J. Math. Crypt. **2** (2008), 365–392

DOI 10.1515 / JMC.2008.017

Minimal weight expansions in Pisot bases

Christiane Frougny and Wolfgang Steiner

Communicated by Tran van Trung

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 real bases β which are Pisot numbers and prove that the expansions with minimal absolute sum of digits are recognizable by finite automata. 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 explicitely the finite automata recognizing all these expansions. The average weight is lower than for the non-adjacent form.

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 [4] 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 [6].

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 [7] 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

This research was supported by the French Agence Nationale de la Recherche, grant ANR-JCJC06-134288 “DyCoNum”.

τ related to Koblitz curves, and has given a τ-NAF form, and the Hamming weight of these representations has been studied in [9].

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 $z = \bullet x_1 x_2 \cdots$. If there exists a n such that $x_j = 0$ for all $j > n$, the expansion is said to be *finite* and we write $z = \bullet x_1 x_2 \cdots x_n$. By shifting, any non-negative real number has a greedy β-expansion: If $z \in [0, \beta^k)$, $k \geq 0$, and $\beta^{-k} z = \bullet x_1 x_2 \cdots$, then $z = x_1 \cdots x_k \bullet x_{k+1} x_{k+2} \cdots$.

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 $z = \bullet x_1 x_2 \cdots x_n$ 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 [12, 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

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

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 $\bullet x_1 x_2 \cdots x_n$ 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 the condition

$$(\mathrm{D}_B): \text{ there exists a word } b \in \{1-B, \ldots, B-1\}^* \text{ such that } B \sim_\beta b \text{ and } \|b\| \leq B$$

for some positive integer B. Corollary 3.2 and Remark 3.4 show that every class of words (with respect to $\sim_\beta$) contains a β-expansion of minimal weight with digits in $\{1-B, \ldots, B-1\}$ if and only if β satisfies (D_B).

If β is a Pisot number, i.e., an algebraic integer greater than 1 such that all the other roots of its minimal polynomial are in modulus less than one, then it satisfies (D_B) for some $B > 0$ by Proposition 3.5. The contrary is not true: There exist algebraic integers $\beta > 1$ satsfying (D_B) which are not Pisot, e.g. the positive solution of $\beta^4 = 2\beta + 1$ is not a Pisot number but satisfies (D_2) since $2 = 1000\bullet(-1)$. The following example provides a large class of numbers β satisfying (D_B).

Example 1.1. If $1 = \bullet t_1 t_2 \cdots t_d (t_{d+1})^\omega$ with integers $t_1 \geq t_2 \geq \cdots \geq t_d > t_{d+1} \geq 0$, then β satisfies (D_B) with $B = t_1 + 1 = \lfloor \beta \rfloor + 1$, 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

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

Recall that the set of greedy β-expansions is recognizable by a finite automaton when β is a Pisot number [3]. In this work, we prove that the set of all β-expansions of minimal weight is recognized by a finite automaton when β is a Pisot number.

We then consider particular Pisot numbers satisfying (D_2) which have been extensively studied from various points of view. When β is the Golden Ratio, we construct a finite transducer which gives, for a strictly β-heavy word as input, a β-lighter word as output. Similarly to the Non-Adjacent Form in base 2, we define a particular unique expansion of minimal weight avoiding a certain given set of factors. We show that there is a finite transducer which converts all words of minimal weight into these expansions avoiding these 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 [2, 5], 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: $\frac{1}{7+2\beta^2}\log_\beta M \approx 0.095 \log_\beta M \approx 0.234 \log_2 M$.

Since the proof techniques for the Tribonacci number and the smallest Pisot number are quite similar to the Golden Ratio case (but more complicated), some parts of the proofs are not contained in the final version of this paper. The interested reader can find them in [13].

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 [10] 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, our aim is to prove that one can construct a finite automaton recognizing the set of β-expansions of minimal weight when β is a Pisot number.

We need first some combinatorial results for bases β satisfying (D_B). Note that β is not assumed to be a Pisot number here.

Proposition 3.1. *If β satisfies* (D_B) *with some integer $B \geq 2$, then for every word $x \in \mathbb{Z}^*$ there exists some $y \in \{1-B, \ldots, B-1\}^*$ with $x \sim_\beta y$ and $\|y\| \leq \|x\|$.*

Corollary 3.2. *If β satisfies* (D_B) *with some integer $B \geq 2$, then for every word $x \in \mathbb{Z}^*$ there exists a β-expansion of minimal weight $y \in \{1-B, \ldots, B-1\}^*$ with $x \sim_\beta y$.*

Remark 3.3. If β satisfies (D_B) for some positive integer B, then it is easy to see that β satisfies (D_C) for every integer $C > B$.

Remark 3.4. If β does not satisfy (D_B), then all words $x \in \{1-B, \ldots, B-1\}^*$ with $x \sim_\beta B$ are β-heavier than B. It follows that the set of β-expansions of minimal weight $x \sim_\beta B$ is $0^* B 0^*$.

Proof of Proposition 3.1. Let $A = \{1-B, \ldots, B-1\}$. If $x = x_1 x_2 \cdots x_n \in A^*$, then there is nothing to do. Otherwise, we use (D_B): there exists some word $b = b_{-k} \cdots b_d \in A^*$ such that $b_{-k} \cdots b_{-1}(b_0 - B) b_1 \cdots b_d \sim_\beta 0$ and $\|b\| \leq B$. We use this relation to decrease the absolute value of a digit $x_h \notin A$ without increasing the weight of x, and we show that we eventually obtain a word in A^* if we always choose the rightmost such digit. More precisely, 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 $\sum_{j\in\mathbb{Z}} |x_j^{(0)}| = \|x\|$, $\sum_{j\in\mathbb{Z}} x_j^{(i+1)} \beta^{-j} = \sum_{j\in\mathbb{Z}} x_j^{(i)} \beta^{-j}$ 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 is a word $y \in A^*$ 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 $i \geq 0$. In particular, the algorithm terminates after at most $\|x\| - B + 1$ steps if $\|b\| < B$.[1]

If $\|b\| = B$ and $\sum_{j\in\mathbb{Z}} |x_j^{(i+1)}| = \sum_{j\in\mathbb{Z}} |x_j^{(i)}|$, then we have

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

Assume that h_i exists for all $i \geq 0$. If $(h_i)_{i\geq 0}$ has a minimum, then there exists an increasing sequence of indices $(i_m)_{m\geq 0}$ such that $h_{i_m} \leq h_\ell$ for all $\ell > i_m$, $m \geq 0$, thus

$$\|x\| \geq \sum_{j=-\infty}^{h_{i_m}-1} |x_j^{(i_m+1)}| \geq \sum_{j=-\infty}^{h_{i_{m-1}}-1} |x_j^{(i_{m-1}+1)}| + \sum_{j=1}^{k} |b_{-j}| \geq \cdots \geq (m+1) \sum_{j=1}^{k} |b_{-j}|.$$

If $\sum_{j=1}^{k} |b_{-j}| > 0$, this is not possible since $\|x\|$ is finite. Similarly, $(h_i)_{i\geq 0}$ has no maximum if $\sum_{j=1}^{d} |b_j| > 0$. Since $x_j^{(i+1)}$ can differ from $x_j^{(i)}$ only for $h_i - k \leq j \leq h_i + d$, we have $h_{i+1} \leq h_i + d$ for all $i \geq 0$. If $h_i < h_{i'}$, $i < i'$, then there is therefore a sequence $(i_m)_{0\leq m\leq M}$, $i \leq i_0 < i_1 < \cdots < i_M = i'$, with $M \geq (h_{i'} - h_i)/d$ such that $h_{i_m} \leq h_\ell$ for all $\ell \in \{i_m, i_m + 1, \ldots, i'\}$, $m \in \{0, \ldots, M\}$. As above, we obtain $\|x\| \geq (M+1) \sum_{j=1}^{k} |b_{-j}|$, but M can be arbitrarily large if $(h_i)_{i\geq 0}$ has neither minimum nor maximum. Hence we have shown that h_i cannot exist for all $i \geq 0$ if $\sum_{j=1}^{k} |b_{-j}| > 0$ and $\sum_{j=1}^{d} |b_j| > 0$.

It remains to consider the case $\|b\| = B$ with $k = 0$ or $d = 0$. Assume, w.l.o.g., $d = 0$. Then we have $h_{i+1} \leq h_i$. If h_i exists for all $i \geq 0$, then both $\sum_{j=0}^{k} |x_{h_i-j}^{(i)}|$ and $\sum_{j=1}^{\infty} |x_{h_i+j}^{(i)}|$ are eventually constant. Therefore we must have some i, i' with $h_{i'} < h_i$ such that $x_{h_{i'}-k}^{(i')} \cdots x_{h_{i'}}^{(i')} = x_{h_i-k}^{(i)} \cdots x_{h_i}^{(i)}$, $x_{h_{i'}+1}^{(i')} x_{h_{i'}+2}^{(i')} \cdots = 0^{h_i - h_{i'}} x_{h_i+1}^{(i)} x_{h_i+2}^{(i)} \cdots$, and $x_{h_i-j}^{(i)} = x_{h_{i'}-j}^{(i')} = 0$ for all $j > k$. This implies $x_{h_i-k}^{(i)} \cdots x_{h_i}^{(i)} \sim_\beta 0$ or $\beta^{h_i - h_{i'}} = 1$. In the first case, $x_{h_i+1}^{(i)} x_{h_i+2}^{(i)} \cdots$ without the trailing zeros is a word $y \in A^*$ with the desired properties. In the latter case, each $x \in \mathbb{Z}^*$ can be easily transformed into some $y \in \{-1, 0, 1\}^*$ with $y \sim_\beta x$ and $\|y\| = \|x\|$, and the proposition is proved. □

The following proposition shows slightly more than the existence of a positive integer B such that β satisfies (D_B) when β is a Pisot number.

Proposition 3.5. *For every Pisot number β, there exists some positive integer B and some word $b \in \mathbb{Z}^*$ such that $B \sim_\beta b$ and $\|b\| < B$.*

Proof. If β is an integer, then we can choose $B = \beta$ and $b = 1$. So let β be a Pisot number of degree $d \geq 2$, i.e., β has $d - 1$ Galois conjugates $\beta^{(j)}$, $2 \leq j \leq d$, with $|\beta^{(j)}| < 1$. For every $z \in \mathbb{Q}(\beta)$ set $z^{(j)} = P(\beta^{(j)})$ if $z = P(\beta)$, $P \in \mathbb{Q}[X]$.

[1] For the proof of Theorem 3.11, it is sufficient to consider the case $\|b\| < B$. However, Corollary 3.2 is particularly interesting in the case $\|b\| = B$, and we use it in the following sections for $B = 2$.

Let B be a positive integer, $L = \lceil \log B / \log \beta \rceil$, and $x_1 x_2 \cdots$ the greedy β-expansion of $z = \beta^{-L} B \in [0,1)$. Since

$$\tau_\beta^k(z) = \beta \tau^{k-1}(z) - x_k = \cdots = \beta^k z - \sum_{\ell=1}^{k} x_\ell \beta^{k-\ell},$$

we have

$$\left|(\tau_\beta^k(z))^{(j)}\right| = \left|(\beta^{(j)})^k z^{(j)} - \sum_{\ell=1}^{k} x_\ell (\beta^{(j)})^{k-\ell}\right| < \left|\beta^{(j)}\right|^k \left|z^{(j)}\right| + \frac{\lfloor \beta \rfloor}{1 - |\beta^{(j)}|}$$

for all $k \geq 0$ and $2 \leq j \leq d$. Set $k = \max_{2 \leq j \leq d} \lceil -\log |z^{(j)}| / \log |\beta^{(j)}| \rceil$. Then $\tau_\beta^k(z)$ is an element of the finite set

$$Y = \left\{ y \in \mathbb{Z}[\beta^{-1}] \cap [0,1) : \ |y^{(j)}| < 1 + \frac{\lfloor \beta \rfloor}{1 - |\beta^{(j)}|} \ \text{ for } \ 2 \leq j \leq d \right\}.$$

For every $y \in Y$, we can choose a β-expansion $y = \bullet a_1 \cdots a_m$. Let W be the maximal weight of all these expansions and $\tau_\beta^k(z) = \bullet a_1' \cdots a_m'$. Since $z = \bullet x_1 \ldots x_k + \tau_\beta^k(z)$, the digitwise addition of $x_1 \cdots x_k$ and $a_1' \cdots a_m'$ provides a word b with $b \sim_\beta B$ and

$$\|b\| \leq k \lfloor \beta \rfloor + W = \max_{2 \leq j \leq d} \left\lceil \left\lceil \frac{\log B}{\log \beta} \right\rceil - \frac{\log B}{\log |\beta^{(j)}|} \right\rceil \lfloor \beta \rfloor + W = \mathcal{O}(\log B).$$

If B is sufficiently large, we have therefore $\|b\| < B$. □

In order to understand the relation $\sim_\beta$ on A^*, $A = \{1-B, \ldots, B-1\}$, we have to consider the words $z \in (A-A)^*$ with $z \sim_\beta 0$. Therefore we set

$$Z_\beta = \left\{ z_1 \cdots z_n \in \{2(1-B), \ldots, 2(B-1)\}^* \;\middle|\; n \geq 0, \ \sum_{j=1}^{n} z_j \beta^{-j} = 0 \right\}$$

and recall a result from [11]. All the automata considered in this paper process words from left to right, that is to say, most significant digit first.

Lemma 3.6 ([11]). *If β is a Pisot number, then Z_β is recognized by a finite automaton.*

For convenience, we quickly explain the construction of the automaton $\mathcal{A}_\beta$ recognizing Z_β. The states of $\mathcal{A}_\beta$ are 0 and all $s \in \mathbb{Z}[\beta] \cap (\frac{2(1-B)}{\beta-1}, \frac{2(B-1)}{\beta-1})$ which are accessible from 0 by paths consisting of transitions $s \xrightarrow{e} s'$ with $e \in A - A$ 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 $\mathcal{A}_\beta$ is symmetric, meaning that if $s \xrightarrow{e} s'$ is a transition, then $-s \xrightarrow{-e} -s'$ is also a transition. The automaton $\mathcal{A}_\beta$ is accessible and co-accessible.

The *redundancy automaton* (or transducer) $\mathcal{R}_\beta$ is similar to $\mathcal{A}_\beta$. Each transition $s \xrightarrow{e} s'$ of $\mathcal{A}_\beta$ is replaced in $\mathcal{R}_\beta$ by a set of transitions $s \xrightarrow{a|b} s'$, with $a, b \in A$ and $a - b = e$. From Lemma 3.6, one obtains the following lemma.

Lemma 3.7. *The redundancy transducer $\mathcal{R}_\beta$ recognizes the set*

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

If β is a Pisot number, then $\mathcal{R}_\beta$ is finite.

From the redundancy transducer $\mathcal{R}_\beta$, one constructs another transducer $\mathcal{T}_\beta$ with states of the form (s,δ), where s is a state of $\mathcal{R}_\beta$ 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 $\mathcal{R}_\beta$ and $\delta'=\delta+|b|-|a|$. The initial state is $(0,0)$, and terminal states are of the form $(0,\delta)$ with $\delta<0$.

Lemma 3.8. *The transducer $\mathcal{T}_\beta$ recognizes the set*

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

Of course, the transducer $\mathcal{T}_\beta$ is not finite, and the core of the proof of the main result consists in showing that we need only a finite part of $\mathcal{T}_\beta$.

We also need the following well-known lemma, and give a proof for it because the construction in the proof will be used in the following sections.

Lemma 3.9. *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 the paths labelled by p end in the same set of states in $\mathcal{H}$ as the paths labelled by q. Since $\mathcal{H}$ is finite, $P/_\equiv$ is finite. Transitions are defined as follows. Let a be in A. If pa is in P, then there is a transition $[p]_\equiv\xrightarrow{a}[pa]_\equiv$. If pa is not in $H\cup P$, then there is a transition $[p]_\equiv\xrightarrow{a}[v]_\equiv$ with v in P maximal in length such that $pa=uv$. Every state is terminal. □

Now, we can prove the following theorem. The main result, Theorem 3.11, will be a special case of it.

Theorem 3.10. *Let β be a Pisot number and B a positive integer such that* (D$_B$) *holds. Then one can construct a finite automaton recognizing the set of β-expansions of minimal weight in $\{1-B,\dots,B-1\}^*$.*

Proof. Let $A=\{1-B,\dots,B-1\}$, $x\in A^*$ 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 3.1. 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 $\mathcal{T}_\beta$ composed of transitions $(s_{j-1},\delta_{j-1})\xrightarrow{x_j|y_j}(s_j,\delta_j)$, $1\le j\le n$, with $s_0=0$, $\delta_0=0$, $s_n=0$, $\delta_n<0$.

We determine bounds for δ_j, $1\le j\le n$, 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 $W=\max\{w_s \mid s \text{ is a state in } \mathcal{A}_\beta\}$. If $\delta_j\le -W-B$, then let $h\le j$ be such that $x_h\ne 0$, $x_i=0$ for $h<i\le j$. Since $|x_h|<B$, we have $\delta_{h-1}<\delta_j+B\le -W\le -w_{s_{h-1}}$, 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 $x_h\ne 0$, this contradicts the assumption that x is strictly β-heavy.

Let $\mathcal{S}_\beta$ be the restriction of $\mathcal{T}_\beta$ to the states (s,δ) with $-W-B<\delta\le w_s$ 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 $\mathcal{S}_\beta$ consists only of β-heavy words and contains all strictly β-heavy words in A^*. Therefore $M=A^*\setminus A^*HA^*$ is the set of β-expansions of minimal weight in A^*, and M is recognizable by a finite automaton by Lemma 3.9. □

Theorem 3.11. *Let β be a Pisot number. Then one can construct a finite automaton recognizing the set of β-expansions of minimal weight.*

Proof. Proposition 3.5 shows that β satisfies (D_B) for some positive integer B, and that no β-expansion of minimal weight $y\in\mathbb{Z}^*$ can contain a digit y_j with $|y_j|\ge B$, since we obtain a β-lighter word if we replace B by b as in the proof of Proposition 3.1. Therefore Theorem 3.10 implies Theorem 3.11. □

4 Golden Ratio case

In this section we give explicit constructions for the case where β is the Golden Ratio $\frac{1+\sqrt5}{2}$. We have $1={\bullet}11$, hence $2=10{\bullet}01$ and β satisfies (D_2), see also Example 1.1. Corollary 3.2 shows that every $z\in\mathbb{Z}[\beta^{-1}]$ can be represented by a β-expansion of minimal weight in $\{-1,0,1\}^*$. For most applications, only these expansions are interesting. Remark that the digits of arbitrary β-expansions of minimal weight are in $\{-2,-1,0,1,2\}$ by the proof of Theorem 3.11, since $3=100{\bullet}01$.

For typographical reasons, we write the digit -1 as $\bar1$ in words and transitions.

4.1 β-expansions of minimal weight for $\beta=\frac{1+\sqrt5}{2}$

Our aim in this section is to construct explicitly the finite automaton recognizing the β-expansions of minimal weight in A^*, $A=\{-1,0,1\}$.

Theorem 4.1. *If $\beta=\frac{1+\sqrt5}{2}$, then the set of β-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.*

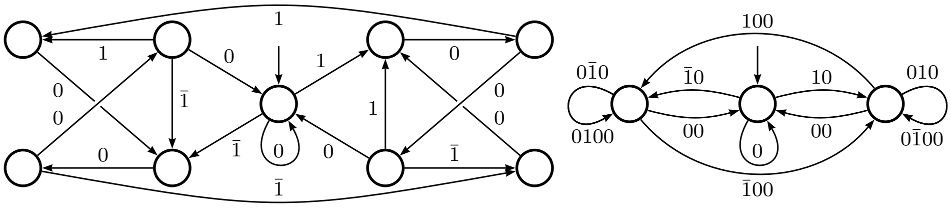

Figure 1. Automaton $\mathcal{M}_\beta$ recognizing β-expansions of minimal weight for $\beta = \frac{1+\sqrt{5}}{2}$ (left) and a compact representation of $\mathcal{M}_\beta$ (right).

It is of course possible to follow the proof of Theorem 3.10, but the states of $\mathcal{A}_\beta$ are

$$0,\ \pm\frac{1}{\beta^3},\ \pm\frac{1}{\beta^2},\ \pm\frac{1}{\beta},\ \pm1,\ \pm\beta,\ \pm\beta^2,\ \pm\beta\pm\frac{1}{\beta^2},\ \pm\beta\pm\frac{1}{\beta^3},\ \pm\beta^2\pm\frac{1}{\beta^2},\ \pm\beta^2\pm\frac{1}{\beta^3},$$

thus $W = 2$ and the transducer $\mathcal{S}_\beta$ has 160 states. For other bases β, the number of states can be much larger. Therefore we have to refine the techniques if we do not want computer-assisted proofs. It is possible to show that a large part of $\mathcal{S}_\beta$ is not needed, e.g. by excluding some β-heavy factors such as 11 from the output, and to obtain finally the transducer in Figure 2. However, it is easier to prove Theorem 4.1 by an indirect strategy, which includes some results which are interesting by themselves.

Lemma 4.2. *All words in* $\{-1,0,1\}^*$ *which are not recognized by the automaton* $\mathcal{M}_\beta$ *in Figure 1 are* β*-heavy.*

Proof. The transducer in Figure 2 is a part of the transducer $\mathcal{S}_\beta$ in the proof of Theorem 3.10. This means that every word which is the input of a path (with full or dashed transitions) going from $(0,0)$ to $(0,-1)$ is β-heavy, because the output has the same value but less weight. Since a β-heavy word remains β-heavy if we omit the leading and trailing zeros, the dashed transitions can be omitted. Then the set of inputs is

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

and $\mathcal{M}_\beta$ is constructed as in the proof of Lemma 3.9. □

Similarly to the NAF in base 2, where the expansions of minimal weight avoid the set $\{11, 1\bar{1}, \bar{1}\bar{1}, \bar{1}1\}$, we show in the next result that, for $\beta = \frac{1+\sqrt{5}}{2}$, every real number admits a β-expansion which avoids a certain finite set X.

Proposition 4.3. *If* $\beta = \frac{1+\sqrt{5}}{2}$*, then every* $z \in \mathbb{R}$ *has a* β*-expansion of the form* $z = y_1 \cdots y_k \raisebox{0.2ex}{.} y_{k+1} y_{k+2} \cdots$ *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.*

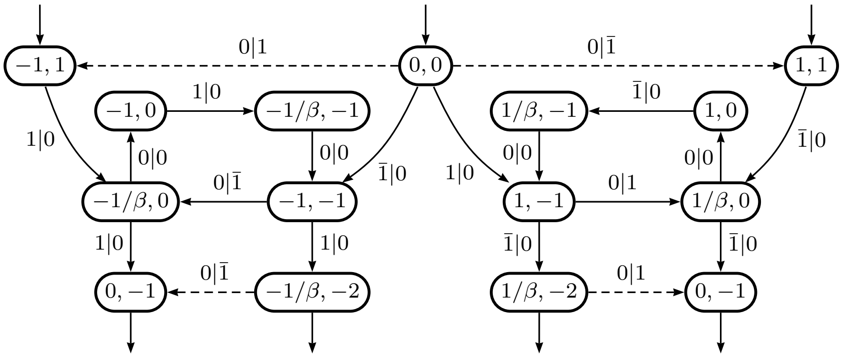

Figure 2. Transducer with strictly β-heavy words as inputs, $\beta = \frac{1+\sqrt{5}}{2}$.

Proof. We determine this β-expansion similarly to the greedy β-expansion in the Introduction. Note that the maximal value of $\bullet x_1x_2\cdots$ for a sequence $x_1x_2\cdots$ avoiding the elements of X is $\bullet(1000)^\omega = \beta^2/(\beta^2+1)$. 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 $y_j = \left\lfloor \frac{\beta^2+1}{2\beta}\tau^{j-1}(z) + 1/2\right\rfloor$ for $z \in \left[\frac{-\beta^2}{\beta^2+1},\frac{\beta^2}{\beta^2+1}\right)$, $j \geq 1$, then $z = \bullet y_1y_2\cdots$. If $y_j = 1$ for some $j \geq 1$, then we have $\tau^j(z) \in \beta \times \left[\frac{\beta}{\beta^2+1},\frac{\beta^2}{\beta^2+1}\right) - 1 = \left[\frac{-1}{\beta^2+1},\frac{1/\beta}{\beta^2+1}\right)$, hence $y_{j+1} = 0$, $y_{j+2} = 0$, and $\tau^{j+2}(z) \in \left[\frac{-\beta^2}{\beta^2+1},\frac{\beta}{\beta^2+1}\right)$, 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 $z \in \left[\frac{-\beta^2}{\beta^2+1},\frac{\beta^2}{\beta^2+1}\right)$. For arbitrary $z \in \mathbb{R}$, the expansion is given by shifting the expansion of $\beta^{-k}z$, $k \geq 0$, to the left.

If we choose $y_j = 0$ in case $\tau^{j-1}(z) > \beta/(\beta^2+1) = \bullet(0100)^\omega$, 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 $\beta\tau^{j-1}(z) - 1 < -1/(\beta^2+1) = \bullet(00\bar{1}0)^\omega$, 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 4.4. 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.

Proposition 4.5. *If x is accepted by $\mathcal{M}_\beta$, then there exists $y \in \{-1,0,1\}^*$ avoiding $X = \{11, 101, 1001, 1\bar{1}, 10\bar{1}$ and their opposites$\}$ with $x \sim_\beta y$ and $\|x\| = \|y\|$. The transducer $\mathcal{N}_\beta$ in Figure 3 realizes the conversion from $0x0$ to y.*

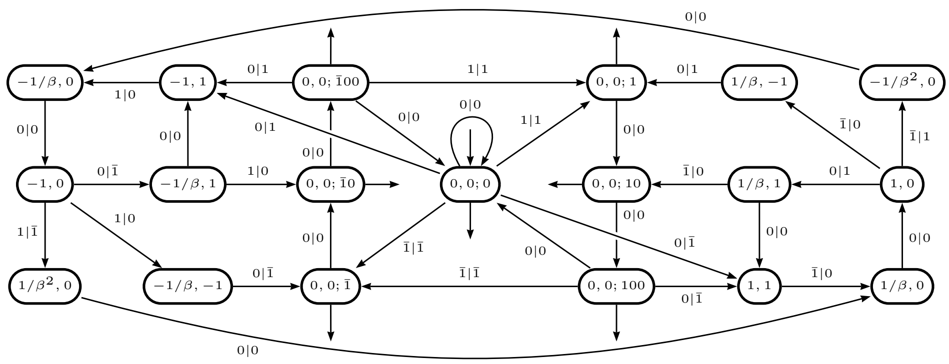

Figure 3. Transducer $\mathcal{N}_\beta$ normalizing β-expansions of minimal weight, $\beta = \frac{1+\sqrt{5}}{2}$.

Proof. Set $Q_0 = \{(0,0;0), (-1,1), (1,1)\} = Q'_0$,

$$Q_1 = \{(0,0;1), (-1/\beta,0)\}, \qquad Q'_1 = \{(0,0;\bar{1}0)\},$$
$$Q_{10} = \{(0,0;10), (-1,0)\}, \qquad Q'_{10} = \{(0,0;\bar{1}00)\},$$
$$Q_{100} = \{(0,0;100), (-1/\beta,1)\}, \qquad Q'_{100} = \{(0,0;0), (-1,1)\},$$
$$Q_{101} = \{(-1/\beta,-1), (1/\beta^2,0)\}, \qquad Q'_{101} = \{(0,0;1)\},$$

and, symmetrically, $Q_{\bar{1}} = \{(0,0;\bar{1}), (1/\beta,0)\}$, $Q'_{\bar{1}} = \{0,0;10\}, \ldots$. 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. 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. □

Proof of Theorem 4.1. For every $x \in \mathbb{Z}^*$, by Proposition 3.1 and Lemma 4.2, there exists a β-expansion of minimal weight y accepted by $\mathcal{M}_\beta$ with $y \sim_\beta x$. By Proposition 4.5, there also exists a β-expansion of minimal weight $y' \in \{-1,0,1\}^*$ avoiding X with $y' \sim_\beta y \sim_\beta x$. By Proposition 4.3, the output of $\mathcal{N}_\beta$ is the same (if we neglect leading and trailing zeros) for every input $0x'0$ such that $x' \sim_\beta x$ and x' is accepted by $\mathcal{M}_\beta$. Therefore $\|x'\| = \|y'\|$ for all these x', and the theorem is proved. □

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 $z = {\scriptstyle\bullet} x_1 \cdots x_n$, $\beta = \frac{1+\sqrt{5}}{2}$. 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*

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

The sequence $(\beta^{j-1}z - x_1\cdots x_{j-1}{\scriptstyle\bullet})_{1\le j\le n}$ 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.

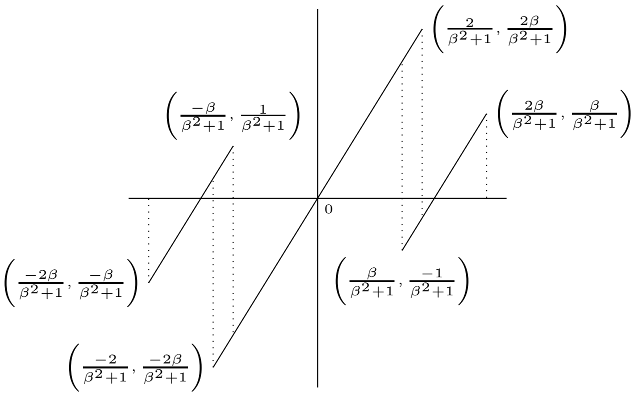

Figure 4. Branching transformation giving all $\frac{1+\sqrt{5}}{2}$-expansions of minimal weight.

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 $\beta^j z - x_1\cdots x_j{\scriptstyle\bullet}$ 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 ${\scriptstyle\bullet}(0010)^\omega = \frac{1}{\beta^2+1}$ and thus ${\scriptstyle\bullet}1(0100)^\omega = \frac{2\beta}{\beta^2+1}$.

If the conditions on z and x_j are not satisfied, then we have either $|{\scriptstyle\bullet}x_j\cdots x_n| > {\scriptstyle\bullet}1(0100)^\omega$, or $x_j = 1$ and ${\scriptstyle\bullet}x_{j+1}\cdots x_n < {\scriptstyle\bullet}(00\bar{1}0)^\omega$, or $x_j = -1$ and ${\scriptstyle\bullet}x_{j+1}\cdots x_n > {\scriptstyle\bullet}(0010)^\omega$ 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 4.2, hence $x_1\cdots x_n$ is β-heavy. □

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

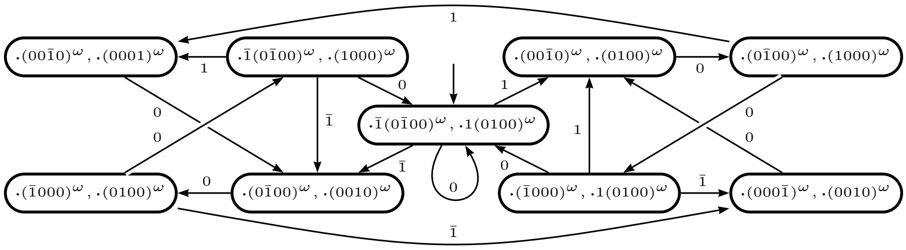

Figure 5. Automaton $\mathcal{M}_\beta$ with intervals as labels.

defined by the sequence of Fibonacci numbers $F = (F_n)_{n\ge0}$ 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_2) 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 $n \ge 2$. Since $20 \sim_F 101$ and $2 \sim_F 10$, we obtain similarly to the proof of Proposition 3.1 that for every $x \in \mathbb{Z}^*$ there exists some $y \in \{-1,0,1\}^*$ with $x \sim_F y$ and $\|y\| \le \|x\|$. 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 4.1. 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 $y_1 \ne 0$ 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. □

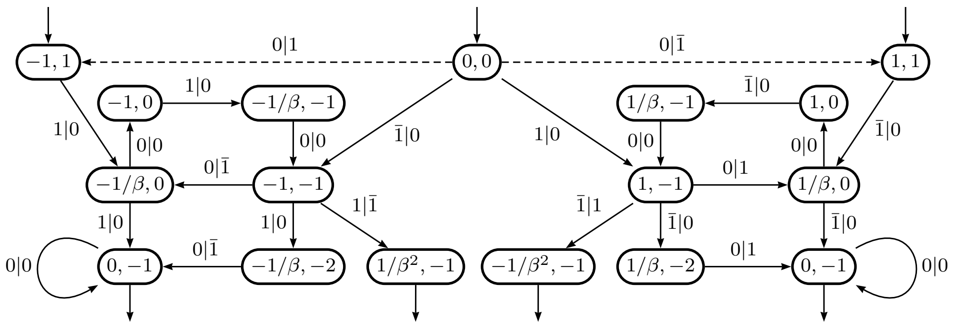

Figure 6. All inputs of this transducer are strongly F-heavy.

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 $\mathcal{R}_F$ for the Fibonacci numeration system is similar to $\mathcal{R}_\beta$, 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

$$\begin{aligned} &\Pr[Y_1 = y_1 y_2 y_3, \ldots, Y_j = y_j y_{j+1} y_{j+2}] \\ &\qquad = \#\{x_1 \cdots x_{n+2} \in W_n 00 :\ x_1 \cdots x_{j+2} = y_1 \cdots y_{j+2}\}/\#W_n, \end{aligned}$$

$\Pr[Y_{j-1} = xyz, Y_j = x'y'z'] = 0$ 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

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

$$1 - 2\Pr[Y_{j+1} = 001 \mid Y_j = 000] = \Pr[Y_{j+1} = 000 \mid Y_j = 000] = \frac{2G_{n-j-3}+1}{2G_{n-j-2}+1},$$

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. [8]. 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 [8], 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 4.3 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 $1 = {\bullet}111$, we have $2 = 10{\bullet}001$ and β satisfies (D_2). Here, the digits of arbitrary β-expansions of minimal weight are in $\{-5, \dots, 5\}$ since $6 = 1000{\bullet}00\bar{1}0\bar{1}0\bar{1}$. We have $5 = 101{\bullet}100011$ and we will show that 101100011 is a β-expansion of minimal weight, thus 5 is also a β-expansion of minimal weight.

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.

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 the transducer in Figure 8 (without the dashed arrows).

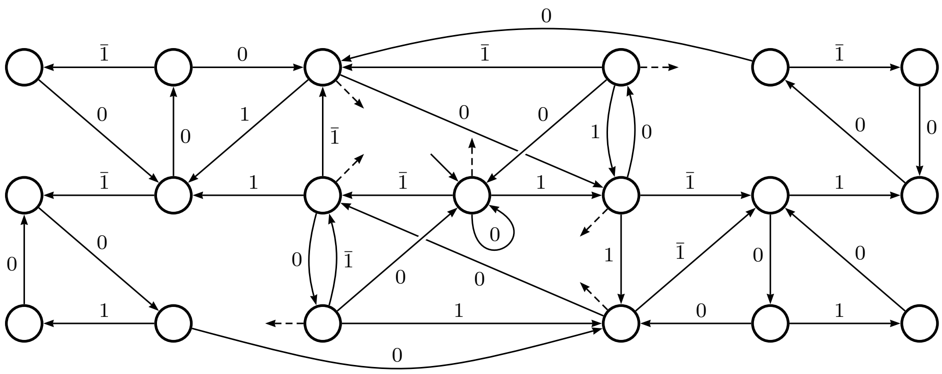

Figure 7. Automata $\mathcal{M}_\beta$, $\beta^3 = \beta^2 + \beta + 1$, and $\mathcal{M}_T$.

Proposition 5.1. *If $\beta > 1$ is the Tribonacci number, then every $z \in \mathbb{R}$ has a β-expansion of the form $z = y_1 \cdots y_k \boldsymbol{.} y_{k+1} y_{k+2} \cdots$ 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 given 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 $(100)^\omega$, $\boldsymbol{.}(100)^\omega = \frac{\beta}{\beta+1}$.

Remark 5.2. The transformation $\tau(z) = \beta z - \left\lfloor \frac{\beta^2-1}{2} z + \frac{1}{2} \right\rfloor$ 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.

Proposition 5.3. *The conversion of an arbitrary expansion accepted by the automaton $\mathcal{M}_\beta$ in Figure 7 into the expansion avoiding $X = \{11, 101, 1\bar{1},$ and their opposites$\}$ is realized by the transducer $\mathcal{N}_\beta$ in Figure 9 and does not change the weight.*

Theorem 5.4. *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 $z = \boldsymbol{.}01(001)^n$, then we have no β-expansion of minimal weight of the form $z = \boldsymbol{.}1x_2x_3\cdots$, whereas $z' = \boldsymbol{.}0011$ has the expansion $\boldsymbol{.}1\bar{1}$, and $z' < z$. On the other hand, $z = \boldsymbol{.}1(100)^n 11$ has no β-expansion of minimal weight of the form $z = \boldsymbol{.}1x_2x_3\cdots$ (since $1(100)^n 11$ is β-heavy but $(100)^n 11$ is not β-heavy), whereas $z' = \boldsymbol{.}1101$ is a β-expansion of minimal

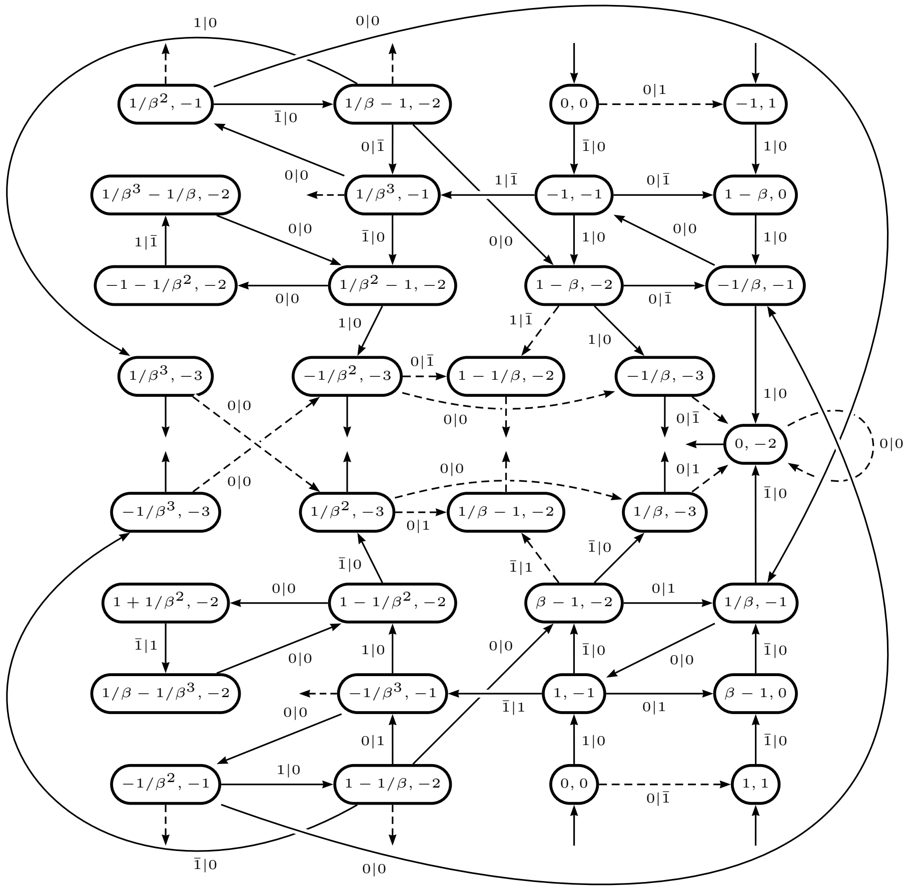

Figure 8. The relevant part of $\mathcal{S}_\beta$, $\beta^3 = \beta^2 + \beta + 1$, and $\mathcal{S}_T$.

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.

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 $n \geq 3$, $200 \sim_T 1001$,

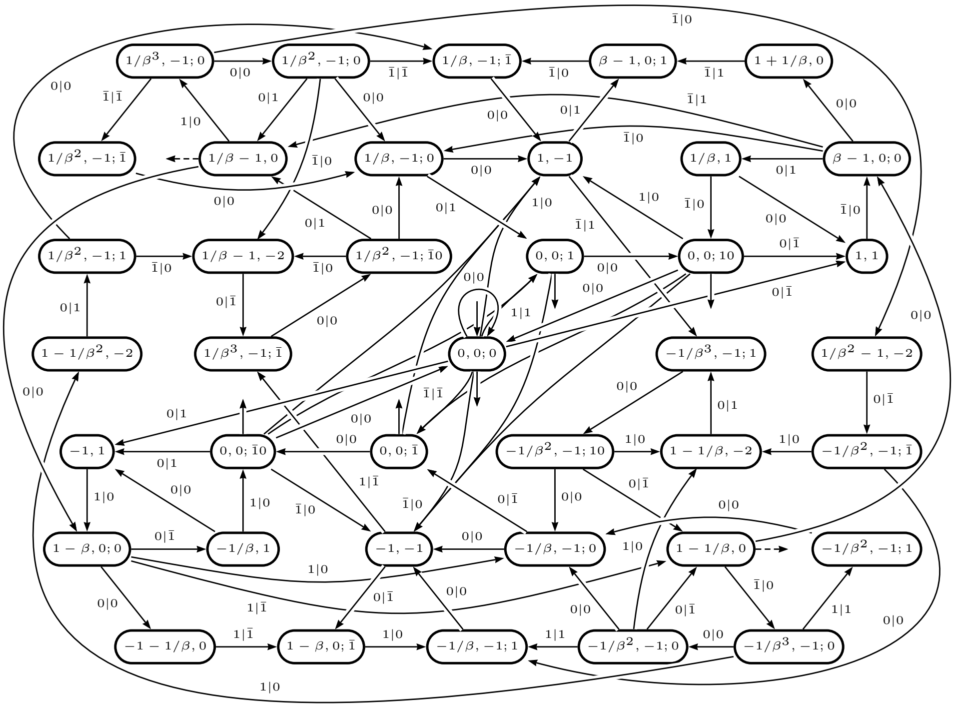

Figure 9. Normalizing transducer $\mathcal{N}_\beta$, $\beta^3 = \beta^2 + \beta + 1$.

$20 \sim_T 100$ 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 5.5. *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 $\mathcal{R}_T$. 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.

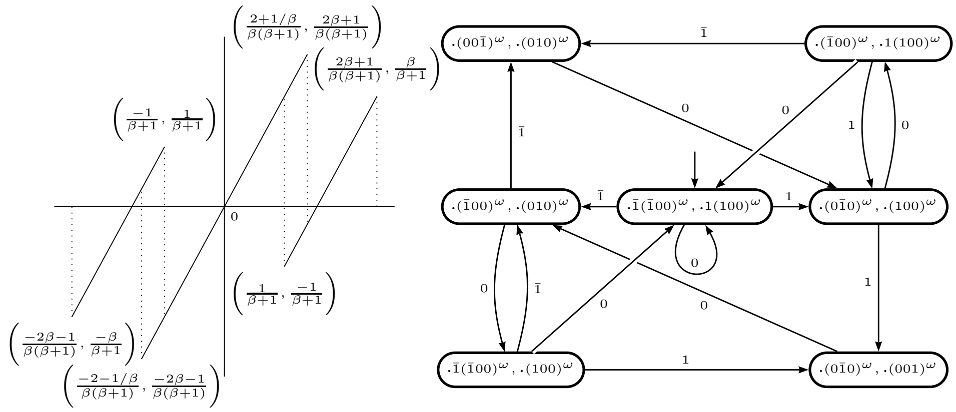

Figure 10. Branching transformation, corresponding automaton, $\beta^3 = \beta^2 + \beta + 1$.

Theorem 5.6. *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 5.5 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

$$\Pr[Y_1 = y_1y_2, \ldots, Y_j = y_jy_{j+1}] = \frac{\#\{x_1 \cdots x_{n+1} \in W_n0 : x_1 \cdots x_{j+1} = y_1 \cdots y_{j+1}\}}{\#W_n}$$

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 5.7. *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 $2 = 1000{\bullet}000\bar{1}$, ($\mathrm{D}_2$) holds. We have furthermore $3 = \beta^4 - \beta^{-9}$, thus all β-expansions of minimal weight have digits in $\{-2, \dots, 2\}$.

6.1 β-expansions of minimal weight

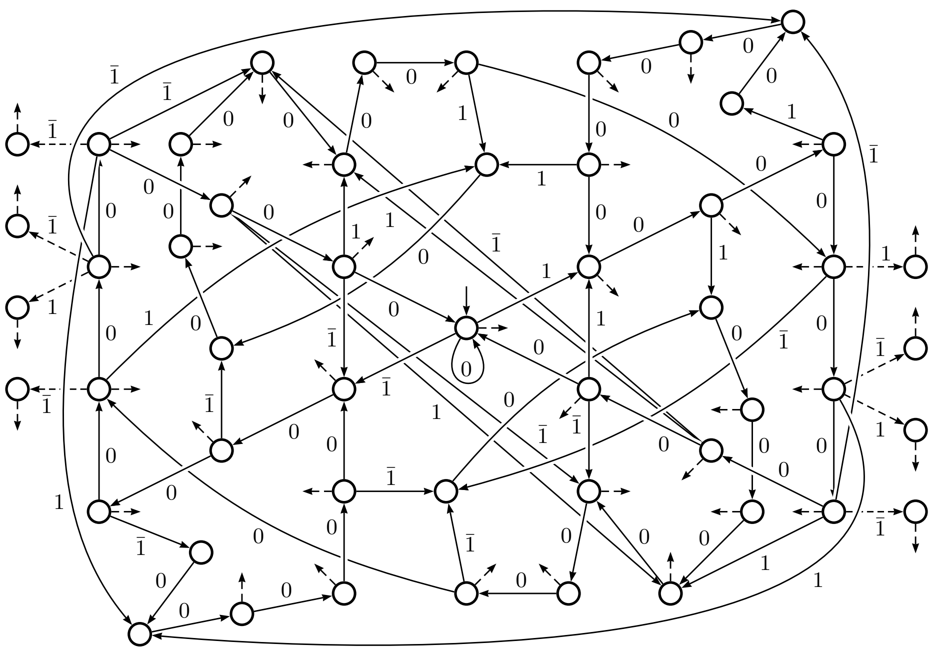

Figure 11. Automata $\mathcal{M}_\beta$, $\beta^3 = \beta + 1$, and $\mathcal{M}_S$.

Let $\mathcal{M}_\beta$ be the automaton in Figure 11 without the dashed arrows where all states are terminal. Then it is a bit more difficult than in the Golden Ration and the Tribonacci cases to see that all words which are not accepted by $\mathcal{M}_\beta$ are β-heavy, not only because the automata are larger but also because some inputs of the transducer in Figure 13 are not strictly β-heavy (but of course still β-heavy). We refer to [13] for details.

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

The expansion in Proposition 6.1 is given by the transformation

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

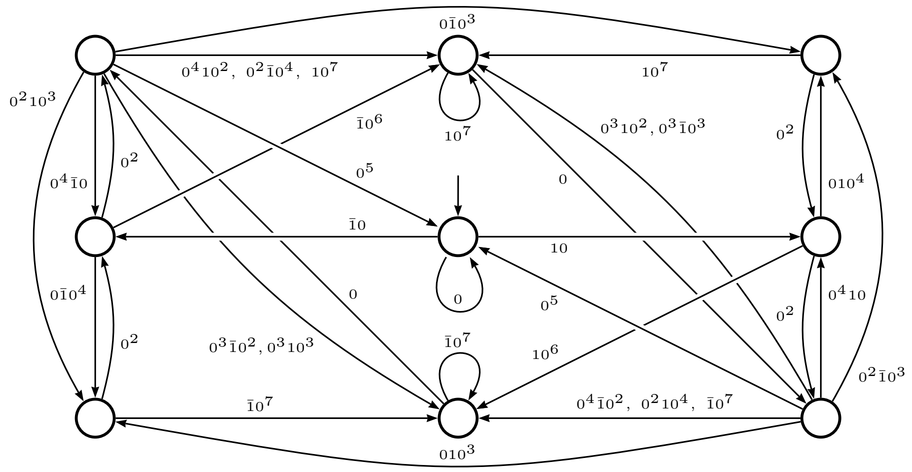

Figure 12. Compact representation of $\mathcal{M}_\beta$.

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 $(10^7)^\omega$, $\boldsymbol{.}(10^7)^\omega = \beta^7/(\beta^8-1) = \beta^3/(\beta^2+1)$.

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 $10^6 1$.

Proposition 6.3. *The conversion of an arbitrary expansion accepted by $\mathcal{M}_\beta$ into the expansion avoiding $X = \{10^6 1, 10^k 1, 10^k \bar{1}, 0 \le k \le 5,$ and their opposites$\}$ is realized by the transducer $\mathcal{N}_\beta$ in Figure 14 and does not change the weight.*

Theorem 6.4. *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, the maximal interval for the digit 1 is $[\boldsymbol{.}(010^6)^\omega, \boldsymbol{.}1(0^5 10^2)^\omega]$, with $\boldsymbol{.}(010^6)^\omega = \frac{\beta^2}{\beta^2+1}$ and $\boldsymbol{.}1(0^5 10^2)^\omega = \frac{\beta^2+1/\beta}{\beta^2+1}$. The corresponding branching transformation and expansions are given in Figure 15.

6.3 Integer expansions

Let $(S_n)_{n\ge0}$ be a linear numeration system associated with the smallest Pisot number β which is defined as follows:

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

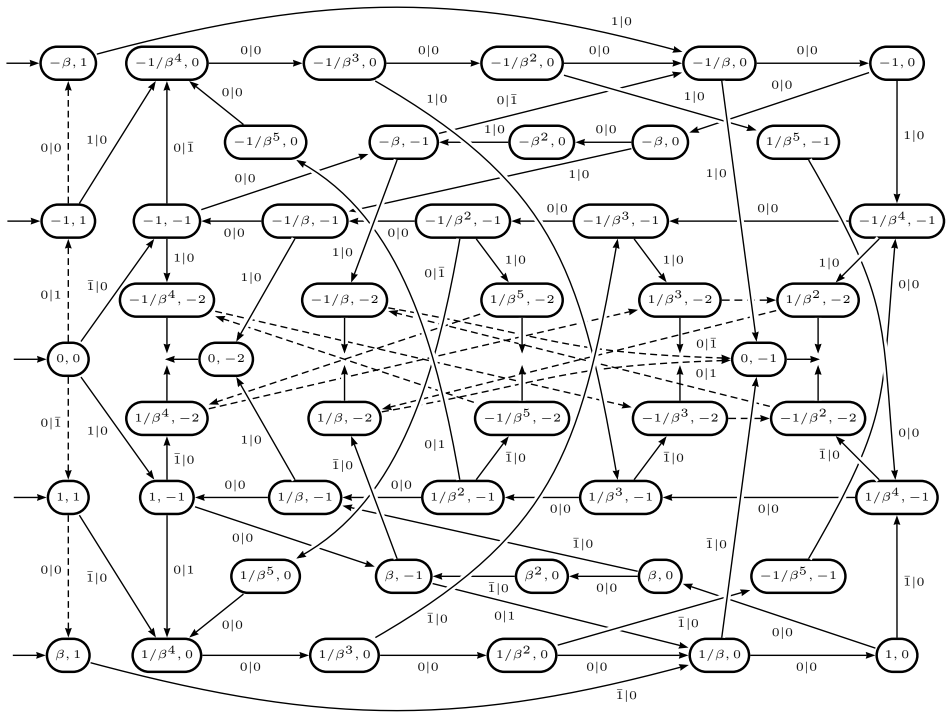

Figure 13. The relevant part of $\mathcal{S}_\beta$, $\beta^3 = \beta + 1$.

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 $n \geq 5$, since $U_n = U_{n-2} + U_{n-3}$ holds only for $n \equiv 1 \bmod 3$, $n \geq 4$.

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

Proposition 6.5. *Every $N \in \mathbb{Z}$ has a unique representation $N = \sum_{j=1}^n y_j S_{n-j}$ with $y_1 \neq 0$ and $y_1 \cdots y_n \in \{-1, 0, 1\}^*$ avoiding the set $X = \{10^6 1, 10^k 1, 10^k \bar{1}, 0 \leq k \leq 5,$ and their opposites$\}$, with the exception that $10^6 1, 10^5 1, 10^5 \bar{1}, 10^4 \bar{1}$ and their opposites are possible suffixes of $y_1 \cdots y_n$.*

As for the Fibonacci numeration system, Proposition 6.5 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, $n \geq 1$, depending on the congruence class of n modulo 8 are given by the following table.

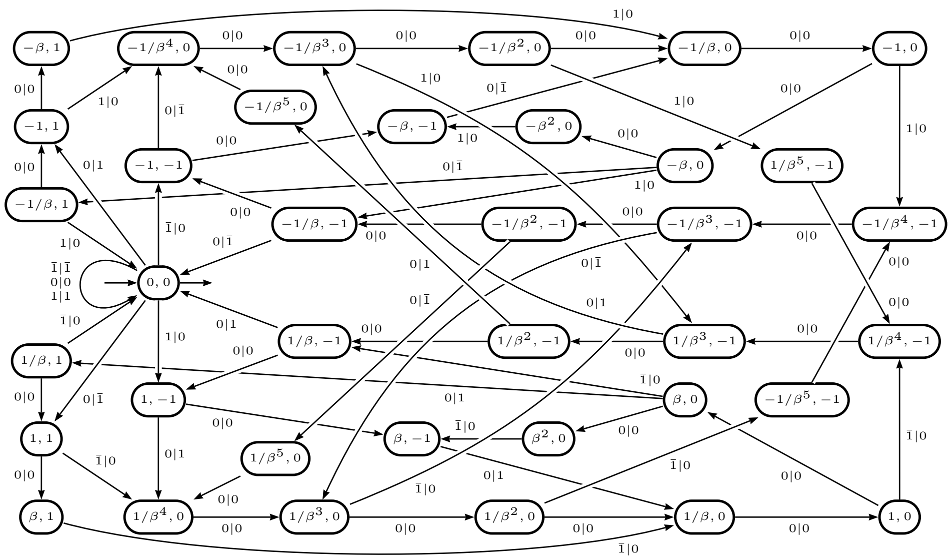

Figure 14. Transducer $\mathcal{N}_\beta$ normalizing β-expansions of minimal weight, $\beta^3 = \beta + 1$.

$n \equiv j \bmod 8$	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	$1(0^6\bar{1}0)^{(n-7)/8}0^6\bar{1}$	$(10^7)^{(n-7)/8}10^5 1$	$1\bar{1}00000\bar{2} \sim_S 10\bar{2} \sim_S 1$
0	$1(0^6\bar{1}0)^{n/8}$	$(10^7)^{n/8-1}10^6 1$	$1\bar{1}00000\bar{1}\bar{1} \sim_S 10\bar{1}\bar{1} \sim_S 1$

For the calculation of $g_{n+1} - G_n$ we have used $S_n - S_{n-1} - S_{n-7} = S_{n-8}$ for $n \geq 9$.

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 $z = a_1 \cdots a_n\bullet = m_3 m_2 m_1 a_n\bullet$, then we have $N = \sum_{j=1}^{n} a_j S_{n-j} = 4m_3 + 3m_2 + 2m_1 + a_n$. We have to distinguish between different values of a_n.

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

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

  In particular, $m_3 m_2' \in \{00, \bar{1}1, 01\}$ provides $N = 0$ if $z \in \{1/\beta^2, 1/\beta^3, 1/\beta^5\}$.

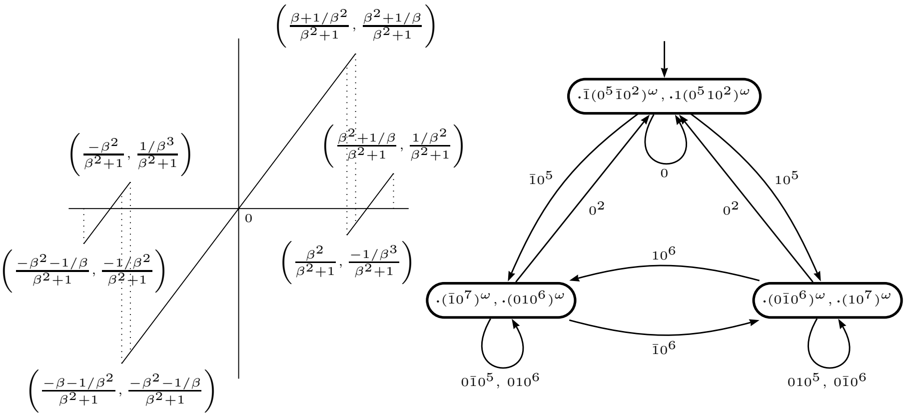

Figure 15. Branching transformation and corresponding automaton, $\beta^3 = \beta + 1$.

- 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 $\mathcal{R}_\beta$ ends in a state z corresponding to $a_n = x_n - y_n$ (or in $-z$, $a_n = y_n - x_n$) and obtain the following theorem.

Theorem 6.6. *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 6.5 are S-expansions of minimal weight.*

For details on the proof of Theorem 6.6, we refer again to [13].

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 6.5. 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 6.7. *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_2), which is not studied in this article, is the Pisot number satisfying $\beta^3 = \beta^2 + 1$, with $2 = 100{\bullet}0000\bar{1}$.

A question which is not approached in this paper concerns β-expansions of minimal weight in $\{1-B,\ldots,B-1\}^*$ when β does not satisfy (D_B), in particular minimal weight expansions on the alphabet $\{-1,0,1\}$ when $\beta < 3$ and (D_2) does not hold.

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

U_n	A	β	average $\|N\|_U$ for $N \in \{-M,\ldots,M\}$
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 $N \in \{-M, \ldots, M\}$, 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 $(1+20/(7+2\beta^2)) \log_\beta M \approx 7.156 \log_2 M < 7.202 \log_2 M \approx (1+20/5) \log_{(1+\sqrt{5})/2} M$.

References

[1] S. Akiyama, *Cubic Pisot units with finite beta expansions*, Algebraic number theory and Diophantine analysis (Graz, 1998), de Gruyter, Berlin, 2000, pp. 11–26.

[2] S. Arno and F. S. Wheeler, *Signed Digit Representations of Minimal Hamming Weight*, IEEE Trans. Computers 42 (1993), pp. 1007–1010.

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

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

[5] W. Bosma, *Signed bits and fast exponentiation*, J. Théor. Nombres Bordeaux 13 (2001), pp. 27–41.

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

[7] V. Dimitrov, T. Cooklev, and B. Donevsky, *Number theoretic transforms over the Golden Section quadratic field*, IEEE Trans. Signal Proc. 43 (1995), pp. 1790–1797.

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

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

[10] S. Eilenberg, *Automata, languages, and machines. Vol. A*. Academic Press, New York, 1974.

[11] Ch. Frougny, *Representations of numbers and finite automata*, Math. Systems Theory 25 (1992), pp. 37–60.

[12] Ch. Frougny and B. Solomyak, *Finite beta-expansions*, Ergodic Theory Dynam. Systems 12 (1992), pp. 713–723.

[13] Ch. Frougny and W. Steiner, *Minimal weight expansions in Pisot bases*, preliminary version, arXiv:0803.2874v2.

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

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

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

[17] M. Joye and C. Tymen, *Compact encoding of non-adjacent forms with applications to elliptic curve cryptography*, Public key cryptography (Cheju Island, 2001), Lecture Notes in Comput. Sci. 1992, Springer, Berlin, 2001, pp. 353–364.

[18] M. Lothaire, *Algebraic combinatorics on words*, Encyclopedia of Mathematics and its Applications 90. Cambridge University Press, Cambridge, 2002.

[19] N. Meloni, *New point addition formulae for ECC applications*, Arithmetic of finite fields, Lecture Notes in Comput. Sci. 4547, Springer, Berlin, 2007, pp. 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), pp. 531–543.

[21] J. A. Muir and D. R. Stinson, *Minimality and other properties of the width-w nonadjacent form*, Math. Comp. 75 (2006), pp. 369–384.

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

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

[24] A. Rényi, *Representations for real numbers and their ergodic properties*, Acta Math. Acad. Sci. Hungar 8 (1957), pp. 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 Cryptogr. 19 (2000), pp. 195–249.

Received 27 March, 2008; revised 16 December, 2008

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