Minimal weight expansions in Pisot bases
Christiane Frougny, Wolfgang Steiner

To cite this version:

HAL Id: hal-00265661
https://hal.science/hal-00265661v3
Submitted on 9 Jan 2009

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
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 real bases $\beta$ which are Pisot numbers and prove that the expansions with minimal absolute sum of digits are recognizable by finite automata. When $\beta$ is the Golden Ratio, the Tribonacci number or the smallest Pisot number, we determine expansions with minimal number of digits $\pm 1$ and give explicitly 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 $x = x_1x_2 \cdots x_n$ 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 $\beta$ 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 $\tau$ related to Koblitz curves, and has given a $\tau$-NAF form, and the Hamming weight of these representations has been studied in [9].

This research was supported by the French 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 $\beta$-expansion given by the $\beta$-transformation $r_{\beta}$, which relies on a greedy algorithm: let $r_{\beta}(z) = \beta z - \lfloor \beta z \rfloor$ and define, for $j \geq 1$, $x_j = \lfloor \beta^{j-1} r_{\beta}(z) \rfloor$. 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 $z = x_1 x_2 \cdots$. If there exists a $n$ such that $x_j = 0$ for all $j > n$, the expansion is said to be finite and we write $z = x_1 x_2 \cdots x_n$. By shifting, any non-negative real number has a greedy $\beta$-expansion: If $z \in [0, \beta^k)$, $k \geq 0$, and $\beta^{-k} z = x_1 x_2 \cdots$, then $z = x_1 \cdots x_k x_{k+1} x_{k+2} \cdots$.

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 $z = x_1 x_2 \cdots x_n$ is therefore $\mathbb{Z}[\beta^{-1}]$. Note that we do not require that the greedy $\beta$-expansion of every $z \in \mathbb{Z}[\beta^{-1}] \cap [0, 1)$ is finite, although this property (F) holds for the three numbers $\beta$ 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 $x = x_1 x_2 \cdots x_n \in A^*$, $y = y_1 y_2 \cdots y_m \in A^*$ by

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

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

In the following, we consider real bases $\beta$ satisfying the condition

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

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 $\beta$-expansion of minimal weight with digits in $\{1 - B, \ldots, B - 1\}$ if and only if $\beta$ satisfies $(D_B)$.

If $\beta$ 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 $\beta > 1$ satisfying $(D_B)$ which are not Pisot, e.g. the positive solution of $\beta^4 = 2\beta + 1$ is not a Pisot number but satisfies $(D_B)$ since $2 = 1000(-1)$. The following example provides a large class of numbers $\beta$ satisfying $(D_B)$.

**Example 1.1.** If $1 = t_1 t_2 \cdots t_d (t_{d+1})^w$ with integers $t_1 \geq t_2 \geq \cdots \geq t_d > t_{d+1} \geq 0$, then $\beta$ 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 $\beta$-expansions is recognizable by a finite automaton when $\beta$ is a Pisot number [3]. In this work, we prove that the set of all $\beta$-expansions of minimal weight is recognizable by a finite automaton when $\beta$ is a Pisot number.

We then consider particular Pisot numbers satisfying $(D_2)$ which have been extensively studied from various points of view. When $\beta$ is the Golden Ratio, we construct a finite transducer which gives, for a strictly $\beta$-heavy word as input, a $\beta$-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 $\beta$-expansions of minimal weight in $\{-1, 0, 1\}^\ast$. We give a branching transformation which provides all $\beta$-expansions of minimal weight in $\{-1, 0, 1\}^\ast$ 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 $\frac{1}{\beta} \log_\beta M$, which means that typically only every fifth digit is non-zero. Note that the corresponding value for 2-expansions of minimal weight is $\frac{1}{2} \log_2 M$, see [2, 5], and that $\frac{1}{2} \log_2 M \approx 0.288 \log_2 M$.

We obtain similar results for the case where $\beta$ 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 $\frac{\beta}{\beta-1} \log_\beta M \approx 0.282 \log_\beta M \approx 0.321 \log_2 M$.

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

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 $A^\ast$. The set $A$ is called alphabet. The set of infinite sequences or infinite words on $A$ is denoted by $A^n$. Let $v$ be a word of $A^\ast$, denote by $v^n$ the concatenation of $v$ to itself $n$ times, and by $v^\omega$ the infinite concatenation $vwv \cdots$.

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 $A$, $A = (Q, A, E, I, T)$, 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 $A^\ast$ is said to be recognizable by a finite automaton if there exists a finite automaton $A$.
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 \( T = (Q, A^* \times A^*, E, I, T) \) 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 \( p \xrightarrow{u} v \). 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 \( \beta \)-expansions of minimal weight when \( \beta \) is a Pisot number.

We need first some combinatorial results for bases \( \beta \) satisfying (D\(_B\)). Note that \( \beta \) is not assumed to be a Pisot number here.

**Proposition 3.1.** If \( \beta \) 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 \( \beta \) satisfies (D\(_B\)) with some integer \( B \geq 2 \), then for every word \( x \in \mathbb{Z}^* \) there exists a \( \beta \)-expansion of minimal weight \( y \in \{1 - B, \ldots, B - 1\}^* \) with \( x \sim_\beta y \).

**Remark 3.3.** If \( \beta \) satisfies (D\(_B\)) for some positive integer \( B \), then it is easy to see that \( \beta \) satisfies (D\(_C\)) for every integer \( C > B \).

**Remark 3.4.** If \( \beta \) does not satisfy (D\(_B\)), then all words \( x \in \{1 - B, \ldots, B - 1\}^* \) with \( x \sim_\beta B \) are \( \beta \)-heavier than \( B \). It follows that the set of \( \beta \)-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 \( x_k \notin \mathbb{Z} \) 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 \( x_{j}^{(i)} = x_j \) for \( 1 \leq j \leq n \), \( x_{j}^{(i)} = 0 \) for \( j \leq 0 \) and \( j > n \), \( b_j = 0 \) for \( j < -k \) and \( j > d \). Define, recursively for \( i \geq 0 \),

\[
h_i = \max \{ j \in \mathbb{Z} : |x_j^{(i)}| \geq B \},
\]

\[
x_{h_i}^{(i+1)} = x_{h_i}^{(i)} + \text{sgn}(x_{h_i}^{(i)})(b_0 - B), \quad x_{h_i}^{(i+1)} = x_{h_i}^{(i)} + \text{sgn}(x_{h_i}^{(i)})b_j
\]

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 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

\[
\sum_{j=-\infty}^{h_i-1} |x_j^{(i+1)}| = \sum_{j=-\infty}^{h_i-1} |x_j^{(i)}| + \sum_{j=h_i+1}^{d} |b_j|.
\]

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

\[
\|x\| \geq \sum_{j=-\infty}^{h_{i_m}+1} |x_j^{(i_m+1)}| \geq \sum_{j=-\infty}^{h_{i_m}+1} |x_j^{(i_m+1)}| + \sum_{j=h_{i_m}+1}^{k} |b_j| \geq \cdots \geq (m+1) \sum_{j=1}^{k} |b_j|.
\]

If \( \sum_{j=1}^{d} |b_{-j}| > 0 \), 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 \( \sum_{j=1}^{d} |b_{-j}| > 0 \) 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 \( x_{h_{i'}-k} \cdots x_{h_{i'}} = x_{h_{i'}-k} \cdots x_{h_i}, x_{h_{i'}+1}x_{h_{i'}+2} \cdots = 0^{h_i-h_{i'}}x_{h_{i'}+1}x_{h_{i'}+2} \cdots \), and \( x_{h_{i}+j} = x_{h_{i'}+j} = 0 \) for all \( j > k \). This implies \( x_{h_{i-k}} \cdots x_{h_i} \sim 0 \) or \( h_{i-k} = 1 \).

In the first case, \( x_{h_{i-k}}+x_{h_{i-k}+2} \cdots \) 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. \( \square \)

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

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

**Proof.** If \( \beta \) is an integer, then we can choose \( B = \beta \) and \( b = 1 \). So let \( \beta \) be a Pisot number of degree \( d \geq 2 \), i.e., \( \beta \) 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 \( z = P(\beta), P \in \mathbb{Q}[X] \).

---

1For 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, $L = \lfloor \log B / \log \beta \rfloor$, and $x_1x_2 \cdots$ the greedy $\beta$-expansion of $z = \beta^{-L}B \in [0, 1)$. Since

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

we have

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

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

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

For every $y \in Y$, we can choose a $\beta$-expansion $y = a_1 \ldots a_m$. Let $W$ be the maximal weight of all these expansions and $\tau^k_{\beta'}(z) = a'_1 \cdots a'_m$. Since $z = x_1 \ldots x_k + \tau^k_{\beta'}(z)$, the digitwise addition of $x_1 \ldots x_k$ and $a'_1 \cdots a'_m$ provides a word $b$ with $b \sim_\beta B$ and

$$\|b\| \leq k \| \beta \| + W = \max_{2 \leq j \leq d} \left[ \frac{\log B}{\log \beta} - \frac{\log B}{\log |\beta^{(j)}|} \right] \| \beta \| + W = O(\log B).$$

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

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

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

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 $\beta$ is a Pisot number, then $Z_\beta$ is recognized by a finite automaton.

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

The redundancy automaton (or transducer) $R_\beta$ is similar to $A_\beta$. Each transition $s \xrightarrow{a} s'$ of $A_\beta$ is replaced in $R_\beta$ by a set of transitions $s \xrightarrow{a|b} s'$, with $a, b \in A$ and $a - b = c$. From Lemma 3.6, one obtains the following lemma.
Lemma 3.7. The redundancy transducer $\mathcal{R}_\beta$ recognizes the set
\[
\{ (x_1 \cdots x_n, y_1 \cdots y_n) \in A^* \times A^* \mid n \geq 0, \ x_1 \cdots x_n = y_1 \cdots y_n \}.
\]
If $\beta$ 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 $(s, \delta)$, where $s$ is a state of $\mathcal{R}_\beta$ and $\delta \in \mathbb{Z}$. The transitions are of the form $(s, \delta) \xrightarrow{ab} (s', \delta')$ if $s \xrightarrow{a} s'$ 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
\[
\{ (x_1 \cdots x_n, y_1 \cdots y_n) \in A^* \times A^* \mid x_1 \cdots x_n = y_1 \cdots y_n, \ |y_1 \cdots y_n| < |x_1 \cdots x_n| \}.
\]
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 $M = A^* \setminus A^*H_A^*$. 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 $[p] \xrightarrow{a} [pa]$. If $pa$ is not in $H \cup P$, then there is a transition $[p] \xrightarrow{a} [v]$ with $v$ in $P$ maximal in length such that $pa = uv$. Every state is terminal. \qed

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

Theorem 3.10. Let $\beta$ 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 $\beta$-expansions of minimal weight in $\{1 - B, \ldots, B - 1\}^*$.

Proof. Let $A = \{1 - B, \ldots, B - 1\}$, $x \in A^*$ be a strictly $\beta$-heavy word and $y \in A^*$ be a $\beta$-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 $x_1 \cdots x_n = y_1 \cdots y_n$. Then there is a path in the transducer $\mathcal{T}_\beta$ composed of transitions $(s_{j-1}, \delta_{j-1}) \xrightarrow{x_1/y_1} (s_j, \delta_j)$, $1 \leq j \leq n$, with $s_0 = 0$, $\delta_0 = 0$, $s_n = 0$, $\delta_n < 0$.

We determine bounds for $\delta_j$, $1 \leq j \leq n$, which depend only on the state $s = s_j$. Choose a $\beta$-expansion of $s$, $s = a_1 \cdots a_{j-1}a_{j+1} \cdots a_m$, 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 $s_j = (x_1 - y_1) \cdots (x_j - y_j)$,
In this section we give explicit constructions for the case where \( \beta \) is the Golden Ratio \( \frac{1+\sqrt{5}}{2} \). We have \( 1 = .11, \) hence \( 2 = 10.01 \) and \( \beta \) 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 \( \beta \)-expansion of minimal weight in \( \{-1,0,1\}^* \). For most applications, only these expansions are interesting. Remark that the digits of arbitrary \( \beta \)-expansions of minimal weight are in \( \{-2,-1,0,1,2\} \) by the proof of Theorem 3.11, since \( 3 = 100.01 \).

For typographical reasons, we write the digit \(-1\) as \( \bar{1} \) in words and transitions.

### 4 Golden Ratio case

In this section we give explicit constructions for the case where \( \beta \) is the Golden Ratio \( \frac{1+\sqrt{5}}{2} \). We have \( 1 = .11, \) hence \( 2 = 10.01 \) and \( \beta \) 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 \( \beta \)-expansion of minimal weight in \( \{-1,0,1\}^* \). For most applications, only these expansions are interesting. Remark that the digits of arbitrary \( \beta \)-expansions of minimal weight are in \( \{-2,-1,0,1,2\} \) by the proof of Theorem 3.11, since \( 3 = 100.01 \).

For typographical reasons, we write the digit \(-1\) as \( \bar{1} \) in words and transitions.

#### 4.1 \( \beta \)-expansions of minimal weight for \( \beta = \frac{1+\sqrt{5}}{2} \)

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

**Theorem 4.1.** If \( \beta = \frac{1+\sqrt{5}}{2} \), then the set of \( \beta \)-expansions of minimal weight in \( \{-1,0,1\}^* \) is recognized by the finite automaton \( M_\beta \) of Figure 1 where all states are terminal.
It is of course possible to follow the proof of Theorem 3.10, but the states of $A_\beta$ are

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

thus $W = 2$ and the transducer $S_\beta$ has 160 states. For other bases $\beta$, 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 $S_\beta$ is not needed, e.g. by excluding some $\beta$-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 $M_\beta$ in Figure 1 are $\beta$-heavy.

**Proof.** The transducer in Figure 2 is a part of the transducer $S_\beta$ 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 $\beta$-heavy, because the output has the same value but less weight. Since a $\beta$-heavy word remains $\beta$-heavy if we omit the leading and trailing zeros, the dashed transitions can be omitted. Then the set of inputs is

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

$$\cup \bar{1}(0\bar{1}00)^*\bar{1} \cup \bar{1}(0\bar{1}00)^*0\bar{10} \cup \bar{1}(0010)^*1 \cup \bar{1}(0010)^*01$$

and $M_\beta$ 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 $\{11, 1\bar{1}, \bar{1}1, \bar{1}\bar{1}\}$, we show in the next result that, for $\beta = \frac{1 + \sqrt{5}}{2}$, every real number admits a $\beta$-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 $\beta$-expansion of the form $z = y_1 \cdots y_k y_{k+1} y_{k+2} \cdots$ with $y_j \in \{-1, 0, 1\}$ such that $y_1 y_2 \cdots$ avoids the set $X = \{11, 101, 1001, 1\bar{1}, 1\bar{1}, 1\bar{1}\bar{1}, \bar{1}1, \bar{1}\bar{1}, \bar{1}\bar{1}\}$ and their opposites. If $z \in \mathbb{Z}[\beta] = \mathbb{Z}[\beta^{-1}]$, then this expansion is unique up to leading zeros.
Proof. We determine this $\beta$-expansion similarly to the greedy $\beta$-expansion in the Introduction. Note that the maximal value of $(1000)^{\omega} = \beta^2/(\beta^2 + 1)$. If we define the transformation

$$\tau: \left[ -\frac{\beta^2}{\beta^2 + 1}, \frac{\beta^2}{\beta^2 + 1}, -\frac{\beta^2}{\beta^2 + 1} \right] \rightarrow \left[ -\frac{\beta^2}{\beta^2 + 1}, \frac{\beta^2}{\beta^2 + 1}, -\frac{\beta^2}{\beta^2 + 1} \right]$$

and set $y_j = \left[ \frac{\beta^2}{\beta^2 + 1}, \tau^{j-1}(z) + 1/2 \right]$ for $z \in \left[ -\frac{\beta^2}{\beta^2 + 1}, \frac{\beta^2}{\beta^2 + 1} \right]$, $j \geq 1$, then $z = \cdot y_1 y_2 \cdots$. If $y_j = 1$ for some $j \geq 1$, then we have $\tau^j(z) \in \beta \times \left[ \frac{\beta^2}{\beta^2 + 1}, \frac{\beta^2}{\beta^2 + 1} \right] - 1 = \left[ 1/\beta, 1/\beta + 1 \right]$, hence $y_{j+1} = 0$, $y_{j+2} = 0$, and $\tau^{j+2}(z) \in \left[ \frac{\beta^2}{\beta^2 + 1}, \frac{\beta^2}{\beta^2 + 1} \right]$. This shows that the given factors are avoided.

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, 11, 101 and 1001 and their opposites.

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

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

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

**Proof.** Set $Q_0 = \{(0, 0; 0), (-1, 1), (1, 1)\} = Q'_0$, 
\[
Q_1 = \{(0, 0; 1), (-1/\beta, 0)\}, \quad Q'_1 = \{(0, 0; \bar{1}0)\},
\]
\[
Q_{10} = \{(0, 0; 10), (-1, 0)\}, \quad Q'_{10} = \{(0, 0; \bar{1}00)\},
\]
\[
Q_{100} = \{(0, 0; 100), (-1/\beta, 1)\}, \quad Q'_{100} = \{(0, 0; 0), (-1, 1)\},
\]
\[
Q_{101} = \{-1/\beta, -1\}, \quad (1/\beta^2, 0), \quad Q'_{101} = \{(0, 0; 1)\},
\]
and, symmetrically, $Q_1 = \{(0, 0; 1), (1/\beta, 0)\}$, $Q'_1 = \{0, 0; 10\}$, $\ldots$. 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 $u \rightarrow v$ 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 $q \xrightarrow{a} r$ 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 $q \xrightarrow{0b}$ $(0, 0; w)$, there exists a path with input $0\ast$ 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 $\beta$-expansion of minimal weight $y$ accepted by $\mathcal{M}_\beta$ with $y \sim_\beta x$. By Proposition 4.5, there also exists a $\beta$-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 $\beta$-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 \( z = x_1 \cdots x_n, \beta = \frac{1+\sqrt{5}}{2} \). Then \( x \) is a \( \beta \)-expansion of minimal weight if and only if \( -\frac{2\beta}{\beta^2+1} < z < \frac{2\beta}{\beta^2+1} \) and
\[
\begin{align*}
x_j = \begin{cases} 
1 & \text{if } \frac{2}{\beta^2+1} < \beta^{j-1} z - x_1 \cdots x_{j-1}. < \frac{2\beta}{\beta^2+1} \\
0 \text{ or } 1 & \text{if } \frac{\beta}{\beta^2+1} < \beta^{j-1} z - x_1 \cdots x_{j-1}. < \frac{2\beta}{\beta^2+1} \\
0 & \text{if } \frac{\beta}{\beta^2+1} < \beta^{j-1} z - x_1 \cdots x_{j-1}. < \frac{\beta}{\beta^2+1} \\
-1 \text{ or } 0 & \text{if } \frac{-2\beta}{\beta^2+1} < \beta^{j-1} z - x_1 \cdots x_{j-1}. < \frac{-2\beta}{\beta^2+1} \\
-1 & \text{if } \frac{-2\beta}{\beta^2+1} < \beta^{j-1} z - x_1 \cdots x_{j-1}. < \frac{-2\beta}{\beta^2+1} 
\end{cases}
\end{align*}
\]

The sequence \( (\beta^{j-1} z - x_1 \cdots x_{j-1})_{1 \leq j \leq n} \) is a trajectory \( (\tau i^{-1}(z))_{1 \leq j \leq n} \), 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 \( \beta \)-expansions of minimal weight, we have drawn in Figure 5 an automaton where every state is labeled by the interval containing all numbers \( \beta^j z - x_1 \cdots x_j \), 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 \( \beta \)-expansions of minimal weight. Recall that \( i(0010)^\omega = \frac{1}{\beta^2+1} \) and thus \( i(0100)^\omega = \frac{2\beta}{\beta^2+1} \).

If the conditions on \( z \) and \( x_j \) are not satisfied, then we have either \( |x_j \cdots x_n| > i(0100)^\omega \), or \( x_j = 1 \) and \( -x_{j+1} \cdots x_n < i(0010)^\omega \), or \( x_j = -1 \) and \( -x_{j+1} \cdots x_n > i(0010)^\omega \) for some \( j, 1 \leq j \leq n \). In every case, it is easy to see that \( x_1 \cdots x_n \) must contain a factor in the set \( H \) of the proof of Lemma 4.2, hence \( x_1 \cdots x_n \) is \( \beta \)-heavy. \( \square \)

### 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.
The properties $F$-expansions, with $\sim_F$ e.g. 2 is a $F$-heavy factor need not be $F$-heavy, 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 $\beta$-expansions, with $\sim_F$ instead of $\sim_\beta$. An important difference between the notions $F$-heavy and $\beta$-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, $xylev$ is $F$-heavy if $x(y\text{length}(y))$ 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 (D2) since $2 = 10.01$. 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 3.1 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 $\beta$-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 $y_1 \neq 0$ and $y_1 \cdots y_n \in \{-1,0,1\}^*$ avoiding $X = \{11,101,1001,11,101, \text{and their opposites}\}$.

**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 $g_{n+1} \sim_F$

![Figure 5. Automaton $M_\beta$ with intervals as labels.](image)
1(00\tilde{1})^{n/4}, G_n \sim_F (1000)^{n/4} and 1(\tilde{1}0\tilde{0}1)^{n/4} \sim_F 1, we obtain g_{n+1} - G_n = 1. (A fractional power \((y_1 \cdots y_k)^{1/k}\) denotes the word \((y_1 \cdots y_k)^{1/k}y_1 \cdots y_{j-1}^1(k)\). Therefore the length \(n\) of an expansion \(y_1y_2 \cdots y_n\) 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 \(X\). \[\square\]

![Figure 6](image_url)

**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 \((x_1 - y_1) \cdots (x_n - y_n) = m / \beta^2\) for some \(m \in \mathbb{Z}\), hence the redundancy transducer \(R_F\) for the Fibonacci numeration system is similar to \(R_\beta\), except that all states \(m / \beta^2, m \in \mathbb{Z}\), are terminal.

The transducer in Figure 6 shows that all strictly \(\beta\)-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. \[\square\]

**Remark 4.9.** If we consider only expansions avoiding the factors 11, 101, \(\tilde{1}\), \(\tilde{1}0\tilde{1}\), 100\(\tilde{1}\), 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 \(y_1 \neq 0, y_1 \cdots y_n \in \{1, 0, 1\}^*\) avoiding the factors 11, \(\tilde{1}\), \(\tilde{1}0\tilde{1}\), 11, \(\tilde{1}\), \(\tilde{1}0\tilde{1}\), 100\(\tilde{1}\) and \(y_{j-2}y_{j-1}y_j = 101\) or \(y_{j-3} \cdots y_{j} = 1001\) 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 $M \to \infty$,

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

**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 $11, 101, 1011, 111$, and their opposites. Then we have

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

where $E X_j$ is the expected value of the random variable $X_j$ defined by

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

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

$$\Pr[Y_1 = y_1 y_2 y_3, \ldots, Y_j = y_j y_{j+1} y_{j+2}] = \frac{\#\{x_1 \cdots x_n+2 \in W_n, 00 : x_1 \cdots x_{j+2} = y_1 \cdots y_{j+2}\}}{\#W_n},$$

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

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

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

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

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

$$(p_{u,v})_{u,v \in \{00,001,000,00,010,01,001,010,011\}} = \begin{pmatrix}
0 & 0 & 0 & \frac{1}{\beta^2} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \frac{1}{\beta} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \frac{1}{\beta^2} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}.$$
The eigenvalues of this matrix are $1, \frac{1}{\beta}, \frac{\beta + 1}{\beta^3}, \frac{1 + \beta}{\beta^3}$. The stationary distribution vector (given by the left eigenvector to the eigenvalue 1) is $(\frac{1}{\beta}, \frac{1}{\beta^3}, \frac{1}{\beta^3}, \frac{1}{\beta^3})$, thus we have

$$E \beta z = \Pr[Y_j = 100] + \Pr[Y_j = \overline{100}] = 1/5 + O(\beta^{-\min(j,n-j)}),$$

cf. [8]. This proves the theorem for $M = G_n$.

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

$$\sum_{N = -M}^M \|N\|_F = \sum_{N = -G_n}^{G_n} \|N\|_F + \sum_{N = -G_{n-2}}^{M-F_n} (1 + \|N\|_F) + \sum_{N = F_n-M}^{G_{n-2}} (1 + \|N\|_F)$$

$$= \sum_{N = -G_n}^{G_n} \|N\|_F + \sum_{N = -G_{n-2}}^{M-F_n} \|N\|_F + \sum_{N = -G_{n-2}}^{G_{n-2}} \|N\|_F + O(M)$$

$$= \frac{2}{5} \log \beta (F_n \log M + (M - F_n) \log |M - F_n|) + O(M) = \frac{2M \log M}{5 \log \beta} + O(M)$$

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

**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 $[\frac{-\beta^2}{\beta^3 + 1}, \frac{\beta^2}{\beta^3 + 1}]$, where the transformation $\tau : z \mapsto \beta z - [\frac{\beta^2 + 1}{\beta^3 + 1} z + 1/2]$ of the proof of Proposition 4.3 is defined, into intervals

$I_{100} = [\frac{-\beta}{\beta^3 + 1}, \frac{-\beta^2}{\beta^3 + 1}], I_{010} = [\frac{-\beta}{\beta^3 + 1}, \frac{-\beta}{\beta^3 + 1}], I_{101} = [\frac{-\beta}{\beta^3 + 1}, \frac{-1/\beta}{\beta^3 + 1}], I_{001} = [\frac{-1/\beta}{\beta^3 + 1}, \frac{1/\beta}{\beta^3 + 1}], I_{011} = [\frac{1/\beta}{\beta^3 + 1}, \frac{1}{\beta^3 + 1}], I_{110} = [\frac{1}{\beta^3 + 1}, \frac{1/\beta}{\beta^3 + 1}], I_{111} = [\frac{1}{\beta^3 + 1}, \frac{1}{\beta^3 + 1}],$ then we have $p_{a,v} = \lambda(\tau(I_a) \cap I_v)/\lambda(\tau(I_v))$, where $\lambda$ 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 $1 = .111$, we have $2 = 10.001$ and $\beta$ satisfies (D2). Here, the digits of arbitrary $\beta$-expansions of minimal weight are in $\{-5, \ldots, 5\}$ since $6 = 1000.0010101$. We have $5 = 101.100011$ and we will show that $101100011$ is a $\beta$-expansion of minimal weight, thus 5 is also a $\beta$-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 $\beta$-expansions of minimal weight

All words which are not accepted by the automaton $M_\beta$ in Figure 7, where all states are terminal, are $\beta$-heavy since they contain a factor which is accepted by the input automaton of the transducer in Figure 8 (without the dashed arrows).
Proposition 5.1. If $\beta > 1$ is the Tribonacci number, then every $z \in \mathbb{R}$ has a $\beta$-expansion of the form $z = y_1 \cdots y_k y_{k+1} y_{k+2} \cdots$ 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

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

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

Remark 5.2. The transformation $\tau(z) = \beta z - \left[\frac{\beta - 1}{2} z + \frac{1}{2}\right]$ on $\left(\frac{-\beta}{\beta + 1}, \frac{\beta}{\beta + 1}\right)$ provides a unique expansion avoiding the factors 11, 11, 101 and their opposites.

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

Theorem 5.4. If $\beta$ is the Tribonacci number, then the set of $\beta$-expansions of minimal weight in $\{-1, 0, 1\}^*$ is recognized by the finite automaton $M_\beta$ of Figure 7 where all states are terminal.

5.2 Branching transformation

Contrary to the Golden Ratio case, we cannot obtain all $\beta$-expansions of minimal weight by the help of a piecewise linear branching transformation: If $z = .01(001)^n$, then we have no $\beta$-expansion of minimal weight of the form $z = .1 \bar{x}_2 \bar{x}_3 \cdots$, whereas $z' = .0011$ has the expansion $.1 \bar{1}$, and $z' < z$. On the other hand, $z = .1(100)^n 11$ has no $\beta$-expansion of minimal weight of the form $z = .1 \bar{x}_2 \bar{x}_3 \cdots$ (since $1(100)^n 11$ is $\beta$-heavy but $(100)^n 11$ is not $\beta$-heavy), whereas $z' = .1101$ is a $\beta$-expansion of minimal
weight, and \( z' > z \). Hence the maximal interval for the digit 1 is \([-((010)^\omega), 1((100)^\omega)]\), with \(-((010)^\omega) = \frac{\beta}{\beta^3 - 1}\) and \(1((100)^\omega) = \frac{2\beta + 1}{\beta(\beta + 1)}\). 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 \( 20^\omega \sim_T 100010^{n-3} \) 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 \( 1(010)^{n/3} \) and \( (100)^{n/3} \) is \( 1(110)^{n/3} \sim_{T} 1 \), 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 \( X = \{11, 101, 11\}, \) and their opposites.

If \( z = a_1 \cdots a_n = m_2 m_1 m_0 \), 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., \( z = -2m_2/\beta^2 + m'_0/\beta^3 \), hence all states \( s = m/\beta^2 + m'/\beta^3 \) with some \( m, m' \in \mathbb{Z} \) are terminal states in the redundancy transducer \( R_T \). The transducer \( S_T \), 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 \( \beta \)-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 \( M_\beta \) 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 \( Q'_u \), \( u \in \{11, 110, 111, 110, 1101\} \), contain states \( (\pm 1/\beta^3, -1; w) \),

---

**Figure 9.** Normalizing transducer \( N_\beta \), \( \beta^3 = \beta^2 + \beta + 1 \).
The eigenvalues of this matrix are 1, ±1/β, −1, and their opposites. Then the sequence of random variables 
\( \{W_n\}_{n \geq 0} \) is Markov with transition probabilities 
\( \Pr[Y_{j+1} = v \mid Y_j = u] = p_{u,v} + O(\beta^{-n+1}) \),

\[
(p_{u,v})_{u,v \in \{0, 1, 01, 10, 00, 01, 11\}} =
\begin{pmatrix}
0 & 0 & \frac{\beta - 1}{\beta^2} & \frac{1}{\beta^2} & 0 \\
1 & 0 & 0 & 0 & 0 \\
0 & \frac{\beta - 1}{\beta^2} & \frac{1}{\beta^2} & 0 & 0 \\
0 & 0 & 0 & 0 & 1 \\
0 & \frac{1}{\beta^2} & \frac{\beta - 1}{\beta^2} & 0 & 0
\end{pmatrix}.
\]

The eigenvalues of this matrix are 
\( 1, \pm \frac{1}{\beta}, \pm \frac{1}{\sqrt{\frac{\beta - 1}{\beta^2} + \beta^2}}, \pm \frac{1}{\sqrt{\frac{\beta - 1}{\beta^2} + \beta^2}} \),

and the stationary distribution vector of the Markov chain is 
\( \left( \frac{\beta + 2}{\beta + 1}, \frac{\beta + 3}{\beta + 1}, \frac{\beta + 2}{\beta + 1}, \frac{\beta + 3}{\beta + 1}, \frac{\beta + 2}{\beta + 1} \right). \) We obtain the following theorem (with \( \frac{\beta^2}{\beta + 1} = (0011010100)^\omega \approx 0.28219 \)).

**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, 11, and their opposites. Then the sequence of random variables 
\( \{Y_j\}_{1 \leq j \leq n} \) defined by

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

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

\[
(p_{u,v})_{u,v \in \{0, 1, 01, 10, 00, 01, 11\}} =
\begin{pmatrix}
0 & 0 & \frac{\beta^2 - 1}{\beta^2} & \frac{1}{\beta^2} & 0 \\
1 & 0 & 0 & 0 & 0 \\
0 & \frac{\beta^2 - 1}{\beta^2} & \frac{1}{\beta^2} & 0 & 0 \\
0 & 0 & 0 & 0 & 1 \\
0 & \frac{1}{\beta^2} & \frac{\beta^2 - 1}{\beta^2} & 0 & 0
\end{pmatrix}.
\]

The eigenvalues of this matrix are 
\( 1, \pm \frac{1}{\beta}, \pm \frac{1}{\sqrt{\frac{\beta^2 - 1}{\beta^2} + \beta^2}}, \pm \frac{1}{\sqrt{\frac{\beta^2 - 1}{\beta^2} + \beta^2}} \),

and the stationary distribution vector of the Markov chain is 
\( \left( \frac{\beta + 2}{\beta + 1}, \frac{\beta + 3}{\beta + 1}, \frac{\beta + 2}{\beta + 1}, \frac{\beta + 3}{\beta + 1}, \frac{\beta + 2}{\beta + 1} \right). \) We obtain the following theorem (with \( \frac{\beta^2}{\beta + 1} = (0011010100)^\omega \approx 0.28219 \)).
Theorem 5.7. For positive integers \( M \), we have, as \( M \to \infty \),

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

6 Smallest Pisot number case

The smallest Pisot number \( \beta \approx 1.325 \) satisfies \( \beta^3 = \beta + 1 \). Since 1 = .011 = .10001 implies 2 = 100.00001 as well as 2 = 1000.0001, \((D_2)\) holds. We have furthermore \( 3 = \beta^4 - \beta^{-9} \), thus all \( \beta \)-expansions of minimal weight have digits in \( \{-2, \ldots, 2\} \).

6.1 \( \beta \)-expansions of minimal weight

![Diagram](image)

**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 \( \beta \)-heavy, not only because the automata are larger but also because some inputs of the transducer in Figure 13 are not strictly \( \beta \)-heavy (but of course still \( \beta \)-heavy). We refer to [13] for details.

Proposition 6.1. If \( \beta \) is the smallest Pisot number, then every \( z \in \mathbb{R} \) has a \( \beta \)-expansion of the form \( z = y_1 \cdots y_k y_{k+1} y_{k+2} \cdots \) with \( y_j \in \{-1, 0, 1\} \) such that \( y_1 y_2 \cdots \) avoids the
set $X = \{10^k 1, 10^k \bar{1}, 0 \leq k \leq 5, \text{ and their opposites}\}$. 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

$$\tau : \left[\frac{-\beta^3}{\beta^2 + 1}, \frac{\beta^3}{\beta^2 + 1}\right) \rightarrow \left[\frac{-\beta^3}{\beta^2 + 1}, \frac{\beta^3}{\beta^2 + 1}\right), \quad \tau(x) = \beta x - \left[\frac{\beta^2 + 1}{2\beta^2} x + \frac{1}{2}\right]$$

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

**Remark 6.2.** The transformation $\tau(z) = \beta z - \lfloor \frac{1}{2} z + \frac{1}{2} \rfloor$ on $[-\frac{\beta^2}{2}, \frac{\beta^3}{2}]$ 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 $X = \{10^k 1, 10^k \bar{1}, 0 \leq k \leq 5, \text{ and their opposites}\}$ is realized by the transducer $N_\beta$ in Figure 14 and does not change the weight.

**Theorem 6.4.** If $\beta$ is the smallest Pisot number, then the set of $\beta$-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 $\beta$, the maximal interval for the digit 1 is $[.010^6)^\omega, .1(0^5 10^2)^\omega$, with $.1(0^5 10^2)^\omega = \frac{\beta^2}{\beta^2 + 1}$ and $.1(0^5 10^2)^\omega = \frac{\beta^2 + 1/\beta}{\beta^2 + 1}$. The corresponding branching transformation and expansions are given in Figure 15.
6.3 Integer expansions

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

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

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

For every \(x \in \mathbb{Z}^*\), there exists \(y \in \{-1, 0, 1\}^*\) with \(x \sim_S y, \|y\| \leq \|x\|\), since \(2 \sim_S 10, 20 \sim_S 1000, 200 \sim_S 1010, 20^3 \sim_S 10100, 20^4 \sim_S 1010^4, 20^n \sim_S 10^n 10^{n-5}\) 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 \(X = \{10^k1, 10^k0, 10^k1, 0 \leq k \leq 5, \text{and their opposites}\}\), with the exception that \(10^41, 10^51, 10^50, 10^51\) 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.

<table>
<thead>
<tr>
<th>( n \equiv j \mod 8 )</th>
<th>( g_{n+1} )</th>
<th>( G_n )</th>
<th>( g_{n+1} - G_n )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2, 3, 4</td>
<td>( 1(0^610)^{n/8} )</td>
<td>( (10^7)^{n/8} )</td>
<td>( 110^{n-1} \sim S 1 )</td>
</tr>
<tr>
<td>5</td>
<td>( 1(0^610)^{(n-5)/8}11 )</td>
<td>( (10^7)^{(n-5)/8}10^4 )</td>
<td>( 1100011 \sim S 1 )</td>
</tr>
<tr>
<td>6</td>
<td>( 1(0^610)^{(n-6)/8}011 )</td>
<td>( (10^7)^{(n-6)/8}10^5 )</td>
<td>( 11000011 \sim S 1 )</td>
</tr>
<tr>
<td>7</td>
<td>( 1(0^610)^{(n-7)/8}0011 )</td>
<td>( (10^7)^{(n-7)/8}10^6 )</td>
<td>( 11000002 \sim S 1 )</td>
</tr>
<tr>
<td>0</td>
<td>( 1(0^610)^{n/8} )</td>
<td>( (10^7)^{n/8-1}10^9 )</td>
<td>( 1100000011 \sim S 1 )</td>
</tr>
</tbody>
</table>

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 \( z = a_1 \cdots a_n \), 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 \( z \in \{0, \pm 1/\beta^4\} \).
\[ (\frac{-\beta + \beta^2}{\beta^2 + 1} : \frac{-1}{\beta^2}) \]

\[ \text{Figure 15. Branching transformation and corresponding automaton, } \beta^3 = \beta + 1. \]

- If \( a_n = 1 \), then \( N = 0 \) if and only if \( m_2 = 2m'_2 - 1, m_1 = -2m_3 - 3m'_2 + 1, \)
  \[ z = m_3(\beta^3 - 2\beta) + m'_2(2\beta^2 - 3\beta) - \beta^2 + \beta + 1 = -m_3/\beta^4 - m'_2(1/\beta^2 + 1/\beta^3) + 1/\beta^2. \]
  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 \( R_\beta \) 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 \( M_S \), 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 \( (Y_j)_{1 \leq j \leq n} \) defined by

\[
\Pr[Y_1 = y_1 \cdots y_7, \ldots, Y_j = y_j \cdots y_{j+6}] = \frac{\#\{x_1 \cdots x_{n+6} \in W_n : x_1 \cdots x_{j+6} = y_1 \cdots y_{j+6}\}}{\#W_n}
\]
is Markov with transition probabilities $\Pr[Y_{j+1} = v \mid Y_j = u] = p_{u,v} + \mathcal{O}(\beta^{-n+j})$.

$$(p_{u,v})_{u,v \in \{0^6, \ldots , 0^3, 0^2, \ldots , 1^6\}} =$$

$$
\begin{pmatrix}
0 & \cdots & \cdots & 0 & \frac{1}{\beta^3} & \frac{1}{\beta^3} & 0 & \cdots & 0 \\
1 & \cdots & \cdots & \cdots & 0 & 0 & \cdots & \cdots & \cdots \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
\vdots & \cdots & 1 & 0 & 0 & 0 & \cdots & \cdots & \cdots \\
\vdots & \cdots & 0 & \frac{1}{\beta^3} & \frac{1}{\beta^3} & 0 & \cdots & \cdots & \cdots \\
\vdots & \cdots & 0 & 0 & 0 & 1 & \cdots & \cdots & \cdots \\
\vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \ddots & \ddots & \cdots \\
\vdots & \cdots & \cdots & \cdots & \cdots & \ddots & \ddots & \ddots & \ddots \\
0 & \cdots & 0 & \frac{1}{\beta^3} & \frac{1}{\beta^3} & 0 & \cdots & \cdots & \cdots \\
\end{pmatrix}
$$

The left eigenvector to the eigenvalue 1 of this matrix is

$$
\frac{1}{1+2\beta^2}(1, \ldots , 1, 4\beta^2, 1, \ldots , 1),
$$

and we obtain the following theorem (with $\frac{1}{1+2\beta^2} \approx 0.09515$).

**Theorem 6.7.** For positive integers $M$, we have, as $M \to \infty$,

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

### 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 $2 = 100.00001$. A question which is not approached in this paper concerns $\beta$-expansions of minimal weight in $\{1 - B, \ldots , B - 1\}^*$ when $\beta$ does not satisfy (D$_2$), 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 $\beta$, with digits in $A = \{0, 1\}$ or in $A = \{-1, 0, 1\}$.

<table>
<thead>
<tr>
<th>$U_n$</th>
<th>$A$</th>
<th>$\beta$</th>
<th>average $|N|_I$ for $N \in {-M, \ldots , M}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^n$</td>
<td>${0, 1}$</td>
<td>2</td>
<td>$(\log_2 M)/2$</td>
</tr>
<tr>
<td>$2^n$</td>
<td>${-1, 0, 1}$</td>
<td>2</td>
<td>$(\log_2 M)/3$</td>
</tr>
<tr>
<td>$F_n$</td>
<td>${0, 1}$</td>
<td>$1+\sqrt{5}$</td>
<td>$(\log_3 M)/(\beta^2 + 1) \approx 0.398 \log_2 M$</td>
</tr>
<tr>
<td>$F_n$</td>
<td>${-1, 0, 1}$</td>
<td>$1-\sqrt{5}$</td>
<td>$(\log_3 M)/(\beta^2 + 1) \approx 0.288 \log_2 M$</td>
</tr>
<tr>
<td>$T_n$</td>
<td>${-1, 0, 1}$</td>
<td>$\beta^3 = \beta^2 + \beta + 1$</td>
<td>$(\log_3 M)/(\beta^2 + 1) \approx 0.321 \log_2 M$</td>
</tr>
<tr>
<td>$S_n$</td>
<td>${-1, 0, 1}$</td>
<td>$\beta^3 = \beta + 1$</td>
<td>$(\log_3 M)/(7 + 2\beta^2) \approx 0.235 \log_2 M$</td>
</tr>
</tbody>
</table>
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 $U_j P$, $0 \leq j \leq n$, by using the recurrence of $U$ and finally $N P = \sum_{j=0}^{n} x_j (U_j P)$. 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 $0 \leq j \leq n \approx \log_{\beta} M$ 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


**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