CHAPTER 10

Words in Number Theory

10.0. Introduction

This chapter shows some examples of applications of combinatorics on words to number theory with a brief incursion into physics. These examples have a common feature: the notion of morphism of the free monoid. Such morphisms have been widely studied in combinatorics on words; they generate infinite words which can be considered as highly ordered, and which occur in an ubiquitous way in mathematics, theoretical computer science, and theoretical physics.

The first part of this chapter is devoted to the notion of automatic sequences and uniform morphisms, in connection with the transcendence of formal power series with coefficients in a finite field. Namely it is possible to characterize algebraicity of these series in a simple way: a formal power series is algebraic if and only if the sequence of its coefficients is automatic, that is, if it is the image by a letter-to-letter map of a fixed point of a uniform morphism. This criterion is known as Christol's theorem. A central tool in the study of automatic sequences is the notion of kernel of an infinite word (sequence) over a finite alphabet: this is the set of subsequences obtained by certain decimations. A rephrasing of Christol's theorem is that transcendence of a formal power series over a finite field is equivalent to infiniteness of the kernel of the sequence of its coefficients: this will be illustrated in this chapter.

Examples of applications of the properties of automatic sequences to transcendence results for power series over the rationals, and for real numbers whose base b-expansion is automatic are also given.

Then, in a second part, this chapter uses a famous infinite word, the Tribonacci word, as a guideline to introduce various applications in

Applied Combinatorics on Words, eds. Jean Berstel and Dominique Perrin.
Published by Cambridge University Press.

Diophantine approximation and in simultaneous approximation. The Tribonacci word was introduced as a generalization of the celebrated Fibonacci word. It is defined as the fixed point of a nonuniform primitive morphism, called the Tribonacci morphism. We first associate in a natural way a numeration system with this morphism, that leads us to the definition of a compact subset of the plane with fractal boundary, called the Rauzy fractal. By closely studying its topological properties, we show that this compact set can be considered as a fundamental domain for a lattice of the plane, and that a particular geometric transformation, namely an exchange of pieces, can be performed on it. This transformation can furthermore be factored as a translation on the two-dimensional torus. The goal of this chapter is then to show how to deduce arithmetic properties of this translation from combinatorial properties of the Tribonacci word. In particular, it is shown how to associate with some prefixes of this infinite word best approximations for a given norm of the corresponding vector of translation. Relations to tilings and quasicrystals via the cut and project method are also mentioned.

10.1. Morphic and automatic sequences: definitions and generalities

In this section we define morphisms, uniform morphisms, morphic sequences, and automatic sequences.

10.1.1. Topology and distance on the set of finite and infinite words

Let $\mathcal{A}$ be a finite alphabet. The set $\mathcal{A}$ is equipped with the discrete topology (that is, every subset is open), and the set $\mathcal{A}^\omega$ of infinite words (that we also call here *infinite sequences*) on $\mathcal{A}$ is equipped with the corresponding product topology. It is well known and not hard to prove that the product topology can also be defined by the following distance:

$$d((u_n)_{n\geq 0}, (v_n)_{n\geq 0}) := 2^{-\min\{j\in\mathbb{N},\ u_j\neq v_j\}}.$$

The topology on $\mathcal{A}^\omega$ can be extended to the set $\mathcal{A}^* \cup \mathcal{A}^\omega$ of all finite and infinite words on $\mathcal{A}$ as follows: let $\sharp$ be a symbol not in $\mathcal{A}$. The set $\mathcal{A} \cup \{\sharp\}$ is equipped with the discrete topology and the set $(\mathcal{A} \cup \{\sharp\})^\omega$ is equipped with the product topology. Finally the set $\mathcal{A}^*$ is naturally embedded in $(\mathcal{A} \cup \{\sharp\})^\omega$ by identifying the word $u_0u_1 \cdots u_d$ in $\mathcal{A}^*$ and the infinite word $u_0u_1 \cdots u_d(\sharp)^\omega$ in $(\mathcal{A} \cup \{\sharp\})^\omega$ (where $(\sharp)^\omega$ stands for the infinite word whose terms are all equal to $\sharp$).

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

Remark 10.1.1. Note that the distance just defined can be informally described by saying that two words are close to each other if they coincide on their first letters. Also note that the set $\mathcal{A}^\omega$ is a compact set.

10.1.2. Morphisms and uniform morphisms

Let $\mathcal{A}$ and $\mathcal{B}$ be two alphabets. Let us recall that a *morphism* $h : \mathcal{A}^* \to \mathcal{B}^*$ is a map from $\mathcal{A}^*$ to $\mathcal{B}^*$ such that for all $u, v \in \mathcal{A}^*$, the relation $h(uv) = h(u)h(v)$ holds. (In other words h is a homomorphism of monoids.)

Remark 10.1.2.

- A morphism $h : \mathcal{A}^* \to \mathcal{B}^*$ is defined by its values on the elements of $\mathcal{A}$.
- The iterates of a morphism $h : \mathcal{A}^* \to \mathcal{A}^*$ are denoted h^j, $j \geq 0$, and defined by $h^0(a) = a$ for all $a \in \mathcal{A}$ and $h^{j+1} := h \circ h^j$.

The morphism $h : \mathcal{A}^* \to \mathcal{B}^*$ is called *uniform* if all the words $h(a)$, $a \in \mathcal{A}$, have the same length. Let d be this common length, the morphism is called a *morphism of length d* or a *d-uniform morphism* or a *d-morphism*.

10.1.3. Fixed points of morphisms, morphic sequences, and automatic sequences

Proposition 10.1.3. *Let $\mathcal{A}$ be an alphabet. Let $h : \mathcal{A}^* \to \mathcal{A}^*$ be a morphism such that there exist $a \in \mathcal{A}$ and $x \in \mathcal{A}^*$ with the properties:*

(i) $h(a) = ax$,

(ii) $\forall j \geq 0$, $h^j(x) \neq \varepsilon$.

Then, the sequence of words $a, h(a), h^2(a), \ldots, h^n(a), \ldots$ converges to an infinite word denoted $h^\omega(a)$. This infinite word is a fixed point of the extension of h by continuity to infinite words.

Proof. The hypotheses easily imply that $h^{j+1}(a) = axh(x)h^2(x)\cdots h^j(x)$, for $j \geq 0$. Hence the word $h^j(a)$ is a nontrivial prefix of the word $h^{j+1}(a)$, which gives the convergence of the sequence of words $h^j(a)$ to an infinite word $h^\omega(a)$. Since $h^{j+1}(a) = h(h^j(a))$, letting j go to infinity establishes the claim. ∎

Remark 10.1.4. In the sequel we will say that an *infinite word u on the alphabet $\mathcal{A}$ is a fixed point of a morphism $h : \mathcal{A}^* \to \mathcal{A}^*$* if and only if it can be obtained as in Proposition 10.1.3 above. One thus has $h(u) = u$.

The fixed points (in the sense of Remark 10.1.4) of uniform morphisms have a simple property that we now give.

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

Proposition 10.1.5. *An infinite word $(u_n)_{n\geq 0}$ on the alphabet $\mathcal{A}$ is a fixed point of the d-morphism $h : \mathcal{A}^* \to \mathcal{A}^*$ (in the sense of Remark 10.1.4) if and only if there exist d maps $h_r : \mathcal{A} \to \mathcal{A}$, $r \in [0, d-1]$, such that*

$$\forall n \geq 0, \quad \forall r \in [0, d-1], \quad u_{dn+r} = h_r(u_n).$$

Proof. Suppose that the infinite word $(u_n)_{n\geq 0}$ is a fixed point of the d-morphism $h : \mathcal{A}^* \to \mathcal{A}^*$, that is the limit when j goes to infinity of the sequence of words $a, h(a), h^2(a), \ldots, h^k(a) \ldots$, with $a \in \mathcal{A}$ and $h(a) = ax$, with $x \in \mathcal{A}^*$ and $h^j(x) \neq \varepsilon$ for all $j \geq 0$. Since h is d-uniform, for each letter $e \in \mathcal{A}$, the word $h(e)$ can be written as $h(e) = \alpha_{e,0}\alpha_{e,1} \cdots \alpha_{e,d-1}$. We define the maps $h_r : \mathcal{A} \to \mathcal{A}$, $r \in [0, d-1]$, by: for each $e \in \mathcal{A}$, $h_r(e) := \alpha_{e,r}$. Now, for each $k \geq 0$, the length of the word $h^k(a)$ is equal to d^k hence

$$h^k(a) = u_0 u_1 \cdots u_{d^k-1}.$$

We thus have

$$\begin{aligned} u_0 u_1 \cdots u_{d^{k+1}-1} &= h^{k+1}(a) = h(h^k(a)) \\ &= h(u_0 u_1 \cdots u_{d^k-1}) \\ &= h(u_0)h(u_1) \cdots h(u_{d^k-1}). \end{aligned}$$

This thus gives:

$$\forall n \in [0, d^k - 1], \quad \forall r \in [0, d-1], \quad u_{dn+r} = h_r(u_n).$$

Since this holds for all $k \geq 0$, we thus have

$$\forall n \geq 0, \quad \forall r \in [0, d-1], \quad u_{dn+r} = h_r(u_n).$$

Conversely suppose that there exist d maps $h_r : \mathcal{A} \to \mathcal{A}, r \in [0, d-1]$, such that

$$\forall n \geq 0, \quad \forall r \in [0, d-1], \quad u_{dn+r} = h_r(u_n).$$

Taking $n = r = 0$, we get $u_0 = h_0(u_0)$. Define the morphism $h : \mathcal{A}^* \to \mathcal{A}^*$, by

$$\forall e \in \mathcal{A}, \quad h(e) := h_0(e)h_1(e) \cdots h_{d-1}(e).$$

Furthermore let $a := u_0$. The morphism h is clearly uniform. We have

$$h(a) = h(u_0) = h_0(u_0)h_1(u_0) \cdots h_{d-1}(u_0) = u_0 h_1(u_0) \cdots h_{d-1}(u_0) = ax,$$

where $x := h_1(u_0) \cdots h_{d-1}(u_0)$. For all $j \geq 0$ we clearly have $|h^j(x)| = d^j(d-1)$, hence $h^j(x) \neq \varepsilon$. Thus Conditions (i) and (ii) of Proposition 10.1.3 are satisfied. It is then easy to check that $h^\omega(a)$ is precisely the word $(u_n)_{n\geq 0}$. ∎

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

A word $(u_n)_{n\geq 0}$ on the alphabet $\mathcal{A}$ is called a *morphic sequence* (or *substitutive sequence*) if there exists an alphabet $\mathcal{C}$, a word $(v_n)_{n\geq 0}$ on $\mathcal{C}$, a morphism $h : \mathcal{C}^* \to \mathcal{C}^*$, and a map $\varphi : \mathcal{C} \to \mathcal{A}$ such that

(i) the word $(v_n)_{n\geq 0}$ is a fixed point of the morphism h (see Remark 10.1.4),

(ii) for all $n \geq 0$, one has $u_n = \varphi(v_n)$.

A word $(u_n)_{n\geq 0}$ on the alphabet $\mathcal{A}$ is called an *automatic sequence* if there exists an alphabet $\mathcal{C}$, a word $(v_n)_{n\geq 0}$ on $\mathcal{C}$, a *uniform* morphism $h : \mathcal{C}^* \to \mathcal{C}^*$, and a map $\varphi : \mathcal{C} \to \mathcal{A}$ such that

(i) the word $(v_n)_{n\geq 0}$ is a fixed point of the uniform morphism h (see Remark 10.1.4),

(ii) for all $n \geq 0$, one has $u_n = \varphi(v_n)$.

If the morphism h has length d, the word $(u_n)_{n\geq 0}$ is called *d-automatic*.

Remark 10.1.6. An automatic sequence is, in particular, morphic. The denomination "automatic" comes from the fact that such an infinite word can be generated by a finite automaton.

10.1.4. Examples of morphic and automatic sequences

The Fibonacci word

The (binary) Fibonacci word is defined as the fixed point (in the sense of Remark 10.1.4) of the morphism $0 \to 01$, $1 \to 0$, on the alphabet $\{0, 1\}$. The first few terms of this word are

$$0\,1\,0\,0\,1\,0\,1\,0\,0\,1\,0\,0\,1\,0\,1\,0\cdots$$

The name of this word comes from the fact that iterating the morphism starting from 0 gives words whose lengths are equal to the Fibonacci numbers $1, 2, 3, 5, 8, \cdots$

$$\begin{array}{l} 0 \\ 0\ 1 \\ 0\ 1\,0 \\ 0\ 1\,0\,0\,1 \\ 0\ 1\,0\,0\,1\,0\,1\,0 \\ \cdots \end{array}$$

It can be shown that this word is a Sturmian word, that is that the number of blocks of consecutive letters of length n occurring in the word is equal to $n + 1$ for each $n \geq 1$ (see Problem 10.7.1).

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

The Tribonacci word

The Tribonacci word is defined as the fixed point (in the sense of Remark 10.1.4) of the morphism $1 \to 12$, $2 \to 13$, $3 \to 1$ on the alphabet $\{1, 2, 3\}$. The first few terms of this word are

$$1\,2\,1\,3\,1\,2\,1\,1\,2\,1\,3\,1\,2\,1\,2\,1\cdots$$

The Fibonacci and the Tribonacci words share many properties, and the Tribonacci word can be considered as a generalization of the Fibonacci word, hence the terminology. We study the Tribonacci word in more detail in Sections 10.7–10.9.

The Thue–Morse word

Let us recall (see Example 1.8.4) that the (Prouhet)–Thue–Morse word is defined as the fixed point (in the sense of Remark 10.1.4) beginning with 0 of the morphism $0 \to 01$, $1 \to 10$. The first few terms of this word are

$$0\,1\,1\,0\,1\,0\,0\,1\,1\,0\,0\,1\,0\,1\,1\,0\,1\cdots$$

The nth term (starting from index 0) of this word is 0 if the sum of the binary digits of n is even, and 1 if this sum is odd. This property can easily been deduced from the results of Section 10.2.3.

The Rudin–Shapiro word

We consider on the alphabet $\{a, b, c, d\}$ the morphism

$$\begin{aligned} a &\to ab \\ b &\to ac \\ c &\to db \\ d &\to dc \end{aligned}$$

Iterating this morphism starting from a gives the following fixed point

$$a\,b\,a\,c\,a\,b\,d\,b\,a\,b\,a\,c\,d\,c\cdots$$

The image of this infinite word by the map $a \to 1$, $b \to 1$, $c \to -1$, $d \to -1$, is called the Rudin–Shapiro word. This word begins as follows

$$+1\ +1\ +1\ -1\ +1\ +1\ -1\ +1\ +1\ +1\ +1\ -1\ -1\ -1\ \ldots$$

Denoting by $a(n)$ the number of (possibly overlapping) blocks 11 in the binary expansion of n, it can be shown that the nth term of the Rudin–Shapiro word is equal to $(-1)^{a(n)}$. Here again, this property can easily been deduced from the results of Section 10.2.3.

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

The regular paperfolding word

We consider on the alphabet $\{a, b, c, d\}$ the morphism

$$\begin{aligned} a &\to ab \\ b &\to cb \\ c &\to ad \\ d &\to cd \end{aligned}$$

Iterating this morphism starting from a gives the following fixed point

$$a\ b\ c\ b\ a\ d\ c\ b\ a\ b\ c\ d\ a\ d\ c\ b \ldots$$

The image of this infinite word by the map $a \to 0, b \to 0, c \to 1, d \to 1$, is called the (regular) paperfolding word. This word begins as follows

$$0\,0\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,0\,1\,1\,0\cdots$$

Denoting this word by $(z_n)_{n\geq 0}$, it is easy to show that

$$z_{4n} = 0, \quad z_{4n+2} = 1, \quad z_{2n+1} = z_n$$

(which gives an alternative definition of the paperfolding word).

The proof of the following property of the paperfolding word is left to the reader. For any word w on the alphabet $\{0, 1\}$, define the word w^R as the word obtained by reading w backwards (in other words $(w_0 w_1 \cdots w_\ell)^R := w_\ell w_{\ell-1} \cdots w_0$). Also define the word $\overline{w}$ as the word obtaining from w by replacing 0s by 1s and 1s by 0s (in other words $\overline{w} := (1 - w_0)(1 - w_1) \cdots (1 - w_\ell)$). Define the map P on $\{0, 1\}^*$ by $P(w) := w0\overline{w^R}$. (The map P is called *perturbed symmetry*.) Then the paperfolding word is equal to $\lim_{j\to\infty} P^j(0)$.

10.2. d-Kernels and properties of automatic sequences

10.2.1. d-Kernels

Let $(u_n)_{n\geq 0}$ be an infinite word defined on the alphabet $\mathcal{A}$. Let $d \geq 2$ be an integer. The d-kernel of the word $(u_n)_{n\geq 0}$, denoted $\mathcal{K}(d, (u_n)_n)$, is the set of subsequences of the word $(u_n)_{n\geq 0}$ defined by

$$\mathcal{K}(d, (u_n)_n) := \{(u_{d^k n+r})_{n\geq 0}, \quad k \geq 0, \quad r \in [0, d^k - 1]\}.$$

Remark 10.2.1. It is easy to prove that the d-kernel of an infinite sequence $(u_n)_{n\geq 0}$ is stable under the maps D_j, $j \in [0, d - 1]$, defined on the set of sequences on $\mathcal{A}$ by

$$\forall (z_n)_{n\geq 0} \in \mathcal{A}^\omega, \quad D_j((z_n)_{n\geq 0}) := (z_{dn+j})_{n\geq 0}.$$

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

Furthermore $\mathcal{K}(d, (u_n)_n)$ is the smallest set that contains the sequence $(u_n)_{n\geq 0}$ and is stable by the maps D_j, $j \in [0, d-1]$.

10.2.2. Combinatorial characterization of automatic sequences

The notion of d-kernel permits us to give a simple combinatorial characterization of automatic sequences.

Proposition 10.2.2. *Let $(u_n)_{n\geq 0}$ be an infinite sequence defined on the alphabet $\mathcal{A}$. Let $d \geq 2$ be an integer. Then, the following properties are equivalent:*

(i) *the sequence $(u_n)_{n\geq 0}$ is d-automatic,*
(ii) *the d-kernel $\mathcal{K}(d, (u_n)_n)$ is a finite set,*
(iii) *there exists a finite set of sequences $\mathcal{F}$ that contains the sequence $(u_n)_{n\geq 0}$ and such that, if the sequence $(v_n)_{n\geq 0}$ belongs to $\mathcal{F}$, then, for every $j \in [0, d-1]$, the sequence $D_j((v_n)_{n\geq 0}) := (v_{dn+j})_{n\geq 0}$ belongs to $\mathcal{F}$.*

Proof. (i) $\Rightarrow$ (ii). We suppose that the sequence $(u_n)_{n\geq 0}$ is d-automatic. Then there exist an alphabet $\mathcal{C}$, a sequence $(v_n)_{n\geq 0}$ on $\mathcal{C}$, a *uniform* morphism $h : \mathcal{C}^* \to \mathcal{C}^*$, and a map $\varphi : \mathcal{C} \to \mathcal{A}$ such that the sequence $(v_n)_{n\geq 0}$ is a fixed point of the uniform morphism h and for all $n \geq 0$, one has $u_n = \varphi(v_n)$.

In order to prove that the set $\mathcal{K}(d, (u_n)_n)$ is finite, it thus suffices to prove that $\mathcal{K}(d, (v_n)_n)$ is finite. We know from Proposition 10.1.5 that there exist d maps $h_r : \mathcal{A} \to \mathcal{A}$, $r \in [0, d-1]$, such that

$$\forall n \geq 0, \quad \forall r \in [0, d-1], \quad v_{dn+r} = h_r(v_n).$$

An easy induction on k shows the following: let $t \in [0, d^k - 1]$; write its base d expansion (possibly with leading zeroes) as $t_{k-1} \dots t_0$; then

$$\forall n \geq 0, \quad v_{d^k n+t} = h_{t_0}((h_{t_1} \dots (h_{t_{k-1}}(v_n))) \dots).$$

In other words there exists a map f_t from $\mathcal{A}$ into itself such that $\forall n \geq 0$, we have $v_{d^k n+t} = f_t(v_n)$. The set $\mathcal{A}$ is finite, hence the set of maps from $\mathcal{A}$ to itself is also finite. This implies that there are only finitely many sequences $(v_{d^k n+t})_{n\geq 0}$, with $k \geq 0$, $t \in [0, d^k - 1]$.

(ii) $\Rightarrow$ (iii). This is an easy consequence of Remark 10.2.1.

(iii) $\Rightarrow$ (i). Let $\mathcal{F} = \{(u_n^{(1)})_{n\geq 0}, (u_n^{(2)})_{n\geq 0}, \dots, (u_n^{(t)})_{n\geq 0}\}$ be a finite set of sequences, with $(u_n^{(1)})_{n\geq 0} = (u_n)_{n\geq 0}$ such that $\mathcal{F}$ is stable by the maps D_j,

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

for $j \in [0, d-1]$. Define the vector $V(n)$ by

$$V(n) := \begin{pmatrix} u_n^{(1)} \\ u_n^{(2)} \\ \vdots \\ u_n^{(t)} \end{pmatrix}.$$

Let $\mathcal{C} \subset \mathcal{A}^t$ be the (finite) set of values of $V(n)$. The fact that the set $\mathcal{F}$ is stable under the maps D_j for $j \in [0, d-1]$ implies that for each $j \in [0, d-1]$ there exists a matrix Θ_j of 0s and 1s, having exactly one 1 on each row, such that

$$\forall n \geq 0, \quad V(dn + j) = \Theta_j V(n).$$

Using Proposition 10.1.5 we see that the sequence $(V(n))_{n\geq 0}$ is a fixed point of the d-morphism h of $\mathcal{A}^*$ defined by

$$\forall \alpha \in \mathcal{C}^*, \quad h(\alpha) := (\Theta_1 \alpha)\,(\Theta_2 \alpha) \cdots (\Theta_t \alpha).$$

Now the sequence $(u_n)_{n\geq 0} = (u_n^{(1)})_{n\geq 0}$ is the (pointwise) image of the sequence $(V(n))_{n\geq 0}$ by the restriction to $\mathcal{C}$ of the first projection $\mathcal{A}^t \to \mathcal{A}$.

■

Remark 10.2.3. We have spoken in the proof of Proposition 10.2.2 (iii) of vectors and matrices, although there is no vector space (nor module): the reader will be easily convinced that this is only a practical terminology (recall the special form of the matrices Θ_j).

10.2.3. Examples of kernels of automatic sequences

The Thue–Morse word, the Rudin–Shapiro word, and the paperfolding word are 2-automatic (see their definitions in Section 10.1.4). Namely their 2-kernels are finite:

(i) the definition of the Thue–Morse word $(u_n)_{n\geq 0}$ shows that $u_{2n} = u_n$ and $u_{2n+1} = 1 - u_n$ for every $n \geq 0$; hence the 2-kernel of the Thue–Morse word is

$$\mathcal{K}(2, (u_n)_n) = \{(u_n)_{n\geq 0}, (1 - u_n)_{n\geq 0}\};$$

(ii) the property of the Rudin–Shapiro word $(v_n)_{n\geq 0}$ that $v_n = (-1)^{a(n)}$, where $a(n)$ counts the number of possibly overlapping blocks 11 in the binary expansion of the integer n, comes from $v_{2n} = v_n$, $v_{4n+1} = v_n$,

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

$v_{4n+3} = -v_{2n+1}$, for every $n \geq 0$; hence the 2-kernel of the Rudin–Shapiro word is

$$\mathcal{K}(2, (v_n)_n) = \{(v_n)_{n\geq 0}, (v_{2n+1})_{n\geq 0}, (-v_n)_{n\geq 0}, (-v_{2n+1})_{n\geq 0}\};$$

(iii) since the regular paperfolding word $(z_n)_{n\geq 0}$ satisfies $z_{4n} = 0$, $z_{4n+2} = 1$, $z_{2n+1} = z_n$ for every $n \geq 0$, its 2-kernel is

$$\mathcal{K}(2, (z_n)_n) = \{0, 1, (z_n)_{n\geq 0}, (z_{2n})_{n\geq 0}\}.$$

10.2.4. Properties of automatic sequences

We give below some properties, in particular closure properties, of automatic sequences.

Proposition 10.2.4. *Let $q \geq 2$ be an integer. Let $(u_n)_{n\geq 0}$ be a q-automatic sequence on the alphabet $\mathcal{A}$. Then the sequences $(u_{q^n})_{n\geq 0}$ and $(u_{q^n-1})_{n\geq 0}$ are periodic from some point on.*

Proof. We prove only the second assertion, the first one is proved analogously. Since the q-kernel of the sequence $(u_n)_{n\geq 0}$ is finite (Proposition 10.2.2), the set of subsequences $\{(u_{q^k n+q^k-1})_{n\geq 0}, k \geq 0\}$ is finite. In particular there exist $k \geq 0$ and $j \geq 1$ such that the sequences $(u_{q^k n+q^k-1})_{n\geq 0}$ and $(u_{q^{k+j} n+q^{k+j}-1})_{n\geq 0}$ are equal. In other words, the sequences $(u_{q^k n-1})_{n\geq 1}$ and $(u_{q^{k+j} n-1})_{n\geq 1}$ are equal. Replacing n by $q^j n$, $q^{2j} n$, ... shows that the sequences $(u_{q^k n-1})_{n\geq 1}$ and $(u_{q^{k+\alpha j} n-1})_{n\geq 1}$ are equal for all $\alpha \geq 0$. Taking $n = 1$ concludes the proof. ∎

Proposition 10.2.5. *Let $d \geq 2$ be an integer. Let $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$ be two d-automatic sequences defined respectively on the alphabets $\mathcal{A}$ and $\mathcal{B}$. Then the sequence $(u_n, v_n)_{n\geq 0}$ defined on the alphabet $\mathcal{A} \times \mathcal{B}$ is d-automatic.*

Let $d \geq 2$ be an integer. Let $(u_n)_{n\geq 0}$ be a d-automatic sequence defined on the alphabet $\mathcal{A}$. Let $\mathcal{B}$ be an alphabet and f be a map $f : \mathcal{A} \to \mathcal{B}$. Then the sequence $(f(u_n))_{n\geq 0}$ is d-automatic.

Proof. The proofs of both assertions are straightforward using the characterization of automatic sequences given in Proposition 10.2.2. ∎

Proposition 10.2.6. *Let $(u_n)_{n\geq 0}$ be a sequence on the alphabet $\mathcal{A}$ that is ultimately periodic (that is periodic from some point on). Then, the sequence $(u_n)_{n\geq 0}$ is d-automatic for every $d \geq 1$.*

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

Proof. Since the sequence $(u_n)_{n\geq 0}$ is ultimately periodic, there exist two integers $n_0 \geq 0$ and $T > 1$, such that $\forall n \geq n_0$, $u_{n+T} = u_n$. Now, for $d \geq 2$, take a sequence in the d-kernel of $(u_n)_{n\geq 0}$, say $(u_{d^k n+\ell})_{n\geq 0}$, with $k \geq 0$ and $\ell \in [0, d^k - 1]$. We have for all $n \geq n_0$

$$u_{d^k(n+T)+\ell} = u_{d^k n+\ell+d^k T} = u_{d^k n+\ell}.$$

In other words all sequences $(v_n)_{n\geq 0}$ in $\mathcal{K}(d, (u_n)_n)$ satisfy $\forall n \geq n_0$, $v_{n+T} = v_n$. Hence the d-kernel of $(u_n)_{n\geq 0}$ is finite with at most $(\mathrm{Card}\,\mathcal{A})^{n_0+T}$ elements. ∎

Proposition 10.2.7. *Let $(u_n)_{n\geq 0}$ be a d-automatic sequence defined on the alphabet $\mathcal{A}$. Then*

(i) *for all $a, b \in \mathbb{N}$, the sequence $(u_{an+b})_{n\geq 0}$ is d-automatic;*

(ii) *the sequence $(v_n)_{n\geq 0}$ defined by $v_0 = a \in \mathcal{A}$ and $v_n = u_{n-1}$ for all $n \geq 1$, is d-automatic.*

Proof.

(i) We may assume, from Proposition 10.2.6, that $a \geq 1$. The d-kernel $\mathcal{K}(d, (u_n)_n)$ of the sequence $(u_n)_{n\geq 0}$ is finite. Let

$$\mathcal{K}(d, (u_n)_n) := \{(u_n^{(1)})_{n\geq 0}, (u_n^{(2)})_{n\geq 0}, \ldots, (u_n^{(t)})_{n\geq 0}\},$$

with $(u_n^{(1)})_{n\geq 0} = (u_n)_{n\geq 0}$. Let us then define the set $\mathcal{L}$ of sequences by

$$\mathcal{L} := \{(u_{an+b'}^{(i)})_{n\geq 0}, \quad i \in [1, t], \quad b' \in [0, a + b - 1]\}.$$

The set $\mathcal{L}$ is clearly finite with at most $t(a + b)$ elements. It thus suffices to prove that the d-kernel of the sequence $(u_{an+b})_{n\geq 0}$ is a subset of $\mathcal{L}$. Let $(u_{a(d^k n+\ell)+b})_{n\geq 0}$ be a sequence in the d-kernel of $(u_{an+b})_{n\geq 0}$, where $k \geq 0$ and $\ell \in [0, d^k - 1]$. We write $a\ell + b = xd^k + y$, with $y \in [0, d^k - 1]$. Thus,

$$u_{a(d^k n+\ell)+b} = u_{d^k(an+x)+y} = u_{an+x}^{(i)}$$

for some i that does not depend on n. Furthermore we have

$$xd^k \leq xd^k + y = a\ell + b \leq a(d^k - 1) + b < ad^k + b \leq (a + b)d^k.$$

Hence $x < a + b$, and the sequence $(u_{a(d^k n+\ell)+b})_{n\geq 0}$ belongs to $\mathcal{L}$.

(ii) Let us write, as above, the (finite) d-kernel of the sequence $(u_n)_{n\geq 0}$ as

$$\mathcal{K}(d, (u_n)_n) := \{(u_n^{(1)})_{n\geq 0}, (u_n^{(2)})_{n\geq 0}, \ldots, (u_n^{(t)})_{n\geq 0}\},$$

with $(u_n^{(1)})_{n\geq 0} = (u_n)_{n\geq 0}$. Let us then define t sequences $(v_n^{(i)})_{n\geq 0}$, $i \in [1, t]$, by: $v_0^{(i)} := a$ and $v_n^{(i)} := u_{n-1}^{(i)}$ for $n \geq 1$. Note that $(v_n^{(1)})_{n\geq 0} = (v_n)_{n\geq 0}$.

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

Consider the (finite) set $\mathcal{M}$ defined by

$$\mathcal{M} := \{(u_n^{(1)})_{n\geq 0}, (u_n^{(2)})_{n\geq 0}, \ldots, (u_n^{(t)})_{n\geq 0}, (v_n^{(1)})_{n\geq 0}, (v_n^{(2)})_{n\geq 0}, \ldots, (v_n^{(t)})_{n\geq 0}\}.$$

It suffices to prove that $\mathcal{K}(d, (v_n)_n) \subset \mathcal{M}$. Let $(v_{d^k n+\ell})_{n\geq 0}$ with $k \geq 0$ and $\ell \in [0, d^k - 1]$ be an element of $\mathcal{K}(d, (v_n)_n)$.

- If $\ell \geq 1$, then, $v_{d^k n+\ell} = u_{d^k n+(\ell-1)}$. Since $(\ell - 1) \in [0, d^k - 1]$, the sequence $(u_{d^k n+(\ell-1)})_{n\geq 0}$ is equal to $(u_n^{(i)})_{n\geq 0}$ for some $i \in [1, t]$ hence it belongs to $\mathcal{M}$.
- If $\ell = 0$, then $(v_{d^k n+\ell})_{n\geq 0} = (v_{d^k n})_{n\geq 0}$. If $n \geq 1$, let $m = n - 1 \geq 0$. We have:

$$v_{d^k n} = u_{d^k n-1} = u_{d^k m+d^k-1} = u_m^{(i)} = u_{n-1}^{(i)}$$

for some i that does not depend on n. Hence

$$v_{d^k n} = \left\{ \begin{array}{ll} a & \text{if } n = 0 \\ u_{n-1}^{(i)} & \text{if } n \geq 1 \end{array} \right\} = v_n^{(i)}.$$ ∎

Remark 10.2.8. This proposition implies in particular, using (i), that shifting a d-automatic sequence gives a d-automatic sequence. Using this remark and (ii) shows that finite modifications of a d-automatic sequence give a d-automatic sequence.

Proposition 10.2.9. *Let $d \geq 2$ be an integer. Let $(u_n)_{n\geq 0}$ be a sequence on an alphabet $\mathcal{A}$, such that there exists $a \in \mathbb{N} \setminus \{0\}$ for which all subsequences $(u_{an+b})_{n\geq 0}$ are d-automatic, for $b \in [0, a - 1]$. Then the sequence $(u_n)_{n\geq 0}$ is d-automatic.*

Proof. In order to prove that the d-kernel of the sequence $(u_n)_{n\geq 0}$ is finite, it suffices to prove that the set of sequences of the form $(u_{d^k(an+b)+\ell})_{n\geq 0}$ for $k \geq 0$, $\ell \in [0, d^k - 1]$ and $b \in [0, a - 1]$ is finite: namely interspersing these sequences produces the sequences $(u_{d^k n+\ell})_{n\geq 0}$ for $k \geq 0$, $\ell \in [0, d^k - 1]$.

Now, for $k \geq 0$, $\ell \in [0, d^k - 1]$, and $b \in [0, a - 1]$, let $d^k b + \ell = ar + s$ with $s \in [0, a - 1]$. This implies

$$ar \leq ar + s = d^k b + \ell \leq d^k b + d^k - 1 < d^k(b + 1) \leq d^k a$$

hence $r \in [0, d^k - 1]$. Then, for $n \geq 0$,

$$u_{d^k(an+b)+\ell} = u_{a(d^k n+r)+s}.$$

This shows that the sequence $(u_{d^k(an+b)+\ell})_{n\geq 0}$ belongs to the d-kernel of the sequence $(u_{an+s})_{n\geq 0}$, hence to the (finite) set

$$\bigcup_{s\in[0,a-1]} \mathcal{K}(d, (u_{an+s})_n).$$ ∎

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

Corollary 10.2.10. *Let $(u_n)_{n\geq 0}$ be a sequence defined on an alphabet $\mathcal{A}$. Let $d \geq 2$ be an integer. Then the following properties are equivalent:*

(i) *the sequence $(u_n)_{n\geq 0}$ is d-automatic;*

(ii) *there exists an integer $\alpha \geq 1$ such that the sequence $(u_n)_{n\geq 0}$ is d^α-automatic;*

(iii) *for every integer $\alpha \geq 1$ the sequence $(u_n)_{n\geq 0}$ is d^α-automatic.*

Proof. The implication (iii) $\Rightarrow$ (ii) is trivial. Furthermore, we clearly have, for any integer $\alpha \geq 1$, the inclusion $\mathcal{K}(d^\alpha, (u_n)_n) \subset \mathcal{K}(d, (u_n)_n)$, which shows that (i) $\Rightarrow$ (iii).

It remains to prove that (ii) $\Rightarrow$ (i). Suppose that the sequence $(u_n)_{n\geq 0}$ is d^α-automatic, for some $\alpha \geq 1$. If $\alpha = 1$ we are done. Hence we can suppose that $\alpha \geq 2$. Define $d' := d^{\alpha-1}$. Fix $j \in [0, d'-1]$, and define the sequence $(v_n)_{n\geq 0}$ by $v_n := u_{d'n+j}$. This sequence $(v_n)_{n\geq 0}$ is d-automatic: namely for each $i \in [0, d-1]$ we have $v_{dn+i} = u_{d'dn+d'i+j} = u_{d^\alpha n+d'i+j}$, hence the sequence $(v_{dn+i})_{n\geq 0}$ belongs to the finite set $\mathcal{K}(d^\alpha, (u_n)_n)$ (note that $d'i + j \leq d^\alpha - 1$). Applying now Proposition 10.2.9 with $a = d' - 1$ ends the proof. ∎

Corollary 10.2.11. *Let $d \geq 2$ be an integer. Let $(u_n)_{n\geq 0}$ be a d-automatic sequence defined on the alphabet $\mathcal{A}$. Let $\mathcal{B}$ be an alphabet and let h be a uniform morphism $h : \mathcal{A}^* \to \mathcal{B}^*$. Then the sequence $(h(u_n))_{n\geq 0}$ is d-automatic.*

Proof. We recall that the morphism h is extended by continuity to infinite sequences. Let us suppose that the length of the morphism h is d'. Hence, for each letter $e \in \mathcal{A}$, the word $h(e)$ can be written as $h(e) = \alpha_{e,0}\alpha_{e,1}\cdots\alpha_{e,d'-1}$. We define the maps $h_i : \mathcal{A} \to \mathcal{A}$, $i \in [0, d'-1]$, by: for each $e \in \mathcal{A}$, $h_i(e) := \alpha_{e,i}$.

We thus can write the sequence $(h(u_n))_{n\geq 0}$ as

$$h_0(u_0)h_1(u_0)\ldots h_{d'}(u_0)h_0(u_1)h_1(u_1)\ldots h_{d'}(u_1)\ldots$$

In other words we have, for all $n \geq 0$ and for all $i \in [0, d'-1]$,

$$u_{d'n+i} = h_i(u_n).$$

But the sequences $(h_i(u_n))_{n\geq 0}$, for $i \in [0, d'-1]$ are d-automatic, from Proposition 10.2.5, hence the sequence $(u_n)_{n\geq 0}$ is d-automatic from Proposition 10.2.9. ∎

Proposition 10.2.12. *Let $d \geq 2$ be an integer. Let $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$ be two d-automatic sequences defined on the alphabet $\mathcal{A}$.*

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

(i) *If $\mathcal{A}$ is a module over a commutative ring $\mathcal{R}$, then the sequences $((u+v)_n)_{n\geq 0} := (u_n + v_n)_{n\geq 0}$ and $((xu)_n)_{n\geq 0} := (xu_n)_{n\geq 0}$, where $x \in \mathcal{R}$, are d-automatic.*

(ii) *If $\mathcal{A}$ is a finite commutative ring, then the (ordinary) product of the sequences $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$, that is the sequence $((uv)_n)_{n\geq 0} := (u_n v_n)_{n\geq 0}$, is d-automatic.*

(iii) *If $\mathcal{A}$ is a finite commutative ring, then the Cauchy product of the sequences $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$, that is the sequence $(\sum_{0\leq j\leq n} u_j v_{n-j})_{n\geq 0}$, is d-automatic.*

Proof. Assertions in (i) and (ii) are easy consequences of Propositions 10.2.5 and 10.2.6. Let us prove assertion (iii). Let $k \geq 0$ and $\ell \in [0, d^k - 1]$. We first note that, for $n \geq 1$, writing any $i \in [0, d^k n + \ell]$ as $i = d^k m + j$, with $j \in [0, d^k - 1]$, we have

$$d^k m \leq d^k m + j = i \leq d^k n + \ell \leq d^k n + d^k - 1 < d^k(n+1).$$

This implies $m < n + 1$, hence $m \leq n$. Hence the inclusion

$$[0, d^k n + \ell] \subset \{d^k m + j, \quad m \leq n-1, \quad 0 \leq j \leq d^k - 1\} \cup \{d^k n + j, \quad j \in [0, \ell]\}.$$

The reverse inclusion is clear, hence

$$[0, d^k n + \ell] = \{d^k m + j, \quad m \leq n-1, \quad 0 \leq j \leq d^k - 1\} \cup \{d^k n + j, \quad j \in [0, \ell]\}.$$

This equality clearly implies

$$[0, d^k n + \ell] = \{d^k m + j, \quad m \leq n-1, \quad \ell \leq j \leq d^k - 1\} \cup \{d^k m + j, \quad m \leq n, \quad j \in [0, \ell]\}.$$

Now let us consider our two d-automatic sequences and let us take an element in the d-kernel of the sequence $(\sum_{0\leq i\leq n} u_i v_{n-j})_{n\geq 0}$, that is let $k \geq 0$ and $\ell \in [0, d^k - 1]$, then

$$\sum_{0\leq i\leq d^k n+\ell} u_i v_{d^k n+\ell-i} = S_1(n) + S_2(n)$$

where

$$S_1(n) := \sum_{\ell < j \leq d^k - 1} \left(\sum_{0\leq m\leq n-1} u_{d^k m + j} v_{d^k n + \ell - d^k m - j} \right)$$

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

and

$$S_2(n) := \sum_{0\le j\le \ell} \left(\sum_{0\le m\le n} u_{d^k m+j} v_{d^k n+\ell-d^k m-j} \right).$$

Writing $S_1(n)$, for $n \ge 1$, as

$$S_1(n) := \sum_{\ell< j\le d^k-1} \left(\sum_{0\le m\le n-1} u_{d^k m+j} v_{d^k(n-1-m)+d^k+\ell-j} \right)$$

we see that, for $n \ge 1$, $S_1(n)$ is a finite sum of sequences of the type

$$\sum_{0\le m\le n-1} u_m^{(r)} v_{n-1-m}^{(s)}$$

where the sequence $(u_n^{(r)})_{n\ge 0}$ (resp. $(v_n^{(s)})_{n\ge 0}$) belongs to the d-kernel of the sequence $(u_n)_{n\ge 0}$ (resp. to the d-kernel of the sequence $(v_n)_{n\ge 0}$).

We also see that $S_2(n)$ is a finite sum of sequences of the type

$$\sum_{0\le m\le n} u_m^{(r)} v_{n-m}^{(s)}$$

where the sequence $(u_n^{(r)})_{n\ge 0}$ (resp. $(v_n^{(s)})_{n\ge 0}$) belongs to the d-kernel of the sequence $(u_n)_{n\ge 0}$ (resp. to the d-kernel of the sequence $(v_n)_{n\ge 0}$).

Hence the sequence $(S_1(n) + S_2(n))_{n\ge 1}$ belongs to a finite set of sequences. Since $S_1(0) + S_2(0)$ can take only finitely many values, we are done. ∎

10.2.5. A density property for "automatic" sets of integers

This section is devoted to proving a density property of sets of integers defined by automatic sequences. Before stating it we need two definitions and a lemma.

A subset $\mathbb{M}$ of the integers is said to have a *density* if the limit

$$\lim_{x\to\infty} \frac{1}{x} \mathrm{Card}\{n \le x, n \in \mathbb{M}\}$$

exists. The value of this limit is called the density of the set $\mathbb{M}$.

A factor w of an infinite word x is said to have a *density* if the set of indices of occurrence of this factor in x admits a density, that is if the limit of the number of occurrences of this factor in the first k terms of the word divided by k exists. The value of this limit, that we denote by $\pi(w)$, is called the *probability* (or the *frequency*) of occurrence of the factor w in x.

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

The following lemma is a direct consequence of the Perron–Frobenius theorem (for more details, see Section 1.7.2).

Lemma 10.2.13. *Let M be a positive stochastic matrix, that is such that all its entries are nonnegative and all the entries in any column sum up to 1. Then the sequence of matrices M^n converges and all the entries in the limit are rational numbers.*

Let h be a morphism on the alphabet $\mathcal{C} := \{c_1, c_2, \cdots c_t\}$. The *incidence matrix* (also called the *transition matrix* or *substitution matrix*) of h is the $t \times t$-matrix $M = (M_{ij})_{i,j}$ defined by

$$M_{ij} = |h(c_j)|_{c_i} := \text{number of occurrences of } c_i \text{ in } h(c_j).$$

Remark 10.2.14. The incidence matrix is the transpose of the matrix introduced in Section 1.8.6. If the incidence matrix of h is M, it is easy to see that the incidence matrix for h^n is M^n. If h is a d-morphism, it is clear that the entries in any column of its incidence matrix M sum up to d. We also introduce this matrix in this chapter in order to deduce probabilities of occurrence of letters.

Proposition 10.2.15. *Let $d \geq 2$ be an integer. Let $(u_n)_{n\geq 0}$ be a d-automatic sequence on the alphabet $\mathcal{A}$. Let a belong to $\mathcal{A}$. If the set $\{n \geq 0,\ u_n = a\}$ has a density, this density (which is the probability $\pi(a)$ of occurrence of the letter a) must be a rational number.*

Proof. Since the sequence $(u_n)_{n\geq 0}$ is d-automatic, there exist an alphabet $\mathcal{C}$, a sequence $(v_n)_{n\geq 0}$ on $\mathcal{C}$, a d-morphism $h : \mathcal{C}^* \to \mathcal{C}^*$, and a map $\varphi : \mathcal{C} \to \mathcal{A}$ such that: the sequence $(v_n)_{n\geq 0}$ is a fixed point of the d-morphism h, and for all $n \geq 0$, one has $u_n = \varphi(v_n)$.

We first note that, for each letter $c \in \mathcal{C}$ the limit

$$\lim_{n\to\infty} \frac{1}{d^n} \operatorname{Card}\{m \leq d^n - 1,\ v_m = c\}$$

exists. Namely, let $M = (M_{ij})_{i,j}$ be the incidence matrix of the d-morphism h, and let $M^n = (M_{ij}^{(n)})_{i,j}$. Then

$$\frac{1}{d^n} \operatorname{Card}\{m \leq d^n - 1, \quad v_n = c\} = \frac{1}{d^n} |h^n(v_0)|_c = \frac{M_{ij}^{(n)}}{d^n} \quad \text{for some } i, j.$$

Since the matrix M/d is clearly positive and stochastic, Proposition 10.2.15 shows that $\lim_{n\to\infty}(M_{ij}^{(n)}/d^n)$ exists and is rational. Hence, if $\mathcal{C}' = \varphi^{-1}(a)$ is the subset of $\mathcal{C}$ consisting of the elements of $\mathcal{C}$ whose image by φ is equal

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

to a, the limit

$$\lim_{n\to\infty} \frac{1}{d^n} \operatorname{Card}\{m \le d^n - 1, u_m = a\}$$

is the sum over $\mathcal{C}'$ of rational numbers, hence a rational number itself. Since the density of the set $\{m, u_m = a\}$ exists, it must be equal to the previous quantity, hence rational. ∎

10.3. Christol's algebraic characterization of automatic sequences

10.3.1. Formal power series

We recall that the ring $K[[X]]$ of formal power series with coefficients in a field K is defined by

$$K[[X]] := \left\{ \sum_{n\ge 0} u_n X^n, u_n \in K \right\},$$

where addition and multiplication of the series $F := \sum_{n\ge 0} u_n X^n$ and $G := \sum_{n\ge 0} b_n X^n$ are defined by

$$F + G := \sum_{n\ge 0} (u_n + b_n) X^n, \quad FG := \sum_{n\ge 0} \left(\sum_{i+j=n} u_i b_j \right) X^n.$$

The ring $K[[X]]$ is a subring of the field $K((X))$ of formal Laurent series

$$K((X)) := \left\{ \sum_{n\ge -n_0} u_n X^n, n_0 \in \mathbb{Z}, u_n \in K \right\},$$

where addition and multiplication are defined analogously.

Note that the field of rational functions $K(X)$ is a subfield of $K((X))$. Hence we can define algebraicity over $K(X)$ for an element belonging to $K((X))$.

The formal power series $F = F(X) = \sum_{n\ge -n_0} u_n X^n$ is said to be *algebraic (over the field $K(X)$)*, if there exist an integer $d \ge 1$ and polynomials $A_0(X)$, $A_1(X)$, …, $A_d(X)$, with coefficients in K and not all zero, such that

$$A_0 + A_1 F + A_2 F^2 + \cdots + A_d F^d = 0.$$

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

Remark 10.3.1.

- Any element of $K(X)$ is algebraic over $K(X)$.
- The sum and product of algebraic elements are algebraic.
- Let $F = \sum_{n \geq -n_0} u_n X^n$ be an algebraic power series. Its derivative $F' := \sum_{n \geq -n_0} n u_n X^{n-1}$ is also algebraic. Namely take an equation as that above with minimal degree d.

$$A_0 + A_1 F + A_2 F^2 + \cdots + A_d F^d = 0.$$

Taking the derivative gives

$$A_0' + A_1' F + A_2' F^2 + \cdots + A_d' F^d + F'(A_1 + 2A_2 F + \cdots + d A_d F^{d-1}).$$

The coefficient of F' cannot be zero (d is minimal and the A_js are not all zero). Hence F' is the quotient of two elements that are algebraic over $K(X)$, thus it is algebraic over $K(X)$.

10.3.2. A simple example

Let $F(X) := \sum_{n \geq 0} u_n X^n$ where $(u_n)_{n \geq 0}$ is the Thue–Morse sequence. We have

$$\begin{aligned} F(X) &= \sum_{n \geq 0} u_{2n} X^{2n} + \sum_{n \geq 0} u_{2n+1} X^{2n+1} = \sum_{n \geq 0} u_n X^{2n} + X \sum_{n \geq 0} (u_n + 1) X^{2n} \\ &= F(X^2) + X F(X^2) + X \frac{1}{1 - X^2}. \end{aligned}$$

Hence we have, over the two-element field $\mathbb{F}_2$,

$$(1 + X)^3 F(X)^2 + (1 + X)^2 F(X) + X = 0.$$

In other words the series $F(X)$ is algebraic (actually quadratic) over the field $\mathbb{F}_2(X)$.

10.3.3. Christol's theorem

The example given in Section 10.3.2 is actually a particular case of a general property of algebraic formal power series over a finite field $\mathbb{F}_q(X)$, which is a characterization of these series. We begin with a definition and a lemma.

Let $q = p^t$ be a positive power of a prime integer p. Let $\mathbb{F}_q$ be the finite field of cardinality q (the characteristic of $\mathbb{F}_q$ is p). For $0 \leq r < q$, we define the linear map λ_r on $\mathbb{F}_q[[X]]$ by

$$\text{if } F = F(X) = \sum_{i \geq 0} u_i X^i, \text{ then } \lambda_r(F) := \sum_{i \geq 0} u_{qi+r} X^i.$$

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

Lemma 10.3.2. *Let $A = A(X)$ and $B = B(X)$ be two formal power series in $\mathbb{F}_q[[X]]$. Then $A = \sum_{0 \le r < q} X^r \lambda_r(A)^q$, and $\lambda_r(A^q B) = A\lambda_r(B)$.*

Proof. The proof is left to the reader who might want to remember that we have in $\mathbb{F}_q[[X]]$ the equality

$$(\sum_{n \ge 0} u_n X^n)^q = \sum_{n \ge 0} u_n X^{qn}. \qquad \blacksquare$$

We will also need a proposition proving that, in positive characteristic, any algebraic formal power series satisfies a "special" algebraic equation.

Proposition 10.3.3. *Let p be a prime number, let $\alpha \ge 1$ be an integer, and $q := p^t$. Let $F(X)$ be a formal power series with coefficients in $\mathbb{F}_q$. Then F is algebraic over $\mathbb{F}_q(X)$ if and only if there exist polynomials $B_0(X), \ldots, B_t(X)$ in $\mathbb{F}_q[X]$ not all equal to zero, such that*

$$B_0 F + B_1 F^q + B_2 F^{q^2} + \cdots + B_t F^{q^t} = 0.$$

Furthermore we can suppose that $B_0 \neq 0$.

Proof. If the formal power series $F(X)$ satisfies

$$B_0 F + B_1 F^q + B_2 F^{q^2} + \cdots + B_t F^{q^t} = 0,$$

where the polynomials $B_j(X)$ are not all equal to zero, then F is clearly algebraic over $\mathbb{F}_q(X)$. Now, if F is algebraic, the series F, F^q, $F^{q^2}, \ldots$, cannot be all linearly independent. Hence there exists a nontrivial linear relation

$$B_0 F + B_1 F^q + B_2 F^{q^2} + \cdots + B_t F^{q^t} = 0.$$

Let us prove that there exists such a relation with $B_0 \neq 0$. Suppose that

$$B_0 F + B_1 F^q + B_2 F^{q^2} + \cdots + B_t F^{q^t} = 0$$

with t minimal, and let j be the smallest nonnegative integer such that $B_j \neq 0$. We will prove that $j = 0$. Since

$$B_j = \sum_{0 \le r < q} X^r (\lambda_r(B_j))^q$$

by Lemma 10.3.2, it follows that there exists r with $\lambda_r(B_j) \neq 0$. Now, since $\sum_{j \le i \le t} B_i F(X)^{q^i} = 0$, we have

$$\sum_{j \le i \le t} \lambda_r(B_i F^{q^i}) = 0$$

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

and, using Lemma 10.3.2, we see that, if $j \neq 0$, then

$$\sum_{j \leq i \leq t} \lambda_r(B_i) F^{q^{i-1}} = 0,$$

which gives a new relation with the coefficient of $F^{q^{j-1}} \neq 0$, a contradiction, hence $j = 0$. We thus have the relation

$$\sum_{0 \leq i \leq t} B_i F^{q^i} = 0,$$

with $B_0 \neq 0$. ∎

We now state Christol's theorem.

Theorem 10.3.4. *Let $\mathcal{A}$ be a nonempty alphabet, and let $(u_n)_{n\geq 0}$ be a sequence of elements of $\mathcal{A}$. Let p be a prime number. Then the sequence $(u_n)_{n\geq 0}$ is p-automatic if and only if there exist an integer $\alpha \geq 1$ and an injective map $\iota : \mathcal{A} \to \mathbb{F}_{p^\alpha}$ such that the formal power series $\sum_{n\geq 0} \iota(u_n) X^n$ is algebraic over $\mathbb{F}_{p^\alpha}(X)$.*

Proof. Let us first suppose that the sequence $(u_n)_{n\geq 0}$ is p-automatic. Choose α such that $|\mathcal{A}| \leq p^\alpha$, and choose an injective map $\iota : \mathcal{A} \to \mathbb{F}_{p^\alpha}$. Up to notation we may suppose that $\mathcal{A} \subset \mathbb{F}_{p^\alpha}$ and that ι is the identity map. We thus want to prove that the formal power series $\sum_{n\geq 0} u_n X^n$ is algebraic over $\mathbb{F}_{p^\alpha}[X]$. Since the sequence $(u_n)_{n\geq 0}$ is p-automatic, it is also p^α-automatic from Corollary 10.2.10. Hence $\mathcal{K}(p^\alpha, (u_n)_n)$ is finite, say

$$\mathcal{K}(p^\alpha, (u_n)_n) = \{(u_n^{(1)})_{n\geq 0}, (u_n^{(2)})_{n\geq 0}, \ldots, (u_n^{(t)})_{n\geq 0}\}$$

with $(u_n^{(1)})_{n\geq 0} = (u_n)_{n\geq 0}$. Let us define

$$F_j(X) := \sum_{n\geq 0} u_n^{(j)} X^n \quad \text{for } j \text{ in } [1, t].$$

Then, for j such that $1 \leq j \leq t$, we have

$$F_j(X) = \sum_{0\leq r\leq p^\alpha - 1} \left(\sum_{m\geq 0} u^{(j)}_{p^\alpha m + r} X^{p^\alpha m + r} \right) = \sum_{0\leq r\leq p^\alpha - 1} X^r \sum_{m\geq 0} u^{(j)}_{p^\alpha m + r} X^{p^\alpha m}.$$

But the sequence $(u^{(j)}_{p^\alpha m+r})_{m\geq 0}$ is one of the sequences $(u^{(i)}(m))_{m\geq 0}$, hence $F_j(X)$ is a linear combination, with coefficients in the field $\mathbb{F}_{p^\alpha}(X)$, of the power series $F_i(X^{p^\alpha})$. In other words, for all $j \in [1, t]$, the formal power series $F_j(X)$ belongs to the $\mathbb{F}_{p^\alpha}(X)$-vector space generated by the t series $F_i(X^{p^\alpha})$, $i \in [1, t]$:

$$F_j(X) \in \langle F_1(X^{p^\alpha}), F_2(X^{p^\alpha}), \ldots, F_t(X^{p^\alpha}) \rangle.$$

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

This implies that for all $j \in [1, t]$

$$F_j(X^{p^\alpha}) \in \langle F_1(X^{p^{2\alpha}}), F_2(X^{p^{2\alpha}}), \dots, F_t(X^{p^{2\alpha}})\rangle,$$

and thus that for all $j \in [1, t]$

$$F_j(X) \in \langle F_1(X^{p^{2\alpha}}), F_2(X^{p^{2\alpha}}), \dots, F_t(X^{p^{2\alpha}})\rangle.$$

Hence, for all $j \in [1, t]$,

$$F_j(X) \text{ and } F_j(X^{p^\alpha}) \in \langle F_1(X^{p^{2\alpha}}), F_2(X^{p^{2\alpha}}), \dots, F_t(X^{p^{2\alpha}})\rangle.$$

This implies that, for all $j \in [1, t]$,

$$F_j(X^{p^\alpha}) \text{ and } F_j(X^{p^{2\alpha}}) \in \langle F_1(X^{p^{3\alpha}}), F_2(X^{p^{3\alpha}}), \dots, F_t(X^{p^{3\alpha}})\rangle.$$

Hence, for all $j \in [1, t]$,

$$F_j(X),\ F_j(X^{p^\alpha}) \text{ and } F_j(X^{p^{2\alpha}}) \in \langle F_1(X^{p^{3\alpha}}), F_2(X^{p^{3\alpha}}), \dots, F_t(X^{p^{3\alpha}})\rangle.$$

Iterating, we have, for all $j \in [1, t]$ and for all $k \in [0, t]$,

$$F_j(X^{p^{k\alpha}}) \in \langle F_1(X^{p^{(t+1)\alpha}}), F_2(X^{p^{(t+1)\alpha}}), \dots, F_t(X^{p^{(t+1)\alpha}})\rangle.$$

But the dimension of a finitely generated vector space is at most the number of its generators. Hence the dimension of the $\mathbb{F}_{p^\alpha}(X)$-vector space

$$\langle F_1(X^{p^{(t+1)\alpha}}), F_2(X^{p^{(t+1)\alpha}}), \dots, F_t(X^{p^{(t+1)\alpha}})\rangle$$

is at most t. Hence for any $j \in [1, t]$, there must exist a nontrivial linear relation between the formal power series

$$F_j(X), F_j(X^{p^\alpha}), \dots, F_j(X^{p^{t\alpha}})$$

over $\mathbb{F}_{p^\alpha}(X)$. Taking $j = 1$, and remembering that $F_j(X^{p^{k\alpha}}) = F_j^{p^{k\alpha}}(X)$ (the ground field is $\mathbb{F}_{p^\alpha}$) this gives that $F(X) = F_1(X) = \sum_{n\geq 0} u_n^{(1)} X^n$ is algebraic over $\mathbb{F}_{p^\alpha}(X)$.

Let us now suppose that there exist an integer $\alpha \geq 1$ and an injective map $\iota : \mathcal{A} \to \mathbb{F}_{p^\alpha}$ such that the formal power series $\sum_{n\geq 0} \iota(u_n) X^n$ is algebraic over $\mathbb{F}_{p^\alpha}(X)$. The sequence $(u_n)_{n\geq 0}$ is p-automatic if and only if the sequence $(\iota(u_n))_{n\geq 0}$ is p-automatic. Up to renaming we can suppose that $\mathcal{A} \subset \mathbb{F}_{p^\alpha}$ and that the formal power series $F := \sum_{n\geq 0} u_n X^n$ is algebraic over $\mathbb{F}_{p^\alpha}(X)$. Then, from Proposition 10.3.3, there exist polynomials $B_0(X), \dots, B_t(X)$ with $B_0 \neq 0$ such that

$$\sum_{0\leq i\leq t} B_i(X) F(X)^{q^i} = 0.$$

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

Define $G = G(X) := F(X)/B_0(X)$. Then

$$\sum_{0\le i\le t} B_i(X)B_0(X)^{q^i}G(X)^{q^i} = 0,$$

that is

$$G(X) = \sum_{1\le i\le t} C_i(X)G(X)^{q^i} \quad \text{where} \quad C_i(X) := -B_i(X)B_0^{q^i-2}(X).$$

Now let $N = \max(\deg B_0, \max\{\deg C_i\})$, and define $\mathcal{H}$ by

$$\mathcal{H} := \left\{ H \in \mathbb{F}_{p^\alpha}[[X]], \quad H = \sum_{0\le i\le t} D_i G^{q^i} \right.$$
$$\left. \text{with } D_i \in \mathbb{F}_{p^\alpha}[X] \text{ and } \deg D_i \le N \right\}.$$

It is clear that $\mathcal{H}$ is a finite set and that $F = B_0G$ belongs to $\mathcal{H}$. We now prove that $\mathcal{H}$ is mapped into itself by λ_r. Let $H \in \mathcal{H}$. Then

$$\lambda_r(H) = \lambda_r\left(D_0G + \sum_{1\le i\le t} D_iG^{q^i}\right) = \lambda_r\left(\sum_{1\le i\le t}(D_0C_i + D_i)G^{q^i}\right)$$
$$= \sum_{1\le i\le t} \lambda_r(D_0C_i + D_i)G^{q^{i-1}}.$$

Since $\deg D_0, \deg D_i, \deg C_i \le N$, we have $\deg(D_0C_i + D_i) \le 2N$, and hence

$$\deg(\lambda_r(D_0C_i + D_i)) \le \frac{2N}{q} \le N.$$

Hence $\mathcal{H}$ is a finite set that contains F and that is stable under the maps λ_r for $r \in [0, p^\alpha - 1]$. This clearly implies that the p^α-kernel of the sequence $(u_n)_{n\ge 0}$ is finite. The sequence $(u_n)_{n\ge 0}$ is thus p^α-automatic, hence p-automatic (Corollary 10.2.10). ∎

10.4. An application to transcendence in positive characteristic

The Christol theorem is a combinatorial criterion that can be used as a tool to prove the transcendence of formal power series over a finite field. We give here an automata-based proof of transcendence for the Carlitz formal power series Π.

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

Let p be a prime number. Let α be an integer ≥ 1 and let $q := p^\alpha$. The Carlitz formal power series Π_q is defined by

$$\Pi_q := \prod_{k\geq 1}\left(1 - \frac{X^{q^k} - X}{X^{q^{k+1}} - X}\right).$$

Remark 10.4.1. Note that Π_q belongs to $\mathbb{F}_q((X^{-1}))$.

Theorem 10.4.2. *The formal power series Π_q is transcendental over the field $F_q(X)$.*

Proof. We first compute Π_q'/Π_q, where Π_q' is the derivative of Π_q (with respect to X). It is easy to obtain:

$$\frac{\Pi_q'}{\Pi_q} = \left(\sum_{k\geq 1}\frac{1}{X^{q^k} - X}\right) - \frac{1}{X^q - X}.$$

If Π_q were algebraic over $\mathbb{F}_q(X)$, then Π_q' would also be algebraic in view of Remark 10.3.1. Hence Π_q'/Π_q would be algebraic. Since $1/(X^q - X)$ is rational, this would imply that $\sum_{k\geq 1}\frac{1}{X^{q^k}-X}$ would be algebraic over $\mathbb{F}_q(X)$. We then write

$$\begin{aligned}\sum_{k\geq 1}\frac{1}{X^{q^k} - X} &= \frac{1}{X}\sum_{k\geq 1}\frac{1}{X^{q^k-1}}\sum_{n\geq 0}\left(\frac{1}{X}\right)^{n(q^k-1)}\\ &= \frac{1}{X}\sum_{\substack{k\geq 1\\ n\geq 0}}\left(\frac{1}{X}\right)^{(n+1)(q^k-1)} = \frac{1}{X}\sum_{\substack{k\geq 1\\ n\geq 1}}\left(\frac{1}{X}\right)^{n(q^k-1)}\\ &= \frac{1}{X}\sum_{m\geq 1}\left(\frac{1}{X}\right)^m c(m),\end{aligned}$$

where

$$c(m) := \sum_{\substack{k,n\geq 1\\ n(q^k-1)=m}} 1 = \sum_{\substack{k\geq 1\\ q^k-1\mid m}} 1 = \sum_{\substack{k\geq 1\\ q^k-1\mid m}} 1.$$

We then note that $\mathbb{F}_q(X) = \mathbb{F}_q(X^{-1})$. Hence, replacing X by X^{-1} in Christol's theorem, we see that the algebraicity of Π_q would imply the q-automaticity of the sequence $(c(m))_{m\geq 1}$.

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

Now, if the sequence $(c(m))_{m\geq 1}$ were q-automatic, then the subsequence $(c(q^n-1))_{n\geq 0}$ would be ultimately periodic by Proposition 10.2.4. But

$$c(q^n-1) = \sum_{\substack{k\geq 1\\ q^k-1\mid q^n-1}} 1 = \sum_{\substack{k\geq 1\\ k\mid n}} 1 = d(n)$$

by Problem 10.4.1, where $d(n)$ is the number of positive integral divisors of n.

Since $q = p^k$ for some $k \geq 1$, where p is a prime, we would have that $(d(n) \bmod p)_{n\geq 1}$ is ultimately periodic. Hence there would exist integers $t \geq 1, n_0 \geq 0$ such that, for all $n \geq n_0$ and $k \geq 1$,

$$d(n+kt) \equiv d(n) \pmod{p}.$$

Take $k = nk'$. Then

$$d(n(1+k't)) \equiv d(n) \pmod{p}$$

for all $k' \geq 1$ and for all $n \geq n_0$. Now by Dirichlet's theorem we can find $k' \geq 1$ such that $p' = 1 + k't$ is a prime $\geq n_0$. Take $n = p'$. We get

$$d(p'^2) \equiv d(p') \pmod{p}$$

and hence $3 \equiv 2 \pmod{p}$, hence the desired contradiction. ∎

10.5. An application to transcendental power series over the rationals

We recall the following definition.

A word w on the alphabet $\mathcal{A}$ is called *primitive* if it cannot be written as $w = v^\alpha$ for some word v in $\mathcal{A}$ and some integer $\alpha \geq 2$.

Proposition 10.5.1. *Let $\psi_k(n)$ be the number of primitive words of length n on the alphabet $\mathcal{A}$ with* Card $\mathcal{A} = k \geq 2$. *Then the formal power series $R(X) = \sum_{k\geq 1} \psi_k(n)X^n$ is transcendental over $\mathbb{Q}(X)$.*

Proof. We recall that $\psi_k(n) = \sum_{d\mid n} \mu(d)k^{n/d}$, where μ is the Möbius function (see Problem 10.5.1). If the series $R(X) = \sum_{k\geq 1} \psi_k(n)X^n$ were algebraic over $\mathbb{Q}(X)$, then the series $\widetilde{R}(X) := \sum_{n\geq 1} \frac{\psi_k(n)}{k} X^n$ would also be algebraic over $\mathbb{Q}(X)$. Thus (note that the number $\psi_k(n)/k$ is an integer for every $n \geq 1$) for any prime number p the series

$$\widetilde{R}_p(X) = \sum_{n\geq 1} (\frac{\psi_k(n)}{k} \bmod p)X^n$$

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

would be algebraic over the field $\mathbb{F}_p(X)$ from Problem 10.5.2. Take any prime number p dividing k (recall that $k \geq 2$). We see that $\psi_k(n)/k \equiv \mu(n) \mod p$. Hence the series

$$\sum_{n\geq 1}(\mu(n) \bmod p)X^n$$

would be algebraic over $\mathbb{F}_p(X)$. It follows, using Theorem 10.3.4, that the sequence $(\mu(n) \bmod p)_{n\geq 0}$ would be p-automatic. From Proposition 10.2.15 this implies that, if the set

$$\{n \geq 1,\ \mu(n) \equiv 0 \bmod p\} = \{n \geq 1,\ \mu(n) = 0\}$$

had a density, this density would be rational. But this set has a density equal to $1 - 6/\pi^2$ (see Problem 10.5.1), which gives the desired contradiction. ∎

Remark 10.5.2. Proposition 10.5.1 and the Chomsky–Schützenberger theorem imply the following result: if the language of primitive words over an alphabet of size ≥ 2 is context-free, it must be inherently ambiguous.

10.6. An application to transcendence of real numbers

We will prove in this section a theorem of transcendence (over the rationals) of real numbers whose base b-expansion is the fixed point of a morphism satisfying some extra hypotheses. This theorem is a consequence of a combinatorial version of a theorem of Ridout. We first give Ridout's theorem without proof.

Theorem 10.6.1. *Let $\xi \neq 0$ be a real algebraic number. Let ρ, c_1, c_2, c_3 be positive constants, and let λ and μ satisfy $0 \leq \lambda, \mu \leq 1$. Let $r', r'' \geq 0$ be integers, and suppose $\omega_1, \omega_2, \ldots, \omega_{r'+r''}$ are finitely many distinct primes. Assume there exist infinitely many fractions p_n/q_n such that*

$$\left|\frac{p_n}{q_n} - \xi\right| \leq c_1\,|q_n|^{-\rho}\,.$$

Furthermore, suppose that p_n and q_n are not zero and can be written in the form

$$p_n = p'_n \prod_{j=1}^{r'} \omega_j^{e_j}, \qquad q_n = q'_n \prod_{j=r'+1}^{r'+r''} \omega_j^{e_j},$$

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

where the e_i are nonnegative integers that may depend on n, and the (p'_n)s and (q'_n)s are positive integers that may depend on n. Finally, suppose that

$$0 < |p'_n| \le c_2 |p_n|^{\lambda}, \quad 0 < |q'_n| \le c_3 |q_n|^{\mu}.$$

for all $n \ge 0$. Then

$$\rho \le \lambda + \mu.$$

Corollary 10.6.2. *Let ξ be an irrational number. Suppose that, for every integer $n \ge 0$, the base-k expansion of ξ begins with $0.U_n V_n V_n V'_n$, where U_n belongs to $\{0, 1, \cdots, k-1\}^*$, V_n belongs to $\{0, 1, \cdots, k-1\}^+$, and the word V'_n is a prefix of V_n. Furthermore suppose that $\lim_{n\to\infty} |V_n| = \infty$, and that there exist real numbers $0 \le \alpha < \infty$ and $\beta > 0$ such that for all $n \ge 0$ we have $|U_n| \le \alpha |V_n|$ and $|V'_n| \ge \beta |V_n|$. Then ξ is a transcendental number.*

Proof. Let $r_n = |U_n|$, $s_n = |V_n|$, and $s'_n = |V'_n|$, so, for all $n \ge 0$, we have $r_n \le \alpha s_n$ and $s'_n \ge \beta s_n$. Define t_n to be the rational number whose base-k expansion is $t_n = 0.U_n V_n V_n V_n \cdots$. Hence $t_n = \dfrac{p_n}{k^{r_n}(k^{s_n} - 1)}$, for some integer p_n. Note that

$$|\xi - t_n| < \frac{1}{k^{r_n + 2s_n + s'_n}}.$$

Now,

$$\frac{s_n}{r_n + s_n} \ge \frac{1}{1 + \alpha}$$

and

$$\frac{r_n + 2s_n + s'_n}{r_n + s_n} \ge 1 + \frac{1 + \beta}{1 + \alpha}.$$

Hence there exist two positive real numbers μ, ρ such that

$$1 + \frac{s_n}{r_n + s_n} < 1 + \mu < \rho < \frac{r_n + 2s_n + s'_n}{r_n + s_n}$$

for infinitely many n. With this choice of μ and ρ, let us take $p'_n = p_n$, $\lambda = 1$, $c_2 = 1$, $q'_n = k^{s_n} - 1$. Let us choose the primes $\omega_{r'+1}, \cdots, \omega_{r'+r''}$ to be the prime divisors of k. Finally, defining $e_{r'+1}, \cdots, e_{r'+r''}$ by $k^{r_n} = \prod_{i=r'+1}^{r'+r''} \omega_j^{e_j}$, we can apply Ridout's theorem if ξ were algebraic irrational, and deduce that $\rho \le \lambda + \mu$, which gives a contradiction. Hence ξ is transcendental. (Note that the t_ns are not necessarily in their irreducible forms, but there is an infinite number of them, since the sequence $(t_n)_n$ converges to ξ, which is irrational from the hypothesis.) ∎

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

We deduce a theorem on transcendence of certain "automatic" real numbers. By abuse of notation with respect to Section 1.2.2, we define here an *overlap* as a word of the form wwa where a is the first letter of w (in other words an overlap is the beginning of a cube just longer than a square).

Theorem 10.6.3. *If the expansion of the real number $\xi \in (0, 1)$ in some integer base $b \geq 2$ is a nonultimately periodic fixed point of a d-morphism h for some $d \geq 2$, and if furthermore this expansion contains an overlap, then the number ξ is transcendental.*

Proof. We write the base-k expansion of ξ as $\xi = 0.UVVa\cdots$, where U and V are finite words, and a is the first letter of V. Since the expansion of ξ is a fixed point of the d-morphism h, then this expansion also begins with $h^n(U)h^n(V)h^n(V)h^n(a)$ for every $n \geq 1$. We can apply the previous corollary with $U_n = h^n(U)$, $V_n = h^n(V)$, and $V'_n = h^n(a)$: namely $|h^n(U)| = d^n|U|$, $|h^n(V)| = d^n|V|$, and $|h^n(a)| = d^n$. ∎

10.7. The Tribonacci word

The aim of this section is to use the Tribonacci word as a guideline to introduce various applications of combinatorics on words and symbolic dynamics to arithmetics.

10.7.1. Definitions and notation

Let us recall that the *Tribonacci word* is defined as the fixed point (in the sense of Remark 10.1.4) of the *Tribonacci morphism* $\sigma\{1, 2, 3\}^* \to \{1, 2, 3\}^*$ defined on the letters of the alphabet $\{1, 2, 3\}$ by $1 \mapsto 12$, $2 \mapsto 13$, $3 \mapsto 1$. Let us observe that the Tribonacci morphism admits a unique one-sided fixed point u in $\{1, 2, 3\}^\omega$.

The *incidence matrix* of the Tribonacci morphism σ is $M_\sigma = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$.

This matrix is easily seen to be primitive. Hence the Perron–Frobenius theorem applies (for more details, see Section 1.7.2).

The characteristic polynomial of M_σ is $X^3 - X^2 - X - 1$; this polynomial admits one positive root $\beta > 1$ (the dominant eigenvalue) and two complex conjugates α and $\overline{\alpha}$, with $|\alpha| < 1$; in particular, one has $1/\beta = \alpha\overline{\alpha}$. Hence β is a *Pisot number*, that is, an algebraic integer with all Galois conjugates having modulus less than 1.

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

In particular, the incidence matrix M_σ admits as eigenspaces in $\mathbb{R}^3$ one *expanding eigenline* (generated by the eigenvector with positive coordinates $v_\beta = (1/\beta, 1/\beta^2, 1/\beta^3)$ associated with the eigenvalue β) and a *contracting eigenplane* $\mathcal{P}$; we denote by v_α and $v_{\overline{\alpha}}$ the eigenvectors in $\mathbb{C}^3$ associated with α and $\overline{\alpha}$, normalized in such a way that the sum of their coordinates equals 1.

One associates with the Tribonacci word $u = (u_n)_{n\geq 0}$ a broken line starting from 0 in $\mathbb{Z}^3$ and approximating the expanding line v_β as follows. Let us first introduce the *abelianization map* f of the free monoid $\{1, 2, 3\}^*$ defined by

$$f : \{1, 2, 3\}^* \to \mathbb{Z}^3, \quad f(w) = |w|_1 e_1 + |w|_2 e_2 + |w|_3 e_3,$$

where $|w|_i$ denotes the number of occurrences of the letter i in the word w, and (e_1, e_2, e_3) denotes the canonical basis of $\mathbb{R}^3$. Note that for every finite word w, we have

$$f(\sigma(w)) = M_\sigma f(w).$$

The *Tribonacci broken line* is defined as the broken line which joins with segments of length 1 the points $f(u_0u_1 \cdots u_{N-1})$, $N \in \mathbb{N}$ (see Figure 10.1). In other words we describe this broken line by starting from the origin, and then by reading successively the letters of the Tribonacci word u, going one step in direction e_i if one reads the letter i.

We will see in Section 10.7.3 that the vectors $f(u_0u_1 \dots u_N)$, $N \in \mathbb{N}$, stay within bounded distance of the expanding line, which is exactly the direction given by the vector of probabilities of occurrence $(\pi(1), \pi(2), \pi(3))$ of the letters 1, 2, 3 in u. It is then natural to try to represent these points by projecting them along the expanding direction onto a transverse plane, that we chose here to be the plane $x + y + z = 0$. The closure of the set

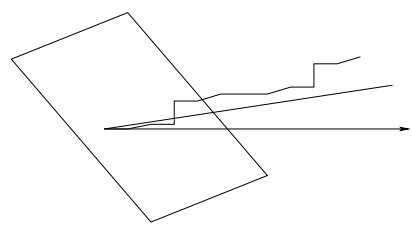

Figure 10.1. The Rauzy broken line.

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

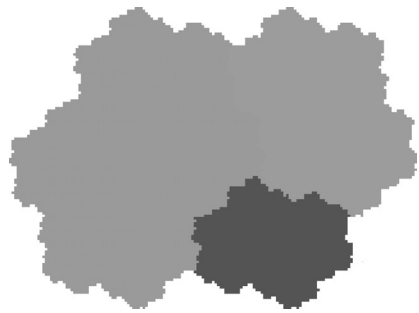

Figure 10.2. The Rauzy fractal.

of projected vertices of the broken line is called the *Rauzy fractal* and is represented on Figure 10.2. We detail this construction in Section 10.8.1. We then study the arithmetic and topological properties of the Rauzy fractal in Sections 10.8.2 and 10.8.4, respectively, which leads to the proof of the main theorem of this section: Theorem 10.8.16 states that the Tribonacci word codes the orbit of the point 0 under the action of the toral translation in $\mathbb{T}^2 : x \mapsto x + (1/\beta, 1/\beta^2)$. We discuss in Section 10.9 some applications of this theorem to simultaneous approximations: it is proved that the vertices of the broken line corresponding to $\sigma^n(1)$, $n \in \mathbb{N}$, produce best approximations for the vector $(1/\beta, 1/\beta^2)$ for a given norm associated with the matrix M_σ.

10.7.2. Numeration in Tribonacci base

We now introduce two numeration systems which will be used to expand here either natural integers or finite factors of the Tribonacci word.

The sequence of lengths $T = (T_n)_{n\geq 0}$ of the words $\sigma^n(1)$ is called the *sequence of Tribonacci numbers*. One has $T_0 = 1$, $T_1 = 2$, $T_2 = 4$ and for all $n \in \mathbb{N}$, $T_{n+3} = T_{n+2} + T_{n+1} + T_n$. Indeed, one has for $n \in \mathbb{N}$

$$\sigma^{n+3}(1) = \sigma^{n+2}(12) = \sigma^{n+2}(1)\sigma^{n+1}(13) = \sigma^{n+2}(1)\sigma^{n+1}(1)\sigma^n(1).$$

Let us observe that this sequence is increasing, and thus tends to infinity.

A *greedy* or *normal representation* in the system T of a nonnegative integer N is a finite sequence of digits $(\varepsilon_i)_{0\leq i\leq k}$ where for all i, $\varepsilon_i \in \{0, 1\}$ and $\varepsilon_{i+2}\varepsilon_{i+1}\varepsilon_i = 0$, $\varepsilon_k \neq 0$ such that

$$N = \sum_{i=0}^{k} \varepsilon_i T_i.$$

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

Lemma 10.7.1. *Every nonnegative integer admits a unique normal T-representation.*

Proof. Let us first prove the existence of the decomposition by induction. We consider the following induction property: for any integer $0 \leq N < T_k$ (with $k \geq 1$), there exists a decomposition $N = \sum_{i=0}^{k-1} \varepsilon_i T_i$, where for all i, $\varepsilon_i \in \{0, 1\}$ and $\varepsilon_{i+2}\varepsilon_{i+1}\varepsilon_i = 0$. This property holds for $k = 1, 2$.

Suppose that the induction hypothesis holds for the integer $k \geq 2$. Let $T_k \leq N < T_{k+1} = T_k + T_{k-1} + T_{k-2}$; we have $N - T_k < T_k$ and by hypothesis, $N - T_k = \sum_{i=0}^{k-1} \varepsilon_i T_i$, hence $N = T_k + \sum_{i=0}^{k-1} \varepsilon_i T_i$. Assume that $\varepsilon_{k-1} = 1$. Since $N < T_{k+1} = T_k + T_{k-1} + T_{k-2}$, then $\varepsilon_{k-2} = 0$, and the property holds for $k + 1$.

The uniqueness of a normal T-expansion is a direct consequence of the following observation: one has $\sum_{i=0}^{k} \varepsilon_i T_i < T_{k+1}$, where for all i, $\varepsilon_i \in \{0, 1\}$ and $\varepsilon_{i+2}\varepsilon_{i+1}\varepsilon_i = 0$.

This can be easily proved by induction. Indeed if $\varepsilon_k = \varepsilon_{k-1} = 1$, then $\varepsilon_{k-2} = 0$ and $\sum_{i=0}^{k} \varepsilon_i T_i = T_k + T_{k-1} + \sum_{i=0}^{k-3} \varepsilon_i T_i$. By induction hypothesis, $\sum_{i=0}^{k-2} \varepsilon_i T_i < T_{k-2}$, hence we get that $\sum_{i=0}^{k} \varepsilon_i T_i < T_k + T_{k-1} + T_{k-2} = T_{k+1}$. ∎

Lemma 10.7.2. *Every prefix w of the Tribonacci word u can be uniquely expanded as*

$$w = \sigma^n(p_n)\sigma^{n-1}(p_{n-1}) \cdots p_0,$$

where the finite words p_i are equal either to the empty word ε or to the letter 1, $p_n \neq \varepsilon$, and if $p_i = p_{i-1} = 1$, then $p_{i-2} = \varepsilon$; furthermore, $|w|$ admits as normal T-representation $|w| = \sum_{i=0}^{k} \varepsilon_i T_i$, with $\varepsilon_i = 1$ if $p_i = 1$, and $\varepsilon_i = 0$ otherwise. Conversely every finite word that can be decomposed under this form is a prefix of the Tribonacci word.

Such a representation is called normal Tribonacci representation.

Proof. The proof works exactly in the same way as the proof of Lemma 10.7.1. Let us prove by induction on $n \geq 1$ that every prefix w of length $|w| < |\sigma^n(1)|$ can be decomposed as

$$w = \sigma^{n-1}(p_{n-1})\sigma^{n-2}(p_{n-2}) \cdots p_0,$$

where the finite words p_i are equal either to the empty word ε or to the letter 1, $p_{n-1} \neq \varepsilon$, and if $p_i = p_{i-1} = 1$, then $p_{i-2} = 0$. The induction property holds for $n = 1, 2$.

Let w be a prefix of length at least 4 of the Tribonacci word. Then there exists a positive integer $n \geq 2$ such that $|\sigma^n(1)| \leq |w| < |\sigma^{n+1}(1)|$. One has $\sigma^{n+1}(1) = \sigma^n(1)\sigma^{n-1}(1)\sigma^{n-2}(1)$. Put $p_n = 1$; put $p_{n-1} = 1$, if $|w| \geq |\sigma^n(1)| + |\sigma^{n-1}(1)|$, and $p_{n-1} = \varepsilon$ otherwise.

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

Let v be such that $w = \sigma^n(p_n)\sigma^{n-1}(p_{n-1})v$ (v may be equal to the empty word); v is a prefix either of $\sigma^{n-1}(1)$ or of $\sigma^{n-2}(1)$. If $p_{n-1} = 1$, then $|v| < |\sigma^{n-2}(1)|$. We conclude by applying the induction hypothesis on v.

The uniqueness of such an expansion, as well as the corresponding normal T-representation for $|w|$, is a direct consequence of the fact that $|\sigma^n(1)| = T_n$ and of the uniqueness of normal T-representations (Lemma 10.7.1).

Let us prove by induction on n that every finite word of the form

$$\sigma^{n-1}(p_{n-1})\sigma^{n-2}(p_{n-2})\cdots p_0,$$

where the finite words p_i are equal either to the empty word ε or to the letter 1, $p_n \neq \varepsilon$, and if $p_i = p_{i-1} = 1$, then $p_{i-2} = 0$, is a prefix of the word $\sigma^{n+1}(1)$. This property holds for $n = 0, 1$. Assume that the induction hypothesis holds for every integer $k \leq n-1$. Let $w = \sigma^n(p_n)\sigma^{n-1}(p_{n-1})\cdots p_0$, with the above mentioned conditions on the "digits" p_i (and in particular $p_n = 1$).

One has

$$\begin{aligned}\sigma^{n+1}(1) &= \sigma^n(1)\sigma^n(2) = \sigma^n(1)\sigma^{n-1}(1)\sigma^{n-1}(3)\\ &= \sigma^n(1)\sigma^{n-1}(1)\sigma^{n-2}(1).\end{aligned}$$

Assume $p_{n-1} = 1$, then one has $p_{n-2} = \varepsilon$. By induction hypothesis the word $\sigma^{n-3}(p_{n-3})\cdots p_0$ is a prefix of $\sigma^{n-2}(1)$, which implies that w is a prefix of $\sigma^n(1)\sigma^{n-1}(1)\sigma^{n-2}(1)$ and thus of $\sigma^{n+1}(1)$.

Assume now that $p_{n-1} = \varepsilon$. Then $\sigma^{n-2}(p_{n-2})\cdots p_0$ is a prefix of $\sigma^{n-1}(1)$, and w is a prefix of $\sigma^{n+1}(1)$, which ends the proof. ∎

Remark 10.7.3. Such a numeration system on finite factors of the Tribonacci word can similarly be introduced for fixed points of morphisms in the sense of Remark 10.1.4 (see Problem 10.7.3).

10.7.3. Density properties: statistics on letters

Since the Tribonacci morphism is primitive, we know from Sections 1.7.2 and 1.8.6 that, by applying the Perron–Frobenius theorem, the letters admit densities in the Tribonacci word and the vector of probabilities of occurrence of letters is equal to the normalized positive (right) eigenvector $v_\beta = (1/\beta, 1/\beta^2, 1/\beta^3)$ associated with the dominant eigenvalue β (let us recall that the incidence matrix is the transpose of the matrix introduced in Section 1.8.6). We give below a direct proof of this result and prove even a stronger result of convergence towards the probabilities of letters.

Proposition 10.7.4. *Each of the letters* $1, 2, 3$ *admits a density in the Tribonacci word. The probabilities of letters are positive. More precisely,*

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

the vector of probabilities $(\pi(1), \pi(2), \pi(3))$ *is equal to the normalized positive eigenvector* $v_\beta = (1/\beta, 1/\beta^2, 1/\beta^3)$ *associated with the dominant eigenvalue* β *of the incidence matrices of the Tribonacci morphism. Furthermore, there exists* $C > 0$ *such that*

$$\forall N, \ | \, |u_0 u_1 \cdots u_{N-1}|_i - \pi(i)N| \leq C.$$

Proof. Let $u_0 u_1 \cdots u_{N-1}$ be a prefix of the Tribonacci word; according to Lemma 10.7.2, let us decompose it as

$$u_0 \cdots u_{N-1} = \sigma^n(p_n)\sigma^{n-1}(p_{n-1}) \cdots p_0,$$

where the finite words p_i are equal either to the empty word ε or to the letter 1, $p_n \neq \varepsilon$, and if $p_k = p_{k-1} = 1$, then $p_{k-2} = 0$. Then for $i = 1, 2, 3$

$$|u_0 \cdots u_{N-1}|_i = \, < f(u_0 \cdots u_{N-1}), e_i >,$$

where $< >$ denotes the Hermitian scalar product in $\mathbb{C}^3$.

Let us write $e_1 = a_\beta v_\beta + a_\alpha v_\alpha + a_{\overline{\alpha}} v_{\overline{\alpha}}$, where $a_\beta, \ a_\alpha, \ a_{\overline{\alpha}} \in \mathbb{C}$. We have

$$f(\sigma^k(1)) = M_\sigma^k e_1 = a_\beta \beta^k v_\beta + a_\alpha \alpha^k v_\alpha + a_{\overline{\alpha}} \overline{\alpha}^k v_{\overline{\alpha}}.$$

Furthermore,

$$f(u_0 \cdots u_{N-1}) = \sum_{k=0}^{n} f(\sigma^k(p_k)),$$

which implies for $i = 1, 2, 3$

$$\begin{aligned} |u_0 \cdots u_{N-1}|_i = {} & a_\beta \left(\textstyle\sum_{k=0}^n |p_n| \beta^k\right) < v_\beta, e_i > + a_\alpha \left(\textstyle\sum_{k=0}^n |p_n| \alpha^k\right) \\ & \times < v_\alpha, e_i > + a_{\overline{\alpha}} \left(\textstyle\sum_{k=0}^n |p_n| \overline{\alpha}^k\right) < v_{\overline{\alpha}}, e_i >. \end{aligned}$$

Let us recall that $|\alpha| < 1$. We have proved that the vectors $f(\sigma^k(1))$ converge exponentially fast to the expanding line, whereas the vectors $f(u_0 \cdots u_{N-1})$ stay within bounded distance of this line (Figure 10.1).

One has

$$\begin{aligned} N &= \textstyle\sum_{i=1,2,3} |u_0 \cdots u_{N-1}|_i \\ &= a_\beta \textstyle\sum_{k=0}^n |p_n| \beta^k + a_\alpha \sum_{k=0}^n |p_n| \alpha^k + a_{\overline{\alpha}} \sum_{k=0}^n |p_n| \overline{\alpha}^k, \end{aligned}$$

since $< v_\beta, e_1 + e_2 + e_3 > \, = \, < v_\alpha, e_1 + e_2 + e_3 > \, = \, < v_{\overline{\alpha}}, e_1 + e_2 + e_3 > = 1$, according to our conventions of normalization.

Hence there exists $C > 0$ such that

$$\forall i = 1, 2, 3, \ | < f(u_0 \cdots u_{N-1}), e_i > \, - N < v_\beta, e_i > | \leq C,$$

which implies in particular that $< v_\beta, e_i > = \pi(i) = 1/\beta^i$, $i = 1, 2, 3$.

■

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

Remark 10.7.5. Proposition 10.7.4 holds more generally for Pisot morphisms (Problem 10.7.4) and is strongly connected to the balance properties of their fixed points (Problem 10.7.5). Let us observe that the statement in Proposition 10.7.4 is stronger than assertion 5 of the Perron–Frobenius theorem.

10.8. The Rauzy fractal

10.8.1. A discrete approximation of the line

The Tribonacci broken line stays within a bounded distance of the expanding line (Proposition 10.7.4 and Figure 10.1). Let us project its vertices $f(u_0 \cdots u_{N-1})$ along the expanding direction v_β, in order to obtain in particular some information on the quality of approximation of the expanding line by the points $f(\sigma^k(1))$, $k \in \mathbb{N}$. We thus choose here to project onto the plane $x + y + z = 0$; this allows us to express the coordinates of the projected points in the basis $(e_3 - e_1, e_2 - e_1)$ of the plane $x + y + z = 0$ in terms of the convergence towards the probabilities of occurrence of the letters, as explained in Equation (10.8.1).

Let π_0 denote the projection in $\mathbb{R}^3$ onto the plane $\mathcal{P}_0$ of equation $x + y + z = 0$ along the expanding line generated by the vector v_β. One has

$$\forall\, P = (x, y, z) \in \mathbb{R}^3, \quad \pi_0(P) = (x, y, z) - <(x, y, z), (1, 1, 1) > v_\beta,$$

that is,

$$\pi_0(P) = (\frac{1}{\beta}(x + y + z) - x)(e_3 - e_1) + (\frac{1}{\beta^2}(x + y + z) - y)(e_3 - e_2).$$

In particular, if $P = f(u_0 \cdots u_{N-1})$, for some $N \in \mathbb{N}$, then

$$\pi_0(P) = (\frac{N}{\beta} - |u_0 \cdots u_{N-1}|_1)(e_3 - e_1) + (\frac{N}{\beta^2} - |u_0 \cdots u_{N-1}|_2)(e_3 - e_2). \tag{10.8.1}$$

We define the set $\mathcal{R}$ as the closure of the projections of the vertices of the Tribonacci broken line:

$$\mathcal{R} := \overline{\{\pi_0(f(u_0 \dots u_{N-1}));\ N \in \mathbb{N}\}},$$

where $u_0 \dots u_{N-1}$ stands for the empty word when $N = 0$. The set $\mathcal{R}$ is called the *Rauzy fractal* associated with the Tribonacci morphism σ (see Figure 10.2).

We now introduce a lattice in the plane $\mathcal{P}_0$ which will play a key rôle in the following. Let $\mathcal{L}_0 := \mathbb{Z}^3 \cap \mathcal{P}_0$; $\mathcal{L}_0$ is equal to the lattice $\mathbb{Z}(e_3 - e_1) + \mathbb{Z}(e_3 - e_2)$.

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

Proposition 10.8.1. *The set $\mathcal{R}$ is compact. The translates of the Rauzy fractal by the vectors of the lattice $\mathcal{L}_0$ cover the plane $\mathcal{P}_0$, that is*

$$\cup_{\gamma\in\mathcal{L}_0}(\mathcal{R}+\gamma)=\mathcal{P}_0. \tag{10.8.2}$$

The interior of $\mathcal{R}$ is not empty.

Proof. We first deduce from (10.8.1) and Proposition 10.7.4 that the Rauzy fractal is bounded, and hence compact.

We then need the following lemma to prove that one has a covering of the plane $\mathcal{P}_0$ by the translates of the Rauzy fractal.

Lemma 10.8.2. *The translates along the lattice $\mathcal{L}_0$ of the vertices of the broken line $f(u_0u_1\dots u_{N-1})$, $N\in\mathbb{N}$, cover the following upper half space:*

$$\begin{aligned}&\{f(u_0u_1\dots u_{N-1})+\gamma;\ N\in\mathbb{N},\ \gamma\in\mathcal{L}_0\}\\&\quad=\{(x,y,z)\in\mathbb{Z}^3; x+y+z\geq 0\}.\end{aligned}$$

Proof. Let $(x,y,z)\in\mathbb{Z}^3$ with $x+y+z\geq 0$; let $N=x+y+z$; one has $N=|u_0u_1\dots u_{N-1}|_1+|u_0u_1\dots u_{N-1}|_2+|u_0u_1\dots u_{N-1}|_3$. Let

$$\gamma=(x-|u_0u_1\dots u_{N-1}|_1, y-|u_0u_1\dots u_{N-1}|_2, z-|u_0u_1\dots u_{N-1}|_3);$$

then $\gamma\in\mathbb{Z}(e_1-e_3)+\mathbb{Z}(e_2-e_3)=\mathcal{L}_0$. ∎

Let us end the proof of Proposition 10.8.1. We need the following theorem known as Kronecker's theorem that we recall here without a proof (a proof of this theorem can be found for instance in Cassels (1957)).

Theorem 10.8.3 (Kronecker's theorem)**.** *Let $r\geq 1$ and let $\alpha_1,\dots,\alpha_r$ be r real numbers such that $1,\alpha_1,\dots,\alpha_r$ are rationally independent. For every $\eta>0$ and for every $(x_1,\dots,x_r)\in\mathbb{R}^r$, there exist $N\in\mathbb{N}$, $(p_1,\dots,p_r)\in\mathbb{Z}^r$ such that*

$$\forall i=1,\dots,r,\ |N\alpha_i-p_i-x_i|<\eta.$$

Let us apply Kronecker's theorem to $1,1/\beta,1/\beta^2$ (which are rationally independent). Let us fix $\eta>0$ and let P be given in $\mathcal{P}_0$ with coordinates (x,y) say, in the basis (e_3-e_1,e_3-e_2). There exist $p,q\in\mathbb{Z}$, $N\in\mathbb{N}$ such that $|N(1/\beta)-p-x|<\eta$ and $|N(1/\beta)^2-q-y|<\eta$. Take $r=N-(p+q)$. Then the coordinates in the basis (e_3-e_1,e_3-e_2) of $\pi_0(p,q,r)$ and P differ by at most η. We thus have proved that $\pi_0(\{(p,q,r)\in\mathbb{Z}^3,\ p+q+r\geq 0\})$ is dense in $\mathcal{P}_0$. Consequently, given any point P of $\mathcal{P}_0$, there exists a sequence of points $(\pi_0(f(u_0u_1\dots u_{N_k-1}))+\gamma_k)_k$ with γ_k in the lattice $\mathcal{L}_0$ which converges to P in $\mathcal{P}_0$. Since $\mathcal{R}$ is bounded, there are infinitely many k for which the points γ_k of the lattice $\mathcal{L}_0$ take the same

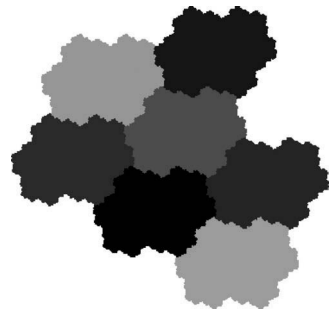

Figure 10.3. A piece of a periodic tiling by the Rauzy fractal.

value, say γ; we thus get $P \in \mathcal{R} + \gamma$, which implies (10.8.2). Since $\mathcal{L}_0$ is countable, we deduce from Baire's theorem that the interior of $\mathcal{R}$ is not empty. ∎

Remark 10.8.4. In fact, we have more than a covering by translates of the Rauzy fractal. We have indeed a periodic tiling of the plane up to sets of zero Lebesgue measure, that is, the union in (10.8.2) is disjoint up to sets of zero measure, as illustrated in Figure 10.3. We prove it in Section 10.8.5.

10.8.2. Arithmetic expression

In order to study more carefully the topological properties of the Rauzy fractal, which is the aim of Section 10.8.4, we introduce some more notation to express the coordinates of the vectors $f(u_0 \cdots u_{N-1})$ in the basis $(e_3 - e_1, e_3 - e_2)$ of the plane $\mathcal{P}_0$.

Let $\delta : \mathbb{N} \to \mathbb{R}^2$, $N \mapsto \delta(N)$, where $\delta(N)$ denotes the vector of coordinates of $\pi_0(f(u_0u_1 \cdots u_{N-1}))$ in the basis $(e_3 - e_1, e_3 - e_2)$ of the plane $x + y + z = 0$. One has according to (10.8.1), for $N \in \mathbb{N}$,

$$\delta(N) = N \cdot (1/\beta, 1/\beta^2) - (|u_0u_1 \cdots u_{N-1}|_1, |u_0u_1 \cdots u_{N-1}|_2). \tag{10.8.3}$$

Let $B = \begin{bmatrix} -1/\beta & -1/\beta \\ 1 - (1/\beta)^2 & -(1/\beta)^2 \end{bmatrix}$. One easily checks that for every word $w \in \{1, 2, 3\}^*$, then the vector of coordinates of $\pi_0(f(\sigma(w)))$ in the basis $(e_3 - e_1, e_3 - e_2)$ is equal to the matrix B applied to the vector of coordinates of $\pi_0(f(w))$ in the same basis. We thus get that if N has for normal T-representation, $N = \sum_{i=0}^{n} \varepsilon_i T_i$, that is, $u_0 \cdots u_{N-1} =$

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

$\sigma^n(p_n)\sigma^{n-1}(p_{n-1})\cdots p_0$, with $|p_i| = \varepsilon_i$, then

$$\delta(N) = \sum_{i=0}^{k} \varepsilon_i B^i z, \quad \text{where we set } z = \delta(1) = (1/\beta - 1, 1/\beta^2).$$

The eigenvalues of the matrix B are of modulus smaller than 1, hence the series $\sum_{i=0}^{\infty} \varepsilon_i B^i z$ are convergent in $\mathbb{R}^2$. The following proposition is thus an immediate consequence of this:

Proposition 10.8.5. *The Rauzy fractal is the set of points of the plane $\mathcal{P}_0$ with coordinates in the basis $(e_3 - e_1, e_3 - e_2)$ in*

$$R := \{\sum_{i=0}^{\infty} \varepsilon_i B^i z;\ (\varepsilon_i)_{i\geq 0} \in \{0,1\}^{\omega}, \forall i\ \varepsilon_i\varepsilon_{i+1}\varepsilon_{i+2} = 0\}.$$

Remark 10.8.6. We will mostly study the set R to deduce topological properties of the Rauzy fractal $\mathcal{R}$; indeed both sets are by definition in one-to-one correspondence, this bijection being the restriction of a topological isomorphism. Let us observe that similarly, the Rauzy fractal and

$$\{\sum_{i=0}^{\infty} \varepsilon_i \alpha^i \in \mathbb{C};\ (\varepsilon_i)_{i\geq 0} \in \{0,1\}^{\omega}, \forall i\ \varepsilon_i\varepsilon_{i+1}\varepsilon_{i+2} = 0\}$$

are also easily seen to be in one-to-one correspondence. Indeed the matrix B admits as characteristic polynomial $(X - \alpha)(X - \overline{\alpha})$, and it is thus similar in $\mathbb{C}^2$ to the matrix $\begin{bmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{bmatrix}$.

10.8.3. An exchange of pieces

Let us introduce the following division of the Rauzy fractal into three sets according to which letter was last read before projecting. For $i \in \{1,2,3\}$ let

$$\mathcal{R}_i = \overline{\{\pi_0(f(u_0 \dots u_{N-1}));\ N \in \mathbb{N},\ u_N = i\}}.$$

We similarly define the subsets R_i of $\mathbb{R}^2$, $i = 1,2,3$, as, respectively, the sets of coordinates of elements of $\mathcal{R}_i$ (in the basis $(e_3 - e_1, e_3 - e_2)$).

Lemma 10.8.7. *One has*

$$R_1 = \left\{\textstyle\sum_{i\geq 0} \varepsilon_i B^i z;\ \forall i,\ \varepsilon_i \in \{0,1\};\ \varepsilon_i\varepsilon_{i+1}\varepsilon_{i+2} = 0;\ \varepsilon_0 = 0\right\},$$
$$R_2 = \left\{\textstyle\sum_{i\geq 0} \varepsilon_i B^i z;\ \forall i,\ \varepsilon_i \in \{0,1\};\ \varepsilon_i\varepsilon_{i+1}\varepsilon_{i+2} = 0;\ \varepsilon_0\varepsilon_1 = 10\right\},$$
$$R_3 = \left\{\textstyle\sum_{i\geq 0} \varepsilon_i B^i z;\ \forall i,\ \varepsilon_i \in \{0,1\};\ \varepsilon_i\varepsilon_{i+1}\varepsilon_{i+2} = 0;\ \varepsilon_0\varepsilon_1 = 11\right\},$$

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

and

$$R_1 = BR, \quad R_2 = z + B^2R, \quad R_3 = z + Bz + B^3R,$$

that is,

$$R_1 = B(R_1 + R_2 + R_3), \quad R_2 = z + BR_1, \quad R_3 = z + BR_2.$$

Proof. It is sufficient to check that if $u_0 \cdots u_{N-1}$ admits for normal Tribonacci representation $\sigma^n(p_n) \cdots \sigma^0(p_0)$, then

$$\begin{cases} p_0 = \varepsilon \text{ implies } u_N = 1, \\ p_0 = 1, \quad p_1 = \varepsilon \text{ implies } u_N = 2, \\ p_0 = 1, \quad p_1 = 1 \text{ implies } u_N = 3. \end{cases}$$

- Assume that $p_0 = \varepsilon$. Then $u_0 \cdots u_{N-1} = \sigma^n(p_n) \cdots \sigma(p_1)$, and $u_0 \cdots u_N = \sigma^n(p_n) \cdots \sigma(p_1)u_N$. Hence u_N needs to be equal to 1, since the images of letters under σ begin with 1, and u is fixed under σ.
- Assume that $p_0 = 1$ and $p_1 = \varepsilon$. One has $u_0 \cdots u_{N-1} = \sigma^n(p_n) \cdots \sigma^2(p_2)1$. The word $\sigma^n(p_n) \cdots \sigma^2(p_2)\sigma(1)$ has length $N + 1$. If either p_2 or p_3 equals ε, then this expansion is a normal Tribonacci representation, and thus a prefix of the Tribonacci word (according to Lemma 10.7.2), which gives $u_N = 2$. Otherwise it can also be represented as $\sigma^n(p_n) \cdots \sigma^2(1) = \sigma^n(p_n) \cdots \sigma^4(1)$. One shows by induction that the last term of the normal Tribonacci representation of this expansion is of the form $\sigma^{3k+1}(1)$, which admits as last letter 2.
- Assume that $p_0 = 1$ and $p_1 = 1$, and thus $p_2 = \varepsilon$. Then $u_0 \cdots u_{N-1} = \sigma^n(p_n) \cdots \sigma^3(p_3)\sigma(1)1$. The word $\sigma^n(p_n) \cdots \sigma^2(1)$ has length $N + 1$. If either p_3 or p_4 equals ε, then this expansion is a normal Tribonacci representation, and thus a prefix of the Tribonacci word (according to Lemma 10.7.2), which gives $u_N = 3$. Otherwise it can also be represented as $\sigma^n(p_n) \cdots \sigma^2(1) = \sigma^n(p_n) \cdots \sigma^5(1)$. One shows by induction that the last term of the normal Tribonacci representation of this expansion is of the form $\sigma^{3k+2}(1)$, which admits as last letter 3. ∎

The sets $\mathcal{R}_i$, $i = 1, 2, 3$ are represented in Figure 10.2. Figure 10.4 illustrates Lemma 10.8.8, that is, one can reorganize the division of $\mathcal{R}$ into these three pieces up to translations.

Lemma 10.8.8. *The following exchange of pieces E is well defined*

$$E : \operatorname{Int} \mathcal{R}_1 \cup \operatorname{Int} \mathcal{R}_2 \cup \operatorname{Int} \mathcal{R}_3 \to \mathcal{R}, \ x \mapsto x + \pi_0(e_i), \quad \textit{when } x \in \operatorname{Int} \mathcal{R}_i.$$

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

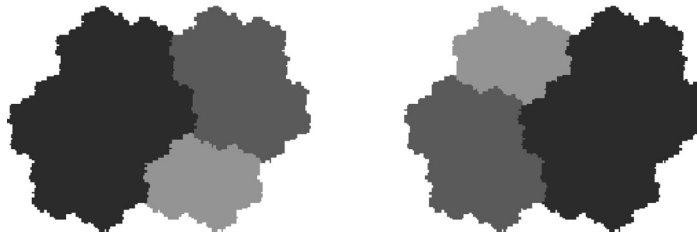

Figure 10.4. The exchange map E.

Proof. Let us first prove that the sets $\mathcal{R}_i$, for $i = 1, 2, 3$, are pairwise disjoint in measure, and hence that their interiors $\operatorname{Int} \mathcal{R}_i$ are pairwise disjoint.

Since $\mathcal{R}$ is compact, then it is measurable for the Lebesgue measure and its Lebesgue measure $\mu(\mathcal{R})$ is finite and nonzero since its interior is not empty according to Proposition 10.8.1.

One has $\mu(\mathcal{R}) \leq \sum_{i=1}^{3} \mu(\mathcal{R}_i)$. Since the determinant of the matrix B equals $1/\beta$, then according to Lemma 10.8.7

$$\mu(\mathcal{R}_1) = 1/\beta\ \mu(\mathcal{R}), \quad \mu(\mathcal{R}_2) = (1/\beta)^2 \mu(\mathcal{R}), \quad \mu(\mathcal{R}_3) = (1/\beta)^3 \mu(\mathcal{R}).$$

Hence one gets $\mu(\mathcal{R}) = \sum_{i=1}^{3} \mu(\mathcal{R}_i)$. This implies in particular that $\mu(\mathcal{R}_i \cap \mathcal{R}_j) = 0$ for $i \neq j$. The same holds for their interiors $\operatorname{Int} \mathcal{R}_i$, that is, $\mu(\operatorname{Int} \mathcal{R}_i \cap \operatorname{Int} \mathcal{R}_j) = 0$ for $i \neq j$, which implies that they are pairwise disjoint.

One easily sees that for $i = 1, 2, 3$, $\mathcal{R}_i + \pi_0(e_i) = \overline{\{\pi(f(u_0 \dots u_N));\ u_N = i\}}$, which implies $\mathcal{R}_i + \pi_0(e_i) \subset \mathcal{R}$. We thus deduce that the map E is well defined. ∎

Remark 10.8.9. The sets $\mathcal{R}_i$, $i = 1, 2, 3$ are not disjoint. Indeed a vector with coordinates in the basis $(e_3 - e_1, e_3 - e_2)$ having several expansions as $\sum_{i=0}^{\infty} \varepsilon_i B^i z$, (with $(\varepsilon_i)_{i \geq 0} \in \{0, 1\}^\omega$ and $\forall i,\ \varepsilon_i \varepsilon_{i+1} \varepsilon_{i+2} = 0$) can belong simultaneously to several of these sets. This is the case in particular of the vector with coordinates $\sum_{i=1}^{\infty} B^{3i} z$. Since $B^3 = B^2 + B + 1$, then $\sum_{i=1}^{\infty} B^{3i} z = \sum_{i=0}^{\infty} B^i z$, and it admits the following three admissible expansions

$$\sum_{i=1}^{\infty} B^{3i} z = z + \sum_{i=0}^{\infty} B^{3i+1} z = z + Bz + \sum_{i=0}^{\infty} B^{3i+2} z.$$

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

10.8.4. Some topological properties

We need now to introduce a suitable norm on $\mathbb{R}^2$ associated with the matrix B that will be crucial for the statement of the first topological properties of the Rauzy fractal, from which the arithmetic properties of Section 10.9 will be deduced.

Let us recall that the matrix B is similar in $\mathbb{C}^2$ to the matrix $\begin{bmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{bmatrix}$. Let

$$M = \begin{bmatrix} \overline{\alpha} + 1/\beta & 1/\beta \\ -(\alpha + 1/\beta) & -1/\beta \end{bmatrix}.$$

One easily checks that $MBM^{-1} = \begin{bmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{bmatrix}$.

The *Rauzy norm* $||\,||$ is defined for $x \in \mathbb{R}^2$ as the Euclidean norm of Mx. Hence, for every $x \in \mathbb{R}^2$

$$||Bx|| = |\alpha|||x|| = \sqrt{1/\beta}||x||.$$

We denote by $|||\ |||$ the distance to the nearest point with integer coordinates.

One checks that

$$||z|| = ||\delta(1)|| = |\alpha|^4 = 1/\beta^2 \quad \text{and} \quad ||\delta(T_n)|| = |\alpha|^n||z|| = |\alpha|^{n+4}.$$

We will mainly work in this section with the set of coordinates R, rather than with $\mathcal{R}$ itself. The following lemma states that if one takes an element of sufficiently small norm which is equal modulo $\mathbb{Z}^2$ to the coordinates $\delta(N)$ of $\pi_0(f(u_0 \cdots u_{N-1}))$, then it has to be exactly equal to $\delta(N)$. The proof is based on the fact that the set R is contained in the square $\{(x, y) \in \mathbb{R}^2;\ |x|, |y| < 1\}$ located at the origin. In particular, 0 is the only element with integer coordinates contained in R. This lemma is fundamental and is a first step towards the fact that if two points of R differ by a vector with integer coordinates, then these two points do coincide.

Lemma 10.8.10. *There exists $C > 0$ such that*

$$\forall N \geq 1,\ \forall v \in \mathbb{Z}^2,\ ||N \cdot (1/\beta, 1/\beta^2) - v|| < C \\ \Longrightarrow v = N \cdot (1/\beta, 1/\beta^2) - \delta(N).$$

Remark 10.8.11. This lemma implies in particular that if the norm of $\delta(N)$ is smaller than C, then $(|u_0 \cdots u_{N-1}|_1, u_0 \cdots u_{N-1}|_2)$ is the nearest point with integer coordinates to $N \cdot (1/\beta, 1/\beta^2)$. For instance, for n large enough,

$$|||T_n \cdot (1/\beta, 1/\beta^2)||| = ||\delta(T_n)||,$$

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

since $||\delta(T_n)|| = |\alpha|^{n+4} < C$. In other words, the projections of the points $f(\sigma^n(1))$ approximate very well the points with coordinates $T_n \cdot (1/\beta, 1/\beta^2)$.

Proof. Let $N \geq 1$ with normal T-representation $N = \sum_{i=0}^{k} \varepsilon_i T_i$. One can write $\delta(N) = \sum_{i=0}^{k} \varepsilon_i B^i z$ as $\delta(N) = \sum_{i \geq 0} \varepsilon_{3i} B^{3i} y_i$, where y_i belongs to the following set F:

$$F := \{0, z, Bz, B^2z, z + Bz, z + B^2z, Bz + B^2z\}.$$

Hence

$$||\delta(N)|| \leq \sum_{i \geq 0} |\alpha|^{3i} \max_{y \in F} ||y||.$$

One checks that $\max_{y \in F} ||y|| = ||z|| = 1/\beta^2$. We thus get

$$||\delta(N)|| \leq \frac{1}{\beta^2(1 - |\alpha^3|)} < 1/2. \tag{10.8.4}$$

One also checks that the set of points $x \in \mathbb{R}^2$ such that $||x|| < 0.53$ is a domain delimited by an ellipse strictly included in the square $\{(x, y) \in \mathbb{R}^2;\ |x|, |y| < 1\}$. Hence R is also included in this square, following (10.8.4).

Let $v \in \mathbb{Z}^2$. Take $C = 0.03$ for instance. Let $N \geq 1$ such that

$$||N \cdot (1/\beta, 1/\beta^2) - v|| < C.$$

Hence according to (10.8.3)

$$\begin{aligned} &||(|u_0 \cdots u_{N-1}|_0, |u_0 \cdots u_{N-1}|_1) - v|| \\ &\quad \leq ||\delta(N)|| + ||N \cdot (1/\beta, 1/\beta^2) - v|| < 0.53, \end{aligned}$$

which implies that $(|u_0 \cdots u_{N-1}|_0, |u_0 \cdots u_{N-1}|_1) - v$ belongs to the square $\{(x, y) \in \mathbb{R}^2; |x|, |y| < 1\}$ and thus $v = (|u_0 \cdots u_{N-1}|_0, |u_0 \cdots u_{N-1}|_1)$, since both vectors have integer coordinates. ∎

Proposition 10.8.12. *The point* 0 *belongs to the interior of the Rauzy fractal* $\mathcal{R}$. *Furthermore, for all* $N \in \mathbb{N}$, $\delta(N)$ *belongs to the interior of* R_{u_N}. *Consequently, the Rauzy fractal is the closure of its interior.*

Proof. Let us prove that 0 is an interior point of the set R. Let C be the constant of Lemma 10.8.13. The sequence $(N \cdot (1/\beta, 1/\beta^2))_{N \geq 0}$ is dense in $\mathbb{R}^2$ modulo $\mathbb{Z}^2$ by Kronecker's theorem (Theorem 10.8.3), since $1, 1/\beta, 1/\beta^2$ are linearly independent over $\mathbb{Q}$. In particular, it is dense modulo $\mathbb{Z}^2$ in the set $\{x \in \mathbb{R}^2;\ ||x|| < C\}$. This implies, according to Lemma 10.8.10, that the points $\delta(N)$ are also dense in this same set. Hence $\{x \in \mathbb{R}^2;\ ||x|| < C\}$

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

is included in the closure R of $\{\delta(N);\ N \in \mathbb{N}\}$. This proves that 0 is an interior point.

One easily deduces that for every $N \in \mathbb{N}$, $\delta(N)$ belongs to the interior of R_{u_N}. Indeed let us consider a given N with normal T-representation $\sum_{i=0}^{k} \varepsilon_i T_i$; by definition, $\delta(N) \in R_{u_N}$; for any $(\varepsilon_i)_{i\geq k+2} \in \{0,1\}^\omega$, with the admissibility condition that no three consecutive 1s occur in this sequence, then $\delta(N + \sum_{i\geq k+2} \varepsilon_l T_l) \in R_{u_N}$, which implies that $\delta(N) + B^{k+2}R$ is still included in R_{u_N}, and thus $\delta(N)$ belongs to the interior of R_{u_N}, since 0 belongs to the interior of R. This easily implies that $\mathcal{R}$ is the closure of its interior. ∎

One can even get more information on the first coefficients of N in its normal T-representation if the distance between $N \cdot (1/\beta, 1/\beta^2)$ and $\mathbb{Z}^2$ is small enough; this provides some knowledge on the repartition of the sequence $(N \cdot (1/\beta, 1/\beta^2))_{N\geq 0}$.

Lemma 10.8.13. *Let $N \geq 1$ with normal T-representation $N = \sum_{i\geq 0} \varepsilon_i T_i$. Then*

$$\forall v \in \mathbb{Z}^2,\ \forall m \in \mathbb{N},\ \big(||N \cdot (1/\beta, 1/\beta^2) - v|| < C\beta^{-m/2} \Rightarrow \forall i < m,\ \varepsilon_i = 0\big).$$

Proof. Let $N \geq 1$ with normal T-representation $N = \sum_{i\geq 0} \varepsilon_i T_i$ and let $v \in \mathbb{Z}^2$ such that there exists $m \geq 1$ with $||N \cdot (1/\beta, 1/\beta^2) - v|| < C\beta^{-m/2}$. Since $||N \cdot (1/\beta, 1/\beta^2) - v|| < C$, and according to Lemma 10.8.10, then $\delta(N) = N \cdot (1/\beta, 1/\beta^2) - v$. Furthermore one has $B^{-m}\delta(N) \in R$; indeed $||B^{-m}\delta(N)|| = \beta^{m/2}||\delta(N)|| < C$, and we have seen in the proof of Proposition 10.8.12 that $\{x;\ ||x|| < C\}$ is included in R.

It remains to prove that if N satisfies $\delta(N) \in B^m R$, then its normal T-representation verifies $N = \sum_{i\geq m} \varepsilon_i$. For that purpose, we introduce the following notation in order to refine the partition of R into the three pieces R_i, $i = 1, 2, 3$. Let us consider the following three maps $\psi_i : \mathbb{R}^2 \to \mathbb{R}^2$, $i = 1, 2, 3$, as follows (recall that $z = \delta(1)$):

$$\psi_1 : v \mapsto Bv, \quad \psi_2 : v \mapsto z + B^2 v, \quad \psi_3 : v \mapsto z + Bz + B^3 v.$$

For $a_1 \cdots a_r \in \{1,2,3\}^r$, let $R_{a_1\cdots a_r} = \psi_{a_0} \circ \cdots \circ \psi_{a_r}(R)$. Let us observe that $R_{a_1\cdots a_r} \subset R$.

One proves by induction that for all N, and for all r, there exists $a_1 \cdots a_r$ such that $\delta(N)$ belongs to $R_{a_1\cdots a_r}$. Indeed, let $v = \sum_{j\geq 0} \varepsilon_j B^j z \in R$; if $v \in R_i$, then there exists $w \in R$ such that $v = \psi_i(w)$. Furthermore, the same argument as in the proof of Proposition 10.8.12 implies that $\delta(N)$ belongs to the interior of $R_{a_1\cdots a_r}$.

Let us prove by induction on r that the interiors of the sets $R_{a_1\cdots a_r}$ are pairwise disjoint. The induction property holds for $r = 1$ according

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

to Lemma 10.8.8. Assume it is true for $k \leq r$, with $r \geq 1$. Let $a_1 \cdots a_r \in \{1, 2, 3\}^r$. One has $\mu(R_{a_1 \cdots a_r i}) = (1/\beta)^i \mu(R_{a_1 \cdots a_r})$, which implies similarly as in the proof of Lemma 10.8.8 that the interiors of the sets $R_{a_1 \cdots a_r i}$, $i = 1, 2, 3$, are pairwise disjoint in measure, as well as the interiors of the sets $R_{a_1 \cdots a_r i}$, for $i = 1, 2, 3$, and $a_1 \cdots a_r \in \{1, 2, 3\}^r$.

Hence for every N, and for every r, there exists a unique $a_1 \cdots a_r$ such that $\delta(N)$ belongs to the interior of $R_{a_1 \cdots a_r}$. Furthermore it is easily seen that if there exists k such that $a_k \neq 1$, then there exists a coefficient ε_i equal to 1, with $i < r$, in the normal T-representation of N. This implies that if $\delta(N) \in B^m R = \psi_1^m(R)$, then all the coefficients ε_i for $i < m$ are equal to 0 in its normal T-representation. ∎

10.8.5. Tiling and Tribonacci translation

We are now able to prove that the covering of the plane $\mathcal{P}_0$ stated in Proposition 10.8.1, that is $\cup_{\gamma \in \mathcal{L}_0} \mathcal{R} + \gamma$, is in fact a periodic tiling (up to sets of zero measure).

Lemma 10.8.14. *The sets* $\operatorname{Int} \mathcal{R} + \gamma$, *for* $\gamma \in \mathcal{L}_0$, *are disjoint, that is,*

$$\text{if } x, y \in \operatorname{Int} R, \text{ with } x - y \in \mathbb{Z}^2, \text{ then } x = y.$$

Proof. Let $x, y \in \operatorname{Int} R$ with $x - y \in \mathbb{Z}^2$. By density of the sequence $(\delta(N))_{N \geq 0}$, there exists a point $\delta(M)$ close enough to x that $\delta(M) + y - x$ is close enough to y, and thus still belongs to R.

Let us choose an integer m large enough so that the coefficients ε_i in the normal T-representation of M are equal to 0 for $i \geq m$. One gets $M = \sum_{i=0}^{m} \varepsilon_i T_i$. By density of the sequence $(\delta(N))_N$, there exists $N > M$ such that

$$||\delta(N) - (\delta(M) + y - x)|| < C \left(\frac{1}{\beta}\right)^{(m+2)/2}.$$

There exists $h \in \mathbb{Z}^2$ such that $\delta(N) - (\delta(M) + y - x) = (N - M) \cdot (1/\beta, 1/\beta^2) - h$. We thus can apply Lemma 10.8.13, and get that the normal T-representation $\sum_{i=0}^{k} \varepsilon_i' T_i$ of $N - M$ satisfies $\varepsilon_i' = 0$ for $i \leq m + 1$. This implies that N admits as normal T-representation $\sum_{i=0}^{m} \varepsilon_i T_i + \sum_{i \geq m+2} \varepsilon_i' T_i$, and hence $\delta(N) - \delta(M) = \delta(N - M)$. Since $||(N - M) \cdot (1/\beta, 1/\beta^2) - h|| < C(1/\beta)^{(m+2)/2} < C$, it follows from Lemma 10.8.10 that

$$\begin{aligned} \delta(N - M) &= (N - M) \cdot (1/\beta, 1/\beta^2) - h = \delta(N) - \delta(M) \\ &= \delta(N) - \delta(M) + x - y, \end{aligned}$$

which implies $y = x$. ∎

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

Remark 10.8.15. The domain R is thus a fundamental domain of the torus $\mathbb{T}^2 = \mathbb{R}^2/\mathbb{Z}^2$, that is,

$$\mathbb{R}^2 = \cup_{v\in\mathbb{Z}^2} R + v,\ \mathcal{P}_0 = \cup_{\gamma\in\mathbb{Z}^2} \mathcal{R} + \gamma,$$

both unions being disjoint up to sets of zero measure.

This tiling property has the following arithmetic formulation: the translation by $(1/\beta, 1/\beta^2)$ in $\mathbb{R}^2/\mathbb{Z}^2 = \mathbb{T}^2$, which is the quotient map of the exchange map E defined in Lemma 10.8.8 with respect to the lattice $\mathcal{L}_0$, is coded by the Tribonacci word:

Theorem 10.8.16. *The Tribonacci word codes the orbit of the point* 0 *under the action of the translation*

$$R_\beta : \mathbb{T}^2 \to \mathbb{T}^2,\ x \mapsto x + (1/\beta, 1/\beta^2)$$

with respect to the partition of the fundamental domain R *of* $\mathbb{T}^2$ *by the sets* (R_1, R_2, R_3)*, that is,*

$$\forall N \in \mathbb{N},\ \forall i = 1, 2, 3,\ u_N = i \iff R_\beta^N(0) \in R_i.$$

Proof. According to Proposition 10.8.12, for every N, there exists $i = 1, 2, 3$ such that $\delta(N)$ belongs to the interior of R_i; hence $R_\beta^N(0)$ (which is congruent modulo $\mathbb{Z}^2$ to $\delta(N)$) also belongs modulo $\mathbb{Z}^2$ to R_i. Furthermore, such an integer i is unique according to Lemma 10.8.14. This implies that the coding of the orbit of 0 under R_β is well defined.

Let E be the exchange of pieces introduced in Lemma 10.8.8. Let us prove by induction on N that $E^N(0) = \pi_0(f(u_0 \cdots u_{N-1}))$. The induction property holds for $N = 0$. Suppose that the induction property holds for N. One has $\pi_0(f(u_0 \cdots u_{N-1})) \in \operatorname{Int} \mathcal{R}_{u_N}$. Hence $E^{N+1}(0) = E(\pi_0(f(u_0 \cdots u_{N-1}))) = \pi_0(f(u_0 \cdots u_{N-1})) + \pi_0(e_{u_N}) = \pi_0(f(u_0 \cdots u_N))$, which ends the induction proof.

One thus deduces that for all $N \in \mathbb{N}$, for all $i = 1, 2, 3$, $E^N(0) = \pi_0(f(u_0 \cdots u_{N-1})) \in \mathcal{R}_i$ if and only if $u_N = i$. In other words, we have proved that the Tribonacci word codes the orbit of 0 under the action of the map E with respect to the partition $(\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3)$, that is,

$$\forall N \in \mathbb{N},\ \forall i = 1, 2, 3,\ u_N = i \iff E^N(0) = i.$$

It remains to check that for all $N \in \mathbb{N}$, for all $i = 1, 2, 3$, $E^N(0) \in \mathcal{R}_i$ if and only if $R_\beta^N(0) \in R_i$. By definition, the coordinates of $E^N(0)$ in the basis $(e_3 - e_1, e_3 - e_2)$ are equal to $\delta(N)$, which is congruent to $R_\beta^N(0)$ modulo $\mathbb{Z}^2$, which ends the proof. ∎

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

10.8.6. A cut and project scheme

The aim of this section is to reformulate the previous results in terms of a "cut and project scheme": Theorem 10.8.18 states that the vertices of the broken line are exactly the points of $\mathbb{Z}^3$ selected by shifting the Rauzy fractal (considered as an "acceptance window"), along the eigendirection v_β.

A *cut and project scheme* consists of a direct product $\mathbb{R}^k \times H$, $k \geq 1$, where H is a locally compact Abelian group, and a lattice D in $\mathbb{R}^k \times H$, such that with respect to the natural projections $p_0 : \mathbb{R}^k \times H \to H$ and $p_1 : \mathbb{R}^k \times H \to \mathbb{R}^k$:

1. $p_0(D)$ is dense in H;
2. p_1 restricted to D is one-to-one onto its image $p_1(D)$.

This cut and project scheme is denoted $(\mathbb{R}^k \times H, D)$.

A subset Γ of $\mathbb{R}^k$ is a *model set* if there exists a cut and project scheme $(\mathbb{R}^k \times H, D)$ and a relatively compact set (i.e. a set such that its closure is compact) Ω of H with nonempty interior such that

$$\Gamma = \{p_1(P);\ P \in D,\ p_0(P) \in \Omega\}.$$

The set Γ is called the *acceptance window* of the cut and project scheme.

A *Meyer set* S is a subset of some model set of $\mathbb{R}^k$, for some $k \geq 1$, which is *relatively dense*, that is, there exists $R > 0$ such that for all $P \in \mathbb{R}^k$, there exists $M \in S$ such that the ball of radius R located at P contains M.

Remark 10.8.17. The locally Abelian compact groups which usually occur in the previous definition are either Euclidean or p-adic spaces.

Let π_1 denote the projection in $\mathbb{R}^3$ on the expanding line generated by v_β along the plane $\mathcal{P}_0$. Let us recall that π_0 denotes the projection on the plane $\mathcal{P}_0$ along the expanding line.

Theorem 10.8.18. *The subset $\pi_1(\{f(u_0 \cdots u_{N-1}); N \in \mathbb{N}\})$ of the expanding eigenline obtained by projecting under π_1 the vertices of the Tribonacci broken line is a Meyer set associated with the cut and project scheme $(\mathbb{R} \times \mathbb{R}^2, \mathbb{Z}^3)$, with acceptance window the interior of the set $\mathcal{R}$ of coordinates of the Rauzy fractal. In other words,*

$$\{f(u_0 \cdots u_{N-1});\ N \in \mathbb{N}\} = \{P = (x, y, z) \in \mathbb{Z}^3;\ x + y + z \geq 0; \pi_0(P) \in \operatorname{Int} \mathcal{R}\}. \tag{10.8.5}$$

Proof. Let $H = \mathbb{R}^2$, $D = \mathbb{Z}^3$, $k = 1$. The set $H = \mathbb{R}^2$ is in one-to-one correspondence with the plane $\mathcal{P}_0$, whereas $\mathbb{R}$ is in one-to-one correspondence with the expanding eigenline. Up to these two bijections, the natural projections become respectively π_0 and π_1 and are easily seen to satisfy the

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

required conditions (the density has been proved in the proof of Proposition 10.8.1). It remains to prove (10.8.5) to conclude.

According to Lemma 10.8.12, for every N, $\pi_0(f(u_0 \cdots u_{N-1})) \in \operatorname{Int} \mathcal{R}$. Conversely, let $P = (x, y, z) \in \mathbb{Z}^3$ with $x + y + z \geq 0$ such that $\pi_0(P) \in \operatorname{Int} \mathcal{R}$. Let $N = x + y + z$. According to Lemma 10.8.2, there exists $\gamma \in \mathcal{L}_0$ such that $P = f(u_0 \cdots u_{N-1}) + \gamma$. Since $\pi_0(P) = \pi_0(f(u_0 \cdots u_{N-1})) + \pi_0(\gamma) = \pi_0(f(u_0 \cdots u_{N-1})) + \gamma$, one gets $P = f(u_0 \cdots u_{N-1})$, following Lemma 10.8.14. ∎

Remark 10.8.19. Cut and project schemes are used to model quasicrystals and to generate aperiodic tilings, as illustrated in Problem 10.8.6.

10.9. An application to simultaneous approximation

We end this chapter with a section devoted to the study of some Diophantine approximation properties of the vector of translation $(1/\beta, 1/\beta^2)$ of the Tribonacci translation. In particular, the sequence of Tribonacci numbers is shown to be the sequence of best approximations of this vector for the Rauzy norm. Indeed, the vertices of the broken line of the form $f(\sigma^n(1))$, $n \in \mathbb{N}$, provide (after projection) very good approximations of the vector $(1/\beta, 1/\beta^2)$, and even, the best approximations for the Rauzy norm.

Let v be a vector and $||\ ||_0$ a norm in $\mathbb{R}^2$. The increasing sequence of positive integers (q_n) is said to be the sequence of *best approximations* of the vector v for the norm $||\ ||_0$ if there exists a sequence of vectors (v_n) such that for each integer n and for every $w \in \mathbb{Z}^2$

$$||q_{n+1}v - v_{n+1}||_0 < ||q_n v - w||_0,$$

and for every $q < q_{n+1}$, $q \neq q_n$, and for every $w \in \mathbb{Z}^2$ then

$$||q_n v - v_n||_0 < ||q v - w||_0.$$

Theorem 10.9.1.

1. *The vector* $(1/\beta, 1/\beta^2)$ *is badly approximable by the rational numbers, that is, there exists* $K > 0$ *such that for every positive integer* N*, then*
$$\sqrt{N}\, |||N \cdot (1/\beta, 1/\beta^2)||| \geq K.$$
2. *For every norm, the sequence* (q_{n+1}/q_n) *is bounded, where* (q_n) *denotes the sequence of best approximations of the vector* $(1/\beta, 1/\beta^2)$.
3. *The Tribonacci sequence* (T_n) *is the sequence of best approximations of the vector* $(1/\beta, 1/\beta^2)$ *for the Rauzy norm.*

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

4. *Furthermore*

$$\lim_{n\to\infty} \sqrt{T_n}\, |||T_n \cdot (1/\beta, 1/\beta^2)||| = \frac{1}{\sqrt{\beta^2+2\beta+3}}.$$

Proof.

1. Let $m \geq 1$ such that $T_{m-1} \leq N < T_m$. Hence the normal T-representation of $N = \sum_{i\geq 0} \varepsilon_i T_i$ satisfies $\varepsilon_{m-1} = 1$. According to Lemma 10.8.13, then $|||N \cdot (1/\beta, 1/\beta^2)||| \geq C(1/\beta)^{m/2}$. There exist two constants C_1, C_2 such that the Tribonacci sequence satisfies: $\forall N \in \mathbb{N},\ C_1\beta^n \leq T_n \leq C_2\beta^n$. Hence

$$|||N \cdot (1/\beta, 1/\beta^2)||| \geq C\sqrt{\frac{C_1}{T_m}} \geq \frac{CC_1}{\sqrt{C_2\beta N}},$$

which ends the proof of the first assertion. Let us observe that such a statement (up to the choice of the positive constant K) also holds for every norm, by equivalence of the norms.

2. Let $||\ ||_0$ be a norm in $\mathbb{R}^2$ and let (q_n) be the sequence of best approximations of $(1/\beta, 1/\beta^2)$ associated with this norm.

   Let n and m be such that $T_m \leq q_n < T_{m+1}$. For all $q < q_{n+1}$, one has by definition $|||q \cdot (1/\beta, 1/\beta^2)|||_0 \geq |||q_n \cdot (1/\beta, 1/\beta^2)|||_0$, where $|||\ |||_0$ denotes the distance to the nearest integer for the norm $|||\ |||_0$. We just have seen (proof of Assertion 1) that $|||q_n \cdot (1/\beta, 1/\beta^2)||| \geq Kq_n^{-1/2}$. Hence

$$|||q_n \cdot (1/\beta, 1/\beta^2)||| > KT_{m+1}^{-1/2}.$$

   On the other hand, one has for l large enough, according to Lemma 10.8.10, that $|||T_{m+1+l} \cdot (1/\beta, 1/\beta^2)||| = ||\delta(T_{m+1+l})||$. Since the norms $||\ ||_0$ and $||\ ||$ are equivalent, then $|||T_{m+1+l} \cdot (1/\beta, 1/\beta^2)|||_0 = ||\delta(T_{m+1+l})||_0$ also holds for l large enough, still following Lemma 10.8.10. By equivalence of the norms, there exists a constant C_3 such that for l large enough

$$\begin{aligned} |||T_{m+1+l} \cdot (1/\beta, 1/\beta^2)|||_0 &= ||\delta(T_{m+1+l})||_0 \leq C_3||\delta(T_{m+1+l})|| \\ &= C_3|\alpha|^{m+l+5} \leq C_3\sqrt{C_2}|\alpha|^{l+4}T_{m+1}^{-1/2}. \end{aligned}$$

   Hence there exists l_0 large enough such that

$$|||T_{m+1+l_0} \cdot (1/\beta, 1/\beta^2)|||_0 < |||q_n \cdot (1/\beta, 1/\beta^2)|||_0,$$

   which implies that $T_{m+1+l_0} \geq q_{n+1}$. Hence one has

$$\frac{q_{n+1}}{q_n} \leq \frac{Tm+1+l_0}{T_m} \leq C_2/C_1\beta^{l_0+1}.$$

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

3. The sequence $(\delta(T_n))_n$ which satisfies $\delta(T_n) = |\alpha|^{n+4}$ is a decreasing sequence. Furthermore, for $n \geq 8$, $||\delta(T_n)|| \leq |\alpha|^{12} < C$, which implies that $|||T_n \cdot (1/\beta, 1/\beta^2)||| = ||\delta(T_n)||$. One checks by considering a finite number of cases that when $n < T_8$, then the properties of good approximation hold for the Tribonacci sequence.

Let us assume from now on that $N \geq T_8$. We want to prove that if $N < T_{n+1}$ and $N \neq T_n$, then for every $v \in \mathbb{Z}^2$

$$||\delta(T_n)|| < ||N \cdot (1/\beta, 1/\beta^2) - v||.$$

Since $||N \cdot (1/\beta, 1/\beta^2) - v|| < C$ implies that $N \cdot (1/\beta, 1/\beta^2) - v = \delta(N)$, it is sufficient to check that $||\delta(T_n)|| < ||\delta(N)||$.

Let $n \in \mathbb{N}$ and let $N < T_{n+1}$, $N \neq T_n$, with normal T-representation $N = \sum_{0 \leq i \leq k} \varepsilon_i T_i$. Let $i_0 = \min\{i \,|\, \varepsilon_i \neq 0\}$ ($i_0 \neq n$ since $N \neq T_n$); hence $N = \sum_{i_0 \leq n} \varepsilon_i T_i$. One has

$$||\delta(N)|| = || \sum_{i_0 \leq i \leq n} \varepsilon_i B^i z|| \geq ||B^{i_0} z + \varepsilon_{i_0+1} B^{i_0+1} z|| - || \sum_{i_0+2 \leq i \leq n} \varepsilon_i B^i z||.$$

Let us prove that $||B^{i_0} z + \varepsilon_{i_0+1} B^{i_0+1} z|| - || \sum_{i_0+2 \leq i \leq n} \varepsilon_i B^i z|| > |\alpha|^{12+i_0}$.

- Assume first that $\varepsilon_{i_0+1} = 0$. Then

$$|| \sum_{i \geq i_0+2}^{n} \varepsilon_i B^i z|| \leq ||B^{i_0+2} \sum_{i \geq 0} \varepsilon_{i_0+2+i} B^i z|| \leq \frac{|\alpha|^{i_0+2} ||z||}{1 - |\alpha|^3} = \frac{|\alpha|^{i_0+6}}{1 - |\alpha|^3}.$$

  Hence $||\delta(N)|| \geq |\alpha|^{i_0+4}((1 - |\alpha|^2 - |\alpha|^3)/(1 - |\alpha^3|)) > 0$.
- Assume now that $\varepsilon_{i_0+1} = 1$, and thus $\varepsilon_{i_0+2} = 0$. One has

$$||\delta(N)|| \geq |\alpha|^{i_0}(||z + Bz|| - \frac{|\alpha|^7}{1 - |\alpha|^3}).$$

  It remains to check that $|\alpha|^4((1 - |\alpha|^2 - |\alpha|^3)/(1 - |\alpha^3|), ||z + Bz|| - |\alpha|^7/(1 - |\alpha|^3) > |\alpha|^{12}$ to conclude.

If $n - i_0 \geq 8$, then $\delta(N) > |\alpha|^{i_0+12} \geq |\alpha|^{n+4} = ||\delta(T_n)||$.

When $n - i_0 \leq 7$, one checks by considering a finite number of cases that $|| \sum_{i=0}^{m} \varepsilon_i B^i z|| > |\alpha|^{m+4}$, for $0 \leq m \leq 7$, which implies

$$\delta(N) = |\alpha|^{i_0} || \sum_{i=0}^{n-i_0} \varepsilon_i B^i z|| > |\alpha|^{i_0} |\alpha|^{n-i_0+4} \geq ||\delta(T_n)||.$$

4. Let K_0 be defined as the smallest real number such that there exist infinitely many integers N satisfying

$$\sqrt{N}\, |||N \cdot (1/\beta, 1/\beta^2)||| \leq K_0.$$

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

From Assertion 1, one deduces that K_0 is finite. In fact, K_0 is the smallest real number such that there exist infinitely many integers N satisfying $\sqrt{T_n}\,||\delta(T_n)|| \leq K_0$, since (T_n) is the sequence of best approximations of $(1/\beta, 1/\beta^2)$. The following limit exists and equals:

$$\lim_{n\to+\infty} \sqrt{T_n}\,||\delta(T_n)|| = \frac{1}{\sqrt{\beta^2+2\beta+3}},$$

hence the result. ∎

Problems

Section 10.4

10.4.1 (gcd). Let $q \geq 2$ be an integer. Prove that for all integers $m, n \geq 1$

$$\gcd(q^m - 1, q^n - 1) = \gcd(m, n).$$

(*Hint*. If $m \geq n$ and $m = \alpha n + \beta$ with $\beta \in [0, n-1]$, prove that an integer divides both $q^m - 1$ and $q^n - 1$ if and only if it divides both $q^m - 1$ and $q^\beta - 1$. Then use the Euclidean algorithm to compute gcds). Deduce that $q^m - 1$ divides $q^n - 1$ if and only if m divides n.

Section 10.5

10.5.1 (Möbius function). Define the Möbius function μ on the integers ≥ 1 by

$$\mu(n) := \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if there exists } k \geq 2 \text{ such that } k^2 \text{ divides } n, \\ (-1)^r & \text{if } n = p_1 p_2 \cdots p_r, \text{ where the } p_i's \text{ are distinct primes.} \end{cases}$$

(a) Prove that, for every $n \geq 1$,

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \geq 2. \end{cases}$$

(*Hint*. Note that, if $n = \prod_{1\leq j\leq r} p_j^{\alpha_j}$ is the decomposition of $n \geq 2$ into primes, then

$$\sum_{d|n} \mu(d) = \sum_{d|p_1\cdots p_r} \mu(d) = \sum_{0\leq j\leq r} \binom{r}{j} (-1)^j = (1-1)^r = 0.)$$

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

(b) Prove the Möbius inversion formula: if f and g are two maps defined on the positive integers, then

$$\forall n \geq 1,\ g(n) = \sum_{d|n} f(d) \Rightarrow \forall n \geq 1,\ f(n) = \sum_{d|n} \mu(d) g(n/d).$$

(c) Prove that, if F and G are two maps defined on the real numbers, then (summing over $n \leq x$ means that the summation is over the integers n such that $n \leq x$)

$$\forall x \geq 0,\ G(x) = \sum_{n \leq x} F(n) \Rightarrow \forall x \geq 0,\ F(x) = \sum_{n \leq x} \mu(n) G(\frac{x}{n}).$$

(d) Define a *square-free* number as an integer that is not divisible by any square of an integer ≥ 2. Prove that for each integer $n \geq 1$ there exists a unique square-free number q and a unique integer a such that $n = a^2 q$.

(e) Let $\lfloor x \rfloor$ be the integral part of the real x. Let $Q(x)$ be the number of square-free numbers smaller than x. Prove that, for each real number $x \geq 0$,

$$Q(x) = \sum_{n \leq \sqrt{x}} \mu(n) \lfloor \frac{x}{n^2} \rfloor.$$

(*Hint*. Start from

$$\lfloor x \rfloor = \sum_{n \leq x} 1 = \sum_{\substack{a^2 q \leq x \\ a \geq 1 \\ q \text{ squarefree}}} 1 = \sum_{a \leq \sqrt{x}} Q(\frac{x}{a^2}).$$

Deduce that

$$\lfloor x^2 \rfloor = \sum_{n \leq x} Q(\frac{x^2}{n^2})$$

and use Part (b) above.)

(f) Prove that the density of the square-free numbers exists and is equal to $\sum_{n \geq 1} \mu(n)/n^2$. (*Hint*. Write

$$\begin{aligned} Q(x) &= \textstyle\sum_{n \leq \sqrt{x}} \mu(n) \lfloor x/n^2 \rfloor = x \sum_{n \leq \sqrt{x}} \mu(n)/n^2 + O(\sqrt{x}) \\ &= x \textstyle\sum_{n \geq 1} \mu(n)/n^2 + O(\sqrt{x}).) \end{aligned}$$

(g) Prove that $\sum_{n \geq 1} \mu(n)/n^2 = 6/\pi^2$. (*Hint*. Write

$$\sum_{m \geq 1} \frac{\mu(m)}{m^2} \sum_{n \geq 1} \frac{1}{n^2} = \sum_{\ell \geq 1} \frac{1}{\ell^2} \sum_{m | \ell} \mu(m)$$

and use that $\sum_{n \geq 1} 1/n^2 = \pi^2/6$.)

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

(h) Let $\psi_k(n)$ denote the number of primitive words of length n on an alphabet of size k. Prove that

$$k^n = \sum_{d|n} \psi_k(d).$$

(*Hint*. Every word w can be written in a unique way as $w = v^d$, where v is a primitive word, and d is an integer ≥ 1. Of course d must divide the length of w.)

Using the inversion formula (b) above deduce that

$$\psi_k(n) = \sum_{d|n} \mu(d) k^{n/d}.$$

10.5.2 (Algebraicity). Prove that, if the formal power series $\sum a_n X^n$ has integral coefficients and is algebraic over the field $\mathbb{Q}(X)$, then the formal power series $\sum (a_n \mod p) X^n$ is algebraic over $\mathbb{F}_p(X)$.

Section 10.7

10.7.1 (Complexity function of the Tribonacci word). First observe that the letters 2 and 3 are only followed or preceded by the letter 1 in the Tribonacci word u. Second, prove that every factor w distinct from the empty word ε of the Tribonacci word u can be uniquely written as follows: $w = r_1 \sigma(v) r_2$, where v is a factor of u, $r_1 \in \{\varepsilon, 2, 3\}$, and $r_2 = 1$ if the last letter of w is 1, and r_2 is the empty word, otherwise. Deduce from this the following combinatorial properties:

(a) Prove that the Tribonacci word u is not ultimately periodic, that is, periodic from some rank on.

(b) A factor w of a word x is said to be *right special* if there exist two distinct letters a and b such that both wa and wb are factors of x. Prove that the Tribonacci word admits exactly one right special factor of each length.

(c) The *complexity function* of an infinite word s is defined as the function $P(s, n)$ which counts the number of distinct factors of length n of s. Deduce that the complexity function $P(u, n)$ of the Tribonacci word satisfies: $\forall n \in \mathbb{N}$, $P(u, n) = 2n + 1$.

(d) Prove that the Tribonacci word is uniformly recurrent, that is, every factor appears infinitely often with bounded gaps.

(e) Use the same method to prove that the Fibonacci word (defined in Section 10.1.4) admits exactly $n + 1$ factors of length n.

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

(f) Prove that the topological entropy (as defined in Section 1.8.3) of the set of factors of the Tribonacci word as well as the topological entropy of the set of factors of the Fibonacci word are equal to 0.

10.7.2 Prove that the Tribonacci word is not an automatic sequence, by considering the probabilities of occurrence of the letters. Deduce from Problem 1.8.1 and Section 1.8.6 the values of the probabilities of occurrence of the factors of length 2 of the Tribonacci word.

10.7.3 (Dumont–Thomas numeration system on words). The aim of this problem is to extend the statement of Lemma 10.7.2 to more general morphisms, following Dumont and Thomas (1989, 1993), and Rauzy (1990).

Let τ be a morphism on the alphabet $\mathcal{A}$ satisfying the assumptions of Proposition 10.1.3. The *prefix automaton* of τ is defined as follows: its edges are the letters of $\mathcal{A}$; there is an edge from a to b labelled by $p \in \mathcal{A}^*$ if $\tau(a) = pas$, where $s \in \mathcal{A}^*$. For instance the prefix automaton of the Fibonacci morphism : $a \to ab$, $b \to a$ is the *Golden mean automaton* as defined in Example 1.3.5, where the label a has to be replaced by 1 and b by 0. Let v be the fixed point of τ having a as first letter, in the sense of Remark 10.1.4. Prove that every finite prefix of v can be uniquely expanded as

$$\tau^n(p_n)\tau^{n-1}(p_{n-1})\cdots p_0,$$

where $p_n \neq \varepsilon$, and $p_n \cdots p_0$ is the sequence of labels of a path in the prefix automaton starting from the letter a. Conversely, prove that any such sequence of labels generates a finite prefix of v.

10.7.4 (Statistics on letters for Pisot morphisms). A morphism $\tau : \mathcal{A}^* \to \mathcal{A}^*$ is said to be of *Pisot type* if first it satisfies the assumptions of Proposition 10.1.3, and second, the eigenvalues of its incidence matrix M_τ satisfy the following: there exists a dominant eigenvalue α such that for every other eigenvalue λ, one gets $\alpha > 1 > |\lambda| > 0$. Deduce from Problem 10.7.3 that the results of Proposition 10.7.4 hold for any fixed point of a Pisot type morphism.

10.7.5 (Uniform balance). An infinite word $v \in \mathcal{A}^\omega$ is said to be *uniformly balanced* if there exists $C > 0$ such that for any two factors w, w' of the same length of v, and for any letter $i \in \mathcal{A}$, then

$$||w|_i - |w'|_i| \leq C.$$

An infinite word $v \in \mathcal{A}^\omega$ is said to have *bounded remainder letters* if first, for every letter i, its probability of occurrence $\pi(i)$ in v

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

exists, and second, there exists C' such that

$$\forall N,\ |\,|v_0v_1\cdots v_{N-1}|_i - \pi(i)N| \le C'.$$

Prove that a sequence is uniformly balanced if and only if it has bounded remainder letters. Deduce from Problem 10.7.4 that a fixed point of a Pisot morphism is uniformly balanced.

For more results on the balance properties of fixed points of morphisms, see Adamczewski (2003).

Section 10.8

10.8.1 (Bounded remainder sets). A measurable set X with respect to the Haar measure $\mu(\,)$ in $\mathbb{T}^2$ is said to be a *bounded remainder set* for the translation R_β if there exists $C > 0$ such that

$$\forall N,\ \ |\,\mathrm{Card}\{i;\ 0 \le i \le N,\ R_\beta^n(0) \in X\} - \mu(X)| \le C.$$

Deduce from Proposition 10.7.4 and Theorem 10.8.16 that the sets $\mathcal{R}_i$, $i = 1, 2, 3$, are bounded remainder sets.

Bounded remainder sets have been widely studied, see for instance Ferenczi (1992).

10.8.2 (Generalized Rauzy fractal and self-similarity). Let τ be a primitive morphism of Pisot type over the alphabet $\{1, \ldots, d\}$. Define similarly to the definition in Section 10.8.1 a generalized Rauzy fractal $\mathcal{R}(\tau)$ as well as its division into the pieces $\mathcal{R}_i(\tau)$, $i = 1, \ldots, d$. Prove that the statement of Proposition 10.8.1 still holds.

Prove that for $i = 1, \ldots, d$,

$$M_\tau^{-1}(\mathcal{R}_i(\tau)) = \cup_{1\le j\le d}\ \cup_{pis,\ \tau(j)=pis}\ (\mathcal{R}_j(\tau) + M_\tau^{-1}(\pi_0 \circ f(p))).$$

(*Hint.* Apply M_τ to this equality.) This equality means that the pieces $\mathcal{R}_i(\tau)$ of the Rauzy fractal are self-similar (and more precisely self-affine), that is they can be inflated under the expanding action of M_τ^{-1}, the image of each piece $\mathcal{R}_i(\tau)$, $i = 1, \ldots, d$ being redivided into translates of the sets $\mathcal{R}_j(\tau)$. This result is a generalization of the statement of Lemma 10.8.7. This self-similarity property is considered for instance in Holton and Zamboni (1998); Arnoux and Ito (2001); Sirvent and Wang (2002).

10.8.3 Deduce from the proof of Proposition 10.8.1 an upper bound on the diameter of the Rauzy fractal $\mathcal{R}$.

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

10.8.4 (β-numeration). Prove that every positive real number can be expanded as (β is the Tribonacci number)

$$x = \sum_{i=-d}^{+\infty} \varepsilon_i \beta^{-i}, \text{ where } d \in \mathbb{Z}, \forall i, \varepsilon_i \in \{0, 1\}, \varepsilon_i \varepsilon_{i+1} \varepsilon_{i+2} = 0, \tag{10.10.1}$$

by introducing the *β-transformation* map $T_\beta : [0, 1[\to [0, 1[, x \mapsto \{\beta x\}$; such an expansion (with the above admissibility conditions (10.10.1)) is called a *β-expansion*; is there unicity of such an expansion? For more details on the β-numeration, see for instance Lothaire (2002).

10.8.5 (F-property). The aim of this problem is to prove that the set $\mathrm{Fin}(\beta)$ of positive real numbers having a finite β-expansion (see Problem 10.8.4) coincides with the set $(\mathbb{Z}[\beta^{-1}])_+$ of positive polynomials in $1/\beta$ with integer coefficients. This property is called the *F-property* and has been introduced in Frougny and Solomyak (1992), see also Akiyama (1999) (β is still the Tribonacci number).

(a) Let $\mathbb{Z}_+[\beta^{-1}]$ denote the set of polynomials in $1/\beta$ with non-negative integer coefficients. Prove that $\mathrm{Fin}(\beta)$ is included in $\mathbb{Z}_+[\beta^{-1}]$. (Use the fact that $1 = \beta^3 + \beta^2 + \beta$.)

(b) The aim of this question is to prove that $\mathbb{Z}_+[\beta^{-1}] = (\mathbb{Z}[\beta^{-1}])_+$. Let $x \in (\mathbb{Z}[\beta^{-1}])_+$. Prove that there exists $s \in \mathbb{N}$ and $(x_0, x_1, x_2) \in \mathbb{Z}^3$ such that

$$x = \frac{1}{\beta^s}(x_0 + x_1\beta^{-1} + x_2\beta^{-2}) = \frac{1}{\beta^{s+1}} < (x_0, x_1, x_2), v_\beta >,$$

(we consider here the Euclidean scalar product in $\mathbb{R}^3$). Deduce that for all $n \in \mathbb{N}$, $x = 1/\beta^{s+n} < {}^t M_\sigma^n (x_0, x_1, x_2), v_\beta >$. Apply the Perron–Frobenius theorem to conclude.

(c) The aim of this question is to prove that $\mathbb{Z}_+[\beta^{-1}] \cap [0, 1]$ is included in $\mathrm{Fin}(\beta)$. For that purpose we introduce an algorithm consisting of the repetition of the action of two steps A_1 and A_2, that transforms a finite β-representation of x (with digits not necessarily satisfying the admissible conditions (10.10.1)) into the β-expansion of x.

Let $x = \sum_{i=1}^{d} x_i \beta^{-i} \in \mathbb{Z}_+[\beta^{-1}] \cap [0, 1]$, where $\forall i$, $x_i \in \mathbb{N}$.

Step A_1. Assume that there exists an integer $k \geq 1$ such that $x_{k+1} \geq 1$, $x_{k+2} \geq 1$, and $x_{k+3} \geq 1$. Let A_1 be the algorithm which maps $(x_i)_{i \geq 1}$ (where we set $x_i = 0$ for $i > d$) to

$$(x_i') = x_1 \cdots (x_k + 1)(x_{k+1} - 1)(x_{k+2} - 1)(x_{k+3} - 1)x_{k+4} \cdots$$

Prove that $\sum_i x_i' < \sum_i x_i$ and that $\sum_i x_i \beta^{-i} = \sum_i x_i' \beta^{-i}$.

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

Step A_2. Assume that there exists an index k such that $x_k \geq 2$. Prove that $k \geq 2$. Let l be the smallest integer such that $x_l \geq 2$. Let A_2 be the algorithm which sends $(x_i)_{i\geq 1}$ to

$$(x'_i) = x_1 \cdots (x_l - 1)(x_{l+1} + 1)(x_{l+2} + 1)(x_{l+3} + 1) \cdots$$

Let $k \geq 1$ be the largest integer such that $k \leq l$ and $x'_{k+1} \geq 1$, $x'_{k+2} \geq 1$, $x'_{k+3} \geq 1$. Then, the algorithm A_2 sends (x'_i) to

$$(x''_i) = x'_1 \cdots (x'_k + 1)(x'_{k+1} - 1)(x'_{k+2} - 1)(x'_{k+3} - 1).$$

The sequence (x''_i) is the image of (x_i) under the action of A_2. Prove that $\sum_i x''_i = \sum_i x_i$ and that $\sum_i x_i \beta^{-i} = \sum_i x''_i \beta^{-i}$.

We now apply repeatedly steps A_1 and A_2 to x, defining a sequence $(x^{(j)})$ such that for all j, $x^{(j)}$ takes finitely but all zero values. If for some value j_0, $x^{(j_0)}$ satisfies the admissibility conditions (10.10.1), then we set $x^{(j)} = x^{(j_0)}$, for $j \geq j_0$, and we no longer apply a step. Prove that for j large enough, step A_1 can no longer be performed.

Let us assume that A_2 can be applied indefinitely. Let J be such that for $j > J$, step A_1 can no longer be performed. Let l_j denote, for $j > J$, the smallest index l such that $x_l^{(j)} \geq 2$. Prove that (l_j) tends to infinity and that the sequence $(x^{(j)})$ is convergent. Find a contradiction.

(d) Conclude.

We have followed here the proof of Frougny and Solomyak (1992).

10.8.6 (A tiling of the line). We have seen in Section 10.8.6, that $\pi_1(\{f(u_0 \cdots u_{N-1}; N \in \mathbb{N}\}))$ is a Meyer set. We associate here in a natural way a tiling of the line with this set of points.

Prove that $\pi_1(\{f(u_0 \cdots u_{N-1}; N \in \mathbb{N}\}))$ defines a tiling $\mathcal{T}$ of the half-line generated by v_β in the positive octant $\{(x, y, z);\ x, y, z > 0\}$ by segments of three distinct lengths, say l_1, l_2, l_3. In other words, prove that the distance between two successive points of $\pi_1(\{f(u_0 \cdots u_{N-1};\ N \in \mathbb{N}\}))$ (with respect to the orientation on the half-line provided by v_β) equals either l_1, l_2, or l_3.

Prove that under a suitable choice of a unit vector on the half-line, then $\pi_1(\{f(u_0 \cdots u_{N-1};\ N \in \mathbb{N}\}))$ is in one-to-one correspondence with the set of *β-integers*

$$\mathbb{Z}_\beta^+ = \{\sum_{i=0}^{d} \varepsilon_i \beta^i;\ d \in \mathbb{N},\ \forall i,\ \varepsilon_i \in \{0, 1\},\ \varepsilon_i \varepsilon_{i+1} \varepsilon_{i+2} = 0\}.$$

Let $(t_n)_{n\geq 0}$ denote the set of elements of $\pi_1(\{f(u_0 \cdots u_{N-1};\ N \in \mathbb{N}\}))$ ordered in increasing order (still with respect to the orientation

https://doi.org/10.1017/CBO9781107341005.011 Published online by Cambridge University Press

on the half-line provided by v_β). One can code the tiling $\mathcal{T}$ as follows: for $n \geq 0$, for $i = 1, 2, 3$, then $v_n = i$ if and only if $t_{n+1} - t_n = l_i$. Prove that $(v_n)_{n\geq 0}$ is equal to the Tribonacci word.

Notes

For general references on substitutive sequences and substitutive dynamical systems, see for instance Queffélec (1987) and Fogg (2002).

The examples in Section 10.1.4 are famous. For more on Sturmian words, one can read for example Lothaire (2002) and Fogg (2002). For more on the Thue–Morse word, its history, and its many occurrences in the literature, see for example Allouche and Shallit (1999). The Rudin–Shapiro word was first introduced in Shapiro (1952). For all these words and for the paperfolding word one can read the notes of Allouche and Shallit (2003).

In Section 10.2.5, Lemma 10.2.13 is a classical result in Perron–Frobenius theory (see for example Gantmacher 1959). The main theorem of Section 10.2.5 (Proposition 10.2.15) is due to Cobham (1972).

The main theorem of Section 10.3.3 (Theorem 10.3.4) was proved in Christol (1979), see also Christol, Kamae, Mendès France, and Rauzy (1980). More generally, it is also possible to give a simple combinatorial characterization of primitive substitutive sequences (see Durand 1998; Holton and Zamboni 1999).

The first proof of Theorem 10.4.2 in Section 10.4 is due to Wade (1941). The proof we give here is adapted from a proof given in Allouche (1990).

The proof of Proposition 10.5.1 that we give in Section 10.5 comes from Allouche (1997). The first proof was given in Petersen (1994, 1996). For a proof of the theorem of Chomsky–Schützenberger, see Chomsky and Schützenberger (1963).

The theorem of Ridout given without proof in Section 10.6 was given in Ridout (1957). Corollary 10.6.2 is due to Ferenczi and Mauduit (1997). Theorem 10.6.3 is also due to Ferenczi and Mauduit (1997) under a more general form. A slightly more precise result in the case of binary alphabets is given in Allouche and Zamboni (1998). For more results on the transcendence of "automatic" real numbers, see for example Allouche and Shallit (2003).

We do not here claim exhaustivity in our choice of applications of the Rauzy fractal in number theory. We have chosen the more representative properties which also motivated G. Rauzy in a study of the Tribonacci word in Rauzy (1982). All the results of Section 10.8 follow carefully the approach of the seminal paper Rauzy (1982), from which come the proofs of Theorem 10.8.16, Lemmas 10.8.10, 10.8.12 and 10.8.13, as well as

the introduction of the matrix B, whereas the proof of Theorem 10.9.1 is due to Chekhova, Hubert, and Messaoudi (2001). The fact that the vector $(1/\beta, 1/\beta^2)$ is badly approximable by the rationals (Assertion 1 of Theorem 10.9.1) is a classical statement for elements of a totally real field number (see for instance Cassels 1957).

Arnoux–Rauzy words. The Tribonacci translation first occurred in Arnoux (1988), where the Tribonacci morphism was used to model an interval exchange map of 6 intervals and to build explicitly a continuous and surjective conjugacy between this interval exchange map and the Rauzy translation (see also Arnoux and Yoccoz 1981); these results have led to the introduction of the family of *Arnoux–Rauzy words* in Arnoux and Rauzy (1991), to which the Tribonacci word belongs, as a generalization of the family of Sturmian words.

Arnoux–Rauzy words are defined as the one-sided words x with complexity $P(x, n) = 2n + 1$ for all n which are recurrent and which have for every length a unique right special factor and a unique left special factor, each of these special factors being extendable in three different ways. Let us note that they can be similarly defined over any alphabet of larger size, say d; one thus obtains infinite words of complexity $(d - 1)n + 1$. Contrary to the Sturmian case, these words are no longer characterized by their complexity function. For instance, codings of nondegenerated three-interval exchanges also have complexity $2n + 1$. Let us observe that Arnoux–Rauzy words can be described as exchanges of six intervals of the unit circle (Arnoux and Rauzy 1991).

The combinatorial properties of the Arnoux–Rauzy words are well-understood and are perfectly described by a two-dimensional continued fraction algorithm defined over a subset of zero measure of the simplex introduced in Arnoux and Rauzy (1991); Risley and Zamboni (2000); Zamboni (1998) and in Chekhova (2000). By using this algorithm, one can express in an explicit way the probabilities of occurrence of factors of given length (Wozny and Zamboni 2001), one can count the number of all the factors of the Arnoux–Rauzy words (Mignosi and Zamboni 2002), or prove that the associated dynamical system has always simple spectrum (Chekhova 2000). See also Castelli, Mignosi, and Restivo (1999), and Justin (2000) for the connections with a generalization of Fine and Wilf's theorem for three periods. The family of Arnoux–Rauzy words has been itself extended to the family of episturmian words (Justin and Pirillo 2002a, 2002b).

Rauzy fractal. The study of the topological properties of the Rauzy fractal is mainly due to Rauzy (1982, 1988), where the Rauzy fractal $\mathcal{R}$ is shown to be connected with a simply connected interior (and so do the three pieces of the Rauzy fractal $\mathcal{R}_i$, $i = 1, 2, 3$). See also Messaoudi (1998) and Messaoudi

(2000a) for a parameterization of its boundary, the points which have several expansions being studied in details (see also Remark 10.8.9). For a study of its fractal boundary, see Ito and Kimura (1991), where it is proved to be a Jordan curve generated by Dekking's fractal generation method (Dekking 1982), from which a computation of its Hausdorff dimension is deduced.

Theorem 10.8.16 states that the translation $v \mapsto v + (1/\beta, 1/\beta^2)$ on $\mathbb{T}^2$ can be coded using the Tribonacci morphism. In dynamical terms, this theorem extends to the fact that the symbolic dynamical system generated by the Tribonacci word is measure-theoretically isomorphic to a translation of the torus $\mathbb{T}^2$, the isomorphism being a continuous onto map. Furthermore it is also possible to construct a Markov partition for the toral automorphism of $\mathbb{T}^3$ of a matrix given by the incidence matrix of the Tribonacci morphism, this construction being based on the Rauzy fractal.

More generally, it is possible to associate a generalized Rauzy fractal to any Pisot unimodular morphism (see Problem 10.8.2). (A morphism is said to be *unimodular* if the determinant of its incidence matrix equals ± 1.) There are several definitions associated with several methods of construction for such Rauzy fractals. We have given here a definition based on formal power series inspired by the seminal paper Rauzy (1982), by Messaoudi (1998, 2000a), and by Canterini and Siegel (2001a, 2001b). A different approach via iterated function systems and generalized substitutions has been developed following ideas from Ito and Kimura (1991); Arnoux and Ito (2001); Sano, Arnoux, and Ito (2001). Indeed, Rauzy fractals can be described as the attractor of some graph iterated function system (IFS), as in Holton and Zamboni (1998) where one can find a study of the Hausdorff dimension of various sets related to Rauzy fractals, and as in Sirvent (2000a, 2000b); Sirvent and Wang (2002) with special focus on the self-similar properties of Rauzy fractals (see Lemma 10.8.7 and Problem 10.8.2). For more details on both approaches, see Chapters 7 and 8 of Fogg (2002). Both methods apply to unimodular morphisms of a Pisot type.

More generally, for any unimodular morphism of a Pisot type the measure-theoretical isomorphism with a translation on the torus (or equivalently the existence of a periodic tiling of the plane by the Rauzy fractal) is conjectured to hold. A large literature is devoted to this question, which is surveyed in Pytheas Fogg 2002, Chapter 7). Inspired by Bedford (1986), Ito and Ohtsuki (1993) extends Rauzy's approach in order to produce Markov partitions for toral automorphisms produced by the modified Jacobi–Perron algorithm. See also Praggastis (1999).

In particular, Arnoux–Rauzy words which are fixed points of primitive morphisms (which are thus unimodular and of Pisot type following Arnoux and Ito 2001) also generate symbolic dynamical systems which are measure-theoretically isomorphic to toral translations. It was believed

that all Arnoux–Rauzy words originated from toral translations, and more precisely, that they were natural codings of translations over $\mathbb{T}^2$. This conjecture was disproved in Cassaigne, Ferenczi, and Zamboni (2000).

Tribonacci numeration system. The Tribonacci numeration system is the canonical numeration system associated with the positive root β of $X^3 = X^2 + X + 1$. More generally, for a given $\beta > 1$, one can expand real numbers in $[0, 1]$ as powers of the number β using the greedy algorithm: $x = \sum_{k=1}^{\infty} b_k \beta^{-k}$, with some conditions on the nonnegative integers b_k (see also Problem 10.8.4); such expansions are called *β-expansions* and are generated by the *β-transformation* $x \mapsto \beta x - [\beta x]$ which also generates as a dynamical system the β-shift (for more details, see for instance Lothaire 2002). One can also represent natural integers in a base given by an infinite sequence of integers (which generalizes Lemma 10.7.1) canonically associated with the β-numeration: the set of factors of greedy representations of natural integers in this base and the factors of the β-shift are the same. Similar compact sets with fractal boundary are considered as geometrical representations of the β-shift when β is a Pisot unit, in Thurston (1989), in Akiyama (1999) and in Praggastis (1999), where topological or tiling properties such as Proposition 10.8.12 or Lemma 10.8.14 are studied in connection with the so-called F-property (Frougny and Solomyak 1992) (see also Problem 10.8.5). Generalized Rauzy fractals issued from the β-numeration are also closely related to canonical number systems (see for instance Akiyama and Pethö (2002)).

There are also some close connections between the dynamical properties of the Rauzy fractal and the extension of the Fibonacci multiplication (introduced in Knuth (1988)) to the Tribonacci recurrence relation, as studied for instance in Arnoux (1989) and Messaoudi (2000b, 2002).

Rauzy fractals can be used to characterize the numbers that have a purely periodic β-expansion, producing a kind of generalized Galois' theorem on classical continuous fractions. It is known following Schmidt (1980) and Bertrand (1977) that elements of $\mathbb{Q}(\beta)$ have an ultimately periodic expansion when β is a Pisot number. A characterization of those points having an immediately periodic expansion is given in Sano (2002), see also Ito and Sano (2001), by introducing a realization of the natural extension of the β-transformation acting on the associated generalized Rauzy fractal for β being a Pisot unit which is a simple β-number. See also Ito (2000) (and more generally Gambaudo *et al*. 2000) for closely related results for elements of cubic fields. Let us observe furthermore that the results of Section 10.9 can be extended following the same ideas to other cubic numbers (Ito 1996; Ito, Fujii, Higashino, and Yasutomi 2003). Such results can also be proved using algebraic geometry following Adams (1969).

Rauzy tilings have also been studied in theoretical physics and quasicrystal theory in Vidal and Mosseri (2000, 2001) as outlined in Section 10.8.6, where we have followed the terminology of Moody (1997). For more on mathematical quasicrystals, see for instance Baake and Moody (2000). See also Burdík *et al.* (1998, 2000); Verger Gaugry and Gazeau (2004) for connected results in the framework of beta-numeration.