2. Codings of rotations

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **44 (1998)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

2. Codings of rotations

The aim of this section is to introduce some definitions concerning sequences defined as codings of irrational rotations on the unit circle, and more precisely measure-theoretic and topological properties of sequences with values in a finite alphabet. For $p \geq 2$, let $F = \{\beta_0 < \beta_1 < \cdots < \beta_{p-1}\}$ be a set of p consecutive points of the unit circle (identified in all that follows with $[0,1[$ or with the unidimensional torus $\mathbf{R}/\mathbf{Z}$) and let $\beta_p = \beta_0$. Let α be an irrational number in $]0,1[$ and let us consider the *positive orbit* of a point x of the unit circle under the rotation by angle α, i.e., the set of points $\{\{\alpha n + x\},\ n \in \mathbf{N}\}$. We denote by $\mathbf{N}$ the set of non-negative integers. The *coding* of the orbit of x under the rotation by angle α with respect to the partition $\{[\beta_0, \beta_1[,\ [\beta_1, \beta_2[, \ldots,\ [\beta_{p-1}, \beta_p[\}$ is the sequence $(u_n)_{n \in \mathbf{N}}$ defined on the finite alphabet $\Sigma = \{0, \ldots, p-1\}$ as follows:

$$u_n = k \Longleftrightarrow \{x + n\alpha\} \in [\beta_k, \beta_{k+1}[, \quad \text{for } 0 \leq k \leq p-1 .$$

A coding of the rotation R means the coding of the orbit of a point x of the unit circle under the rotation R with respect to a finite partition of the unit circle consisting of left-closed and right-open intervals.

For instance, consider the case $F = \{0, 1-\alpha\}$, i.e.,

$$\mathcal{P} = \{[0, 1-\alpha[,\ [1-\alpha, 1[\} ,$$

where α is an irrational number in $]0,1[$. We could also choose to code the orbit of the rotation with respect to the following partition:

$$\mathcal{P}' = \{]0, 1-\alpha],\ ]1-\alpha, 1]\} .$$

As α is irrational, the two sequences obtained by coding with respect to $\mathcal{P}$ or to $\mathcal{P}'$ are ultimately equal. Such sequences are called *Sturmian sequences* (such a coding is called a *Sturmian coding*). Sturmian sequences have received considerable attention in the literature. We refer the reader to the impressive bibliography of [9]. A recent account on the subject can also be found in [6]. The most famous Sturmian sequence is the Fibonacci sequence ($\alpha = \tau - 1$, $x = \alpha$, where $\tau = (\sqrt{5}+1)/2$ denotes the *golden ratio*); this sequence is the fixed point of the following substitution

$$\sigma(1) = 10, \quad \sigma(0) = 1 .$$

Let us recall that a *substitution* defined on the finite alphabet $\mathcal{A}$ is a map from $\mathcal{A}$ to the set of words defined on $\mathcal{A}$, denoted by $\mathcal{A}^\star$, extended to $\mathcal{A}^\star$ by concatenation or, in other words, a homomorphism of the free monoid $\mathcal{A}^\star$.

The results stated for codings of rotations with respect to left-closed and right-open intervals are obviously true for left-open and right-closed partitions.

2.1 Complexity and frequencies of codings of rotations

A *factor of the infinite sequence* u is a finite block w of consecutive letters of u, say $w = u_{n+1} \cdots u_{n+d}$; d is called the *length* of w, denoted by $|w|$. Let $p(n)$ denote the *complexity function* of the sequence u with values in a finite alphabet: it counts the number of distinct factors of given length of the sequence u. For more information on the subject, we refer the reader to the survey [2].

With the above notation, consider a coding u of the orbit of a point x under the rotation by angle α with respect to the partition $\{[\beta_0, \beta_1[, [\beta_1, \beta_2[, \ldots, [\beta_{p-1}, \beta_p[\}$. Let $I_k = [\beta_k, \beta_{k+1}[$ and let R denote the rotation by angle α. A finite word $w_1 \cdots w_n$ defined on the alphabet $\Sigma = \{0, 1, \ldots, p-1\}$ is a factor of the sequence u if and only if there exists an integer k such that

$$\{x + k\alpha\} \in I(w_1, \ldots, w_n) = \bigcap_{j=0}^{n-1} R^{-j}(I_{w_{j+1}}) .$$

As α is irrational, the sequence $(\{x+n\alpha\})_{n\in\mathbf{N}}$ is dense in the unit circle, which implies that $w_1 w_2 \cdots w_n$ is a factor of u if and only if $I(w_1, \ldots, w_n) \neq \varnothing$. In particular, the set of factors of a coding does not depend on the initial point x of this coding. Furthermore, the connected components of these sets are bounded by the points

$$\{k(1-\alpha) + \beta_i\}, \text{ for } 0 \leq k \leq n-1,\ 0 \leq i \leq p-1 .$$

Let us recall that the *frequency* $f(B)$ of a factor B of a sequence is the limit, if it exists, of the number of occurrences of this block in the first k terms of the sequence divided by k. Thus the frequency of the factor $w_1 \cdots w_n$ exists and is equal to the density of the set

$$\big\{k \;\big|\; \{x + k\alpha\} \in I(w_1, \ldots, w_n)\big\},$$

which is equal to the length of $I(w_1, \ldots, w_n)$, by uniform distribution of the sequence $(\{x + n\alpha\})_{n\in\mathbf{N}}$. These sets consist of finite unions of intervals. More precisely, if for every k, $\beta_{k+1} - \beta_k \leq \sup(\alpha, 1-\alpha)$, then these sets are connected; if there exists K such that $\beta_{K+1} - \beta_K > \sup(\alpha, 1-\alpha)$, then the sets are connected except for $w_1 \cdots w_n$ of the form a_K^n (see [1]) (the notation a_K^n denotes the word of length n obtained by successive concatenations of the letter a_K). Let us note that there exists at most one integer K satisfying $\beta_{K+1} - \beta_K > \sup(\alpha, 1-\alpha)$. We thus have the following lemma, which links the three distance theorem and related results to the frequencies of codings of rotations.

LEMMA 1. *Let u be a coding of a rotation by irrational angle α on the unit circle with respect to the partition*

$$\{[\beta_0, \beta_1[, [\beta_1, \beta_2[, \ldots, [\beta_{p-1}, \beta_p[\} ,$$

such that the lengths of the intervals of the partition are less than or equal to $\sup(\alpha, 1-\alpha)$. *Then the frequencies of factors of length n of the sequence u are equal to the lengths of the intervals bounded by the points*

$$\{k(1-\alpha)+\beta_i\} , \textit{ for } 0 \leq k \leq n-1, \ 0 \leq i \leq p-1 .$$

In particular, if the partition is equal to $\{[0, 1-\alpha[, [1-\alpha, 1[\}$, i.e., if u is a Sturmian sequence, the intervals $I(w_1, \ldots, w_n)$ are exactly the $(n+1)$ intervals bounded by the points

$$0, \{(1-\alpha)\}, \ldots, \{(n(1-\alpha)\} .$$

Therefore there are exactly $n+1$ factors of length n and the complexity of a Sturmian sequence satisfies $p(n) = n+1$, for every n. Furthermore, the lengths of these intervals are equal to the frequencies of factors of length n.

In fact, this complexity function characterizes Sturmian sequences. Indeed, any sequence of complexity $p(n) = n+1$, for every n, is a Sturmian sequence, i.e., there exists α irrational in $]0, 1[$ and x such that this sequence is the coding of the orbit of x under the rotation by angle α with respect either to the partition $\{[0, 1-\alpha[, [1-\alpha, 1[\}$ or $\{]0, 1-\alpha],]1-\alpha, 1]\}$ (see [40]) (the coding of the orbit of α is called the *characteristic sequence* of α). Note that a sequence whose complexity satisfies $p(n) \leq n$, for some n, is ultimately periodic (see [19] and [39]). Sturmian sequences thus have the minimal complexity among sequences not ultimately periodic. Sturmian sequences are also characterized by the following properties.

- Sturmian sequences are exactly the non-ultimately periodic balanced sequences over a two-letter alphabet. A sequence is balanced if the difference between the number of occurrences of a letter in any two factors of the same length is bounded by one in absolute value.

- Sturmian sequences are codings of trajectories of irrational initial slope in a square billiard obtained by coding horizontal sides by the letter 0 and vertical sides by the letter 1.

In the general case of a coding of an irrational rotation, the complexity has the form $p(n) = an + b$, for n large enough (see Theorem 10 below and [1], for the whole proof). The converse is not true: every sequence of ultimately affine complexity is not necessarily obtained as a coding of rotation. Didier gives in [23] a characterization of codings of rotations. See also [46], where Rote studies the case of sequences of complexity $p(n) = 2n$, for every n. However, if the complexity of a sequence u has the form $p(n) = n + k$, for n large enough, then u is the image of a Sturmian sequence by a morphism, up to a prefix of finite length (see for instance [22] or [1]).

2.2 THE GRAPH OF WORDS

The aim of this section is to introduce the Rauzy graph of words of a sequence, in order to obtain results concerning the frequencies of factors of this sequence. This follows an idea of Dekking, who expressed the block frequencies for the Fibonacci sequence by using the graph of words (see [20] and also [8]). Note that Boshernitzan also introduces in [8] a graph for interval exchange maps (homeomorphic to the Rauzy graph of words) in order to prove Theorem 3, which can be seen as a result on frequencies.

Let us note that precise knowledge of the frequencies of a sequence with values in a finite alphabet $\mathcal{A}$ allows a precise description of the measure associated with the dynamical system $(\overline{\mathcal{O}(u)}, T)$: here T denotes the one-sided shift which associates to a sequence $(u_n)_{n\in\mathbf{N}}$ the sequence $(u_{n+1})_{n\in\mathbf{N}}$ and $\overline{\mathcal{O}(u)}$ is the orbit closure under the shift T of the sequence u in $\mathcal{A}^{\mathbf{N}}$, equipped with the product of the discrete topologies (it is easily seen that $\overline{\mathcal{O}(u)}$ is the set of sequences of factors belonging to the set of factors of u). Indeed, we define a probability measure μ on the Borel sets of $\overline{\mathcal{O}(u)}$ as follows: the measure μ is the unique T-invariant measure defined by assigning to each cylinder $[w]$ corresponding to the sequences of $\overline{\mathcal{O}(u)}$ of prefix w, the frequency of w, for any finite block w with letters from $\mathcal{A}$. Let us note that a dynamical system obtained via a coding of irrational rotation is *uniquely ergodic*, i.e., there exists a unique T-invariant probability measure on this dynamical system, which is thus determined by the block frequencies.

The Rauzy graph Γ_n of words of length n of a sequence with values in a finite alphabet is an oriented graph (see, for instance, [41]), which is a subgraph of the de Bruijn graph of words. Its vertices are the factors of length n of the sequence and the edges are defined as follows: there is an edge from U to V if V follows U in the sequence, i.e., more precisely, if there exists a word W and two letters x and y such that $U = xW$, $V = Wy$ and xWy is a factor of the sequence (such an edge is labelled by xWy). Thus there are $p(n+1)$ edges and $p(n)$ vertices, where $p(n)$ denotes the complexity function. A sequence is said to be *recurrent* if every factor appears at least twice, or equivalently if every factor appears an infinite number of times in this sequence. For instance, codings of rotations are recurrent. Note that the Rauzy graphs of words of a sequence are always connected; furthermore, they are strongly connected if and only if this sequence is recurrent.

If B is a factor, then a letter x such that Bx (respectively, xB) is also a factor is called *right extension* (respectively, *left extension*). Let U be a vertex of the graph. Denote by U^+ the number of edges of Γ_n with origin U and U^- the number of edges of Γ_n with end vertex U. In other words, U^+ (respectively, U^-) counts the number of right (respectively, left) extensions of U. Note that

$$p(n+1) - p(n) = \sum_{U \in V(\Gamma_n)} (U^+ - 1) = \sum_{U \in V(\Gamma_n)} (U^- - 1),$$

where $V(\Gamma_n)$ is the vertex set of Γ_n.

In this section we restrict ourselves to sequences with values in a finite alphabet, for which the frequencies exist. Note that the function which associates to an edge labelled by xWy the frequency of the factor xWy is a *flow*. Indeed, it satisfies Kirchhoff's current law: the total current flowing into each vertex is equal to the total current leaving the vertex. This common value is equal to the frequency of the word corresponding to this vertex. Let us see how to deduce, from the topology of a graph of words, information on the number of frequencies for factors of given length. We will use the following obvious result.

LEMMA 2. *Let U and V be two vertices joined by an edge such that $U^+ = 1$ and $V^- = 1$. Then the two factors U and V have the same frequency.*

A *branch* of the graph Γ_n is a maximal directed path of consecutive vertices $(U_1, \ldots, U_m)$ (possibly $m = 1$), satisfying

$$U_i^+ = 1, \text{ for } i < m, \quad U_i^- = 1, \text{ for } i > 1\,.$$

Therefore, the vertices of a branch have the same frequency and the number of frequencies of factors of given length is bounded by the number of branches of the corresponding graph, as expressed below (for a proof of this result due to Boshernitzan, see [8]).

THEOREM 6. *For a recurrent sequence of complexity function $(p(n))$, the frequencies of factors of given length, say n, take at most $3(p(n+1) - p(n))$ values.*

REMARK. In fact, one can prove the following: the frequencies of factors of length n take at most $p(n+1)-p(n)+r_n+l_n$ values, where r_n (respectively, l_n) denotes the number of factors having more than one right (respectively, left) extension.

We deduce from this theorem that if $p(n+1)-p(n)$ is uniformly bounded with n, the frequencies of factors of given length take a finite number of values. Indeed, using a theorem of Cassaigne quoted below (see [10]), we can easily state the following corollary.

THEOREM 7. *If the complexity $p(n)$ of a sequence with values in a finite alphabet is sub-affine then $p(n+1)-p(n)$ is bounded.*

COROLLARY 1. *If a sequence over a finite alphabet has a sub-affine complexity, then the frequencies of its factors of given length take a finite number of values.*

Examples of sequences with sub-affine complexity function include the fixed point of a uniform substitution (i.e., of a substitution such that the images of the letters have the same length), the coding of a rotation or the coding of the orbit of a point under an interval exchange map with respect to the intervals of the interval exchange map.

2.3 FREQUENCIES OF FACTORS OF STURMIAN SEQUENCES

In particular, in the Sturmian case ($p(n) = n+1$, for every integer n), Theorem 6 implies the following result (see [3]).

THEOREM 8. *The frequencies of factors of given length of a Sturmian sequence take at most three values.*

Consider a Sturmian sequence of angle α. We have seen in Section 2.1 that the frequency of a factor $w_1 \cdots w_n$ of u is equal to the length of the interval

$$I(w_1, \ldots, w_n) = \bigcap_{j=0}^{n-1} R^{-j}(I_{w_{j+1}}),$$

and that these sets $I(w_1, \ldots, w_n)$ are exactly the intervals bounded by the points

$$0, \{1-\alpha\}, \ldots, \{n(1-\alpha)\}.$$

We deduce from Theorem 8 that the lengths of the intervals $I(w_1, \ldots, w_n)$, and thus the lengths of the intervals obtained by placing the points $0, \{1-\alpha\}, \ldots, \{n(1-\alpha)\}$ on the unit circle, take at most three values. Hence Theorem 8 is equivalent to the three distance theorem and provides a combinatorial proof of this result.

REMARK. In fact this point of view, and more precisely the study of the evolution of the graphs of words with respect to the length n of the factors, allows us to give a proof of the most complete version of the three distance theorem as given in [53] (for more details, the reader is referred to [3]).

3. THE THREE DISTANCE THEOREM

The three distance theorem was initially conjectured by Steinhaus, first proved by V. T. Sós (see [53] and also [52]), and then by Świerczkowski [56], Surányi [55], Slater [51], Halton [31]. More recent proofs have also been given by van Ravenstein [44] and Langevin [35]. A survey of the different approaches used by these authors is to be found in [44, 51, 35]. In the literature this theorem is called *the Steinhaus theorem, the three length, three gap* or *the three step theorem*. In order to avoid any ambiguity, we will always call it the three distance theorem, reserving the name *three gap* for the theorem introduced in the next section.

THREE DISTANCE THEOREM. *Let $0 < \alpha < 1$ be an irrational number and n a positive integer. The points $\{i\alpha\}$, for $0 \leq i \leq n$, partition the unit circle into $n+1$ intervals, the lengths of which take at most three values, one being the sum of the other two.*

More precisely, let $\left(\frac{p_k}{q_k}\right)_{k \in \mathbf{N}}$ and $(c_k)_{k \in \mathbf{N}}$ be the sequences of convergents and partial quotients associated to α in its continued fraction expansion (if $\alpha = [0, c_1, c_2, \ldots]$, then $\frac{p_n}{q_n} = [0, c_1, \ldots, c_n]$). Let $\eta_k = (-1)^k (q_k \alpha - p_k)$. Let n be a positive integer. There exists a unique expression for n of the form

$$n = mq_k + q_{k-1} + r,$$

with $1 \leq m \leq c_{k+1}$ and $0 \leq r < q_k$. Then the circle is divided by the points $0, \{\alpha\}, \{2\alpha\}, \ldots, \{n\alpha\}$ into $n+1$ intervals which satisfy: