Two groups associated with quadratic Pisot units

Christiane Frougny* & Jacques Sakarovitch†

Corresponding author: Christiane Frougny,
LIAFA - Case 7014, 2 place Jussieu, 75251 Paris Cedex 05 - France.
Mail : Christiane.Frougny@liafa.jussieu.fr

AMS Mathematics Subject Classification: 11A63, 11A67, 11B39, 20F05, 68Q42

*Université Paris 8 and Laboratoire Informatique Algorithmique: Fondements et Applications, C. N. R. S. UMR 7089 and Université Paris 7

†Laboratoire Traitement et Communication de l'Information (C. N. R. S. URA 820), E. N. S. T., Paris.

Abstract

In a previous work, we have investigated an automata-theoretic property of numeration systems associated with quadratic Pisot units that yields, for every such number θ, a certain group G_θ.

In this paper, we characterize a cross-section of a congruence γ_θ of $\mathbb{Z}^4$ that had arisen when constructing G_θ. This allows us to completely describe the quotient H_θ of $\mathbb{Z}^4$ by γ_θ, that becomes then a second group associated with θ. Moreover, the cross-section thus described is very similar to the symbolic dynamical system associated, by a theorem of Parry, with the two numeration systems attached to θ.

The proof is combinatorial, and based upon rewriting techniques.

Résumé

Dans un article précédent, nous avions associé à chaque nombre de Pisot quadratique unitaire θ un certain groupe G_θ par le biais de la construction d'un automate qui réalise le passage entre les représentations des entiers dans deux systèmes de numération naturellement attachés à θ.

Dans cet article, nous donnons une caractérisation d'un ensemble de représentants pour une congruence γ_θ de $\mathbb{Z}^4$ qui avait été utilisée pour la définition de G_θ. Cette caractérisation permet la description complète du quotient H_θ de $\mathbb{Z}^4$ par γ_θ, autre groupe associé à θ. Elle est d'autre part remarquablement similaire à la description, donnée par un théorème de Parry, du système dynamique symbolique associé aux deux systèmes de numération attachés à θ.

La preuve est combinatoire et utilise les techniques des systèmes de réécriture.

Dedicated to the memory of David Klarner

We describe here two commutative finite groups that are associated with quadratic Pisot units, *via* numeration systems.

It is straightforward to associate numeration systems to Pisot numbers and recent publications have shown spectacular appearance of these systems in several questions, putting an emphasis on quadratic Pisot units. For instance, Pisot numbers are involved in the mathematical description of quasicrystals (see [3]); and every quasicrystal observed so far in the real world is indeed defined by a Pisot number that is quadratic and a unit. As another example, these numeration systems are also present in the realization of arithmetic codings of hyperbolic automorphisms of the torus (see [13]). Along the same line, in [14], a group whose order is equal to the discriminant of θ is associated with any Pisot unit θ. In the quadratic case this group is sitting between the two groups we describe here (with the three groups collapsing into one only in the special case of the golden mean).

There are indeed *two* numeration systems associated with every Pisot number. In a previous work of ours, we showed that, in the case of a *quadratic Pisot unit*, there exists a finite two-tape automaton that translates the representation of integers in one system into the representation of the same integer in the other system ([6]). The first of the two groups quoted above is the transition monoid of that automaton. In the course of the construction, a certain congruence γ_θ of $\mathbb{Z}^4$ has naturally arisen.

In the present paper, we characterize a cross-section of γ_θ from which we are able to describe the second group, namely the quotient of $\mathbb{Z}^4$ by γ_θ. A feature of the cross-section, which makes its characterization particularly appealing to us, is a great similarity with a theorem of Parry describing symbolic dynamical systems associated with the same Pisot number.

*

In the first section, we recall some definitions that will serve as a framework for the definition of the congruence γ_θ. The description of the cross-section for γ_θ is given in Section 2 (Theorem 1), together with the structure of the group that can be then computed. The proof of Theorem 1 follows then, which is combinatorial, and based upon rewriting techniques.

A preliminary version of this paper has been presented in [7].

1 Two numeration systems and two groups

As in [6], let us start with the simplest, as well as the most popular, example: the *two numeration systems* associated with *the golden mean*, *i.e.,* the larger zero φ of the polynomial

$$P_\varphi(X) = X^2 - X - 1 \ .$$

We have first the *Fibonacci numeration system.* The sequence of Fibonacci numbers, $F = (F_n)_{n\geq 0}$, is a linear recurrent sequence whose characteristic polynomial is $P_\varphi(X)$. It is well-known[1] that every positive integer is represented, in several different ways, as a sum of Fibonacci numbers, and that — with the convention that $F_0 = 1$ and $F_1 = 2$ — every integer has a unique representation, called its *Fibonacci representation*, with the property that no two consecutive Fibonacci numbers occur. For instance, $15 = F_5 + F_1$; thus the Fibonacci representation of 15 is $(100010)_F$.

The other numeration system associated with the golden mean φ consists in taking φ as a *base*: it is known that every positive real number, and thus every integer, is represented, in several different ways, as a sum of powers of φ, and that every positive real number, and thus every integer, has a unique representation, called its *φ-expansion*, with the property that no two consecutive powers of φ occur (*cf.* [9][2]). For instance,

$$15 = \varphi^5 + \varphi^2 + \varphi^0 + \varphi^{-3} + \varphi^{-6} \ ,$$

thus the φ-expansion of 15 is $(100101.001001)_\varphi$.

We have shown in [6] that there exists a finite two-tape automaton $\mathcal{A}_\varphi$ which maps the Fibonacci representation of any positive integer onto its φ-expansion, provided the latter is folded around the radix point, *e.g.* the Fibonacci representation of 15, 100010, is mapped onto $\substack{100101\\100100}$.

The result in [6] holds indeed for any *quadratic Pisot unit* as well. In order to explain this generalization, we have first to go quickly through few definitions and notations.

A Pisot number is an algebraic integer greater than 1 such that every of its algebraic conjugates has a modulus smaller than 1. A *quadratic Pisot unit* θ is thus the root greater than 1 of a polynomial

$$P_\theta(X) = X^2 - rX - \varepsilon \ ,$$

with either:

$\varepsilon = +1$ and $r \geq 1$, and this will be referred to as Case 1,
or $\varepsilon = -1$ and $r \geq 3$, and this will be referred to as Case 2.

[1] And usually credited to Zeckendorf [15]; *cf.* also [9, Exercise 1.2.8.34].

[2] Exercise 1.2.8.35.

As for the golden mean, we consider two numeration systems: the one defined by *the base* θ, and the one defined by the linear recurrent sequence U_θ whose characteristic polynomial is P_θ: the sequence $U_\theta = (u_k)_{k\geq 0}$ is defined[3] by:

$$u_{k+2} = r\,u_{k+1} + \varepsilon\,u_k \ , \qquad k \geq 0 \ ,$$

and by the initial conditions[4]

$$u_0 = 1 \quad \text{and} \quad u_1 = [\theta] + 1.$$

Every positive integer N is equal, in several different ways, to a sum of the u_k's with coefficients taken in $A_\theta = \{0, 1, \ldots, [\theta]\}$ — the *canonical alphabet of digits* for θ — and thus can be represented, in several different ways, as a word over A_θ; these words are the *U_θ-representations* of N. Similarly, every positive integer N is equal, in several different ways, to a sum of (positive and negative) powers of θ with coefficients taken in the same A_θ. Together with a *radix point*, these words, possibly infinite, are the *θ-representations* of N.

In a way that will be described in Section 3, one of the U_θ-representations of N is distinguished and is called *the normal U_θ-representation of N*. Likewise, one of the θ-representations of N is distinguished and is called *the θ-expansion of N*. It is obtained by the so-called greedy algorithm, see Section 3.

Because θ is a quadratic Pisot unit, the θ-expansion of any positive integer *is finite* (*cf.* [8]) and can thus be folded around the radix point.

The result in [6] can be stated as follows: *for any quadratic Pisot unit θ, there exists a finite two tape automaton $\mathcal{A}_\theta$ which maps the normal U_θ-representation of any positive integer onto its folded θ-expansion.*

Let us give some ideas on how the contruction works. There is a property of quadratic Pisot units which is that the θ-expansion of u_k, the k-th element of U_θ has, roughly, period 4. And the succession of digits in a U_θ-representation corresponds — for the represented integer — to the *summation* of elements of U_θ.

The main step in the construction of $\mathcal{A}_\theta$ is the construction of another finite two-tape automaton $\mathcal{T}_\theta$ which is much simpler. Building $\mathcal{A}_\theta$ from $\mathcal{T}_\theta$ is then done by means of standard automata constructions that are explained in [6]. The automaton $\mathcal{T}_\theta$ reads words where the letters have been *grouped into blocks of length* 4, and with the property that there is *at most one digit* 1 *in every block*. Stated otherwise, $\mathcal{T}_\theta$ reads words written on the five letter alphabet $B = \{z, a, b, c, d\}$ with:

$$z = 0\,0\,0\,0\ , \quad a = 0\,0\,0\,1\ , \quad b = 0\,0\,1\,0\ , \quad c = 0\,1\,0\,0 \quad \text{and} \quad d = 1\,0\,0\,0\ ,$$

and it ouputs some blocks of 4 double digits (taken in an alphabet that depends on θ and that is much larger than A_θ). The underlying input automaton of $\mathcal{T}_\theta$ is the *Cayley graph* of a certain group G_θ, which is described by the following[5]:

[3] *cf.* [2].

[4] $[\theta]$ is the *integral part* of θ.

[5] Propositions 11 and 12 in [6].

Proposition 1 *Let θ be the zero larger than 1 of $P_\theta(X) = X^2 - rX - \varepsilon$ and let $\Delta_\theta = r^2 + 4\varepsilon$ be the discriminant of $P_\theta(X)$.*

i) *If r is odd, then* $G_\theta \simeq \mathbb{Z}/\Delta_\theta\mathbb{Z}$.

ii) *If r is even, then:*

in Case 1*:* a) *if $r = 4m$, then* $G_\theta \simeq \mathbb{Z}/(\frac{1}{2}\Delta_\theta)\mathbb{Z}$ *;*

b) *if $r = 4m+2$, then* $G_\theta \simeq [\mathbb{Z}/(\frac{1}{4}\Delta_\theta)\mathbb{Z}] \times [\mathbb{Z}/2\mathbb{Z}]$ *;*

in Case 2*:* $G_\theta \simeq [\mathbb{Z}/(\frac{1}{2}\Delta_\theta)\mathbb{Z}] \times [\mathbb{Z}/2\mathbb{Z}]$.

As explained in [6], the *states* of $\mathcal{T}_\theta$, that is to say, the elements of G_θ, can be seen as elements of $\mathbb{Z}^4$. The *transitions* of $\mathcal{T}_\theta$, when reading one of the elements a, b, c, d, or z of B correspond *to the addition* of the current state with certain elements $\hat{a}$, $\hat{b}$, $\hat{c}$, $\hat{d}$ or $\hat{z}$ of $\mathbb{Z}^4$. In Case 1, $\hat{a} = 0\ r{-1}\ 0\ 1$, $\hat{b} = r{-1}\ 0\ 1\ 0$, $\hat{c} = 0\ 1\ 0\ r{-1}$, $\hat{d} = 1\ 0\ r{-1}\ 0$ and $\hat{z} = 0\ 0\ 0\ 0$; In Case 2, $\hat{a} = \hat{c} = 0\ 1\ 0\ 1$ and $\hat{b} = \hat{d} = 1\ 0\ 1\ 0$. This addition is not the usual addition on $\mathbb{Z}^4$, but the addition *modulo* the equivalence γ_θ on $\mathbb{Z}^4$ generated by the following equalities[6]:

$$1\ \bar{r}\ \bar{\varepsilon}\ 0 = \bar{r}\ \bar{\varepsilon}\ 0\ 1 = \bar{\varepsilon}\ 0\ 1\ \bar{r} = 0\ 1\ \bar{r}\ \bar{\varepsilon} = 0\ 0\ 0\ 0$$

directly deduced from the minimal polynomial of θ.

Let us denote by H_θ the quotient of $\mathbb{Z}^4$ by γ_θ. As $\hat{a} + \hat{c} = \hat{b} + \hat{d} = \hat{z}$, G_θ is the subgroup of H_θ generated by $\hat{a}$ and $\hat{b}$. This description of G_θ was aimed at introducing the congruence γ_θ and the group H_θ which are here under investigation.

Example 1 : $\varepsilon = +1$, $r = 1$. Then

$$G_\varphi \simeq [\mathbb{Z}/5\mathbb{Z}] \ .$$

□

Example 2 : $\varepsilon = +1$, $r = 2$. Let α be the larger zero of $X^2 - 2X - 1 = 0$. Then

$$G_\alpha \simeq [\mathbb{Z}/2\mathbb{Z}] \times [\mathbb{Z}/2\mathbb{Z}] \ .$$

The Cayley graph of G_α with generators $0\,1\,0\,1$ and $1\,0\,1\,0$ is presented on Figure 1. □

2 The group H_θ

In order to describe the group $H_\theta = \mathbb{Z}^4/\gamma_\theta$, we first characterize a set of representatives for the congruence γ_θ. For that purpose we need a few more definitions.

[6] With the convention that if n is an integer, $\bar{n}$ denotes $-n$.

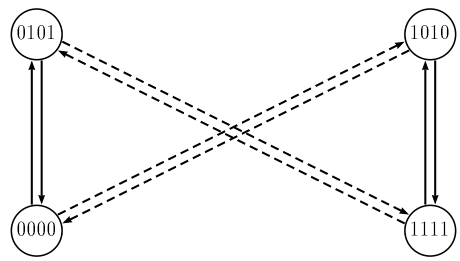


Figure 1: The action of B on G_α.
The transitions represented are those labelled by $\hat{a} = 0\,1\,0\,1$ (bold arrows), and by $\hat{b} = 1\,0\,1\,0$ (dashed arrows).

Two words of $\mathbb{Z}^4$ are said to be *conjugate*[7] if there exists a circular permutation of their digits that sends one onto the other.

The definition of the set R_θ of *reduced words* depends then upon the case we consider:

Case 1. $r \geq 1$ and $\varepsilon = +1$. A word of $\mathbb{N}^4$ is in R_θ if itself and its three conjugates are strictly smaller than $r\ 0\ r\ 0$ in the lexicographic order.

Case 2. $r \geq 3$ and $\varepsilon = -1$. A word of $\mathbb{N}^4$ is in R_θ if itself and its three conjugates are strictly smaller than $r-1\ r-2\ r-2\ r-2$ in the lexicographic order and different from $r-2\ r-2\ r-2\ r-2$.

The main purpose of this paper is to establish the following statement.

Theorem 1 *Every class of $\mathbb{Z}^4$ modulo γ_θ contains exactly one element in R_θ.*

The proof of Theorem 1 we give here — in Section 4 — is purely combinatorial and goes through the definition of a rewriting system associated with θ.

The enumeration of the elements of R_θ gives the order of H_θ. With the notation used in Proposition 1, we have:

Proposition 2 *The order of H_θ is $r^2\,\Delta_\theta$.*

Proof. In spite of the fact that, remarkably, the expression of the order H_θ does not depend on the case considered — this is encoded in the value of Δ_θ indeed — the proof itself forces us to distinguish the following two cases.

Case 1. $r \geq 1$ and $\varepsilon = +1$. A word w of $\mathbb{N}^4$ is in R_θ if and only if it, and its three conjugates, are (strictly) smaller than $r\ 0\ r\ 0$.

[7]Though this is *not* the conjugacy relation in the group $\mathbb{Z}^4$ (which is the identity since $\mathbb{Z}^4$ is commutative).

There are two possibilities:

a) every digit of w is smaller than r: there are r^4 such words.

b) one digit of w is equal to r; then the next digit has to be a 0 and the other two digits can take any value smaller than r: there are r^2 such words once the position of the digit equal to r is fixed among the 4 possible ones.

It then comes

$$|H_\theta| = r^4 + 4r^2 = r^2(r^2+4) = r^2\,\Delta_\theta \quad .$$

Case 2. $r \geq 3$ and $\varepsilon = -1$. A word w of $\mathbb{N}^4$ is in R_θ if and only if it, and its three conjugates, are (strictly) smaller than $r{-}1\; r{-}2\; r{-}2\; r{-}2$ and different from $r{-}2\; r{-}2\; r{-}2\; r{-}2$.

There are three possibilities:

a) every digit of w is smaller than $r-1$ and not all are equal to $r-2$: there are $(r-1)^4-1$ such words.

b) one digit of w is equal to $r-1$; then the other three digits can take any value smaller than $r-1$ and not all are equal to $r-2$: there are $(r-1)^3-1$ such words once the position of the digit equal to $r-1$ is fixed among the 4 possible ones.

c) two digits of w are equal to $r-1$; then they cannot be consecutive ones and the other two digits can take any value smaller than $r-2$: there are $(r-2)^2$ such words once the position of the digits equal to $r-1$ is fixed among the 2 possible ones.

It then comes

$$|H_\theta| = [(r-1)^4-1] + 4[(r-1)^3-1] + 2[(r-2)^2] = r^2(r+2)(r-2) = r^2\,\Delta_\theta \quad . \qquad \blacksquare$$

With the same notation as in Proposition 1 again, it then holds:

Theorem 2 *Let θ be the zero larger than 1 of* $P_\theta(X) = X^2 - rX - \varepsilon$ *and let* $\Delta_\theta = r^2 + 4\varepsilon$ *be the discriminant of $P_\theta(X)$.*

i) *If r is odd, then* $H_\theta \simeq [\mathbb{Z}/r\mathbb{Z}] \times [\mathbb{Z}/r\mathbb{Z}] \times [\mathbb{Z}/\Delta_\theta\mathbb{Z}]$.

ii) *If r is even, then:*

in Case 1*:* a) *if $r = 4m$, then* $H_\theta \simeq [\mathbb{Z}/2r\mathbb{Z}] \times [\mathbb{Z}/2r\mathbb{Z}] \times [\mathbb{Z}/(\frac{1}{4}\Delta_\theta)\mathbb{Z}]$;
b) *if $r = 4m+2$, then* $H_\theta \simeq [\mathbb{Z}/4r\mathbb{Z}] \times [\mathbb{Z}/2r\mathbb{Z}] \times [\mathbb{Z}/(\frac{1}{8}\Delta_\theta)\mathbb{Z}]$;

in Case 2*:* $H_\theta \simeq [\mathbb{Z}/2r\mathbb{Z}] \times [\mathbb{Z}/2r\mathbb{Z}] \times [\mathbb{Z}/(\frac{1}{4}\Delta_\theta)\mathbb{Z}]$.

Proof. We already know the order of H_θ and, in every case, the subgroup G_θ by Proposition 1. As we can, by Theorem 1, compute in H_θ, we find elements in $H_\theta \setminus G_\theta$ of sufficiently large order to give the key to the structure of H_θ by a simple consideration on the order of the generated subgroup.

Case 1. $\Delta_\theta = r^2 + 4$ and $0\; r\; 0\; r \;=\; r\; 0\; r\; 0 \;=\; 0\; 0\; 0\; 0$.

i) r is odd; $\qquad G_\theta \simeq \mathbb{Z}/\Delta_\theta\mathbb{Z}$.

We observe that $0\ 1\ 0\ 1$ and $1\ 0\ 1\ 0$ are both of order r. Hence the set of $x\ y\ x\ y$, $0 \le x, y < r$, is isomorphic to $J_\theta = [\mathbb{Z}/r\mathbb{Z}] \times [\mathbb{Z}/r\mathbb{Z}]$.

Since no divisor of r (odd) is a divisor of $\Delta_\theta = r^2 + 4$, the intersection of J_θ with G_θ must be the identity. As their product has the same order as H_θ, the latter is isomorphic to this product:

$$H_\theta \simeq [\mathbb{Z}/r\mathbb{Z}] \times [\mathbb{Z}/r\mathbb{Z}] \times [\mathbb{Z}/\Delta_\theta\mathbb{Z}] \ .$$

ii) $r = 2p$ is even; $\qquad \Delta_\theta = 4(p^2+1)$.

We observe that $(\,0\ 0\ p\ 1\,) + (\,0\ 0\ p\ 1\,) = 0\ 0\ r\ 2 = 0\ 1\ 0\ 1$ which is, as above, of order r. Hence $0\ 0\ p\ 1$ is of order $2r$ and $J_\theta = [\mathbb{Z}/2r\mathbb{Z}] \times [\mathbb{Z}/2r\mathbb{Z}]$ is a subgroup of H_θ of order $4r^2$.

a) $p = 2m$ is even; $\qquad G_\theta \simeq [\mathbb{Z}/\frac{1}{2}\Delta_\theta\mathbb{Z}] = [\mathbb{Z}/2(p^2+1)\mathbb{Z}]$.

The square[8] of elements[9] of G_θ is of order p^2+1. No divisor of $2r = 4p$ is a divisor of p^2+1 and

$$H_\theta \simeq [\mathbb{Z}/2r\mathbb{Z}] \times [\mathbb{Z}/2r\mathbb{Z}] \times [\mathbb{Z}/\tfrac{1}{4}\Delta_\theta\mathbb{Z}] \ .$$

b) $p = 2m+1$ is odd; $\qquad G_\theta \simeq [\mathbb{Z}/\frac{1}{4}\Delta_\theta\mathbb{Z}] \times [\mathbb{Z}/2\mathbb{Z}]$.

As above, $(\,0\ 0\ p\ 1\,) + (\,0\ p\ 1\ 0\,) = 0\ p\ {\scriptstyle p+1}\ 1$ is of order $2r$. We observe then that

$$(\,0\ m\ {\scriptstyle p+m+1}\ 1\,) + (\,0\ m\ {\scriptstyle p+m+1}\ 1\,) = 0\ {\scriptstyle 2m}\ {\scriptstyle r+p+1}\ 2 = 0\ p\ {\scriptstyle p+1}\ 1 \quad ,$$

and $0\ m\ {\scriptstyle p+m+1}\ 1$ is of order $4r$: $J'_\theta = [\mathbb{Z}/4r\mathbb{Z}] \times [\mathbb{Z}/2r\mathbb{Z}]$ is a subgroup of H_θ.

As p^2+1 is even but not divisible by 4, no divisor of r, different from 2, is a divisor of p^2+1. The intersection of J'_θ with G_θ is thus at most of order 4 — and equal to $[\mathbb{Z}/2\mathbb{Z}] \times [\mathbb{Z}/2\mathbb{Z}]$ — and at least of order 4 because of the order of H_θ. Thus:

$$H_\theta \simeq [\mathbb{Z}/4r\mathbb{Z}] \times [\mathbb{Z}/2r\mathbb{Z}] \times [\mathbb{Z}/\tfrac{1}{8}\Delta_\theta\mathbb{Z}] \ .$$

Case 2. $\Delta_\theta = r^2 - 4$ and $0\ 0\ r\ 0 = 0\ 1\ 0\ 1$, ${\scriptstyle r-2}\ {\scriptstyle r-2}\ {\scriptstyle r-2}\ {\scriptstyle r-2} = 0\ 0\ 0\ 0$.

i) r is odd; $\qquad G_\theta \simeq \mathbb{Z}/\Delta_\theta\mathbb{Z}$.

Since $0\ 0\ r\ r = 1\ 1\ 1\ 1$, it has order ${\scriptstyle r-2}$. Then $0\ 0\ 1\ 1$ has order $r({\scriptstyle r-2})$ and $0\ 0\ {\scriptstyle r-2}\ {\scriptstyle r-2}$ has order r. Similarly, $0\ {\scriptstyle r-2}\ {\scriptstyle r-2}\ 0$ has order r.

Hence the set of elements equivalent to $0\ \ x({\scriptstyle r-2})\ \ (x+y)({\scriptstyle r-2})\ \ y({\scriptstyle r-2})$, $0 \le x, y < r$, is isomorphic to $J_\theta = [\mathbb{Z}/r\mathbb{Z}] \times [\mathbb{Z}/r\mathbb{Z}]$.

[8] As G_θ is written additively, the square of x is $x + x$.

[9] Different from the identity of G_θ, obviously.

As in CASE 1, since no divisor of r (odd) is a divisor of $\Delta_\theta = r^2 - 4$, the intersection of J_θ with G_θ must be the identity. As their product has the same order as H_θ, the latter is isomorphic to this product:

$$H_\theta \simeq [\mathbb{Z}/r\mathbb{Z}] \times [\mathbb{Z}/r\mathbb{Z}] \times [\mathbb{Z}/\Delta_\theta\mathbb{Z}] \ .$$

ii) $r = 2p$ is even; $\quad \Delta_\theta = 4(p^2 - 1)$ and $G_\theta \simeq [\mathbb{Z}/\frac{1}{2}\Delta_\theta\mathbb{Z}] \times [\mathbb{Z}/2\mathbb{Z}]$.

We observe that $(0\ 0\ p{-}1\ p{-}1) + (0\ 0\ p{-}1\ p{-}1) = 0\ 0\ r{-}2\ r{-}2$ which is, as above, of order r. Hence $0\ 0\ p{-}1\ p{-}1$ is of order $2r$ and $J_\theta = [\mathbb{Z}/2r\mathbb{Z}] \times [\mathbb{Z}/2r\mathbb{Z}]$ is a subgroup of H_θ of order $4r^2$.

As no divisor of $r = 2p$, different from 2, is a divisor of $p+1$ or of $p-1$, the intersection of J_θ with G_θ is at most of order 4 — and equal to $[\mathbb{Z}/2\mathbb{Z}] \times [\mathbb{Z}/2\mathbb{Z}]$ — and at least of order 4 because of the order of H_θ. Thus:

$$H_\theta \simeq [\mathbb{Z}/2r\mathbb{Z}] \times [\mathbb{Z}/2r\mathbb{Z}] \times [\mathbb{Z}/\tfrac{1}{4}\Delta_\theta\mathbb{Z}] \ . \qquad \blacksquare$$

Example 2 (continued) : $\varepsilon = +1$, $r = 2$. The larger zero of $X^2 - 2X - 1 = 0$ is $\alpha = \frac{1+\sqrt{2}}{2}$. We have $0\,0\,2\,1 = 0\,1\,0\,0$ and, since we are in CASE 1, R_α is the set of words of $\mathbb{N}^4$ with the property that they, and all their conjugates, are strictly smaller than $2\,0\,2\,0$ in the lexicographic order.

We are in the case i) b. of the proof of Theorem 2, with $r = 2$, $p = 1$ and $m = 0$. The elements $0\,0\,1\,1$ and $0\,1\,1\,0$ generate $J_\alpha = [\mathbb{Z}/4\mathbb{Z}] \times [\mathbb{Z}/4\mathbb{Z}]$. The element $0\ m\ p{+}m{+}1\ 1 = 0\,0\,2\,1 = 0\,1\,0\,0$ is of order 8. In this case, $J'_\alpha = H_\alpha$ and G_α is contained in J'_α.

$$J'_\alpha = H_\alpha \simeq [\mathbb{Z}/8\mathbb{Z}] \times [\mathbb{Z}/4\mathbb{Z}] \ ,$$

and G_α is contained in J'_α.

Figure 2 shows the elements of H_α with “names” taken in R_α. $\square$

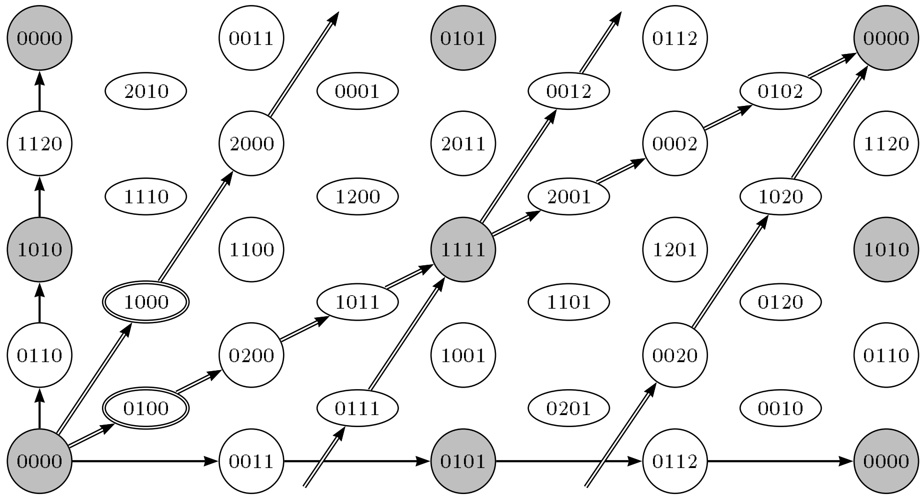


Figure 2: The group $H_\alpha \simeq [\mathbb{Z}/8\mathbb{Z}] \times [\mathbb{Z}/4\mathbb{Z}]$.
The elements of J_α are represented by circles, and those of its coset in H_α by ovals. All these elements are arranged on a torus which is, as usual, represented by a rectangle the edges of which are identified by pairs. For readability, some of the elements of H_α are put on these edges and appear then twice. The figure shows the intersecting orbits of 0 1 0 0 and 1 0 0 0 (double arrows). The elements of G_α are indicated in gray.

3 Symbolic dynamical systems

We now give the definitions and results that are necessary in order to present the above mentioned result of Parry, as well as its relationship with Theorem 1. The *θ-expansion* of a positive real number y can be computed by the so-called "greedy algorithm" that can be described as follows, see [12]. Let us denote by $[x]$ the integral part and by $\{x\}$ the fractional part of x. There exists $k \in \mathbb{Z}$ such that $\theta^k \leq x < \theta^{k+1}$. Let $x_k = [x/\theta^k]$, and $r_k = \{x/\theta^k\}$. Then, for $i < k$, put $x_i = [\theta r_{i+1}]$, and $r_i = \{\theta r_{i+1}\}$. We get an expansion $x = x_k\theta^k + x_{k-1}\theta^{k-1} + \cdots$. If $x < 1$, then $k < 0$, and we put $x_0 = x_{-1} = \cdots = x_{k+1} = 0$. The digits obtained are elements of the alphabet A_θ.

An expansion ending with infinitely many zeroes is said to be *finite*, and the trailing zeroes are omitted.

The number 1 is treated as a special case. Let $t_1 = [\theta]$, $r_1 = \{\theta\}$, and for $i \geq 2$, let $t_i = [r_{i-1}\theta]$ and $r_i = \{r_{i-1}\theta\}$. The infinite word $(t_i)_{i\geq 1}$ is called *the θ-expansion* of 1 and is denoted by $d_\theta(1)$. Finally, the sequence $d^*_\theta(1)$ is defined as follows:

$$\begin{array}{llll} \text{if} & d_\theta(1) \ \text{ is infinite} & \text{then} & d^*_\theta(1) = d_\theta(1) \ , \\ \text{if} & d_\theta(1) = t_1 \cdots t_m & \text{then} & d^*_\theta(1) = (t_1 \cdots t_{m-1}(t_m - 1))^\omega \ . \end{array}$$

For instance, when θ is a quadratic Pisot unit, we get :

in CASE 1, $A_\theta = \{0, \cdots, r\}$, $d_\theta(1) = r1$ and $d^*_\theta(1) = (r0)^\omega$;

in CASE 2, $A_\theta = \{0, \cdots, r-1\}$ and $d_\theta(1) = d^*_\theta(1) = r{-}1\,(r{-}2)^\omega$.

Let D_θ be the set of θ-expansions of numbers in the interval $[0, 1[$ and let σ be the shift on $A_\theta^{\mathbb{N}}$. The result of Parry can then be stated as follows ([11]): *A sequence s of $A_\theta^{\mathbb{N}}$ is in D_θ if and only if, for every $p \geq 0$, $\sigma^p(s)$ is smaller in the lexicographic order than $d^*_\theta(1)$.*

A very fundamental property of Pisot numbers (as far as θ-expansions are concerned) is given by the following result [1]: If θ is a Pisot number, then $d_\theta(1)$ is eventually periodic. This property makes it possible to canonically associate a linear recurrent sequence U_θ with every Pisot number θ ([2]). In Section 1, we have given the construction of the sequence U_θ.

By a greedy algorithm, every positive integer has a *normal U_θ-representation* (see [5]): given integers m and p, let us denote by $q(m, p)$ and $r(m, p)$ the quotient and the remainder of the Euclidean division of m by p. Let $k \geq 0$ such that $u_k \leq N < u_{k+1}$ and let $d_k = q(N, u_k)$ and $r_k = r(N, u_k)$, and, for $i = k-1, \cdots, 0$, $d_i = q(r_{i+1}, u_i)$ and $r_i = r(r_{i+1}, u_i)$. Then $N = d_k u_k + \cdots + d_0 u_0$. For the linear recurrent sequences U_θ considered here, the digits d_i belong to A_θ, and the word $d_k \cdots d_0$ of A^*_θ is the normal U_θ-representation of N. The sequence U_θ together with the alphabet A_θ define *the linear numeration system associated with θ.*

This system U_θ is characterized by the fact that normal U_θ-representations and θ-expansions are defined by the same set of forbidden words [2]. Hence these two numeration systems define the *same symbolic dynamical system.* For notions on symbolic dynamical systems, for example systems of finite type, sofic systems, ... , the reader may consult [10].

If θ is the root of $X^2 - rX - 1$, with $r \geq 1$ [CASE 1], the symbolic dynamical system associated with θ is the set of bi-infinite words on A_θ with no factor greater than or equal to the word $r\,1$ in the lexicographic order. Since it is defined by the interdiction of a finite number of words, it is a system of finite type. It is the set of labels of bi-infinite paths in the graph represented Figure 3.

If θ is the root of $X^2 - rX + 1$, with $r \geq 3$ [CASE 2], the symbolic dynamical system associated with θ is the set of bi-infinite words on A_θ with no factor greater than or equal in the lexicographic order to a word of the form $r{-}1\,(r{-}2)^n\,r{-}1$ for some $n \geq 0$. It is the set of labels of bi-infinite paths in the graph represented Figure 4. Since this graph is a finite automaton, the symbolic dynamical system associated with θ is sofic.

For the unitary quadratic Pisot numbers, the result of Parry can be expressed as follows. In CASE 1, an infinite sequence (resp. a finite word) over A_θ is a θ-expansion

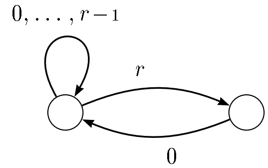


Figure 3: Symbolic dynamical system of finite type in CASE 1

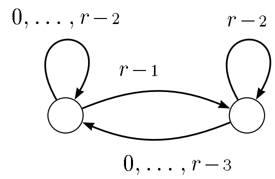


Figure 4: Sofic symbolic dynamical system in CASE 2

(resp. is a normal U_θ-representation) if and only if this sequence and all the shifted ones are lexicographically smaller than $(r\,0)^\omega$. Similarly in CASE 2, an infinite sequence (resp. a finite word) over A_θ is a θ-expansion (resp. is a normal U_θ-representation) if and only if this sequence and all the shifted ones are lexicographically smaller than $d_\theta(1) = r{-1}\,(r{-2})^\omega$.

Let $\pi_\theta \colon \mathbb{Z}^\mathbb{N} \to \mathbb{R}$ be the function mapping an infinite word $s = (s_n)_{n\geq 1}$ onto its numerical value $\sum_{n\geq 1} s_n \theta^{-n}$, and let α_θ be the congruence defined by $s\ \alpha_\theta\ s'$ if and only if $\pi_\theta(s) = \pi_\theta(s')$. Let $I_\theta = \{s \in \mathbb{Z}^\mathbb{N} \mid \pi_\theta(s) \in [0, 1[\}$. Then the result of Parry just recalled can be formulated as follows, in a manner very similar to Theorem 1:

Every class of I_θ modulo α_θ contains exactly one element in D_θ.

Let $Per_4(A_\theta^\mathbb{N})$ denote the set of periodic words of $A_\theta^\mathbb{N}$ of period 4. Then from our result follows that

$$D_\theta \cap Per_4(A_\theta^\mathbb{N}) = \begin{cases} \{w^\omega \mid w \in R_\theta\} & \text{in CASE 1} \\ \{w^\omega \mid w \in R_\theta\} \cup (\,r{-2}\ r{-2}\ r{-2}\ r{-2})^\omega & \text{in CASE 2.} \end{cases}$$

4 Proof of Theorem 1

The proof of Theorem 1 is quite different in CASE 1 and in CASE 2, much simpler in the latter case. For CASE 1, it is first easily established that every class contains at least one element of R_θ (Part A). The proof of uniqueness is more involved. An element, or word, of $\mathbb{Z}^4$ is said to be *positive* if all its digits belong to $\mathbb{N}$. We first consider only positive words and we give *an orientation* to the relations defining γ_θ. If the *rewriting system* obtained that way were *confluent* — that is to say, if "no matter how one diverges from a common ancestor, there are paths joining at a common descendent" [4] — the uniqueness of a reduced positive word would follow from a standard argument. What is developped in Part B through a detailed analysis is that this reduction "behaves" as if the system were confluent, though it is not. The last (and easy) step amounts to verify that reduction paths through non-positive words do not bring any further possibilities of equivalence between words (Part C). For CASE 2, we directly derive a *confluent rewriting system* from the relations defining γ_θ.

4.1 Proof for Case 1

Notation and conventions. By definition, γ_θ is generated by the following relations:

$$1\ \bar{r}\ \bar{1}\ 0\ = 0\ 0\ 0\ 0 \qquad (1) \qquad\qquad \bar{1}\ 0\ 1\ \bar{r}\ = 0\ 0\ 0\ 0 \qquad (3)$$

$$\bar{r}\ \bar{1}\ 0\ 1\ = 0\ 0\ 0\ 0 \qquad (2) \qquad\qquad 0\ 1\ \bar{r}\ \bar{1}\ = 0\ 0\ 0\ 0 \qquad (4)$$

Any linear combination of these relations gives rise to another relation that is also satisfied by the congruence γ_θ . In particular (1)+(3), and (2)+(4), yield respectively:

$$0\ \bar{r}\ 0\ \bar{r}\ = 0\ 0\ 0\ 0 \qquad (5) \qquad\qquad \bar{r}\ 0\ \bar{r}\ 0\ = 0\ 0\ 0\ 0 \qquad (6)$$

The opposite of a relation (α) is another relation, denoted by $\overline{(\alpha)}$; *e.g.*

$$\bar{1}\ r\ 1\ 0 = 0\ 0\ 0\ 0\ . \qquad \overline{(1)}$$

By abuse, we denote as the sum $w + (\alpha)$ the digit-addition of w and the non-zero member of the relation (α), $1 \le \alpha \le 4$; *e.g.*

$$\text{if} \quad w = x\ y\ u\ t\ , \quad \text{then} \quad w + (1) = x{+}1\ y{-}r\ u{-}1\ t\ \ .$$

The notation extends to subtraction: $w - (\alpha) = w + \overline{(\alpha)}$.

If w' is obtained from w by adding one of the four relations defining γ_θ or of their opposites, we write $w \leftrightarrow w'$; if moreover w and w' are both positive, we write $w \Leftrightarrow w'$. If w' is obtained by a sequence of such additions we write $w \overset{*}{\leftrightarrow} w'$ and such a sequence is called a *path* from w to w'. If moreover every word encountered on the path is positive, we write $w \overset{*}{\Leftrightarrow} w'$. By definition, w and w' are equivalent modulo γ_θ if and only if $w \overset{*}{\leftrightarrow} w'$.

The four relations (1) to (4) will also be considered as reductions and written as such:

$$w \overset{(\alpha)}{\rightarrow} w + (\alpha)\ \ .$$

If *both* w *and* $w + (\alpha)$ *are positive*, we write

$$w \overset{(\alpha)}{\Rightarrow} w + (\alpha)$$

and we say that w is *positively reducible* by (α). If it is not the case, w, *supposed to be positive*, is said to be (α)*-irreducible.* A positive word is called *positively irreducible*, or *p-irreducible*, if no such reduction is possible.

Every word in R_θ is p-irreducible but the converse obviously does not hold; *e.g.* $0\ r{+}1\ 0\ 0$ is p-irreducible but not in R_θ.

In addition to the cases described by these general conventions, we shall also write

$$0\ r\ 0\ r\ \overset{(5)}{\Rightarrow}\ 0\ 0\ 0\ 0 \qquad \text{and} \qquad r\ 0\ r\ 0\ \overset{(6)}{\Rightarrow}\ 0\ 0\ 0\ 0\ ,$$

which state that $0\ r\ 0\ r$, and $r\ 0\ r\ 0$, are *positively* reducible to $0\ 0\ 0\ 0$. But this word $w =\ 0\ r\ 0\ r$ (resp. $w =\ r\ 0\ r\ 0$) is the only one to which the reduction (5), (resp. (6)) may be applied, since they would be otherwise even more cases to be analysed later.

A positive path between two positive words f and g is thus a sequence of positive reductions following each other either in the direct or in the reverse direction; *e.g.*

$$f \overset{(\alpha)}{\Rightarrow} f + (\alpha) \overset{(\beta)}{\Leftarrow} f + (\alpha) + \overline{(\beta)} = g\ .$$

A last definition: the sum of the digits of an element w of $\mathbb{Z}^4$ is called the *weight* of w, and is denoted by $W(w)$. A positive word has positive weight but the converse does not hold. For any w in $\mathbb{Z}^4$ and for any reductions α, β, and γ it holds:

$$W(w + (\alpha)) = W(w + (\alpha) + \overline{(\beta)} + (\gamma)) = W(w) - r\ ,$$
$$\text{and} \qquad W(w + (\alpha) + \overline{(\beta)}) = W(w)\ .$$

Part A. Every class modulo γ_θ contains positive words, by adding $\overline{(1)} + \overline{(3)}$ and $\overline{(2)} + \overline{(4)}$ a sufficient number of times to any word of $\mathbb{Z}^4$.

We show, by case examination, that for any positive word w not in R_θ, it is possible to find a positive path (of length 1, 2 or 3) that leads to a word w' which is either in R_θ or has a weight reduced by r. Hence, from any positive word there exists a positive path reaching R_θ, for otherwise it would be possible to build a positive path reaching a word of non-positive weight, and thus, non-positive, a contradiction. And then, every class modulo γ_θ contains at least one element in R_θ.

Let $w =\ x\ y\ u\ t$ be in $\mathbb{N}^4$ and not in R_θ. Without loss of generality, one can suppose that x and u on one hand, and y and t on the other hand, are not both greater than r, for otherwise a sequence of reductions $(2) + (4)$ or $(1) + (3)$ could be used[10]. Similarly, one can suppose that no digit greater than r is followed by a positive digit for otherwise one of the reductions (1) to (4) could obviously be used.

Since γ_θ commutes with any circular permutation, one can suppose, without loss of generality, that $y\ u\ t\ x$ is the largest circular factor (in the lexicographic order) of $w =$

[10]in the case where the other two digits (y and t, or x and u) are 0, this sequence is prefixed by $\overline{(1)}$ (resp. $\overline{(2)}$) and suffixed by (1) (resp. (2))

$x\ y\ u\ t$. Since we suppose that w is not in R_θ, *i.e.*, $y\ u\ t\ x$ is greater than $r\ 0\ r\ 0$ in the lexicographic order, this implies from the above remark that

$$x \le r-1, \qquad y \ge r+1, \qquad u=0 \quad \text{and} \quad t \le r-1\,.$$

We then apply $\overline{(4)}$ followed by (1):

$$w = x\ y\ 0\ t \overset{(4)}{\Leftarrow} x\ \ y{-}1\ \ r\ \ t{+}1 \overset{(1)}{\Rightarrow} x{+}1\ \ y{-}r{-}1\ \ r{-}1\ \ t{+}1\ = w'\ .$$

We have $W(w) = W(w')$. Which relation can be further applied to w' then depends on the actual values of x, y, and t, and we have to examine the different possible cases.

1 If $t = r-1$, then $w' = \ x{+}1\ \ y{-}r{-}1\ \ r{-}1\ \ r \overset{(3)}{\Rightarrow} x\ \ y{-}r{-}1\ \ r\ \ 0\ = w''$.

2 If $t \le r-2$ (and thus $r \ge 2$), then

2.1 If $x = r-1$, then

2.1.1 If $y = r+1$, then $w' = \ r\ \ 0\ \ r{-}1\ \ t{+}1$ is in R_θ .

2.1.2 If $y \ge r+2$, then

$$w' = \ r\ \ y{-}r{-}1\ \ r{-}1\ \ t{+}1 \overset{(2)}{\Rightarrow} 0\ \ y{-}r{-}2\ \ r{-}1\ \ t{+}2\ = w''$$

2.2 If $x \le r-2$, then

2.2.1 If $y \le 2r$, then $w' = \ x{+}1\ \ y{-}r{-}1\ \ r{-}1\ \ t{+}1$ is in R_θ .

2.2.2 If $y \ge 2r+1$, then

$$w' = \ x{+}1\ \ y{-}r{-}1\ \ r{-}1\ \ t{+}1 \overset{(1)}{\Rightarrow} x{+}2\ \ y{-}2r{-}1\ \ r{-}2\ \ t{+}1\ = w''$$

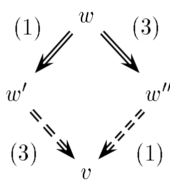
is a positive word since $r \ge 2$.

Thus, as announced, in any case, a positive word w leads either to a word of strictly smaller weight by a positive path of length 1 or 3 or into R_θ by a positive path of length 2.

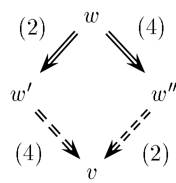
Part B. The system defined by the relations (1) to (4) — oriented, as in Part A, from left to right — is not confluent when it is restricted to positive words. With the hope of making the reading easier, we have illustrated, or more exactly, *translated*, the statements given in the claims which follow by diagrams. In these diagrams, the hypotheses, namely the existence of certain reductions, are depicted by solid arrows, and the conclusions, namely the existence of certain other reductions, are depicted by dashed arrows. In both cases these are doublelined arrows as they correspond to positive reductions.

It is easy to verify, by inspection on the possible values of the digits of w, the first two following claims.

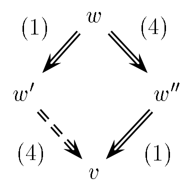
Claim 1 *Let w be a positive word; then,* i) $w \overset{(1)}{\Rightarrow} w'$ *and* $w \overset{(3)}{\Rightarrow} w''$ *imply that there exists a (positive) word v such that* $w' \overset{(3)}{\Rightarrow} v$ *and* $w'' \overset{(1)}{\Rightarrow} v$. *Similarly,* ii) $w \overset{(2)}{\Rightarrow} w'$ *and* $w \overset{(4)}{\Rightarrow} w''$ *imply that there exists a (positive) word v such that* $w' \overset{(4)}{\Rightarrow} v$ *and* $w'' \overset{(2)}{\Rightarrow} v$.



Claim 1, i)



Claim 1, ii)



Claim 2, i)

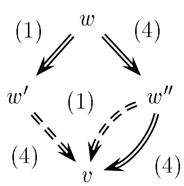
Claim 2 *Let w be a positive word and suppose that $w \overset{(1)}{\Rightarrow} w'$ and $w \overset{(4)}{\Rightarrow} w''$ hold. Then:*

i) *w'' (1)-reducible implies that w' is (4)-reducible and vice versa;*

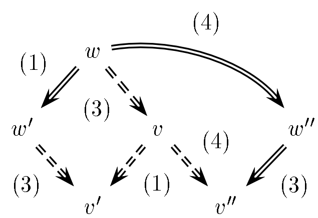
ii) *w'' (4)-reducible implies that w'' is (1)-reducible as well (and thus w' is (4)-reducible);*

iii) *w'' (3)-reducible implies that both w and w' are (3)-reducible;*

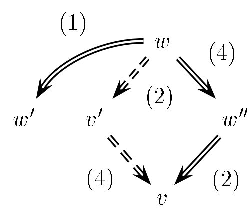
iv) *w'' (2)-reducible implies that w is (2)-reducible.*



Claim 2, ii)



Claim 2, iii)

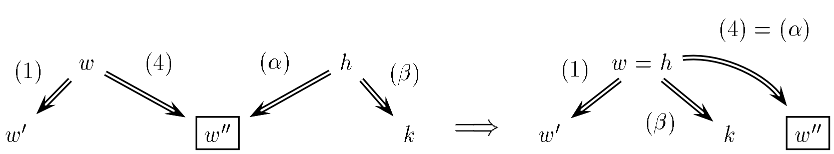


Claim 2, iv)

These first two claims deal with the cases where the reduction behaves as if it were confluent; the next one describes in detail the case where the reduction is not confluent: one of the branch happens to be a dead end from where one cannot escape by another derivation than the branch itself.

Claim 3 *Let w be a positive word. Suppose that $w \overset{(1)}{\Rightarrow} w'$ and $w \overset{(4)}{\Rightarrow} w''$ hold and that w'' is p-irreducible. If there exists two (positive) words h and k and two distincts reductions (α) and (β) such that $h \overset{(\alpha)}{\Rightarrow} w''$ and $h \overset{(\beta)}{\Rightarrow} k$, then necessarily*

i) *$h = w$ [and $(\alpha) = (4)$];* ii) *if $k \neq w'$ then $(\beta) = (3)$.*



Proof. Let $w = x\ y\ u\ t$; thus $w'' = x\ \ y{+}1\ \ u{-}r\ \ t{-}1$.

The hypothesis implies that:

$y \geq r$ since w is (1)-reducible; $u = r$, since w'' is (1)-irreducible and $y \geq r$;

$x < r$, since w'' is (2)-irreducible; and $t < r + 1$, since w'' is (3)-irreducible.

Now, $h \overset{(3)}{\Rightarrow} w''$ is impossible since $w'' = \ x \ \ y{+}1 \ \ 0 \ \ t{-}1 \ .$

Suppose $h \overset{(2)}{\Rightarrow} w''$; then $h = \ x{+}r \ \ y{+}2 \ \ 0 \ \ t{-}2$ which makes $h \overset{(4)}{\Rightarrow} k$ or $h \overset{(1)}{\Rightarrow} k$ impossible; $h \overset{(3)}{\Rightarrow} k$ is impossible as well since $t < r + 1$.

Suppose $h \overset{(1)}{\Rightarrow} w''$; then $h = \ x{-}1 \ \ y{+}r{+}1 \ \ 1 \ \ t{-}1$ which implies $r > 1$ since $x < r$. Now $h \overset{(4)}{\Rightarrow} k$ is impossible since $r > 1$; $h \overset{(3)}{\Rightarrow} k$ is impossible since $t < r + 1$ and $h \overset{(2)}{\Rightarrow} k$ is impossible since $x < r$.

The only possibility left by $(\alpha) \neq (\beta)$ is thus $(\alpha) = (4)$.

As before, $(\beta) = (2)$ is impossible since $x < r$ and the claim is established. ∎

A simple verification leads to the following claim.

Claim 4 *Let w be a positive word; $w \overset{(1)}{\Rightarrow} w'$ and $w \overset{(4)}{\Rightarrow} w''$ imply that w'' does not belong to R_θ. Similarly, $w \overset{(4)}{\Rightarrow} w'$ and $w \overset{(3)}{\Rightarrow} w''$, or $w \overset{(3)}{\Rightarrow} w'$ and $w \overset{(2)}{\Rightarrow} w''$, or $w \overset{(2)}{\Rightarrow} w'$ and $w \overset{(1)}{\Rightarrow} w''$ imply $w'' \notin R_\theta$.* ∎

The collection of claims we have just established allows us to adapt the classical scheme of demonstration of the uniqueness of reduced words in a class modulo a confluent relation. Let us suppose, by way of contradiction, that there exist f and g in R_θ with the property that there exists a positive path between them. [Recall that a positive path is a sequence of reductions (1), (2), (3) or (4) between positive words — together with the possible occurrence of $0 \ r \ 0 \ r \overset{(5)}{\Rightarrow} 0 \ 0 \ 0 \ 0$ and of $r \ 0 \ r \ 0 \overset{(6)}{\Rightarrow} 0 \ 0 \ 0 \ 0$ — in either directions.]

Since f and g are both p-irreducible, such a path Π must contain a "*peak*", that is a factor

$$w' \Leftrightarrow w \Leftrightarrow w'' \qquad \text{of the form} \qquad w' \overset{(\alpha)}{\Leftarrow} w \overset{(\beta)}{\Rightarrow} w'' \ .$$

The path Π thus contains a peak of *maximal weight*; the weight of such a peak will be *the weight of the path* Π. Paths are then *ordered by weight* and paths of equal weight are *ordered by the number of peaks* of maximal weight.

In the set of all positive paths between f and g — a non-empty subset by hypothesis — let us choose a minimal path Π_0 *i.e.,* a path of minimal weight with a minimal number of peaks of maximal weight. Let w be one of these peaks of maximal weight and let $w \overset{(\alpha)}{\Rightarrow} w'$ and $w \overset{(\beta)}{\Rightarrow} w''$ be the two reductions that go out of w on Π_0, which can thus be written in the following form:

$$f \overset{*}{\Leftrightarrow} w' \overset{(\alpha)}{\Leftarrow} w \overset{(\beta)}{\Rightarrow} w'' \overset{*}{\Leftrightarrow} g$$

By Claim 1, it is not possible to have $\alpha = 1$ and $\beta = 3$; for otherwise we would have a word v such that $w' \overset{(3)}{\Rightarrow} v$ and $w'' \overset{(1)}{\Rightarrow} v$ and thus the path

$$f \overset{*}{\Leftrightarrow} w' \overset{(3)}{\Rightarrow} v \overset{(1)}{\Leftarrow} w'' \overset{*}{\Leftrightarrow} g$$

is smaller than Π_0, a contradiction. For the same reason it is not possible to have $\alpha = 2$ and $\beta = 4$.

Up to a circular permutation of every word on Π_0, and a possible exchange of f and g, we can assume that $\alpha = 1$ and $\beta = 4$. By Claim 2 i) and ii), and with the same argument as just above, w'' is neither (1)- nor (4)-reducible. By Claim 2 iii), w'' is not (3)-reducible for otherwise we would have $w' \overset{(3)}{\Rightarrow} v'$, $w \overset{(3)}{\Rightarrow} v$ and $w'' \overset{(3)}{\Rightarrow} v''$ and since reductions commute we would get the path

$$f \overset{*}{\Leftrightarrow} w' \overset{(3)}{\Rightarrow} v' \overset{(1)}{\Leftarrow} v \overset{(4)}{\Rightarrow} v'' \overset{(3)}{\Leftarrow} w'' \overset{*}{\Leftrightarrow} g$$

which again is smaller than Π_0. We have now to consider the remaining two cases: **case a)** w'' *is not* (2)-reducible (and thus w'' is p-irreducible), or **case b)** w'' *is* (2)-reducible. Note that w'' is neither (5) nor (6)-reducible.

case a.– w'' is p-irreducible. By Claim 4, w'' is not in R_θ and thus not equal to g. The path Π_0 factorizes into

$$f \overset{*}{\Leftrightarrow} w' \overset{(1)}{\Leftarrow} w \overset{(4)}{\Rightarrow} w'' \overset{(\alpha)}{\Leftarrow} h \Leftrightarrow k \overset{*}{\Leftrightarrow} g\,.$$

The only possibilities left by Claim 3 for the reductions $w'' \overset{(\alpha)}{\Leftarrow} h \Leftrightarrow k$ are either

case a.1.– $w'' \overset{(4)}{\Leftarrow} h \overset{(1)}{\Rightarrow} k = w'$ in which case w'' is indeed a dead end in Π_0 and

$$f \overset{*}{\Leftrightarrow} w' \overset{*}{\Leftrightarrow} g$$

is a path smaller than Π_0, a contradiction; or

case a.2.– $w'' \overset{(\alpha)}{\Leftarrow} h \overset{(\gamma)}{\Leftarrow} k$ in which case k has a weight greater than w, another contradiction.

case b.– w'' is (2)-reducible. By Claim 2 iv), w is (2)-reducible as well. If w' is also (2)-reducible the situation is the same as if w'' were (3)-reducible and leads to a contradiction. Let us suppose then that w' is (2)-irreducible and let us sum up the constraints on the digits of $w = x\ y\ u\ t$ given by all hypotheses we have made up to this point. We have:

$$w' = \ x{+}1\ \ y{-}r\ \ u{-}1\ \ t\ \ \overset{(1)}{\Leftarrow} w = \ x\ \ y\ \ u\ \ t\ \overset{(4)}{\Rightarrow} w'' = \ x\ \ y{+}1\ \ u{-}r\ \ t{-}1\ \ \overset{(2)}{\Rightarrow}\ x{-}r\ \ y\ \ u{-}r\ \ t$$

The hypothesis w'' (1)-irreducible implies $u = r$ and thus w' is (4)-irreducible; w' (2)-irreducible implies $y = r$ (and thus w' is (1)-irreducible). There are thus two possibilities: case b.1), w' is (3)-reducible or, case b.2), w' is p-irreducible.

case b.1.– w' is (3)-reducible; w'' (3)-irreducible implies $t = r$. The path Π_0 reads then

$$f \overset{*}{\Leftrightarrow}\ x{+}1\ \ 0\ \ r{-}1\ \ r\ \ \overset{(1)}{\Leftarrow} w = \ x\ \ r\ \ r\ \ r\ \overset{(4)}{\Rightarrow}\ x\ \ r{+}1\ \ 0\ \ r{-}1\ \overset{*}{\Leftrightarrow} g\,.$$

If x is greater than r, the path

$$f \overset{*}{\Leftrightarrow} \ x{+}1 \ 0 \ r{-}1 \ r \ \overset{(3)}{\Rightarrow} x \ 0 \ r \ 0 \overset{(1)}{\Leftarrow} \ x{-}1 \ r \ r{+}1 \ 0 \ \overset{(2)}{\Rightarrow} \ x{-}r{-}1 \ r{-}1 \ r{+}1 \ 1$$
$$\overset{(3)}{\Leftarrow} \ x{-}r \ r{-}1 \ r \ r{+}1 \ \overset{(4)}{\Rightarrow} \ x{-}1 \ r \ 0 \ r \ \overset{(2)}{\Leftarrow} \ x \ r{+}1 \ 0 \ r{-}1 \ \overset{*}{\Leftrightarrow} g$$

is smaller than Π_0. If $x = r$, the path

$$f \overset{*}{\Leftrightarrow} \ x{+}1 \ 0 \ r{-}1 \ r \ \overset{(3)}{\Rightarrow} r \ 0 \ r \ 0 \overset{(6)}{\Rightarrow} 0\,0\,0\,0 \overset{(5)}{\Leftarrow} 0 \ r \ 0 \ r \ \overset{(2)}{\Leftarrow} \ x \ r{+}1 \ 0 \ r{-}1 \ \overset{*}{\Leftrightarrow} g$$

is again smaller than Π_0, and of a form consistent with the hypothesis on a positive path. Contradiction for any possible value of x.

case b.2.– w' is p-irreducible. Since w is (2)-reducible and using Claim 1, we can transform the path Π_0 into a path $\Pi_0{}'$

$$f \overset{*}{\Leftrightarrow} w' \overset{(1)}{\Leftarrow} w \overset{(2)}{\Rightarrow} w''' \overset{*}{\Leftrightarrow} g$$

which is also minimal. The image of $\Pi_0{}'$ by the permutation σ^{-1} then reads

$$k \overset{*}{\Leftrightarrow} m'' \overset{(4)}{\Leftarrow} m \overset{(1)}{\Rightarrow} m' \overset{*}{\Leftrightarrow} l$$

with $k = \sigma^{-1}(f)$, $l = \sigma^{-1}(g)$, $m = \sigma^{-1}(w)$, $m'' = \sigma^{-1}(w')$ and $m' = \sigma^{-1}(w''')$. As w', m'' is p-irreducible and we are back to **case a)**, that leads to a contradiction.

This terminates the proof of the fact that no two distinct elements of R_θ can be joined by a positive path.

Part C. It remains to show that if two elements f and g of R_θ are congruent modulo γ_θ, they are equal. Indeed, f and g are congruent modulo γ_θ if and only if $f \overset{*}{\leftrightarrow} g$, that is, if and only if there exists a path Σ between f and g. The idea is to "lift" the path Σ into a *positive path* Π between f and g (as sketched on Figure 5) and the conclusion follows from Part B.

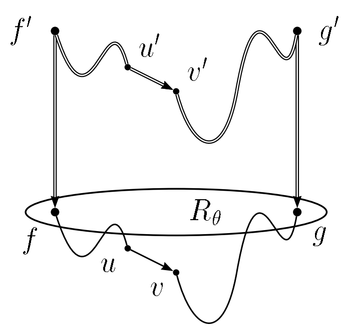


Figure 5: Σ lifts to Π .

The lifting relies on a lemma and a remark.

Lemma 3 *Let n be any positive integer and let h_n be the word*

$$h_n = \; nr \; nr \; nr \; nr \quad .$$

For any f in R_θ there exists a positive path $f + h_n \overset{*}{\Rightarrow} f$.

Proof. If $f = \; 0\;0\;0\;0$ one may begin the path with

$$0\;0\;0\;0 \overset{(6)}{\Leftarrow} r\;0\;r\;0$$

and thus one can assume that at least one digit of $f = \; x\;y\;u\;t$ is positive. Up to a circular permutation, it is possible to suppose that this digit is x. One has the sequence:

$$f = \; x\;y\;u\;t \overset{(1)}{\Leftarrow} x{-}1\;y{+}r\;u{+}1\;t \overset{(3)}{\Leftarrow} x\;y{+}r\;u\;t{+}r$$
$$\overset{(2)}{\Leftarrow} x{+}r\;y{+}r{+}1\;u\;t{+}r{-}1 \overset{(4)}{\Leftarrow} x{+}r\;y{+}r\;u{+}r\;t{+}r \; = f + h_1 \quad .$$

Without any further care on the order of the rewriting one has

$$f + h_i \overset{(1)+(2)+(3)+(4)}{\Longleftarrow} f + h_{i+1}$$

for any positive i and then $f \overset{*}{\Leftarrow} f + h_n$ for any positive n. ■

Remark 1 Let u and v be two non-positive elements of $\mathbb{Z}^4$ and k the lower bound of the digits in u and v; let n be a positive integer such that $nr > -k$. If $u \overset{(\alpha)}{\to} v$, then $u + h_n \overset{(\alpha)}{\Rightarrow} v + h_n$, for any reduction (α).

Let Σ be any path of reductions that links f and g, which we write

$$f \overset{\Sigma}{\longleftrightarrow} g$$

It is clear now how to lift Σ: let k be the lower bound of the digits of the words that appear in Σ and let n as above, *i.e.,* such that $nr > -k$. Let $f' = f + h_n$ and $g' = g + h_n$. We have, by Lemma 3,

$$f \overset{*}{\Leftarrow} f' \overset{\Sigma + h_n}{\longleftrightarrow} g' \overset{*}{\Rightarrow} g$$

and by the remark " $\Sigma + h_n$ " is a positive path. Thus $f \overset{*}{\leftrightarrow} g$ implies $f \overset{*}{\Leftrightarrow} g$ which has been shown impossible and this complete the proof of the theorem in Case 1. ■

4.2 Proof for Case 2

Unless otherwise stated, all notations and conventions described in the previous section are still valid. The congruence γ_θ is now generated by the following relations:

$1\;\bar{r}\;1\;0$	$= 0\;0\;0\;0$	(1')	$1\;0\;1\;\bar{r}$	$= 0\;0\;0\;0$	(3')
$\bar{r}\;1\;0\;1$	$= 0\;0\;0\;0$	(2')	$0\;1\;\bar{r}\;1$	$= 0\;0\;0\;0$	(4')

which can be turned into a rewriting system $(\mathcal{S})$ by giving the orientation from left to right:

$$1\ \bar{r}\ 1\ 0 \rightarrow 0\ 0\ 0\ 0 \qquad (1')\ \textit{etc.}$$

Let us recall also that R_θ is now the set of words of $\mathbb{N}^4$ with the property that they, and all their conjugates, are different from $\overline{r-2}\ \overline{r-2}\ \overline{r-2}\ \overline{r-2}$ and strictly smaller than $\overline{r-1}\ \overline{r-2}\ \overline{r-2}\ \overline{r-2}$ in the lexicographic order.

It is immediate to check that for any positive word w and any two reductions (α) and (β) in $(\mathcal{S})$, if $w \overset{(\alpha)}{\Rightarrow} w'$ and $w \overset{(\beta)}{\Rightarrow} w''$ hold, then $w' \overset{(\beta)}{\Rightarrow} v$ and $w'' \overset{(\alpha)}{\Rightarrow} v$ hold as well.

This fundamental difference with Case 1 can be stated as follows:

Claim 5 $(\mathcal{S})$ *is confluent on the set of positive words.* ■

We are not yet done, for the rewriting system $(\mathcal{S})$ is not equivalent to γ_θ on the set of positive words. But the solution is at hand and will be reached by the construction of a richer system.

Let $(\mathcal{T})$ be the rewriting system obtained by adding any subset of relations in $(\mathcal{S})$. We get then the following relations.

$$\overline{r-1}\ \overline{r-1}\ 1\ 1 \rightarrow 0\ 0\ 0\ 0 \qquad (5')$$
$$\overline{r-1}\ 1\ 1\ \overline{r-1} \rightarrow 0\ 0\ 0\ 0 \qquad (6')$$
$$1\ 1\ \overline{r-1}\ \overline{r-1} \rightarrow 0\ 0\ 0\ 0 \qquad (7')$$
$$1\ \overline{r-1}\ \overline{r-1}\ 1 \rightarrow 0\ 0\ 0\ 0 \qquad (8')$$

that is: $(5') = (1') + (2')$, $(6') = (2') + (3')$, $(7') = (3') + (4')$ and $(8') = (4') + (1')$.

$$\overline{r-1}\ 2\ \overline{r-1}\ \overline{r-2} \rightarrow 0\ 0\ 0\ 0 \qquad (9')$$
$$2\ \overline{r-1}\ \overline{r-2}\ \overline{r-1} \rightarrow 0\ 0\ 0\ 0 \qquad (10')$$
$$\overline{r-1}\ \overline{r-2}\ \overline{r-1}\ 2 \rightarrow 0\ 0\ 0\ 0 \qquad (11')$$
$$\overline{r-2}\ \overline{r-1}\ 2\ \overline{r-1} \rightarrow 0\ 0\ 0\ 0 \qquad (12')$$

that is: $(9') = (2') + (3') + (4')$, $(10') = (3') + (4') + (1')$, $(11') = (4') + (1') + (2')$ and $(12') = (1') + (2') + (3')$. And finally $(13') = (1') + (2') + (3') + (4')$:

$$\overline{r-2}\ \overline{r-2}\ \overline{r-2}\ \overline{r-2} \rightarrow 0\ 0\ 0\ 0 \qquad (13')$$

A simple case inspection shows that

Claim 6 *R_θ is the set of irreducible words for the system $(\mathcal{S} + \mathcal{T})$.* ■

The core of the proof lies then in the following:

Claim 7 *$(\mathcal{S}+\mathcal{T})$ is confluent on the set of positive words.*

Proof. Since we have not spared him the slightest detail yet, the reader may be scared by the prospect of checking the 78 critical pairs of the system $(\mathcal{S}+\mathcal{T})$. Hopefully, thanks to the symmetries and the very specific form of the relations, the number of cases to be examined boils down to 11, of which we shall make only 3 explicit.

Let $w = x\ y\ u\ t$ be a positive word and suppose that $w \overset{(\alpha)}{\Rightarrow} w'$ and $w \overset{(\beta)}{\Rightarrow} w''$ hold. By Claim 5, one can assume that (α) and (β) are not both in $(\mathcal{S})$. Up to an exchange of (α) and (β), we suppose that β is in $(\mathcal{T})$.

1 (α) is in $(\mathcal{S})$. Up to a circular permutation, one can assume that $(\alpha) = (1')$.

1.1 (β) "contains" (α), *i.e.,* it exists (γ) in $(\mathcal{S}+\mathcal{T})$ such that $(\beta) = (\alpha) + (\gamma)$.

Then, obviously, $w' \overset{(\gamma)}{\Rightarrow} w''$.

1.2 (β) does not "contain" (α); the only possibilities are $(\beta) = (6')$, (7'), or (9'). Immediate computations show that $w' \overset{(\beta)}{\Rightarrow} v$ and $w'' \overset{(\alpha)}{\Rightarrow} v$ hold as well.

For instance, let $(\beta) = (9')$; it comes:

$$x\ y\ u\ t \overset{(1')}{\Longrightarrow} x{+}1\ \ y{-}r\ \ u{+}1\ \ t\ = w' \qquad (14')$$

and

$$x\ y\ u\ t \overset{(9')}{\Longrightarrow} x{-}r{+}1\ \ y{+}2\ \ u{-}r{+}1\ \ t{-}r{+}2\ = w''\ . \qquad (15')$$

From (14') follows $y \geq r$ and thus $w'' \overset{(9')}{\Longrightarrow} v$; from (15') follows $x,\ u \geq r{-}1,\ t \geq r{-}2$ and thus $w' \overset{(1')}{\Longrightarrow} v$.

2 (α) is not in $(\mathcal{S})$. By symmetry, one can assume that (β) is as "large" as (α), *i.e.,* is the sum of as many relations from $(\mathcal{S})$ as (α). Up to a circular permutation, one can assume that $(\alpha) = (5')$ or $(9')$ (since $(\alpha) = (13')$ implies $(\beta) = (13')$).

2.1 (β) "contains" (α). Same solution as in 1.1.

2.2 Case 2.1 does not hold. Then there exist (γ), (δ) and (ε) in $(\mathcal{S}+\mathcal{T})$ such that $(\alpha) = (\gamma) + (\delta)$ and $(\beta) = (\gamma) + (\varepsilon)$. It is then a matter of immediate computation to verify that, in every case, $w' \overset{(\varepsilon)}{\Rightarrow} v$ and $w'' \overset{(\delta)}{\Rightarrow} v$ hold. The only possibilities are:

2.2.1 if $(\alpha) = (5')$, then $(\beta) = (6')$, (7'), (8'), (9') or (10').

For instance, let $(\beta) = (6')$; it comes:

$$x\ y\ u\ t \overset{(5')}{\Longrightarrow} x{-}r{+}1\ \ y{-}r{+}1\ \ u{+}1\ \ tpu\ = w' \qquad (16')$$

and

$$x\ y\ u\ t \overset{(6')}{\Longrightarrow} x{-}r{+}1\ \ y{+}1\ \ u{+}1\ \ t{-}r{+}1\ = w''\ . \qquad (17')$$

From (16') follows $y \geq r{-}1$, thus $y{+}1 \geq r$ and thus $w'' \overset{(1')}{\Longrightarrow} v$; from (17') follows $t \geq r{-}1$, thus $t{+}1 \geq r$ and thus $w' \overset{(3')}{\Longrightarrow} v$.

2.2.2 if $(\alpha) = (9')$, then $(\beta) = (10')$, (11'), or (12').

For instance, let $(\beta) = (10')$; it comes:

$$x\ y\ u\ t \overset{(9')}{\Longrightarrow} x{-}r{+}1\ \ y{+}2\ \ u{-}r{+}1\ \ t{-}r{+}2\ = w' \qquad (18')$$

and

$$x\ y\ u\ t \overset{(10')}{\Longrightarrow} x{+}2\ \ y{-}r{+}1\ \ u{-}r{+}2\ \ t{-}r{+}1\ = w'' \ . \qquad (19')$$

From (18') follows $x \geq r{-}1$, thus $y{+}2 > r$ and thus $w'' \overset{(2')}{\Longrightarrow} v$; from (19') follows $y \geq r{-}1$, thus $y{+}2 > r$ and thus $w' \overset{(1')}{\Longrightarrow} v$.

The claim is established. ■

Case 2 is now immediately settled. Every class modulo γ_θ contains positive words, by adding $\overline{(13')}$ to any word of $\mathbb{Z}^4$, a sufficient number of times. And any positive word reduces to a unique word in R_θ, using reductions in $(\mathcal{S} + \mathcal{T})$.

Two words f and g of R_θ are congruent modulo γ_θ if and only if $f \overset{*}{\leftrightarrow} g$, that is, if and only if there exists between f and g a path Σ consisting of reductions of $(\mathcal{S})$ taken in either directions. As in Case 1, this path Σ can be "lifted" into a *positive path* Π by using the same reduction (13') as before. Since we can use that reduction, the actual value of f has not to be taken into consideration — in other words, Lemma 3 becomes trivial — and the lifting is even simpler than in Case 1.

By construction, the path Π consists of reductions of $(\mathcal{S} + \mathcal{T})$. By Claims 6 and 7, two distincts words of R_θ cannot be joined by such a path, hence $f = g$.

And this completes the proof of Theorem 1. ■

Acknowledgements

We were fixing the last details of this paper when we learn the passing away of our friend David Klarner. David was the editor who read the first version of our work on the translation from the Fibonacci system to the golden mean base by a finite automaton. His advice and enthusiastic encouragement were of great help to us for giving the final shape to our result. We sorrowfully dedicate this subsequent work to his memory.

References

[1] A. Bertrand-Mathis, Développement en base de Pisot et répartition modulo 1. *C. R. Acad. Sci. Paris Sér. A* **285** (1977), 419–421.

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

[3] Č. Burdík, Ch. Frougny, J.-P. Gazeau, and R. Krejcar, Beta-integers as natural counting systems for quasicrystals. *J. Phys. A: Math. Gen.* **31** (1998), 6449–6472.

[4] N. Dershowitz and J.-P. Jouannaud, Rewrite Systems, in *Handbook of Theoretical Computer Science* (J. van Leeuwen, ed.), Vol. B, Elsevier, 1990, 243–320.

[5] A.S. Fraenkel, Systems of numeration. *Amer. Math. Monthly* **92(2)** (1985), 105–114.

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

[7] Ch. Frougny and J. Sakarovitch, A rewrite system associated with quadratic Pisot units. In *Proceedings of Rewriting Techniques and Applications'99*, Trento, Lecture Notes in Computer Science **1641** (1999), 356–370.

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

[9] D. E. Knuth, *The Art of Computer Programming*, Vol. 1, Addison-Wesley, 1968.

[10] D. Lind and B. Marcus, *An Introduction to Symbolic Dynamics*, Cambridge University Press, 1995.

[11] W. Parry, On the β-expansions of real numbers. *Acta Math. Acad. Sci. Hungar.* **11** (1960), 401–416.

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

[13] N. Sidorov and A. Vershik, Bijective arithmetic codings of hyperbolic automorphisms of the 2-torus, and binary quadratic forms. *J. Dynam. Control Systems* **4** (1998), 365–399.

[14] N. Sidorov, An arithmetic group associated with a Pisot unit and its symbolic-dynamical representation. *Acta Arithm.*, to appear, available at `http://www.arxiv.org/abs/math.NT/9912194`.

[15] E. Zeckendorf, Représentation des nombres naturels par une somme de nombres de Fibonacci ou de nombre de Lucas, *Bull. Soc. Roy. Liège* **41** (1972), 179–182.