background of the proof that the map betwen the representations of numbers in different bases cannot be realised by finite automata). Speaking of this theorem, it is interesting to quote this seminal paper (Cobham 1969):

> This adds further evidence [...] that, insofar as the recognition of set of numbers goes, finite automata are weak, and somewhat unnatural.

We think, and we hope the reader will be convinced, that the matter developed in this chapter supports the view that finite automata are on the contrary a natural and powerful concept for studying numeration systems.

† Notions defined in that Section 2.6 are shown *slanted* in the text.

2.2 Representation in integer base

We first recall how numbers, integers or real numbers, may be represented in an integer base, like 2 or 10, that is, in the way that everyone does, in the everyday life. The statements and proofs in these first two subsections are thus simple and well-known, when not even trivial. We nevertheless write them explicitely for they allow to see how the several generalisations to come in the sections below differ from, and are similar to, the basic case of integer base numeration systems.

Let p be a fixed integer greater than 1, which we call the *base* (in our running examples, we choose $p = 2$, or $p = 3$ when 2 differs from the general case). The *canonical alphabet* of digits A_p associated with p is $A_p = \{0, 1, \ldots, p-1\}$. The integer p together with A_p defines the *base p numeration system.*

Note that A_p is naturally (and totally) ordered and thus A_p^* is naturally (and totally) ordered by the *lexicographic* and by the *radix* orders.

2.2.1 Representation of integers

The choice of the base p implicitly gives every word of A_p^* an integer value, via the *evaluation map* π_p: for every word w of A_p^*, we have

$$w = a_k\, a_{k-1} \cdots a_1\, a_0 \quad \longmapsto \quad \pi_p\,(w) = \sum_{i=0}^{k} a_i p^i\ .$$

This definition of π_p implies that numbers are written with the *most significant digit* on the left.†

Lemma 2.2.1 *The map π_p is injective on A_p^k, for every integer k.*

Proof Let $u = a_{k-1}a_{k-2}\cdots a_0$ and $v = b_{k-1}b_{k-2}\cdots b_0$ be two distinct words of A_p^* of length k such that $\pi_p\,(u) = \pi_p\,(v)$. Hence

$$\sum_{i=0}^{k-1} a_i\, p^i - \sum_{i=0}^{k-1} b_i\, p^i = 0 \qquad \text{and therefore} \qquad P(X) = \sum_{i=0}^{k-1} (a_i - b_i)\, X^i$$

is a polynomial in $\mathbb{Z}[X]$ vanishing at $X = p$. By Gauss Lemma on primitive polynomials, $P(X)$ is divisible by the minimal polynomial $X - p$. Contradiction, since $|a_0 - b_0|$ is strictly smaller than p. □

† A convention which certainly is the most common one, even in languages written from right to left, but not universal, in particular among computer scientists (see (Cohen 1981) on the endianness problem).

The map π_p is not injective on the whole A_p^* since $\pi_p\left(0^h u\right) = \pi_p(u)$ holds for any u in A_p^* and any integer h. On the other hand, Lemma 2.2.1 implies that this is the only possibility and we have:

$$\pi_p(u) = \pi_p(v) \ \text{ and } \ |u| > |v| \quad \Longrightarrow \quad u = 0^h v \ \text{ with } \ h = |u| - |v| \, .$$

Conversely, every integer N in $\mathbb{N}$ can be given a representation as a word in A_p^* which, thanks to the foregoing, is unique under the condition it does not begin with a zero. This representation can be computed in two different ways, which we call, for further references, the *greedy algorithm* — which computes the digits *from left to right*, that is, *most significant digit first* — and the *division algorithm* — which computes the (same) digits *from right to left*, that is, *least significant digit first*.

The greedy algorithm. Let N be any positive integer. There exists a unique k such that $p^k \leq N < p^{k+1}$. We write $N_k = N$ and, for every i, from $i = k$ to $i = 0$,

$$a_i = \left\lfloor \frac{N_i}{p^i} \right\rfloor \qquad \text{and} \qquad N_{i-1} = N_i - a_i \, p^i \ .$$

Then, a_i is in A_p, a_k is different from 0 and $N_i < p^i$. It holds:

$$N = \sum_{i=0}^{k} a_i \, p^i = \pi_p\left(a_k \cdots a_0\right) \quad .$$

The division algorithm. Let N be any positive integer. Write $N_0 = N$ and, for $i \geqslant 0$, write

$$N_i = p \, N_{i+1} + b_i \tag{2.1}$$

where b_i is the remainder of the division of N_i by p, and thus belongs to A_p. Since N_{i+1} is strictly smaller than N_i, the division (2.1) can be repeated only a finite number of times, until eventually $N_\ell \neq 0$ and $N_{\ell+1} = 0$ for some ℓ (and thus $b_\ell \neq 0$). The sequence of successive divisions (2.1) for $i = 0$ to $i = \ell$ produces the digits $b_0, b_1, \ldots, b_\ell$, and it holds:

$$N = \sum_{i=0}^{\ell} b_i \, p^i = \pi_p\left(b_\ell \cdots b_0\right) \quad .$$

The integer N can also be written as

$$N = \left(\left(\cdots\left(b_\ell \, p + b_{\ell-1}\right)\cdots\right)p + b_1\right)p + b_0 \ \ ,$$

that is, as the evaluation of a polynomial by a *Horner scheme*. By Lemma 2.2.1, $k = \ell$ and $a_k \cdots a_0 = b_\ell \cdots b_0$. We have thus proved the following.

Theorem 2.2.2 *Every non-negative integer N has a unique representation in base p which does not begin with a zero. It is called the p-*expansion *of N and denoted by $\langle N \rangle_p$.*

Note that the representation of 0 is the empty word ε. It also follows that the *set of p-expansions* is the *rational language*

$$L_p = \{\langle N \rangle_p \mid N \in \mathbb{N}\} = {A_p}^* \setminus 0\,{A_p}^* = \{A_p \setminus \{0\}\}\,{A_p}^* \cup \{\varepsilon\} \ .$$

The map π_p is not only a bijection between L_p and $\mathbb{N}$ but also a morphism of ordered sets (when L_p is ordered by the trace of the *radix order* $\prec$ on ${A_p}^*$).

Proposition 2.2.3 *For all n and m in $\mathbb{N}$, $\langle n \rangle_p \prec \langle m \rangle_p$ holds if, and only if, $n < m$.*

Remark 2.2.4 It also follows from Proposition 2.2.3 that for any two words v and w of ${A_p}^*$ and of the *same length*, $v \prec w$ if, and only if, $\pi_p(v) < \pi_p(w)$.

A first finite transducer: the divider by q. Let q be a fixed positive integer and let $[q] = \{0, \ldots, q-1\}$ be the set of remainders modulo q. For every integers s and a, the Euclidean division by q yields unique integers b and r such that

$$p\,s + a = q\,b + r \ . \tag{2.2}$$

If s is in $[q]$ and a is in A_p, then b is in A_p — and by definition r is in $[q]$. Equation (2.2) thus defines a transducer:

$$\mathcal{Q}_{p,q} = (\,[q], A_p, A_p, E, \{0\}, [q]\,) \ \text{ with } \ E = \{\big(s, (a, b), r\big) \mid p\,s + a = q\,b + r\} \,.$$

The transducer $\mathcal{Q}_{p,q}$ is *sequential.* (Indeed, $\mathcal{Q}_{p,q}$ is *co-sequential* as well if p and q are co-prime.) Figure 2.2 shows $\mathcal{Q}_{2,5}$.

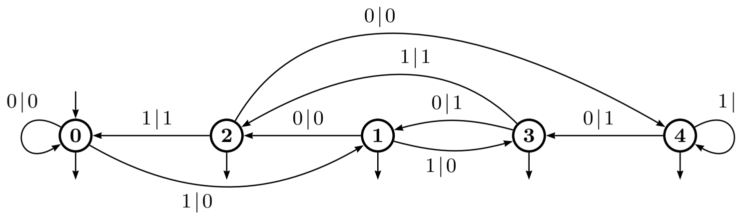


Fig. 2.2. The divider $\mathcal{Q}_{2,5}$.

The realisation of division by finite automata (together with arithmetic operations modulo q) is exactly what is behind computation rules such as the *casting out nines* or divisibility criteria such as the divisibility by 11 (a number is divisible by 11 if, and only if, the sum of digits of odd rank is equal to the sum of digits of even rank). That such criterium exists in every base for any fixed divisor was already observed by Pascal (*cf.* (Pascal 1963, pp. 84–89), see also (Sakarovitch 2003, Prologue)).

2.2.2 The evaluator and the converters

Finite automata really come into play with number representation when we allow ourselves to use sets of digits *larger than the canonical alphabet.* Let p be the base fixed as before but the digits be a priori *any integer*, positive or negative. Consider then the (doubly infinite) automaton $\mathcal{Z}_p$ whose states are the integers, that is, $\mathbb{Z}$, which reads (from left to right) the numbers (thus written on the 'alphabet' $\mathbb{Z}$), and which runs in such a way that, at every step of the reading, the reached state indicates the value of the portion of the number read so far. The initial state of $\mathcal{Z}_p$ is thus 0 and its transitions are of the form:

$$\forall s, t, a \in \mathbb{Z} \qquad s \xrightarrow[\mathcal{Z}_p]{a} t \quad \text{if, and only if,} \quad t = p\,s + a \ , \tag{2.3}$$

from which we get the expected behaviour:

$$\forall w \in \mathbb{Z}^* \qquad 0 \xrightarrow[\mathcal{Z}_p]{w} \pi_p\,(w) \ .$$

It follows from (2.3) that $\mathcal{Z}_p$ is both *deterministic* and *co-deterministic*. It is logical to call $\mathcal{Z}_p$ the *evaluator*.

In fact, we shall consider only finite parts of $\mathcal{Z}_p$. First, we restrict our alphabet to be a *finite* symmetrical part B_d of $\mathbb{Z}$: $B_d = \{-d, \ldots, d\}$ where d is a positive integer, $d \geq p-1$ and thus $A_p \subset B_d$. Second, we choose 0 as a unique final state and we get an automaton $\mathcal{Z}_{p,d} = (\,\mathbb{Z}, B_d, E, \{0\}, \{0\}\,)$ where the transitions in E are those defined by (2.3). This automaton accepts thus the writings of 0 (in base p and on the alphabet B_d) and we call it a *zero automaton*. It is still infinite but we have the following.

Proposition 2.2.5 *The* trim *part of $\mathcal{Z}_{p,d}$ is finite and its set of states is $H = \{-h, \ldots, h\}$ where h is the largest integer (strictly) smaller than $d/(p-1)$.*

Proof As B_d contains A_p and is symmetrical, every z in $\mathbb{Z}$ is *accessible* in $\mathcal{Z}_{p,d}$.

If m is a positive integer larger than, or equal to, $d/(p-1)$, the 'smallest' reachable state from m is $mp - d$, which is also larger than, or equal to, $d/(p-1)$: m is not co-accessible in $\mathcal{Z}_{p,d}$ and the same is true if m is smaller than, or equal to, $-d/(p-1)$.

If m is a positive integer smaller than $d/(p-1)$, then the integer $k = m(p-1)+1$ is smaller than, or equal to, d, and $m \xrightarrow{\overline{k}} (m-1)$ is a transition in $\mathcal{Z}_{p,d}$. (A signed digit $-k$ is denoted by $\overline{k}$.) Hence, by induction, a path from m to 0 in $\mathcal{Z}_{p,d}$. The same is true if m is a negative integer strictly larger than $-d/(p-1)$. □

Figure 2.3 shows $\mathcal{Z}_{2,2}$. By definition, the trim part of $\mathcal{Z}_{p,d}$ is the *strongly connected component* of 0. From now on, and unless otherwise stated, we let $\mathcal{Z}_{p,d}$ denote the automaton reduced to its trim part only. The automaton $\mathcal{Z}_{p,d}$ is not so much interesting in itself but as the core of the construction of a series of transducers that transform representations of a number into others and that we call by the generic name of *digit-conversion transducers*, or *converters* for short.

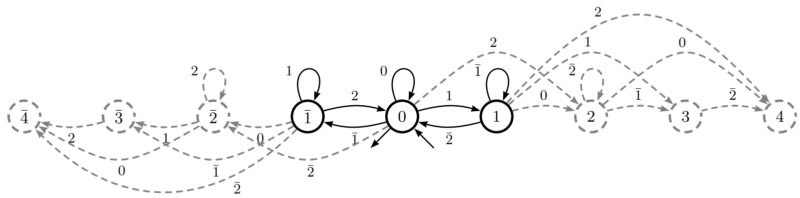


Fig. 2.3. A finite view on $\mathcal{Z}_{2,2}$. The part which is not co-accessible is shown in grey and dashed.

2.2.2.1 The converters and the normalisers

We need some more elementary notation and definitions. From any two alphabets of integers C and A, we build the alphabet $C + A$ (resp. $C - A$) of all sums (resp. differences):

$$C + A = \{z \mid \exists c \in C, \exists a \in A \quad z = c + a\} ,$$
$$C - A = \{z \mid \exists c \in C, \exists a \in A \quad z = c - a\} .$$

Let $u = c_{k-1}c_{k-2}\cdots c_0$ and $v = a_{k-1}a_{k-2}\cdots a_0$ be two words of length k of C^* and A^* respectively. The *digitwise addition* of u and v is the word $u \oplus v = s_{k-1}s_{k-2}\cdots s_0$ of $(C+A)^*$ such that $s_i = c_i + a_i$ (resp. the *digitwise subtraction* is the word $u \ominus v = d_{k-1}d_{k-2}\cdots d_0$ of $(C-A)^*$ such that $d_i = c_i - a_i$), for every i, $0 \leq i < k$. If u and v have not the same length, the shortest is silently padded on the left by 0's and both $u \oplus v$

and $u \ominus v$ are thus defined for all pairs of words. In any case, the following obviously holds:

$$\pi_p(u \oplus v) = \pi_p(u) + \pi_p(v) \quad \text{and} \quad \pi_p(u \ominus v) = \pi_p(u) - \pi_p(v) \ .$$

Let $B_d = \{-d, \ldots, d\}$ be the (smallest) symmetrical part of $\mathbb{Z}$ that contains $C - A$: $d = \max\{|c-a| \mid c \in C, \quad a \in A\}$. From $\mathcal{Z}_{p,d} = (H, B_d, E, \{0\}, \{0\})$, we then define a letter-to-letter (left) transducer $\mathcal{C}_p(C \times A) = (H, C, A, F, \{0\}, \{0\})$, whose transitions are defined by

$$s \xrightarrow[\mathcal{C}_p(C\times A)]{c|a} t \qquad \text{if, and only if,} \qquad s \xrightarrow[\mathcal{Z}_{p,d}]{c-a} t \ , \tag{2.4}$$

for every s and t in H, c in C, and a in A, that is, if, and only if,

$$p\,s + c = t + a \ . \tag{2.5}$$

Both (2.4) and (2.5) show that a given transition in $\mathcal{Z}_{p,d}$ may give rise to no or several transitions (or to a transition with several labels) in $\mathcal{C}_p(C\times A)$. This transducer relates every u in C^* with all words in A^* with the same length and same value in base p, as stated by the following.

Proposition 2.2.6 *Let $\mathcal{C}_p(C \times A)$ be the digit-conversion transducer in base p for the alphabets C and A. For all u in C^* and all v in A^*,*

$$(u, v) \in |\mathcal{C}_p(C \times A)| \quad \textit{if, and only if,} \quad \pi_p(u) = \pi_p(v) \ \textit{and} \ |u| = |v| \ .$$

Proof If (u, v) is in $|\mathcal{C}_p(C\times A)|$, then $|u| = |v|$ as $\mathcal{C}_p(C \times A)$ is letter-to-letter and, on the other hand, the successful computation labeled by (u, v) in $\mathcal{C}_p(C\times A)$ maps onto a successful computation labeled by $u \ominus v$ in $\mathcal{Z}_{p,d}$ and thus $\pi_p(u \ominus v) = 0$, that is, $\pi_p(u) = \pi_p(v)$.

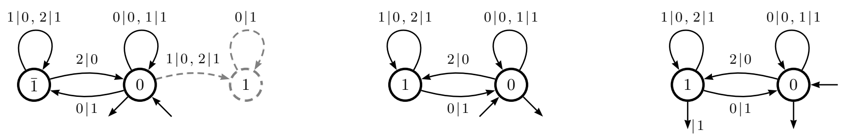
Conversely, if $u = c_{k-1}c_{k-2}\cdots c_0$ and $v = a_{k-1}a_{k-2}\cdots a_0$ are in C^* and A^* respectively, $u \ominus v$ is in B_d^* and if $\pi_p(u) = \pi_p(v)$, then $u \ominus v$ is the label of a successful computation of $\mathcal{Z}_{p,d}$, every transition (s, d_i, t) of which is the image of a transition (s, c_i, a_i, t) in $\mathcal{C}_p(C\times A)$. These transitions form a successful computation whose label is (u, v). □

If $A = A_p$, $\mathcal{C}_p(C \times A_p)$ is *input co-deterministic*, or *co-sequential*, since $p\,s + c = t + a$ and $p\,s' + c = t + a'$ would imply $p(s - s') = a - a'$, and then $s = s'$ as both a and a' are in A_p. Every word u in C^*, padded on the left by the number of 0's necessary to give it the length of $\langle \pi_p(u) \rangle_p$ is thus the input of a unique successful computation in $\mathcal{C}_p(C\times A_p)$ whose output is the unique p-expansion of $\pi_p(u)$.

This is the reason why $\mathcal{C}_p(C\times A_p)$ is rather called *normaliser* (in base p and for the alphabet C), denoted by $\mathcal{N}_p(C)$, and more often described by its *transpose*, a letter-to-letter *right* transducer, which is thus input deterministic, or *sequential*. In order to keep (2.5) valid, we also change the sign of the states in the transpose. Finally, every state is given a *final function* which outputs the p-expansion of the value of the state: it is equivalent to reaching the state 0 by reading enough leading 0's on the input. In conclusion, we have shown the following.

Theorem 2.2.7 *Normalisation in base p for any input alphabet of digits is realised by a finite letter-to-letter sequential right transducer.*

Figure 2.4 shows $\mathcal{N}_2(C_2)$ and its transpose, where $C_2 = A_2 + A_2 = \{0, 1, 2\}$ is the alphabet on which are written words obtained by *digitwise* addition of two binary expansions of integers: $\mathcal{N}_2(C_2)$ realises the addition in base 2.



(a) The transducer $\mathcal{N}_2(C_2)$, (b) its trim transpose, (c) with final function.

Fig. 2.4. A normaliser in base 2.

2.2.2.2 The signed-digit representation

The zero automaton uses negative digits as well as positive ones; we can make use of these digits not only as *computational means* but for the *representation* of numbers as well.

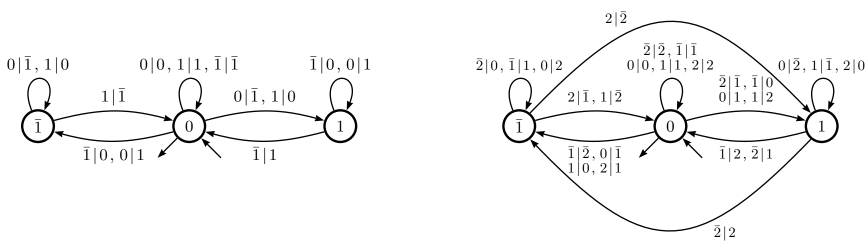
Let us first remark that if an alphabet of integers A contains a complete set of representatives of $\mathbb{Z}/p\mathbb{Z}$, all of which are smaller than p in modulus, then the division algorithm (2.1) may be run with digits taken in A instead of A_p in such a way that it terminates, which proves that every positive integer has a p-representation as a word in A^*, that is, $\pi_p\colon A^* \to \mathbb{N}$ is surjective. On the other hand, π_p is injective if, and only if, there is at most one digit in A for every representatives of $\mathbb{Z}/p\mathbb{Z}$. Both conditions are met if $p = 2q + 1$ is odd and A is the symmetric alphabet $B_q = \{-q, \ldots, q\}$. The first case, $p = 3$ and $A = \{-1, 0, 1\}$, yields a beautiful numeration system, celebrated in (Knuth 1998). But now we are more interested in systems were numbers may have indeed *several representations*. In what follows, we choose A to be a symmetric alphabet B_h:

$$B_h = \{-h, \ldots, h\} \qquad \text{with} \qquad h \geq \left\lfloor \frac{p+1}{2} \right\rfloor \ .$$

As B_h is symmetrical, every integer, positive *and* negative, has a p-representation as a word in ${B_h}^*$. Equation (2.3) and the construction of $\mathcal{Z}_p$ immediately yield the following.

Proposition 2.2.8 *In base p, and with the symmetric digit alphabet B_h, the sign of a number is always given by (the sign of) its left-most digit if, and only if, h is less than p.*

More important, $\pi_p \colon {B_h}^* \to \mathbb{Z}$ is not only surjective, but also *not injective.* The converter $\mathcal{C}_p(B_h \times B_h)$ maps every word in ${B_h}^*$ to all words of ${B_h}^*$ that have the same value (modulo some possible padding on the left by 0's): we call it the *redundancy transducer* (in base p on the alphabet B_h) and denote it by $\mathcal{R}_p(B_h)$. If $h = \left\lfloor \frac{p+1}{2} \right\rfloor$, it follows from Proposition 2.2.5 that $\mathcal{R}_p(B_h)$ has 3 states. Figure 2.5 shows $\mathcal{R}_2(B_1)$ and $\mathcal{R}_3(B_2)$.



(a) The transducer $\mathcal{R}_2(B_1)$. (b) The transducer $\mathcal{R}_3(B_2)$.

Fig. 2.5. Two redundancy transducers.

This symmetric representation of numbers is an old folklore.† It has been given a renewed interest in computer arithmetic for the redundancy in the representations allows to improve the way operations are performed, as we shall see now. The following is to be found in (Avizienis 1961) for bases larger than 2, in (Chow and Robertson 1978) for the binary case — although the original statements and proofs are not formulated in terms of automata.

Theorem 2.2.9 *In base $p \geq 3$ with the symmetric digit alphabet B_h, where $h = \left\lfloor \frac{p}{2} \right\rfloor + 1$, the addition may be realised by a 1-local letter-to-letter transducer, and by a 2-local one if $p = 2$ and $h = 1$.*

Note that a '1-local letter-to-letter transducer' is by definition a 'sequential letter-to-letter transducer', that a '2-local letter-to-letter transducer' is

† It was known (at least) as early as Cauchy who advocated such system for $p = 10$ and $h = 5$ with the argument that it makes the learning of addition and multiplication easier: the size of the tables is rougly divided by 4 (see (Cauchy 1840)).

equivalent to a 'sequential transducer' but not necessarily to a 'sequential letter-to-letter transducer' (*cf.* Section 2.6).

Proof We assume first that $p \geq 3$; the cases of odd $p = 2q + 1$ and of even $p = 2q$ will induce slight variations in the definitions but the core will be the same. In both cases, $h = q + 1$. The alphabet for digitwise addition is B_{2h} with $2h = p + 1$ if p is odd, $2h = p + 2$ if p is even. Let

$$V_p = \begin{cases} \{-(h-1), \ldots, h-1\} & \text{if } p \text{ is odd,} \\ \{-(h-2), \ldots, h-1\} & \text{if } p \text{ is even.} \end{cases}$$

In both cases, $\operatorname{Card} V_p = p$ and is a set of representatives of $\mathbb{Z}/p\mathbb{Z}$. Not only we have $V_p \subset B_h$, but for any s in V_p, $s+1$ and $s-1$ belong to B_h as well (this is the condition which is not verified when $p = 2$).

Let $\mathcal{V}_p$ be the subautomaton of $\mathcal{Z}_p$, with V_p as set of states, 0 as initial state, and every state is final. We turn $\mathcal{V}_p$ into a transducer $\mathcal{W}_p$ with input alphabet B_{2h}. Every transition

$$s \xrightarrow[\mathcal{V}_p]{d} t = p\,s + d \quad \text{gives}$$

$$s \xrightarrow[\mathcal{W}_p]{t|ps} t \quad \text{and also} \quad s \xrightarrow[\mathcal{W}_p]{t+p|p(s+1)} t \quad \text{or} \quad s \xrightarrow[\mathcal{W}_p]{t-p|p(s-1)} t\,,$$

or both, according to whether $t+p$, $t-p$, or both, are in B_{2h}. By construction, the input automaton of $\mathcal{W}_p$ is

(i) deterministic,
(ii) complete (over the alphabet B_{2h}), and
(iii) 1-local (that is, the end of a transition is determined by the label).

Since $t = p\,s+d$, $\mathcal{W}_p$ is a converter and if (u, v) is the label of a computation of $\mathcal{W}_p$ which (begins in 0 and) ends in t, then

$$\pi_p\,(u) = \pi_p\,(v) + t \quad .$$

Let now $\mathcal{W}_p'$ be the transducer obtained from $\mathcal{W}_p$ by replacing every transition

$$s \xrightarrow[\mathcal{W}_p]{m|pn} t \qquad \text{by} \qquad s \xrightarrow[\mathcal{W}_p']{m|n} t\,,$$

and by setting the final function T as $T(t) = t$ for every t in V_p. By construction, and the above remark, the output alphabet of $\mathcal{W}_p'$ is B_h. If (u, v') is the label of a computation of $\mathcal{W}_p'$ which (begins in 0 and) ends in t, then

$$\pi_p\,(u) = p\,\pi_p\,(v') + t = \pi_p\,(v'\,t) \quad .$$

As $v'\,t$ is the output of $\mathcal{W}_p'$ for the input u, $\mathcal{W}_p'$ answers the question.

For $p = 2$, the foregoing construction, starting from $V_2 = \{0, 1\}$, works perfectly well, but for the fact that $\mathcal{W}_2'$ contains one, and only one, transition whose output is not in B_1:

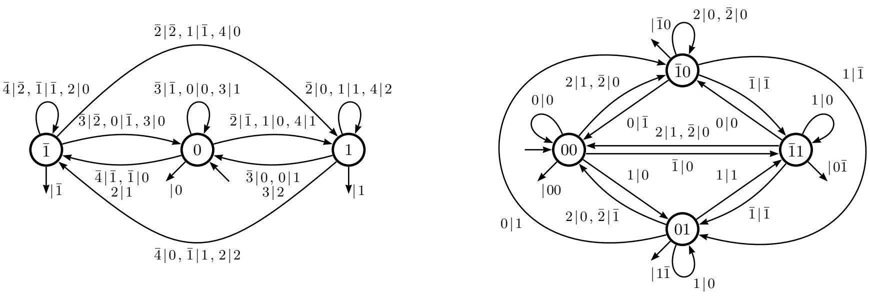
$$1 \xrightarrow[\mathcal{W}_2']{2|2} 0 \ .$$

The same construction is then carried out again, but starting from $\overline{V_2} = \{\bar{1}, 0\}$, which yields a transducer $\overline{\mathcal{W}_2'}$ which contains one, and only one, transition whose output is not in B_1:

$$\bar{1} \xrightarrow[\overline{\mathcal{W}_2'}]{\bar{2}|\bar{2}} 0 \ .$$

The composition $\mathcal{W}_2'' = \mathcal{W}_2' \circ \overline{\mathcal{W}_2'}$ is a 2-local letter-to-letter sequential transducer in which no transition has an output outside B_1 since no transition in $\mathcal{W}_2'$ has a transition with output $\bar{2}$ and no transition in $\overline{\mathcal{W}_2'}$ with input 2 has an output outside B_1: $\mathcal{W}_2''$ answers the question. □

Figure 2.6 shows $\mathcal{W}_3'$ and $\mathcal{W}_2''$.



(a) The transducer $\mathcal{W}_3'$. (b) The transducer $\mathcal{W}_2''$.

Fig. 2.6. Two local adders.

Remark 2.2.10 The same construction as the one for $p = 2$ can be carried out for any even $p = 2q$ and would yield a 2-local automaton for the addition if the numbers are written on the smaller alphabet B_h with $h = q$.

2.2.2.3 The minimal weight representation

Multiplication by a fixed integer obviously falls in the case of normalisation but, in contrast with addition, multiplication (between two numbers) cannot be realised by a finite automaton. However, redundant alphabets and redundancy transducers are not irrelevant to the subject for they allow useful preprocessing to efficient multiplication algorithms.

Let A be a digit alphabet and $u = u_k\, u_{k-1} \cdots u_1\, u_0$ be in A^* with the u_i in A. The *weight* of u is the *absolute sum of digits* $\|u\| = \sum_{i=0}^{k} |u_i|$. The *Hamming weight* of u is the *number* of non-zero digits in u. Of course, when $A \subseteq \{-1, 0, 1\}$, the two definitions coincide; as, for sake of simplicity, we consider here this case only, we do not introduce another notation and speak simply of 'weight'.

The multiplication of two numbers represented by u and v respectively amounts to a series of addition of u with shifted copies of u itself, as many times as there are non-zero digits in v: the smaller the weight of v, the more efficient the multiplication by $\pi_p\,(v)$. Hence the interest for representation of minimal weight. The following statement and proof is an 'automata translation' of a classical description of (binary) representations of minimal weight as 'non-adjacent form' due to Booth (Booth 1951) and Reitwiesner (Reitwiesner 1960).

Theorem 2.2.11 *The computation of a* 2*-representation of minimal weight over the alphabet* $B_1 = \{-1, 0, 1\}$ *from the* 2*-expansion of an integer* x *is realised by a finite sequential right transducer. The result is a representation with no adjacent non-zero digits.*

Remark 2.2.12 The study of minimal weight representations goes on with the computation of the mean weight (that gives an evaluation of the benefits of the construction). These minimal weight representations have also applications to cryptography. See also Section **??**.

2.2.3 Representation of reals

Real numbers from the interval $[0, 1)$ are traditionally represented as infinite sequences of digits (infinite on the right), that is, by elements of $A_p^{\mathbb{N}}$. *By convention*, and although $\mathbb{N}$ contains 0, we consider, in this context and for sake of simplicity of the writing, that an element u of $A_p^{\mathbb{N}}$ is a sequence of digits whose *indices begin with* 1: $u = (u_i)_{i \geq 1}$ where every u_i is in A_p.

The set $A_p^{\mathbb{N}}$ is naturally a *topological space* equipped with the (total) *lexicographic order*: for u and v in $A_p^{\mathbb{N}}$, $u < v$ if, and only if, if $w = u \wedge v$ is the longest common prefix to u and v, then $u = w\, a\, u'$ and $v = w\, b\, v'$ with a and b in A_p and $a < b$. With our convention, the evaluation map, still denoted by π_p, gives every word u of $A_p^{\mathbb{N}}$ a real value:

$$u = u_1\, u_2 \cdots \qquad \longmapsto \qquad \pi_p\,(u) = \sum_{i=1}^{\infty} u_i\, p^{-i} \,.$$

When finite and infinite words are mixed in the same context, the latter are prefixed with the *radix point* inside the function π_p. For instance, it holds:

$$\forall u = (u_i)_{i\geq 1} \in A_p^{\mathbb{N}} \qquad \pi_p\,(\boldsymbol{.}u) = \lim_{n\to+\infty} \frac{1}{p^n}\,\pi_p\,(u_1\,u_2\cdots u_n)\ , \qquad (2.6)$$

$$\forall u \in A_p^{\mathbb{N}}\ ,\ \forall w \in A_p^{*} \qquad \pi_p\,(\boldsymbol{.}w\,u) = \frac{1}{p^{|w|}}\,(\pi_p\,(w) + \pi_p\,(\boldsymbol{.}u))\ . \qquad (2.7)$$

Proposition 2.2.13 *The map* $\pi_p\colon A_p^{\mathbb{N}} \to [0,1]$ *is a continuous and order-preserving function. Moreover, for* u *and* v *in* $A_p^{\mathbb{N}}$*,* $u < v$*, and* $w = u \wedge v$ *,* $\pi_p\,(u) = \pi_p\,(v)$ *if, and only if,* $u = w\,a\,(p\!-1)^{\omega}$ *and* $v = w\,(a\!+\!1)\,0^{\omega}$ *.*

Proof Let us first make the obvious remark — which will be used silently in the sequel — that if u and v are such that for every i, $u_i \leq v_i$ and if there exists at least one j such that $u_j \neq v_j$, then $\pi_p\,(u) < \pi_p\,(v)$.

Next, the not less obvious identity

$$\sum_{i=1}^{+\infty}(p-1)\,p^{-i} = (p-1)\left(\frac{\frac{1}{p}}{1-\frac{1}{p}}\right) = 1 \qquad (2.8)$$

implies in particular that $\pi_p\left(A_p^{\mathbb{N}}\right) \subseteq [0,1]$.

The set $A_p^{\mathbb{N}}$ is a metric space with $d\,(u,v) = 2^{-|u\wedge v|}$ if $u \neq v$ (and $d\,(u,u) = 0$ of course). Then, again by (2.8), $|\pi_p\,(u) - \pi_p\,(v)| \leq 2\,p^{-(|u\wedge v|-1)}$ and π_p is Lipschitz, hence continuous.

Let then u and v be in $A_p^{\mathbb{N}}$, $u < v$, and let k be the smallest index such that $u_k \neq v_k$, that is, $u_k \leq v_k - 1$. Let

$$u' = u_1\,u_2\cdots u_{k-1}\,u_k\,p{-}1\,p{-}1\cdots \quad \text{and} \quad v' = v_1\,v_2\cdots u_{k-1}\,(u_k+1)\,0\,0\cdots$$

By the foregoing, $\pi_p\,(u') = \pi_p\,(v')$ and, if $u \neq u'$, then $\pi_p\,(u) < \pi_p\,(u')$, and if $v \neq v'$, then $\pi_p\,(v') < \pi_p\,(v)$, which shows that π_p is order-preserving. □

Let x be a non-negative real number. If $x \geq 1$, a first way for representing x is to treat its *integral part* $\lfloor x \rfloor$ and its *fractional part* $\{x\}$ separately, to compute $\langle\lfloor x\rfloor\rangle_p$ as we have done in the previous section, to compute $\langle\{x\}\rangle_p$ as we shall see below, and to combine them with the radix point:

$$\langle x\rangle_p = \langle\lfloor x\rfloor\rangle_p\boldsymbol{.}\langle\{x\}\rangle_p\ .$$

Another way is to determine the (unique) integer k such that $p^{k-1} \leq x < p^k$ first, to consider the real $y = \dfrac{x}{p^k}$ which belongs to $[0,1)$, to compute $\langle y\rangle_p = u_1\,u_2\cdots$ and to recover the representation of x by setting the radix point at the right place: $\langle x\rangle_p = u_1\,u_2\cdots u_k\boldsymbol{.}\,u_{k+1}u_{k+2}\cdots$. We shall obviously take the second option, and from now on consider real numbers from $[0,1)$ only. Given such an x in $[0,1)$ which is then likely to have a p-representation which is an infinite sequence on the right, there is no hope to have *an algorithm* which computes the digits *from right to left*, and we are left with the right algorithm which computes the digits *from left to right*.

The greedy algorithm. Let x be in $[0,1)$. Write $z_0 = x$ and, for every $i \geq 1$, let

$$u_i = \lfloor p\, z_{i-1} \rfloor \quad \text{and} \quad z_i = \{p\, z_{i-1}\} \quad . \tag{2.9}$$

Every u_i is in A_p, and it holds

$$z_0 = u_1\, p^{-1} + z_1\, p^{-1} = u_1\, p^{-1} + u_2\, p^{-2} + z_2\, p^{-2} = \cdots = \sum_{i=1}^{+\infty} u_i\, p^{-i} \ , \tag{2.10}$$

that is, the infinite word $u = (u_i)_{i\geq 1}$ in $A_p^{\mathbb{N}}$ is a p-representation of x. It is *the p-expansion* of x, denoted by $\langle x \rangle_p$ or $\mathsf{d}_p(x)$ (when a more functional notation is needed). The computation described by (2.9) is refered to as the *greedy algorithm*.

By convention (and by abuse), we say that a p-representation u is *finite* if it ends with the infinite word 0^ω: $u = w\, 0^\omega$ with w in A_p^* (and indeed the finite word w is sufficient to compute $\pi_p(u)$). An x in $[0,1)$ is said to be *p-decimal* if x has a finite p-representation, that is, if, and only if, x is an integer divided by a (sufficiently large) power of p.

Corollary 2.2.14 *The map $\pi_p \colon A_p^{\mathbb{N}} \to [0,1]$ is a surjective function. An x in $[0,1)$ has more than one p-representation in $A_p^{\mathbb{N}}$ if, and only if, it is p-decimal, in which case it has only two of them, and its p-expansion is the finite one, which is larger in the lexicographic order than the other infinite one.*

It also follows that the *set of p-expansions* is the rational language (of infinite words):

$$D_p = \{\langle x \rangle_p \mid x \in [0,1)\} = A_p^{\mathbb{N}} \setminus A_p^*\, (p-1)^\omega \quad .$$

Figure 2.7 shows a finite Büchi automaton which recognises D_2.

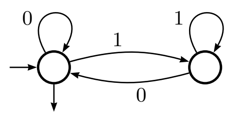


Fig. 2.7. A finite Büchi automaton for the language of 2-expansions D_2.

A first finite transducer over infinite words: the divider by q.

Let us consider the transducer $\mathcal{Q}_{p,q}$ of Section 2.2.1 again (q is a fixed integer and $[q]$ the set of remainders modulo q):

$$\mathcal{Q}_{p,q} = (\,[q], A_p, A_p, E, \{0\}, [q]\,) \text{ with } E = \{\big(s,(a,b),r\big) \mid p\,s + a = q\,b + r\}\ ,$$

where a and b are in A_p and s and r in $[q]$ (see Figure 2.2). We are now interested in the *infinite* computation of $\mathcal{Q}_{p,q}$.

Let u be the p-expansion of an x in $[0,1)$, let c be *the* computation of $\mathcal{Q}_{p,q}$ with input u (it exists as $\mathcal{Q}_{p,q}$ is input-complete and is unique as $\mathcal{Q}_{p,q}$ is input-deterministic), and let v be the output of c, in $A_p^{\mathbb{N}}$. Let $r_0 = 0$ and for every $i \geq 1$ it holds:

$$p\,r_{i-1} + u_i = q\,v_i + r_i\ \ .$$

Equation (2.10) then becomes

$$x = u_1\,p^{-1} + z_1\,p^{-1} = q\,v_1\,p^{-1} + p^{-1}\,(r_1 + z_1) = \cdots = q\sum_{i=1}^{+\infty} v_i\,p^{-i}\ ,$$

that is, $\pi_p\,(u) = q\;\pi_p\,(v)$. And $\mathcal{Q}_{p,q}$ realises the division by the integer q over the p-representations of the reals of $[0,1)$.

As a rational number is the quotient of an integer by another integer, and since $\mathcal{Q}_{p,q}$ is input-deterministic, a computation whose input is ultimately a sequence of 0's ends in a circuit, therefore the description of the division as a finite sequential transducer is a proof of the following classical statement.

Proposition 2.2.15 *The p-expansion of a rational number r/q, in any integer base p, is eventually periodic (of period less than q).*

The zero (Büchi) automaton and (Büchi) converters

The 'zero-automaton' for real number representations is basically the same as the one we have built for the representations of the integers, that is, it is based upon the automaton $\mathcal{Z}_p$ (*cf.* Section 2.2.2). As above, let $B_d = \{-d,\ldots,d\}$ be a finite symmetrical part of $\mathbb{Z}$ with $d \geq p-1$.

Proposition 2.2.16 *An infinite word u in $B_d^{\mathbb{N}}$ has value* 0 *in base p if, and only if, it is accepted by the Büchi automaton $\mathcal{Z}'_{p,d} = (\,H', B_d, E, \{0\}, H'\,)$ with $H' = \{-h',\ldots,h'\}$ where h' is the largest integer smaller than,* or equal to, *$d/(p-1)$.*

Proof By the definition of $\mathcal{Z}'_{p,d}$, every infinite word u that labels an infinite computation in $\mathcal{Z}'_{p,d}$ is accepted by $\mathcal{Z}'_{p,d}$. For every (finite) prefix w of u, $|\pi_p\,(w)| \leq h'$ and then, by (2.6), $\pi_p\,(\centerdot u) = 0$.

Conversely, let u in $B_d^{\mathbb{N}}$ which does not label a computation in $\mathcal{Z}'_{p,d}$, that is, there exists a prefix w of u such that

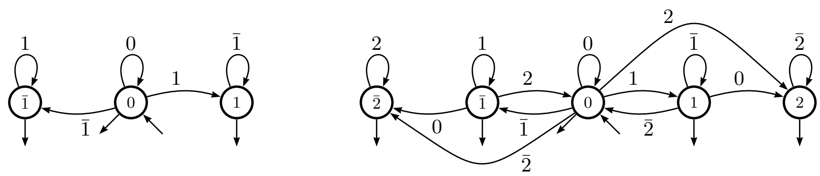
$$0 \xrightarrow[\mathcal{Z}_p]{w} t = \pi_p(w) \qquad \text{with} \qquad t > d/(p-1) \ .$$

We have, on the one hand, $\pi_p(\centerdot u) \geq \pi_p\left(\centerdot w\, \overline{d}^{\omega}\right)$ and, on the other hand,

$$\pi_p\left(\centerdot w\, \overline{d}^{\omega}\right) = \frac{1}{p^{|w|}}\left(t - \frac{d}{p-1}\right) > 0 \,.$$

(The case $t < -d/(p-1)$ is identical.) □

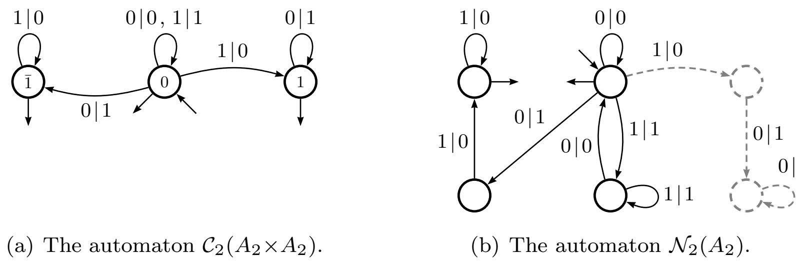
The proof also yields the characterisation of $\mathcal{Z}'_{p,d}$ as the (full) $\mathcal{Z}'_{p,d}$ restricted to its (non-trivial) *strongly connected components*. Figure 2.8 shows $\mathcal{Z}'_{2,1}$ and $\mathcal{Z}'_{2,2}$.



(a) The automaton $\mathcal{Z}'_{2,1}$. (b) The automaton $\mathcal{Z}'_{2,2}$.

Fig. 2.8. Two 'zero automata' for binary representations of reals.

From the zero automaton for real representations, one derives *converters* and *normalisers*, as in the case of the representations of integers, but for the point that not every word in $A_p^{\mathbb{N}}$ is a p-expansion and that there exists thus a distinction between a converter to the canonical alphabet and a normaliser to the same alphabet. For instance, Figure 2.9 shows these converter and normaliser from and to the canonical alphabet, in the binary case.



(a) The automaton $\mathcal{C}_2(A_2 \times A_2)$. (b) The automaton $\mathcal{N}_2(A_2)$.

Fig. 2.9. The converter and normaliser over the canonical alphabet for binary representations of reals.

2.2.4 Base changing

As soon as we want *to compare* the representation of integers in different bases, finite automata show a kind of weakness, that is, no finite transducers exist in general which transform the p-expansion of an integer N into its q-expansion. This follows in fact from the fundamental theorem, due to Alan Cobham, which we refered to in the introduction and which has been presented in Chapter **??** (see Theorem **??**).

This deep result obviously implies, and stays behind, the fact that no finite transducer $\mathcal{T}$ may relate the expansions of integers in base p and in base q, for multiplicatively independent p and q. For, if there was one such $\mathcal{T}$, the image of the p-expansions of a p-recognisable set X by $\mathcal{T}$ would be a rational set of A_q^* and X would thus be q-recognisable as well. It is not necessary however to establish Cobham's Theorem in order to prove the non-existence of such a transducer $\mathcal{T}$. For the latter, it is sufficient for instance to prove that the set of powers of 2 is not 3-recognisable — a simple, and classical, exercise (see (Eilenberg 1974)).

On the other hand, every integer in $\{0, 1, \ldots, p^k - 1\}$ has a p-representation which is a word of A_p^* of length k (by padding on the left with enough 0's) and this defines a *morphism* τ from ${A_{p^k}}^*$ to A_p^* such that $\pi_p\left(\tau\left(\langle N\rangle_{p^k}\right)\right) = N$ for every N in $\mathbb{N}$. Using inversion and composition of finite transducers, we then get the following.

Proposition 2.2.17 *If p and q are two multiplicatively dependent positive integers, then there exists a finite transducer from A_p^* to A_q^* which maps the p-expansion of every positive integer onto its q-expansion.*

Corollary 2.2.18 *If p and q are two multiplicatively dependent positive integers, then the p-recognisable sets and q-recognisable sets of positive integers coincide.*

2.3 Representation in real base

This section is about the so-called *beta-expansions* where the base is a real number $\beta > 1$. By a greedy algorithm producing the most significant digit first, every positive real number is given a β-expansion, which is an infinite word on a canonical alphabet of integer digits. The main difference with the case where β is an integer is that a number may have several representations on the canonical alphabet, the greedy expansion being the greatest in the lexicographic order.

The set of greedy β-expansions forms a symbolic dynamical system, the β-shift, and we start this chapter by establishing some properties of symbolic dynamical systems defined by means of the lexicographic order, and not related to numeration systems. From this, we derive some properties of the β-shift. We then describe several properties of β-expansions in the important case where β is a Pisot number.

Instead of taking a base, which is a number, it is also possible to take a *basis*, that is, a sequence of integers, like the sequence of Fibonacci numbers. This allows to represent any non-negative integer. We study these systems more particularly when the basis is a linear recurrent sequence and investigate the conditions under which the set of greedy expansions is recognisable by a finite automaton.

We also consider the problem of changing the basis and describe cases where the conversion between the expansions in the two numeration systems is realisable by a finite transducer.

2.3.1 Symbolic dynamical systems

Definitions for symbolic dynamical systems have been given in Chapter **??**; we briefly recall some of them as we adopt slightly different notation (see also (Lothaire 2002, Chapter 1)). Let A be a finite alphabet. A word s in $A^{\mathbb{N}}$ *avoids* a set $X \subset A^+$ if no factor of s is in X. Denote $S(X)$ the set of words of $A^{\mathbb{N}}$ which avoid X.

A (one-sided) *symbolic dynamical system*, or *subshift*, is a subset of $A^{\mathbb{N}}$ of the form $S(X)$ for some $X \subset A^+$. Equivalently, it is a closed shift-invariant subset of $A^{\mathbb{N}}$. In this chapter, the *shift* on $A^{\mathbb{N}}$ is denoted σ, and is implicit in all our notations.

A subshift S of $A^{\mathbb{N}}$ is of finite type if $S = S(X)$ for a finite set $X \subset A^+$. A subshift S of $A^{\mathbb{N}}$ is sofic if $S = S(X)$ for a rational set $X \subset A^+$, or, equivalently, if $L(S)$ is rational.

A subshift S of $A^{\mathbb{N}}$ is *coded* if there exists a prefix code $Y \subset A^*$ such that $S = \overline{Y^\omega}$, or, equivalently, if the language of S is equal to the set of factors of Y^*, that is, $L(S) = F(Y^*)$, (Blanchard and Hansel 1986).

In the remaining of this section, A is a totally ordered alphabet.

Definition 2.3.1 A word v in $A^{\mathbb{N}}$ is said to be a *lexicographically shift maximal* word (lsm-word for short) if it is larger than, or equal to, any of its shifted images: for every $k \geq 0$, $\sigma^k(v) \leq v$.

Definition 2.3.2 Let $v = (v_i)_{i \geq 1}$ in $A^{\mathbb{N}}$. We denote by

(i) $v_{[n]}$ the prefix of length n of v: $v_{[n]} = v_1 v_2 \cdots v_n$. By convention, $v_{[0]} = \varepsilon$.

(ii) $S_v = \{u \in A^{\mathbb{N}} \mid \forall k \geq 0,\ \sigma^k(u) \leq v\}$, the set of words in $A^{\mathbb{N}}$, all the shifted images of which are smaller than, or equal to, v.

(iii) $D_v = \{u \in A^{\mathbb{N}} \mid \forall k \geq 0,\ \sigma^k(u) < v\}$, the set of words in $A^{\mathbb{N}}$, all the shifted images of which are smaller than v.

(iv) $Y_v = \{v_{[n]}a \in A^* \mid \forall n \geq 0, \forall a \in A,\ a < v_{n+1}\}$.

Proposition 2.3.3 *If v in $A^{\mathbb{N}}$ is an lsm-word, then S_v is a subshift coded by Y_v.*

Proof From their definition follows that S_v is shift-invariant and closed and that Y_v is a prefix code. Let w be in $L(S_v)$; then $w \leq v_{[n]}$ with $n = |w|$. Either $w = v_{[n]}$ and thus a prefix of a word in Y_v or $w < v_{[n]}$ and thus of the form $w = v_1 \cdots v_{n_1-1}a_1w_1$, with $a_1 < v_{n_1}$ and $w_1 \leq v_1 \cdots v_{|w_1|}$, that is $w = y_1w_1$ with y_1 in Y_v and w_1 in $L(S_v)$. Iterating this process, we see that w belongs to $F(Y_v^*)$. Conversely, let $w = (w_n)_{n\geq 1} = y_1y_2 \cdots$ be in Y_v^ω, with y_i in Y_v. Then $w < v$. For each k, $w_kw_{k+1} \cdots$ begins with a word of the form $v_{j_k}v_{j_k+1} \cdots v_{j_k+r-1}a_{j_k+r}$ with $a_{j_k+r} < v_{j_k+r}$, thus $w_kw_{k+1} \cdots < v_{j_k}v_{j_k+1} \cdots \leq v$, and thus w is in S_v. □

Proposition 2.3.4 *Let v be an lsm-word in $A^{\mathbb{N}}$. Then, the following conditions are equivalent:*

(i) *the subshift S_v is recognised by a finite Büchi automaton, and thus, is sofic;*

(ii) *the set D_v is recognised by a finite Büchi automaton;*

(iii) *the word v is eventually periodic.*

Proof [Sketch] Let $\mathcal{S}_v$ be the (infinite) automaton whose states are the $v_{[n]}$ for all n in $\mathbb{N}$, and whose transitions are $v_{[n]} \xrightarrow{v_{n+1}} v_{[n+1]}$ and $v_{[n]} \xrightarrow{a} v_{[0]}$ for every $a < v_{n+1}$. All states are final and $v_{[0]}$ is initial. This automaton $\mathcal{S}_v$ recognises $\mathrm{Pref}(Y_v^*)$, which is equal to $F(Y_v^*)$. As a Büchi automaton, $\mathcal{S}_v$ recognises S_v.

Let $\mathcal{D}_v$ be the automaton obtained from $\mathcal{S}_v$ by taking $v_{[0]}$ as unique final state. As a Büchi automaton, $\mathcal{D}_v$ recognises D_v (*cf.* Figure 2.10).

Now, the automata $\mathcal{S}_v$ and $\mathcal{D}_v$ have both finite minimal quotients, $\mathcal{S}'_v$ and $\mathcal{D}'_v$ respectively, if, and only if, v is eventually periodic. These automata $\mathcal{S}'_v$ and $\mathcal{D}'_v$ recognise the same sets of finite words and the same sets of infinite words as $\mathcal{S}_v$ and $\mathcal{D}_v$ respectively. □

Remark 2.3.5 In the case where v is eventually periodic but not purely periodic, the minimal quotients $\mathcal{S}'_v$ and $\mathcal{D}'_v$ have the same underlying graph,

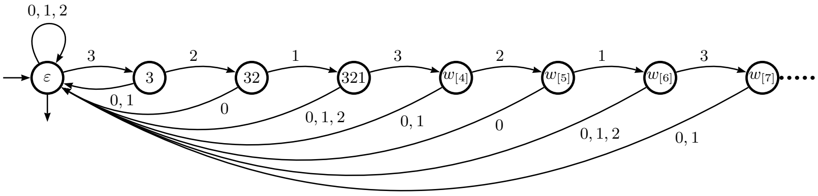
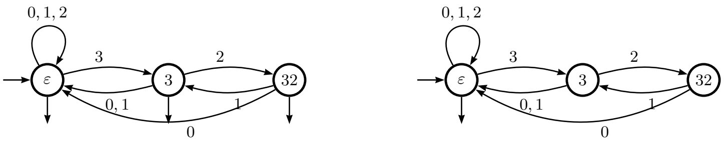


Fig. 2.10. The infinite automaton $\mathcal{D}_w$, for $w = (3\,2\,1)^\omega$.

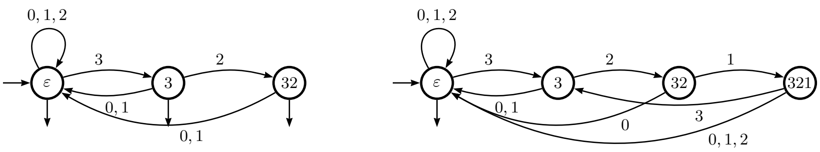
and $\mathcal{D}'_v$ can also be obtained from $\mathcal{S}'_v$ by taking the image of $v_{[0]}$ as unique final state, see Figure 2.11.

In the case where v is purely periodic, of the form $(v_1 v_2 \cdots v_p)^\omega$, the situation is slightly different and $\mathcal{S}'_v$ and $\mathcal{D}'_v$ have not the same underlying graph. However, $\mathcal{D}'_v$ can also be obtained from $\mathcal{S}'_v$ by performing an in-splitting of the image of $v_{[0]}$ and by keeping as a unique final state the one that does not belong to the loop labelled by $v_1 \cdots v_p$, see Figure 2.12.



(a) $\mathcal{S}'_v$ (b) $\mathcal{D}'_v$

Fig. 2.11. Finite automata for S_v and D_v, $v = 3\,(2\,1)^\omega$.



(a) $\mathcal{S}'_w$ (b) The minimal (finite) quotient $\mathcal{D}'_w$

Fig. 2.12. Finite automata for S_w and D_w, $w = (3\,2\,1)^\omega$.

Proposition 2.3.6 *Let v be an lsm-word in $A^{\mathbb{N}}$. Then, the subshift S_v is of finite type if, and only if, v is purely periodic.*

Proof Suppose that $v = (v_1 v_2 \cdots v_p)^\omega$ and consider the set

$$X'_v = \{v_{[n]} b \in A^* \mid 0 \leq n \leq p-1, \forall b \in A,\ b > v_{n+1}\} \ .$$

It is easy to check that $S_v = S(X'_v)$. The converse follows from the fact that v is a lsm-word. □

2.3.2 Real base

In this section we consider a base β which is a real number > 1. The reader can consult (Lothaire 2002, Chapter 7) for the proof of some results presented below, and other related results.

Any number x in the interval $[0,1)$ has a so-called *greedy β-expansion* given by a greedy algorithm (Rényi 1957): let $r_0 = x$, and, for $j \geq 1$, let $x_j = \lfloor \beta r_{j-1} \rfloor$ and $r_j = \{\beta r_{j-1}\}$. Then $x = \sum_{j=1}^{\infty} x_j \beta^{-j}$, where the x_j's are integer digits in the alphabet $A_\beta = \{0, 1, \ldots, \lceil \beta \rceil - 1\}$. The greedy β-expansion of x is denoted by $\mathsf{d}_\beta(x)$. We also write $x = {\bullet} x_1 x_2 \cdots$. The same expansion can be obtained by the *β-transformation* on $[0,1)$: let $\tau_\beta(x) = \{\beta x\}$. Then, for $j \geq 1$, $x_j = \lfloor \beta \tau_\beta^{j-1}(x) \rfloor$.

Note that, when β is an integer, we recover the classical expansion of any x in $[0,1)$ defined in Section 2.2.

The same algorithm can be applied to $x = 1$, and we obtain the so-called *β-expansion* of 1, $\mathsf{d}_\beta(1)$. Note that, if β is not an integer, then $\mathsf{d}_\beta(1)$ is an infinite word on A_β, but if β is an integer then $\mathsf{d}_\beta(1) = \beta 0^\omega$.

If $x > 1$, there exists $k \geq 0$ such that x/β^k belongs to the interval $[0,1)$. If $\mathsf{d}_\beta(x/\beta^k) = {\bullet} x_1 x_2 \cdots$, then $x = x_1 \cdots x_k {\bullet} x_{k+1} x_{k+2} \cdots$. The greedy β-expansion of x is also denoted $\langle x \rangle_\beta$. The following lemma is an immediate consequence of the greedy algorithm.

Lemma 2.3.7 *An infinite sequence of non-negative integers $(x_i)_{i \geq 1}$ is the greedy β-expansion of a real number x of $[0,1)$ (resp. of 1) if, and only if, for every $i \geq 1$ (resp. $i \geq 2$), $x_i \beta^{-i} + x_{i+1} \beta^{-i-1} + \cdots < \beta^{-i+1}$.*

As in the usual numeration systems, the order between real numbers is given by the lexicographic order on greedy β-expansions.

Proposition 2.3.8 *Let x and y be two real numbers from $[0,1)$. Then $x < y$ if, and only if, $\mathsf{d}_\beta(x) < \mathsf{d}_\beta(y)$.*

Proof Let $\mathsf{d}_\beta(x) = (x_i)_{i \geq 1}$ and let $\mathsf{d}_\beta(y) = (y_i)_{i \geq 1}$, and suppose that $\mathsf{d}_\beta(x) < \mathsf{d}_\beta(y)$. 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 $x_{k+1}\beta^{-k-1} + x_{k+2}\beta^{-k-2} + \cdots < \beta^{-k}$ by Lemma 2.3.7. The converse is immediate. □

A number may have several different writings in base β, which we call β-representations. The greedy β-expansion is characterised by the following property.

Proposition 2.3.9 *The greedy β-expansion of a real number x of $[0,1)$ is* *the greatest of all the β-representations of x with respect to the lexicographic order.*

Example 2.3.10 Let φ be the Golden Ratio $\frac{1+\sqrt{5}}{2}$. The greedy φ-expansion of $x = 3 - \sqrt{5}$ is equal to 10010^ω. Different φ-representations of x are 01110^ω, or $100(01)^\omega$ for instance.

If a representation ends in infinitely many zeros, like $u0^\omega$, the trailing zeros are omitted and the representation is said to be *finite*.

The greedy β-expansion of $x \in [0,1]$ is finite if, and only if, $\tau_\beta^i(x) = 0$ for some i, and it is eventually periodic if, and only if, the set $\{\tau_\beta^i(x) \mid i \geq 1\}$ is finite.

2.3.2.1 The β-shift

Denote by D_β the set of greedy β-expansions of numbers of $[0,1)$. It is a shift-invariant subset of $A_\beta^{\mathbb{N}}$. The *β-shift* S_β is the closure of D_β. Note that D_β and S_β have the same set of finite factors. When β is an integer, S_β is the full β-shift $A_\beta^{\mathbb{N}}$.

A finite (resp. infinite) word is said to be *β-admissible* if it is a factor of an element of D_β (resp. an element of D_β).

The greedy β-expansion of 1 plays a special role in this theory. Let $\mathsf{d}_\beta(1) = (t_n)_{n\geq 1}$ be the greedy β-expansion of 1. We define also the *quasi-greedy expansion* $\mathsf{d}^*_\beta(1)$ of 1 by: if $\mathsf{d}_\beta(1) = t_1 \cdots t_m$ is finite, then $\mathsf{d}^*_\beta(1) = (t_1 \cdots t_{m-1}(t_m - 1))^\omega$, $\mathsf{d}^*_\beta(1) = \mathsf{d}_\beta(1)$ otherwise.

Theorem 2.3.11 (Parry 1960) *Let $\beta > 1$ be a real number, and let s be an infinite sequence of non-negative integers. The sequence s belongs to D_β if and only if for all $k \geq 0$*

$$\sigma^k(s) < \mathsf{d}^*_\beta(1)$$

and s belongs to S_β if, and only if, for all $k \geq 0$

$$\sigma^k(s) \leq \mathsf{d}^*_\beta(1).$$

Definition 2.3.12 A number β such that $\mathsf{d}_\beta(1)$ is eventually periodic is called a *Parry number*. If $\mathsf{d}_\beta(1)$ is finite then β is called a *simple Parry number.*

Example 2.3.13 1. Let φ be the Golden Ratio $\frac{1+\sqrt{5}}{2}$. The expansion of 1 is finite, equal to 11.
2. Let $\theta = \frac{3+\sqrt{5}}{2}$. The expansion of 1 is eventually periodic, equal to $\mathsf{d}_\theta(1) = 21^\omega$.
3. Let $\beta = \frac{3}{2}$. Then $\mathsf{d}_\beta(1) = 101000001\cdots$ is aperiodic.

Remark 2.3.14 Note that the greedy β-expansion of 1 is never purely periodic.

As a corollary of Theorem 2.3.11 follows that $\mathsf{d}^*_\beta(1)$ is an lsm-word and $S_\beta = S_{\mathsf{d}^*_\beta(1)}$ with the notation of Definition 2.3.2. By Propositions 2.3.3, 2.3.4 and 2.3.6 follow then the well-known properties of the β-shift (established in (Ito and Takahashi 1974), (Bertrand-Mathis 1986), (Blanchard 1989)).

Theorem 2.3.15 *The β-shift S_β is a coded symbolic dynamical system which is*

(i) *sofic if, and only if, $\mathsf{d}_\beta(1)$ is eventually periodic,* i.e., *β is a Parry number*
(ii) *of finite type if, and only if, $\mathsf{d}_\beta(1)$ is finite,* i.e., *β is a simple Parry number.*

Remark 2.3.16 Since a sofic symbolic dynamical system is of finite type if, and only if, it can be recognised by a local automaton, see (Béal 1993), it follows that, when β is a simple Parry number the automaton recognising the β-shift can be chosen to be local.

Example 2.3.17 1. Let φ be the Golden Ratio $\frac{1+\sqrt{5}}{2}$. The automaton of Figure 2.14 (a) below recognising S_φ is local, because every admissible word with last letter 0 (resp. 1) arrives in state 0 (resp. 1).
2. Let $\theta = \frac{3+\sqrt{5}}{2}$. Then $\mathsf{d}_\theta(1) = 21^\omega$. The automaton of Figure 2.13 recognising S_θ is not local, since there are two different loops labelled by 1.

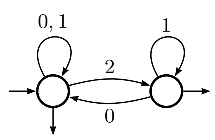
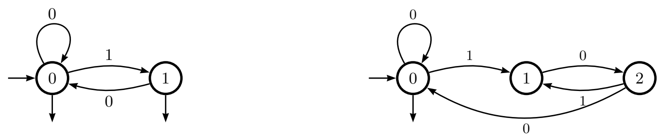


Fig. 2.13. Finite automaton for the θ-shift, $\theta = \frac{3+\sqrt{5}}{2}$.

The following result is a reformulation of Proposition 2.3.4.

Proposition 2.3.18 *The set D_β is recognisable by a finite Büchi automaton if, and only if, $\mathsf{d}_\beta(1)$ is eventually periodic.*

Example 2.3.19 Since $\mathsf{d}_\varphi(1) = 11$, the φ-shift is a system of finite type, recognised by the finite automaton of Figure 2.14 (a). The set D_φ is recognised by the finite Büchi automaton of Figure 2.14 (b).



(a) $\mathcal{S}_\varphi$ for S_φ.

(b) $\mathcal{D}_\varphi$ for D_φ.

Fig. 2.14. Finite automata for S_φ and D_φ, $\varphi = \frac{1+\sqrt{5}}{2}$.

There is an important case where the β-expansion of 1 is eventually periodic. A *Pisot number* is an algebraic integer greater than 1 such that all its Galois conjugates have modulus less than one. The natural integers and the Golden Ratio are Pisot numbers.

Theorem 2.3.20 (Schmidt 1980) *If β is a Pisot number, then every number of $\mathbb{Q}(\beta) \cap [0,1]$ has an eventually periodic β-expansion.*

As a consequence we obtain the important result, see also (Bertrand 1977).

Theorem 2.3.21 *If β is a Pisot number, then the β-shift is a sofic system.*

The *topological entropy* of a subshift $S \subseteq A^{\mathbb{N}}$ is defined as

$$h(S) = \lim_{n \to \infty} \frac{1}{n} \log(L_n(S))$$

where $L_n(S)$ denotes the number of factors of length n in S. One proof of the following well-known result using the fact that the β-shift is a coded system can be found in (Lothaire 2002, Chapter 1).

Proposition 2.3.22 *The topological entropy of the β-shift is equal to* $\log \beta$.

2.3.2.2 The (F) Property

If β is an integer, then every positive integer has a *finite* β-expansion, but this is not true in general when β is not an integer. However, it is easy to see that for the Golden Ratio φ, every positive integer has a finite expansion, for instance, $\langle 2 \rangle_\varphi = 10{\bullet}01$.

More generally, it is interesting to find numbers having this property. We recall some definitions and results from (Frougny and Solomyak 1992).

Definition 2.3.23 A number β is said to *satisfy the (F) Property* if every element of $\mathbb{Z}[\beta^{-1}] \cap [0, 1)$ has a finite greedy β-expansion.
A number β is said to *satisfy the (PF) Property* if every element of $\mathbb{N}[\beta^{-1}] \cap [0, 1)$ has a finite greedy β-expansion.

Proposition 2.3.24 *If β satisfies the (F) Property then β is a Pisot number. Moreover, the following are equivalent:*

- *β satisfies the (F) Property*
- *β satisfies the (PF) Property and $\mathsf{d}_\beta(1)$ is finite.*

There are Pisot numbers β with $\mathsf{d}_\beta(1)$ finite that do not satisfy the (F) Property, for instance the Pisot number with minimal polynomial $X^4 - 2X^3 - X - 1$. Here $\mathsf{d}_\beta(1) = 2011$ and $\langle 3 \rangle_\beta = 10{\scriptstyle\bullet}111(00012)^\omega$.

The problem of characterising Pisot numbers satisfying the (F) Property is still open. Up to now, the only families satisfying this property are the following ones.

Theorem 2.3.25 *Let $\beta > 1$ be a root of a polynomial in $\mathbb{Z}[X]$ of the form $M(X) = X^g - b_1 X^{g-1} - b_2 X^{g-2} - \cdots - b_g$. If one of the following properties holds, then β satisfies the (F) Property:*
(i) $b_1 \geq b_2 \geq \cdots \geq b_g > 0$,
(ii) $b_i \geq 0$ *for* $1 \leq i \leq g$ *and* $b_1 > \sum_{i=2}^{g} b_i$.

Part (i) is from (Frougny and Solomyak 1992) and Part (ii) from (Hollander 1996).

Cubic Pisot units satisfying (F) are characterised by the following.

Theorem 2.3.26 (Akiyama 2000) *A cubic Pisot unit β satisfies the (F) Property if, and only if, it is a root of the polynomial $M(X) = X^3 - aX^2 - bX - 1$ of $\mathbb{Z}[X]$ with $a \geq 0$ and $-1 \leq b \leq a + 1$.*

A family of Pisot numbers satisfying (PF) is the following one.

Theorem 2.3.27 *Let β be such that $\mathsf{d}_\beta(1) = t_1 t_2 \cdots t_m (t_{m+1})^\omega$ with $t_1 \geq t_2 \geq \cdots \geq t_m > t_{m+1} > 0$. Then β is a Pisot number which satisfies the (PF) Property.*

Corollary 2.3.28 *Every quadratic Pisot number satisfies the (PF) Property.*

Example 2.3.29 The number $\theta = \frac{3+\sqrt{5}}{2}$, with $\mathsf{d}_\theta = 21^\omega$ satisfies the (PF) Property, but not the (F) Property, since $\langle \theta - 1 \rangle_\theta = 1{\scriptstyle\bullet}1^\omega$.

2.3.2.3 Digit-set conversion and normalisation

Let C be an arbitrary alphabet of digits. The *normalisation* $\nu_{\beta,C}$ in base β on C is the partial function which maps any β-representation on C of a given number of $[0,1)$ onto the greedy β-expansion of that number:

$$\nu_{\beta,C}\colon C^{\mathbb{N}} \to A_\beta^{\mathbb{N}} \qquad (c_i)_{i\geq 1} \mapsto \mathsf{d}_\beta(\sum_{i\geq 1} c_i\beta^{-i}) \ .$$

The function $\nu_{\beta,C}$ is partial since as C may contain negative digits, a word of C^* may represent a negative number, which has no β-expansion. Note that, as for the integer bases, addition and multiplication by a positive integer constant K are particular instances of normalisation. Addition consists in normalising on the alphabet $\{0,\ldots,2(\lceil\beta\rceil-1)\}$, and multiplication by K on the alphabet $\{0,\ldots,K(\lceil\beta\rceil-1)\}$.

We first adapt the notions of zero automaton and digit-conversion transducers given in Section 2.2.3 for integer base to the non-integer base β.

Zero automaton The evaluator $\mathcal{Z}_\beta$ in base β is defined as in integer base but for the set of states which is $\mathbb{Z}[\beta]$. The initial state is 0 and the transitions are of the form:

$$\forall s,t \in \mathbb{Z}[\beta] \qquad \forall a \in \mathbb{Z} \qquad s \xrightarrow[\mathcal{Z}_\beta]{a} t \quad \text{if, and only if,} \quad t = \beta\, s + a \ . \qquad (2.11)$$

Let $B_d = \{-d,\ldots,d\}$ where d is a positive integer, $d \geq \lfloor\beta\rfloor$.

Proposition 2.3.30 *An infinite word z in $B_d^{\mathbb{N}}$ has value* 0 *in base β if, and only if, it is accepted by the Büchi automaton $\mathcal{Z}_{\beta,d} = (\,Q_d, B_d, E, \{0\}, Q_d\,)$ where the transitions in E are those defined by (2.11) and $Q_d = \mathbb{Z}[\beta] \cap [-\frac{d}{\beta-1}, \frac{d}{\beta-1}]$.*

Proof By the definition of $\mathcal{Z}_{\beta,d}$, every infinite word z that labels an infinite computation in $\mathcal{Z}_{\beta,d}$ is accepted by $\mathcal{Z}_{\beta,d}$. For every $n \geq 1$, $|\pi_p\,(z_1\cdots z_n)| \leq \frac{d}{\beta-1}$ and then $\pi_\beta\,(\centerdot z) = \lim_{n\to+\infty} \frac{1}{\beta^n}\,\pi_p\,(z_1\,z_2\cdots z_n) = 0$.

Conversely, let z in $B_d^{\mathbb{N}}$ which does not label a computation in $\mathcal{Z}_{\beta,d}$, that is, there exists a prefix w of z such that

$$0 \xrightarrow[\mathcal{Z}_{\beta,d}]{w} t \qquad \text{with} \qquad t > d/(\beta-1) \ .$$

We have

$$\pi_p\,(\centerdot z) \geq \pi_p\left(\centerdot w\,\overline{d}^{\omega}\right) = \frac{1}{\beta^{|w|}}\left(t - \frac{d}{\beta-1}\right) > 0 \,.$$

(The case $t < -d/(\beta-1)$ is identical.) □

This automaton is called the *zero automaton* in base β over the alphabet B_d. It is not finite in general. Our aim is now to prove the following result.

Theorem 2.3.31 *The following conditions are equivalent:*
(i) *the zero automaton $\mathcal{Z}_{\beta,d}$ is finite for every $d \geq \lfloor\beta\rfloor$*
(ii) *the zero automaton $\mathcal{Z}_{\beta,d}$ is finite for one $d \geq \lfloor\beta\rfloor + 1$*
(iii) *β is a Pisot number.*

The proof relies on the following statements.

Lemma 2.3.32 *If $\mathcal{Z}_{\beta,d}$ is finite, then β is an algebraic integer.*

Proof Let $\mathsf{d}_\beta(1) = (t_i)_{i\geq 1}$. Then $(-1)t_1t_2\cdots$ is the label of a path in $\mathcal{Z}_{\beta,d}$, and there exist n and p such that the states $\pi_\beta((-1)t_1t_2\cdots t_n)$ and $\pi_\beta((-1)t_1t_2\cdots t_n\cdots t_{n+p})$ are the same. □

We now suppose that β is an algebraic integer with minimal polynomial M_β of degree g. Denote $\beta_1 = \beta$, β_2, ..., β_g the roots of M_β. On the discrete lattice of rank g, $\mathbb{Z}[X]/(M_\beta) \simeq \mathbb{Z}[\beta]$, a norm is defined as

$$||P(X)|| = \max_{1\leq i\leq g} |P(\beta_i)|. \tag{2.12}$$

Proposition 2.3.33 *If β is a Pisot number, then $\mathcal{Z}_{\beta,d}$ is finite for every $d \geq \lfloor\beta\rfloor$.*

Proof Every state s in Q_d is associated with the label of the shortest path $z_1z_2\cdots z_n$ from 0 to s in the automaton. Thus $s = s(\beta) = z_1\beta^{n-1} + \cdots + z_n$, with $s(X)$ in $\mathbb{Z}[X]/(M_\beta)$ and $|s| = |s(\beta)| \leq \frac{d}{\beta-1}$. For every conjugate β_i with $|\beta_i| < 1$, we have $|s(\beta_i)| \leq \frac{d}{1-|\beta_i|}$. Since β is Pisot, this is true for $2 \leq i \leq g$. Thus every state of Q_d is bounded in norm, and so there is only a finite number of them. □

Example 2.3.34 The zero automaton on $\{-1, 0, 1\}$ for $\varphi = \frac{1+\sqrt{5}}{2}$ is drawn in Figure 2.15.

Part (i) implies (iii) of Theorem 2.3.31 is proved in (Berend and Frougny 1994).

Proposition 2.3.35 *If the zero automaton $\mathcal{Z}_{\beta,d}$ is finite for every $d \geq \lfloor\beta\rfloor$, then β is a Pisot number.*

The core of Proposition 2.3.35 consists in using, with techniques of complex analysis, the following lemma *for every integer d*.

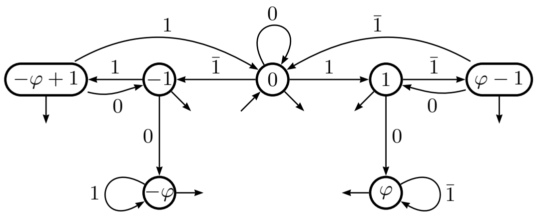


Fig. 2.15. Finite zero automaton $\mathcal{Z}_{\varphi,1}$, $\varphi = \frac{1+\sqrt{5}}{2}$.

Lemma 2.3.36 *If the automaton $\mathcal{Z}_{\beta,d}$ is finite, then for every conjugate β_i with $|\beta_i| > 1$, if $s = s(\beta)$ belongs to Q_d then $|s(\beta_i)| \leq \frac{d}{|\beta_i|-1}$.*

Proof Let $z_1 z_2 \cdots$ be the label of a path recognised by $\mathcal{Z}_{\beta,d}$ with origin 0. Since Q_d is finite there exist n and p such that $s = s(\beta) = z_1\beta^{n-1} + \cdots + z_n = z_1\beta^{n+p-1} + \cdots + z_{n+p}$. Thus for every conjugate β_i with $|\beta_i| > 1$, $z_1\beta_i^{n-1} + \cdots + z_n = z_1\beta_i^{n+p-1} + \cdots + z_{n+p} = \beta_i^p(z_1\beta_i^{n-1} + \cdots + z_n) + z_{n+1}\beta_i^{p-1} + \cdots + z_{n+p}$, thus

$$|z_1\beta_i^{n-1} + \cdots + z_n| \leq \frac{d}{|\beta_i|^p - 1}\frac{|\beta_i|^p - 1}{|\beta_i| - 1} = \frac{d}{|\beta_i| - 1}.$$

□

Example 2.3.37 Take β the root > 1 of the polynomial $X^4 - 2X^3 - 2X^2 - 2$. Then $\mathsf{d}_\beta(1) = 2202$ and β is a simple Parry number, but it is not a Pisot number, since there is another root $\alpha \approx -1.134186$. By a direct computation it can be shown that the path of label $\bar{1}221\bar{1}1\bar{2}201$ in $\mathcal{Z}_{\beta,2}$ with origin 0 leads to a state $s = s(\beta)$ such that $s(\alpha) > 2/(|\alpha|-1)$. Lemma 2.3.36 implies that, for every $d \geq 2$, the set of words of $B_d^{\mathbb{N}}$ having value 0 is not recognisable by a finite automaton.

Normalisation Take two alphabets of integers C and A. Let $d = \max(|c - a|)$ for c in C and a in A, and let $B_d = \{-d, \ldots, d\}$ as above. As in Section 2.2.2.1, one constructs from the zero automaton $\mathcal{Z}_{\beta,d}$ a *digit-conversion transducer* or *converter* $\mathcal{C}_\beta(C \times A)$. The transitions are defined by

$$s \xrightarrow[\mathcal{C}_\beta(C\times A)]{c|a} t \quad \text{if, and only if,} \quad s \xrightarrow[\mathcal{Z}_{\beta,d}]{c-a} t\ .$$

Thus one obtains the following proposition.

Proposition 2.3.38 *The converter $\mathcal{C}_\beta(C \times A)$ recognises the set*

$$\{(x,y) \in C^{\mathbb{N}} \times A^{\mathbb{N}} \mid \pi_\beta(x) = \pi_\beta(y)\}.$$

If β is a Pisot number, then $\mathcal{C}_\beta(C \times A)$ is finite.

Theorem 2.3.39 (Frougny 1992) *If β is a Pisot number, then normalisation in base β on any alphabet C is realisable by a finite letter-to-letter transducer.*

Proof Since β is a Pisot number the automaton $\mathcal{D}_\beta$ recognising D_β is finite by Proposition 2.3.18. The normaliser $\mathcal{N}_\beta(C)$ is obtained as the composition of $\mathcal{C}_\beta(C \times A_\beta)$ with the transducer which realises the intersection with D_β. □

It is easy to check that for any fixed digit alphabet C, normalisation in base β on C is a *bounded-length discrepancy function* (see Section 2.6.3). It follows then, that if normalisation in base β on an alphabet C is realisable by a finite transducer, it is realisable by a finite *letter-to-letter* transducer, and then that the *zero automaton* $\mathcal{Z}_{\beta,d}$ is finite for $d = \max(|c - a|)$, for c in C and a in A_β.

The following result allows to prove that (ii) implies (i) in Theorem 2.3.31.

Proposition 2.3.40 (Frougny and Sakarovitch 1999) *If normalisation in base β on the alphabet $A'_\beta = \{0, \ldots, \lfloor\beta\rfloor, \lfloor\beta\rfloor + 1\}$ is realisable by a finite transducer, then normalisation in base β is realisable by a finite transducer on any alphabet.*

In view of Example 2.3.37, we set the following conjecture.

Conjecture 2.3.41 If the zero automaton $\mathcal{Z}_{\beta,d}$ is finite for $d = \lfloor\beta\rfloor$ then β is a Pisot number.

2.3.3 U-systems

We now consider another generalisation of the integer base numeration systems which only allows to represent natural integers. The base is replaced by a *basis* which is an infinite sequence of positive integers (also called *scale*) and which plays the role of the sequence of the powers of the integer base. The classical example is the Fibonacci numeration system. These systems have been first defined and studied in full generality in (Fraenkel 1985).

We shall see that, under mild and natural hypotheses, the basis is associated with a real number β, as the Fibonacci numeration system is associated with the Golden Ratio. Then, many of the properties established for numeration in base β transfer to the U-system, but the situation is far more intricate. In fact, even in the simple case where the β is an integer, the language of the numeration system may or may not be a rational language according to the initial conditions (see Example 2.3.58).

2.3.3.1 Rationality of U-expansions

A *basis* is a strictly increasing sequence of integers $U = (u_n)_{n\geq 0}$ with $u_0 = 1$. A *representation in the system U* — or a *U-representation* — of a non-negative 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 non-negative integer N, one is distinguished and called the *U-expansion* of N. It is also called the *greedy* U-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 U-expansion of N is denoted by $\langle N\rangle_U$.

By convention the U-expansion of 0 is the empty word ε. Under the hypothesis that the ratio u_{n+1}/u_n is bounded by a constant as n tends to infinity, the digits of the U-expansion of any positive integer N are bounded and contained in a *canonical* finite alphabet A_U associated with U.

Example 2.3.42 Let $F = (F_n)_{n\geq 0}$ be the sequence of Fibonacci numbers, $F = \{1, 2, 3, 5, \ldots\}$. The canonical alphabet is equal to $\{0, 1\}$. The F-expansion of the number 11 is 10100, another F-representation is 10011.

The U-expansions are characterised by the following.

Lemma 2.3.43 *The word $d_k \cdots d_0$, where each d_i, for $k \geq i \geq 0$, is a non-negative integer and $d_k \neq 0$, is the U-expansion of some positive integer if, and only if, for each i, $d_i u_i + \cdots + d_0 u_0 < u_{i+1}$.*

Proposition 2.3.44 *The U-expansion of an integer is the greatest in the radix order of all the U-representations of that integer.*

Proof Let $v = d_k \cdots d_0$ be the greedy U-representation of N, and let $w =$

$w_j \cdots w_0$ be another representation. Since $u_k \le N < u_{k+1}$, then $k \ge j$. If $k > j$, then $v \succ w$. If $k = j$, suppose $v \prec w$. Thus there exist i, $k \ge i \ge 0$, 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 $d_i u_i + \cdots + d_0 u_0 \le (w_i - 1)u_i + d_{i-1}u_{i-1} + \cdots + d_0 u_0$, so $u_i + w_{i-1}u_{i-1} + \cdots + w_0 u_0 \le d_{i-1}u_{i-1} + \cdots + d_0 u_0 < u_i$ since v is greedy, a contradiction. □

As for the beta-expansions, the order between integers is given by the radix order on their U-expansions.

Proposition 2.3.45 *Let M and N be two positive integers. Then $M < N$ if, and only if, $\langle M\rangle_U \prec \langle N\rangle_U$.*

The set of U-expansions of all the non-negative integers is denoted by $L(U)$.

Example 2.3.46 Let F be the sequence of Fibonacci numbers. Then $L(F)$ is the set of words without the factor 11, and not beginning with a 0:

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

When the sequence U satisfies a linear recurrence with integral coefficients, that is, when U is a linear recurrent sequence, we say that U defines a *linear numeration system* or that U is a *linear recurrent basis.*

Proposition 2.3.47 (Shallit 1994) *Let U be a basis. If $L(U)$ is a rational language, then U is a linear recurrent sequence.*

Proof (Loraud 1995) Let ℓ_n (resp. k_n) be the number of words of length n in $L(U)$ (resp. in $0^*L(U)$). Since a word in $L(U)$ does not begin with a 0, we have $k_n = \ell_0 + \ell_1 + \cdots + \ell_n$ for every n and then $k_n = u_n$ by Lemma 2.3.43. If $L(U)$ is a rational language, so is $0^*L(U)$ and $U = (u_n)_{n\ge 0}$ is a linear recurrent sequence, a classical result in automata theory (see Theorem 2.6.2). □

The results on β-expansions transfer to the U-expansions when U satisfies some conditions. The results below were established in (Hollander 1998). A linear recurrent basis $U = (u_n)_{n\ge 0}$ is said to satisfy the *dominant root condition* if $\lim_{n\to\infty} u_{n+1}/u_n = \beta$ for some $\beta > 1$.

Lemma 2.3.48 *Let U be a linear recurrent basis, with characteristic polynomial $C_U(X)$. Assume that $C_U(X)$ has a unique root β, possibly with multiplicity, of maximum modulus, and assume that β is real. Then U satisfies the dominant root condition for β.*

For a language L, we denote by $\mathsf{Maxlg}\,(L)$ the set of words of L which have no greater word of the same length in L in the radix order. It is known that if L is rational, so is $\mathsf{Maxlg}\,(L)$ (Proposition 2.6.4). The following is also a classical result of automata theory (see Proposition 2.6.3).

Lemma 2.3.49 *Let M be a language which contains exactly one word of every length. If M is rational, then there exist an integer p, a finite family of words x_i, y_i, and z_i, with $|y_i| = p$, and a finite set of words M_0 such that*

$$M = \bigcup_{i=1}^{i=p} x_i y_i^* z_i \cup M_0 \qquad (2.13)$$

where the union is disjoint.

For every n in $\mathbb{N}$, let m_n be the word of length n of $L(U)$ which is maximum in the radix order : $m_n = \langle u_n - 1 \rangle_U$, and $\mathsf{Maxlg}\,(L(U)) = \cup_{n \geq 0} m_n$. Note that the empty word $\varepsilon = m_0$ belongs to M. The following result is similar to the lexicographical characterisation of the β-shift given by Parry, see Theorem 2.3.11.

Proposition 2.3.50 *The following holds:*

$$L(U) = \cup_{n \geq 0} \{ v \in A_U^n \mid \text{every suffix of length } i \leq n \text{ of } v \text{ is } \preceq m_i \} \ .$$

Using the previous result, one can construct a finite automaton similar to the one defined for the β-shift.

Proposition 2.3.51 *If $\mathsf{Maxlg}\,(L(U))$ is rational, so is $L(U)$.*

The following lemma shows that the β-expansion of 1 governs the U-expansions when β is the dominant root of U.

Lemma 2.3.52 *Suppose that U has a dominant root β, and let $\mathsf{d}_\beta(1) = (t_n)_{n \geq 1}$. Then for each j there exist n and a word w_j of length $n - j$ such that $m_n = \langle u_n - 1 \rangle_U = t_1 \cdots t_j w_j$.*

Proposition 2.3.53 (Hollander 1998) *Let U be a linear recurrent basis with dominant root β. If $L(U)$ is rational then β is a Parry number.*

Proof [Sketch] If $L(U)$ is rational, then $\mathsf{Maxlg}\,(L(U))$ is of the form (2.13). By Lemma 2.3.52, for each j, there exist an n and a word w_j of length $n-j$ such that $m_n = t_1 \cdots t_j w_j$. Combining the two properties, it follows that $\mathsf{d}_\beta(1)$ must be finite or eventually periodic. □

From now on β is a Parry number. In this case, there is a polynomial satisfied by β which arises from the greedy expansion of 1. If $\mathsf{d}_\beta(1)$ is finite, $\mathsf{d}_\beta(1) = t_1 \cdots t_m$, then set

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

If $\mathsf{d}_\beta(1)$ is infinite eventually periodic, $\mathsf{d}_\beta(1) = t_1 \cdots t_m (t_{m+1} \cdots t_{m+p})^\omega$, with m and p minimal, then set

$$G_\beta(X) = X^{m+p} - \sum_{i=1}^{m+p} t_i X^{m+p-i} - X^m + \sum_{i=1}^{m} t_i X^{m-i}.$$

Such a polynomial is called the *canonical beta-polynomial* for β. Note that in general G_β is not equal to the minimal polynomial of β but is a multiple of it.

Example 2.3.54 Let η be the root > 1 of the polynomial $M_\eta = X^3 - X - 1$. This number is the smallest Pisot number. Since $\mathsf{d}_\eta(1) = 10001$, the canonical beta-polynomial is $G_\eta = X^5 - X^4 - 1$.

We will need a slightly more general definition. If $\mathsf{d}_\beta(1)$ is infinite eventually periodic, $\mathsf{d}_\beta(1) = t_1 \cdots t_m (t_{m+1} \cdots t_{m+p})^\omega$, with m and p minimal, set $r = p$. If $\mathsf{d}_\beta(1)$ is finite, $\mathsf{d}_\beta(1) = t_1 \cdots t_m$, then set $r = m$. An *extended beta-polynomial* is a polynomial of the form

$$H_\beta(X) = G_\beta(X)(1 + X^r + \cdots + X^{rk})X^n$$

for k in $\mathbb{N}$ and n in $\mathbb{N}$.

When $\mathsf{d}_\beta(1)$ is infinite an extended beta-polynomial corresponds to taking m and p not minimal. When $\mathsf{d}_\beta(1)$ is finite an extended beta-polynomial corresponds to taking improper expansions of 1 of the form $(t_1 \cdots t_{m-1}(t_m - 1))^k t_1 \cdots t_m$, and to any writing of $\mathsf{d}^*_\beta(1)$ as uv^ω.

Example 2.3.55 The canonical beta-polynomial for the Golden Ratio is $G_\varphi = X^2 - X - 1$. The polynomial $X^4 - X^3 - X - 1 = G_\varphi(1 + X^2)$ is an extended beta-polynomial corresponding to the improper expansion 1011 of 1.

Lemma 2.3.56 *Let $H_\beta(X)$ be an extended polynomial for $\beta > 1$, and assume that $H_\beta(X) = C_U(X)$. Then U satisfies the dominant root condition for β, and β is a simple root of $H_\beta(X)$.*

The following theorem shows that the situation for linear numeration systems is much more complicated than for the β-shift.

Theorem 2.3.57 (Hollander 1998) *Let U be a linear recurrent basis whose dominant root β is a Parry number.*

- *If $\mathsf{d}_\beta(1)$ is infinite eventually periodic, then $L(U)$ is rational if, and only if, U satisfies an extended beta-polynomial for β.*
- *If $\mathsf{d}_\beta(1)$ is finite, of length m, then: if U satisfies an extended beta-polynomial for β then $L(U)$ is rational; and conversely if $L(U)$ is rational, then U satisfies either an extended beta-polynomial for β, $H_\beta(X)$, or a polynomial of the form $(X^m - 1)H_\beta(X)$.*

In the finite case, rationality indeed depends on initial conditions.

Example 2.3.58 (Hollander 1998) Take $u_n = 4u_{n-1} - 3u_{n-2}$ with $C_U(X) = (X-1)(X-3)$. The dominant root is $\beta = 3$.
Take $u_0 = 1$ and $u_1 = 4$. Then $u_n = 3u_{n-1} + 1$, and so the language of maximal words is $M = 30^*$, and $L(U)$ is rational.
Take $u_0 = 1$ and $u_1 = 2$. Then $u_n = 3u_{n-1} - 1 = (3^n + 1)/2$, and $A_U = \{0, 1, 2\}$. Let k be the largest integer such that m_n begins with k digits 2. Thus k is the largest integer such that

$$\frac{3^n+1}{2} > 2(\frac{3^{n-1}+1}{2} + \cdots + \frac{3^{n-k}+1}{2})$$

that is, $3^{n-k} + 1 > 2n$, and $3^{n-k} + 1 + 2(n-k) > 2n$. As $n \to \infty$, both $k \to \infty$ and $n - k \to \infty$, and $L(U)$ is not rational.

We now define a numeration system canonically associated with a real number β in a way that gives the numeration system the same dynamical properties as the β-shift.

Definition 2.3.59 The *numeration system associated with β* is defined by the basis $U_\beta = (u_n)_{n\geq 0}$ as follows:
If $\mathsf{d}_\beta(1)$ is finite, $\mathsf{d}_\beta(1) = t_1 \cdots t_m$, set

$$u_n = t_1 u_{n-1} + \cdots + t_m u_{n-m} \text{ for } n \geq m,$$

$$u_0 = 1, \text{ and for } 1 \leq i \leq m-1, \ u_i = t_1 u_{i-1} + \cdots + t_i u_0 + 1.$$

If $\mathsf{d}_\beta(1) = (t_i)_{i\geq 1}$ is infinite, set

$$u_n = t_1 u_{n-1} + t_2 u_{n-2} + \cdots + t_n u_0 + 1, \text{for } n \geq 1, \ u_0 = 1.$$

If $\mathsf{d}_\beta(1)$ is finite or eventually periodic, the sequence U_β is linearly recurrent, and its characteristic polynomial is thus the canonical beta-polynomial of β.

Example 2.3.60 The linear numeration system associated with the Golden Ratio is the Fibonacci numeration system.

Proposition 2.3.61 (Bertrand-Mathis 1989) *Let $\beta > 1$ be a real number. Then $L(U_\beta) = L(S_\beta)$.*

Example 2.3.62 Take the Pisot number $\theta = \frac{3+\sqrt{5}}{2}$, then $\mathsf{d}_\theta(1) = 21^\omega$, and $U_\theta = \{1, 3, 8, 21, 55, 144, 377, \ldots\}$ is the sequence of Fibonacci numbers of even index. The beta-polynomial $G_\theta(X) = X^2 - 3X + 1$ is equal to the minimal polynomial of θ. The set $L(U_\theta)$ is recognisable by the finite automaton of Figure 2.13 above, which recognises the θ-shift.

On the other hand, consider the linear recurrent basis $R_\theta = \{1, 2, 6, 17, 46, 122, 321, \ldots\}$ defined by $r_n = 4r_{n-1} - 4r_{n-2} + r_{n-3}$ for $n \geq 3$, $r_0 = 1$, $r_1 = 2$, $r_2 = 6$. Then θ is the dominant root of R_θ; the characteristic polynomial of R_θ is equal to $(X-1)(X^2-3X+1)$. By showing that R_θ does not satisfy an extended beta-polynomial, Theorem 2.3.57 implies that the set $L(R_\theta)$ is not recognisable by a finite automaton. A direct combinatorial proof can be found in (Frougny 2002).

2.3.3.2 Normalisation

Let C be an arbitrary alphabet of digits. The *normalisation* $\nu_{U,C}$ in basis U on C is the partial function which maps any U-representation on C of any positive integer n onto the U-expansion of n:

$$\nu_{U,C} \colon C^* \to {A_U}^* \qquad\qquad c_k \cdots c_0 \mapsto \langle \sum_{i=0}^{k} c_i u_i \rangle_U \ .$$

As for beta-expansions, one can define the zero automaton and the converter for a U-system. Let us say that U is a *Pisot basis* if U is a linear recurrent basis whose characteristic polynomial is the minimal polynomial of a Pisot number. It follows from Theorem 2.3.57 that if U is a Pisot basis, then $L(U)$ is rational.

Proposition 2.3.63 *Let U be a Pisot basis. Then, for any alphabet of digits, the zero automaton and the converter in the system U are finite.*

Example 2.3.64 The zero automaton in the Fibonacci numeration system and for the alphabet $\{-1, 0, 1\}$ is the automaton of Figure 2.15, without the states labelled φ and $-\varphi$, and with 0 as unique final state.

By a similar construction to the one exposed in Section 2.3.2.3, we obtain the following result.

Proposition 2.3.65 (Frougny and Solomyak 1996) *Let U be a Pisot basis. For any digit alphabet C, the normalisation $\nu_{U,C}$ is realisable by a finite letter-to-letter transducer.*

Example 2.3.66 Normalisation on $\{0, 1\}$ in the Fibonacci numeration system consists in replacing every factor 011 by 100. The finite transducer realising normalisation is shown in Figure 2.16. For sake of simplicity, this normaliser does not accept words which begin with 11.

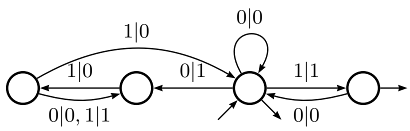


Fig. 2.16. Finite normaliser on $\{0, 1\}$ for the Fibonacci numeration system.

2.3.3.3 Successor function

The successor function is usually and canonically defined on $\mathbb{N}$: $n \mapsto n+1$. What we call 'successor function' here is of course the same function, but lifted at the level of expansions in the system we consider. Successor function is a special case of addition and thus of normalisation. When the latter is a rational function, or even realised by a letter-to-letter (right sequential) transducer, so is the successor function, without any ado. But this successor function is such a special case that we can give statements under weaker hypotheses than the ones that assure the rationality of normalisation.

Let U be a basis and, as above, $L = L(U)$ the set of U-expansions. The successor function in the basis U is thus the function Succ_L which maps every word of L onto its successor in L in the radix order. If L is a rational language, it is thus known that Succ_L is a synchronous relation, even a (left and right) letter-to-letter rational relation, even a piecewise right sequential function (see Proposition 2.6.7, Corollary 2.6.11, Proposition 2.6.14 in Section 2.6). From Proposition 2.3.61 above, we then have the following consequence of these results.

Proposition 2.3.67 *Let β be a Parry number and U_β the linear numeration system associated with β. The successor function in the numeration system U_β is realisable by a letter-to-letter transducer.*

In general, the successor function in a linear numeration system is *not co-sequential*, as shown by the next example.

Example 2.3.68 Take the Pisot number $\theta = \frac{3+\sqrt{5}}{2}$, see Example 2.3.62. By the foregoing, $L(U_\theta)$ is rational, and $\mathrm{Succ}_{L(U_\theta)}$ is realisable by a finite transducer. For every n, the words $v_n = 021^n$ and $w_n = 01^{n+1}$ are in $L(U_\theta)$. We have $\mathrm{Succ}_{L(U_\theta)}(v_n) = 10^{n+1}$ and $\mathrm{Succ}_{L(U_\theta)}(w_n) = 01^n2$.

The *suffix distance* $\mathrm{d}_s(x, y)$ of two words x and y is

$$\mathrm{d}_s(x, y) = |x| + |y| - 2\,|x \wedge_s y|$$

where $x \wedge_s y$ is the *longest common suffix* of x and y. It comes $\mathrm{d}_s(v_n, w_n) = 4$ and $\mathrm{d}_s\big(\mathrm{Succ}_{L(U_\theta)}(v_n), \mathrm{Succ}_{L(U_\theta)}(w_n)\big) = 2(n+2)$. By the characterisation of co-sequential functions due to Choffrut (see Theorem 2.6.13), $\mathrm{Succ}_{L(U_\theta)}$is not co-sequential.

The conditions under which the successor function in a linear numeration system is co-sequential are indeed completely determined.

Theorem 2.3.69 (Frougny 1997) *Let U be a numeration system such that $L(U)$ is rational. The successor function in the system U is co-sequential if, and only if, the set* $\mathsf{Maxlg}(L(U))$ *is of the form*

$$\mathsf{Maxlg}(L(U)) = \bigcup_{i=1}^{i=p} y_i^* z_i \cup M_0 \tag{2.14}$$

where M_0 is finite, $|y_i| = p$ and the union is disjoint.

In the case of linear numeration system with dominant root, the previous result can be refined.

Theorem 2.3.70 *Let U be a linear recurrent basis whose dominant root β is a Parry number. Then the successor function in the system U is co-sequential if, and only if, the following conditions hold:*
(i) *β is a simple Parry number;*
(ii) *U satisfies the canonical beta-polynomial for β.*

Example 2.3.71 The successor function in the Fibonacci numeration system is realised by a finite right sequential transducer, see Figure 2.17.

2.3.4 Base changing

As far as comparison, or conversion, of the expansions of numbers in different real bases is concerned, the situation is very similar to the one with integer bases. In the background, and for the negative part, stand the generalisations of Cobham's Theorem — we choose the one due to Bès. If U

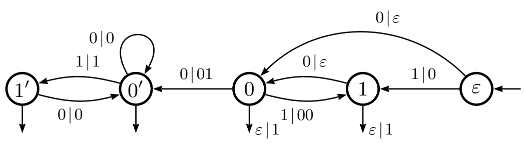


Fig. 2.17. Finite right sequential transducer for the successor function in the Fibonacci numeration system.

is a basis, a set of natural integers is said to be U*-recognisable* if the set of the U-expansions of its elements is a rational set.

Theorem 2.3.72 (Bès 2000) *Let U and V be two Pisot basis, associated with two multiplicatively independent Pisot numbers. A set X of positive integers is both U- and V-recognisable if, and only if, it is recognisable.*

From this result follows that the conversion between the expansions in two such linear numeration systems U and V cannot be realised by a finite transducer.

2.3.4.1 Multiplicatively dependent bases

We now consider the case where the bases β and γ are multiplicatively dependent. When β and γ are integers, then the conversion from base β to base γ is realisable by a finite right sequential transducer (Proposition 2.2.17).

Proposition 2.3.73 *Let β and γ be two multiplicatively dependent Pisot numbers. The conversion from base γ to base β is realisable by a finite transducer.*

Proof Set $\delta = \beta^k = \gamma^\ell$ and let $(x_i)_{i\geq 1} = \mathsf{d}_\delta(x)$ where x is in $[0, 1)$. Then $0^{k-1}x_1 0^{k-1}x_2 0^{k-1}\cdots$ is a β-representation of x on the alphabet A_δ. Since β is Pisot, normalisation in base β on the alphabet A_δ is realisable by a finite transducer. Similarly the conversion from base δ to base γ is realisable by a finite transducer. By composition and inversion of relations realised by finite transducers, the result follows (see Section 2.6). □

Now, as in Theorem 2.3.72, we consider linear numeration systems. We first suppose that the two systems have the same characteristic polynomial.

Proposition 2.3.74 *Let U and V be two Pisot basis, associated with the* *same Pisot number, but defined by different initial conditions. The conversion from a V-representation of a positive integer to the U-expansion of that integer is computable by a finite transducer.*

Proof By Proposition 2.3.65 normalisation in the system U is computable by a finite transducer on any alphabet. Suppose that M_β, the minimal polynomial of β, has degree g. The family $\{u_n, u_{n+1}, \ldots, u_{n+g-1} \mid n \geq 0\}$ is free, because its annihilator polynomial is M_β. Since U and V have the same characteristic polynomial, it is known from standard results of linear algebra that there exist rational constants λ_i such that, for each $n \geq 0$, $v_n = \lambda_1 u_{n+g-1} + \cdots + \lambda_g u_n$. One can assume that the λ_i's are all of the form p_i/q where the p_i's belong to $\mathbb{Z}$ and q belongs to $\mathbb{N}$, $q \neq 0$. Let N be a positive integer and consider a V-representation $c_j \cdots c_0$ of N, where the c_i's are in an alphabet of digits $B \supseteq A_V$. Then $qN = c_j q v_j + \cdots + c_0 q v_0$. Since for $n \geq 0$, $qv_n = p_1 u_{n+g-1} + \cdots + p_g u_n$, we get that qN is of the form $qN = d_{j+g-1} u_{j+g-1} + \cdots + d_0 u_0$. Since each digit d_i, for $0 \leq i \leq j+g-1$, is a linear combination of q, p_1, $\ldots$, p_g, and the c_i's, we get that d_i is an element of a finite alphabet of digits $D \supset A_U$. By assumption, $\nu_{U,D}$ is computable by a finite automaton. It remains to show that the function which maps $\nu_{U,D}(d_{j+g-1} \cdots d_0) =< qN >_U$ onto $< N >_U$ is computable by a finite automaton, and this is due to the fact that it is the inverse of the multiplication by the natural q, which is computable by a finite automaton in the system U. □

Definition 2.3.75 Let β be a Pisot number of degree g, and denote $\beta_1 = \beta, \ldots, \beta_g$ the roots of the minimal polynomial M_β. The *Lucas-like numeration system* associated with β is the system defined by the basis $V_\beta = (v_n)_{n \geq 0}$ where

$$v_0 = 1, \text{ and for } n \geq 1, \; v_n = \beta_1^n + \cdots + \beta_g^n.$$

The characteristic polynomial of V_β is equal to M_β.

This terminology comes from the fact that for the Golden Ratio φ, V_φ is the sequence of Lucas numbers. On the other hand, the numeration system U_β associated with β in Definition 2.3.59 is a *Fibonacci-like* numeration system, since, for the Golden Ratio φ, U_φ is the sequence of Fibonacci numbers.

Proposition 2.3.76 *Let β be a Pisot number, and let $\delta = \beta^k$. The conversion from the Lucas-like numeration system V_δ to the the Lucas-like numeration system V_β is realisable by a finite transducer.*

Proof The conjugates of δ are of the form $\delta_i = \beta_i^k$, for $2 \le i \le g$. Set $V_\delta = (w_n)_{n \ge 0}$ with $w_n = \delta_1^n + \cdots + \delta_m^n$ for $n \ge 1$. For $n \ge 1$, $w_n = v_{kn}$. Thus any V_δ-representation of an integer N of the form $d_j \cdots d_0$ gives a V_β-representation of N of the form $d_j 0^{k-1} d_{j-1} 0^{k-1} \cdots d_1 0^{k-1} d_0$. Since the normalisation in the system V_β is computable by a finite transducer on any alphabet by Proposition 2.3.65, the result follows. □

Theorem 2.3.77 (Frougny 2002) *Let U and V be two Pisot basis, associated with two multiplicatively dependent Pisot numbers. Then the conversion from a V-representation of a positive integer to the U-expansion of that integer is computable by a finite transducer.*

Proof Set $\delta = \beta^k = \gamma^\ell$. As in Proposition 2.3.76, the conversion from the Lucas-like numeration system V_δ to the the Lucas-like numeration system V_γ is realisable by a finite transducer. By Proposition 2.3.74, the conversion from V to V_γ and the conversion from V_β to U are realisable by a finite transducer, and the result follows. □

Corollary 2.3.78 *Let U and V be two Pisot basis, associated with two multiplicatively dependent Pisot numbers. Then the U-recognisable sets and V-recognisable sets of natural integers coincide.*

2.3.4.2 Base β and U_β numeration system

When β is an integer, β-expansions and U_β-expansions of the positive integers are the same. There is a particular case of Pisot numbers for which the conversion from base β to the U_β numeration system is realisable by means of a finite transducer.

Let us take the example of the Golden Ratio φ and the Fibonacci numeration system. By Theorem 2.3.25, φ satisfies the (F) Property, so the greedy φ-expansion of every positive integer is finite. In this section we want to answer the following questions. Does there exist a characterisation of the greedy φ-expansions of the positive integers? Is there any relation between the greedy φ-expansion of a positive integer and its greedy representation in the Fibonacci system? Table 2.1 below gives the φ-expansion of the 10 first integers together with their Fibonacci greedy representation.

In fact the results are not only valid for the Golden Ratio, but for the larger class of *quadratic Pisot units*. A quadratic Pisot unit is an algebraic number whose minimal polynomial is of the form $X^2 - rX - 1$ with $r \ge 1$ or $X^2 - rX + 1$ with $r \ge 3$. By Corollary 2.3.28, every quadratic Pisot number satisfies the (PF) Property, and thus the expansion of every positive integer is finite. If the β-expansion of a positive integer n is of the form $u{\cdot}v$, by

N	Fibonacci representations	φ-expansions	Folded φ-expansions
1	1	1.	$\begin{smallmatrix}1\\0\end{smallmatrix}$
2	10	10.01	$\begin{smallmatrix}1&0\\1&0\end{smallmatrix}$
3	100	100.01	$\begin{smallmatrix}1&0&0\\0&1&0\end{smallmatrix}$
4	101	101.01	$\begin{smallmatrix}1&0&1\\0&1&0\end{smallmatrix}$
5	1000	1000.1001	$\begin{smallmatrix}1&0&0&0\\1&0&0&1\end{smallmatrix}$
6	1001	1010.0001	$\begin{smallmatrix}1&0&1&0\\1&0&0&0\end{smallmatrix}$
7	1010	10000.0001	$\begin{smallmatrix}1&0&0&0&0\\0&1&0&0&0\end{smallmatrix}$
8	10000	10001.0001	$\begin{smallmatrix}1&0&0&0&1\\0&1&0&0&0\end{smallmatrix}$
9	10001	10010.0101	$\begin{smallmatrix}1&0&0&1&0\\0&1&0&1&0\end{smallmatrix}$
10	10010	10100.0101	$\begin{smallmatrix}1&0&1&0&0\\0&1&0&1&0\end{smallmatrix}$

Table 2.1. *Fibonacci expansions, φ-expansions, and folded φ-expansions of the 10 first integers.*

padding the shortest word by 0's one can suppose that they have the same length. The *folded β-expansion* of n is the couple $(\begin{smallmatrix}u\\ \widetilde{v}\end{smallmatrix})$, where $\widetilde{v}$ is the mirror image of v.

Theorem 2.3.79 (Frougny and Sakarovitch 1999) *Let β be a quadratic Pisot unit. There exists a letter-to-letter finite transducer that maps the U_β-representation of any positive integer onto its folded β-expansion.*

Since the image of a function computable by a finite letter-to-letter transducer is a rational language, it then follows immediately from Theorem 2.3.79 that we have:

Corollary 2.3.80 *Let β be a quadratic Pisot unit. The set of folded β-expansions of all the non-negative integers is a rational language.*

By a result of (Rosenberg 1967) follows thus that the set of β-expansions of all the non-negative integers is a *linear context-free language*. The following result shows that only quadratic Pisot units enjoy this property.

Theorem 2.3.81 (Frougny and Solomyak 1999) *Let $\beta > 1$ be a non-integral real number such that the β-expansion of every non-negative integer is finite. Let $R_\beta \subset A_\beta^* . A_\beta^*$ be the set of β-expansions of all the non-negative integers. If R_β is a context-free language, then β must be a quadratic Pisot unit.*

2.4 Canonical numeration systems

In this section we present another generalisation of the integer base number system, in which the expansion of a number is given by a right-to-left algorithm. The canonical numeration systems have been extensively studied, and we refer the reader to (Scheicher and Thuswaldner 2004), (Akiyama and Rao 2005), (Brunotte, Huszti, and Pethő 2006) for some recent contributions, and (Barat, Berthé, Liardet, and Thuswaldner 2006) for a survey.

We also present briefly a new concept, the shift radix systems, which is a generalisation of both the Pisot base and the canonical numeration systems.

2.4.1 Canonical numeration systems in algebraic number fields

The elements of this section are taken in particular from (Gilbert 1981, Gilbert 1991, Kátai and Kovács 1981)).

Let β be an algebraic integer of modulus > 1, and let A be a finite set of elements of $\mathbb{Z}[\beta]$ containing zero.

Definition 2.4.1 The pair (β, A) is a *canonical numeration system* (CNS for short) if every element z of $\mathbb{Z}[\beta]$ has a unique integer representation $d_k \cdots d_0$ with d_j in A, $d_k \neq 0$, that we denote $\langle z \rangle_\beta = d_k \cdots d_0$, and such that $z = \pi_\beta(d_k \cdots d_0) = \sum_{j=0}^{k} d_j \beta^j$.

Example 2.4.2 • The negative integer base $\beta = -b$, with $b \geq 2$, forms a CNS with the alphabet $\{0, \ldots, b-1\}$, see (Grünwald 1885).
- Base $\beta = 3$ with the alphabet $\{-1, 0, 1\}$ forms a CNS, see (Knuth 1998).
- The Penney numeration system with base $\beta = -1 \pm i$ and digit set $\{0, 1\}$ forms a CNS, see (Penney 1964).

Let $M_\beta(X) = X^g + b_{g-1}X^{g-1} + \cdots + b_0$ be the minimal polynomial of β. The *norm* of β is $N(\beta) = |b_0|$. A set $R \subset \mathbb{Z}[\beta]$ is a *complete residue system* for $\mathbb{Z}[\beta]$ modulo β if every element of $\mathbb{Z}[\beta]$ is congruent modulo β to a unique element of R.

It is classical (Theorem of Sylvester) that a complete residue system of elements of $\mathbb{Z}[\beta]$ modulo β contains $N(\beta)$ elements, for instance the set $A_\beta = \{0, \ldots, N(\beta) - 1\}$.

Proposition 2.4.3 *Suppose that every element of $\mathbb{Z}[\beta]$ has a finite integer representation in the CNS (β, A). Then this representation is unique if, and only if, A is a complete residue system for $\mathbb{Z}[\beta]$ modulo β, that contains zero.*

Proof Suppose that the representation of $z \in \mathbb{Z}[\beta]$ is $d_k \cdots d_0$. Then $z \sim d_0 \pmod{\beta}$, thus A must contain a complete residue system modulo β.

Now suppose that two digits c and d of A are congruent modulo β. Then $c - d = e\beta$ for some e in $\mathbb{Z}[\beta]$. Let $\langle e \rangle_\beta = e_k \cdots e_0$. Then $c = e\beta + d$, so c has two representations, c itself, and $e_k \cdots e_0 d$.

Conversely, suppose that there exists $z \in \mathbb{Z}[\beta]$ with two different representations, $d_k \cdots d_0$ and $c_\ell \cdots c_0$. One can suppose that $k \geq \ell$, and set $c_j = 0$ for $\ell + 1 \leq j \leq k$. Then the polynomial $(d_k - c_k)X^k + \cdots + (d_0 - c_0)$ vanishes at $X = \beta$, and it is thus divisible by the minimal polynomial $M_\beta(X)$. Contradiction, since $|d_0 - c_0| < N(\beta)$. □

Given β and A a complete residue system, a word $d_k \cdots d_0$ with d_j in A is a representation of $z \in \mathbb{Z}[\beta]$ if $d_0 \sim z \pmod{\beta}$ and $d_k \cdots d_1$ is the representation of $(z - d_0)/\beta$. Thus we define

$$\begin{array}{rcl} \Phi_\beta : \mathbb{Z}[\beta] & \to & \mathbb{Z}[\beta] \\ z & \mapsto & \dfrac{z - d}{\beta} \text{ with } d \sim z \pmod{\beta}. \end{array} \tag{2.15}$$

The digits d_j in the representation of z are given by $d_j = \Phi_\beta^j(z) \pmod{\beta}$. Thus the representation of z in the system (β, A) is finite if, and only if, the iterates $\Phi_\beta^j(z)$, $j \geq 0$, eventually reach 0.

Remark that all words of A^* are admissible.

Proposition 2.4.4 *If (β, A) is a canonical numeration system then*
(i) *β and all its conjugates have moduli greater than 1*
(ii) *β has no positive real conjugate.*

Proof (i) Suppose that there is a conjugate β_i with $|\beta_i| < 1$. Let z be in $\mathbb{Z}[\beta]$ with $\langle z \rangle_\beta = d_k \cdots d_0$, d_j in A. Let $z_i = \sum_{j=0}^k d_j \beta_i^j$. Set $m_A = \max(|a|, a \in A)$. Then $|z_i| < m_A/(1 - |\beta_i|)$, and so there exist elements in $\mathbb{Z}[\beta]$ with no representation in (β, A).
(ii) Let β_i be a conjugate of β which is real and positive. Suppose -1 could be represented in the system as $-1 = \sum_{j=0}^k d_j \beta^j$. Then $-1 = \sum_{j=0}^k d_i \beta_i^j$, which is impossible. □

Note that (ii) implies that if (β, A) is a CNS then the constant term of the minimal polynomial is positive.

An element z in $\mathbb{Q}(\beta)$ has a representation $\langle z\rangle_\beta = d_k \cdots d_0 . d_{-1} d_{-2} \cdots$ in the CNS (β, A) if $z = \sum_{i=-\infty}^{k} d_i \beta^i$ with d_i in A. The following result is similar to the results in integer and non-integer real base, see (Gilbert 1981, Gilbert 1991).

Proposition 2.4.5 *If (β, A) is a canonical numeration system then every element of the field $\mathbb{Q}(\beta)$ has an eventually periodic representation in (β, A).*

2.4.2 Normalisation in canonical numeration systems

The results presented in this section primarily appeared in (Grabner, Kirschenhofer, and Prodinger 1998), (Thuswaldner 1998), (Safer 1998), (Scheicher and Thuswaldner 2004).

Let (β, A) be a canonical numeration system. Let $C \supset A$ be a finite alphabet of digits in $\mathbb{Z}[\beta]$. The normalization on C in the system (β, A) is the function

$$\nu_{\beta,C} : C^* \longrightarrow A^* \qquad c_k \cdots c_0 \longmapsto \langle \sum_{j=0}^{k} c_j \beta^j \rangle_\beta \ .$$

As in the previous sections, we define the zero automaton, on a finite symmetric alphabet D of digits in $\mathbb{Z}[\beta]$, that contains A. The *zero automaton* $\mathcal{Z}_{\beta,D}$ on D is defined as follows: $\mathcal{Z}_{\beta,D} = (\,\mathbb{Z}[\beta], D, E, \{0\}, \{0\}\,)$ where the transitions in E are defined by

$$\forall s,t \in \mathbb{Z}[\beta], \qquad \forall a \in D,\ s \xrightarrow[\mathcal{Z}_{\beta,D}]{a} t \quad \text{if, and only if,} \quad t = \beta\, s + a \ . \tag{2.16}$$

This automaton accepts the writings of 0 in base β on the alphabet D. Let $m_D = \max\{|a| \mid a \in D\}$ and let $Q_D = \{s \in \mathbb{Z}[\beta] \mid |s| \leq \frac{m_D}{|\beta|-1}\}$.

Proposition 2.4.6 *The* trim *part of $\mathcal{Z}_{\beta,D}$ contains only states belonging to Q_D.*

Proof As D contains A and is symmetrical, every element of $\mathbb{Z}[\beta]$ is accessible in $\mathcal{Z}_{\beta,D}$.

Suppose that $e_k \cdots e_0$ is a word of D^* such that $\sum_{j=0}^{k} e_j \beta^j = 0$. Then, for $1 \leq j \leq k$, $s_j = \beta^{j-1} e_k + \cdots + e_{k-j+1} = -\beta^{-j+1}(\beta^{j-2} e_{j-2} + \cdots + e_0)$, thus $|s_j| < \frac{m_D}{|\beta|-1}$, and $e_k \cdots e_0$ is the label of a path

$$0 \xrightarrow{e_k} s_1 \xrightarrow{e_{k-1}} \cdots s_k \xrightarrow{e_0} s_{k+1} = 0$$

in $\mathcal{Z}_{\beta,D}$ with all the states in Q_D.

□

Lemma 2.4.7 *If β and all its conjugates have moduli greater than 1 then for every finite alphabet D the zero automaton $\mathcal{Z}_{\beta,D}$ is finite.*

Proof Recall that the norm defined on $\mathbb{Z}[\beta] \simeq \mathbb{Z}[X]/(M_\beta)$ is defined by $||P(X)|| = \max_{1\le i\le g} |P(\beta_i)|$, see (2.12). Let $s = s(\beta)$ be in Q_D. Then for $1 \le i \le g$, $|s(\beta_i)| < \frac{m_D}{|\beta_i|-1}$. Since the elements of Q_D are bounded in norm in the discrete lattice $\mathbb{Z}[\beta]$, Q_D is finite and the automaton $\mathcal{Z}_{\beta,D}$ is finite.

□

We now consider the normalisation from an alphabet C in the CNS (β, A). Let D be a symmetrized alphabet of digits in $\mathbb{Z}[\beta]$ containing the set $\{c-a \mid c \in C, a \in A\}$. As explained in the integer base case, one can associate with the zero automaton $\mathcal{Z}_{\beta,D}$ a converter $\mathcal{C}_\beta(C\times A)$. The transitions are defined by

$$s \xrightarrow[\mathcal{C}_\beta(C\times A)]{c|a} t \quad \text{if, and only if,} \quad s \xrightarrow[\mathcal{Z}_{\beta,D}]{c-a} t \ .$$

Lemma 2.4.8 *If A is a complete residue system modulo β then the converter $\mathcal{C}_\beta(C\times A)$ is input co-deterministic.*

Proof By definition there is an edge $s \xrightarrow{c|a} t$ in $\mathcal{C}_\beta(C\times A)$ if, and only if, $\beta s + c = t + a$. If there is another edge $s' \xrightarrow{c|a'} t$ in $\mathcal{C}_\beta(C\times A)$, then $\beta(s - s') = a - a'$, which is impossible since A is a complete residue system.

□

It is thus more natural to define a right sequential letter-to-letter transducer, the normaliser $\mathcal{N}_\beta(C)$, with

$$t \xrightarrow[\mathcal{N}_\beta(C)]{c|a} s \quad \text{if, and only if,} \quad (-s) \xrightarrow[\mathcal{C}_\beta(C\times A)]{c|a} (-t)\,.$$

Let $c_k \cdots c_0 \in C^*$. Setting $s_0 = 0$, there is a unique path in $\mathcal{N}_\beta(C)$

$$s_{k+1} \xleftarrow{c_k|d_k} s_k \xleftarrow{c_{k-1}|d_{k-1}} s_{k-1} \cdots \xleftarrow{c_1|d_1} s_1 \xleftarrow{c_0|d_0} s_0$$

and

$$\sum_{j=0}^{k} c_j\beta^j = (\sum_{j=0}^{k} d_j\beta^j) + s_{k+1}\beta^{k+1}. \tag{2.17}$$

Remark 2.4.9 If any element of Q_D has a finite integer representation in the system (β, A) (with A a complete residue system modulo β) then the normaliser $\mathcal{N}_\beta(C)$ converts any element z in $\mathbb{Z}[\beta]$ with a representation in C^* into its (β, A) integer representation.

Proof If $z = \sum_{j=0}^{k} c_j \beta^j$, then there exists a path in $\mathcal{N}_\beta(C)$ satisfying (2.17), and $\langle z \rangle_\beta = \langle s_{k+1} \rangle_\beta d_k \cdots d_0$. □

Remark 2.4.10 The normaliser $\mathcal{N}_\beta(C)$ can be used as an algorithm to represent any $z \in \mathbb{Z}[\beta]$ in the system (β, A) (with A a complete residue system modulo β). In fact, given z, there exists a C such that z belongs to C. Feed the transducer with z as input. There exists a unique path

$$\Phi_\beta^{k+1}(z) \xleftarrow{0|d_k} \Phi_\beta^{k}(z) \xleftarrow{0|d_{k-1}} \Phi_\beta^{k-1}(z) \cdots \xleftarrow{0|d_1} \Phi_\beta(z) \xleftarrow{z|d_0} 0$$

and $\langle z \rangle_\beta = d_k \cdots d_0$ if, and only if, $\Phi_\beta^{k+1}(z) = 0$.

From Proposition 2.4.4, Lemma 2.4.7 and Lemma 2.4.8 follows the following result.

Proposition 2.4.11 *If the system (β, A) is a canonical numeration system then the right sequential normaliser $\mathcal{N}_\beta(C)$ is finite for every alphabet C.*

2.4.3 Bases for canonical numeration systems

In general, it is difficult to determine which numbers are suitable bases for a CNS. However, several results are known. In the particular case where β is a Gaussian integer and A is an alphabet of natural integers there is a nice characterisation due to (Kátai and Szabó 1975).

Theorem 2.4.12 *Let β be a Gaussian integer of norm N, and let $A = \{0, \ldots, N-1\}$. Then (β, A) is a canonical numeration system for the complex numbers if, and only if, $\beta = -n \pm i$, for some $n \geq 1$ (and $N = n^2$).*

It is noteworthy that any complex number has a representation — not necessarily unique — in this system.

Quadratic CNS have been characterised in (Kátai and Kovács 1981) and in (Gilbert 1981). In (Brunotte 2001, Brunotte 2002) are characterised all CNS whose bases are roots of trinomials. In the general case (Akiyama and Pethő 2002) have given an algorithm to decide whether a number β is the base of a CNS.

Theorem 2.4.13 *Let β be an algebraic integer with minimal polynomial $M_\beta(X) = X^g + b_{g-1}X^{g-1} + \cdots + b_0$. If one of the following properties is satisfied then β is a base for a CNS:*

(i) $b_0 \geq 2$ *and* $b_0 \geq b_1 \geq \cdots \geq b_{g-1} \geq 1$
(ii) $b_2 \geq 0, \ldots, b_{g-1} \geq 0,\ 1 + \sum_{i=0}^{g-1} b_i \geq 0$ *and* $b_0 > 1 + \sum_{i=1}^{g-1} |b_i|$.

Part (i) is due to (Kovács 1981), and Part (ii) has been obtained by (Scheicher and Thuswaldner 2004) using automata.

2.4.4 Shift radix systems

The concept of shift radix system was introduced in (Akiyama, Borbély, Brunotte, Pethő, and Thuswaldner 2005) to unify canonical numeration systems and β-expansions. Although these two numeration systems are quite different, they are close relatively to some finiteness properties, which means that all numbers of a certain set admit finite expansions.

Definition 2.4.14 Let $\mathbf{r} = (r_1, \ldots, r_d)$ be an element of $\mathbb{R}^d$. Define a mapping $\mu_\mathbf{r} : \mathbb{Z}^d \to \mathbb{Z}^d$ by

$$\mu_\mathbf{r}((z_1, \ldots, z_d)) = (z_2, \ldots, z_d, -\lfloor r_1 z_1 + \cdots + r_d z_d \rfloor).$$

We say that $\mu_\mathbf{r}$ has the *finiteness property* if for every $\mathbf{z}$ in $\mathbb{Z}^d$ there exists a k such that $\mu_\mathbf{r}^k(\mathbf{z}) = 0$. In that case $(\mathbb{Z}, \mu_\mathbf{r})$ is called a *shift radix system* or SRS.

2.4.4.1 Connection with Pisot numbers and the (F) property

In (Akiyama and Scheicher 2005) it is indicated that the origin of SRS can be found in (Hollander 1996).

Theorem 2.4.15 (Akiyama, Borbély, Brunotte, Pethő, and Thuswaldner 2005) *Let $\beta > 1$ be an algebraic integer with minimal polynomial*

$$M_\beta(X) = X^g + b_{g-1}X^{g-1} + \cdots + b_0 \in \mathbb{Z}[X].$$

Write $M_\beta(X) = (X - \beta)(X^{g-1} + r_{g-1}X^{g-2} + \cdots + r_1)$ and let $\mathbf{r} = (r_1, \ldots, r_{g-1})$. Then β satisfies the (F) property if, and only if, $\mathbf{r}$ gives a $(g-1)$-dimensional SRS.

Proof It is easy to see that β satisfies the (F) property if, and only if, each element of $\mathbb{Z}[\beta] \cap [0, \infty)$ has a finite greedy β-expansion. For $1 \leq i \leq$

$g-1$, $r_i = -(\frac{b_{i-1}}{\beta} + \cdots + \frac{b_0}{\beta^i})$ and $r_g = 1$. The ring $\mathbb{Z}[\beta]$ is generated by $\{1, \beta, \ldots, \beta^{g-1}\}$ as a $\mathbb{Z}$-module; the same is true for $\{r_1, \ldots, r_g\}$. Thus every element z of $\mathbb{Z}[\beta] \cap [0,1)$ can be expressed as $z = \sum_{i=1}^{g} z_i r_i$. The β-transformation of z can be written $\tau_\beta(z) = \sum_{i=1}^{g} z_{i+1} r_i$ with z_{g+1} such that $0 \leq z_2 r_1 + \cdots + z_{g+1} r_g < 1$, more precisely

$$z_{g+1} = -\lfloor z_2 r_1 + \cdots + z_g r_{g-1} \rfloor .$$

Then $\mu_{\mathbf{r}}(z_1, \ldots, z_{g-1}) = (z_2, \ldots, z_g)$. □

The roots of the polynomial $X^{g-1} + r_{g-1}X^{g-2} + \cdots + r_1$ have modulus less than one, and it can be proved that the SRS algorithm associated with $(r_1, \ldots, r_{g-1})$ always leads to a periodic orbit, and thus that every positive element of $\mathbb{Z}[\beta]$ has an eventually periodic greedy β-expansion. The same can be proved for every positive element of $\mathbb{Q}[\beta]$, which reproves Theorem 2.3.20.

2.4.4.2 Connection with canonical numeration systems

Theorem 2.4.16 (Akiyama, Borbély, Brunotte, Pethő, and Thuswaldner 2005) *The polynomial $X^g + b_{g-1}X^{g-1} + \cdots + b_0$ gives a CNS if, and only if,*

$$\mathbf{r} = (\frac{1}{b_0}, \frac{b_{g-1}}{b_0}, \ldots, \frac{b_1}{b_0})$$

gives a g–dimensional SRS.

Proof Take z in $\mathbb{Z}[\beta]$. Then z can be written as $z = \sum_{i=0}^{g-1} z_i \beta^i$ with z_i in $\mathbb{Z}$. The mapping Φ_β (see (2.15)) can be extended as a mapping $\widetilde{\Phi_\beta} : \mathbb{Z}^g \to \mathbb{Z}^g$ defined as

$$\widetilde{\Phi_\beta}((z_0, \ldots, z_{g-2}, z_{g-1})) = (z_1 - qb_1, \ldots, z_{g-1} - qb_{g-1}, -q))$$

with $q = \lfloor z_0 / b_0 \rfloor$.

For easier notation, set $b_g = 1$. The basis $\{1, \beta, \ldots, \beta^{g-1}\}$ can be replaced by the basis $\{w_1, \ldots, w_g\}$ with $w_j = \sum_{i=g-j+1}^{g} b_j \beta^{i+j-g-1}$ for $1 \leq j \leq g$. Now, if $z = \sum_{i=1}^{g} y_j w_j$, we can define a map Ψ_β playing the same role as Φ_β by

$$\Psi_\beta(z) = (\sum_{i=1}^{g-1} y_{j+1} w_j) - w_g \lfloor \frac{b_1 y_g + \cdots + b_g y_1}{b_0} \rfloor .$$

This maps is extended as a mapping $\widetilde{\Psi_\beta} : \mathbb{Z}^g \to \mathbb{Z}^g$ defined by

$$\widetilde{\Psi_\beta}((y_1, \ldots, y_{g-1}, y_g)) = (y_2, \ldots, y_g, -\lfloor \frac{b_1 y_g + \cdots + b_g y_1}{b_0} \rfloor)$$

and $\widetilde{\Psi_\beta}$ is just the SRS mapping $\mu_{\mathbf{r}}$. $\square$

2.5 Representation in rational base

We now turn to the problem of the representation of numbers, integers or reals, again in a base *which is not an integer* but a rational number — and thus certainly *not a Pisot number*, as it has been the case in most of the preceeding sections. The greedy algorithm which was ubiquitous there and underlying almost every construction is now inappropriate or, to tell the truth, one cannot tell anything of its outcome. We shall make use instead of an algorithm which is reminiscent of the division algorithm defined with integer base and which produces, as the division algorithm, the digits of the representations *from right to left*.

All the results of this section are taken, and their presentation is adapted, from (Akiyama, Frougny, and Sakarovitch 2008).

2.5.1 Representation of integers

Let p and q be two co-prime integers, $p > q \geqslant 1$. The *definition* of the numeration system in base $\frac{p}{q}$ itself, and thus the evaluation map, will follow from the algorithm which computes the representation of the integers.

2.5.1.1 The modified division algorithm

Let N be any positive integer; let us write $N_0 = N$ and, for $i \geqslant 0$, write

$$q\,N_i = p\,N_{i+1} + a_i \tag{2.18}$$

where a_i is the remainder of the division of $q\,N_i$ by p, and thus belongs to $A_p = \{0, \ldots, p-1\}$. Since N_{i+1} is strictly smaller than N_i, the division (2.18) can be repeated only a finite number of times, until eventually $N_{k+1} = 0$ for some k. The sequence of successive divisions (2.18) for $i = 0$ to $i = k$ is thus an *algorithm* — that in the sequel is referred to as the *Modified Division*, or *MD*, *algorithm* — which given N produces the digits a_0, a_1, …, a_k, and it holds:

$$N = \sum_{i=0}^{k} \frac{a_i}{q} \left(\frac{p}{q}\right)^i \quad . \tag{2.19}$$

We will say that the word $a_k \cdots a_0$, computed from N from right to left, that is to say *least significant digit first*, is a $\frac{p}{q}$*-representation* of N.

Let $U_{\frac{p}{q}}$ be the sequence defined by:

$$U_{\frac{p}{q}} = \{u_i = \frac{1}{q}\left(\frac{p}{q}\right)^i \mid i \in \mathbb{Z}\} \ .$$

We will say that $U_{\frac{p}{q}}$, *together with* the digit alphabet A_p is the numeration system in base $\frac{p}{q}$ or the $\frac{p}{q}$ *numeration system.* If $q = 1$, it is exactly the classical numeration system in base p. But, on the other hand, this definition *does not* match the one we have given for the numeration system in base β in Section 2.3: $U_{\frac{p}{q}}$ *is not* the sequence of powers of $\frac{p}{q}$ but rather these powers *divided by* q and the digits *are not* the integers smaller than $\frac{p}{q}$ but rather the integers *whose quotient by* q is smaller than $\frac{p}{q}$. The *evaluation map* $\pi_{\frac{p}{q}} : {A_p}^* \to \mathbb{Q}$ is defined accordingly: for every word w of ${A_p}^*$, we have

$$w = a_k\, a_{k-1} \cdots a_1\, a_0 \quad \longmapsto \quad \pi_{\frac{p}{q}}(w) = \sum_{i=0}^{k} a_i u_i = \sum_{i=0}^{k} \frac{a_i}{q}\left(\frac{p}{q}\right)^i \ . \qquad (2.20)$$

With the same proof as for integer base system (*cf.* Lemma 2.2.1), we have:

Lemma 2.5.1 *The restriction of* $\pi_{\frac{p}{q}}$ *to* ${A_p}^k$ *is* injective*, for every* k*.*

As for integer base, $\pi_{\frac{p}{q}}$ is not injective on the whole ${A_p}^*$ since for any u in ${A_p}^*$ and any integer h it holds: $\pi_{\frac{p}{q}}(0^h u) = \pi_{\frac{p}{q}}(u)$. On the other hand, Lemma 2.5.1 implies that this is the only possibility and we have:

$$\pi_{\frac{p}{q}}(u) = \pi_{\frac{p}{q}}(v) \ \text{ and } \ |u| > |v| \quad \Longrightarrow \quad u = 0^h v \ \text{ with } \ h = |u| - |v| \ . \qquad (2.21)$$

Theorem 2.5.2 *Every non-negative integer* N *has a* $\frac{p}{q}$*-representation which is an* integer *representation. It is the* unique finite $\frac{p}{q}$-representation *of* N*.*

Proof Let $a_k \cdots a_0$ be the $\frac{p}{q}$-representation given to N by the MD algorithm, and suppose that there exists another *finite* representation of N in the system $U_{\frac{p}{q}}$, of the form $e_\ell e_{\ell-1} \cdots e_0{\scriptstyle\bullet} e_{-1} \cdots e_{-m}$ with $e_{-m} \neq 0$. Then

$$q\left(\frac{p}{q}\right)^m N = \sum_{i=-m}^{\ell} e_i \left(\frac{p}{q}\right)^{m+i} = \sum_{i=0}^{k} a_i \left(\frac{p}{q}\right)^{m+i}$$

and therefore $\pi_{\frac{p}{q}}(e_\ell \cdots e_0 e_{-1} e_{-2} \cdots e_{-m}) = \pi_{\frac{p}{q}}(a_k a_{k-2} \cdots a_0 0^m)$. Contradiction between (2.21) and $e_{-m} \neq 0$. □

This unique finite $\frac{p}{q}$-representation of N (under the condition that the leading digit is not 0) will be called the $\frac{p}{q}$-*expansion* of N and written $\langle N\rangle_{\frac{p}{q}}$. *By convention* and as in the three preceeding sections, the $\frac{p}{q}$-expansion of 0 is the empty word ε.

Example 2.5.3 Let $p = 3$ and $q = 2$, then $A_3 = \{0, 1, 2\}$ — this will be our main running example in this section. Table 2.2 gives the $\frac{3}{2}$-expansions of the twelve first non-negative integers.

ε	0	2120	6
2	1	2122	7
21	2	21011	8
210	3	21200	9
212	4	21202	10
2101	5	21221	11

Table 2.2. *The* $\frac{3}{2}$-*expansion of the twelve first integers.*

We let $L_{\frac{p}{q}}$ denote the set of $\frac{p}{q}$-*expansions* of the non-negative integers:

$$L_{\frac{p}{q}} = \{\langle N\rangle_{\frac{p}{q}} \mid N \in \mathbb{N}\} \ .$$

In contrast with the three preceeding sections, and as we shall see below, $L_{\frac{p}{q}}$ is not a rational set. Before getting to this point, let us note that the same order properties as for integer base systems hold for the $\frac{p}{q}$ numeration system, provided only the words in $L_{\frac{p}{q}}$ are considered.

Proposition 2.5.4 *Let* v *and* w *be in* $L_{\frac{p}{q}}$. *Then* $v \preceq w$ *if, and only if,* $\pi_{\frac{p}{q}}(v) \leqslant \pi_{\frac{p}{q}}(w)$.

Proof Let $v = a_k \cdots a_0$ and $w = b_\ell \cdots b_0$ be the $\frac{p}{q}$-expansions of the integers $m = \pi_{\frac{p}{q}}(v)$ and $n = \pi_{\frac{p}{q}}(w)$ respectively. By Theorem 2.5.2, we already know that $v = w$ if, and only if, $\pi_{\frac{p}{q}}(v) = \pi_{\frac{p}{q}}(w)$. The proof goes by induction on ℓ, which is (by hypothesis) greater than or equal to k. The proposition holds for $\ell = 0$.

Let us write $v' = a_k \cdots a_1$ and $w' = b_\ell \cdots b_1$, and $m' = \pi_{\frac{p}{q}}(v')$ and $n' = \pi_{\frac{p}{q}}(w')$ are integers. It holds:

$$n - m = \frac{p}{q}(n' - m') + \frac{1}{q}(b_0 - a_0) \ .$$

Now $v \prec w$ implies that either $v' \prec w'$ or $v' = w'$ and $a_0 < b_0$. If $v' \prec w'$, then $n' - m' \geqslant 1$ by induction hypothesis and thus $n - m > 0$ since $b_0 - a_0 \geqslant -(p-1)$. If $v' = w'$, then $n - m = \frac{1}{q}(b_0 - a_0) > 0$. □

Corollary 2.5.5 *Let v and w be in $0^* L_{\frac{p}{q}}$ and of equal length. Then $v \leq w$ if, and only if, $\pi_{\frac{p}{q}}(v) \leqslant \pi_{\frac{p}{q}}(w)$.*

It is to be noted also that these statements do not hold without the hypothesis that v and w belong to $L_{\frac{p}{q}}$ (to $0^* L_{\frac{p}{q}}$ respectively). For instance, $\pi_{\frac{3}{2}}(10) = 3/4 < \pi_{\frac{3}{2}}(2) = 1$ and $\pi_{\frac{3}{2}}(2000) = 27/16 < \pi_{\frac{3}{2}}(0212) = 4$.

2.5.1.2 The set of $\frac{p}{q}$-expansions of the integers

It is a very intriguing, and totally open, question to characterise the set $L_{\frac{p}{q}}$. As far as now, we can only make basic observations.

By construction, $L_{\frac{p}{q}}$ is *prefix-closed*, that is, any prefix of any word of $L_{\frac{p}{q}}$ is in $L_{\frac{p}{q}}$. A simple look at Table 2.2 shows that it is *not suffix-closed*. In fact, *every word* of A_p^* is a suffix of some words in $L_{\frac{p}{q}}$. More precisely, we have the following statement.

Proposition 2.5.6 *For every integer k and every word w in A_p^k, there exists a unique integer n, $0 \leqslant n < p^k$ such that w is the suffix of length k of the $\frac{p}{q}$-expansion of all integers m congruent to n modulo p^k.*

Proof Given any integer $n = n_0$, the division (2.18) repeated k times yields:

$$q^k n_0 = p^k n_k + q^k \, \pi_{\frac{p}{q}}(a_{k-1}a_{k-2}\cdots a_0) \; . \tag{2.22}$$

If we do the same for another integer $m = m_0$ and perform the subtraction on the two sides of Equation (2.22), it comes:

$$q^k (n_0 - m_0) = p^k (n_k - m_k) + q^k \left(\pi_{\frac{p}{q}}(a_{k-1}a_{k-2}\cdots a_0) - \pi_{\frac{p}{q}}(b_{k-1}b_{k-2}\cdots b_0) \right) \; .$$

As q^k is prime with p^k, and using Lemma 2.5.1, it comes:

$$n - m \equiv 0 \pmod{p^k} \iff a_{k-1}a_{k-2}\cdots a_0 = b_{k-1}b_{k-2}\cdots b_0 \; . \tag{2.23}$$

Since there are exactly p^k words in A_p^k, each of them must appear once and only once when n ranges from 0 to $p^k - 1$ and (2.23) gives the second part of the statement. □

It follows that a word w of length k is a *right context* for the $\frac{p}{q}$-expansions $\langle n \rangle_{\frac{p}{q}}$ and $\langle m \rangle_{\frac{p}{q}}$ of two integers n and m for $L_{\frac{p}{q}}$, that is, both $\langle n \rangle_{\frac{p}{q}} w$ and $\langle m \rangle_{\frac{p}{q}} w$ are in $L_{\frac{p}{q}}$, if, and only if, n and m are congruent modulo q^k. This implies immediately that the *coarsest right regular equivalence* that saturates $L_{\frac{p}{q}}$ is the identity, hence in particular is not of finite index. A classical statement in formal language theory (see for instance (Hopcroft, Motwani, and Ullman 2006)) then implies:

Corollary 2.5.7 *If* $q \neq 1$ *, then* $L_{\frac{p}{q}}$ *is not a regular language.*

Along the same line it is easy to give a more precise statement on suffixes that are powers of a given word.

Lemma 2.5.8 *Let* w *be in* $L_{\frac{p}{q}}$ *and* $w = u\,v$ *be a proper factorization of* w*. Then* $u\,v^k$ *belongs to* $L_{\frac{p}{q}}$ *only if* $q^{(k-1)|v|}$ *divides* $\pi_{\frac{p}{q}}(w) - \pi_{\frac{p}{q}}(u)$ *.*

Proof The word $u\,v^k$ belongs to $L_{\frac{p}{q}}$ only if

$$\begin{aligned}\pi_{\frac{p}{q}}\left(u\,v^k\right) - \pi_{\frac{p}{q}}\left(u\,v^{k-1}\right) &= \left(\frac{p}{q}\right)^{|v|}\left(\pi_{\frac{p}{q}}\left(u\,v^{k-1}\right) - \pi_{\frac{p}{q}}\left(u\,v^{k-2}\right)\right) = \cdots \\ &= \left(\frac{p}{q}\right)^{(k-1)|v|}\left(\pi_{\frac{p}{q}}(u\,v) - \pi_{\frac{p}{q}}(u)\right)\end{aligned}$$

is in $\mathbb{Z}$. And this is possible only if $q^{(k-1)|v|}$ divides $\pi_{\frac{p}{q}}(u\,v) - \pi_{\frac{p}{q}}(u)$. □

Lemma 2.5.8 will be used in the sequel to show that the closure of $L_{\frac{p}{q}}$ does not contain eventually periodic infinite words; combined with the classical 'pumping lemma' (see (Hopcroft, Motwani, and Ullman 2006) and Lemma **??**), it implies another statement related to formal language theory:

Corollary 2.5.9 *If* $q \neq 1$ *, then* $L_{\frac{p}{q}}$ *is not a context-free language.*

2.5.1.3 The evaluator and the converters

We build an evaluator and zero automata in a similar way as the one we followed for integer base. Let $\frac{p}{q}$ be the base fixed as before but the digits be a priori *any integer*, positive or negative. The evaluator $\mathcal{Z}_{\frac{p}{q}}$ has the set of *q-decimal* numbers, that is, $\mathbb{Z}[\frac{1}{q}]$, as set of states, it reads (from left to right) the numbers (written on the 'alphabet' $\mathbb{Z}$), and runs in such a way that, at every step of the reading, the reached state indicates the value of the portion of the number read so far. The initial state of $\mathcal{Z}_{\frac{p}{q}}$ is thus 0 and its transitions are of the form:

$$\forall s, t \in \mathbb{Z}[\frac{1}{q}]\,,\ \forall a \in \mathbb{Z} \qquad s \xrightarrow[\mathcal{Z}_{\frac{p}{q}}]{a} t \quad \text{if, and only if,} \quad q\,t = p\,s + a\,, \tag{2.24}$$

from which we get the expected behaviour:

$$\forall w \in \{\mathbb{Z}\}^* \qquad 0 \xrightarrow[\mathcal{Z}_{\frac{p}{q}}]{w} \pi_{\frac{p}{q}}(w) \quad .$$

It follows from (2.24) that $\mathcal{Z}_{\frac{p}{q}}$ is both *deterministic* and *co-deterministic*.

As above, we shall make use of finite parts of $\mathcal{Z}_{\frac{p}{q}}$. First, we restrict the alphabet to be a finite subset of $\mathbb{Z}$: $B_d = \{-d, \ldots, d\}$ with $d \geq p-1$ and thus $A_p \subset B_d$. Second, we choose 0 as unique final state and we get a zero automaton $\mathcal{Z}_{\frac{p}{q},d} = \left(\mathbb{Z}[\frac{1}{q}], B_d, E, \{0\}, \{0\} \right)$ where the transitions in E are those defined by (2.24). This automaton accepts thus the writings of 0 (in base $\frac{p}{q}$ and on the alphabet B_d). It is still infinite but we have the following.

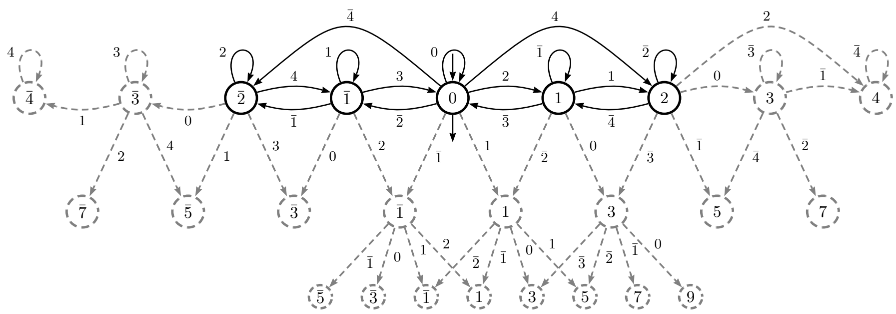


Fig. 2.18. A partial view of $\mathcal{Z}_{\frac{3}{2},4}$.
The upper row consists of the states whose labels are integers; the row below of the states whose labels are of the form $n/2$, with odd n; the next row of those whose labels are of the form $n/4$, with odd n; etc. For the readibility of the figure, not all transitions labelled in B_4 are drawn.

Proposition 2.5.10 *The* trim *part of* $\mathcal{Z}_{\frac{p}{q},d}$ *is finite and its set of states is* $H = \{-h, \ldots, h\}$ *where* $h = \left\lfloor \frac{d-q}{p-q} \right\rfloor$.

Proof As B_d contains A_p and is symmetrical, every z in $\mathbb{Z}$ is *accessible* in $\mathcal{Z}_{\frac{p}{q},d}$. On the other hand, no state in $\mathbb{Z}[\frac{1}{q}] \setminus \mathbb{Z}$ is co-accessible to 0 in $\mathcal{Z}_{\frac{p}{q},d}$.

If m is a positive integer strictly larger than $(d-q)/(p-q)$, the 'smallest' reachable state from m, that is, the smallest integer which is larger than, or equal to, $\frac{1}{q}(mp-d)$, is also larger than, or equal to, m: m is not co-accessible in $\mathcal{Z}_{\frac{p}{q},d}$ and the same is true if m is strictly smaller than $-(d-q)/(p-1)$.

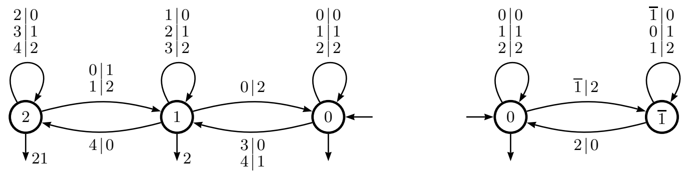
Conversely, if m is a positive integer smaller than $(d-q)/(p-q)$, then the integer $k = p + (m-1)(p-q)$ is smaller than, or equal to, d and

$m \xrightarrow{\bar{k}} (m-1)$ is a transition in $\mathcal{Z}_{\frac{p}{q},d}$. Hence, by induction, a path from m to 0 in $\mathcal{Z}_{\frac{p}{q},d}$. □

By definition, the trim part of $\mathcal{Z}_{\frac{p}{q},d}$ is the *strongly connected component* of 0. Figure 2.18 shows $\mathcal{Z}_{\frac{3}{2},4}$.

Let $\mathcal{Z}_{\frac{p}{q},d}$ denote the automaton reduced to its trim part only, with set of states H. And as above again, the automaton $\mathcal{Z}_{\frac{p}{q},d}$ will serve as the base for the construction of a series of converters and normalisers exactly as in the case of integer base.

Figure 2.19 (a) shows the right sequential converter that realises addition in the $\frac{3}{2}$ numeration system; Figure 2.19 (b) shows the right sequential converter on the alphabet $\{\bar{1}, 0, 1, 2\}$ in the $\frac{3}{2}$ numeration system.



(a) The converter for the addition.

(b) The converter on $\{-1, 0, 1, 2\}$.

Fig. 2.19. Two converters for the $\frac{3}{2}$ numeration system.

Remark 2.5.11 A converter reads words on a digit alphabet C, and output an equivalent $\frac{p}{q}$-representation on another alphabet A, even for words v such that $\pi_{\frac{p}{q}}(v)$ is not an integer.

As a corollary to the construction of the converter, it is easy to build a *letter-to-letter right sequential transducer* that realizes the successor function for the $\frac{p}{q}$ numeration system.

2.5.2 Representation of the reals

Every infinite word $u = (a_i)_{i \geq 1}$ in $A_p^{\mathbb{N}}$ is given a real value x by the evaluation map $\pi_{\frac{p}{q}}$:

$$u = a_1 a_2 \cdots \quad \longmapsto \quad x = \pi_{\frac{p}{q}}(u) = \sum_{i=1}^{\infty} \frac{a_i}{q} \left(\frac{p}{q}\right)^{-i}$$

and u is called a $\frac{p}{q}$*-representation* of x. We use the same conventions as in the preceeding sections and we have:

$$\forall u = (a_i)_{i\geq 1} \in {A_p}^{\mathbb{N}} \qquad \pi_{\frac{p}{q}}\left(\centerdot u\right) = \lim_{n\to+\infty} \left(\frac{q}{p}\right)^n \pi_{\frac{p}{q}}\left(a_1\, a_2 \cdots a_n\right) \ , \quad (2.25)$$

$$\forall u \in {A_p}^{\mathbb{N}}\, ,\ \forall w \in {A_p}^{*} \qquad \pi_p\left(\centerdot w\, u\right) = \left(\frac{q}{p}\right)^{|w|} \left(\pi_p\left(w\right) + \pi_p\left(\centerdot u\right)\right) \ .$$

Proposition 2.5.12 *The map* $\pi_{\frac{p}{q}} \colon {A_p}^{\mathbb{N}} \to \mathbb{R}$ *is continuous.*

Our purpose here is to associate with every real number a $\frac{p}{q}$-representation which will be as canonical as possible. In contrast with what is done in integer or Pisot base numeration systems, where the canonical representation — the *greedy expansion* — is defined by an algorithm which *computes* it for every real, we set *a priori* what are these canonical $\frac{p}{q}$-expansions.

2.5.2.1 Construction of the tree $T_{\frac{p}{q}}$

The free monoid ${A_p}^*$ is classically represented as the nodes of the (infinite) full p-ary tree: every node is labeled by a word in ${A_p}^*$ and has p children, every edge between a node and its children is labeled by one of the letter of A_p and the label of a node is precisely the label of the (unique) path that goes from the root to that node.

As the language $L_{\frac{p}{q}}$ is prefix-closed, it can naturally be seen as a subtree of the full p-ary tree, obtained by cutting some edges. This will form the tree $T_{\frac{p}{q}}$ (after we have changed the label of nodes from words to the numbers represented by these words). This tree, or more precisely its infinite paths, will be the basis for the representation of reals in the $\frac{p}{q}$ number system. We give now an 'internal' description of $T_{\frac{p}{q}}$, based on the definition of a family of maps from $\mathbb{N}$ to $\mathbb{N}$, which will proved to be effective for the study of infinite paths.

Definition 2.5.13 (i) For each a in A_p, let $\psi_a \colon \mathbb{N} \to \mathbb{N}$ be the *partial* map defined by:

$$\forall n \in \mathbb{N} \qquad \psi_a(n) = \begin{cases} \frac{1}{q}\,(p\,n + a) & \text{if} \quad \frac{1}{q}\,(p\,n+a) \in \mathbb{N} \\ \text{undefined} & \text{otherwise} \end{cases}$$

We write $\mathsf{e}(n) = \{a \in A_p \mid \psi_a(n) \text{ is defined}\}$, $\mathsf{Me}(n) = \max\{\mathsf{e}(n)\}$ for the largest digit for which $\psi_a(n)$ is defined, and $\mathsf{me}(n) = \min\{\mathsf{e}(n)\}$ for the smallest digit with the same property.

(ii) The tree $T_{\frac{p}{q}}$ is the labeled infinite tree (*where both nodes and edges*

are labeled) constructed as follows. The nodes are labeled in $\mathbb{N}$, and the edges in A, the root is labeled by 0. The children of a node labeled by n are nodes labeled by $\psi_a(n)$ for a in $\mathsf{e}(n)$, and the edge from n to $\psi_a(n)$ is labeled by a.
(iii) We call *path label* of a node s of $T_{\frac{p}{q}}$, and write $\mathrm{p}(s)$, the label of *the* path from the root of $T_{\frac{p}{q}}$ to s. We denote by $I_{\frac{p}{q}}$ the subtree of $T_{\frac{p}{q}}$ made of nodes whose path label does not begin with a 0.

The very way $T_{\frac{p}{q}}$ is defined implies that if two nodes have the same label, they are the root of two isomorphic subtrees of $T_{\frac{p}{q}}$ and it follows from Proposition 2.5.6 that the converse is true, that is two nodes which hold distinct labels are the root of two distinct subtrees of $T_{\frac{p}{q}}$. As no two nodes of $I_{\frac{p}{q}}$ have the same label, it comes:

Proposition 2.5.14 *If $q \neq 1$ no two subtrees of $I_{\frac{p}{q}}$ are isomorphic.*

Definition 2.5.13 and the MD algorithm imply directly the following facts.

Lemma 2.5.15 *For every n in $\mathbb{N}$, it holds:*

(i) $\mathsf{me}(n) = \mathsf{e}(n) \cap \{0, 1, \ldots, q-1\}$ *and* $\mathsf{Me}(n) = \mathsf{e}(n) \cap \{p-q, \ldots, p-1\}$.

(ii) $a \in \mathsf{e}(n)$ *and* $a + q \in A_p \implies a + q \in \mathsf{e}(n)$.

(iii) $a, a+q \in \mathsf{e}(n) \implies \psi_{a+q}(n) = \psi_a(n) + 1$.

(iv) $\mathsf{me}(n+1) = \mathsf{Me}(n) + q - p$ *and* $\psi_{\mathsf{me}(n+1)}(n+1) = \psi_{\mathsf{Me}(n)}(n) + 1$.
And finally:

(v) *The label of every node s of $T_{\frac{p}{q}}$ is $\pi_{\frac{p}{q}}(\mathrm{p}(s))$.*

We denote by $\mathsf{W}(n)$ (resp. by $\mathsf{w}(n)$) the label of the infinite path that starts from a node with label n and that follows always the edges with the maximal (resp. minimal) digit label. Such a word is said to be a *maximal* word (resp. a *minimal* word) in $T_{\frac{p}{q}}$. We note: $\mathbf{t}_{\frac{p}{q}} = \mathsf{W}(0)$ and $\boldsymbol{\omega}_{\frac{p}{q}} = \pi_{\frac{p}{q}}\left(\boldsymbol{.}\,\mathbf{t}_{\frac{p}{q}}\right)$. (It holds $\boldsymbol{\omega}_{\frac{p}{q}} < \frac{p-1}{p-q}$.)
The infinite word $\mathbf{t}_{\frac{p}{q}}$ is the maximal element with respect to the lexicographic order of the label of all infinite paths of $T_{\frac{p}{q}}$ that start from the root. Notice that, for any rational $\frac{p}{q}$, 0^ω is the minimal element with respect to the lexicographic order of the label of all infinite paths of $T_{\frac{p}{q}}$ and that, if $q = 1$, that is, in an integer base, $\mathsf{W}(n) = (p-1)^\omega$, and $\mathsf{w}(n) = 0^\omega$ for every n in $\mathbb{N}$.

Example 2.5.16 For $\frac{p}{q} = \frac{3}{2}$, $\mathbf{t}_{\frac{3}{2}} = 2\,1\,2\,2\,1\,1\,1\,2\,2\,1\,2\,1\,1\,2\,2\,1\,2\,1\,2\,1\,1\cdots$.

We call *branching* a node v of $T_{\frac{p}{q}}$ if it has at least two children, that is, if $\mathsf{e}(\pi_{\frac{p}{q}}(\mathrm{p}(v)))$ has at least two elements. Direct computations yields the following.

Lemma 2.5.17 *Let v be any branching node in $T_{\frac{p}{q}}$, and $n = \pi_{\frac{p}{q}}(\mathrm{p}(v))$ its label. Let a_1 and $b_1 = a_1 + q$ be in $\mathsf{e}(n)$ and let $m_1 = \psi_{a_1}(n)$ and $m_2 = \psi_{b_1}(n) = m_1 + 1$. Write $\mathsf{W}(m_1) = a_2\, a_3 \cdots$ and $\mathsf{w}(m_2) = b_2\, b_3 \cdots$. It then holds:*

$$\pi_{\frac{p}{q}}(\,.\,a_1\, a_2\, a_3 \cdots) = \pi_{\frac{p}{q}}(\,.\,b_1\, b_2\, b_3 \cdots) \quad . \tag{2.26}$$

2.5.2.2 The $\frac{p}{q}$-expansions of real numbers

Notation 2.5.18 Let us denote by $W_{\frac{p}{q}}$ the subset of $A_p^{\mathbb{N}}$ that consists of the labels of infinite paths starting from the root of $T_{\frac{p}{q}}$.

Note that the finite prefixes of the elements of $W_{\frac{p}{q}}$ are the words in $0^* L_{\frac{p}{q}}$. A direct consequence of Lemma 2.5.8 is the following.

Proposition 2.5.19 *If $q > 1$, then no element of $W_{\frac{p}{q}}$ is eventually periodic, but 0^ω.*

As announced, the set of $\frac{p}{q}$-expansions is defined *a priori* and not algorithmically.

Definition 2.5.20 The set of expansions in the $\frac{p}{q}$ numeration system is $W_{\frac{p}{q}}$.

In other words, an element u of $W_{\frac{p}{q}}$ is a $\frac{p}{q}$-expansion of the real $x = \pi_{\frac{p}{q}}(u)$ and conversely any element of $A_p^{\mathbb{N}}$ which does not belong to $W_{\frac{p}{q}}$ *is not* a $\frac{p}{q}$-expansion. The following Lemma 2.5.21 and Theorem 2.5.23 tell that $\frac{p}{q}$-expansions are not too many nor too few respectively and vindicate the definition.

Lemma 2.5.21 *The map $\pi_{\frac{p}{q}} : W_{\frac{p}{q}} \to \mathbb{R}$ is order preserving.*

Proof Let $u = (a_i)_{i\geq 1}$ and $v = (b_i)_{i \geq 1}$ be in $W_{\frac{p}{q}}$. If $u \leq v$ then, for every k in $\mathbb{N}$, $a_1\, a_2 \cdots a_k \leq b_1\, b_2 \cdots b_k$ and then, by Corollary 2.5.5, $\pi_{\frac{p}{q}}(a_1\, a_2 \cdots a_k) \leqslant \pi_{\frac{p}{q}}(b_1\, b_2 \cdots b_k)$. By (2.25), $\pi_{\frac{p}{q}}(\,.\,u) \leqslant \pi_{\frac{p}{q}}(\,.\,v)$. □

By contrast, it follows from the examples given after Corollary 2.5.5 that the map $\pi_{\frac{p}{q}} : A_p^{\mathbb{N}} \to \mathbb{R}$ is not order preserving.

Notation 2.5.22 Let $X_{\frac{p}{q}} = \pi_{\frac{p}{q}}\left(W_{\frac{p}{q}}\right)$. The elements of $X_{\frac{p}{q}}$ are non-negative real numbers less than or equal to $\boldsymbol{\omega}_{\frac{p}{q}}$:
$X_{\frac{p}{q}} \subseteq [0, \boldsymbol{\omega}_{\frac{p}{q}}]$.

Theorem 2.5.23 *Every real in* $[0, \boldsymbol{\omega}_{\frac{p}{q}}]$ *has at least one* $\frac{p}{q}$*-expansion, that is,* $X_{\frac{p}{q}} = [0, \boldsymbol{\omega}_{\frac{p}{q}}]$.

Proof By definition, the set $W_{\frac{p}{q}}$ is the set of infinite words w in $A_p^{\mathbb{N}}$ such that any prefix of w is in $0^* L_{\frac{p}{q}}$. As $0^* L_{\frac{p}{q}}$ is *prefix-closed* — since $L_{\frac{p}{q}}$ is prefix-closed *and* the empty word belongs to $L_{\frac{p}{q}}$ — $W_{\frac{p}{q}}$ is closed (see (Perrin and Pin 2003)) in the compact set $A_p^{\mathbb{N}}$, hence compact. Since $\pi_{\frac{p}{q}}$ is continuous, $X_{\frac{p}{q}}$ is closed.

Suppose that $[0, \boldsymbol{\omega}_{\frac{p}{q}}] \setminus X_{\frac{p}{q}}$ is a non-empty open set, containing a real t. Let $y = \sup\{x \in X_{\frac{p}{q}} \mid x < t\}$ and $z = \inf\{x \in X_{\frac{p}{q}} \mid x > t\}$. Since $X_{\frac{p}{q}}$ is closed, y and z both belong to $X_{\frac{p}{q}}$. Let $u = a_1 a_2 \cdots$ be the largest $\frac{p}{q}$-expansion of y and $v = b_1 b_2 \cdots$ the smallest $\frac{p}{q}$-expansion of z (in the lexicographic order). Of course, $u < v$ since $u \neq v$. Let $a_1 \cdots a_N$ be the *longest common prefix* of u and v (with the convention that N can be 0). Set $m = \pi_{\frac{p}{q}}(a_1 \cdots a_N \boldsymbol{.})$, $n = \pi_{\frac{p}{q}}(a_1 \cdots a_N a_{N+1} \boldsymbol{.})$ and $r = \pi_{\frac{p}{q}}(a_1 \cdots a_N b_{N+1} \boldsymbol{.})$. Then

$$u \leq a_1 \cdots a_N a_{N+1} \mathsf{W}(n) < a_1 \cdots a_N b_{N+1} \mathsf{w}(r) \leq v \ .$$

By the choice of v, $\pi_{\frac{p}{q}}(\boldsymbol{.} a_1 \cdots a_N a_{N+1} \mathsf{W}(n)) < z$, and by the choice of u, $u = a_1 \cdots a_N a_{N+1} \mathsf{W}(n)$. Symmetrically, $v = a_1 \cdots a_N b_{N+1} \mathsf{w}(r)$.

If $a_{N+1} + q < b_{N+1}$, then there exists a digit c in $\mathsf{e}(m)$ such that $a_{N+1} + q \leqslant c < b_{N+1}$. For any w' in $A_p^{\mathbb{N}}$ such that $w = a_1 \cdots a_N c w'$ is in $W_{\frac{p}{q}}$ (and there exist some), we have

$$u < w < v \ .$$

Whatever the value of $\pi_{\frac{p}{q}}(\boldsymbol{.} w)$, y or z, we have a contradiction with the extremal choice of u and v.

If $a_{N+1} + q = b_{N+1}$, then $r = n + 1$ and $z = y$ by Lemma 2.5.17, hence a contradiction. And thus $X_{\frac{p}{q}} = [0, \boldsymbol{\omega}_{\frac{p}{q}}]$. □

A word in $W_{\frac{p}{q}}$ is said to be *eventually maximal* (resp. *eventually minimal*) if it has a suffix which is a maximal (resp. minimal) word.

The following statement shows that in spite of the non-rationality of $W_{\frac{p}{q}}$ the $\frac{p}{q}$-expansions of reals behave very much as the expansions obtained by a greedy algorithm in an integer or in a real base.

Theorem 2.5.24 *The set of reals in $X_{\frac{p}{q}}$ that have more than one $\frac{p}{q}$-expansion is countably infinite in bijection with the set of branching nodes in $T_{\frac{p}{q}}$. The $\frac{p}{q}$-expansions of such reals are eventually maximal or eventually minimal. If $p \geqslant 2q-1$, then no real number has more than two $\frac{p}{q}$-expansions.*

Remark 2.5.25 In contrast with the classical representations of reals, the finite prefixes of a $\frac{p}{q}$-expansion of a real number, completed by zeroes, *are not* $\frac{p}{q}$-expansions of real numbers (though they can be given a value by the function π of course), that is to say, if a non-empty word w is in $L_{\frac{p}{q}}$, then the word $w\,0^{\omega}$ does not belong to $W_{\frac{p}{q}}$.

It is an open problem, a challenging one, to prove that the hypothesis $p \geqslant 2q-1$ in Theorem 2.5.24 is not necessary and that a real has never more than two $\frac{p}{q}$-expansions (with the meaning we have given to it) for any rational $\frac{p}{q}$.

2.6 A primer on finite automata and transducers

The matter developed in this chapter calls for definitions and results on finite automata and transducers that go beyond those given in Chapter **??** and we have gathered them in this section.

The notation follows the one adopted in (Sakarovitch 2003), where the proofs of the statements can be found as well — unless otherwise stated. The definitions are sometimes made simpler for their intended scope is the content of this chapter only.

2.6.1 Automata

Let us first complete the definitions and results on finite automata given at Chapter **??**. We call *recognisable* or *rational* the languages of A^* recognised by a finite automaton — that were rather called *regular* in Section **??** — and we denote this family by $\mathrm{Rat}\,A^*$. Since every finite automaton is equivalent to a deterministic one, we have:

Theorem 2.6.1 $\mathrm{Rat}\,A^*$ *is an effective Boolean algebra of languages.*

The *generating function* of a language L of A^* is the series

$$\Psi_L(X) = \sum_{n\in\mathbb{N}} \ell_n\, X^n$$

where ℓ_n is the number of words of L of length n: $\ell_n = \text{Card}\,(L \cap A^n)$.

A series $\Phi(X)$ is called a *rational function* if it is the quotient of two polynomials $P(X)$ and $Q(X)$ of $\mathbb{Z}[X]$: $\Phi(X) = \frac{P(X)}{Q(X)}$. A classical result in algebra states that a series $\Phi(X) = \sum_{n \in \mathbb{N}} a_n X^n$ is rational if, and only if, its coefficients a_n satisfy a linear recurrence relation with coefficients in $\mathbb{Z}$. The following result is not for nothing in the choice of *rational* rather than *regular* for languages recognised by finite automata.

Theorem 2.6.2 (Chomsky and Miller 1958) *The generating function of a rational language is a rational function.*

Proof Let $\mathcal{A}$ be a finite *deterministic* automaton (of dimension Q) which recognises the language L and let $\mathbf{M}$ be the *adjacency matrix* of $\mathcal{A}$. Write $\mathbf{l}(n)$ for the vector of dimension Q whose p-th entry is the number of words of length n which label paths from state p to a final state in $\mathcal{A}$: $\ell_n = \mathbf{l}_i(n)$ for the initial state i of $\mathcal{A}$. As $\mathcal{A}$ is deterministic, it holds

$$\forall n \in \mathbb{N} \;\; \mathbf{l}(n+1) = \mathbf{M}\,\mathbf{l}(n) \; . \tag{2.27}$$

By the Cayley–Hamilton Theorem, $\mathbf{M}$ is a zero of its *characteristic polynomial*, that is:

$$\mathbf{M}^k - z_1\,\mathbf{M}^{k-1} - \cdots - z_{k-1}\,\mathbf{M} - z_k\,\mathbf{I} = 0 \;\; ,$$

which by (2.27) yields a linear recurrence relation for the $\ell(n)$ and thus for their ith entries. □

A language L of A^* is said to have *bounded growth* if the coefficients of its generating function are uniformly bounded, that is, if for every n there are less than k words of length n in L, for a fixed integer k. If x, y, and z are words in A^*, the language $x\,y^*z$ is called a *ray language*. A ray language, or any finite union of ray languages, is rational and has bounded growth. The following converse is folklore (see (Sakarovitch 2003) and see also in Section **??**, the proof of Theorem **??**).

Proposition 2.6.3 *A rational language L has bounded growth if and only if it is a finite union of ray languages.*

An automaton is said to be k-*local* if the end of any computation of length k depends on its label only, and not on its origin. Remark that a 1-local automaton is deterministic.

2.6.2 Transducers

As defined in Chapter **??**, a transducer $\mathcal{T}$ (from A^* to B^*) is an automaton whose transitions are labelled by pairs of words (elements of $A^* \times B^*$). We write $\mathcal{T} = (\,Q, A, B, E, I, T\,)$ where $E \subseteq Q \times A^* \times B^* \times Q$ is the set of transitions and where I and T are subsets of Q which we consider as functions from Q into $\mathbb{B}$ in view of forthcoming generalisations. The transducer $\mathcal{T}$ is *finite* if E, and thus the useful part of Q, is finite.

The set of labels of successful computations, which we denote by $|\mathcal{T}|$, is a subset of $A^* \times B^*$, that is, the graph of a relation from A^* to B^*, the *relation realised by* $\mathcal{T}$. If $\mathcal{T}$ is finite, $|\mathcal{T}|$ is a *rational subset* of $A^* \times B^*$, hence realises a *rational relation.* If the labels of the transitions of a (finite) transducer $\mathcal{T}$ are projected on the first (resp. the second) component, we get a (finite) automaton, which we call the *(underlying) input automaton* (resp. the *(underlying) output automaton*) which recognises the domain (resp. the image) of the relation $|\mathcal{T}|$: both are rational languages of A^* (resp. of B^*). Remark also that *morphisms* (from a free monoid into another) are realised by one state transducers.

In contrast with Theorem 2.6.1, rational relations *are not closed under intersection*, and thus the set of rational relations is not a Boolean algebra. Moreover, as the Post Correspondence Problem may easily be described as the intersection of the graph of two morphisms, it is not decidable whether the intersection of two rational relations is empty, from which one deduces that equivalence of rational relations is not decidable.

On the positive side, rational relations from a free monoid into another one are *closed under composition*, and the image of a rational language by a rational relation is rational. From the definition itself follows that the inverse of a rational relation is a rational relation (it suffices to exchange the first and the second components of the labels).

The model of finite transducers may be transformed, without changing the class of realised relations, in order to allow various proofs. In particular, the initial and final functions (from Q to $\mathbb{B}$) may be generalised to functions from Q into $(\varepsilon \times B^*)$ — or, by abuse, from Q into B^* — together with the adequate, and obvious, modification of the definition of the label of a computation.

Figure 2.20 shows three transducers: one for the identity ι, one for ι_K the identity restricted to the rational set $K = a^*b^*$, that is, the intersection with K, and one for the relation γ' which maps every word w onto the set of words of the same length as w and greater in the lexicographic order (assuming that $a < b$).

As an example of the usefulness of rational relations in the study of ra-

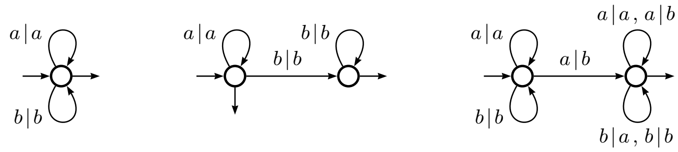


Fig. 2.20. Three transducers.

tional languages, let us give a simple and short proof of a classical property often credited to (Shallit 1994) and that appears several times in this chapter. If L is a language, we denote by $\mathsf{minlg}\,(L)$ (resp. $\mathsf{Maxlg}\,(L)$) the set of words of L which have no lesser (resp. greater) word of the same length in L in the lexicographic, or radix order (they coincide on words of the same length).

Proposition 2.6.4 *If* L *is a rational language, then so are* $\mathsf{minlg}\,(L)$ *and* $\mathsf{Maxlg}\,(L)$.

Proof Any word v of L which is greater (in the lexicographic order) than another word u of L of the same length belongs to $\iota_L(\gamma'(\iota_L(u)))$. Thus $\mathsf{minlg}\,(L) = L \setminus \mathsf{Im}[\iota_L \circ \gamma' \circ \iota_L]$, and is rational when L is.

An analogous equality holds for $\mathsf{Maxlg}\,(L)$. □

2.6.3 Synchronous transducers and relations

The three transducers of Figure 2.20 have the property that the label of every transition is a pair of letters, which immediately implies that they realise *length preserving* relations. Being length preserving however is somewhat too strong a restriction and this constraint is relaxed by allowing the replacement, in either component, of a letter by a padding symbol which does not belong to any alphabet — traditionally denoted by a \$ — under the 'padding condition', that is, no letter can appear after the padding symbol on the same component. Such transducers are called *synchronous transducers*. They realise *synchronous relations*,† obtained by the projection which erases the padding symbol, and the family of synchronous relations (from A^* into B^*) is denoted by $\mathrm{Syn}\, A^* \times B^*$.

The introduction of the padding symbol is more than a technical trick since in particular it is not decidable whether a given rational relation is synchronous or not (see (Frougny and Sakarovitch 1993)).

† In (Sakarovitch 2003), synchronous relations are defined as relations realised by letter-to-letter transducers whose final functions maps states into $(\mathrm{Rat}\, A^* \times \varepsilon) \cup (\varepsilon \times \mathrm{Rat}\, B^*)$. Hopefully, the two definitions are equivalent; the present one is preferred as it makes Theorem 2.6.5 and Theorem 2.6.6 more evident.

However synchronous relations are a very natural subfamily of rational relations and they have been given a logical characterisation in (Eilenberg, Elgot, and Shepherdson 1969). Most of the rational relations that are considered in this chapter are synchronous. Figure 2.21 shows a synchronous transducer for the complement of the identity ι, and one for the relation γ which maps every word w onto the set of words which are greater than w in the radix order.

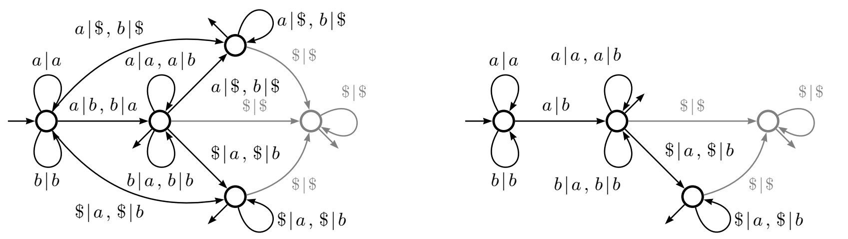


Fig. 2.21. Two synchronous transducers.

Thanks to the following two properties, Syn $A^* \times B^*$ provides a family of rational relations which can be fruitfully used in constructions and proofs. The first one follows from the fact that the pairs of letters from two alphabets can be considered as letters from the product alphabet and thus synchronous tranducers as finite automata.

Theorem 2.6.5 Syn $A^* \times B^*$ *is an effective Boolean algebra of rational relations.*

Theorem 2.6.6 Syn $A^* \times B^*$ *is closed under composition.*

Let $\mathcal{T} = (\,Q, A_\$, B_\$, E, I, T\,)$ and $\mathcal{U} = (\,R, B_\$, C_\$, F, J, U\,)$ be two synchronous transducers which realise the two relations $|\mathcal{T}|\colon A^* \to B^*$ and $|\mathcal{U}|\colon B^* \to C^*$ respectively. Let then $\mathcal{T} \circ \mathcal{U}$ be the synchronous transducer $\mathcal{T} \circ \mathcal{U} = (\,Q \times R, A_\$, C_\$, G, I \times J, T \times U\,)$ defined by

$$G = \{\big((p,r),(a,c),(q,s)\big) \mid \exists b \in B_\$ \quad \big(p,(a,b),q\big) \in E, \big(r,(b,c),s\big) \in F\} \;..$$

Without loss of generality, we can assume that both $\mathcal{T}$ and $\mathcal{U}$ are completed by transitions labelled by $(\$, \$)$ and that go from every final state to a sink state equipped with a loop labelled in the same way (the grey part in the transducers of Figure 2.21). Under this assumption, it is a formality to check that $\mathcal{T} \circ \mathcal{U}$ realises the relation $|\mathcal{U}| \circ |\mathcal{T}|\colon A^* \to C^*$. This construction is used at § 2.2.2.2 for the construction of $\mathcal{W}_2''$.

The fruitfulness of the notion is visible in establishing the following property. If A is a totally ordered alphabet, the *radix order* is a well-ordering on A^* and thus on any of its subset L; we denote by Succ_L the function which maps every word of L onto its successor in L in the radix order.

Proposition 2.6.7 *If L is a rational language, then* Succ_L *is a synchronous (functional) relation.*

Proof As above, we write γ the relation which maps every word w onto the set of words which are greater than w in the radix order. For any subset K of A^*, $\min(K) = K \setminus \gamma(K)$. For any word u of L, the set of words of L that are greater than u is $\iota_L(\gamma(\iota_L(u)))$. Hence $\mathrm{Succ}_L(u) = \min(\iota_L(\gamma(\iota_L(u)))) = \iota_L(\gamma(\iota_L(u))) \setminus \gamma(\iota_L(\gamma(\iota_L(u))))$ and $\mathrm{Succ}_L = \iota_L \circ \gamma \circ \iota_L \setminus \gamma \circ \iota_L \circ \gamma \circ \iota_L$ is a synchronous relation by Theorem 2.6.5 and Theorem 2.6.6. □

Remark 2.6.8 If we take a slightly more general definition for the successor function, namely, a function ω whose restriction on L realises Succ_L, we may find *non-rational languages* whose successor fonction is realised by a finite (letter-to-letter right) transducer. In this case, L is strictly contained in $\mathsf{Dom}\,\omega$. Such an example is given by the numeration system in rational base (see Section 2.5).

2.6.4 The left-right duality

Before studying further specialised classes of transducers, let us recall and precise the conventions and terminology relative to the duality between the *left-to-right* and *right-to-left* reading.

The *transpose* of a word of A^*, $w = a_1 a_2 \cdots a_n$, with the a_i's in A, is the word $w^t = a_n a_{n-1} \cdots a_1$, that is, the sequence of letters obtained by reading w *from right to left.* Transposition is additively extended to subsets of A^*: $L^t = \bigcup_{w \in L} w^t$.

The *transpose* of an automaton $\mathcal{A} = (\, Q, A, E, I, T\,)$, is the automaton $\mathcal{A}^t = (\, Q, A, E^t, T, I\,)$ where $E^t = \{(q,a,p) \mid (p,a,q) \in E\}$. Obviously, $L(\mathcal{A}^t) = [L(\mathcal{A})]^t$.

A number of properties of automata are *directed*, that is, corresponds to properties of the reading of words from left to right; *e.g.* being deterministic. If $\mathcal{A}^t$ has such a property P, $\mathcal{A}$ is said to have the property *co-P*. For instance, $\mathcal{A}$ is *co-deterministic* if $\mathcal{A}^t$ is deterministic.

Another way to bring the left-right duality into play is to consider *right automata*, that is, automata that read words *from right to left* (a procedure that can prove to be natural when reading numbers: from least to most significant digit). It amounts to the same thing to say that w is accepted by a right automaton $\mathcal{A}$ or that it is accepted by the (left) automaton $\mathcal{A}^t$.

These notions go over to transducers. The *transpose* of a transducer $\mathcal{T} = (Q, A, B, E, I, T)$, is the transducer $\mathcal{T}^t = (Q, A, B, E^t, T, I)$ where $E^t = \{(q, (f^t, g^t), p) \mid (p, (f, g), q) \in E\}$ and $|\mathcal{T}^t| = |\mathcal{T}|^t$. A *right transducer* reads the input word, and 'write' the output word from right to left. As above, the relation realised by a right transducer $\mathcal{T}$ is the same as the one realised by the (left) transducer $\mathcal{T}^t$.

Being synchronous is a *directed* notion, because of the 'padding condition' or, to state it in another way, because the padding symbols are written at the *right end* of words, and we have (implicitly) defined it for (left) transducer, thus we have defined the *left synchronous relations*. A relation is *co-synchronous* — we also say *right synchronous* if it is realised by a synchronous right transducer, or by the transpose of a synchronous transducer. In general, a left synchronous relation is not a right synchronous one. Relations that are both left and right synchronous have been characterised recently (Carton 2009). We consider below an important particular case of such relations.

2.6.5 Letter-to-letter transducers and bld-relations

We call *letter-to-letter transducer* (with a slight abuse of words) a transducer whose transitions are labelled by pairs of letters *and* whose initial and final functions map states into $(A^* \times \varepsilon) \cup (\varepsilon \times B^*)$. In a relation realised by such a transducer, the lengths of a word and its images are not necessarily equal but their difference is bounded. More important, the converse of this simple observation is true.

Let $\theta \colon A^* \to B^*$ be a relation with the property that there exists an integer k such that, for every f in A^* and every g in $\theta(f)$, then $\big||f| - |g|\big| \leqslant k$. If $k = 0$, θ is a *length preserving relation*; for an arbitrary k, θ has been called a *bounded length difference relation* ((Frougny and Sakarovitch 1993)) or *bounded length discrepancy relation* ((Sakarovitch 2003)), *bld-relation* for short in any case.

It is not difficult to verify that a rational relation is bld if, and only if, any transducer $\mathcal{T}$ (without padding symbol!) which realises θ has the property that the label of every circuit in $\mathcal{T}$ is such that the length of the 'input' is equal to the length of the 'output', a property which is thus decidable. The following result is essentially due to Eilenberg who proves it for length-preserving relations ((Eilenberg 1974)); it has been extended to bld-relations in (Frougny and Sakarovitch 1993). It relates a property of the graph of a rational relation (being bld) to the way this relation may be realised (being synchronous).

Proposition 2.6.9 *A bld-rational relation is both left and right synchronous.*

The next characterisation of bld relations within synchronous ones goes back to (Elgot and Mezei 1965).

Proposition 2.6.10 *A left (or right) synchronous relation with finite image and finite co-image is a bld-rational relation.*

Corollary 2.6.11 *If L is a rational language, then* Succ_L *is realised by a finite letter-to-letter transducer*

2.6.6 Sequential transducers and functions

A transducer (from A^* to B^*) is said to be *sequential* (resp. *co-sequential*) if its underlying input automaton is *deterministic* (resp. *co-deterministic*) and the initial and final functions map its states into $\varepsilon{\times}B^*$. this definition, a sequential, or co-sequential, transducer realises a *functional* relation. A function (from A^* to B^*) is said to be *sequential* (resp. *co-sequential*) if it is realised by a *sequential* (resp. *co-sequential*) transducer. Of course, a co-sequential function is realised by a sequential right transducer.

Sequential functions are characterised within rational functions by a topological criterion in the following way: the *prefix distance* d of two words u and v is defined as $\mathrm{d}\,(u,v) = |u| + |v| - 2\,|u \wedge v|$, where $u \wedge v$ is the *longest common prefix* of u and v.

Definition 2.6.12 A function φ is said to be k-Lipschitz (for the prefix distance) if:

$$\forall u, v \in \mathsf{Dom}\,\varphi \quad , \quad \mathrm{d}\,(\varphi(u), \varphi(v)) \leq k\,\mathrm{d}\,(u,v) \quad .$$

The function φ is Lipschitz if there exists a k such that φ is k-Lipschitz.

Theorem 2.6.13 (Choffrut 1977) *A rational function is sequential if, and only if, it is Lipschitz.*

By the left-right duality, we define the *suffix distance* d_s on A^*: $\mathrm{d}_s\,(u,v) = |u| + |v| - 2\,|u \wedge_s v|$, where $u \wedge_s v$ is the *longest common suffix* of u and v. A rational function is co-sequential if, and only if, it is Lipschitz for the suffix distance. At this point, it cannot be skipped that sequentiality is a decidable property for functions realised by finite transducers (see (Choffrut 1977)) although this does not play any role in this chapter.

We call *piecewise (co-)sequential* a function that is a finite union of (co-)sequential functions (thus with disjont domains). And we have the following.

Proposition 2.6.14 (Angrand and Sakarovitch 2009) *If L is a rational language, then* Succ_L *is a piecewise co-sequential function.*

2.7 Notes

As we have already mentioned, we consider only *positional* numeration systems. However, we indicate a pioneer work on the relations between numeration and finite automata, which is the paper (Raney 1973), in which it is proved that the continued fractions expansion of a real number can be coded by an infinite word on a two-letter alphabet, and that homographic transformations can be realised by finite transducers.

2.7.1 Representation in integer base

On the links between numeration, logic and finite automata there is a survey (Bruyère, Hansel, Michaux, and Villemaire 1994).

A generalisation of Cobham's Theorem to real numbers has been established in a series of papers (Boigelot and Brusten 2009, Boigelot, Brusten, and Bruyère 2008). It is proved in particular that, if a set S of positive real numbers is recognised by a finite weak deterministic automaton in two integer bases that are multiplicatively independent, then S is definable in $\langle \mathbb{R}, \mathbb{Z}, +, < \rangle$, which means that S is a finite union of intervals with rational endpoints.

2.7.2 Representation in real base

Symbolic dynamical systems defined by a particular order on the set of infinite words on a finite alphabet have been studied from an ergodic point of view in (Takahashi 1980).

An algebraic integer $\beta > 1$ is a *Salem number* if all its Galois conjugates have modulus ≤ 1, with at least one conjugate with modulus 1. It has been proved in (Boyd 1989) that every Salem number of degree 4 is a Parry number. Boyd also conjectured that it is still true in degree 6, but false for degree ≥ 8. An algebraic integer $\beta > 1$ is a *Perron number* if all its Galois conjugates have modulus $< \beta$. Perron numbers are introduced in

(Lind 1984). Every Parry number is a Perron number. In (Solomyak 1994) and in (Flatto, Lagarias, and Poonen 1994) is proved that all the Galois conjugates of a Parry number have modulus strictly less than the Golden Ratio. Beta-expansions also appear in the mathematical description of quasicrystals, see (Gazeau, Nešetřil, and B. Rovan, eds 2007).

The study of the β-shift from the point of view of the Chomsky hierarchy has been done by K. Johnson. A symbolic dynamical system is said to be *context-free* if the set of its finite admissible factors is a context-free language. It is proved in (Johnson 1999) that the β-shift is context-free if, and only if, it is sofic.

In Section 2.2.2.3 we have presented expansions of minimal weight in base 2. Recently, the investigation of minimal weight expansions has been extended to the Fibonacci numeration system in (Heuberger 2004), and an equivalent to the NAF has been defined. When β is a Pisot number the set of β-expansions of minimal weight, where the weight is the absolute sum of the digits, is recognisable by a finite automaton, (Frougny and Steiner 2008). For the Golden Ratio φ the average weight of φ-expansions on the alphabet $\{-1,0,1\}$ of the numbers of absolute value less than M is $\frac{1}{5}\log_\varphi M$, which means that typically only every fifth digit is non-zero. Note that the corresponding value for 2-expansions of minimal weight is $\frac{1}{3}\log_2 M$, see (Arno and Wheeler 1993, Bosma 2001), and that $\frac{1}{5}\log_\varphi M \approx 0.288\log_2 M$.

Fractals and tilings are the subject of Chapter **??** of this book. Let us just mention some works using finite automata associated with numeration in an irrational base. The celebrated Rauzy fractal is associated with numeration in base the *Tribonacci number* which is the root >1 of the polynomial X^3-X^2-X-1. The boundary of the Rauzy fractal (and of more general fractals associated with Pisot numbers) has been described by a finite automaton in (Messaoudi 1998, Messaoudi 2000) and (Durand and Messaoudi 2009).

Finite automata and substitutions are treated in (Pytheas Fogg 2002, Chapter 7). (Canterini and Siegel 2001a, Canterini and Siegel 2001b) have defined the prefix-suffix automaton associated with a substitution of Pisot type.

Beta-expansions have been extended to finite fields by (Hbaib and Mkaouar 2006) and (Scheicher 2007). Here β is an element of the field of formal Laurent series $\mathbb{F}((X^{-1}))$, with $|\beta|>1$. The main difference with the classical real base is that all the expansions are admissible. Moreover the (F) Property is satisfied if and only if β is a Pisot element of $\mathbb{F}((X^{-1}))$, that is to say, β is an algebraic integer over $\mathbb{F}[X]$ such that for all Galois conjugate $|\beta_i|<1$ (Scheicher 2007).

2.7.3 Canonical numeration systems

In the case where the alphabet associated with a number β is $A_\beta = \{0, 1, \ldots, N(\beta) - 1\}$, the 'clearing algorithm' of (Gilbert 1981) gives an easy way of computing the expansion of an integer in the system (β, A_β).

Tilings generated by a canonical numeration system have been investigated by many authors. The first one is probably the *twin dragon* tiling, linked to the Penney CNS defined by the base $-1 + i$, which was obtained by Knuth as the set $\{z \in \mathbb{C} \mid z = \sum_{j \geq 0} d_j (-1 + i)^{-j}, d_j \in \{0, 1\}\}$, see (Knuth 1998).

There are interesting contributions on fractals and tilings in (Gilbert 1991), (Scheicher and Thuswaldner 2002) and (Akiyama and Thuswaldner 2005).

There have been a number of generalisations of CNS. Let us mention that the case where β is not an algebraic integer but an algebraic number has been considered in particular in (Gilbert 1991). It is mentioned that for any rational $p/q > 1$, $\beta = -p/q$ with digit set $\{0, 1, \ldots, p - 1\}$ forms a CNS in which any number of $\mathbb{Z}[1/q]$ has a finite representation.

Scheicher and Thuswaldner investigated number systems in polynomial rings over finite fields (Scheicher and Thuswaldner 2003).

2.7.4 Representation in rational base

Expansions in rational base are linked to the problem of the distribution of the fractional part of the powers of rational numbers.

The distribution modulo 1 of the powers of a rational number, indeed the problem of proving whether they form a dense set or not, is an old problem. Pisot, Vijayaraghavan and André Weil have shown that there are infinitely many limit points. With this problem as a background, Mahler asked in (Mahler 1968) whether there exists a non-zero real z such that the fractional part of $z\,(3/2)^n$ for $n = 0, 1, \ldots$ fall into $[0, 1/2[$. It is not known whether such a real — called a Z-number — does exist but Mahler showed that the set of Z-numbers is at most countable. His proof is based on the fact that the fractional part of a Z-number (if it exists) has an expansion in base $3/2$ which is entirely determined by its integral part.

Koksma proved that for almost every real number $\theta > 1$ the sequence $(\{\theta^n\})_n$ is uniformly distributed in $[0, 1]$, but very few results are known for specific values of θ. One of these is that *if θ is a Pisot number*, then the above sequence converges to 0 if we identify $[0, 1[$ with $\mathbb{R}/\mathbb{Z}$.

The next step in attacking this problem has been *to fix the rational* $\frac{p}{q}$

and to study the distribution of the sequence

$$f_n(z) = \left\{ z \left(\frac{p}{q}\right)^n \right\}$$

according to the value of the real number z. Once again, the sequence $f_n(z)$ is uniformly distributed for almost all $z > 0$, but nothing is known for specific values of z.

In the search for z's for which the sequence $f_n(z)$ is *not uniformly distributed*, Mahler considered those for which the sequence is eventually contained in $\left[0, \frac{1}{2}\right[$. Mahler's notation is generalized as follow: let I be a (strict) subset of $[0, 1[$ and let

$$\mathbf{Z}_{\frac{p}{q}}(I) = \{z \in \mathbb{R} \mid \left\{ z \left(\frac{p}{q}\right)^n \right\} \quad \text{stays eventually in } I \ \} \ .$$

Mahler's problem is to ask whether $\mathbf{Z}_{\frac{3}{2}}\left(\left[0, \frac{1}{2}\right[\right)$ is empty or not.

Mahler's work has been developed in two directions: the search for subsets I as large as possible such that $\mathbf{Z}_{\frac{p}{q}}(I)$ is empty and conversely the search for subsets I as small as possible such that $\mathbf{Z}_{\frac{p}{q}}(I)$ is non-empty.

Along the first line, remarkable progress has been made by Flatto *et al.* (Flatto, Lagarias, and Pollington 1995) who proved that the set of reals s such that $\mathbf{Z}_{\frac{p}{q}}\left(\left[s, s + \frac{1}{p}\right[\right)$ is empty is *dense* in $[0, 1 - \frac{1}{p}]$, and Bugeaud (Bugeaud 2004) proved that its complement is of Lebesgue measure 0. Along the other line, Pollington (Pollington 1981) showed that $\mathbf{Z}_{\frac{3}{2}}\left(\left[\frac{4}{65}, \frac{61}{65}\right[\right)$ is non-empty.

It is proved in (Akiyama, Frougny, and Sakarovitch 2008) that if $p \geqslant 2q - 1$, there exists a subset $Y_{\frac{p}{q}}$ of $[0, 1[$, of Lebesgue measure $\frac{q}{p}$, such that $\mathbf{Z}_{\frac{p}{q}}\left(Y_{\frac{p}{q}}\right)$ is countably infinite. The elements of $\mathbf{Z}_{\frac{p}{q}}\left(Y_{\frac{p}{q}}\right)$ are indeed the reals which have two $\frac{p}{q}$-expansions. Coming back to the historical 3/2 case, we have that the set of positive numbers z such that $\left\{ z \left(\frac{3}{2}\right)^n \right\} \in [0, 1/3[\cup [2/3, 1[$ for $n = 0, 1, 2, \ldots$ is countably infinite. It is noteworthy that the expansion 'computed' by Mahler for his Z-numbers happens to be exactly one of the $\frac{3}{2}$-expansions presented in Section 2.5 — if it exists.

References

[Akiyama and Pethő 2002] Akiyama, S. and Pethő, A. On Canonical Number Systems. *Theoret. Comput. Sci.* **270**, (2002) 921–933.

[Akiyama and Rao 2005] Akiyama, S. and Rao, H. New criteria for canonical number systems. *Acta Arith.* **111**, (2005) 5–25.

[Akiyama and Scheicher 2005] Akiyama, S. and Scheicher, K. From number systems to shift radix systems. *Nihonkai Math. J.* **16**, (2005) 95–106.

[Akiyama and Thuswaldner 2005] Akiyama, S. and Thuswaldner, J. On the Topological Structure of Fractal Tilings Generated by Quadratic Number Systems. *Comput. Math. Appl.* **49**, (2005) 1439–1485.

[Akiyama, Borbély, Brunotte, Pethő, and Thuswaldner 2005] Akiyama, S., Borbély, T., Brunotte, H., Pethő, A., and Thuswaldner, J. Generalized radix representations and dynamical systems I. *Acta Math. Hungarica* **108**, (2005) 207–238.

[Akiyama, Frougny, and Sakarovitch 2008] Akiyama, S., Frougny, C., and Sakarovitch, J. Powers of rationals modulo 1 and rational base number systems. *Israel J. Math.* **168**, (2008) 53–91.

[Akiyama 2000] Akiyama, S. Cubic Pisot units with finite beta expansions. In F. Halter-Koch and R. F. Tichy, eds., *Algebraic Number Theory and Diophantine Analysis*, pp. 11–26. Walter de Gruyter, 2000.

[Angrand and Sakarovitch 2009] Angrand, P.-Y. and Sakarovitch, J. Radix enumeration of rational languages. *RAIRO Inform. Théor. App.* **nnn**, (2009) xxx–yyy. To appear.

[Arno and Wheeler 1993] Arno, S. and Wheeler, F. S. Signed Digit Representations of Minimal Hamming weight. *IEEE Trans. Comput.* **42**, (1993) 1007–1010.

[Avizienis 1961] Avizienis, A. Signed-digit number representations for fast parallel arithmetic. *IRE Trans. Electron. Comput.* **10**, (1961) 389–400.

[Barat, Berthé, Liardet, and Thuswaldner 2006] Barat, G., Berthé, V., Liardet, P., and Thuswaldner, J. Dynamical directions in numeration. *Ann. Inst. Fourier (Grenoble)* **56**, (2006) 1987–2092.

[Béal 1993] Béal, M.-P. *Codage symbolique.* Masson, 1993.

[Berend and Frougny 1994] Berend, D. and Frougny, C. Computability by finite automata and Pisot bases. *Math. Systems Theory* **27**, (1994) 275–282.

[Bertrand-Mathis 1986] Bertrand-Mathis, A. Développements en base θ, répartition modulo un de la suite $(x\theta^n)_{n\geq 0}$, langages codés et θ-shift. *Bull. Soc. Math. France* **114**(3), (1986) 271–323.

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

[Bertrand 1977] Bertrand, A. Développements en base de Pisot et répartition modulo 1. *C. R. Acad. Sci. Paris Sér. A-B* **285**(6), (1977) A419–A421.

[Bès 2000] Bès, A. An extension of the Cobham-Semenov Theorem. *Journal of Symbolic Logic* **65**, (2000) 201–211.

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

[Blanchard 1989] Blanchard, F. β-expansions and symbolic dynamics. *Theoret. Comput. Sci.* **65**, (1989) 131–141.

[Boigelot and Brusten 2009] Boigelot, B. and Brusten, J. A Generalization of Cobham's Theorem to Automata over Real Numbers. *Theoret. Comput. Sci.* **410**, (2009) 1694–1703.

[Boigelot, Brusten, and Bruyère 2008] Boigelot, B., Brusten, J., and Bruyère, V.

On the Sets of Real Numbers Recognized by Finite Automata in Multiple Bases. In *ICALP 2008, LNCS 5126*, pp. 112–123. Springer, 2008.

[Booth 1951] Booth, A. D. A signed binary multiplication technique. *Quart. J. Mech. Appl. Math.* **4**, (1951) 236–240.

[Bosma 2001] Bosma, W. Signed bits and fast exponentiation. *J. Théorie Nombres Bordeaux* **13**, (2001) 27–41.

[Boyd 1989] Boyd, D. W. Salem numbers of degree four have periodic expansions. In J. H. de Coninck and C. Levesque, eds., *Number Theory*, pp. 57–64. Walter de Gruyter, 1989.

[Brunotte, Huszti, and Pethő 2006] Brunotte, H., Huszti, A., and Pethő, A. Bases of canonical number systems in quartic algebraic number fields. *J. Théorie Nombres Bordeaux* **18**, (2006) 537–557.

[Brunotte 2001] Brunotte, H. On trinomial bases of radix representation of algebraic integers. *Acta Sci. Math. (Szeged)* **67**, (2001) 553–559.

[Brunotte 2002] Brunotte, H. Characterisation of CNS trinomials. *Acta Sci. Math. (Szeged)* **68**, (2002) 673–679.

[Bruyère, Hansel, Michaux, and Villemaire 1994] Bruyère, V., Hansel, G., Michaux, C., and Villemaire, R. Logic and p-recognizable sets of integers. *Bull. Belg. Math. Soc.* **1**, (1994) 191–238. Corrigendum, *Bull. Belg. Math. Soc.* **1** (1994), 577.

[Bugeaud 2004] Bugeaud, Y. Linear mod one transformations and the distribution of fractional parts $\{\xi(\frac{p}{q})^n\}$. *Acta Arith.* **114**, (2004) 301–311.

[Canterini and Siegel 2001a] Canterini, V. and Siegel, A. Automate des préfixes-suffixes associé à une substitution primitive. *J. Théorie Nombres Bordeaux* **13**, (2001) 353–369.

[Canterini and Siegel 2001b] Canterini, V. and Siegel, A. Geometric representation of substitutions of Pisot type. *Trans. Amer. Math. Soc.* **353**, (2001) 5121–5144.

[Carton 2009] Carton, O. Left and right synchronous relations. In *DLT 2009, LNCS 5583*, pp. 170–182. Springer, 2009.

[Cauchy 1840] Cauchy, A. Sur les moyens d'éviter les erreurs dans les calculs numériques. *C. R. Acad. Sci. Paris* **11**, (1840) 789–798. Reprinted in A. Cauchy, *Œuvres complètes*, 1ère série, Tome V, Gauthier-Villars, 1885, pp. 431-442.

[Choffrut 1977] Choffrut, C. Une caractérisation des fonctions séquentielles et des fonctions sous-séquentielles en tant que relations rationnelles. *Theoret. Comput. Sci.* **5**, (1977) 325–337.

[Chomsky and Miller 1958] Chomsky, N. and Miller, G. A. Finite state languages. *Information and Control* **1**, (1958) 91–112.

[Chow and Robertson 1978] Chow, C. and Robertson, J. Logical design of a redundant binary adder. In *Proceedings of the 4th Symposium on Computer Arithmetic*, pp. 109–115. IEEE Computer Society Press, 1978.

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

[Cohen 1981] Cohen, D. On Holy Wars and a Plea for Peace. *Computer* **14**, (1981) 48–54.

[Durand and Messaoudi 2009] Durand, F. and Messaoudi, A. Boundary of the Rauzy fractal sets in $\mathbb{R} \times \mathbb{C}$ generated by $P(x) = x^4 - x^3 - x^2 - x - 1$. *Osaka J. Math.* To appear.

[Eilenberg, Elgot, and Shepherdson 1969] Eilenberg, S., Elgot, C. C., and Shepherdson, J. C. Sets recognized by n-tape automata. *J. Algebra* **13**, (1969) 447–464.

[Eilenberg 1974] Eilenberg, S. *Automata, Languages, and Machines*, vol. A. Academic Press, 1974.

[Elgot and Mezei 1965] Elgot, C. C. and Mezei, J. E. On relations defined by generalized finite automata. *IBM J. Res. Develop.* **9**, (1965) 47–68.

[Flatto, Lagarias, and Pollington 1995] Flatto, L., Lagarias, J., and Pollington, A. On the range of fractional parts $\{\xi(p/q)^n\}$. *Acta Arith.* **70**, (1995) 125–147.

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

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

[Frougny and Sakarovitch 1993] Frougny, C. and Sakarovitch, J. Synchronized relations of finite and infinite words. *Theoret. Comput. Sci.* **18**, (1993) 45–82.

[Frougny and Sakarovitch 1999] Frougny, C. and Sakarovitch, J. Automatic conversion from Fibonacci representation to representation in base φ, and a generalization. *Internat. J. Algebra Comput.* **9**, (1999) 351–384.

[Frougny and Solomyak 1992] Frougny, C. and Solomyak, B. Finite beta-expansions. *Ergod. Th. & Dynam. Sys.* **12**, (1992) 713–723.

[Frougny and Solomyak 1996] Frougny, C. and Solomyak, B. On representation of integers in linear numeration systems. In M. Pollicott and K. Schmidt, eds., *Ergodic Theory of* $\mathbb{Z}^d$ *Actions (Warwick, 1993–1994)*, vol. 228 of *London Mathematical Society Lecture Note Series*, pp. 345–368. Cambridge University Press, 1996.

[Frougny and Solomyak 1999] Frougny, C. and Solomyak, B. On the context-freeness of the theta-expansions of the integers. *Internat. J. Algebra Comput.* **9**, (1999) 347–350.

[Frougny and Steiner 2008] Frougny, C. and Steiner, W. Minimal weight expansions in Pisot bases. *Journal of Mathematical Cryptology* **2**, (2008) 365–392.

[Frougny 1992] Frougny, C. Representations of numbers and finite automata. *Math. Systems Theory* **25**, (1992) 37–60.

[Frougny 1997] Frougny, C. On the sequentiality of the successor function. *Inform. Comput.* **139**, (1997) 17–38.

[Frougny 2002] Frougny, C. On multiplicatively dependent linear numeration systems, and periodic points. *Theoret. Informatics Appl.* **36**, (2002) 293–314.

[Gazeau, Nešetřil, and B. Rovan, eds 2007] Gazeau, J., Nešetřil, J., and B. Rovan, eds. *Physics and Theoretical Computer Science*. IOS Press, 2007.

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

[Gilbert 1991] Gilbert, W. J. Gaussian integers as bases for exotic number systems, 1991. Unpublished manuscript.

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

[Grünwald 1885] Grünwald, V. Intorno all'aritmetica dei sistemi numerici a base negativa con particolare riguardo al sistema numerico a base negativo-decimale per lo studio delle sue analogie coll'aritmetica (decimale). *Giornale di Matematiche di Battaglini* **23**, (1885) 203–221. Errata, p. 367.

[Hbaib and Mkaouar 2006] Hbaib, M. and Mkaouar, M. Sur le bêta-développement de 1 dans le corps des séries formelles. *Int. J. Number Theory* **2**, (2006) 365?378.

[Heuberger 2004] Heuberger, C. Minimal expansions in redundant number systems: Fibonacci bases and greedy algorithms. *Period. Math. Hungar.* **49**(2), (2004) 65–89.

[Hollander 1996] Hollander, M. *Linear Numeration systems, Finite Beta Expansions, and Discrete Spectrum of Substitution Dynamical Systems.* Ph.D. thesis, University of Washington, 1996.

[Hollander 1998] Hollander, M. Greedy numeration systems and regularity. *Theory Comput. Systems* **31**, (1998) 111–133.

[Hopcroft, Motwani, and Ullman 2006] Hopcroft, J. E., Motwani, R., and Ullman, J. D. *Introduction to Automata Theory, Languages, and Computation.* Addison-Wesley, 2006. 3rd Edition.

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

[Johnson 1999] Johnson, K. *Beta-shift, Dynamical Systems and Their Associated Languages.* Ph.D. thesis, University of North Carolina at Chapel Hill, 1999.

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

[Kátai and Szabó 1975] Kátai, I. and Szabó, J. Canonical number systems for complex integers. *Acta Sci. Math. (Szeged)* **37**, (1975) 255–260.

[Knuth 1998] Knuth, D. E. *The Art of Computer Programming. Volume 2: Seminumerical Algorithms.* Addison-Wesley, 1998. 3nd edition.

[Kovács 1981] Kovács, B. Canonical number systems in algebraic number fields. *Acta Math. Hung.* **37**, (1981) 405–407.

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

[Loraud 1995] Loraud, N. β-shift, systèmes de numération et automates. *J. Théorie Nombres Bordeaux* **7**, (1995) 473–498.

[Lothaire 2002] Lothaire, M. *Algebraic Combinatorics on Words*, vol. 90 of *Encyclopedia of Mathematics and Its Applications.* Cambridge University Press, 2002.

[Mahler 1968] Mahler, K. An unsolved problem on the powers of 3/2. *J. Austral. Math. Soc.* **8**, (1968) 313–321.

[Messaoudi 1998] Messaoudi, A. Propriétés arithmétiques et dynamiques du fractal de Rauzy. *J. Théorie Nombres Bordeaux* **10**, (1998) 135–162.

[Messaoudi 2000] Messaoudi, A. Frontière du fractal de Rauzy et systèmes de numération complexes. *Acta Arith.* **95**, (2000) 195–224.

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

[Pascal 1963] Pascal, B. *Œuvres complètes.* Seuil, 1963. The treatise *De numeris multiplicibus*, written with the other arithmetical treatises before 1654, was published by Guillaume Desprez in 1665.

[Penney 1964] Penney, W. A numeral system with a negative base. *Math. Student Journal* **11**(4), (1964) 1–2.

[Perrin and Pin 2003] Perrin, D. and Pin, J.-E. *Infinite Words: Automata, Semigroups, Logic and Games*, vol. 141 of *Pure and Applied Mathematics.* Academic Press, 2003.

[Pollington 1981] Pollington, A. Progressions arithmétiques généralisées et le problème des $(3/2)^n$. *C.R. Acad. Sc. Paris série I* **292**, (1981) 383–384.

[Pytheas Fogg 2002] Pytheas Fogg, N. *Substitutions in Dynamics, Arithmetics and Combinatorics*, vol. 1794 of *Lecture Notes in Mathematics.* Springer-Verlag, 2002. Ed. by V. Berthé and S. Ferenczi and C. Mauduit and A. Siegel.

[Raney 1973] Raney, G. N. On continued fractions and finite automata. *Math. Annalen* **206**, (1973) 265–283.

[Reitwiesner 1960] Reitwiesner, G. W. Binary arithmetic. In F. L. Alt, ed., *Advances in Computers*, vol. 1, pp. 231–308. Academic Press, 1960.

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

[Rosenberg 1967] Rosenberg, A. A machine realization of the linear context-free languages. *Information and Control* **10**, (1967) 175–188.

[Safer 1998] Safer, T. Radix representations of algebraic number fields and finite automata. In M. Morvan, C. Meinel, and D. Krob, eds., *STACS 98, Proc. 15th Symp. Theoretical Aspects of Comp. Sci.*, vol. 1373 of *Lecture Notes in Computer Science*, pp. 356–365. Springer-Verlag, 1998.

[Sakarovitch 2003] Sakarovitch, J. *Éléments de théorie des automates.* Vuibert, 2003. English corrected edition: *Elements of Automata Theory*, Cambridge University Press, 2009.

[Scheicher and Thuswaldner 2002] Scheicher, K. and Thuswaldner, J. M. Canonical number systems, counting automata and fractals. *Math. Proc. Camb. Philos. Soc.* **133**, (2002) 163–182.

[Scheicher and Thuswaldner 2003] Scheicher, K. and Thuswaldner, J. M. Digit systems in polynomial rings over finite fields. *Finite Fields Appl.* **9**, (2003) 322–333.

[Scheicher and Thuswaldner 2004] Scheicher, K. and Thuswaldner, J. M. On the Characterization of Canonical Number Systems. *Osaka J. Math.* **41**, (2004) 1–25.

[Scheicher 2007] Scheicher, K. Beta-expansions in algebraic function fields over finite fields. *Finite Fields Appl.* **13**, (2007) 394–410.

[Schmidt 1980] Schmidt, K. On periodic expansions of Pisot numbers and Salem numbers. *Bull. London Math. Soc.* **12**(4), (1980) 269–278.

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

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

[Takahashi 1980] Takahashi, Y. A Formula for Topological Entropy of One-dimensional Dynamics. *Sci. Papers College Gen. Ed. Univ. Tokyo* **30**, (1980) 11–22.

[Thuswaldner 1998] Thuswaldner, J. M. Elementary properties of canonical number systems in quadratic fields. In G. B. et al., ed., *Applications of Fibonacci Numbers*, vol. 7, pp. 405–414. Kluwer Academic Publisher, 1998.

Notation Index

General Index