Functiones et Approximatio
47.2 (2012), 207–231
doi: 10.7169/facm/2012.47.2.6

CIRCULAR WORDS AND THREE APPLICATIONS: FACTORS OF THE FIBONACCI WORD, $\mathcal{F}$-ADIC NUMBERS, AND THE SEQUENCE 1, 5, 16, 45, 121, 320,...

Benoît Rittaud, Laurent Vivier

Abstract: We introduce the notion of *circular words* with a combinatorial constraint derived from the Zeckendorf (Fibonacci) numeration system, and get explicit group structures for these words. As a first application, we establish a new result on factors of the Fibonacci word *abaababaabaab*... Second, we present an expression of the sequence A004146 of [Sloane] in terms of a product of expressions involving roots of unity. Third, we consider the equivalent of p-adic numbers that arise by the use of the numeration system defined by the Fibonacci sequence instead of the usual numeration system in base p. Among such $\mathcal{F}$*-adic numbers*, we give a characterization of the subset of those which are *rational* (that is: a root of an equation of the form $qX = p$, for integral values of p and q) by a periodicity property. Eventually, with the help of circular words, we give a complete description of the set of roots of $qX = p$, showing in particular that it contains exactly q $\mathcal{F}$-adic elements.

Keywords: Fibonacci numeration system, words, Fibonacci substitution, adic representation.

Classically, a (finite) *word* is a finite sequence of elements (or *letters*) of a given set, the *alphabet*. Here, we mean by *circular word* a finite word $w_0 \dots w_n$ in which the last letter, w_n, is assumed to be followed by the first one, w_0. This definition gives rise to interesting properties when circular words are assumed to be *admissible*, that is, made of letters in the alphabet $\{0, 1\}$ without any two successive letters equal to 1. These properties derive from an underlying algebraic structure: the set of admissible circular words of fixed even length is an abelian group, which can be explicitely written as a product of finite monogenetic groups. Some previous works with links to this notion mainly adopted a dynamical point of view ([Sch], [S],[SV]), whereas we consider here only number-theoretic aspects. In [FS], investigating the links between the two natural representation of integers given by a Pisot number, Christiane Frougny and Jacques Sakarovitch dealt with circular words of length 4 and some groups associated with automatas.

2010 Mathematics Subject Classification: primary: 68R15; secondary: 11A63, 11E95, 37B10

One of the properties of circular admissible words of length 2ℓ is that their cardinality c_ℓ is given by the sequence A004146 of [Sloane] (which starts by 1, 5, 16, 45, 121, 320,...), which has many important combinatorial properties (see [R]). The link between this sequence and admissible circular words appears also in the sequence of determinants of a sequence of linear operators we consider for our study. This fact gives rise to a formula that expresses each element of the sequence A004146 as an explicit product of expressions of the form $1-\alpha-\alpha^2$, where α is a root of unity.

Another application of circular words is the study of factors of the Fibonacci word $M = abaababaabaab\ldots$, defined as the only fixed point of the substitution $a \mapsto ab$ and $b \mapsto a$. It appears that admissible circular words are closely linked to this word, and the underlying arithmetic on these objects allows to write the word bM in the form $A^{(1)} \ldots A^{(q)} M'$, where all the $A^{(q)}$s are of length k and contain the same number of a (and, thus, also the same number of b), where k and q are explicit (and non-trivial) numbers.

A third application of circular words deals with what we call *$\mathcal{F}$-adic numbers.* For any integer $p > 1$, the set of p-adic integers is obtained by considering the projective limit of the sequence of sets $(\mathbb{Z}/p^n\mathbb{Z})_n$. In an intuitive way, it corresponds to numbers whose "integral part" is made of infinitely many digits in base p. Such a projective limit still makes sense for other numeration systems, as for example numeration systems in non-integers bases (see [AF]). We consider here the case of the Zeckendorf numeration system [Z]: define the Fibonacci sequence $(F_n)_n$ by $F_0 = 1$, $F_1 = 2$ and $F_n = F_{n-1} + F_{n-2}$ for any $n \geqslant 2$. For any integer N, there exists a unique sequence $(w_n)_{n \geqslant 0}$ of 0s and 1s such that $w_n w_{n+1} = 0$ for any n (this property makes the sequence an *admissible* one) and such that $N = \sum_n w_n F_n$ (for a survey of numeration systems of this kind from a dynamical point of view, see [BL]). Such a sequence has the property that, for some n_0, $w_n = 0$ for all $n \geqslant n_0$. Considering a sequence $(w_n)_n$ without this latter property leads to $\mathcal{F}$-adic numbers. It is worth noting that, contrarily to the case of p-adic numbers, we do not need to consider any "fractional part" to deal with $\mathcal{F}$-adic numbers.

In [GLT], Peter Grabner, Pierre Liardet and Robert Tichy investigated $\mathcal{F}$-adic numbers and generalizations by taking a dynamical standpoint. Here, we take a number-theoretic perspective, considering the set of $\mathcal{F}$-adic numbers as a number set. We define an addition on the set of $\mathcal{F}$-adic numbers and investigate the properties of *rational* $\mathcal{F}$-adic numbers, that is, $\mathcal{F}$-adic numbers X such that, for some integers p and q, $qX = p$. Circular words, then, appear to be a natural tool to investigate such rational $\mathcal{F}$-adic numbers, since their set corresponds to the set of $\mathcal{F}$-adic numbers whose expansion is ultimately periodic. The proof involves tools from algebra and combinatorics on words. As an application of circular words, together with the use of some more algebra, we show that the equation $qX = p$ (with X $\mathcal{F}$-adic number and p, q integers) has q or $(q+1)$ $\mathcal{F}$-adic roots, depending only on whether p/q is an integer or not.

Of course, it would be possible to consider other constraints on circular words or $\mathcal{F}$-adic numbers than the Zeckendorf one. We will not address here a general theory, and postpone to another paper some results in some of these more general cases.

1. General definitions and notations

1.1. Words

We will make use of the classical definitions on words, that are to be found for example in [L]. Here, we consider words W on an alphabet $\mathcal{A}$ which will be always made of integral numbers (with only one exception in section 3.1). We usually write words in the form $W = w_0 \dots w_n = w_0^n$ for a finite word, $W = w_0^\infty = w_0 \dots w_n \dots$ for an infinite word (note that the set of indices always starts at 0), where the w_is are the letters. The notation $\varnothing$ stands for the empty word. Recall that $|W|$ is the length of W, $|W|_a$ is the number of occurrences of the letter a in W, and W_n is the prefix of length n of the word W, with the convention $W_0 := \varnothing$.

For $W = w_0^n$, we put $\Sigma(W) := \sum_{i=0}^n w_i = \sum_{a\in\mathcal{A}} a|W|_a$.

As usual, the concatenation of W and W' (for W finite) is written WW', and we put $W^n := WW^{n-1}$ (with $W^0 = \varnothing$) and W^∞ (resp. VW^∞) for the periodic (resp. ultimately periodic) infinite word of period W. Frequently in the sequel, a finite word W of length ℓ will have to be considered as a word of length $\ell + \ell'$, or even as an infinite word of period 0, by identifying W with $W0^{\ell'}$ or $W0^\infty$.

Let $W := w_0^n$ and $W' := {w'}_0^{n'}$ be two words with (without loss of generality) $n \geqslant n'$ (with n and n' possibly infinite). The sum $W + W'$ is the word such that its i-th letter is $w_i + w'_i$ for i from 0 to n (the letter w'_i for $i > n'$ being defined as 0, identifying W with $W0^{n'-n}$ as said previously).

1.2. Admissible words

A word $W = w_0^n$ or w_0^∞ on the alphabet $\{0, 1\}$ is *admissible* iff $w_i w_{i+1} \neq 11$ for any i.

We define $(F_n)_n$ as the following *Fibonacci sequence*: $F_0 = 1$, $F_1 = 2$ and, for any $n \geqslant 2$, $F_n := F_{n-1} + F_{n-2}$. The *Zeckendorf numeration system* is the function that associates to each nonnegative integer k the only finite admissible word $Z(k) = w_0^{n(k)}$ satisfying $k = \sum_{i=0}^{n(k)} w_i F_i$ with $w_{n(k)} = 1$. A classical result asserts that the word $Z(k)$ is obtained by the natural greedy algorithm, and that Z is one-to-one from the set of nonnegative integers to the set of finite admissible words ending with a 1. The reciprocal function of Z is written N.

Two finite words $W := w_0^n$ and $W' := {w'}_0^{n'}$ on the alphabet $\mathbb{N}$ are *equivalent* iff $\sum_i w_i F_i = \sum_i w'_i F_i$. We write $W \equiv W'$ in this case. What precedes indicates that to any finite word W corresponds a unique admissible word equivalent to it, again written $Z(W)$. For infinite words W and W', we write $W \equiv W'$ iff there exists two finite words X and X' and an infinite word Y such that $X \equiv X'$, $W = XY$ and $W' = X'Y$.

For any finite admissible word V, we write $\overline{V}$ for the unique finite admissible word such that $Z(V+\overline{V}) = 0^{|V|}1$. (Of course, we cannot use the identification of V and $V0^n$ when considering $\overline{V}$.)

Let W be a word on the alphabet $\{0,1\}$, finite or infinite, different from the null sequence. The *valuation* of W is the value

$$\mathrm{Val}(W) := \min(n \geqslant 0 : W_n \neq 0^n).$$

Define the following transformations on words $W = w_0^n$ on the alphabet $\mathbb{N}$:

$$\tau_1(W) : \begin{cases} w_0 := w_0 - 2, \\ w_1 := w_1 + 1, \\ w_i \text{ unchanged for } i \geqslant 2; \end{cases}$$

and, for $k \geqslant 2$:

$$\tau_k(W) : \begin{cases} w_k := w_k + 1, \\ w_{k-1} := w_{k-1} - 1, \\ w_{k-2} := w_{k-2} - 1, \\ w_i \text{ unchanged for } i \notin \{k-2, k-1, k\}. \end{cases}$$

Let $W := w_0^n$ be an admissible word, and let $m \geqslant 0$. The following reduction algorithm takes W and m as input, and returns $W := Z(W + 0^m1)$ as an output (the proof is a routine):

```
• Initialization: put $w_m := w_m + 1$, and $i := m$;
• while $w_i = 2$ and $i \geqslant 1$, do
    – put $W := \tau_{i+1} \circ \tau_i^{-1}(W)$;
    – put $i := i - 2$;
• if $w_0 = 2$ then put $w_0 w_1 := 01$;
• while $E := \{k : w_{k-1}w_{k-2} = 11\}$ is non empty, do
    – put $i := \max(E)$;
    – put $W := \tau_i(W)$.
```

We will very often make implicit use of the following result:

Proposition 1.1. *[Ultimate stationnarity principle] For any finite word W on the alphabet $\mathbb{N}$ there exists a finite admissible word $A(W)$ and a value $a(W) \geqslant 0$ such that, for any $n \geqslant a(W)$, we have $Z(0^nW) = 0^{n-a(W)}A(W)$.*

Proof. Assume that the ultimate stationnarity principle is true for any word W such that $\Sigma(W) \leqslant j$ for some j, and consider a word W such that $\Sigma(W) = j+1$. We find $m \geqslant 0$ such that $W = W' + 0^m1$, where W' is a word on $\mathbb{N}$. By induction hypothesis, for some admissible word $A = A(W')$ and some $a = a(W') \geqslant 0$, for any $n \geqslant a$, we have $Z(0^nW') = 0^{n-a}A$. Hence, we have $Z(0^nW) = Z(0^{n-a}A + 0^{m+n}1)$.

Observe that, for any finite word W, any $i \geqslant 2$ and any $m \geqslant 0$, we have $\tau_{i+m}(0^m W) = 0^m \tau_i(W)$, so the ultimate stationnary principle is true for the finite word W iff it is true for $\tau_i(W)$ $(i \geqslant 2)$. Hence, if, in the execution of the previous reduction algorithm (when applied to the word $0^{n-a}A$ and the value $m+n$), we always get $i \geqslant 2$, then the proposition is true for W.

The case for which the algorithm leads to $i = \varepsilon \in \{0,1\}$ is when we get this equality just after the end of the iteration of the first while loop. A simple verification shows that this occurs only if $0^{n-a}A+0^{m+n}1$ is of the form $0^{\varepsilon}(10)^k 20X$ with X admissible and $k \geqslant 0$. We hence have $0^{(n+2)-a}A + 0^{m+(n+2)}1$ of the form $0^{2+\varepsilon}(10)^k 20X$, for which the reduction algorithm does never leads to $w_0 = 2$ or $w_1 = 2$. We thus have proved that $a(W) \leqslant a(W') + 2$. ■

Lemma 1.1. *If W and W' are finite admissible words, then* $\mathrm{Val}(Z(WW')) \geqslant \mathrm{Val}(W)$*. Moreover,* $\mathrm{Val}(Z(WW')) > \mathrm{Val}(W)$ *iff $W = 0^n1$ for some $n \geqslant 0$ and* $\mathrm{Val}(W') = 0$.

Proof. Immediate. ■

Lemma 1.2. *Let V and V' be two finite admissible words. We have $|Z(V+V')| \leqslant 2 + \max(|V|, |V'|)$.*

Proof. Since V and V' are admissible, we have $N(V) < F_{|V|}$ and $N(V') < F_{|V'|}$, so, assuming without loss of generality that $|V| \geqslant |V'|$, we get $N(V + V') \leqslant 2(F_{|V|} - 1) < F_{|V|+2}$, so we get the lemma. ■

Lemma 1.3. *Let W be a finite word on the alphabet $\{0,1\}$. We have* $\mathrm{Val}(Z(W)) \geqslant \mathrm{Val}(W)$*. Moreover,* $\mathrm{Val}(Z(W)) - \mathrm{Val}(W)$ *is even.*

Proof. To get $Z(W)$ from W, we can apply the second loop of the previous algorithm. Each time we apply some τ_i, the valuation either remains constant or increases by two units, so we get the result. ■

Proposition 1.2. *Let W be a finite admissible word such that* $\mathrm{Val}(W) \geqslant 2$*, let $m \geqslant 2$. There exists an integer $n \geqslant -1$ such that* $\mathrm{Val}(Z(W+0^m1)) = \mathrm{Val}(W)+2n$*. Moreover, $n = -1$ iff $W + 0^m1$ is of the form $0^r(10)^s 20W'$ with W' admissible.*

Proof. For any $i \geqslant 2$, $\mathrm{Val}(\tau_i(W))$ is equal either to $\mathrm{Val}(W)$ or to $\mathrm{Val}(W) + 2$ (and, so, $\mathrm{Val}(\tau_i^{-1}(W))$ equal either to $\mathrm{Val}(W)$ or to $\mathrm{Val}(W) - 2$). By the previous algorithm, we then get that $\mathrm{Val}(Z(W + 0^m1)) \in \mathrm{Val}(W) + 2\mathbb{Z}$. The inequality $\mathrm{Val}(Z(W + 0^m1)) < \mathrm{Val}(W)$ can occur only if we need to go into the first loop of the algorithm, to apply some τ_i^{-1}. Consider the first iteration of this loop for which the valuation of W decreases (of two units). This means that, at that moment of the algorithm, W is of the form $0^u20W'$ (with W' a word on $\{0,1\}$) and becomes $0^{u-2}1001W'$. There is then no letter 2 anymore, and the iteration of the second loop will only involve the part $1W'$ of the word and will not change the valuation. Hence, we have proved that $n \geqslant -1$.

Finally, if $\mathrm{Val}(Z(W+0^m1)) = \mathrm{Val}(W) - 2$, then we must have went through the first loop to get the form $0^u20W'$; a simple induction shows that this forces $W + 0^m1$ to be of the required form. ■

Corollary 1.4. *Let W and W' be two finite admissible words such that $m := \min(\mathrm{Val}(W), \mathrm{Val}(W')) \geqslant 2$. There exists an integer $i \geqslant -1$ such that $\mathrm{Val}(Z(W+W')) = m + 2i$. Moreover, we have*

$$\mathrm{Val}(Z(W+W')) = m - 2 \Longleftrightarrow W + W' = 0^m(10)^n 20(U+U')$$

where $n \geqslant 0$ and U (resp. U') is the suffix of W (resp. of W') of length $\max(0, |W| - (m+2n+2))$ (resp. $\max(0, |W'| - (m+2n+2))$).

The proof is left as an exercice.

2. Circular words

2.1. Generalities

A finite word $W := w_0^n$ being given (on some alphabet), we denote by $\sigma(W)$ the word $w_1 \dots w_n w_0$. Define the *circular equivalence* $\approx$ between finite words by:

$$W \approx W' \Longleftrightarrow \sigma^k(W) = W' \quad \text{for some } k.$$

A *circular word* is an ordered set of the form $[W, \sigma(W), \dots, \sigma^{|W|-1}(W)]$, for a chosen finite word W. For any finite word W, we denote by $\widetilde{W}$ the circular word containing W as a first element. Its *length*, $|\widetilde{W}|$, is defined as the length of W. A circular word is a *power* if we can write it of the form $\widetilde{X^k}$ for some word X and some integer $k > 1$. It is *primitive* if it is not a power. A circular word $\widetilde{W} := \widetilde{w_0^n}$ on the alphabet $\{0,1\}$ is *admissible* if $w_{i \bmod (n+1)} w_{(i+1) \bmod (n+1)} \neq 11$ for any i.

For $\widetilde{W}$ and $\widetilde{W'}$ two circular words, we put $\widetilde{W}\widetilde{W'} := \widetilde{WW'}$.

We define the transformations $\tilde{\tau}_i$ on circular words $\widetilde{W}$ on the alphabet $\mathbb{N}$ and of length at least 3 (with $W = w_0^{|W|-1}$) by $\tilde{\tau}_i(\widetilde{W}) = \widetilde{W'}$, where $W' = {w'}_0^{|W|-1}$ is defined by:

$$w'_j := \begin{cases} w_{i \bmod |W|} + 1 & \text{for } j = i \bmod |W|; \\ w_{(i-1) \bmod |W|} - 1 & \text{for } j = (i-1) \bmod |W|; \\ w_{(i-2) \bmod |W|} - 1 & \text{for } j = (i-2) \bmod |W|; \\ w_j & \text{for any other } j. \end{cases}$$

For $\widetilde{W}$ and $\widetilde{W'}$ belonging to the same orbit under the τ_is, we write $\widetilde{W} \equiv \widetilde{W'}$ and say that these words are *equivalent*.

For any circular word $\widetilde{W}$, we define $\tilde{N}(\widetilde{W}) := N(W)$.

Proposition 2.1. *Let $\widetilde{W}$ be a circular word on $\mathbb{N}$ of length at least 2 and not equivalent to 1^{2n+3} $(n \geqslant 0)$. There exists a unique admissible circular word $\tilde{Z}(\widetilde{W})$ equivalent to $\widetilde{W}$, assuming the identification $\widetilde{(01)}^n = \widetilde{(10)}^n$ for any n.*

If $\widetilde{W} = 1^{2n+3}$, then its orbit under the τ_is does not contains any admissible circular word.

Proof. We start by the existence. Assume $\widetilde{W}$ contains only 0s and 1s. If it does contains at least one 0, then we write W as a circular concatenation of subwords of the form 10^k (with $k > 1$), 1^k0^n (with $k > 1$ and $n \geqslant 1$) and $(10)^n$ (with $n \geqslant 1$), possibly adding the prefix 0^k (with $k \geqslant 1$). We then make use of the τ_is to reduce each 1^k0^n either into $0(01)^{k/2}0^{n-1}$ (for k even) or into $10(01)^{(k-1)/2}0^{n-1}$ (for k odd). Such an operation makes the number of 1s becoming strictly less, so its iteration eventually ends, and leads to a circular word with only 0s and 1s and free of any factor of the form 11, so an admissible word. If $\widetilde{W} = 1^{2\ell}$, then we have $\tau_0 \circ \tau_2 \circ \cdots \circ \tau_{2(\ell-1)}(\widetilde{W}) = (10)^\ell$; note that we also have $\tau_1 \circ \tau_3 \circ \cdots \circ \tau_{2\ell-1}(\widetilde{W}) = (01)^\ell$, which justifies the identification $\widetilde{(01)}^n = \widetilde{(10)}^n$.

Now, let $\widetilde{W}$ be admissible and consider $\widetilde{W} + 0^{i-1}10^{i-|\widetilde{W}|}$ for some $i > 0$. This latter word is either on $\{0,1\}$ (then we are done, by what precedes), or on $\{0,1,2\}$ with exactly one 2, surrounded by two 0s, and nowhere the factor 11. The rank of the letter 2 is i. Apply $\tau_{i+1} \circ \tau_i^{-1}$ (from now, all the indices are to be understood modulo $|\widetilde{W}|$). The factor $w_{i-2}020$ of $\widetilde{W}$ is then replaced by $(w_{i-2}+1)001$. If $w_{i-2} = 0$, then we are back to a word on $\{0,1\}$ and we are done. Otherwise, we iterate the same process at the rank $i-2$, then $i-4$, etc., until we get a word on $\{0,1\}$ (so we are done) or we get a 2 at the rank $i+1$. In this latter case, we get that $\widetilde{W} + 0^{i-1}10^{|\widetilde{W}|-i}$ is of the form $\widetilde{(10)^n200}$, which is equivalent to 1^{2n+3}. Then, for any value j, we have $\widetilde{W} + 0^{i-1}10^{|\widetilde{W}|-i} + 0^{j-1}10^{|\widetilde{W}|-j} \equiv 1^{j-1}21^{|\widetilde{W}|-j} \equiv 0^{j-3}10^{|\widetilde{W}|-(j+2)}$, which is admissible.

Hence, iterating the process of adding words of the form $0^{i-1}10^{|\widetilde{W}|-i}$ and reducing the result either leads to an admissible word or leads to 1^{2n+3}; this gives us the existence part of the proposition.

Now, let us consider the unicity part.

Lemma 2.1. *The circular word 0^ℓ is equivalent to no other circular word on $\mathbb{N}$.*

Proof. Let W be a finite word on $\mathbb{N}$ with $W = w_0^n$ containing at least one letter different from 0. For any τ_i or τ_i^{-1} that can be applied to $\widetilde{W}$, the number of letters different from 0 cannot become null, so we are done. ■

Let $\widetilde{W}$ and $\widetilde{X}$ be two equivalent admissible circular words of length $n+1$. Regardless of the negative values possibly involved in the following expression, write $\widetilde{X} = \tilde{\tau}_0^{a_0} \circ \cdots \circ \tilde{\tau}_n^{a_n}(\widetilde{W})$, with integer values for all the a_is. Write A for the vector $(a_i)_{0 \leqslant i \leqslant n}$ and define the linear operator $M = (m_{ij})_{i,j}$ on $\mathbb{R}^{n+1}$ by $m_{i,i} = 1$, $m_{i,((i+1) \bmod (n+1))} = -1$ and $m_{i,((i+2) \bmod (n+1))} = -1$ for any $0 \leqslant i \leqslant n$.

Lemma 2.2. *For any i, we have $-1 \leqslant a_i \leqslant 1$.*

Proof. For any i, we have $x_i = w_i + (MA)_i$. Hence, since w_i and x_i are equal to 0 or 1, we have $-1 \leqslant (MA)_i \leqslant 1$ for any i. Moreover, since $x_i x_{i+1} \neq 11$, we have $(MA)_i = 1 \Rightarrow (MA)_{i+1} \leqslant 0$ and, since $w_i w_{i+1} \neq 11$, we have $(MA)_i = -1 \Rightarrow (MA)_{i+1} \geqslant 0$ (in the present proof, all the indices are to be understood mod $n+1$).

Without loss of generality, assume $a_0 =: a = \|A\|_\infty$. We write $MA =: B := (b_i)_{i=0}^n$. The inequalities $|a - a_1 - a_2| = |b_0| \leqslant 1$, $|a_1| \leqslant a$ and $|a_2| \leqslant a$ implies $|a_1| \geqslant -1$. The inequalities $|a_n - a - a_1| = |b_n| \leqslant 1$, $|a_n| \leqslant a$ and $|a_1| \leqslant a$ implies $a_1 \leqslant 1$. If $a_1 = 1$, then $b_n = a_n - (a+1)$, so, since $b_n \geqslant -1$, we get $a_n = a$. Hence, since $a_{n-1} \leqslant a$, we get $b_{n-1} = a_{n-1} - a_n - a = a_{n-1} - 2a \leqslant -a < -1$, which is forbidden. If $a_1 = 0$, then $|b_n| = a_n - a$, so $a_n = a$ or $a - 1$. If $a_n = a$, then $b_{n-1} = a_{n-1} - 2a \leqslant -a < -1$, a contradiction. Hence, $a_n = a - 1$, which gives $b_n = -1$ and $b_{n-1} = a_{n-1} - 2a + 1 < 0$, also a contradiction.

Therefore, we have proved that $a_0 = a = \|A\|_\infty$ implies $a_1 = -1$. Hence, $b_1 = a + 1 - a_2$, so $a_2 = a$. By induction, we then get that $a_{2i+1} = -1$ and $a_{2i} = a$ for any i, so $b_1 = a_1 - a_2 - a_3 = -a < -1$, a contradiction, and the lemma is proved. ■

Lemma 2.3. *Let $\widetilde{W}$ be a circular word of length $n > 3$ on $\mathbb{N}$. For any i, we have*

$$N(\tilde{\tau}_i(\widetilde{W})) = \begin{cases} N(\widetilde{W}) & \text{for } 2 \leqslant i \leqslant n; \\ N(\widetilde{W}) + 1 - F_n & \text{for } i = 1; \\ N(\widetilde{W}) + 1 - F_{n+1} & \text{for } i = 0. \end{cases}$$

Proof. Simple verification. ■

By Lemma 2.3, there exists two integers a_0 and a_1 such that $N(\widetilde{W}) = N(\widetilde{X}) + a_0(1 - F_{n+1}) + a_1(1 - F_n)$. By Lemma 2.2, we also have $\max(|a_0|, |a_1|) \leqslant 1$. Without loss of generality, we assume $N(\widetilde{W}) \leqslant N(\widetilde{X})$. Recall also that both $N(\widetilde{W})$ and $N(\widetilde{X})$ are upper-bounded by $F_{n+1} - 1$. All these conditions can be satisfied only in the following cases: $(a_0, a_1) = (0, -1)$, $(-1, 0)$, $(0, 0)$ and $(-1, 1)$.

The case $(a_0, a_1) = (0, 0)$ gives $N(\widetilde{W}) = N(\widetilde{X})$, that is $N(W) = N(X)$, which implies $W = X$ by unicity of the Zeckendorf expansion. For $(a_0, a_1) = (-1, 0)$, we get $N(\widetilde{X}) - N(\widetilde{W}) = F_{n+1} - 1$, so $W = 0^{n+1}$ and X is of the form $\ldots 01010101$ (which implies that n is even, otherwise $\widetilde{X}$ would not be admissible). By Lemma 2.1, $\widetilde{W}$ and $\widetilde{X}$ are not equivalent. For $(a_0, a_1) = (-1, 1)$, the condition $-1 \leqslant (MA)_i \leqslant 1$ for all i gives by a simple induction that $a_i = (-1)^{i+1}$ for all i. This gives that $x_i = w_i + (-1)^{i+1}$ for any i, so $W = (10)^{(n+1)/2}$ and $X = (01)^{(n+1)/2}$.

The last remaining case is $(a_0, a_1) = (0, -1)$, for which we have $N(\widetilde{X}) - N(\widetilde{W}) = F_n - 1$. Extending the definition of the $\tilde{\tau}_i$s to circular words on $\mathbb{Z}$

makes the τ_is commuting, so we can write $\tilde{\tau}_0^{a_0} \circ \cdots \circ \tilde{\tau}_n^{a_n}(\widetilde{W}) = \widetilde{X}$, and we can apply the $\tilde{\tau}_i$s in any order. Since $a_0 = 0$ and $a_1 = -1$, we get

$$\widetilde{X} = \tilde{\tau}_2^{a_2} \circ \cdots \circ \tilde{\tau}_n^{a_n}((w_0+1)(w_1-1)w_2 \ldots w_{n-1}(w_n+1)) \tag{2.1}$$

(in which we write circular words as classical words). Note that, for any i, the only values j for which the application of $\tilde{\tau}_j$ changes the letter of rank i are $j = i$, $i+1$ and $i+2 \bmod (n+1)$. Hence, if $w_0 = 1$ (so $w_1 = 0$), then Equation (2.1) forces $a_2 = 1$, which gives

$$\widetilde{X} = \tilde{\tau}_3^{a_3} \circ \cdots \circ \tilde{\tau}_n^{a_n}(1(-2)(w_2+1)w_3 \ldots w_{n-1}(w_n+1)).$$

The value -2 at the rank number 1 cannot become 0 or 1 with the remaining $\tilde{\tau}_i$s, since only the operation $\tilde{\tau}_3^{a_3}$ can change its value, adding at most 1 to it. Hence, we cannot have $w_0 = 1$, so $w_0 = 0$. Thus, we have

$$\widetilde{X} = \tilde{\tau}_2^{a_2} \circ \cdots \circ \tilde{\tau}_n^{a_n}(1(w_1-1)w_2 \ldots w_{n-1}(w_n+1)). \tag{2.2}$$

Since the latter word starts with a 1 and ends with $w_n + 1 \geqslant 1$, and since the only operation that can still be used to avoid these two successive (circularily) positive letters is $\tilde{\tau}_n^{-1}$, we have $a_n = -1$, and:

$$\widetilde{X} = \tilde{\tau}_2^{a_2} \circ \cdots \circ \tilde{\tau}_{n-1}^{a_{n-1}}(1(w_1-1)w_2 \ldots w_{n-3}(w_{n-2}+1)(w_{n-1}+1)w_n). \tag{2.3}$$

The admissibility condition then gives that $w_n = 0$. If $w_{n-1} = 1$ (then $w_{n-2} = 0$), then a simple checking show that no pair (a_{n-2}, a_{n-1}) of numbers among -1, 0 and 1 can transform this part of the word into an admissible word (and the $\tilde{\tau}_i$ for $i < n-2$ are of no effect on this part of the word). Hence, we must have $w_{n-1} = 0$.

Now, if $w_{n-2} = 1$, then $(w_{n-2}+1)(w_{n-1}+1)w_n = 210$ and, again, a checking shows that no pair (a_{n-2}, a_{n-1}) of numbers among -1, 0 and 1 can transform this part of the word into an admissible word. Hence, $w_{n-2} = 0$, so $(w_{n-2}+1)$ $(w_{n-1}+1)w_n = 110$. Thus, we cannot have $a_{n-1} = 1$. If $a_{n-1} = -1$, then

$$\widetilde{X} = \tilde{\tau}_2^{a_2} \circ \cdots \circ \tilde{\tau}_{n-2}^{a_{n-2}}(1(w_1-1)w_2 \ldots w_{n-4}(w_{n-3}+1)200), \tag{2.4}$$

which leads to the same problem that appeared previously. Hence, $a_{n-1} = 0$, so $a_{n-2} = -1$ and

$$\widetilde{X} = \tilde{\tau}_2^{a_2} \circ \cdots \circ \tilde{\tau}_{n-3}^{a_{n-3}}(1(w_1-1)w_2 \ldots w_{n-5}(w_{n-4}+1)(w_{n-3}+1)010). \tag{2.5}$$

Iterating the reasoning eventually leads to:

$$\widetilde{X} = \begin{cases} \tilde{\tau}_2^{a_2}\tilde{\tau}_3^{a_3}(1(w_1-1)(w_2+1)(w_3+1)01010\ldots1010) & \text{if } n \text{ is even;} \\ \tilde{\tau}_2^{a_2}\tilde{\tau}_3^{a_3}\tilde{\tau}_4^{a_4}(1(w_1-1)w_2(w_3+1)(w_4+1)01010\ldots1010) & \text{if } n \text{ is odd,} \end{cases}$$

with $w_i = 0$ for all $i \geqslant 4$ for n odd and all $i \geqslant 5$ for n even.

Take n even. By the same kind of reasoning, we successively get $w_3 = 0$, then $w_2 = 0$, so $1(w_1 - 1)(w_2 + 1)(w_3 + 1) = 1(w_1 - 1)11$. A check then shows that no pair (a_2, a_3) can give an admissible circular word in the right hand side of the previous equality.

Now, consider the case n odd. We also get successively $w_4 = 0$, then $w_3 = 0$, then $a_4 = 0$, then $a_3 = -1$, then $a_2 = 0$, then $w_2 = 0$ and finally $w_1 = 0$, so $W = 0^{|W|}$ and $X = (01)^{(n+1)/2}$, a contradiction with Lemma 2.1. Hence, the unicity is proved.

Finally, let us consider the case $\widetilde{W} = \widetilde{1^{2n+3}}$. Assume that $\widetilde{1^{2n+3}} \equiv \widetilde{X}$, where $\widetilde{X}$ is admissible, and write $\widetilde{X} = \tilde{\tau}_0^{a_0} \circ \cdots \tilde{\tau}_{2n+2}^{a_{2n+2}}(\widetilde{1^{2n+3}})$. Since $\widetilde{1^{2n+3}}$ is invariant under σ, the words $\sigma^k(\widetilde{X})$ are admissible and equivalent circular words for any k. Moreover, since X is not of the form x^{2n+3} ($x = 1$ would give a non-admissible word, and $x = 0$ would contradict Lemma 2.1), the set $\{\sigma^k(\widetilde{X}) : k \geqslant 0\}$ has cardinality at least two, a fact which contradicts the unicity we just proved. ■

2.2. Group structures

We define the operation $\oplus$ between circular admissible words of the same even length, $\widetilde{W}$ and $\widetilde{W'}$, by: $\widetilde{W} \oplus \widetilde{W'} := \widetilde{Z}(\widetilde{W} + \widetilde{W'})$. We will also write, for any $n \geqslant 1$, $n \cdot \widetilde{W} := ((n-1) \cdot \widetilde{W}) \oplus \widetilde{W}$, with $0 \cdot \widetilde{W} := (01)^{|W|/2}$.

Theorem 2.4. *Define the sequences $(c_\ell)_{\ell \geqslant 1}$ and $(d_\ell)_{\ell \geqslant 1}$ by:*

$$c_1 := 1 \qquad c_\ell := F_{2\ell-1} + F_{2\ell-3} - 2 \quad \text{for } \ell \geqslant 2;$$

$$d_1 := 1 \qquad d_\ell := \begin{cases} F_{\ell-2} & \text{if } \ell > 1 \text{ is even;} \\ F_{\ell-1} + F_{\ell-3} & \text{if } \ell > 1 \text{ is odd.} \end{cases}$$

For any $n \geqslant 1$, we have $c_{2k+1} = d_{2k+1}^2$ and $c_{2k} = 5d_{2k}^2$.

The set $\mathcal{G}_\ell^*$ of circular admissible words of length 2ℓ excluding $\widetilde{0^{2\ell}}$ and with the identification $\widetilde{(01)^\ell} = \widetilde{(10)^\ell}$ is an abelian group for the addition $\oplus$, with $\widetilde{(01)^\ell} = \widetilde{(10)^\ell}$ as identity element. More precisely, this group has cardinality c_ℓ and is isomorphic to $(\mathbb{Z}/d_\ell\mathbb{Z})^2$ for odd ℓ, and isomorphic to $(\mathbb{Z}/5d_\ell\mathbb{Z}) \times (\mathbb{Z}/d_\ell\mathbb{Z})$ for even ℓ.

The star $*$ is here to recall that the word $0^{2\ell}$ is *not* considered (in particular, it is not the identity element).

It is worth noting that the sequence $(c_\ell)_\ell$ defined in Theorem 2.4 possesses numerous combinatorial properties (see [R]); it corresponds to the integer sequence A004146 in [Sloane].

Proof. The relations $c_{2k+1} = d_{2k+1}^2$ and $c_{2k} = 5d_{2k}^2$ are trivial consequences of the classical Binet formula $F_n = (\varphi^{n+2} - \overline{\varphi}^{n+2})/\sqrt{5}$ for any n (where $\varphi = (1 + \sqrt{5})/2$ and $\overline{\varphi} = (1 - \sqrt{5})/2$).

By Lemma 2.1, if $\widetilde{W}$ and $\widetilde{W'}$ are elements of $\mathcal{G}_\ell^*$, then $\widetilde{W}\oplus\widetilde{W'}$ is also an element of $\mathcal{G}_\ell^*$ (that is: $\widetilde{W}\oplus\widetilde{W'}\neq\widetilde{0^{2\ell}}$), so $\oplus$ is well-defined in $\mathcal{G}_\ell^*$.

Observe that any element of $\mathcal{G}_\ell^*$ can be written as a (unique and finite) sum (in the usual sense) of words of the form $0^k\widetilde{10^{2\ell-k-1}}$. To prove that $\widetilde{(01)}^\ell = \widetilde{(10)}^\ell$ is the identity element, by the associativity (and commutativity) of $\oplus$, it is therefore enough to show that $0^k\widetilde{10^{2\ell-k-1}} \oplus \widetilde{(10)}^\ell = 0^k\widetilde{10^{2\ell-k-1}} \oplus \widetilde{(01)}^\ell = 0^k\widetilde{10^{2\ell-k-1}}$, and these latter equalities are obtained by straightforward computations. Also, since $0^{2k}\widetilde{10^{2(\ell-k)-1}}$ (resp. $0^{2k+1}\widetilde{10^{2(\ell-k-1)}}$) admits $(10)^k\widetilde{00(10)}^{\ell-k-1}$ (resp. $(01)^k\widetilde{00(10)}^{\ell-k-1}$) as an opposite element, we obtain that $\mathcal{G}_\ell^*$ is an abelian group for $\oplus$.

Now, let us consider the cardinality of $\mathcal{G}_\ell^*$. We first count the number of admissible words of length 2ℓ, excluding those which starts and ends with a 1. We split this latter set in two subset: the first one is made of words not ending with a 1, its cardinality is equal to $1 + N(1(01)^{\ell-1}) = F_{2\ell-1}$. The second one is made of words ending with 01 and starting with a 0, its cardinality is equal to the cardinality of admissible words of length $2\ell-3$ (by the bijection $W \longmapsto 0W01$), which is equal to $F_{2\ell-3}$. Hence, the number of admissible words of length 2ℓ not both starting and ending with a 1 is equal to $F_{2\ell-1}+F_{2\ell-3}$. To get the cardinality of $\mathcal{G}_\ell^*$, it only remains to suppress the word $0^{2\ell}$ and to identify $(01)^\ell$ with $(10)^\ell$, which eventually leads to the value c_ℓ.

To prove the end of the theorem, note first that the circular words $\widetilde{10^{2\ell-1}}$ and $\widetilde{010^{2\ell-2}}$ generate the full group $\mathcal{G}_\ell^*$. Indeed, the relation $F_{k-1}\cdot(\widetilde{10^{2\ell-1}}) + F_k \cdot (\widetilde{010^{2\ell-2}}) = 0^{k+2}10^{2\ell-k-5}$ for any $k \geqslant 0$ (with $F_{-1} := 1$) proves that the subgroup generated by these two words contains the set of words with only one 1, which obviously generates $\mathcal{G}_\ell^*$ itself. Hence, $\mathcal{G}_\ell^*$ is an abelian group generated by at most two elements.

Assume $\ell = 2k+1$. By induction, we easily get that $d_\ell = v_\ell$, where v_ℓ is defined in the proof of Lemma 4.1 (see section 4.1). By the same technique as in the proof of this lemma, we obtain that $\tilde{Z}(d_\ell\cdot(\widetilde{10^{2\ell-1}})) = (10)^\ell$. Both generators are hence of order at most d_ℓ. Hence, since $\mathcal{G}_\ell^*$ is of cardinality strictly bigger than d_ℓ, $\mathcal{G}_\ell^*$ is necessarily of the form $(\mathbb{Z}/a\mathbb{Z})\times(\mathbb{Z}/b\mathbb{Z})$ with $ab = d_\ell^2$; moreover, we must have a and b both upper-bounded by d_ℓ, so $a = b = d_\ell$.

Assume $\ell = 2k$. Again by the same kind of technique, we get this time that $\tilde{Z}(5d_\ell\cdot(\widetilde{10^{2\ell-1}})) = (10)^\ell$. Hence, $\mathcal{G}_\ell^*$ is of the form $(\mathbb{Z}/a\mathbb{Z})\times(\mathbb{Z}/b\mathbb{Z})$ with $ab = 5d_\ell^2$ and $\max(a,b) \leqslant 5d_\ell$, so we are done. ■

In passing, a simple way to find the opposite of an element $\widetilde{W} = \widetilde{w_0^{2\ell-1}}$ of $\mathcal{G}_\ell^*$ is the following (see also the proof of Theorem 4.4): define the word W' as the word whose i-th letter is equal to $1-w_i$ (for all $0 \leqslant i < 2\ell$). We then easily verify that: $-\widetilde{W} = \tilde{Z}(\widetilde{W'})$.

We can get natural embeddings between the groups $\mathcal{G}_\ell^*$ by making use of the following result.

Proposition 2.2. *Let k and ℓ be positive integers. The application $\widetilde{W} \longmapsto \widetilde{W^k}$ is a morphism from $\mathcal{G}_\ell^*$ into $\mathcal{G}_{k\ell}^*$.*

Proof. Simple verification. ■

Let $\widetilde{W}$ and $\widetilde{W'}$ be circular admissible words, non necessarily of the same length. By Proposition 2.2, we can put both $\widetilde{W}$ and $\widetilde{W'}$ in the same $\mathcal{G}_\ell^*$, by a convenient choice of k for each word. This allows us to extend the definition of the operation $\oplus$ to words $\widetilde{W}$ and $\widetilde{W'}$ of possibly different (even) lengths, in the following way:

$$\widetilde{W} \oplus \widetilde{W'} := \tilde{Z}\left(\widetilde{W^{m/|W|} + W'^{m/|W'|}}\right), \qquad \text{where } m = \mathrm{lcm}(|W|, |W'|).$$

Theorem 2.5. *For $q \geqslant 1$, let $\mathcal{P}_q^*$ be the set of circular admissible words $\widetilde{W}$ of even length, containing at least one 1 and satisfying $\widetilde{qW} = \widetilde{(01)^{|W|/2}}$. Assume also the identifications $\widetilde{(01)^n} = \widetilde{(10)^n}$ and $\widetilde{W} = \widetilde{W^n}$ for any n. The set $\mathcal{P}_q^*$ equipped with the addition $\oplus$ is an abelian group isomorphic to $(\mathbb{Z}/q\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$.*

Proof. The fact that $\mathcal{P}_q^*$ is a group for $\oplus$ is trivial. Hence, for any ℓ, the subset of $\mathcal{P}_q^*$ made of words of length 2ℓ is a subgroup of $\mathcal{G}_\ell^*$.

Lemma 2.6. *For any $q \geqslant 2$, there exists an ℓ such that q divides d_ℓ.*

Proof. Consider the sequence of pairs $(G_i, G_{i+1}) := (F_i \bmod q, F_{i+1} \bmod q)$ for all $i \geqslant 0$. Since there are finitely many pairs of integers between 0 and $q-1$, we can find two different values, i and j, such that $(G_i, G_{i+1}) = (G_j, G_{j+1})$, so the definition of the sequence implies that $(G_i, G_{i+1})_i$ is ultimately periodic. Moreover, for any pair (a, b) of integers between 0 and $q-1$, the pair $((b-a) \bmod q, a)$ is the only pair (y, z) for which there can be an i such that $(a, b) = (G_i, G_{i+1})$ and $(y, z) = (G_{i-1}, G_i)$. Hence, the sequence $(G_i, G_{i+1})_i$ is purely periodic, and we can find a value $m > 1$ such that $(G_{m+1}, G_{m+2}) = (F_0 \bmod q, F_1 \bmod q) = (1, 2)$. We then get that $(G_m, G_{m+1}) = (1, 1)$, so $(G_{m-2}, G_{m-1}) = (-1, 0)$. Therefore, if $m-1$ is even, then q divides $d_\ell := d_{m-1} = F_{m-1}$, and if $m-1$ is odd, then q divides $d_\ell := d_{m+2} = F_m + F_{m-2}$. ■

The value of q being given, we fix by Lemma 2.6 an ℓ such that q divides d_ℓ. By Theorem 2.4, the maximal subgroup $\mathcal{M}_\ell$ of elements of $\mathcal{G}_\ell^*$ of order q is $(\mathbb{Z}/q\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$.

Now, let ℓ' be another integer. Again by Theorem 2.4, in $\mathcal{G}_{\ell'}^*$, the maximal subgroup $\mathcal{M}_{\ell'}$ of elements of order q is isomorphic $(\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$, where a and b are divisors of q. Since $\ell\ell'$ divides q, we have that $\mathcal{M}_{\ell\ell'}$ is isomorphic to $(\mathbb{Z}/q\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$. By Proposition 2.2, $\mathcal{G}_{\ell'}^*$ and $\mathcal{G}_\ell^*$ are subgroups of $\mathcal{G}_{\ell\ell'}^*$, so $\mathcal{M}_\ell$ and $\mathcal{M}_{\ell'}$ are subgroups of $\mathcal{M}_{\ell\ell'}$. Since $\mathcal{M}_\ell = \mathcal{M}_{\ell\ell'}$, the result follows. ■

2.3. Size of circular words of order q, and natural generators of $\mathcal{P}_q^*$

For a given q, consider the smallest ℓ for which $\mathcal{P}_q^* \subset \mathcal{G}_\ell^*$. The value 2ℓ is denoted by $T(q)$ in the sequel. In general, the inclusion of $\mathcal{P}_q$ in $\mathcal{G}_{T(q)/2}^*$ is strict. The set of values q for which the equality arise is simply the set of q for which q^2 is equal to the cardinality of $\mathcal{G}_\ell^*$ for some ℓ. That is: q satisfies $\mathcal{P}_q^* = \mathcal{G}_\ell^*$ for some ℓ iff $q = d_{2k+1}$ for some k (and, in this case, we have $T(q) = 4k+2$). The following result gives a precise description of the function $q \longmapsto T(q)$. It also reveals the existence of two particular generators of $\mathcal{P}_q^*$, denoted by Π and Π', which are of great importance for the understanding of algebraic structures arising from circular words.

Theorem 2.7. *For any $q \geqslant 2$, the minimal value ℓ for which $\mathcal{P}_q^* \subset \mathcal{G}_\ell^*$ satisfies the formula*

$$2\ell = \min(n > 2,\ n \text{ even} : (F_n \bmod q) = (F_{n-1} \bmod q) = 1).$$

Moreover, let $\widetilde{\Pi}$ (resp. $\widetilde{\Pi'}$) be the circular word of length 2ℓ equal to $Z((F_n - 1)/q)$ (resp. $Z((F_{n-1} - 1)/q)$). We have $\widetilde{\sigma(\Pi)} = \widetilde{\Pi'}$ and, for any $0 \leqslant i \leqslant q$:

$$i \cdot \widetilde{\Pi} = \widetilde{i\Pi} \qquad \text{and} \qquad i \cdot \widetilde{\Pi'} = \widetilde{i\Pi'}.$$

The circular words $\widetilde{\Pi}$ and $\widetilde{\Pi'}$ are the only non-trivial elements of $\mathcal{P}_q^*$ satisfying this latter property.

The following part of this section is mostly devoted to the proof of this theorem. Note first that the existence, for any q, of an even value $n > 2$ such that $(F_n \bmod q) = (F_{n-1} \bmod q) = 1$ is proved in a similar way as Lemma 2.6.

Lemma 2.8. *Define the sequence $(d'_\ell)_\ell$ as:*

$$d'_1 := 1 \qquad d'_2 := 3 \qquad d'_\ell := \begin{cases} F_{\ell-1} + F_{\ell-3} & \text{if } \ell > 1 \text{ is even;} \\ F_{\ell-2} & \text{if } \ell > 1 \text{ is odd.} \end{cases}$$

For any $\ell > 0$, we have

(i) *if ℓ is odd, then $(F_{2\ell-1} - 1)/d_\ell = F_{\ell-1}$ and $(F_{2\ell} - 1)/d_\ell = F_\ell$;*
(ii) *if ℓ is even, then $(F_{2\ell-1} - 1)/d_\ell = d_{\ell+1}$ and $(F_{2\ell} - 1)/d_\ell = d'_{\ell+2}$.*

Proof. Simple calculation. ■

Corollary 2.9. *For any $\ell > 0$, we have* $\gcd(F_{2\ell} - 1, F_{2\ell-1} - 1) = d_\ell$.

Proof. For ℓ odd, the result derives from the fact that $F_{\ell-1}$ and F_ℓ are mutually prime. For ℓ even, observe that any common divisor $d > 0$ of $d_{\ell+1} = F_\ell + F_{\ell-2}$ and $d'_{\ell+2} = F_{\ell+1} + F_{\ell-1}$ is also a divisor of $d'_{\ell+2} - d_{\ell+1} = F_{\ell-1} + F_{\ell-3}$ and, by induction, also a divisor of $F_3 + F_1 = 7$ and of $F_2 + F_0 = 4$, so $d = 1$. ■

From now, we consider the notation of Theorem 2.7. In the sequel, we take $q = d_\ell$ since, by Corollary 2.9, this case is enough to get Theorem 2.7. In this case, also, Lemma 2.8 gives that $\Pi = 0^{\ell-1}10^{\ell}$ and $\Pi' = 0^{\ell}10^{\ell-1}$ for odd ℓ, and $\Pi = 0^{\ell-2}1010^{\ell-1}$ and $\Pi' = 0^{\ell-1}1010^{\ell-2}$ for even ℓ. Consider for example the case ℓ odd (the other case leading to the same case of study, with the help of the decomposition $0^{\ell-2}1010^{\ell-1} = 0^{\ell-2}10^{\ell+1} + 0^{\ell}10^{\ell-1}$). By Lemma 4.1 applied to the case $m = \ell - 1$ and $n \leqslant m/2$, and also by Lemma 4.2, we get that, for any $k \leqslant u_n = F_{\ell-2} + F_{\ell-4}$, $k \cdot \widetilde{\Pi} = \widetilde{k\Pi}$, and $\widetilde{u_n\Pi} = 0^{m-2n}\widetilde{10^{4n-1}}10^{\ell-2n}$. Hence, more generally, we get that, for any $k \leqslant \sum_{j=0}^{n} u_j = d_\ell$ (this latter equality coming from a simple induction), $k \cdot \widetilde{\Pi} = \widetilde{k\Pi}$, and $d_\ell \cdot \widetilde{\Pi} = \widetilde{d_\ell\Pi} = \widetilde{(10)^{\ell}}$. The same study for Π' works as well, so Theorem 2.7 is proved.

Theorem 2.7 gives an explicit way to get the full set $\mathcal{P}_q^*$ that is useful in itself:

(i) Let $n > 3$ be the smallest even integer such that $(F_n \bmod q) = (F_{n-1} \bmod q) = 1$.
(ii) Let Π be the admissible word of length $2\ell := n$ such that $Z(\Pi) = (F_{n-1} - 1)/q$.
(iii) We have $\mathcal{P}_q^* = \{(a \cdot \widetilde{\Pi}) \oplus (b \cdot \widetilde{\sigma^{-1}(\Pi)}) : a, b \in \{0, \ldots, q-1\}\}$.

In passing, we conjecture that, apart for the case $q = 2$, the smallest value $n > 3$ such that $(F_n \bmod q) = (F_{n-1} \bmod q) = 1$ is always even, so the assumption n even in Theorem 2.7 is useless for $q > 2$.

3. Two applications of circular words

3.1. A property of the Fibonacci word

This section is devoted to the proof of the following theorem.

Theorem 3.1. *Let $M := abaababaabaab\ldots$ be the* Fibonacci word*, that is: the fixed point of the substitution defined on the alphabet $\{a, b\}$ by $a \mapsto ab$ and $b \mapsto a$. For $\ell > 2$, let $N_\ell := bM_{F_{2\ell-2}}$. Define the words $A^{(1)}, \ldots, A^{(k)}$ by $N_\ell = A^{(1)} \cdots A^{(k)}a$ and $|A^{(i)}| = d_\ell$, where $k = F_{2\ell-2}/d_\ell$. The value $|A^{(i)}|_a$ (and, hence, the value $|A^{(i)}|_b$) does not depend on $i \leqslant k$.*

It is highly probable that, defining A as the word of length d_ℓ such that $bM = A_1 \cdots A_k A M'$, we have $|A|_a \neq |A^{(i)}|_a$. Also, we can get that $|A^{(i)}|_a = d'_{\ell-2}$ and $|A^{(i)}|_b = d_{\ell-1}$.We will not prove this here.

Note that the fact that $F_{2\ell-2}/d_\ell$ is an integer is a direct consequence of Lemma 2.8.

Definition 3.2. *Let $\widetilde{W} \in \mathcal{G}_\ell^*$ different from the identity element, let $X \in \{(10)^\ell, (01)^\ell, (11)^\ell\}$. We say that $\widetilde{W}$ is of* type X *iff*

$$\tilde{N}(\widetilde{W}) + \tilde{N}(-\widetilde{W}) = N(X).$$

We denote by $\mathcal{T}_X^*$ the set of elements of type X in $\mathcal{G}_\ell^*$. For $X \in \{(01)^\ell, (10)^\ell\}$, we also put $\mathcal{T}_X := \mathcal{T}_X^* \cup \{X\}$.

Proposition 3.1. *Let $\widetilde{W}$ and $\widetilde{W'}$ be two elements of the set $\mathcal{T}_X^*$ for some $X \in \{(10)^\ell, (01)^\ell, (11)^\ell\}$. We have*

$$\tilde{N}(\widetilde{W}) + \tilde{N}(\widetilde{W'}) = N(X) \Longleftrightarrow \widetilde{W} = -\widetilde{W'}.$$

Proof. Simple consequence of the injectivity of N. ■

Proposition 3.2. *We have*

$$\mathcal{T}_{(10)^\ell} \cup \mathcal{T}_{(01)^\ell} \cup \mathcal{T}_{(11)^\ell}^* = \mathcal{G}_\ell^*.$$

More precisely:

(i) *The set $\mathcal{T}_{(10)^\ell}$ is the set of circular words $\widetilde{W} \in \mathcal{G}_\ell^*$ such that W admits $0^{2m}1$ as a prefix (for some $m \geqslant 0$) and 0 as a suffix.*

(ii) *The set $\mathcal{T}_{(01)^\ell}$ is the set of circular words $\widetilde{W} \in \mathcal{G}_\ell^*$ such that W admits $0^{2m+1}1$ as a prefix (for some $m \geqslant 0$).*

(iii) *The set $\mathcal{T}_{(11)^\ell}^*$ is the set of circular words $\widetilde{W} \in \mathcal{G}_\ell^*$ such that W admits $0^{2m}1$ as a prefix (for some $m > 0$) and 1 as a suffix.*

In particular, we have $\sigma(\mathcal{T}_{(01)^\ell}) = \mathcal{T}_{(10)^\ell}$, and:

$$\mathrm{Card}(\mathcal{T}_{(10)^\ell}) = \mathrm{Card}(\mathcal{T}_{(01)^\ell}) = F_{n-2} \qquad \textit{and} \qquad \mathrm{Card}(\mathcal{T}_{(11)^\ell}^*) = F_{n-5} - 1.$$

The proof of Proposition 3.2 basically consists in writing the opposite of $\widetilde{w_0^{2\ell-1}}$ on the form $\tilde{Z}(\widetilde{w'^{2\ell-1}_0})$, where $w'_i = 1 - w_i$ for any i, in studying in which case the transformations $\tilde{\tau}_0$ and $\tilde{\tau}_1$ are to be considered to get the admissible form of $\widetilde{w'^{2\ell-1}_0}$ and in applying Lemma 2.3. The details are left to the reader.

The form of the element of $\mathcal{T}_{(10)^\ell}$ and $\mathcal{T}_{(01)^\ell}$ leads to the following characterization of the structure of these sets.

Proposition 3.3. *Recall that $M = abaababaabaab\ldots$ is the Fibonacci word. We have*

$$\begin{aligned}
N(\mathcal{T}_{(10)^\ell}^*) &= \{1 + 2|M_k|_a + |M_k|_b,\ 0 \leqslant k < F_{2\ell-2}\},\\
N(\mathcal{T}_{(01)^\ell}^*) &= \{1 + 3|M_k|_a + 2|M_k|_b,\ 0 \leqslant k < F_{2\ell-2}\},\\
N(\mathcal{T}_{(11)^\ell}^*) &= \{F_{2\ell-1} + 3 + 5|M_k|_a + 3|M_k|_b,\ 0 \leqslant k < F_{2\ell-5} - 1\}.
\end{aligned}$$

Proof. Consider for example the case of $N(\mathcal{T}_{(10)^\ell}^*)$, the other ones being similar. Assume the property true until $N(\mathcal{T}_{(10)^{\ell-1}}^*)$ and consider $N(\mathcal{T}_{(10)^\ell}^*)$. For $0 \leqslant k < F_{2\ell-2}$, we have either $k < F_{2\ell-4}$ (for which we can apply the induction hypothesis), or $F_{2\ell-4} \leqslant k < F_{2\ell-2}$. In this latter case, define k' by $k = F_{2\ell-4} + k'$, so

$0 \leqslant k' < F_{2\ell-3}$. Recall here the classical characterization of M by blocks: if we put $B^{(-1)} := b$, $B^{(0)} := a$ and, for any $j \geqslant 1$, $B^{(j)} := B^{(j-1)}B^{(j-2)}$, then we have $M = \lim_j(B^{(j)})$. Therefore, we have

$$\begin{aligned} 1 + 2|M_k|_a + |M_k|_b &= 1 + 2(F_{2\ell-5} + |M_{k'}|_a) + (F_{2\ell-6} + |M_{k'}|_b) \\ &= F_{2\ell-3} + (1 + 2|M_{k'}|_a + |M_{k'}|_b). \end{aligned}$$

If $k' < F_{2\ell-4}$, then, by induction hypothesis, the value in the last parenthesis admits $W00$ as a Zeckendorf representation, where W is of type $(10)^{\ell-1}$. Moreover, we have $Z(F_{2\ell-3}) = 0^{2\ell-3}100$, so we eventually get that $Z(1 + 2|M_k|_a + |M_k|_b)$ has the desired form, by Proposition 2 if W admits 00 as a prefix, by a simple case study if W begins with a 1.

If $F_{2\ell-4} \leqslant k' < F_{2\ell-3}$, then we put $k' = F_{2\ell-4} + k''$, and the reasoning is similar.

Hence, we have otained that any number of the form $1 + |M_k|_a + |M_k|_b$ for $0 \leqslant k < F_{2\ell-2}$ belongs to $N(\mathcal{T}^*_{(10)^\ell})$. Since we know by Proposition 3.2 that this latter set has precisely $F_{2\ell-2}$ elements, we are done. ■

In passing, it is also possible to describe in similar terms the set of *forbidden values* for $\mathcal{G}^*_\ell$, that is, the set of positive integers k strictly less than F_n and such that the word $Z(k)$, assumed of length 2ℓ, admits 1 as a prefix and also as a suffix (hence does not correspond to an admissible circular word of $\mathcal{G}^*_\ell$). Here is the result, without proof.

Proposition 3.4. *With the notation of Proposition 3.3, the set $\mathcal{U}_{2\ell}$ of forbidden values for $\mathcal{G}^*_\ell$ satisfies*

$$\mathcal{U}_{2\ell} = \{F_{n-1} + 1 + 3|M_k|_a + 2|M_k|_b,\ 0 \leqslant k < F_{2\ell-4}\}.$$

Proposition 3.5. *Let $\widetilde{\Pi}$ and $\widetilde{\Pi}'$ be the circular words defined in Theorem 2.7, for $q := d_\ell$. For any $k \leqslant q$, $\widetilde{k\Pi}$ is of type $(10)^\ell$ and $\widetilde{k\Pi'}$ is of type $(01)^\ell$.*

Proof. This is a consequence of an observation made in the proof of Theorem 2.7: in the case $q = d_\ell$, we have $\Pi = 0^{\ell-1}10^\ell$ and $\Pi' = 0^\ell 10^{\ell-1}$ for odd ℓ, and $\Pi = 0^{\ell-2}1010^{\ell-1}$ and $\Pi' = 0^{\ell-1}1010^{\ell-2}$ for even ℓ. In any case, Π is of type $(10)^\ell$ and Π' of type $(01)^\ell$. We also observed that, also in the case $q = d_\ell$, for any $k < d_\ell$, $\mathrm{Val}(k\Pi)$ satisfies $\mathrm{Val}((k+1)\Pi) = \mathrm{Val}(k\Pi)$ or $\mathrm{Val}(k\Pi) - 2$, so the type of $k\Pi$ remains constant. The same result holds for Π', so the proposition is proved in the case $q = d_\ell$, hence also for any divisor of d_ℓ. ■

To end the proof of Theorem 3.1, observe that, by Theorem 2.7 and Propositions 3.2 and 3.5, we have, for any $0 < i \leqslant d_\ell$, $N(\Pi) = iN(\Pi) - (i-1)N(\Pi) = 2|A^{(i)}|_a + |A^{(i)}|_b$. Moreover, it is well-known that M is balanced, that is: for a given length m and two factors V and V' of M of length m, we have $||V|_a - |V'|_a| \leqslant 1$. Together with the previous fact asserting that $2|A^{(i)}|_a + |A^{(i)}|_b$ is constant, this implies that $|A^{(i)}|_a$ and $|A^{(i)}|_b$ are constant.

3.2. A formula for the integer sequence A004146

Recall the definition of the integer sequence defined in Theorem 2.4:

$$c_1 := 1 \qquad c_n := F_{2n-1} + F_{2n-3} - 2 \quad \text{for } n \geqslant 2.$$

The aim of this section is to prove the following result:

Theorem 3.3. *For any $n \geqslant 0$, let $\alpha_n := \mathrm{e}^{2\mathrm{i}\pi/n}$. We have, for any $n \geqslant 2$:*

$$c_n = -\prod_{j=0}^{2n-1} (1 - \alpha_n^j - \alpha_n^{2j}).$$

To this end, we consider again, for any $n \geqslant 2$, the linear operator $M = M_{n+1}$ on $\mathbb{R}^{n+1}$ defined after Lemma 2.1: $M_{n+1} = (m_{ij})_{i,j}$ with

$$m_{i,i} = 1, \qquad m_{i,((i+1) \bmod (n+1))} = -1 \qquad \textit{and} \qquad m_{i,((i+2) \bmod (n+1))} = -1$$

for any $0 \leqslant i \leqslant n$.

Lemma 3.4. *For any $0 \leqslant j \leqslant n$, the value $1 - \alpha^j - \alpha^{2j}$ is an eigenvalue of M_{n+1}, associated to the vector $V_j := (\alpha^{kj})_{k=0}^n$.*

Proof. Simple verification. ■

Since the family $\{V_j,\ 0 \leqslant j \leqslant n\}$ is a base of $\mathbb{R}^{n+1}$ (since the vectors V_j make a Vandermonde matrix), we get that M_{n+1} is diagonalizable, and that its determinant is equal to $\prod_{j=0}^n (1 - \alpha_n^j - \alpha_n^{2j})$.

Now, let us give another way to get this determinant.

Lemma 3.5. *The characteristic polynomial $P_n(X) = \det(M_n - XI)$ of M_n satisfies, for any $n \geqslant 5$:*

$$P_n(X) = P_{n-1}(X) + (1-X)P_{n-2}(X) - (1+X)(1-X)^{n-1} + (-1)^{n+1}(X-1) + 2\cdot(-1)^n.$$

Proof. For any $n \geqslant 2$, we denote by $R_n(X)$ the determinant of the operator $(r_{i,j})_{1 \leqslant i,j \leqslant n}$ of $\mathbb{R}^n$ defined for all i for which the following expressions make sense: $r_{i,i} = -1$, $r_{i,i+1} = -1$ and $r_{i,i-1} = 1 - X$.

Now, take $n \geqslant 5$. Write the expansion along the first line of the determinant $P_n(X)$ as $(1 - X)A_{n-1}(X) + B_{n-1}(X) - C_{n-1}(X)$. The expansion of $A_{n-1}(X)$ along the first column gives that $A_{n-1}(X) = (1 - X)^{n-1} - (-1)^n R_{n-2}(X)$. Write $B_{n-1}(X) = (-1)^n D_{n-2}(X) - (-1)^n R_{n-2}(X)$ for the expansion of $B_{n-1}(X)$ along the first column; the expansion of $D_{n-2}(X)$ along the last line gives that $D_{n-2}(X) = (1 - X)R_{n-3}(X)$. Write $C_{n-1}(X) = -(1 - X)B_{n-2}(X) - E_{n-2}(X)$ for the expansion of $C_{n-1}(X)$ along the first line. The expansion along the first line of $E_{n-2}(X)$ followed by a simple induction gives that $E_{n-2}(X) = (-1)^n$.

Putting together all these results gives

$$\begin{aligned} P_n(X) = {} & (1 - X)^n + (-1)^n - (-1)^n(2 - X)R_{n-2}(X) \\ & + (-1)^n(2 - 2X)R_{n-3}(X) - (-1)^n(1 - X)^2 R_{n-4}(X). \end{aligned}$$

It is a classical exercice to show that, for any $n \geqslant 4$, $R_n(X) = (1-X)R_{n-2}(X) - R_{n-1}(X)$, with $R_2(X) = 2 - X$ and $R_3(X) = 2X - 3$. Eventually, a simple calculation gives the desired result. ■

Lemma 3.5 for $X = 0$ then gives that $\det(M_n) = \det(M_{n-1}) + \det(M_{n-2}) - 1 + 3 \cdot (-1)^n$. Then, an induction shows that, for any n, $\det(M_{2n}) = -c_n$ and $\det(M_{2n+1}) = -d_{2n+1}$ (with the definition of $(d_n)_n$ given in Theorem 2.4). With the expression of $\det(M_n)$ obtained in Lemma 3.4, we get Theorem 3.3.

4. $\mathcal{F}$-adic numbers

Before giving the definition that appears to be the most convenient, we feel interesting to consider first some alternative definitions and explain why we do not retain them.

4.1. First attempt

A first quite natural idea to define the set of $\mathcal{F}$-adic numbers consists in considering the set of integer sequences $\mathbb{N}^{\mathbb{N}}$ (each element of which being regarded as an infinite word on the alphabet $\mathbb{N}$) equipped with the cylinder topology. Consider the quotient of this set given by the closure of equivalence classes defined by the relation $\equiv$ (see section 1.2). This first attempt of definition is not convenient, because all the integers would belong to the same closed equivalence class, as shown by the following

Proposition 4.1. *Let $W = w_0^\infty$ be the infinite word defined by:*

$$w_n = \begin{cases} F_{n-1} + F_{n-3} & \text{if } n = 2^2; \\ F_{n-1} + F_{n-3} - 1 & \text{if } n = 2^p \text{ with } p \geqslant 3; \\ 0 & \text{else.} \end{cases}$$

The closed equivalence class of W contains all infinite words of the form $X0^\infty$ with X finite and admissible.

Proof. We need two lemmas first.

Lemma 4.1. *Let $(u_n)_n$ be the sequence defined by $u_0 = 1$, $u_1 = 3$ and, for any $n \geqslant 2$:*

$$u_n := 2u_{n-1} + \sum_{i=0}^{n-2} u_i.$$

Let $n \geqslant 1$, let $m \geqslant 2n$. The finite word $0^m u_n$ is equivalent to the finite word $0^{m-2n}10^{4n-1}1$.

Proof. Define, for any $n \geqslant 0$:

$$v_n := \sum_{i=0}^{n} u_n.$$

We prove the lemma by induction, adding to it the following complementary induction hypothesis: The finite word $0^m v_n$ is equivalent to the finite word $0^{m-2n}(10)^{2n}1$.

Assuming that both the two properties are true until some value $n \geqslant 1$, choose $m \geqslant 2(n+1)$. Since $u_{n+1} = u_n + v_n$, we have the following equivalence of finite words:

$$\begin{aligned} 0^m u_{n+1} &\equiv 0^{m-2n} 20(10)^{2n-1}2 \\ &\equiv 0^{m-2(n+1)}1001(10)^{2n-1}2 \\ &\equiv 0^{m-2(n+1)}10^{4n}12 \\ &\equiv 0^{m-2(n+1)}10^{4n+3}1, \end{aligned}$$

which is the desired property for u_{n+1}.

Now, since $v_{n+1} = v_n + u_{n+1}$, the induction hypothesis and the previous result for u_{n+1} immediately give the desired form for $0^m v_{n+1}$. ■

Lemma 4.2. *With the notation of Lemma 4.1, we have, for any* $i \geqslant 2$, $u_i = F_{2i-1} + F_{2i-3}$.

Proof. Simple induction with the relation $u_n = 3u_{n-1} - u_{n-2}$. ■

Now, by Lemmas 4.1 and 4.2, we get that:

$$\begin{aligned} W &= 00^3 u_2 0^3 (u_4 - 1) 0^7 (u_8 - 1) 0^{15} (u_{16} - 1) 0^{31} \dots \\ &\equiv 10^7 u_4 0^7 (u_8 - 1) 0^{15} (u_{16} - 1) 0^{31} \dots \\ &\equiv 20^{15} u_8 0^{15} (u_{16} - 1) 0^{31} \dots \\ &\equiv 30^{31} u_{16} 0^{31} \dots \end{aligned}$$

Since $|Z(n)| \leqslant \lceil \log_\varphi(n) \rceil$, we get by induction that, for any finite admissible word V of length n and any integer k, there exists an infinite word $X_{n,k}$ such that $W \equiv V0^k X_{n,k}$. This is the desired conclusion. ■

4.2. Second attempt

To avoid the previous problem, one may restrict the set of integers to the subset of bounded ones, hence excluding the previous case. Unfortunately, this is still not a convenient definition, because it does not prevent us from the following problem.

Proposition 4.2. *The closed equivalence class of* 0^∞ *contains infinitely many admissible sequences.*

Proof. Choose $n_0 > 0$, put $X^{(0)} := 0^{2n_0}u_{n_0}$ and let $W^{(0)} := Z(X^{(0)})$. (By Lemma 4.1, we have $W^{(0)} = 10^{4n_0-1}1$.) Choose any $n_1 > n_0$ big enough so that, defining $X^{(1)} := 0^{2n_0}u_{n_0}0^{4n_1-1}u_{n_0}$, we have $W^{(1)} := Z(X^{(1)}) = W^{(0)}0^{k_1}W^{(0)}$ for some $k_1 > 0$. More generally, for any $i > 0$, choose any $n_i > n_{i-1}$ big enough so that, defining $X^{(i)} := X^{(i-1)}0^{4n_{i-1}-1}X^{(i-1)}$, we have $W^{(i)} := Z(X^{(i)}) = W^{(i-1)}0^{k_i}W^{(i-1)}$ for some $k_i > 0$. Let us show that the infinite and admissible word $W := \lim_n(W^{(n)})$ belongs to the closed equivalence class of 0^∞. Define $\pi_i := u_{n_0} \cdots u_{n_i}$ for any $i \geqslant 0$. By construction and Lemma 4.1, $X^{(1)}$ is equivalent to $0^{2(n_0+n_1)}\pi_1$ and, more generally and by an immediate induction, $X^{(i)}$ is equivalent to $0^{2(n_0+\cdots+n_i)}\pi_i$. Hence, the infinite word W and the null sequence belong to the same closed equivalence class in the cylinder topology. ■

4.3. Final definition of the set of $\mathcal{F}$-adic numbers

Our aim is now to consider only admissible infinite sequences for the set of $\mathcal{F}$-adic numbers. Let W and W' be two admissible sequences. The natural definition for their sum $W + W'$ is to consider the limit $\lim_n(Z(W_n + W'_n))$. The point is to ensure that such a limit exists, which is not always the case, as the example $W := (01)^\infty$ and $W' := (10)^\infty$ shows (we have $Z(W_{2n} + W'_{2n}) = 00(10)^n$ and $Z(W_{2n+1} + W'_{2n+1}) = 10(01)^n$). A more general example is given by the words $W = X(10)^\infty$ and $W' = X'(01)^\infty$, where X and X' are finite admissible words of the same length. It appears that this latter example contains essentially all possible contentious issues.

Definition 4.3. *The set $\mathcal{F}$ of $\mathcal{F}$-*adic numbers *is defined as the set of admissible infinite sequences, with the identifications* $(01)^\infty = (10)^\infty$ *and* $V0(01)^\infty = Z(V10(01)^\infty)$ *for any admissible finite word V, and equipped with the (quotient) cylinder topology. A* negative $\mathcal{F}$-integer *is an admissible sequence ultimately periodic with period* 01 *(that is: negative $\mathcal{F}$-integers are the $\mathcal{F}$-adic numbers admitting two different writings).*

The sum *of two $\mathcal{F}$-adic numbers W and W' is defined as:*

$$W \oplus W' := \lim_n (Z(W_n + W'_n)).$$

For any word W with letters on a bounded subinterval of $\mathbb{N}$, we define $Z(W) := \lim_n(Z(W_n))$.

To ensure the consistence of this definition, we have to show that the sum is well-defined (which immediately implies the consistence of the definition of $Z(W)$). This is done in the proof of the following result, which is a strong justification for our choice of definition. Before it, let us explain the terminology of negative $\mathcal{F}$-integers. Consider a negative $\mathcal{F}$-integer $V0(01)^\infty = Z(V10(01)^\infty)$, and put $W := \overline{V0}$ (recall that, for any finite word X, we have $Z(X + \overline{X}) = 0^{|X|}1$). Since

$Z(W + V0(01)^{\infty}) = Z(W + Z(V10(01)^{\infty})) = 0^{\infty}$, the negative $\mathcal{F}$-integer can be regarded as the word corresponding to the value $-N(W)$. In the same way, the $\mathcal{F}$-adic number $(01)^{\infty} = (10)^{\infty}$ can be regarded as -1 (or, to avoid ambiguous notation, $(-1)_{\mathcal{F}}$). Note also that, because of the negative $\mathcal{F}$-integers, the notion of valuation is consistent only for words, and not for $\mathcal{F}$-adic numbers in general.

Now, let us give the main result of this section.

Theorem 4.4. $(\mathcal{F}, +)$ *is a topologic abelian group.*

Proof. Let us start by showing that the addition is well-defined. We consider first the case of two $\mathcal{F}$-adic numbers, W and W', which are not negative $\mathcal{F}$-integers. If, for any $k \geqslant 0$, the sequence of letters of rank k of the words $Z(W_n + W'_n)$ converges, then $W + W'$ is well-defined. Else, let k be the smallest index such that the sequence of letters of rank k of $Z(W_n + W'_n)$ does not converge. The sequence of prefixes of length k (which may be $\varnothing$ if $k = 0$) of the sequence $(Z(W_n + W'_n))_n$ converges to some admissible word V. Since both W and W' contains infinitely many 1s (to ensure the existence of k), we can find an n_0 such that $N(W_{n_0}) > N(V)$. By replacing the word $W =: W_{n_0}U$ by the word $Z(N(W_{n_0}) - N(V))0^{|W_{n_0}|-|Z(N(W_{n_0})-N(V))|}U$, we can assume that $V = 0^k$.

The successive words $Z(W_n + W'_n)$ can be obtained by iterating the algorithm that computes $Z(W + 0^m1)$ for finite admissible W, with a sequence of values of m going to infinity. With a little abuse in notation (since the successive m is an increasing sequence but non necessarily strictly increasing), we write X_m for the successive admissible words hence obtained.

Assume $k \geqslant 1$. By Proposition 1.2, we have, for any m, $\mathrm{Val}(X_m) = k$ or $k + 2$, and, by hypothesis, there are infinitely many values of m for which $\mathrm{Val}(X_m) = k$ and also infinitely many for which $\mathrm{Val}(X_m) = k + 2$. Consider an m such that $\mathrm{Val}(X_m) = k + 2$ and $\mathrm{Val}(X_{m+1}) = k$. By Proposition 2, X_m is of the form $0^{k+2}(10)^{s_m}Y_m$, with Y_m admissible. When m goes to infinity, s_m must go to infinity as well. Hence, the sequence $(Z(W_n + W'_n))_n$ admits $0^{k+2}(10)^{\infty}$ (the limit of the X_ms) and $0^k10(01)^{\infty}$ (the limit of the X_{m+1}s) as accumulation points. Since the values of m for which $\mathrm{Val}(X_m) = \mathrm{Val}(X_{m+1})$ does not add any other accumulation point, we are done for this case.

Now, assume $k = 0$. If, for all but finitely many of m such that $\mathrm{Val}(X_m) > 0$, we have $\mathrm{Val}(X_m) = 2$, then we can apply Proposition 1.2 as in the case $k > 0$. Hence, we assume that, for any big enough m such that $\mathrm{Val}(X_m) > 0$, we have $\mathrm{Val}(X_m) = 1$. Take m such that $\mathrm{Val}(X_m) = 1$ and $\mathrm{Val}(X_{m+1}) = 0$. By Lemma 1.3, the computation of X_{m+1} from X_m by the algorithm necessarily involves the first loop. Hence, we necessarily have $X_{m+1} = Z(0(10)^{s_m}20Y_{m+1})$ for some admissible Y_{m+1} and some $s_m \geqslant 0$. Since s_m must go to infinity as m goes to infinity, the word $(01)^{\infty}$ is an accumulation point of the sequence $(X_m)_m$. The same reasoning starting from $\mathrm{Val}(X_m) = 0$ and $\mathrm{Val}(X_{m+1}) = 1$ gives that $(10)^{\infty}$ is an accumulation point as well. Since no other accumulation point arise from the cases $\mathrm{Val}(X_m) = \mathrm{Val}(X_{m+1})$ $(= 0$ or $1)$, we are also done for $k = 0$.

Now, assume that W is a negative $\mathcal{F}$-integer. For some finite admissible word V, we have $W = V0(01)^\infty = Z(V10(01)^\infty)$, and the point is to verify that the result of the computation of $W \oplus W'$ does not depend on the choice of the two equivalent representations of W. If W' is also a negative $\mathcal{F}$-integer, then the result is obtained by a simple verification (and gives that, for any a, $b \in \mathbb{N}$, we have $(-a_\mathcal{F}) \oplus (-b_\mathcal{F}) = (-(a+b))_\mathcal{F})$. Therefore, from now, we assume that W' is not a negative $\mathcal{F}$-integer. We put $X_n := Z(W_n + W'_n)$ (with a fixed choice for the representation of W). We then have, for any big enough n, that $Z(X_n + \overline{V0}) = Z(W'_n + 0^n 1)$. Since W' is not a negative $\mathcal{F}$-integer, the sequence of words $Z(W'_n + 0^n 1)$ converges to an admissible limit word Y, which is also the limit of $Z(X_n + \overline{V0})$. Since $\overline{V0}$ is a finite word, the sequen ce X_n is also converging to an admissible limit word X, which consistently defines $W \oplus W'$, independently of the choice of the representation of W.

The same reasoning, where the $\mathcal{F}$-adic numbers W and W' are replaced by sequences $(W^{(n)})_n$ and $(W'^{(n)})_n$ of $\mathcal{F}$-adic numbers converging to W and W', is easily adapted to show that $\oplus$ is bicontinuous.

Now, let us show the associativity of $\oplus$. If W, W', W'', $W \oplus W'$ and $W' \oplus W''$ are not negative $\mathcal{F}$-integers, then for any n there exists an i such that the prefix of length n of $(W \oplus W') \oplus W''$ and of $W \oplus (W' \oplus W'')$ is determined by the prefix of length i of W, W' and W''. Hence, in this case, the equality $(W \oplus W') \oplus W'' = W \oplus (W' \oplus W'')$ derives from the associativity of $\oplus$ in the case of finite words. The other cases, left to the reader, are essentially similar, with only some additional verifications due to the possible existence of two different representations for some of the involved expressions.

To complete the proof, it only remains to show that any $\mathcal{F}$-adic number $W = w_0^\infty$ admits an opposite. We already know that this is the case when W is a negative $\mathcal{F}$-integer, so we exclude this case in the sequel. We also exclude the case where W is ultimately periodic of period 0 (that is: W is a positive $\mathcal{F}$-integer). Consider the word $W' := {w'}_0^\infty$, where $w'_n = 1 - w_n$ for any n. Since W' is a word on the alphabet $\{0,1\}$, not ultimately periodic of period 1 (by hypothesis on W), there exists a unique admissible word W'' such that, for any n, $Z(W'_n) = W''_n$ (if 1^{2i-1} is a suffix of W'_n but not 1^{2i}, for some i) or W''_{n+1} (in the other case). For any n, we have $W_n + W'_n = 1^n$, so $Z(W_n + W'_n) = 0(01)^{n/2}$ (for even n) or $10(01)^{(n-1)/2}$ (for odd n). Hence, the sequence $(Z(W_n + W''_n))_n$ converges to $-2_\mathcal{F}$, so $W'' \oplus (-2_\mathcal{F})$ is the opposite of W. ■

5. Rational $\mathcal{F}$-adic numbers

A $\mathcal{F}$-adic number X is *rational* iff there exists two integers p and q such that $Z(qX) = Z(p)$. In the sequel, we simply write $qX = p$ for this equation. The goal of this section consists in proving the following two theorems:

Theorem 5.1. *The $\mathcal{F}$-adic number X is rational iff it is ultimately periodic.*

Theorem 5.2. *Let p and q be two integers, with $q > 0$. The set of roots of $qX = p$ is of cardinality $q + 1$ if $p/q \in \mathbb{Z}$ and of cardinality q otherwise.*

The proof of Theorem 5.2 will lead us to a simple and general expression of the set of solutions of the equation $qX = p$ (see Theorem 5.5, at the end of this paper).

5.1. Proof of Theorem 5.1

Periodic ⇒ rational

Proposition 5.1. *Let $X := WP^\infty$ and $X' := W'P'^\infty$ be two ultimately periodic $\mathcal{F}$-adic numbers with $|W| = |W'|$. The sum $X \oplus X'$ is ultimately periodic, of period Q such that $\widetilde{Q} = \widetilde{P} \oplus \widetilde{P}'$.*

Proof. Without loss of generality, we assume P and P' of the same even length 2ℓ, and take $W = W' = 0^k$ with big enough k. By induction, we can also assume P' of the form $10^{2\ell-1}$. If $\widetilde{P} \oplus \widetilde{P}' = \widetilde{P + P'}$, then the result is immediate. Otherwise, writing $P = p_0 \dots p_{2\ell-1}$, we have either $p_0 = 1$ or $P = (01)^\ell$. In this latter case, the proposition is easily verified. Assume now $p_0 = 1$. We either have $P = (10)^\ell$ or, for some admissible word R and some integer j, $P = 10R00(10)^j$. In both cases, the proposition is routinely verified. ■

Corollary 5.3. *For any integer q and any finite admissible word P (containing at least one 1 and which first and last letters are not both equal to 1), $Z(qP^\infty)$ is a ultimately periodic $\mathcal{F}$-adic number, and admits the word Q as a period, where $\widetilde{Q} := \tilde{Z}(\widetilde{qP})$.*

Proof. Immediate. ■

Now, let $X := WP^\infty$ be a ultimately periodic $\mathcal{F}$-adic number, where W and P are finite admissible words (as well as WP). If $P = 0$, then there is nothing to prove. We thus consider only the case where P contains at least one 1. Without loss of generality, we may also assume P of even length 2ℓ (otherwise, we simply replace P by P^2).

Since P does not contains only 0s, we have $\widetilde{P} \in \mathcal{G}_\ell^*$. Denoting by q the order of $\widetilde{P}$ in $\mathcal{G}_\ell^*$, we get by Corollary 5.3 that, for some finite admissible word Y, $Z(q(0^{|W|}P^\infty)) = Y(01)^\infty$, which is a negative $\mathcal{F}$-integer, say $-r$. Since qW is an integer, say s, we get that $q(WP^\infty) = qW + q(0^{|W|}P^\infty) = s - r$, so we are done.

Rational ⇒ periodic

Let $X := x_0^\infty \in \mathcal{F}$ be a root of $qX = p$, where p and q are integers. By changing the value of p, we can assume that, for any chosen value $k \geqslant 1$, we have $x_0 \dots x_{k-1} = 0^k$.

Define the application Φ: $\mathcal{F} \longrightarrow [-1, 1]$ by $\Phi(w_0^\infty) = \sum_{n=0}^{+\infty} w_n(-\varphi)^{-n}$. Since k can be chosen big enough independently of q, we can assume that $\Phi(qX) = q\Phi(X)$.

Hence, we have $\Phi(X) = \Phi(qX)/q = \Phi(p)/q$. This latter element belongs to $\mathbb{Q}(\varphi)$, and it is well-known that the elements of $\mathbb{Q}(\varphi)$ are exactly the ones that admit a periodic expansion in the numeration system in base $-\varphi$. Hence, $\Phi(X)$ has the form $\sum_{n=0}^{\infty} y_n(-\varphi)^{-n}$ with y_0^{∞} admissible and ultimately periodic. Since, moreover, Φ is injective, we eventually get the desired result.

5.2. Proof of Theorem 5.2

We know by Theorem 5.1 that any root of the equation is of the form WP^{∞}, where W and P are finite admissible words. If $P = 0$, then we are back to an usual integer equation, with one root (p/q) if $p/q \in \mathbb{Z}$ and no root otherwise. So, from now, we exclude the case $P = 0$, and show that exactly q roots of the equation $qX = p$ are to be found.

Let $\Psi : \mathcal{P}_q^* \longrightarrow \mathbb{Z}/q\mathbb{Z}$ be defined by $\Psi(\widetilde{P}) := Z(q \cdot P^{\infty}) \bmod q$ (The function Ψ is well-defined, since we know that $Z(q \cdot P^{\infty})$ is ultimately periodic of period 01 by section 5.1, hence is a negative $\mathcal{F}$-integer.) The function Ψ is a morphism of groups. Let $\Pi \in \mathcal{P}_q^*$ be the word given in the algorithm presented after the proof of Theorem 2.7. We have $q\Pi^{\infty} = (-1)_{\mathcal{F}}$, so $\Psi(\widetilde{\Pi}) = q - 1 = -1$, so Ψ is surjective, and $\Psi^{-1}(0)$ has q elements (since $\mathcal{P}_q^*$ has q^2 elements by Theorem 2.5).

Let $\widetilde{P} \in \mathcal{P}_q^*$. We have $Z(q \cdot (10^{\infty} \oplus P^{\infty})) = Z(qP^{\infty}) + q$ and $Z(q \cdot ((-1)_{\mathcal{F}} \oplus P^{\infty})) = Z(qP^{\infty}) - q$, so, with the help of the surjectivity of Ψ, we get that the number of solutions of the equation $qX = p$ does not depend on p.

Lemma 5.4. *Let X and X' be such that $qX = 0$ and $qX' = 0$, with $X = WP^{\infty}$ and $X' = W'P^{\infty}$ for some finite admissible words W and W' and some $P \in \mathcal{P}_q^*$. If $|W| = |W'|$, then $W = W'$.*

Proof. Immediate. ■

Now, the desired result is a simple consequence of Lemma 5.4 and the fact that $\Psi^{-1}(0)$ has exactly q elements.

5.3. An explicit expression of the roots of $qX = p$

As we said after the statement of Theorem 5.2, the proof of this theorem provides a full characterization of the set of $\mathcal{F}$-adic solutions of $qX = p$.

Theorem 5.5. *Let p and q be integers, with $q > 0$ and $p \neq 0$. Denote by Π the word defined in the end of section 2.3, and put $\widetilde{P_a} := \widetilde{(a-1)\Pi} \oplus (\widetilde{-a\sigma^{-1}(\Pi)})$ for any $0 \leqslant a < q$. Apart the possible integer solution p/q (if $p \in q\mathbb{Z}$), the roots of the equation $qX = p$ are pP_a^{∞} for $0 \leqslant a < q$.*

Denote $\widetilde{P'_a} := \widetilde{a\Pi} \oplus (\widetilde{-a\sigma^{-1}(\Pi)})$ for any $0 \leqslant a < q$. The roots of the equation $qX = 0$ are P'_a for $0 \leqslant a < q$.

The proof is immediate.

References

[AF] P. Ambrož and Ch. Frougny, *On alpha-adic expansions in Pisot bases*, Theoret. Comput. Sci. **380** (2007), 238–250.

[BL] G. Barat and P. Liardet, *Dynamical systems originated in the Ostrowski alpha-expansion*, Ann. Univ. Sci. Budapest Sect. Comput. **24** (2004), 133–184.

[FS] Ch. Frougny and J. Sakarovitch, *Two groups associated with quadratic Pisot units*, Internat. J. Algebra Comput **12** (2002), 825–847.

[GLT] P. Grabner, P. Liardet and R. Tichy, *Odometers and systems of numeration*, Acta Arith. **LXX** (1995), 103–123.

[L] M. Lothaire, *Combinatorics on words*, Cambridge University Press, Cambridge, 1997.

[R] K. Rebman, *The sequence:* 1 5 16 45 121 320 . . . *in combinatorics*, Fibonacci Quart. **13** (1975), 51–55.

[Sloane] N. Sloane, http://oeis.org/A004146

[Sch] K. Schmidt, *Algebraic codings of expansive group automorphisms and two-sided beta-shifts*, Monatsh. Math **129** (2000), 37-61.

[S] N. Sidorov, *An arithmetic group associated with a Pisot unit, and its symbolic-dynamical representation*, Acta Arith. **101** (2002), 199–213.

[SV] N. Sidorov and A. Vershik, *Ergodic properties of the Erdős measure, the entropy of the golden shift, and related problems*, Monatsh. Math. **126** (1998), 215-261.

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

Addresses: Benoît Rittaud: Université Paris-13, Institut Galilée, Laboratoire Analyse, Géométrie et Applications, 99 avenue Jean-Baptiste Clément, 93 430 Villetaneuse, France; Laurent Vivier: Université Paris Diderot, Laboratoire de Didactique André Revuz, Site Chevaleret - Case 7018, 75 205 Paris Cedex 13, France.

E-mail: rittaud@math.univ-paris13.fr, laurent.vivier@univ-paris-diderot.fr

Received: 5 October 2011