Minimal weight expansions in Pisot bases

Christiane Frougny and Wolfgang Steiner

Abstract. For applications to cryptography, it is important to represent numbers with a small number of non-zero digits (Hamming weight) or with small absolute sum of digits. The problem of finding representations with minimal weight has been solved for integer bases, e.g. by the non-adjacent form in base 2. In this paper, we consider numeration systems with respect to a real base β which is a Pisot number. When β is the Golden Ratio, the Tribonacci number or the smallest Pisot number, we determine expansions with minimal number of digits ± 1 and give finite automata recognizing all these expansions. The average weight is lower than for the non-adjacent form.

In the general case of a base β which is a Pisot number satisfying a certain condition (D$'$), we prove that the expansions with minimal absolute sum of digits are recognizable by a finite automaton.

Keywords. Minimal weight, Beta-expansions, Pisot numbers, Fibonacci numbers, Automata.

AMS classification. 11A63, 11B39, 68Q45, 94A60.

1 Introduction

Let A be a set of (integer) digits and $x = x_1 x_2 \cdots x_n$ be a word with letters x_j in A. The *weight* of x is the *absolute sum of digits* $\|x\| = \sum_{j=1}^{n} |x_j|$. The *Hamming weight* of x is the number of non-zero digits in x. Of course, when $A \subseteq \{-1, 0, 1\}$, the two definitions coincide.

Expansions of minimal weight in integer bases β have been studied extensively. When $\beta = 2$, it is known since Booth [5] and Reitwiesner [23] how to obtain such an expansion with the digit set $\{-1, 0, 1\}$. The well-known non-adjacent form (NAF) is a particular expansion of minimal weight with the property that the non-zero digits are isolated. It has many applications to cryptography, see in particular [20, 17, 21]. Other expansions of minimal weight in integer base are studied in [14, 16]. Ergodic properties of signed binary expansions are established in [7].

Non-standard number systems — where the base is not an integer — have been studied from various points of view. Expansions in a real non-integral base $\beta > 1$ have been introduced by Rényi [24] and studied initially by Parry [22]. Number theoretic transforms where numbers are represented in base the Golden Ratio have been introduced in [8] for application to signal processing and fast convolution. Fibonacci representations have been used in [19] to design exponentiation algorithms based on addition chains. Recently, the investigation of minimal weight expansions has been extended to the Fibonacci numeration system by Heuberger [15], who gave an equivalent to the NAF. Solinas [26] has shown how to represent a scalar in a complex base τ related to Koblitz curves, and has given a τ-NAF form, and the Hamming weight of these representations has been studied in [10].

First author: supported by the Agence Nationale de la Recherche, grant ANR-JCJC06-134288 “DyCoNum”.

Second author: supported by the Agence Nationale de la Recherche, grant ANR-JCJC06-134288 “DyCoNum”.

In this paper, we study expansions in a real base $\beta > 1$ which is not an integer. Any number z in the interval $[0,1)$ has a so-called *greedy β-expansion* given by the β-transformation τ_β, which relies on a greedy algorithm: let $\tau_\beta(z) = \beta z - \lfloor \beta z \rfloor$ and define, for $j \geq 1$, $x_j = \lfloor \beta \tau_\beta^{j-1}(z) \rfloor$. Then $z = \sum_{j=1}^\infty x_j \beta^{-j}$, where the x_j's are integer digits in the alphabet $\{0, 1, \ldots, \lfloor \beta \rfloor\}$. We write $z = \raisebox{0.1ex}{\textbf{.}} x_1 x_2 \cdots$. If there exists a n such that $x_j = 0$ for all $j > n$, the expansion is said to be *finite* and we write $z = \raisebox{0.1ex}{\textbf{.}} x_1 x_2 \cdots x_n$. By shifting, any non-negative real number has a greedy β-expansion: If $z \in [\beta^k, \beta^{k+1})$, $k \geq 0$, and $z/\beta^k = \raisebox{0.1ex}{\textbf{.}} x_1 x_2 \cdots$, then $z = x_1 \cdots x_k \raisebox{0.1ex}{\textbf{.}} x_{k+1} x_{k+2} \cdots$.

We consider the sequences of digits $x_1 x_2 \cdots$ as words. Since we want to minimize the weight, we are only interested in finite words $x = x_1 x_2 \cdots x_n$, but we allow a priori arbitrary digits x_j in $\mathbb{Z}$. The corresponding set of numbers $z = \raisebox{0.1ex}{\textbf{.}} x_1 x_2 \cdots x_n$ is therefore $\mathbb{Z}[\beta^{-1}]$. Note that we do not require that the greedy β-expansion of every $z \in \mathbb{Z}[\beta^{-1}] \cap [0,1)$ is finite, although this property (F) holds for the three numbers β studied in Sections 4 to 6, see [13, 1].

The set of finite words with letters in an alphabet A is denoted by A^*, as usual. We define a relation on words $x = x_1 x_2 \cdots x_n \in \mathbb{Z}^*$, $y = y_1 y_2 \cdots y_m \in \mathbb{Z}^*$ by

$$x \sim_\beta y \quad \text{if and only if} \quad \raisebox{0.1ex}{\textbf{.}} x_1 x_2 \cdots x_n = \beta^k \times \raisebox{0.1ex}{\textbf{.}} y_1 y_2 \cdots y_m \text{ for some } k \in \mathbb{Z}.$$

A word $x \in \mathbb{Z}^*$ is said to be *β-heavy* if there exists $y \in \mathbb{Z}^*$ such that $x \sim_\beta y$ and $\|y\| < \|x\|$. We say that y is *β-lighter* than x. This means that an appropriate shift of y provides a β-expansion of the number $\raisebox{0.1ex}{\textbf{.}} x_1 x_2 \cdots x_n$ with smaller absolute sum of digits than $\|x\|$. If x is not β-heavy, then we call x a *β-expansion of minimal weight*. It is easy to see that every word containing a β-heavy factor is β-heavy. Therefore we can restrict our attention to *strictly β-heavy* words $x = x_1 \cdots x_n \in \mathbb{Z}^*$, which means that x is β-heavy, and $x_1 \cdots x_{n-1}$ and $x_2 \cdots x_n$ are not β-heavy.

In the following, we consider real bases β satisfying one of the following conditions:

$$\text{(D):} \quad \begin{array}{l} \beta^{d+1} - B\beta^d + b_1 \beta^{d-1} + b_2 \beta^{d-2} + \cdots + b_d = 0 \\ \text{for some } B, b_1, b_2 \ldots, b_d \in \mathbb{Z} \text{ with } B > \sum_{j=1}^d |b_j| \end{array}$$

$$\text{(D}'\text{):} \quad \begin{array}{l} \text{there exists } B \in \mathbb{Z},\ B > 0, \text{ and a word } b \in \{1-B, \ldots, B-1\}^* \\ \text{such that } B \sim_\beta b \text{ and } \|b\| \leq B \end{array}$$

Note that Condition (D) is a special case of (D′) since $B \sim_\beta 10 b_1 b_2 \cdots b_d$ in this case. It was shown in [2] for $\beta > 1$ satisfying (D) that every $z \in \mathbb{Z}[\beta^{-1}] \cap [0,1)$ can be written as $z = z_+ - z_-$ with some $z_+ \in [0, \beta)$, $z_- \in [0,1)$ having finite greedy β-expansions. This property has some important consequences (see [2]) and is conjectured to hold true for all Pisot numbers β. Recall that a Pisot number is an algebraic integer $\beta > 1$ such that all the other roots of its minimal polynomial are in modulus less than one. In the Appendix we show that a number $\beta > 1$ which satisfies Condition (D) is necessarily a Pisot number. Furthermore, we have $B \in \{\lfloor \beta \rfloor, \lceil \beta \rceil\}$, see [2].

Example 1.1. If $1 = \raisebox{0.1ex}{\textbf{.}} t_1 t_2 \cdots t_d (t_{d+1})^\omega$ with integers $t_1 \geq t_2 \geq \cdots \geq t_d > t_{d+1} \geq 0$, then β satisfies (D) since

$$\beta^{d+1} - t_1 \beta^d - \cdots - t_d \beta - t_{d+1} = \frac{t_{d+1}}{\beta - 1} = \beta^d - t_1 \beta^{d-1} - \cdots - t_d$$

and thus

$$\beta^{d+1} - (1+t_1)\beta^d + (t_1 - t_2)\beta^{d-1} + \cdots + (t_{d-1} - t_d)\beta + (t_d - t_{d+1}) = 0.$$

We show that Condition (D′) implies that every class of words (with respect to $\sim_\beta$) contains a β-expansion of minimal weight in $\{1-B,\ldots,B-1\}^*$. Recall that the set of greedy β-expansions is recognizable by a finite automaton when β is a Pisot number [4]. In this work, we show that the set of β-expansions of minimal weight in $\{-c,\ldots,c\}^*$ is recognized by a finite automaton if β is a Pisot number satisfying (D′) and $c \geq B-1$.

We then consider particular Pisot numbers satisfying (D′) which have been extensively studied from various points of view. When β is the Golden Ratio, we construct a transducer which gives, for a strictly β-heavy word as input, a β-lighter word as output, and another transducer which converts all words without β-heavy factors into some unique expansion avoiding certain factors. From these transducers, we derive the minimal automaton recognizing the set of β-expansions of minimal weight in $\{-1,0,1\}^*$. We give a branching transformation which provides all β-expansions of minimal weight in $\{-1,0,1\}^*$ of a given $z \in \mathbb{Z}[\beta^{-1}]$. Similar results are obtained for the representation of integers in the Fibonacci numeration system. The average weight of expansions of the numbers $-M,\ldots,M$ is $\frac{1}{5}\log_\beta M$, which means that typically only every fifth digit is non-zero. Note that the corresponding value for 2-expansions of minimal weight is $\frac{1}{3}\log_2 M$, see [3, 6], and that $\frac{1}{5}\log_\beta M \approx 0.288\log_2 M$.

We obtain similar results for the case where β is the so-called *Tribonacci number*, which satisfies $\beta^3 = \beta^2 + \beta + 1$ ($\beta \approx 1.839$), and the corresponding representations for integers. In this case, the average weight is $\frac{\beta^3}{\beta^5+1}\log_\beta M \approx 0.282\log_\beta M \approx 0.321\log_2 M$.

Finally we consider the smallest Pisot number, $\beta^3 = \beta + 1$ ($\beta \approx 1.325$), which provides representations of integers with even lower weight than the Fibonacci numeration system: $\frac{1}{7+2\beta^2}\log_\beta M \approx 0.095\log_\beta M \approx 0.234\log_2 M$.

2 Preliminaries

A finite sequence of elements of a set A is called a *word*, and the set of words on A is the free monoid A^*. The set A is called *alphabet*. The set of infinite sequences or infinite words on A is denoted by $A^{\mathbb{N}}$. Let v be a word of A^*, denote by v^n the concatenation of v to itself n times, and by v^ω the infinite concatenation $vvv\cdots$.

A finite word v is a *factor* of a (finite or infinite) word x if there exists u and w such that $x = uvw$. When u is the empty word, v is a *prefix* of x. The prefix v is *strict* if $v \neq x$. When w is empty, v is said to be a *suffix* of x.

We recall some definitions on automata, see [11] and [25] for instance. An *automaton over* A, $\mathcal{A} = (Q, A, E, I, T)$, is a directed graph labelled by elements of A. The set of vertices, traditionally called *states*, is denoted by Q, $I \subset Q$ is the set of *initial* states, $T \subset Q$ is the set of *terminal* states and $E \subset Q \times A \times Q$ is the set of labelled *edges*. If $(p, a, q) \in E$, we write $p \xrightarrow{a} q$. The automaton is *finite* if Q is finite. A subset H of A^* is said to be *recognizable by a finite automaton* if there exists a finite automaton $\mathcal{A}$

such that H is equal to the set of labels of paths starting in an initial state and ending in a terminal state.

A *transducer* is an automaton $\mathcal{T} = (Q, A^* \times A'^*, E, I, T)$ where the edges of E are labelled by couples of words in $A^* \times A'^*$. It is said to be *finite* if the set Q of states and the set E of edges are finite. If $(p, (u, v), q) \in E$, we write $p \xrightarrow{u|v} q$. In this paper we consider *letter-to-letter* transducers, where the edges are labelled by elements of $A \times A'$. The *input automaton* of such a transducer is obtained by taking the projection of edges on the first component.

3 General case

In this section, we prove the following result.

Theorem 3.1. *If β is a Pisot number satisfying* (D′) *and c is an integer, $c \geq B - 1$, then one can construct a finite automaton recognizing the set of β-expansions of minimal weight in $\{-c, \ldots, c\}^*$.*

We begin with a combinatorial result which shows that Condition (D′) is necessary and sufficient when we want to have a finite alphabet such that every class of words (with respect to $\sim_\beta$) contains a β-expansion of minimal weight with digits in this alphabet. Note that β can be an arbitrary complex number for the following proposition.

Proposition 3.2. *Let β satisfy Condition* (D′) *with $B \geq 2$. Then for every $x \in \mathbb{Z}^*$ there exists some $y \in \{1 - B, \ldots, B - 1\}^*$ with $x \sim_\beta y$ and $\|y\| \leq \|x\|$.*

If β does not satisfy Condition (D′)*, then for every $B \in \mathbb{Z}$ the set of β-expansions of minimal weight x with $x \sim_\beta B$ is $0^* B 0^*$.*

Proof. The second statement is an immediate consequence of the definition of (D′).

The proof of the first statement is similar to the proof of Theorem 4 in [2]. If $x = x_1 x_2 \cdots x_n \in \{1 - B, \ldots, B - 1\}^*$, then there is nothing to do. Otherwise, we use Condition (D′): there exists some word $b = b_{-k} \cdots b_d \in \{1 - B, \ldots, B - 1\}^*$ such that $b_{-k} \cdots b_{-1}(b_0 - B) b_1 \cdots b_d \sim_\beta 0$ and $\|b\| \leq B$. Set $x_j^{(0)} = x_j$ for $1 \leq j \leq n$, $x_j^{(0)} = 0$ for $j \leq 0$ and $j > n$, $b_j = 0$ for $j < -k$ and $j > d$. Define, recursively for $i \geq 0$, $h_i = \max\{j \in \mathbb{Z} : |x_j^{(i)}| \geq B\}$,

$$x_{h_i}^{(i+1)} = x_{h_i}^{(i)} + \mathrm{sgn}(x_{h_i}^{(i)})(b_0 - B),\ x_{h_i+j}^{(i+1)} = x_{h_i+j}^{(i)} + \mathrm{sgn}(x_{h_i}^{(i)}) b_j \text{ for } j \neq 0,$$

as long as h_i exists. Then we have $\sum\limits_{j\in\mathbb{Z}} |x_j^{(0)}| = \|x\|$, $\sum\limits_{j\in\mathbb{Z}} x_j^{(i+1)} \beta^{-j} = \sum\limits_{j\in\mathbb{Z}} x_j^{(i)} \beta^{-j}$ and

$$\sum_{j\in\mathbb{Z}} |x_j^{(i+1)}| = |x_{h_i}^{(i+1)}| + \sum_{j\neq 0} |x_{h_i+j}^{(i+1)}| \leq |x_{h_i}^{(i)}| + |b_0| - B + \sum_{j\neq 0} (|x_{h_i+j}^{(i)}| + |b_j|) \leq \sum_{j\in\mathbb{Z}} |x_j^{(i)}|.$$

If h_i does not exist, then we have $|x_j^{(i)}| < B$ for all $j \in \mathbb{Z}$, and the sequence $(x_j^{(i)})_{j\in\mathbb{Z}}$ without the leading and trailing zeros provides a word $y \in \{1 - B, \ldots, B - 1\}^*$ with the desired properties.

Since $\|x\|$ is finite, we have $\sum_{j\in\mathbb{Z}} |x_j^{(i+1)}| < \sum_{j\in\mathbb{Z}} |x_j^{(i)}|$ only for finitely many $i \ge 0$. In particular, the algorithm terminates after at most $\|x\| - B + 1$ steps if $\|b\| < B$. If $\|b\| = B$ and $\sum_{j\in\mathbb{Z}} |x_j^{(i+1)}| = \sum_{j\in\mathbb{Z}} |x_j^{(i)}|$, then we have

$$\sum_{j=-\infty}^{h_i-1} |x_j^{(i+1)}| = \sum_{j=-\infty}^{h_i-1} |x_j^{(i)}| + \sum_{j=1}^{k} |b_{-j}| \quad\text{and}\quad \sum_{j=h_i+1}^{\infty} |x_j^{(i+1)}| = \sum_{j=h_i+1}^{\infty} |x_j^{(i)}| + \sum_{j=1}^{d} |b_j|.$$

If there exists a subsequence $(h_{i_j})_{1\le j\le J}$ such that $h_{i_j} \le h_m$ for all j, m with $i_j < m \le i_J$, then we have therefore $\sum_{j=-\infty}^{h_{i_J}-1} |x_j^{(i_J+1)}| \ge J \sum_{j=1}^{k} |b_{-j}|$, hence J is bounded if $\sum_{j=1}^{k} |b_{-j}| > 0$. Similarly, the length of subsequences $(h_{i_j})_{1\le j\le J}$ such that $h_{i_j} \ge h_m$ for all j, m with $i_j < m \le i_J$ is bounded if $\sum_{j=1}^{d} |b_j| > 0$. Since $h_{i+1} \le h_i + d$, no infinite sequence $(h_i)_{i\ge 0}$ can exist in this case and the algorithm terminates.

It remains to consider the case that $\sum_{j=1}^{k} |b_{-j}| = 0$ or $\sum_{j=1}^{d} |b_j| = 0$. Assume, w.l.o.g., $\sum_{j=1}^{d} |b_j| = 0$. Then we have $h_{i+1} \le h_i$ since $x_{h_i+j}^{(i+1)} = x_{h_i+j}^{(i)}$ for $j > 0$. If h_i exists for all $i \ge 0$, then both $\sum_{j=0}^{k} |x_{h_i-j}^{(i)}|$ and $\sum_{j=1}^{\infty} |x_{h_i+j}^{(i)}|$ must be eventually constant. Therefore we must have some i, i' with $h_{i'} < h_i$ such that $x_{h_{i'}-k}^{(i')} \cdots x_{h_{i'}}^{(i')} = x_{h_i-k}^{(i)} \cdots x_{h_i}^{(i)}$ and $x_{h_{i'}+1}^{(i')} x_{h_{i'}+2}^{(i')} \cdots = 0^{h_i-h_{i'}} x_{h_i+1}^{(i)} x_{h_i+2}^{(i)} \cdots$. Since $\sum_{j=0}^{k} |x_{h_i-j}^{(i)}| > 0$, this implies $\beta^{h_i-h_{i'}} = 1$. In this case, it is easy to see that each $x \in \mathbb{Z}^*$ can be transformed into some $y \in \{-1,0,1\}^*$ with $y \sim_\beta x$ and $\|y\| = \|x\|$, and the proposition is proved. □

In order to understand the relation $\sim_\beta$ on $\{-c,\ldots,c\}^*$, we have to consider the set

$$Z_\beta(2c) = \Big\{ z_1 \cdots z_n \in \{-2c,\ldots,2c\}^* \;\Big|\; n \ge 0,\ \sum_{j=1}^{n} z_j \beta^{-j} = 0 \Big\}.$$

We recall a result from [12]. All the automata considered in this paper process words from left to right, that is to say, most significant digit first.

Theorem 3.3. *If β is a Pisot number, then the set $Z_\beta(2c)$ is recognized by a finite automaton.*

For convenience, we quickly explain the construction of the automaton $\mathcal{A}_\beta(2c)$ recognizing $Z_\beta(2c)$. The states of $\mathcal{A}_\beta(2c)$ are 0 and all $s \in \mathbb{Z}[\beta] \cap (\frac{-2c}{\beta-1}, \frac{2c}{\beta-1})$ which are accessible from 0 by paths consisting of transitions $s \xrightarrow{e} s'$ with $e \in \{-2c,\ldots,2c\}$ such that $s' = \beta s + e$. The state 0 is both initial and terminal. When β is a Pisot number, then the set of states is finite. Note that the automaton $\mathcal{A}_\beta(2c)$ is symmetric, meaning that if $s \xrightarrow{e} s'$ is a transition, then $-s \xrightarrow{-e} -s'$ is also a transition. The automaton $\mathcal{A}_\beta(2c)$ is accessible and co-accessible.

The *redundancy automaton* (or transducer) $\mathcal{R}_\beta(c)$ is similar to $\mathcal{A}_\beta(2c)$. Each transition $s \xrightarrow{e} s'$ of $\mathcal{A}_\beta(2c)$ is replaced in $\mathcal{R}_\beta(c)$ by a set of transitions $s \xrightarrow{a|b} s'$, with $a, b \in \{-c,\ldots,c\}$ and $a - b = e$. From Theorem 3.3, one obtains the following proposition.

Proposition 3.4. *The redundancy transducer $\mathcal{R}_\beta(c)$ recognizes the set*

$$\big\{(x_1\cdots x_n, y_1\cdots y_n) \in A^* \times A^* \;\big|\; n \geq 0,\ {\bullet}x_1\cdots x_n = {\bullet}y_1\cdots y_n\big\},$$

where $A = \{-c, \ldots, c\}$. If β is a Pisot number, then $\mathcal{R}_\beta(c)$ is finite.

From the redundancy transducer $\mathcal{R}_\beta(c)$, one constructs another transducer $\mathcal{T}_\beta(c)$ with states of the form (s, δ), where s is a state of $\mathcal{R}_\beta(c)$ and $\delta \in \mathbb{Z}$. The transitions are of the form $(s, \delta) \xrightarrow{a|b} (s', \delta')$ if $s \xrightarrow{a|b} s'$ is a transition in $\mathcal{R}_\beta(c)$ and $\delta' = \delta + |b| - |a|$. The initial state is $(0, 0)$, and terminal states are of the form $(0, \delta)$ with $\delta < 0$. Of course, this transducer $\mathcal{T}_\beta(c)$ is not finite.

Proposition 3.5. *The transducer $\mathcal{T}_\beta(c)$ recognizes the set*

$$\big\{(x_1\cdots x_n, y_1\cdots y_n) \in A^* \times A^* \;\big|\; {\bullet}x_1\cdots x_n = {\bullet}y_1\cdots y_n,\ \|y_1\cdots y_n\| < \|x_1\cdots x_n\|\big\}.$$

For the proof of Theorem 3.1, we use the following general construction.

Lemma 3.6. *Let $H \subset A^*$ and $M = A^* \setminus A^*HA^*$. If H is recognized by a finite automaton, then so is M.*

Proof. Suppose that H is recognized by a finite automaton $\mathcal{H}$. Let P be the set of strict prefixes of H. We construct the minimal automaton $\mathcal{M}$ of M as follows. The set of states of $\mathcal{M}$ is the quotient $P/_\equiv$ where $p \equiv q$ if p and q arrive at the same set of states in $\mathcal{H}$. Since $\mathcal{H}$ is finite, $P/_\equiv$ is finite. Transitions are defined as follows. Let a be in A. There is a transition $p \xrightarrow{a} q$ if pa is in P and $q = [pa]_\equiv$, or if pa is not in P, $p = uv$ with v in P maximal in length, and $q = [v]_\equiv$. Every state is terminal. □

Proof of Theorem 3.1. Let $A = \{-c, \ldots, c\}$, $x \in A^*$ be a strictly β-heavy word and $y \in A^*$ be a β-expansion of minimal weight with $x \sim_\beta y$. Such a y exists because of Proposition 3.2. Extend x, y to words x', y' by adding leading and trailing zeros such that $x' = x_1\cdots x_n$, $y' = y_1\cdots y_n$ and ${\bullet}x_1\cdots x_n = {\bullet}y_1\cdots y_n$. Then there is a path in the transducer $\mathcal{T}_\beta(c)$ composed of transitions $(s_{j-1}, \delta_{j-1}) \xrightarrow{x_j|y_j} (s_j, \delta_j)$, $1 \leq j \leq n$, with $s_0 = 0$, $\delta_0 = 0$, $s_n = 0$, $\delta_n < 0$.

We determine bounds for δ_j, $1 \leq j \leq n$, which depend only on the state $s = s_j$. Choose a β-expansion of s, $s = a_1\cdots a_i{\bullet}a_{i+1}\cdots a_m$, and set $w_s = \|a_1\cdots a_m\|$. If $\delta_j > w_s$, then we have $\|y_1\cdots y_j\| > \|x_1\cdots x_j\| + w_s$. Since $s_j = (x_1-y_1)\cdots(x_j-y_j){\bullet}$, the digitwise subtraction of $0^{\max(i-j,0)}x_1\cdots x_j0^{m-i}$ and $0^{\max(j-i,0)}a_1\cdots a_m$ provides a word which is β-lighter than $y_1\cdots y_j$, which contradicts the assumption that y is a β-expansion of minimal weight.

Let $W = \max\{w_s \mid s \text{ is a state in } \mathcal{A}_\beta(2c)\}$. If $\delta_j < -W - c$, then let $h \leq j$ be such that $x_h \neq 0$, $x_i = 0$ for $h < i \leq j$. Since $|x_h| \leq c$, we have $\delta_{h-1} \leq \delta_j + c < -W \leq -w_{s_{h-1}}$, hence $\|x_1\cdots x_{h-1}\| > \|y_1\cdots y_{h-1}\| + w_{s_{h-1}}$. Let $a_1\cdots a_m$ be the word which was used for the definition of $w_{s_{h-1}}$, i.e., $s_{h-1} = a_1\cdots a_i{\bullet}a_{i+1}\cdots a_m$, $w_{s_{h-1}} = \|a_1\cdots a_m\|$. Then the digitwise addition of $0^{\max(i-h+1,0)}y_1\cdots y_{h-1}0^{m-i}$ and $0^{\max(h-1-i,0)}a_1\cdots a_m$ provides a word which is β-lighter than $x_1\cdots x_{h-1}$. Since $x_h \neq 0$, this contradicts the assumption that x is strictly β-heavy.

Let $\mathcal{S}_\beta(c)$ be the restriction of $\mathcal{T}_\beta(c)$ to the states (s, δ) with $-W - c \leq \delta \leq w_s$ with some additional initial and terminal states: Every state which can be reached from $(0, 0)$ by a path with input in 0^* is initial, and every state with a path to $(0, \delta)$, $\delta < 0$, with an input in 0^* is terminal. Then the set H which is recognized by the input automaton of $\mathcal{S}_\beta(c)$ consists only of β-heavy words and contains all strictly β-heavy words in A^*. Therefore the set M given by Lemma 3.6 is the set of β-expansions of minimal weight in A^*. ∎

4 Golden Ratio case

In this section we give explicit constructions for the case where β is the Golden Ratio $\frac{1+\sqrt{5}}{2}$. We have $1 = \bullet 110^\omega$, hence the condition of Example 1.1 is satisfied and $B = 2$. The digit -1 will be written as $\bar{1}$ in words and transitions.

4.1 β-expansions of minimal weight for $\beta = \frac{1+\sqrt{5}}{2}$

Lemma 4.1. *All words in $\{-1, 0, 1\}^*$ which are not recognized by the automaton $\mathcal{M}_\beta$ in Figure 1 (where all states are terminal) are β-heavy.*

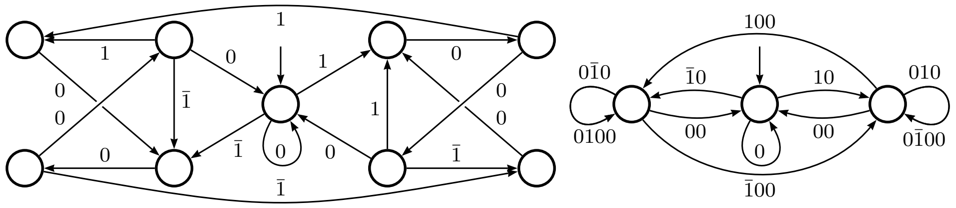

Figure 1: Automaton $\mathcal{M}_\beta$ recognizing β-expansions of minimal weight for $\beta = \frac{1+\sqrt{5}}{2}$ (left) and a compact representation of $\mathcal{M}_\beta$ (right).

Proof. The transducer in Figure 2 is a part of $\mathcal{S}_\beta(1)$, which is constructed in the proof of Theorem 3.1. The set of inputs of paths accepted by it is

$$H = 1(0100)^*1 \,\cup\, 1(0100)^*0101 \,\cup\, 1(00\bar{1}0)^*\bar{1} \,\cup\, 1(00\bar{1}0)^*0\bar{1}$$
$$\cup\, \bar{1}(0\bar{1}00)^*\bar{1} \,\cup\, \bar{1}(0\bar{1}00)^*0\bar{1}0\bar{1} \,\cup\, \bar{1}(0010)^*1 \,\cup\, \bar{1}(0010)^*01$$

and $\mathcal{M}_\beta$ is constructed as in the proof of Lemma 3.6. ∎

Proposition 4.2. *If $\beta = \frac{1+\sqrt{5}}{2}$, then every $z \in \mathbb{R}$ has a β-expansion of the form $z = y_1 \cdots y_k \bullet y_{k+1} y_{k+2} \cdots$ with $y_j \in \{-1, 0, 1\}$ such that $y_1 y_2 \cdots$ avoids the set $X = \{11, 101, 1001, 1\bar{1}, 10\bar{1},$ and their opposites$\}$. If $z \in \mathbb{Z}[\beta] = \mathbb{Z}[\beta^{-1}]$, then this expansion is unique up to leading zeros.*

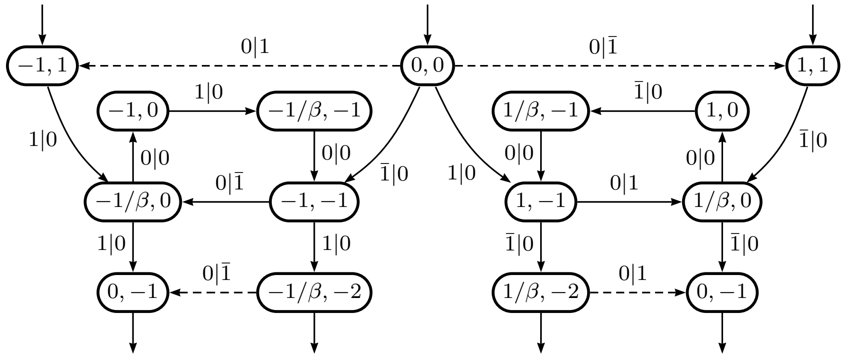

Figure 2. Transducer with strictly β-heavy words as inputs, $\beta = \frac{1+\sqrt{5}}{2}$.

Proof. We determine this β-expansion similarly to the greedy β-expansion in the Introduction. Note that the sequence $x_1x_2\cdots$ avoiding the elements of X with maximal value $\boldsymbol{.}x_1x_2\cdots$ is $(1000)^\omega$, $\boldsymbol{.}(1000)^\omega = \beta^2/(\beta^2+1)$. Consider first $z \in \big[\frac{-\beta^2}{\beta^2+1}, \frac{\beta^2}{\beta^2+1}\big)$. If we define the transformation

$$\tau:\ \left[\frac{-\beta^2}{\beta^2+1}, \frac{\beta^2}{\beta^2+1}\right) \to \left[\frac{-\beta^2}{\beta^2+1}, \frac{\beta^2}{\beta^2+1}\right), \quad \tau(z) = \beta z - \left\lfloor \frac{\beta^2+1}{2\beta} z + 1/2 \right\rfloor,$$

and set $y_j = \big\lfloor \frac{\beta^2+1}{2\beta}\tau^{j-1}(z) + 1/2 \big\rfloor$ for $j \geq 1$, then we have $z = \boldsymbol{.}y_1y_2\cdots$. If $y_j = 1$ for some $j \geq 1$, then we have $\tau^j(z) \in \beta \times \big[\frac{\beta}{\beta^2+1}, \frac{\beta^2}{\beta^2+1}\big) - 1 = \big[\frac{-1}{\beta^2+1}, \frac{1/\beta}{\beta^2+1}\big)$, hence $y_{j+1} = 0$, $y_{j+2} = 0$, and $\tau^{j+2}(z) \in \big[\frac{-\beta^2}{\beta^2+1}, \frac{\beta}{\beta^2+1}\big)$, hence $y_{j+3} \in \{\bar{1}, 0\}$. This shows that the given factors are avoided. A similar argument for $y_j = -1$ shows that the opposites are avoided as well, hence we have shown the existence of the expansion for $z \in \big[\frac{-\beta^2}{\beta^2+1}, \frac{\beta^2}{\beta^2+1}\big)$. For arbitrary $z \in \mathbb{R}$, the expansion is given by shifting the expansion of $z\beta^{-k}$, $k \geq 0$, to the left.

If we choose $y_j = 0$ in case $\tau^{j-1}(z) > \beta/(\beta^2+1) = \boldsymbol{.}(0100)^\omega$, then it is impossible to avoid the factors 11, 101 and 1001 in the following. If we choose $y_j = 1$ in case $\tau^{j-1}(z) < \beta/(\beta^2+1)$, then $\beta\tau^{j-1}(z) - 1 < -1/(\beta^2+1) = \boldsymbol{.}(00\bar{1}0)^\omega$, and thus it is impossible to avoid the factors $1\bar{1}$, $10\bar{1}$, $\bar{1}\bar{1}$, $\bar{1}0\bar{1}$ and $\bar{1}00\bar{1}$. Since $\beta/(\beta^2+1) \notin \mathbb{Z}[\beta]$, we have $\tau^{j-1}(z) \neq \beta/(\beta^2+1)$ for $z \in \mathbb{Z}[\beta]$. Similar relations hold for the opposites, thus the expansion is unique. ☐

Remark 4.3. Similarly, the transformation $\tau(z) = \beta z - \lfloor z + 1/2 \rfloor$ on $[-\beta/2, \beta/2)$ provides for every $z \in \mathbb{Z}[\beta]$ a unique expansion avoiding the factors 11, 101, $1\bar{1}$, $10\bar{1}$, $100\bar{1}$ and their opposites.

Lemma 4.4. *If $x \in \{-1,0,1\}^*$ is accepted by $\mathcal{M}_\beta$, then there exists $y \in \{-1,0,1\}^*$ avoiding the set X of Proposition 4.2 with $x \sim_\beta y$ and $\|x\| = \|y\|$.*

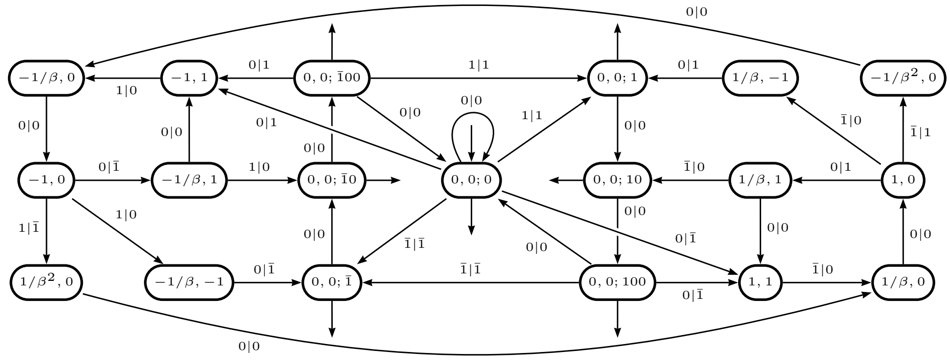

Figure 3. Transducer $\mathcal{N}_\beta$ normalizing β-expansions of minimal weight, $\beta = \frac{1+\sqrt{5}}{2}$.

Proof. We show that the conversion of an arbitrary expansion accepted by $\mathcal{M}_\beta$ into the expansion avoiding X is done by the transducer $\mathcal{N}_\beta$ in Figure 3. Set

$$
\begin{aligned}
Q_0 &= \{(0,0;0),\, (-1,1),\, (1,1)\} = Q'_0, \\
Q_1 &= \{(0,0;1),\, (-1/\beta,0)\}, & Q'_1 &= \{(0,0;\bar{1}0)\}, \\
Q_{10} &= \{(0,0;10),\, (-1,0)\}, & Q'_{10} &= \{(0,0;\bar{1}00)\}, \\
Q_{100} &= \{(0,0;100),\, (-1/\beta,1)\}, & Q'_{100} &= \{(0,0;0),\, (-1,1)\}, \\
Q_{101} &= \{(-1/\beta,-1),\, (1/\beta^2,0)\}, & Q'_{101} &= \{(0,0;1)\}.
\end{aligned}
$$

Then the paths in $\mathcal{N}_\beta$ with input in 00^* lead to the three states in Q_0, the paths with input 01 lead to the two states in Q_1, and more generally the paths in $\mathcal{N}_\beta$ with input $0x$ such that x is accepted by $\mathcal{M}_\beta$ lead to all states in Q_u or to all states in Q'_u, where u labels the shortest path in $\mathcal{M}_\beta$ leading to the state reached by x. Moreover Q_u, Q'_u are given by symmetry if they are not in the above list. Indeed, if $u \xrightarrow{a} v$ is a transition in $\mathcal{M}_\beta$, then we have $Q_u \xrightarrow{a} Q_v$ or $Q_u \xrightarrow{a} Q'_v$, and $Q'_u \xrightarrow{a} Q_v$ or $Q'_u \xrightarrow{a} Q'_v$, where $Q \xrightarrow{a} R$ means that for every $r \in R$ there exists a transition $q \xrightarrow{a|b} r$ in $\mathcal{N}_\beta$ with $q \in Q$.

Since every Q_u and every Q'_u contains a state q with a transition of the form $q \xrightarrow{0|b} (0,0;w)$, there exists a path with input $0x0$ going from $(0,0;0)$ to $(0,0;w)$ for every word x accepted by $\mathcal{M}_\beta$. By construction, the output y of this path satisfies $x \sim_\beta y$ and $\|x\| = \|y\|$. It can be easily checked that all outputs of $\mathcal{N}_\beta$ avoid the factors in X. ◻

By Proposition 4.2, the word y in Lemma 4.4 is unique up to leading and trailing zeros and does not change if we replace x by some x' accepted by $\mathcal{M}_\beta$ with $x' \sim_\beta x$. Therefore all these x' satisfy $\|x'\| = \|y\| = \|x\|$. By Proposition 3.2 and Lemma 4.1, there exists a β-expansions of minimal weight x' accepted by $\mathcal{M}_\beta$ with $x' \sim_\beta x$, and we obtain the following theorem.

Theorem 4.5. *The set of* $\frac{1+\sqrt{5}}{2}$*-expansions of minimal weight in* $\{-1,0,1\}^*$ *is recognized by the finite automaton* $\mathcal{M}_\beta$ *of Figure 1 where all states are terminal.*

4.2 Branching transformation

All β-expansions of minimal weight can be obtained by a branching transformation.

Theorem 4.6. *Let* $x = x_1 \cdots x_n \in \{-1, 0, 1\}^*$ *and* $z = \mathbf{.}x_1 \cdots x_n$, $\beta = \frac{1+\sqrt{5}}{2}$. *Then* x *is a* β*-expansion of minimal weight if and only if* $-\frac{2\beta}{\beta^2+1} < z < \frac{2\beta}{\beta^2+1}$ *and*

$$x_j = \begin{cases} 1 & \text{if } \frac{2}{\beta^2+1} < \beta^{j-1} z - x_1 \cdots x_{j-1}\mathbf{.} < \frac{2\beta}{\beta^2+1} \\ 0 \text{ or } 1 & \text{if } \frac{\beta}{\beta^2+1} < \beta^{j-1} z - x_1 \cdots x_{j-1}\mathbf{.} < \frac{2}{\beta^2+1} \\ 0 & \text{if } \frac{-\beta}{\beta^2+1} < \beta^{j-1} z - x_1 \cdots x_{j-1}\mathbf{.} < \frac{\beta}{\beta^2+1} \\ -1 \text{ or } 0 & \text{if } \frac{-2}{\beta^2+1} < \beta^{j-1} z - x_1 \cdots x_{j-1}\mathbf{.} < \frac{-\beta}{\beta^2+1} \\ -1 & \text{if } \frac{-2\beta}{\beta^2+1} < \beta^{j-1} z - x_1 \cdots x_{j-1}\mathbf{.} < \frac{-2}{\beta^2+1} \end{cases} \quad \text{for all } j,\ 1 \le j \le n.$$

The sequence $(\beta^{j-1} z - x_1 \cdots x_{j-1}\mathbf{.})_{1 \le j \le n}$ is a trajectory $(\tau^{j-1}(z))_{1 \le j \le n}$, where the branching transformation $\tau : z \mapsto \beta z - x_1$ with $x_1 \in \{-1, 0, 1\}$ is given in Figure 4.

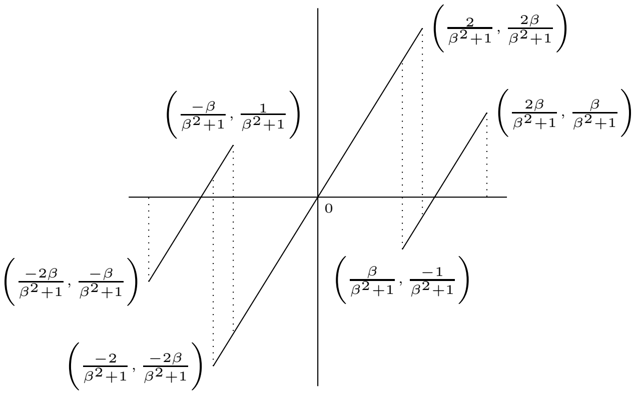

Figure 4. Branching transformation giving all $\frac{1+\sqrt{5}}{2}$-expansions of minimal weight.

Proof. To see that all words $x_1 \cdots x_n$ given by the branching transformation are β-expansions of minimal weight, we have drawn in Figure 5 an automaton where every state is labeled by the interval containing all numbers $\beta^j z - x_1 \cdots x_j\mathbf{.}$ such that $x_1 \cdots x_j$ labels a path leading to this state. This automaton turns out to be the automaton $\mathcal{M}_\beta$ in Figure 1 (up to the labels of the states), which accepts exactly the β-expansions of minimal weight. Recall that $\mathbf{.}(0010)^\omega = \frac{1}{\beta^2+1}$ and thus $\mathbf{.}1(0100)^\omega = \frac{2\beta}{\beta^2+1}$.

If the conditions on z and x_j are not satisfied, then we have either $|\mathbf{.}x_j \cdots x_n| > \mathbf{.}1(0100)^\omega$, or $x_j = 1$ and $\mathbf{.}x_{j+1} \cdots x_n < \mathbf{.}(00\bar{1}0)^\omega$, or $x_j = -1$ and $\mathbf{.}x_{j+1} \cdots x_n > \mathbf{.}(0010)^\omega$ for some j, $1 \le j \le n$. In every case, it is easy to see that $x_j \cdots x_n$ must contain a factor in the set H of the proof of Lemma 4.1, hence $x_1 \cdots x_n$ is β-heavy. $\square$

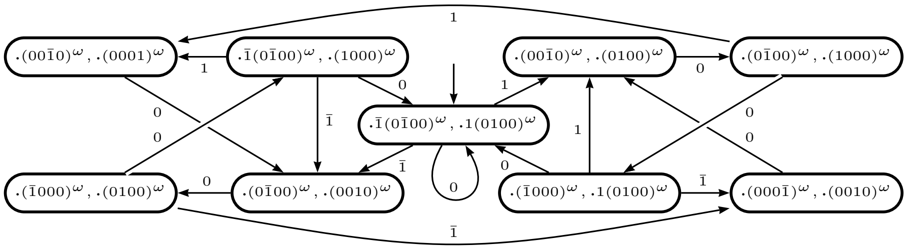

Figure 5. Automaton $\mathcal{M}_\beta$ with intervals as labels.

4.3 Fibonacci numeration system

The reader is referred to [18, Chapter 7] for definitions on numeration systems defined by a sequence of integers. Recall that the linear numeration system canonically associated with the Golden Ratio is the Fibonacci (or Zeckendorf) numeration system defined by the sequence of Fibonacci numbers $F = (F_n)_{n \geq 0}$ with $F_n = F_{n-1} + F_{n-2}$, $F_0 = 1$ and $F_1 = 2$. Any non-negative integer $N < F_n$ can be represented as $N = \sum_{j=1}^n x_j F_{n-j}$ with the property that $x_1 \cdots x_n \in \{0,1\}^*$ does not contain the factor 11. For words $x = x_1 \cdots x_n \in \mathbb{Z}^*$, $y = y_1 \cdots y_m \in \mathbb{Z}^*$, we define a relation

$$x \sim_F y \quad \text{if and only if} \quad \sum_{j=1}^n x_j F_{n-j} = \sum_{j=1}^m y_j F_{m-j}.$$

The properties *F-heavy* and *F-expansion of minimal weight* are defined as for β-expansions, with $\sim_F$ instead of $\sim_\beta$. An important difference between the notions F-heavy and β-heavy is that a word containing a F-heavy factor need not be F-heavy, e.g. 2 is F-heavy since $2 \sim_F 10$, but 20 is not F-heavy. However, uxv is F-heavy if $x0^{\text{length}(v)}$ is F-heavy. Therefore we say that $x \in \mathbb{Z}^*$ is *strongly F-heavy* if every element in $x0^*$ is F-heavy. Hence every word containing a strongly F-heavy factor is F-heavy.

The Golden Ratio satisfies (D′) since $2 = 10{\bullet}01$. For the Fibonacci numbers, the corresponding relation is $2F_n = F_{n+1} + F_{n-2}$, hence $20^n \sim_F 10010^{n-2}$ for all $n \geq 2$. Since $20 \sim_F 101$ and $2 \sim_F 10$, we obtain similarly to the proof of Proposition 3.2 that for every $x \in \mathbb{Z}^*$ there exists some $y \in \{-1,0,1\}^*$ with $x \sim_F y$ and $\|y\| \leq \|x\|$. We will show the following theorem.

Theorem 4.7. *The set of F-expansions of minimal weight in $\{-1,0,1\}^*$ is equal to the set of β-expansions of minimal weight in $\{-1,0,1\}^*$ for $\beta = \frac{\sqrt{5}+1}{2}$.*

The proof of this theorem runs along the same lines as the proof of Theorem 4.5. We use the unique expansion of integers given by Proposition 4.8 (due to Heuberger [15]) and provide an alternative proof of Heuberger's result that these expansions are F-expansions of minimal weight.

Proposition 4.8 ([15]). *Every $N \in \mathbb{Z}$ has a unique representation $N = \sum_{j=1}^n y_j F_{n-j}$ with $y_1 \neq 0$ and $y_1 \cdots y_n \in \{-1,0,1\}^*$ avoiding $X = \{11, 101, 1001, 1\bar{1}, 10\bar{1}$, and their opposites$\}$.*

Proof. Let g_n be the smallest positive integer with an F-expansion of length n starting with 1 and avoiding X, and G_n be the largest integer of this kind. Since $g_{n+1} \sim_F 1(00\bar{1}0)^{n/4}$, $G_n \sim_F (1000)^{n/4}$ and $1(\bar{1}0\bar{1}0)^{n/4} \sim_F 1$, we obtain $g_{n+1} - G_n = 1$. (A fractional power $(y_1 \cdots y_k)^{j/k}$ denotes the word $(y_1 \cdots y_k)^{\lfloor j/k \rfloor} y_1 \cdots y_{j-\lfloor j/k \rfloor k}$.) Therefore the length n of an expansion $y_1 y_2 \cdots y_n$ of $N \neq 0$ with $y_1 \neq 0$ avoiding X is determined by $G_{n-1} < |N| \leq G_n$. Since $g_n - F_{n-1} = -G_{n-3}$ and $G_n - F_{n-1} = G_{n-4}$, we have $-G_{n-3} \leq N - F_{n-1} \leq G_{n-4}$ if $y_1 = 1$, hence $y_2 = y_3 = 0$, $y_4 \neq 1$, and we obtain recursively that N has a unique expansion avoiding X. □

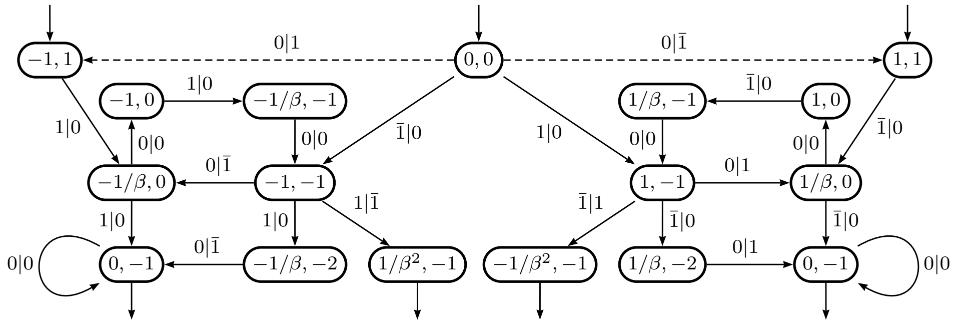

Figure 6. All inputs of this transducer are strongly F-heavy.

Proof of Theorem 4.7. Let $a_1 \cdots a_n \in \mathbb{Z}^*$, $z = \sum_{j=1}^{n} a_j \beta^{n-j}$, $N = \sum_{j=1}^{n} a_j F_{n-j}$. By using the equations $\beta^k = \beta^{k-1} + \beta^{k-2}$ and $F_k = F_{k-1} + F_{k-2}$, we obtain integers m_0 and m_1 such that $z = m_1 \beta + m_0$ and $N = m_1 F_1 + m_0 F_0 = 2m_1 + m_0$. Clearly, $z = 0$ implies $m_1 = m_0 = 0$ and thus $N = 0$, but the converse is not true: $N = 0$ only implies $m_0 = -2m_1$, i.e., $z = -m_1/\beta^2$. Therefore we have $x_1 \cdots x_n \sim_F y_1 \cdots y_n$ if and only if $(x_1 - y_1) \cdots (x_n - y_n)_{\bullet} = m/\beta^2$ for some $m \in \mathbb{Z}$, hence the redundancy transducer $\mathcal{R}_F(1)$ for the Fibonacci numeration system is similar to $\mathcal{R}_\beta(1)$, except that all states m/β^2, $m \in \mathbb{Z}$, are terminal.

The transducer in Figure 6 shows that all strictly β-heavy words in $\{-1, 0, 1\}^*$ are strongly F-heavy. Therefore all words which are not accepted by $\mathcal{M}_\beta$ are F-heavy. Let $\mathcal{N}_F$ be as $\mathcal{N}_\beta$, except that the states $(\pm 1/\beta^2, 0)$ are terminal. Every set Q_u and Q'_u contains a state of the form $(0, 0; w)$ or $(\pm 1/\beta^2, 0)$. If x is accepted by $\mathcal{N}_\beta$, then $\mathcal{N}_F$ transforms therefore $0x$ into a word y avoiding the factors given in Proposition 4.8. Hence x is an F-expansion of minimal weight. □

Remark 4.9. If we consider only expansions avoiding the factors 11, 101, $1\bar{1}$, $10\bar{1}$, $100\bar{1}$, then the difference between the largest integer with expansion of length n and the smallest positive integer with expansion of length $n+1$ is 2 if n is a positive multiple of 3. Therefore there exist integers without an expansion of this kind, e.g. $N = 4$. However, a small modification provides another "nice" set of F-expansions of minimal weight: Every integer has a unique representation of the form $N = \sum_{j=1}^{n} y_j F_{n-j}$ with

$y_1 \neq 0$, $y_1 \cdots y_n \in \{\bar{1}, 0, 1\}^*$ avoiding the factors $11, \bar{1}\bar{1}, \bar{1}0\bar{1}, 1\bar{1}, \bar{1}1, 10\bar{1}, \bar{1}01, 100\bar{1}$ and $y_{j-2}y_{j-1}y_j = 101$ or $y_{j-3} \cdots y_j = \bar{1}001$ only if $j = n$.

4.4 Weight of the expansions

In this section, we study the average weight of F-expansions of minimal weight. For every $N \in \mathbb{Z}$, let $\|N\|_F$ be the weight of a corresponding F-expansion of minimal weight, i.e., $\|N\|_F = \|x\|$ if x is an F-expansion of minimal weight with $x \sim_F N$.

Theorem 4.10. *For positive integers M, we have, as $M \to \infty$,*

$$\frac{1}{2M+1} \sum_{N=-M}^{M} \|N\|_F = \frac{1}{5} \frac{\log M}{\log \frac{1+\sqrt{5}}{2}} + \mathcal{O}(1).$$

Proof. Consider first $M = G_n$ for some $n > 0$, where G_n is defined as in the proof of Proposition 4.8, and let W_n be the set of words $x = x_1 \cdots x_n \in \{-1, 0, 1\}^n$ avoiding $11, 101, 1001, 1\bar{1}, 10\bar{1}$, and their opposites. Then we have

$$\frac{1}{2G_n+1} \sum_{N=-G_n}^{G_n} \|N\|_F = \frac{1}{\#W_n} \sum_{x \in W_n} \|x\| = \sum_{j=1}^{n} \mathbf{E}\, X_j,$$

where $\mathbf{E}\, X_j$ is the expected value of the random variable X_j defined by

$$\Pr[X_j = 1] = \frac{\#\{x_1 \cdots x_n \in W_n : x_j \neq 0\}}{\#W_n}, \Pr[X_j = 0] = \frac{\#\{x_1 \cdots x_n \in W_n : x_j = 0\}}{\#W_n}$$

Instead of $(X_j)_{1 \le j \le n}$, we consider the sequence of random variables $(Y_j)_{1 \le j \le n}$ defined by

$$\begin{aligned}&\Pr[Y_1 = y_1y_2y_3, \ldots, Y_j = y_jy_{j+1}y_{j+2}] \\ &\qquad\qquad = \#\{x_1 \cdots x_{n+2} \in W_n00 :\, x_1 \cdots x_{j+2} = y_1 \cdots y_{j+2}\}/\#W_n,\end{aligned}$$

$\Pr[Y_{j-1} = xyz, Y_j = x'y'z'] = 0$ if $x' \neq y$ or $y' \neq z$. It is easy to see that $(Y_j)_{1 \le j \le n}$ is a Markov chain, where the non-trivial transition probabilities are given by

$$\begin{aligned}1 - \Pr[Y_{j+1} = 000 \mid Y_j = 100] = \Pr[Y_{j+1} = 00\bar{1} \mid Y_j = 100] &= \frac{G_{n-j-2} - G_{n-j-3}}{G_{n-j+1} - G_{n-j}}, \\ 1 - 2\Pr[Y_{j+1} = 001 \mid Y_j = 000] = \Pr[Y_{j+1} = 000 \mid Y_j = 000] &= \frac{2G_{n-j-3} + 1}{2G_{n-j-2} + 1},\end{aligned}$$

and the opposite relations. Since $G_n = c\beta^n + \mathcal{O}(1)$ (with $\beta = \frac{1+\sqrt{5}}{2}$, $c = \beta^3/5$), the transition probabilities satisfy $\Pr[Y_{j+1} = v \mid Y_j = u] = p_{u,v} + \mathcal{O}(\beta^{-n+j})$ with

$$(p_{u,v})_{u,v\in\{100,010,001,000,00\bar{1},0\bar{1}0,00\bar{1}\}} = \begin{pmatrix} 0 & 0 & 0 & \frac{2}{\beta^2} & \frac{1}{\beta^3} & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2\beta^2} & \frac{1}{\beta} & \frac{1}{2\beta^2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & \frac{1}{\beta^3} & \frac{2}{\beta^2} & 0 & 0 & 0 \end{pmatrix}.$$

The eigenvalues of this matrix are $1, \frac{-1}{\beta}, \frac{\pm i}{\beta}, \frac{1\pm i\sqrt{3}}{2\beta}, \frac{-1}{\beta^2}$. The stationary distribution vector (given by the left eigenvector to the eigenvalue 1) is $(\frac{1}{10}, \frac{1}{10}, \frac{1}{10}, \frac{2}{5}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10})$, thus we have

$$\mathbf{E}\, X_j = \Pr[Y_j = 100] + \Pr[Y_j = \bar{1}00] = 1/5 + \mathcal{O}\big(\beta^{-\min(j,n-j)}\big),$$

cf. [9]. This proves the theorem for $M = G_n$.

If $G_n < M \le G_{n+1}$, then we have $\|N\|_F = 1 + \|N - F_n\|_F$ if $G_n < N \le M$, and a similar relation for $-M \le N < -G_n$. With $G_n + 1 - F_n = -G_{n-2}$, we obtain

$$\begin{aligned} \sum_{N=-M}^{M} \|N\|_F &= \sum_{N=-G_n}^{G_n} \|N\|_F + \sum_{N=-G_{n-2}}^{M-F_n} (1 + \|N\|_F) + \sum_{N=F_n-M}^{G_{n-2}} (1 + \|N\|_F) \\ &= \sum_{N=-G_n}^{G_n} \|N\|_F + \sum_{N=-G_{n-2}}^{G_{n-2}} \|N\|_F + \operatorname{sgn}(M - F_n) \sum_{N=-|M-F_n|}^{|M-F_n|} \|N\|_F + \mathcal{O}(M) \\ &= \frac{2}{5\log\beta}\big(F_n \log M + (M - F_n)\log|M - F_n|\big) + \mathcal{O}(M) = \frac{2M\log M}{5\log\beta} + \mathcal{O}(M) \end{aligned}$$

by induction on n and using $\frac{M-F_n}{M}\log|\frac{M-F_n}{M}| = \mathcal{O}(1)$. ∎

Remark 4.11. As in [9], a central limit theorem for the distribution of $\|N\|_F$ can be proved, even if we restrict the numbers N to polynomial sequences or prime numbers.

Remark 4.12. If we partition the interval $\big[\frac{-\beta^2}{\beta^2+1}, \frac{\beta^2}{\beta^2+1}\big)$, where the transformation $\tau : z \mapsto \beta z - \big\lfloor \frac{\beta^2+1}{2\beta} z + 1/2 \big\rfloor$ of the proof of Proposition 4.2 is defined, into intervals $I_{\bar{1}00} = \big[\frac{-\beta^2}{\beta^2+1}, \frac{-\beta}{\beta^2+1}\big)$, $I_{0\bar{1}0} = \big[\frac{-\beta}{\beta^2+1}, \frac{-1}{\beta^2+1}\big)$, $I_{00\bar{1}} = \big[\frac{-1}{\beta^2+1}, \frac{-1/\beta}{\beta^2+1}\big)$, $I_{000} = \big[\frac{-1/\beta}{\beta^2+1}, \frac{1/\beta}{\beta^2+1}\big)$, $I_{001} = \big[\frac{1/\beta}{\beta^2+1}, \frac{1}{\beta^2+1}\big)$, $I_{010} = \big[\frac{1}{\beta^2+1}, \frac{\beta}{\beta^2+1}\big)$, $I_{100} = \big[\frac{\beta}{\beta^2+1}, \frac{\beta^2}{\beta^2+1}\big)$, then we have $p_{u,v} = \lambda(\tau(I_u) \cap I_v)/\lambda(\tau(I_u))$, where λ denotes the Lebesgue measure.

5 Tribonacci case

In this section, let $\beta > 1$ be the Tribonacci number, $\beta^3 = \beta^2 + \beta + 1$ ($\beta \approx 1.839$). Since $1 = \mathbf{.}1110^\omega$, the condition of Example 1.1 is satisfied. The proofs of the results in this section run along the same lines as in the Golden Ratio case. Therefore we give only an outline of them and point out the differences to the Golden Ratio case.

5.1 β-expansions of minimal weight

All words which are not accepted by the automaton $\mathcal{M}_\beta$ in Figure 7, where all states are terminal, are β-heavy since they contain a factor which is accepted by the input automaton of $\mathcal{S}_\beta$ (without the dashed arrows) in Figure 8.

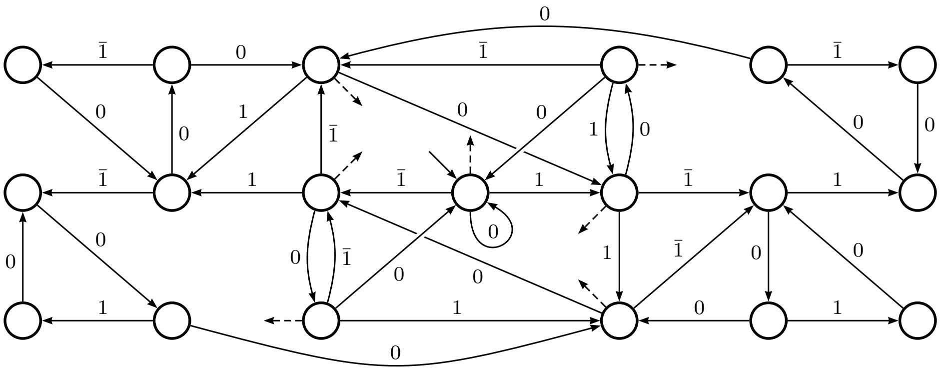

Figure 7. Automata $\mathcal{M}_\beta$, $\beta^3 = \beta^2 + \beta + 1$, and $\mathcal{M}_T$.

Proposition 5.1. *If $\beta > 1$ is the Tribonacci number, then every $z \in \mathbb{R}$ has a β-expansion of the form $z = y_1 \cdots y_k \centerdot y_{k+1} y_{k+2} \cdots$ with $y_j \in \{-1, 0, 1\}$ such that $y_1 y_2 \cdots$ avoids the set $X = \{11, 101, 1\bar{1},$ and their opposites$\}$. If $z \in \mathbb{Z}[\beta] = \mathbb{Z}[\beta^{-1}]$, then this expansion is unique up to leading zeros.*

The expansion in Proposition 5.1 is provided by the transformation

$$\tau : \left[\frac{-\beta}{\beta+1}, \frac{\beta}{\beta+1}\right) \to \left[\frac{-\beta}{\beta+1}, \frac{\beta}{\beta+1}\right), \quad \tau(z) = \beta z - \left\lfloor \frac{\beta+1}{2} z + \frac{1}{2} \right\rfloor .$$

Note that the word avoiding X with maximal value is $(100)^\omega$, $\centerdot(100)^\omega = \frac{\beta}{\beta+1}$.

Remark 5.2. The transformation $\tau(z) = \beta z - \lfloor \frac{\beta^2-1}{2} z + \frac{1}{2} \rfloor$ on $\left[\frac{-\beta}{\beta^2-1}, \frac{\beta}{\beta^2-1}\right)$ provides a unique expansion avoiding the factors 11, $1\bar{1}$, $10\bar{1}$ and their opposites.

If x is a word accepted by $\mathcal{M}_\beta$, then there exists a path in the transducer $\mathcal{N}_\beta$ in Figure 9 going from $(0,0;0)$ to a state $(0,0;w)$ with input $0x0^4$ and output of the same weight avoiding the set X given by Proposition 5.1. The sets Q_u and Q'_u are given by

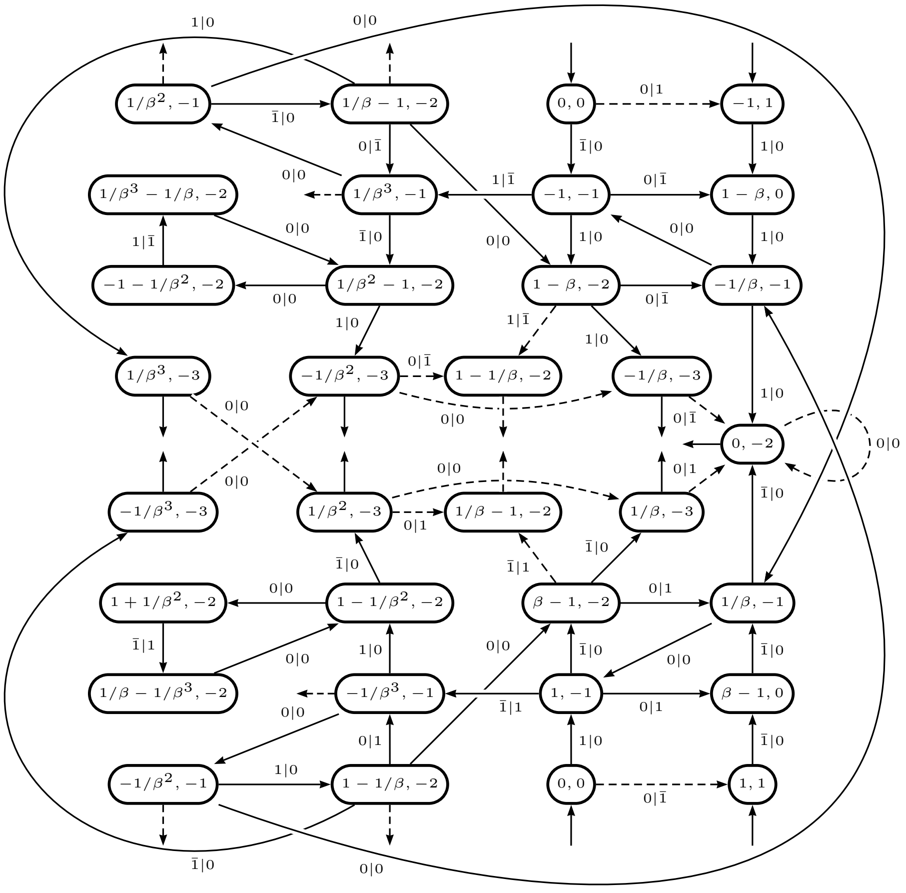

Figure 8. The relevant part of $\mathcal{S}_\beta(1)$, $\beta^3 = \beta^2 + \beta + 1$, and $\mathcal{S}_T(1)$.

$$Q_0 = \{(0,0;0),\,(1,1),\,(-1,1)\} = Q'_0, \quad Q_{1\bar{1}10\bar{1}} = \{(1/\beta-1,-2)\} = Q'_{1\bar{1}10\bar{1}},$$

$$Q_1 = \{(0,0;1),\,(1,-1),\,(1-\beta,0;0)\}, \qquad Q'_1 = \{(0,0;\bar{1}0),\,(1,-1),\,(1-\beta,0;\bar{1})\},$$

$$Q_{10} = \{(0,0;10),\,(\beta-1,0;1),\,(-1-1/\beta,0),\,(-1/\beta,1)\},$$

$$Q'_{10} = \{(0,0;0),\,(-1,1),\,(\beta-1,0;1)\},$$

$$Q_{11} = \{(-1/\beta,-1;0),\,(1-1/\beta,0)\}, \qquad Q'_{11} = \{(0,0;1),\,(1,-1),\,(-1/\beta,-1;1)\},$$

$$Q_{1\bar{1}} = \{(-1,-1),\,(-1/\beta^3,-1;1)\}, \qquad Q'_{1\bar{1}} = \{(-1/\beta^3,-1;0)\},$$

$$Q_{1\bar{1}0} = \{(1-\beta,0;\bar{1}),\,(-1/\beta^2,-1;10)\}, \qquad Q'_{1\bar{1}0} = \{(-1/\beta^2,-1;0)\},$$

$$Q_{1\bar{1}01} = \{(-1/\beta,-1;1),\,(1-1/\beta,-2)\} = Q'_{1\bar{1}01},$$

$$Q_{1\bar{1}1} = \{(1/\beta^3,-1;\bar{1})\}, \qquad Q'_{1\bar{1}1} = \{(1-1/\beta^2,-2),(-1/\beta^2,-1;1)\},$$

$$Q_{1\bar{1}10} = \{(1/\beta^2,-1;\bar{1}0)\}, \qquad Q'_{1\bar{1}10} = \{(1/\beta^2,-1;1),\,(-1/\beta,-1;0)\}.$$

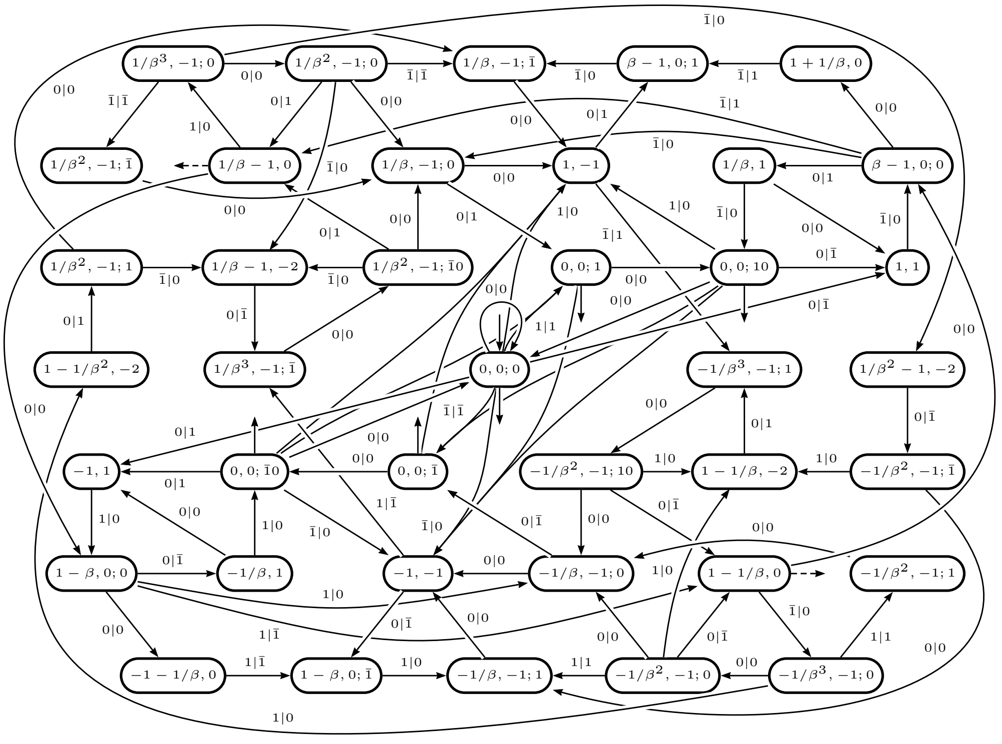

Figure 9. Normalizing transducer $\mathcal{N}_\beta$, $\beta^3 = \beta^2 + \beta + 1$.

Theorem 5.3. *If β is the Tribonacci number, then the set of β-expansions of minimal weight in $\{-1, 0, 1\}^*$ is recognized by the finite automaton $\mathcal{M}_\beta$ of Figure 7 where all states are terminal.*

5.2 Branching transformation

Contrary to the Golden Ratio case, we cannot obtain all β-expansions of minimal weight by the help of a piecewise linear branching transformation: If $z = \bullet 01(001)^n$, then we have no β-expansion of minimal weight of the form $z = \bullet 1x_2x_3\cdots$, whereas $z' = \bullet 0011$ has the expansion $\bullet 1\bar{1}$, and $z' < z$. On the other hand, $z = \bullet 1(100)^n 11$ has no β-expansion of minimal weight of the form $z = \bullet 1x_2x_3\cdots$ (since $1(100)^n 11$ is β-heavy but $(100)^n 11$ is not β-heavy), whereas $z' = \bullet 1101$ is a β-expansion of minimal weight, and $z' > z$. Hence the maximal interval for the digit 1 is $[\bullet(010)^\omega, \bullet 1(100)^\omega]$, with $\bullet(010)^\omega = \frac{\beta}{\beta^3-1} = \frac{1}{\beta+1}$ and $\bullet 1(100)^\omega = \frac{2\beta+1}{\beta(\beta+1)}$. The corresponding branching transformation and the possible expansions are given in Figure 10.

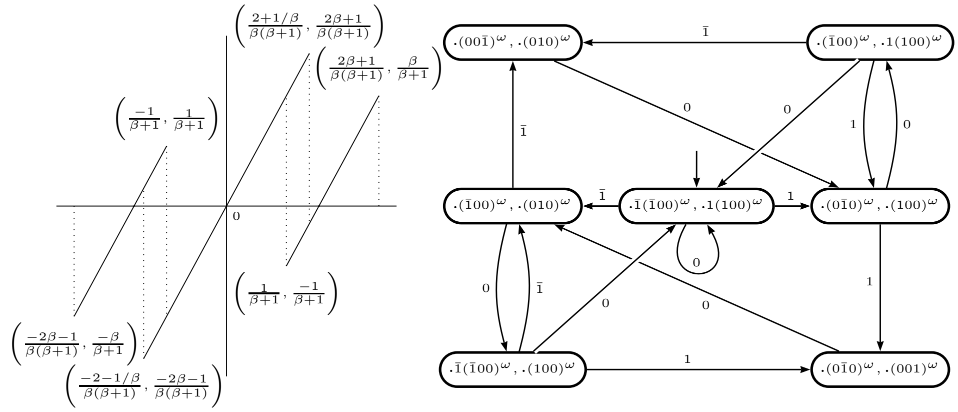

Figure 10. Branching transformation, corresponding automaton, $\beta^3 = \beta^2 + \beta + 1$.

5.3 Tribonacci numeration system

The linear numeration system canonically associated with the Tribonacci number is the Tribonacci numeration system defined by the sequence $T = (T_n)_{n \geq 0}$ with $T_0 = 1$, $T_1 = 2$, $T_2 = 4$, and $T_n = T_{n-1} + T_{n-2} + T_{n-3}$ for $n \geq 3$. Any non-negative integer $N < T_n$ has a representation $N = \sum_{j=1}^{n} x_j T_{n-j}$ with the property that $x_1 \cdots x_n \in \{0,1\}^*$ does not contain the factor 111. The relation $\sim_T$ and the properties T*-heavy*, T*-expansion of minimal weight* and *strongly* T*-heavy* are defined analogously to the Fibonacci numeration system. We have $20^n \sim_T 100010^{n-3}$ for $n \geq 3$, $200 \sim_T 1001$, $20 \sim_T 100$ and $2 \sim_T 10$, therefore for every $x \in \mathbb{Z}^*$ there exists some $y \in \{-1,0,1\}^*$ with $x \sim_T y$ and $\|y\| \leq \|x\|$. Since the difference of $1(0\bar{1}0)^{n/3}$ and $(100)^{n/3}$ is $1(\bar{1}\bar{1}0)^{n/3} \sim_T 1$, we obtain the following proposition.

Proposition 5.4. *Every* $N \in \mathbb{Z}$ *has a unique representation* $N = \sum_{j=1}^{n} y_j T_{n-j}$ *with* $y_1 \neq 0$ *and* $y_1 \cdots y_n \in \{-1,0,1\}^*$ *avoiding* $X = \{11, 101, 1\bar{1},$ *and their opposites*$\}$.

If $z = a_1 \cdots a_n{\bullet} = m_2 m_1 m_0{\bullet}$, then $N = \sum_{j=1}^{n} a_j T_{n-j} = 4m_2 + 2m_1 + m_0 = 0$ if and only if $m_0 = 2m_0'$ and $m_1 = -2m_2 - m_0'$, i.e., $z = -m_2/\beta^2 + m_0'/\beta^3$, hence all states $s = m/\beta^2 + m'/\beta^3$ with some $m, m' \in \mathbb{Z}$ are terminal states in the redundancy transducer $\mathcal{R}_T(1)$. The transducer $\mathcal{S}_T$, which is given by Figure 8 including the dashed arrows except that the states $(\pm 1/\beta, -3)$ are not terminal, shows that all strictly β-heavy words in $\{-1,0,1\}^*$ are strongly T-heavy, but that some other $x \in \{-1,0,1\}^*$ are T-heavy as well. Thus the T-expansions of minimal weight are a subset of the set recognized by the automaton $\mathcal{M}_\beta$ in Figure 7. Every set Q_u and Q_u', $u \in \{0, 1, 10, 11\}$, contains a terminal state $(0, 0; w)$ or $(1 - 1/\beta, 0)$, hence the words labelling paths ending in these states are T-expansions of minimal weight. The sets Q_u and Q_u', $u \in \{1\bar{1}, 1\bar{1}0, 1\bar{1}1, 1\bar{1}0, 1\bar{1}01\}$, contain states $(\pm 1/\beta^3, -1; w)$, $(\pm 1/\beta^2, -1; w)$, $(\pm(1 - 1/\beta), -2)$, hence the words labelling paths ending in these states are T-heavy, and we obtain the following theorem.

Theorem 5.5. *The* T*-expansions of minimal weight in* $\{-1,0,1\}^*$ *are exactly the* *words which are accepted by $\mathcal{M}_T$, which is the automaton in Figure 7 where only the states with a dashed outgoing arrow are terminal. The words given by Proposition 5.4 are T-expansions of minimal weight.*

5.4 Weight of the expansions

Let W_n be the set of words $x = x_1 \cdots x_n \in \{-1, 0, 1\}^n$ avoiding the factors 11, 101, $1\bar{1}$, and their opposites. Then the sequence of random variables $(Y_j)_{1 \le j \le n}$ defined by

$$\Pr[Y_1 = y_1 y_2, \ldots, Y_j = y_j y_{j+1}] = \frac{\#\{x_1 \cdots x_{n+1} \in W_n 0 : \, x_1 \cdots x_{j+1} = y_1 \cdots y_{j+1}\}}{\# W_n}$$

is Markov with transition probabilities $\Pr[Y_{j+1} = v \mid Y_j = u] = p_{u,v} + \mathcal{O}(\beta^{-n+j})$,

$$(p_{u,v})_{u,v \in \{10,01,00,0\bar{1},\bar{1}0\}} = \begin{pmatrix} 0 & 0 & \frac{\beta^2-1}{\beta^2} & \frac{1}{\beta^2} & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & \frac{\beta-1}{2\beta} & \frac{1}{\beta} & \frac{\beta-1}{2\beta} & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & \frac{1}{\beta^2} & \frac{\beta^2-1}{\beta^2} & 0 & 0 \end{pmatrix}.$$

The eigenvalues of this matrix are $1, \pm\frac{1}{\beta}, \frac{-\beta-1 \pm i\sqrt{3\beta^3-\beta}}{2\beta^3}$, and the stationary distribution vector of the Markov chain is $\left(\frac{\beta^3/2}{\beta^5+1}, \frac{\beta^3/2}{\beta^5+1}, \frac{\beta^3+\beta^2}{\beta^5+1}, \frac{\beta^3/2}{\beta^5+1}, \frac{\beta^3/2}{\beta^5+1}\right)$. We obtain the following theorem (with $\frac{\beta^3}{\beta^5+1} = \bullet(0011010100)^\omega \approx 0.28219$).

Theorem 5.6. *For positive integers M, we have, as $M \to \infty$,*

$$\frac{1}{2M+1} \sum_{N=-M}^{M} \|N\|_T = \frac{\beta^3}{\beta^5+1} \frac{\log M}{\log \beta} + \mathcal{O}(1).$$

6 Smallest Pisot number case

The smallest Pisot number $\beta \approx 1.325$ satisfies $\beta^3 = \beta + 1$. Since $1 = \bullet 011 = \bullet 10001$ implies $2 = 100\bullet 00001$ as well as $2 = 1000\bullet 000\bar{1}$, (D$'$) is satisfied with $B = 2$.

6.1 β-expansions of minimal weight

Let $\mathcal{M}_\beta$ be the automaton in Figure 11 without the dashed arrows where all states are terminal and $\mathcal{S}_\beta$ be the automon in Figure 13. To see that all words which are not accepted by $\mathcal{M}_\beta$ are β-heavy, we put labels on its states which stand for sets of states in $\mathcal{S}_\beta$: A, B, C, D, E, F, G stand for $(1/\beta^5, -1), (1/\beta^4, -1), \ldots, (\beta, -1)$, H, I, J, K stand for $(1/\beta, 0), \ldots, (\beta^2, 0)$, L, M, N, O stand for $(1/\beta^5, 0), \ldots, (1/\beta^2, 0)$, and the lowercase letters stand for the corresponding states (s, δ) with $s < 0$. If the label of a state u contains z, then all paths leading to u in $\mathcal{M}_\beta$ have a suffix which is the input

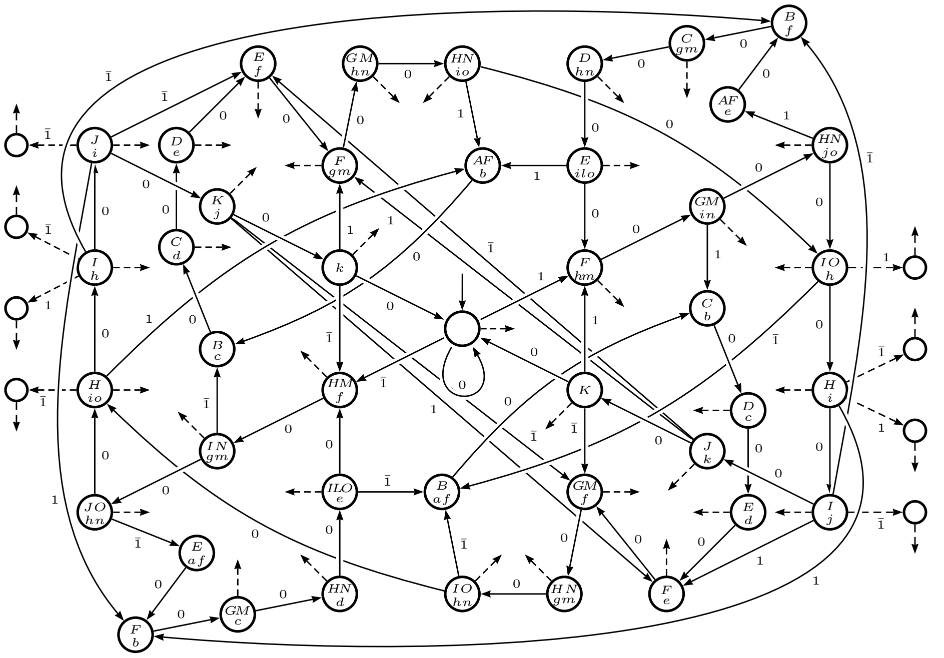

Figure 11. Automata $\mathcal{M}_\beta$, $\beta^3 = \beta + 1$, and $\mathcal{M}_S$.

of a path in $\mathcal{S}_\beta$ leading to z. This implies that the following lettter cannot be $\bar{1}$ if the label of u contains one of the states $B, C, \dots, H$. If it contains $b, c, \dots, h$, then 1 is forbidden.

Proposition 6.1. *If β is the smallest Pisot number, then every $z \in \mathbb{R}$ has a β-expansion of the form $z = y_1 \cdots y_k {\bf .} y_{k+1} y_{k+2} \cdots$ with $y_j \in \{-1, 0, 1\}$ such that $y_1 y_2 \cdots$ avoids the set $X = \{10^6 1, 10^k 1, 10^k \bar{1}, 0 \le k \le 5,$ and their opposites$\}$. If $z \in \mathbb{Z}[\beta] = \mathbb{Z}[\beta^{-1}]$, then this expansion is unique up to leading zeros.*

The expansion is provided by the transformation

$$\tau : \Big[\frac{-\beta^3}{\beta^2+1}, \frac{\beta^3}{\beta^2+1}\Big) \to \Big[\frac{-\beta^3}{\beta^2+1}, \frac{\beta^3}{\beta^2+1}\Big), \quad \tau(x) = \beta x - \Big\lfloor \frac{\beta^2+1}{2\beta^2} x + \frac{1}{2} \Big\rfloor$$

since $\tau\big[\frac{\beta^2}{\beta^2+1}, \frac{\beta^3}{\beta^2+1}\big) = \big[\frac{\beta^3}{\beta^2+1} - 1, \frac{\beta^4}{\beta^2+1} - 1\big) = \big[-\frac{1/\beta^3}{\beta^2+1}, \frac{1/\beta^4}{\beta^2+1}\big)$. The word avoiding X with maximal value is $(10^7)^\omega$, ${\bf .}(10^7)^\omega = \beta^7/(\beta^8 - 1) = \beta^3/(\beta^2 + 1)$.

Remark 6.2. The transformation $\tau(z) = \beta z - \big\lfloor \frac{1}{\beta} z + \frac{1}{2} \big\rfloor$ on $\big[-\frac{\beta^2}{2}, \frac{\beta^2}{2}\big)$ provides a unique expansion avoiding $10^6\bar{1}$ instead of $10^6 1$.

If x is a word accepted by $\mathcal{M}_\beta$, then there exists a path in the transducer $\mathcal{N}_\beta$ in Figure 14 going from $(0,0;0)$ to a state $(0,0;w)$ with input $00x0^5$ and output of the same weight. Since an automaton where all outputs avoiding the factors given by

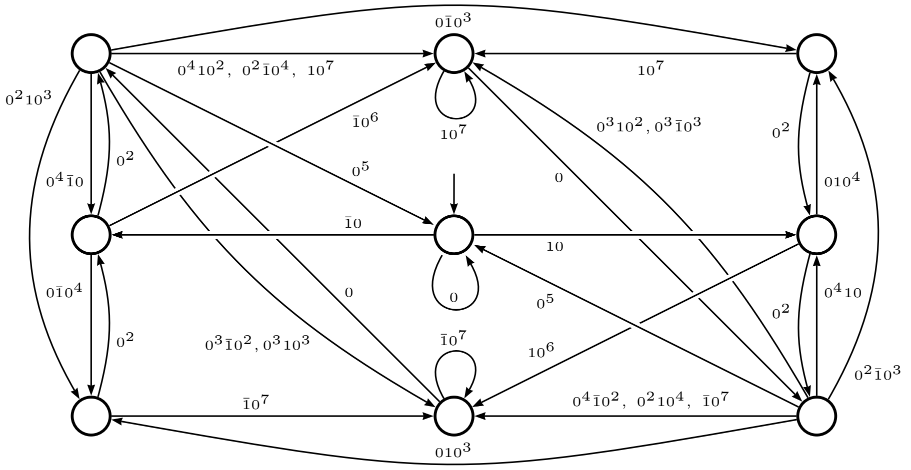

Figure 12. Compact representation of $\mathcal{M}_\beta$.

Proposition 6.1 would be very large, we decided to draw a smaller automaton and to split up the states (s, δ) into states $(s, \delta; w)$ only in the sets Q_u and Q'_u.

$$\begin{aligned}
Q_0 = Q'_0 &= \{(0,0;0),\ (1,1;\bar{1}),\ (-1,1;1),\ (\beta,1;\bar{1}0),\ (-\beta,1;10)\}\\
Q_1 &= \{(0,0;1),\ (1,-1;0),\ (-1/\beta^4,0;10),\ (-1/\beta,0;10^2)\}\\
Q'_1 &= \{(0,0;1),\ (1,-1;0),\ (-1/\beta^4,0;\bar{1}0^2), (-1/\beta,0;\bar{1}0)\}\\
Q_{10} &= \{(0,0;10),\ (1/\beta^4,0;1),\ (\beta,-1;0),\ (-1/\beta^3,0;10^2),\ (-1,0;10^3)\}\\
Q'_{10} &= \{(0,0;10),\ (1/\beta^4,0;1),\ (\beta,-1;0),\ (-1/\beta^3,0;\bar{1}0^3),\ (-1,0;\bar{1}0^2)\}\\
Q_{100} &= \{(0,0;10^2),\ (1/\beta^3,0;10),\ (1/\beta,0;1),\ (-1/\beta^2,0;10^3),\ (-\beta,0;10^4)\}\\
Q'_{100} &= \{(0,0;10^2),\ (1/\beta^3,0;10),\ (1/\beta,0;1),\ (-1/\beta^2,0;\bar{1}0^4),\ (-\beta,0;\bar{1}0^3)\}\\
Q_{10^3} = Q'_{10^3} &= \{(0,0;10^3),\ (1/\beta^2,0;10^2),\ (1,0;10),\ (-1/\beta,0;10^4)\}\\
Q_{10^4} = Q'_{10^4} &= \{(0,0;10^4),\ (1/\beta,0;10^3),\ (-1,0;10^5)\}\\
Q_{10^5} = Q'_{10^5} &= \{(0,0;10^5),\ (1,0;10^4),\ (-\beta,0;10^6)\}\\
Q_{10^6} = Q'_{10^6} &= \{(0,0;10^6),\ (\beta,0;10^5),\ (-\beta^2,0;0),\ (-1/\beta,1;\bar{1})\}\\
Q_{10^7} = Q'_{10^7} &= \{(0,0;0),\ (1,1;\bar{1}),\ (\beta^2,0;10^6),\ (-\beta,1;\bar{1}),\ (-1,1;\bar{1}0)\}\\
Q_{101} &= \{(1/\beta^3,-1;10^3),\ (-1/\beta^4,-1;10^4)\},\ Q'_{101} = \{(1/\beta^3,-1;\bar{1}0^4),\ (-1/\beta^4,-1;\bar{1}0^3)\}\\
Q_{1010} &= \{(1/\beta^2,-1;10^4),\ (-1/\beta^3,-1;10^5)\},\ Q'_{1010} = \{(1/\beta^2,-1;\bar{1}0^5), (-1/\beta^3,-1;\bar{1}0^4)\}\\
Q_{10100} &= \{(1/\beta,-1;10^5),\ (-1/\beta^2,-1;10^6)\},\ Q'_{10100} = \{(1/\beta,-1;\bar{1}0^6),\ (-1/\beta^2,-1;\bar{1}0^5)\}
\end{aligned}$$

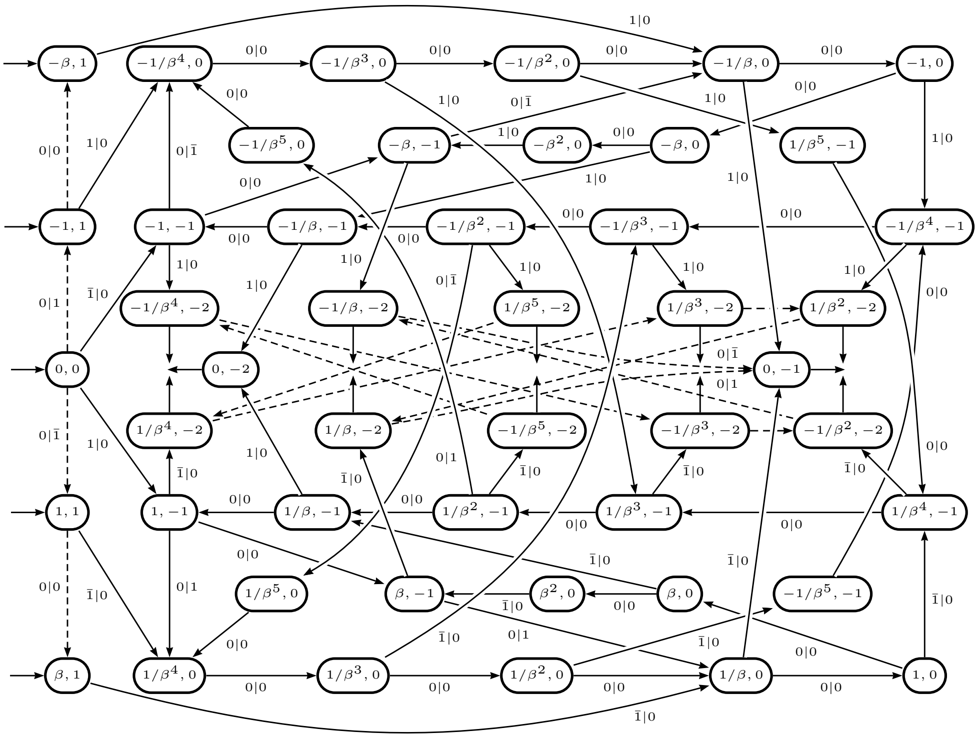

Figure 13. The relevant part of $\mathcal{S}_\beta(1)$, $\beta^3 = \beta + 1$.

$$
\begin{aligned}
Q_{1010^3} &= \{(1,-1;10^6),\ (-1/\beta,-1;0),\ (1/\beta^5,0;\bar{1})\}\\
Q'_{1010^3} &= \{(1,-1;0),\ (-1/\beta,-1;\bar{1}0^6),(0,0;1)\}\\
Q_{1010^4} &= \{(\beta,-1;0),\ (-1,-1;0),\ (0,0;\bar{1}),\ (1/\beta^4,0;\bar{1}0)\}\\
Q'_{1010^4} &= \{(\beta,-1;0),\ (-1,-1;0),\ (0,0;10),\ (1/\beta^4,0;1)\}\\
Q_{1010^5} &= \{(1/\beta,0;1),\ (-\beta,-1;0),\ (-1/\beta^4,0;\bar{1}),\ (0,0;\bar{1}0),\ (1/\beta^3,0;\bar{1}0^2)\}\\
Q'_{1010^5} &= \{(1/\beta,0;1),\ (-\beta,-1;0),\ (-1/\beta^4,0;\bar{1}),\ (0,0;10^2),\ (1/\beta^3,0;10)\}\\
Q_{1010^6} &= \{(1,0;10),\ (-1/\beta,0;\bar{1}),\ (-1/\beta^3,0;\bar{1}0),\ (0,0;\bar{1}0^2),\ (1/\beta^2,0;\bar{1}0^3)\}\\
Q'_{1010^6} &= \{(1,0;10),\ (-1/\beta,0;\bar{1}),\ (-1/\beta^3,0;\bar{1}0),\ (0,0;10^3),\ (1/\beta^2,0;10^2)\}
\end{aligned}
$$

$$Q_{1001} = \{(1/\beta^5,-1;10^4),\ (-1/\beta,-1;10^5)\},\ Q'_{1001} = \{(1/\beta^5,-1;\bar{1}0^5),\ (-1/\beta,-1;\bar{1}0^4)\}$$

$$Q_{10010} = \{(1/\beta^4,-1;10^5),\ (-1,-1;10^6)\},\ Q'_{10010} = \{(1/\beta^4,-1;\bar{1}0^6),\ (-1,-1;\bar{1}0^5)\}$$

$$
\begin{aligned}
Q_{100100} &= \{(1/\beta^3,-1;10^6),\ (-\beta,-1;0),\ (-1/\beta^4,0;\bar{1})\}\\
Q'_{100100} &= \{(1/\beta^3,-1;0),\ (-\beta,-1;\bar{1}0^6),\ (-1/\beta^2,0;1)\}
\end{aligned}
$$

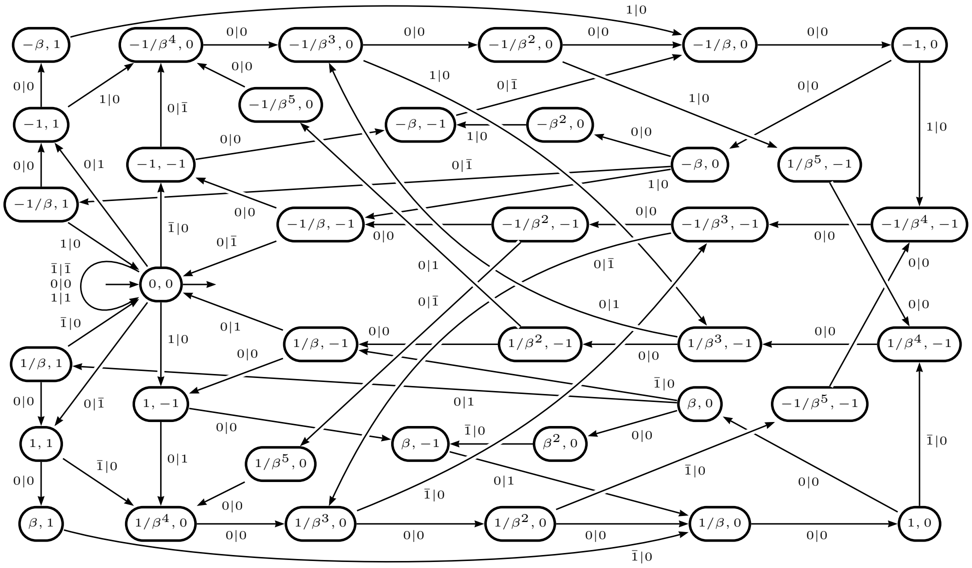

Figure 14. Transducer $\mathcal{N}_\beta$ normalizing β-expansions of minimal weight, $\beta^3 = \beta + 1$.

$$Q_{10010^3} = \{(1/\beta^2, -1; 0),\ (-1/\beta, 0; \bar{1}),\ (-1/\beta^3, 0; \bar{1}0)\}$$

$$Q'_{10010^3} = \{(1/\beta^2, -1; 0),\ (-1/\beta, 0; 10),\ (-1/\beta^3, 0; 1)\}$$

$$Q_{10010^4} = \{(1/\beta, -1; 0),\ (-1/\beta^5, 0; 1),\ (-1, 0; \bar{1}0),\ (-1/\beta^2, 0; \bar{1}0^2)\}$$

$$Q'_{10010^4} = \{(1/\beta, -1; 0),\ (-1/\beta^5, 0; 1),\ (-1, 0; 10^2),\ (-1/\beta^2, 0; 10)\}$$

$$Q_{1000\bar{1}} = \{(1/\beta^4, -1; 10^2),\ (-1/\beta^5, -1; 10^3)\},\ Q'_{1000\bar{1}} = \{(1/\beta^4, -1; \bar{1}0^3),\ (-1/\beta^5, -1; \bar{1}0^2)\}$$

If $u \xrightarrow{a} v$ is a transition in $\mathcal{M}_\beta$, then we have $Q_u \xrightarrow{a} Q_v$ or $Q_u \xrightarrow{a} Q'_v$, and $Q'_u \xrightarrow{a} Q_v$ or $Q'_u \xrightarrow{a} Q'_v$, where $Q \xrightarrow{a} R$ now means that for every $(s', \delta'; w') \in R$ there exists $(s, \delta; w) \in Q$ such that $(s, \delta) \xrightarrow{a|b} (s', \delta')$ is a transition in $\mathcal{N}_\beta$ and $w \xrightarrow{b} w'$ is allowed. The allowed transitions $w \xrightarrow{b} w'$ are $0 \xrightarrow{1} 1$, $\bar{1}0^6 \xrightarrow{1} 1$, $10^k \xrightarrow{0} 10^{k'}$ with $k' \le k + 1$, $10^k \xrightarrow{0} \bar{1}0^{k'}$ with $k' \le k$, $10^6 \xrightarrow{0} 0$, $0 \xrightarrow{0} w'$ for all w' and the opposites. This implies that if x labels a path leading to u in $\mathcal{M}_\beta$, then there exists paths with input $00x$ and output avoiding the set X given by Proposition 6.1 leading to all states in Q_u or to all states in Q'_u, and we obtain the following theorem.

Theorem 6.3. *If β is the smallest Pisot number, then the set of β-expansions of minimal weight in $\{-1, 0, 1\}^*$ is recognized by the finite automaton $\mathcal{M}_\beta$ of Figure 11 (without the dashed arrows) where all states are terminal.*

6.2 Branching transformation

In the case of the smallest Pisot number β, it is easy to see that the maximal interval for the digit 1 is $[.(010^6)^\omega, .1(0^510^2)^\omega]$, with $.(010^6)^\omega = \frac{\beta^2}{\beta^2+1}$ and $.1(0^510^2)^\omega = \frac{\beta^2+1/\beta}{\beta^2+1}$. The corresponding branching transformation and expansions are given in Figure 15.

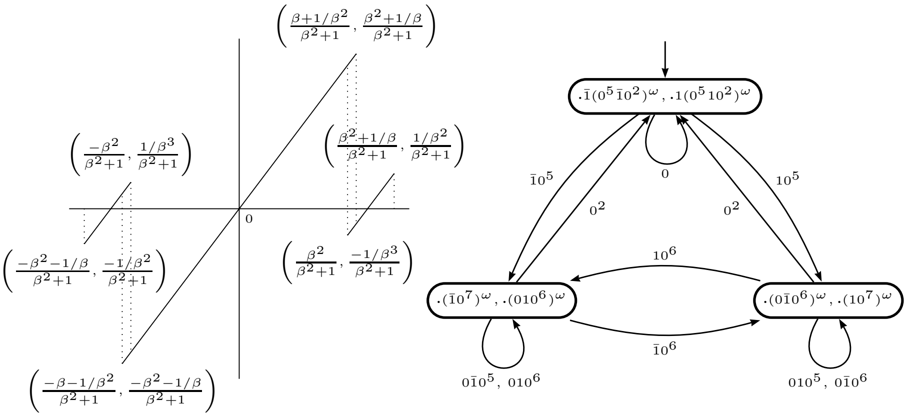

Figure 15. Branching transformation and corresponding automaton, $\beta^3 = \beta + 1$.

6.3 Integer expansions

Let $(S_n)_{n\ge 0}$ be a linear numeration system associated with the smallest Pisot number β which is defined as follows:

$$S_0 = 1,\ S_1 = 2,\ S_2 = 3,\ S_3 = 4, \quad S_n = S_{n-2} + S_{n-3} \ \text{for } n \ge 4.$$

Note that we do not choose the canonical numeration system associated with the smallest Pisot number, which is defined by $U_0 = 1, U_1 = 2, U_2 = 3, U_3 = 4, U_4 = 5, U_n = U_{n-1} + U_{n-5}$ for $n \ge 5$, since $U_n = U_{n-2} + U_{n-3}$ holds only for $n \equiv 1 \bmod 3$, $n \ge 4$.

For every $x \in \mathbb{Z}^*$, there exists $y \in \{-1,0,1\}^*$ with $x \sim_S y$, $\|y\| \le \|x\|$ since $2 \sim_S 10$, $20 \sim_S 1000$, $200 \sim_S 1010$, $20^3 \sim_S 10100$, $20^4 \sim_S 100100$, $20^5 \sim_S 1010^4$, $20^n \sim_S 10^610^{n-5}$ for $n \ge 6$.

Proposition 6.4. *Every $N \in \mathbb{Z}$ has a unique representation $N = \sum_{j=1}^n y_j S_{n-j}$ with $y_1 \ne 0$ and $y_1 \cdots y_n \in \{-1,0,1\}^*$ avoiding the set $X = \{10^61, 10^k1, 10^k\bar{1}, 0 \le k \le 5$, and their opposites$\}$, with the exception that $10^61, 10^51, 10^5\bar{1}, 10^4\bar{1}$ and their opposites are possible suffixes of $y_1 \cdots y_n$.*

As for the Fibonacci numeration system, this proposition is proved by considering g_n, the smallest positive integer with an expansion of length n starting with 1 avoiding these factors, and G_n, the largest integer of this kind. The representations of g_{n+1} and G_n, $n \ge 1$, depending on the congruence class of n modulo 8 are given by the following table.

$n \equiv j \bmod 8$	g_{n+1}	G_n	$g_{n+1} - G_n$
$1, 2, 3, 4$	$1(0^6\bar{1}0)^{n/8}$	$(10^7)^{n/8}$	$1\bar{1}0^{j-1} \sim_S 1$
5	$1(0^6\bar{1}0)^{(n-5)/8}0^4\bar{1}$	$(10^7)^{(n-5)/8}10^4$	$1\bar{1}000\bar{1} \sim_S 1$
6	$1(0^6\bar{1}0)^{(n-6)/8}0^5\bar{1}$	$(10^7)^{(n-6)/8}10^5$	$1\bar{1}0000\bar{1} \sim_S 1\bar{1} \sim_S 1$
7	$1(0^6\bar{1}0)^{(n-7)/8}0^6\bar{1}$	$(10^7)^{(n-7)/8}10^51$	$1\bar{1}00000\bar{2} \sim_S 10\bar{2} \sim_S 1$
0	$1(0^6\bar{1}0)^{n/8}$	$(10^7)^{n/8-1}10^61$	$1\bar{1}00000\bar{1}\bar{1} \sim_S 10\bar{1}\bar{1} \sim_S 1$

For the calculation of $g_{n+1}-G_n$ we have used $S_n-S_{n-1}-S_{n-7} = S_{n-5}-S_{n-7} = S_{n-8}$ for $n \geq 9$. In the rest of the section, we prove the following theorem.

Theorem 6.5. *The set of S-expansions of minimal weight in $\{-1,0,1\}^*$ is recognized by $\mathcal{M}_S$, which is the automaton in Figure 11 including the dashed arrows. The words given by Proposition 6.4 are S-expansions of minimal weight.*

Since $S_n = S_{n-2} - S_{n-3}$ holds only for $n \geq 4$ and not for $n = 3$, determining when $x \sim_S y$ is more complicated than for $\sim_F$ and $\sim_T$. If $z = a_1 \cdots a_n \bullet = m_3m_2m_1a_n\bullet$, then we have $N = \sum_{j=1}^n a_jS_{n-j} = 4m_3 + 3m_2 + 2m_1 + a_n$. We have to distinguish between different values of a_n.

If $a_n = 0$, we obtain $N = 0$ if and only if $m_2 = 2m_2'$, $m_1 = -2m_3 - 3m_2'$, hence

$$z = m_3(\beta^3 - 2\beta) + m_2'(2\beta^2 - 3\beta) = -m_3/\beta^4 - m_2'(1/\beta^4 + 1/\beta^7).$$

In particular, $m_2' = 0, m_3 \in \{0, \pm 1\}$ implies $N = 0$ if $z \in \{0, \pm 1/\beta^4\}$.

If $a_n = 1$, we obtain $N = 0$ if and only if $m_2 = 2m_2' - 1, m_1 = -2m_3 - 3m_2' + 1$, hence

$$z = m_3(\beta^3-2\beta)+m_2'(2\beta^2-3\beta)-\beta^2+\beta+1 = -m_3/\beta^4-m_2'(1/\beta^4+1/\beta^7)+1/\beta^2.$$

In particular, $m_3m_2' \in \{00, \bar{1}1, 01\}$ provides $N = 0$ if $z \in \{1/\beta^2, 1/\beta^3, 1/\beta^5\}$.

If $a_n = 2$, then $m_3m_2m_1 \in \{00\bar{1}, \bar{1}01\}$ provides $N = 0$ if $z \in \{2 - \beta, 1\}$.

We have $x_1 \cdots x_n \sim_S y_1 \cdots y_n$ if the corresponding path in $\mathcal{R}_\beta(1)$ ends in a state z corresponding to $a_n = x_n - y_n$ (or in $-z$, $a_n = y_n - x_n$).

It is easy to see that 11, $10\bar{1}$ and their opposites are strongly S-heavy. Therefore $x1$ is strongly S-heavy if x is the input of a path in $\mathcal{S}_\beta$ leading to $(-1/\beta^4, -1)$. The same is true for the states $(-1/\beta^3, -1), \ldots, (-1, -1)$ because of the following transitions leading to terminal states in $\mathcal{S}_F$:

- $(-1/\beta^3, -1) \xrightarrow{1|0} (1/\beta^3, -2) \xrightarrow{0|1} (-1/\beta^3, -1)$;
  $(-1/\beta^3, -1) \xrightarrow{1|0} (1/\beta^3, -2) \xrightarrow{0|0} \xrightarrow{0|1} (-1/\beta^5, -1) \xrightarrow{0|0} (-1/\beta^4, -1)$;
  $(-1/\beta^3, -1) \xrightarrow{1|0} (1/\beta^3, -2) \xrightarrow{0|0} \xrightarrow{0|0} \xrightarrow{0|\bar{1}} \xrightarrow{0|0} (0, -1)$
- $(-1/\beta^2, -1) \xrightarrow{1|0} (1/\beta^5, -2) \xrightarrow{0|0} (1/\beta^4, -2) \xrightarrow{0|1} (-1/\beta^3, -1)$;
  $(-1/\beta^2, -1) \xrightarrow{1|0} \xrightarrow{0|0} \xrightarrow{0|0} (1/\beta^3, -2)$ can be continued as above
- $(-1/\beta, -1) \xrightarrow{1|\bar{1}} (1, -1)$; $(-1/\beta, -1) \xrightarrow{1|0} \xrightarrow{0|0} (0, -2)$

- $(-1,-1) \xrightarrow{1|\bar{1}} (2-\beta,-1)$; $(-1,-1) \xrightarrow{1|0} \xrightarrow{0|\bar{1}} (1/\beta^2,-1)$;
  $(-1,-1) \xrightarrow{1|0} \xrightarrow{0|0} (-1/\beta^3,-2)$ can be continued as above

For $(-\beta,-1)$, we can assume that the incoming transition is $(-1,-1) \xrightarrow{0|0} (-\beta,-1)$ since we already know that 11 is strongly S-heavy. With $(-1,-1) \xrightarrow{0|\bar{1}} \xrightarrow{1|0} (1/\beta^2,-1)$, $(-\beta,-1) \xrightarrow{1|\bar{1}} \xrightarrow{0|0} (1/\beta^4,-1)$, $(-\beta,-1) \xrightarrow{1|0} \xrightarrow{0|\bar{1}} \xrightarrow{0|0} (0,-1)$, we obtain that these $x1$ are strongly S-heavy as well. If x is the input of a path in $\mathcal{S}_\beta$ ending in $(-1/\beta,0)$, then $x10^j$ is S-heavy for $j \geq 1$, but not necessarily for $j=0$, e.g. 10001 is not S-heavy.

In other words, if the label of a state in Figure 11 contains a letter b,c,d,e,f,g, then the following letter cannot be 1. The same is true if it contains h, except if the following letter is the last letter of the word. For the last letter we have other restrictions: Because of $(-1/\beta^4,0) \xrightarrow{1|0} (1/\beta^2,-1)$, $(-1/\beta^3,0) \xrightarrow{1|0} (1/\beta^3,-1)$, $(-1/\beta^2,0) \xrightarrow{1|0} (1/\beta^5,-1)$, it cannot be 1 if the state contains m,n,o. By symmetry, the last letter cannot be -1 if the label contains a corresponding capital letter. With $(\pm 1/\beta^5,-1) \xrightarrow{0|0} (\pm 1/\beta^4,-1)$, the last letter cannot be 0 if the label contains a or A.

Therefore all words which are not accepted by $\mathcal{M}_S$, which is the automaton in Figure 11 including the dashed arrows, are S-heavy. It remains to show that for every terminal transition $u \xrightarrow{a} v$ in $\mathcal{M}_S$, there exists transitions $q \xrightarrow{a|b} r$, $q' \xrightarrow{a|b'} r'$ with $q \in Q_u$, $q' \in Q'_u$, leading to terminal states, with output satisfying the conditions of Proposition 6.4. We provide this transition in case that it is not of the form $(0,0;w) \xrightarrow{a|a} (0,0)$.

$$
\begin{aligned}
10^2 10^4 \xrightarrow{0} 1 &: (-1/\beta^5,0;1) \xrightarrow{0|0} (-1/\beta^4,0) \\
101 \xrightarrow{0} 1010 &: (-1/\beta^4,-1;10^4) \xrightarrow{0|\bar{1}} (1/\beta^2,0), (1/\beta^3,-1;\bar{1}0^4) \xrightarrow{0|1} (-1/\beta^3,0) \\
1010 \xrightarrow{0} 1010^2 &: (-1/\beta^3,-1;10^5) \xrightarrow{0|\bar{1}} (1/\beta^3,0), (1/\beta^2,-1;\bar{1}0^5) \xrightarrow{0|1} (-1/\beta^5,0) \\
1010^2 \xrightarrow{0} 1010^3 &: (-1/\beta^2,-1;10^6) \xrightarrow{0|\bar{1}} (1/\beta^5,0), (-1/\beta^2,-1;\bar{1}0^5) \xrightarrow{0|\bar{1}} (1/\beta^5,0) \\
1010^3 \xrightarrow{0} 1010^4 &: (1/\beta^5,0;\bar{1}) \xrightarrow{0|0} (1/\beta^4,0) \\
10^2 10 \xrightarrow{0} 10^2 10^2 &: (1/\beta^4,-1;10^5) \xrightarrow{0|1} (-1/\beta^2,0), (1/\beta^4,-1;\bar{1}0^6) \xrightarrow{0|1} (-1/\beta^2,0) \\
10^2 10^2 \xrightarrow{0} 10^2 10^3 &: (1/\beta^3,-1;10^6) \xrightarrow{0|1} (-1/\beta^3,0), (1/\beta^3,-1;0) \xrightarrow{0|1} (-1/\beta^3,0) \\
10^2 10^3 \xrightarrow{0} 10^2 10^4 &: (1/\beta^2,-1;0) \xrightarrow{0|1} (-1/\beta^5,0) \\
10^3 \xrightarrow{1} 10^3 1 &: (-1/\beta,0;10^4) \xrightarrow{1|\bar{1}} (1,0) \\
10^4 \xrightarrow{1} 10^4 1 &: (-1,0;10^5) \xrightarrow{1|\bar{1}} (2-\beta,0)
\end{aligned}
$$

6.4 Weight of the expansions

Let W_n be the set of words $x = x_1 \cdots x_n \in \{-1, 0, 1\}^n$ avoiding the factors given by Proposition 6.4. Then the sequence of random variables $(Y_j)_{1 \le j \le n}$ defined by

$$\begin{aligned}\Pr[Y_1 = y_1 \cdots y_7, \ldots, Y_j = y_j \cdots y_{j+6}]& \\ = \#\{x_1 \cdots x_{n+6} \in W_n 0^6 :\ & x_1 \cdots x_{j+6} = y_1 \cdots y_{j+6}\} / \# W_n\end{aligned}$$

is Markov with transition probabilities $\Pr[Y_{j+1} = v \mid Y_j = u] = p_{u,v} + \mathcal{O}(\beta^{-n+j})$,

$$(p_{u,v})_{u,v \in \{10^6, \ldots, 0^6 1, 0^7, 0^6 \bar{1}, \ldots, \bar{1} 0^6\}} = \begin{pmatrix} 0 & \cdots & \cdots & 0 & \frac{2}{\beta^3} & \frac{1}{\beta^7} & 0 & \cdots & 0 \\ 1 & \ddots & & \vdots & 0 & 0 & \vdots & & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ \vdots & \ddots & 1 & 0 & 0 & 0 & \vdots & & \vdots \\ \vdots & & 0 & \frac{1}{2\beta^5} & \frac{1}{\beta} & \frac{1}{2\beta^5} & 0 & & \vdots \\ \vdots & & \vdots & 0 & 0 & 0 & 1 & \ddots & \vdots \\ \vdots & & \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & 0 \\ \vdots & & \vdots & 0 & 0 & \vdots & & \ddots & 1 \\ 0 & \cdots & 0 & \frac{1}{\beta^7} & \frac{2}{\beta^3} & 0 & \cdots & \cdots & 0 \end{pmatrix}.$$

The left eigenvector to the eigenvalue 1 of this matrix is $\frac{1}{14+4\beta^2}(1, \ldots, 1, 4\beta^2, 1, \ldots, 1)$, and we obtain the following theorem (with $\frac{1}{7+2\beta^2} \approx 0.09515$).

Theorem 6.6. *For positive integers M, we have, as $M \to \infty$,*

$$\frac{1}{2M+1} \sum_{N=-M}^{M} \|N\|_S = \frac{1}{7+2\beta^2} \frac{\log M}{\log \beta} + \mathcal{O}(1).$$

7 Concluding remarks

Another example of a number $\beta < 2$ of small degree satisfying (D′), which is not studied in this article, is the Pisot number satisfying $\beta^3 = \beta^2 + 1$, with $2 = 100{\bullet}00000\bar{1}$.

A question which is not approached in this paper concerns β-expansions of minimal weight restricted to alphabets which do not contain $\{1 - B, \ldots, B - 1\}$, in particular if β does not satisfy (D′).

In view of applications to cryptography, we present a summary of the average minimal weight of representations of integers in linear numeration systems $(U_n)_{n \ge 0}$ associated with different β, with digits in $A = \{0, 1\}$ or in $A = \{-1, 0, 1\}$.

U_n	A	β	average $\|N\|_U$ for $N \in \{-M, \dots, M\}$
2^n	$\{0, 1\}$	2	$(\log_2 M)/2$
2^n	$\{-1, 0, 1\}$	2	$(\log_2 M)/3$
F_n	$\{0, 1\}$	$\frac{1+\sqrt{5}}{2}$	$(\log_\beta M)/(\beta^2 + 1) \approx 0.398 \log_2 M$
F_n	$\{-1, 0, 1\}$	$\frac{1+\sqrt{5}}{2}$	$(\log_\beta M)/5 \approx 0.288 \log_2 M$
T_n	$\{-1, 0, 1\}$	$\beta^3 = \beta^2 + \beta + 1$	$(\log_\beta M)\beta^3/(\beta^5 + 1) \approx 0.321 \log_2 M$
S_n	$\{-1, 0, 1\}$	$\beta^3 = \beta + 1$	$(\log_\beta M)/(7 + 2\beta^2) \approx 0.235 \log_2 M$

If we want to compute a scalar multiple of a group element, e.g. a point P on an elliptic curve, we can choose a representation $N = \sum_{j=0}^{n} x_j U_j$ of the scalar, compute $U_j P$, $0 \le j \le n$, by using the recurrence of U and finally $NP = \sum_{j=0}^{n} x_j (U_j P)$. In the cases which we have considered, this amounts to $n + \|N\|_U$ additions (or subtractions). Since $n \approx \log_\beta N$ is larger than $\|N\|_U$, the smallest number of additions is usually given by a 2-expansion of minimal weight. (We have $\log_{(1+\sqrt{5})/2} N \approx 1.44 \log_2 N$, $\log_\beta N \approx 1.137 \log_2 M$ for the Tribonacci number, $\log_\beta N \approx 2.465 \log_2 N$ for the smallest Pisot number.)

If however we have to compute several multiples NP with the same P and different $N \in \{-M, \dots, M\}$, then it suffices to compute $U_j P$ for $0 \le j \le n \approx \log_\beta M$ once, and do $\|N\|_U$ additions for each N. Starting from 10 multiples of the same P, the Fibonacci numeration system is preferable to base 2 since $(1 + 10/5) \log_{(1+\sqrt{5})/2} M \approx 4.321 \log_2 M < (1 + 10/3) \log_2 M$. Starting from 20 multiples of the same P, S-expansions of minimal weight are preferable to the Fibonacci numeration system since $(1{+}20/(7{+}2\beta^2)) \log_\beta M \approx 7.156 \log_2 M < 7.202 \log_2 M \approx (1{+}20/5) \log_{(1+\sqrt{5})/2} M$.

Appendix

Proposition A.1. *If β satisfies* (D), *$\beta > 1$, then β is a Pisot number.*

Proof. First note that every polynomial $P(X) = X^{d+1} - BX^d + b_1 X^{d-1} + \cdots + b_d \in \mathbb{Z}[X]$ with $B > \sum_{j=1}^{d} |b_j|$ has a root $\beta > 1$ except for the trivial cases $X - 1$ and $X^2 - 2X + 1$. It is easy to see (e.g. by multiplying both sides with $\beta - 1$) that

$$1 = \bullet(B-1)(B-b_1-1)\cdots(B-b_1-\cdots-b_{d-1}-1)(B-b_1-\cdots-b_d-1)^\omega$$

is an expansion of 1 in base β with non-negative digits. We have

$$X^{d+1} - BX^d + b_1 X^{d-1} + \cdots + b_d = (X - \beta)(X^d - r_1 X^{d-1} - \cdots - r_d)$$

with $r_j = \bullet b_j b_{j+1} \cdots b_d$, and

$$\begin{aligned}
\sum_{j=1}^{d} |r_j| &= \sum_{j=1}^{d} \left| \sum_{i=j}^{d} \frac{b_i}{\beta^{i-j+1}} \right| \\
&\le \sum_{j=1}^{d} \sum_{i=j}^{d} \frac{|b_i|}{\beta^{i-j+1}} = \bullet(|b_1| + \cdots + |b_d|)(|b_2| + \cdots + |b_d|) \cdots (|b_d|) \\
&\le \bullet(B-1)(B-|b_1|-1) \cdots (B-|b_1|-\cdots-|b_{d-1}|-1) \\
&\le \bullet(B-1)(B-b_1-1) \cdots (B-b_1-\cdots-b_{d-1}-1) \\
&\le 1
\end{aligned}$$

We have equality everywhere if and only if $B = \sum_{j=1}^{d} b_j + 1$. In this case,

$$1 = \bullet t_1 t_2 \cdots t_d = \bullet(B-1)(B-b_1-1) \cdots (B-b_1-\cdots-b_{d-1}-1)$$

with $t_1 \ge t_2 \ge \cdots \ge t_d$, and it is well known that β is a Pisot number. If $\sum_{j=1}^{d} |r_j| < 1$, then

$$|x^d| > \sum_{j=1}^{d} |r_j|\, |x|^d \ge \sum_{j=1}^{d} |r_j|\, |x|^{d-j} \ge |r_1 x^{d-1} + \cdots + r_{d-1} x + r_d|$$

for all x with $|x| \ge 1$, hence x cannot be a root of $P(X)$ and β is a Pisot number. □

References

[1] S. Akiyama, Cubic Pisot units with finite beta expansions, in *Algebraic Number Theory and Diophantine Analysis*, ed. F. Halter-Koch and R. F. Tichy, de Gruyter (2000) 11-26.

[2] S. Akiyama, H. Rao and W. Steiner, A certain finiteness property of Pisot number systems, *J. Number Theory* **107** (2004) 135–160.

[3] S. Arno and F. S. Wheeler, Signed digit representations of minimal Hamming weight, *IEEE Trans. Comput.* **42** (1993) 1007–1010.

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

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

[6] W. Bosma, Signed bits and fast exponentiation, *J. Théor. Nombres Bordx.* **13** (2007) 27–41.

[7] K. Dajani, C. Kraaikamp, and P. Liardet, Ergodic properties of signed binary expansions, *Discrete Contin. Dyn. Syst.* **15** (2006) 87–119.

[8] V. Dimitrov, T. Cooklev, and B. Donevsky, Number theoretic transforms over the Golden Section quadratic field, *IEEE Trans. Signal Proc.* **43** (1995) 190–1797.

[9] M. Drmota and W. Steiner, The Zeckendorf expansion of polynomial sequences, *J. Théor. Nombres Bordx.* **14** (2002) 439–475.

[10] N. Ebeid and M.A. Hasan, On τ-adic representations of integers, *Des. Codes Cryptography* **45** (2007) 271–296.

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

[12] Ch. Frougny, Representation of numbers and finite automata, *Math. Syst. Theory* **25** (1992) 37–60.

[13] Ch. Frougny and B. Solomyak, Finite beta-expansions, *Ergod. Theory Dyn. Syst.* **12** (1992) 713–723.

[14] P. Grabner and C. Heuberger, On the number of optimal base 2 representations of integers, *Des. Codes Cryptography* **40** (2006) 25–39.

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

[16] C. Heuberger and H. Prodinger, Analysis of alternative digit sets for nonadjacent representations, *Monatsh. Math.* **147** (2006) 219–248.

[17] M. Joye and C. Tymen, Compact encoding of non-adjacent forms with applications to elliptic curve cryptography, in *Public Key Cryptography*, L.N.C.S. **1992** (2001) 353–364.

[18] M. Lothaire, *Algebraic Combinatorics on Words*, Cambridge University Press, 2002.

[19] N. Meloni, New point addition formulae for EEC applications, in *Proceedings WAIFI 2007*, L.N.C.S. **4547** (2007) 189–201.

[20] F. Morain and J. Olivos, Speeding up the computations on an elliptic curve using addition-subtraction chains, *RAIRO, Inform. Théor. Appl.* **24** (1990) 531–543.

[21] J. A. Muir and D. R. Stinson, Minimality and other properties of the width-w nonadjacent form, *Math. Comput.* **75** (2005) 369–384.

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

[23] G. W. Reitwiesner, Binary arithmetic, *Advances in Computers*, vol. 1, Academic Press, New York, 1960, 231–308.

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

[25] J. Sakarovitch, *Eléments de théorie des automates*, Vuibert (2003). English translation: *Elements of Automata Theory*, Cambridge University Press, to appear.

[26] J. A. Solinas, Efficient arithmetic on Koblitz curves, *Des. Codes Cryptography* **19** (2000) 195–249.

Received

Author information

Christiane Frougny, LIAFA, CNRS UMR 7089, and Université Paris 8, France.
Email: christiane.frougny@liafa.jussieu.fr

Wolfgang Steiner, LIAFA, CNRS UMR 7089, Université Paris Diderot – Paris 7, Case 7014, 75205 Paris Cedex 13, France.
Email: steiner@liafa.jussieu.fr