REDUNDANCY OF MINIMAL WEIGHT EXPANSIONS IN PISOT BASES

PETER J. GRABNER† AND WOLFGANG STEINER

ABSTRACT. Motivated by multiplication algorithms based on redundant number representations, we study representations of an integer n as a sum $n = \sum_k \varepsilon_k U_k$, where the digits ε_k are taken from a finite alphabet Σ and $(U_k)_k$ is a linear recurrent sequence of Pisot type with $U_0 = 1$. The most prominent example of a base sequence $(U_k)_k$ is the sequence of Fibonacci numbers. We prove that the representations of minimal weight $\sum_k |\varepsilon_k|$ are recognised by a finite automaton and obtain an asymptotic formula for the average number of representations of minimal weight. Furthermore, we relate the maximal order of magnitude of the number of representations of a given integer to the joint spectral radius of a certain set of matrices.

1. INTRODUCTION

Forming large multiples of elements of a given group plays an important role in public key cryptosystems based on the Diffie-Hellman scheme (cf. for instance [CFA+06], especially [Doc06]). In practice, the underlying groups are often chosen to be the multiplicative group of a finite field $\mathbb{F}_q$ or the group law of an elliptic curve (elliptic curve cryptosystems).

For P an element of a given group (written additively), we need to form nP for large $n \in \mathbb{N}$ in a short amount of time. One way to do this is the *binary method* (cf. [vzGG99]), which is simply an applications of Horner's scheme to the binary expansion of n. This method uses the operations of "doubling" and "adding P". If we write n in its binary representation, the number of doublings is fixed by $\lfloor \log_2 n \rfloor$ and each *one* in this representation corresponds to an addition. Thus the cost of the multiplication depends on the length of the binary representation of n and the number of ones in this representation.

In the case of the point group of an elliptic curve, addition and subtraction are given by very similar expressions and are therefore equally costly. Thus it makes sense to work with *signed binary representations*, i.e., binary representations with digits $\{0, \pm 1\}$. The advantage of these representations is their redundancy: in general, n has many different signed binary representations. Then the number of non-zero digits in a signed binary representation of n is called the *Hamming weight* of this representation. Since each non-zero digit causes a group addition (1 causes addition of P, -1 causes subtraction of P),

Date: February 22, 2011.

2000 *Mathematics Subject Classification.* Primary: 11A63, Secondary: 68Q45, 11K16, 11K55.

Key words and phrases. redundant systems of numeration, linear recurrent base sequence, Fibonacci numbers, Pisot numbers, representation of minimal weight, fast multiplication.

†This author is supported by the Austrian Science Foundation FWF, project S9605, part of the Austrian National Research Network "Analytic Combinatorics and Probabilistic Number Theory".

one is interested in finding a representation of n having minimal Hamming weight. Such a minimal representation was exhibited by Reitwiesner [Rei60]. The number of binary representations of minimal weight has been analysed in [GH06].

In the present paper we propose to use Fibonacci-multiples instead of powers of 2. The advantage of this choice is to avoid successive duplication (most of the time), which uses a different formula in the case of the group law of an elliptic curve. A further advantage of these representations is the smaller average weight compared to the binary representation (cf. [FS08]). More generally, we study representations with linear recurrent base sequences of Pisot type. We calculate the number of representations of minimal weight with respect to these numeration systems and obtain an asymptotic formula for the average number of representations in the range $[-N, N]$.

A main tool of our study will be automata, which recognise the various representations. As a general reference for automata in the context of number representation we refer to [Fro02, FS10]. The books [LM95, Sak09] provide the basic notions of symbolic dynamics and automata theory.

2. U-expansions and β-expansions of minimal weight

2.1. **Setting.** Let $U = (U_k)_{k\ge 0}$ be a strictly increasing sequence of integers with $U_0 = 1$, and $z = z_k z_{k-1} \cdots z_0$ a finite word on an alphabet $\Sigma \subseteq \mathbb{Z}$. We say that z is a *U-expansion* of the number $\sum_{j=0}^k z_j U_j$. The *greedy U-expansions* of positive integers n, which are defined by

$$n = \sum_{j=0}^{k} z_j U_j \quad \text{with} \quad \sum_{j=0}^{\ell} z_j U_j < U_{\ell+1} \quad \text{for } \ell = 0, 1, \ldots, k,\ z_k \neq 0,$$

are well studied, in particular for the case when U is the Fibonacci sequence $F = (F_k)_{k\ge 0}$ with $F_0 = 1$, $F_1 = 1$, $F_k = F_{k-1} + F_{k-2}$ for $k \ge 2$, see e.g. [Fro02]. The sum-of-digits function of greedy U-expansions with U satisfying suitable linear recurrences has been studied by [PT89] and in several subsequent papers.

In the present paper we are interested in words with the smallest weight among all U-expansions of the same number. Here the *weight* of z is the absolute sum of digits $\|z\| = \sum_{j=0}^k |z_j|$. This weight is equal to the Hamming weight when $z \subseteq \{-1, 0, 1\}^*$, where Σ^* denotes the set of finite words with letters in the alphabet Σ.

We define the relation $\sim_U$ on words in $\mathbb{Z}^*$ by $z \sim_U y$ when z and y are U-expansions of the same number, i.e.,

$$z_k z_{k-1} \cdots z_0 \sim_U y_\ell y_{\ell-1} \cdots y_0 \quad \text{if and only if} \quad \sum_{j=0}^{k} z_j U_j = \sum_{j=0}^{\ell} y_j U_j.$$

Then the set of *U-expansions of minimal weight* is

$$L_U = \{z \in \mathbb{Z}^* :\ \|z\| \le \|y\| \text{ for all } y \in \mathbb{Z}^* \text{ with } z \sim_U y\}.$$

Of course, leading zeros do not change the value and weight of a U-expansion. In particular, every element of 0^*z is in L_U if $z \in L_U$.

Throughout the paper, we assume that there exists a *Pisot number* β, i.e., an algebraic integer $\beta > 1$ with $|\beta_i| < 1$ for every Galois conjugate $\beta_i \neq \beta$, such that U satisfies (eventually) a linear recurrence with characteristic polynomial equal to the minimal polynomial of β. Then there exists some constant $c > 0$ such that

$$U_k = c\,\beta^k + \mathcal{O}(|\beta_2|^k), \tag{2.1}$$

where β_2 is the second largest conjugate of β in modulus.

2.2. **Regularity of L_U.** For three particular sequences U (the Fibonacci sequence, the Tribonacci sequence and a sequence related to the smallest Pisot number), the set $L_U \cap \{-1, 0, 1\}^*$ is given explicitely in [FS08] by means of a finite automaton, see Figure 1 for the Fibonacci sequence. Recall that an *automaton* $\mathcal{A} = (Q, \Sigma, E, I, T)$ is a directed graph, where Q is the set of vertices, traditionally called states, $I \subseteq Q$ is the set of initial states, $T \subseteq Q$ is the set of terminal states and $E \subseteq Q \times \Sigma \times Q$ is the set of edges (or transitions) which are labelled by elements of Σ. If $(p, a, q) \in E$, then we write $p \xrightarrow{a} q$. A word in Σ^* is *accepted by* $\mathcal{A}$ if it is the label of a path starting in an initial state and ending in a terminal state. The set of words which are accepted by $\mathcal{A}$ is said to be *recognised by* $\mathcal{A}$. A *regular language* is a set of words which is recognised by a finite automaton. The main result of this subsection is the following theorem.

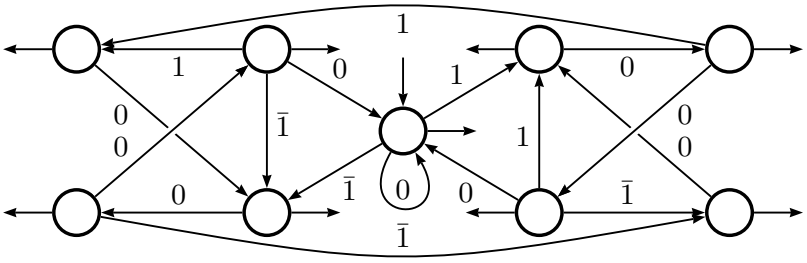

FIGURE 1. Automaton recognising the set of F-expansions of minimal weight in $\{-1, 0, 1\}^*$.

Theorem 2.1. *Let $U = (U_k)_{k\geq 0}$ be a strictly increasing sequence of integers with $U_0 = 1$, satisfying eventually a linear recurrence with characteristic polynomial equal to the minimal polynomial of a Pisot number. Then the set of U-expansions of minimal weight is recognised by a finite automaton.*

First note that the structure of L_U is similar to the structure of the β-expansions of minimal weight. Here, $z = z_k z_{k-1} \cdots z_0 \in \mathbb{Z}^*$ is a *β-expansion* of the number $\sum_{j=0}^{k} z_j \beta^j$. Similarly to $\sim_U$, we define the relation $\sim_\beta$ on $\mathbb{Z}^*$ by

$$z_k z_{k-1} \cdots z_0 \sim_\beta y_\ell y_{\ell-1} \cdots y_m \quad \text{if} \quad \sum_{j=0}^{k} z_j \beta^j = \sum_{j=m}^{\ell} y_j \beta^j. \tag{2.2}$$

A difference with $\sim_U$ is that m can be chosen freely in $\mathbb{Z}$; we have $z \sim_\beta y$ if (2.2) holds for some $m \in \mathbb{Z}$. The set of *β-expansions of minimal weight* is

$$L_\beta = \{z \in \mathbb{Z}^* : \ \|z\| \le \|y\| \text{ for all } y \in \mathbb{Z}^* \text{ with } z \sim_\beta y\}.$$

(These definitions are equivalent to the ones in [FS08].) Now, leading and trailing zeros do not change the minimal weight property, i.e., $0^* L_\beta\, 0^* = L_\beta$. Theorem 3.11 in [FS08] states that one can construct a finite automaton recognising L_β. The proof of the corresponding result for L_U is slightly more complicated. We start with the following proposition, which resembles Proposition 3.5 in [FS08].

Proposition 2.2. *Let U be as in Theorem 2.1. Then there exists a positive integer B such that*

$$\forall\, k \ge 0,\ \exists\, b^{(k)} \in \mathbb{Z}^* :\ B\, 0^k \sim_U b^{(k)},\ \|b^{(k)}\| < B. \tag{2.3}$$

Proof. Let U be a strictly increasing sequence of integers with $U_0 = 1$, β a Pisot number of degree d, and $h \ge 0$ an integer such that, for all $k \ge h + d$, U_k is given by the linear recurrence with respect to the minimal polynomial of β. By [FS08, Proposition 3.5], we know that for sufficiently large B there exists some $b = b_\ell \cdots b_m \in \mathbb{Z}^*$ such that $B = \sum_{j=m}^{\ell} b_j \beta^j$ and $\|b\| < B$. Then we have $B\, 0^k \sim_U b_\ell \cdots b_m\, 0^{k+m}$ for all $k \ge h - m$. For $0 \le k < h - m$, the weight of the greedy U-expansion of the integer $B\, U_k$ grows with $\mathcal{O}(\log B)$. Therefore, there exists some positive integer B satisfying (2.3). □

Proposition 2.3. *Let U be as in Theorem 2.1. If B is a positive integer satisfying* (2.3)*, then $L_U \subseteq \{1 - B, \dots, B - 1\}^*$. If B is a positive integer satisfying*

$$\forall\, k \ge 0,\ \exists\, b^{(k)} \in \mathbb{Z}^* :\ B\, 0^k \sim_U b^{(k)},\ \|b^{(k)}\| \le B, \tag{2.4}$$

then there exists for every $n \in \mathbb{Z}$ some $z \in L_U \cap \{1 - B, \dots, B - 1\}^*$ with $z \sim_U n$.

Proof. This can be proved similarly to Proposition 3.1 in [FS08]. □

For $U = F$, (2.4) holds with $B = 2$ since $2 \sim_F 10$, $20 \sim_F 4 \sim_F 101$ and $2\, 0^k \sim_F 1001\, 0^{k-2}$ for $k \ge 2$. Therefore, we are mainly interested in the language $L_F \cap \{-1, 0, 1\}^*$, which is recognised by the automaton in Figure 1 [FS08, Theorem 4.7]. The minimal positive integer satisfying (2.3) is $B = 3$. Here, we have $3 \sim_F 100$, $30 \sim_F 6 \sim_F 1001$ and $3\, 0^k \sim_F 10001\, 0^{k-2}$ for $k \ge 2$, whereas 20 is clearly a F-expansion of minimal weight.

Next we show the following generalisation of a well known result for β-expansions [Fro92, Corollary 3.4]. For a subclass of sequences U, this result can be found in [Fro89, Fro92].

Proposition 2.4. *Let U be as in Theorem 2.1. Then, for every finite alphabet $\Sigma \subset \mathbb{Z}$,*

$$Z_{U,\Sigma} = \{z \in \Sigma^* :\ z \sim_U 0\}$$

is recognised by a finite automaton.

Proof. Let U be as in the proof of Proposition 2.2. Let $\beta = \beta_1, \beta_2, \dots, \beta_d$ be the conjugates of β. Then there exist constants $c_i \in \mathbb{Q}(\beta_i)$ such that

$$U_{h+k} = \sum_{i=1}^{d} c_i \beta_i^k \quad \text{for all} \quad k \ge 0. \tag{2.5}$$

For any word $z_k \cdots z_0 \in \Sigma^*$ we can write

$$\sum_{j=0}^{k-h} z_{h+j}\beta^j = \sum_{j=0}^{d-1} m_j\beta^j \quad \text{with} \quad m_{d-1}\cdots m_0 \in \mathbb{Z}^d. \tag{2.6}$$

We have $z_k \cdots z_0 \sim_U m_{d-1}\cdots m_0\, z_{h-1}\cdots z_0$ (with $z_j = 0$ for $k \le j < h$), thus

$$z_k \cdots z_0 \sim_U 0 \quad \text{if and only if} \quad \sum_{j=0}^{d-1} m_j U_{h+j} + \sum_{j=0}^{h-1} z_j U_j = 0. \tag{2.7}$$

By (2.6), we obtain

$$\left| \sum_{j=0}^{d-1} m_j \beta_i^j \right| \le \frac{\max_{a\in\Sigma} |a|}{1 - |\beta_i|} \quad \text{for} \quad i = 1, 2, \ldots, d-1. \tag{2.8}$$

By (2.7), (2.5) and (2.8), we obtain that $|\sum_{j=0}^{d-1} m_j\beta^j|$ is bounded as well if $z_k \cdots z_0 \sim_U 0$. There are only finitely many words $m_{d-1}\cdots m_0 \in \mathbb{Z}^d$ such that all conjugates of $\sum_{j=0}^{d-1} m_j\beta^j$ are bounded. Therefore, there are only finitely many possibilities for $m_{d-1}\cdots m_0 \in \mathbb{Z}^d$, $z_{h-1}\cdots z_0 \in \Sigma^*$ such that $m_{d-1}\cdots m_0\, z_{h-1}\cdots z_0 \sim_U 0$. Set

$$T_U(z_{h-1}\cdots z_0) = \left\{ \sum_{j=0}^{d-1} m_j\beta_{h+j} + \sum_{j=0}^{h-1} z_j\beta_j \;\middle|\; m_{d-1}\cdots m_0\, z_{h-1}\cdots z_0 \sim_U 0 \right\}$$

and $M = \max \bigcup_{z'\in\Sigma^h} T_U(z')$.

Let $\mathcal{A}_{U,\Sigma}$ be the automaton with initial state $(0, 0^h)$ and transitions $(s, z_{h-1}\cdots z_0) \xrightarrow{a} (\beta s - a, z_{h-2}\cdots z_0 a)$, $a \in \Sigma$, such that $|\beta s - a| < M + \max_{b\in\Sigma}|b|/(\beta - 1)$. A state $(s, z') \in \mathbb{Z}[\beta] \times \Sigma^h$ is terminal if and only if $s \in T_U(z')$. Then $\mathcal{A}_{U,\Sigma}$ is finite and recognises $Z_{U,\Sigma}$. □

Now, we can prove Theorem 2.1. As in [FS08], we make use of *letter-to-letter transducers*, which are automata with transitions labelled by pairs of digits. If $(z_k, y_k)\cdots(z_0, y_0)$ is the sequence of labels of a path from an initial to a terminal state, we say that the transducer accepts the pair of words (z, y), with $z = z_k \cdots z_0$ being the input and $y = y_k \cdots y_0$ being the output of the transducer.

Proof of Theorem 2.1. By Propositions 2.2 and 2.3, there exists a positive integer B such that $L_U \subseteq \Sigma^*$ with $\Sigma = \{1 - B, \ldots, B - 1\}$.

In the proof of Theorem 3.10 in [FS08], it was shown that there exists a finite letter-to-letter transducer $\mathcal{T}$ with the following property: For every word $z \in (\Sigma L_\beta \cap L_\beta\Sigma) \setminus L_\beta$, i.e., $z \in \Sigma^* \setminus L_\beta$ and every proper factor of z is in L_β, there exist integers ℓ, m and a word $y \in \Sigma^*$ such that $(0^\ell z\, 0^m, y)$ is the label of a path in $\mathcal{T}$ leading from $(0, 0)$ to $(0, \delta)$, with $\delta < 0$. The transitions are of the form $(s, \delta) \xrightarrow{(a,b)} (\beta s + b - a, \delta + |b| - |a|)$, $a, b \in \Sigma$. This means that $y \sim_\beta z$ and $\|y\| < \|z\|$. Since $\mathcal{T}$ is finite, we can choose $m \le K$ for some constant K. By the assumptions on U, we obtain that $z\, 0^k \sim_U y\, 0^{k-m}$ for all $k \ge h + K$, thus $z\, 0^k \notin L_U$. Note that $z\, 0^k \notin L_U$ implies that $z' z\, z'' \notin L_U$ for all $z' \in \Sigma^*$, $z'' \in \Sigma^k$. Now,

since $\Sigma^* \setminus L_\beta$ is recognised by a finite automaton, we also have an automaton recognising the set of words $z = z_k \cdots z_0 \in \Sigma^* \setminus L_U$ with $z_k \cdots z_{h+K} \notin L_\beta$.

It remains to consider the words $z = z_k \cdots z_0 \in \Sigma^* \setminus L_U$ with $z_k \cdots z_{h+K} \in L_\beta$ (if $k \ge h + K$). Let $y = y_\ell \cdots y_0 \sim_U z$ with $y \in L_U$, and assume w.l.o.g. $\ell \ge k$. All these pairs of words $(0^{\ell-k}z, y)$ are accepted by a letter-to-letter transducer $\mathcal{T}'$ with $(0, 0^h, 0^h, 0)$ as initial state, transitions

$$(s,\, z_{h-1} \cdots z_0,\, y_{h-1} \cdots y_0,\, \delta) \xrightarrow{(a,b)} (\beta s + b - a,\, z_{h-2} \cdots z_0 a,\, y_{h-2} \cdots y_0 b,\, \delta + |b| - |a|),$$

$a, b \in \Sigma$, and terminal states (s, z', y', δ) such that $s \in T_U(y') - T_U(z')$, $\delta < 0$. We show that $\mathcal{T}'$ is a finite transducer. As in the proof of Proposition 2.4, we obtain states (s, z', y', δ) with s in a finite subset of $\mathbb{Z}[\beta]$, more precisely $|s| < 2M + 2(B-1)/(\beta-1)$ and the conjugate of s corresponding to β_i is bounded by $2(B-1)/(1-|\beta_i|)$ for $2 \le i \le d$. Clearly, there are only finitely many possibilities for $z', y' \in \Sigma^h$. By the previous paragraph, $y \in L_U$ implies $y_\ell \cdots y_{h+K} \in L_\beta$. As in the proof of Theorem 3.10 in [FS08], for $m \ge h + K$, a large difference $\delta = \|y_k \cdots y_m\| - \|z_k \cdots z_m\|$ contradicts the assumption that $z_k \cdots z_m \in L_\beta$ and $y_k \cdots y_m \in L_\beta$. Since $h + K$ and Σ are finite, the difference between $\|z_k \cdots z_m\|$ and $\|y_k \cdots y_m\|$ is bounded for $0 \le m < h + K$ as well, thus $\mathcal{T}'$ is finite.

If we modify $\mathcal{T}'$ by adding those states to the set of initial states which can be reached from $(0, 0^h, 0^h, 0)$ by a path with input consisting only of zeros, then the input automaton of the modified transducer recognises a subset of $\Sigma^* \setminus L_U$ containing all words $z_k \cdots z_0 \in \Sigma^* \setminus L_U$ with $z_k \cdots z_{h+K} \in L_\beta$. Therefore, $\Sigma^* \setminus L_U$ is regular as the union of two regular languages, and the complement L_U is regular as well. □

2.3. **Properties of the automata.** The *trim minimal automaton* recognising a set H is the deterministic automaton with minimal number of states recognising H, where *deterministic* means that there is a unique initial state and from every state there is at most one transition labelled by a for every $a \in \Sigma$. Let $\mathcal{M}_{U,\Sigma}$ and $\mathcal{M}_{\beta,\Sigma}$ be the trim minimal automata recognising $L_U \cap \Sigma^*$ and $L_\beta \cap \Sigma^*$ respectively; let $A_{U,\Sigma}$ and $A_{\beta,\Sigma}$ be the respective adjacency matrices. We will see that the automata $\mathcal{M}_{U,\Sigma}$ and $\mathcal{M}_{\beta,\Sigma}$ are closely related. We show first that the matrix $A_{\beta,\Sigma}$ is primitive, using the following lemma.

Lemma 2.5. *Let $\mathcal{T}$ be a finite letter-to-letter transducer with transitions of the form $(s, \delta) \xrightarrow{(a,b)} (\beta s + b - a, \delta + |b| - |a|)$, $\beta \ne 0$, $a, b \in \mathbb{Z}$. Then the number of consecutive zeros in the input of a path in $\mathcal{T}$ not running through a state of the form $(0, \delta)$ is bounded.*

Proof. Let $(0^k, y)$ be the label of a path starting from (s, δ) with $s \ne 0$. Then the path leads to a state $(s', \delta + \|y\|)$, thus $\|y\|$ is bounded by the finiteness of $\mathcal{T}$. If y starts with 0^j, then the path leads to $(\beta^j s, \delta)$, thus the finiteness of $\mathcal{T}$ implies that j is bounded. If the path avoids states (s, δ) with $s = 0$, then the boundedness of $\|y\|$ and the boundedness of consecutive zeros in y imply that k, which is the length of y, is bounded. □

Proposition 2.6. *Let β be a Pisot number and $0 \in \Sigma \subseteq \mathbb{Z}$. Then $A_{\beta,\Sigma}$ is primitive.*

Proof. We show that, from every state in $\mathcal{M}_{\beta,\Sigma}$, the path labelled by 0^k leads to the initial state if k is sufficiently large.

First note that $z \in L_\beta$ implies $z\,0^k \in L_\beta$ for all $k \geq 0$, thus there always exists a path labelled by 0^k. Suppose that this path does not lead to the initial state from some state. Then there exist words $z, z' \in L_\beta \cap \Sigma^*$ with $z\,0^k\,z' \notin L_\beta$. We can assume w.l.o.g. $z\,0^k\,z' \in (\Sigma L_\beta \cap L_\beta \Sigma) \setminus L_\beta$. As in the proof of Theorem 2.1, there exist integers ℓ, m and a word $y \in \Sigma^*$ such that $(0^\ell z\,0^m, y)$ is the label of a path in $\mathcal{T}$ leading from $(0,0)$ to $(0,\delta)$, with $\delta < 0$. If this path ran through a state $(0,\delta)$ while reading the input 0^k between z and z', then the corresponding prefix of y would be a word $y' \sim_\beta z$ and the corresponding suffix of y would be a word $y'' \sim_\beta z'$. Since $\|y'\| + \|y''\| = \|y\| < \|z\| + \|z'\|$, we had $\|y'\| < \|z\|$ or $\|y''\| < \|z'\|$, contradicting that $z, z' \in L_\beta$. Therefore, Lemma 2.5 yields that k is bounded.

Hence, for sufficiently large k, 0^k is a synchronizing word of $\mathcal{M}_{\beta,\Sigma}$ leading to the initial state. Since $\mathcal{M}_{\beta,\Sigma}$ was assumed to be a trim minimal automaton, this implies that $\mathcal{M}_{\beta,\Sigma}$ is strongly connected, thus $A_{\beta,\Sigma}$ is irreducible. Now, the primitivity of $A_{\beta,\Sigma}$ follows from the fact that there is a loop labelled by 0 in the initial state. □

Proposition 2.7. *Let U be as in Theorem 2.1 and $0 \in \Sigma \subseteq \mathbb{Z}$. Then the automaton $\mathcal{M}_{U,\Sigma}$ has a unique strongly connected component. Up to the set of terminal states, this component is equal to $\mathcal{M}_{\beta,\Sigma}$.*

Proof. We first show that every word $z \in L_\beta$ is the label of a path starting in the initial state of $\mathcal{M}_{U,\Sigma}$. Suppose that $z\,0^k \notin L_U$ for some large $k \geq 0$, then there exists an integer ℓ and a word $y \in \Sigma^*$ such that $(0^\ell z\,0^k, y)$ is accepted by the finite transducer $\mathcal{T}'$ in the proof of Theorem 2.1. As in Lemma 2.5, we obtain that the path must run through a state $(0, z', y', \delta)$ while reading 0^k, which implies that $y \sim_\beta z$. Moreover, we have $\delta < 0$, thus $\|y\| < \|z\|$, contradicting that $z \in L_\beta$. This shows that the directed graph $\mathcal{M}_{U,\Sigma}$ contains the directed graph $\mathcal{M}_{\beta,\Sigma}$.

Now, consider an arbitary word $z \in L_U$ such that the corresponding path ends in a strongly connected component of $\mathcal{M}_{U,\Sigma}$. This means that we have $z\,z' \in L_U$ for arbitarily long words z'. Since $z\,z' \in L_U$ implies $z\,0^k \in L_U$, where k is the length of z', we obtain that $z \in L_\beta$. Therefore, the strongly connected components of $\mathcal{M}_{U,\Sigma}$ are contained in $\mathcal{M}_{\beta,\Sigma}$. Since $\mathcal{M}_{\beta,\Sigma}$ has a unique strongly connected component by Proposition 2.6, the same holds for $\mathcal{M}_{U,\Sigma}$. □

In Section 3, we also use that the difference between the length of the longest U-expansion of minimal weight (without leading zeros) and e.g. the greedy U-expansion is bounded.

Lemma 2.8. *Let U be as in Theorem 2.1 and Σ a finite subset of $\mathbb{Z}$. Let $z = z_k \cdots z_0 \in \Sigma^*$ with $z_k \neq 0$, $y = y_\ell \cdots y_0 \in L_U$ with $y_\ell \neq 0$. There exists a constant $m \geq 0$ such that $z \sim_U y$ implies $\ell \leq k + m$.*

Proof. For $\ell < k$, the assertion is trivially true. If $\ell \geq k$, then $(0^{\ell-k}z, y)$ is accepted by a transducer similar to $\mathcal{T}'$ in the proof of Theorem 2.1, with states (s, z', y', δ) such that s is in a finite set. Now δ can be unbounded. However, $y \in L_U$ implies that the path labelled by $(0^{\ell-k}, y_\ell \cdots y_{k+1})$ starting from $(0, 0^h, 0^h, 0)$ runs through states (s, z', y', δ) with bounded δ, cf. the proof of Theorem 3.10 in [FS08]. As in Lemma 2.5, we obtain that $\ell - k$ is bounded. □

3. Average number of representations

In this section we study the function $f(n)$ counting the number of different U-expansions of minimal weight (without leading zeros) of the integer n in Σ^*, with $\{0,1\} \subseteq \Sigma \subseteq \mathbb{Z}$. As in Theorem 2.1, $U = (U_k)_{k\ge 0}$ is assumed to be a strictly increasing sequence of integers with $U_0 = 1$, satisfying eventually a linear recurrence with characteristic polynomial equal to the minimal polynomial of a Pisot number β. We will give precise asymptotic information about the average number of representations $\frac{1}{2N-1}\sum_{|n|<N} f(n)$. As a general reference for the study of the asymptotic behaviour of digital functions we refer to [DG10]. In order to exhibit the fluctuating main term of this sum we introduce a measure μ on $\left[\frac{\min\Sigma}{\beta-1}, \frac{\max\Sigma}{\beta-1}\right]$. The construction of this measure is similar to the distribution measures of infinite Bernoulli convolutions as studied in [Erd39]. There it encodes the number of representations of integers as sums of Fibonacci numbers.

As in Section 2, let $\mathcal{M}_{U,\Sigma}$ be the trim minimal automaton recognising $L_U \cap \Sigma^*$. Denote by $A_{U,a}$ the adjacency matrix of all transitions in $\mathcal{M}_{U,\Sigma}$ labelled by the digit a. The total adjacency matrix of the automaton is then $A_{U,\Sigma} = \sum_{a\in\Sigma} A_{U,a}$. Let $\mathcal{M}_{\beta,\Sigma}, A_{\beta,a}, A_{\beta,\Sigma}$ be the corresponding objects for β-expansions.

Let $f_k(n)$ denote the number of words $z \in L_U \cap \Sigma^k$ with $z \sim_U n$, i.e., the number of U-expansions of minimal weight of length k of an integer n. If $|n| < U_k$, then the length of the greedy U-expansion of $|n|$ is at most k. Then, by Lemma 2.8, there exists a constant $m \ge 0$ such that every U-expansions of minimal weight without leading zeros is of length at most $k+m$. By adding leading zeros, we obtain that $f_j(n) = f(n)$ for all $j \ge k+m$.

We define a sequence of measures by

$$\mu_k = \frac{1}{M_k}\sum_{n\in\mathbb{Z}} f_k(n)\,\delta_{\frac{n}{U_k}}, \tag{3.1}$$

where δ_x denotes the unit point mass concentrated in x and

$$M_k = \sum_{n\in\mathbb{Z}} f_k(n) = \#(L_U \cap \Sigma^k).$$

We notice that all points $\frac{n}{U_k}$ with $f_k(n) > 0$ lie in the interval $\big(\sum_{j=0}^{k-1}\frac{U_j}{U_k}\big)[\min\Sigma, \max\Sigma]$.

As a first step of reduction we replace the measure μ_k by the measure ν_k given by

$$\nu_k = \frac{1}{M_k}\sum_{z\in L_U\cap\Sigma^k} \delta_{g(z)} \quad \text{with} \quad g(z_{k-1}\cdots z_0) = \sum_{j=0}^{k-1} z_j\beta^{j-k}.$$

By (2.1), we have

$$\sum_{j=0}^{k-1} z_j\frac{U_j}{U_k} - g(z_{k-1}\cdots z_0) = \mathcal{O}(\beta^{-k}),$$

thus

$$|\widehat{\mu}_k(t) - \widehat{\nu}_k(t)| = \mathcal{O}(|t|\,\beta^{-k}). \tag{3.2}$$

From this it follows that $(\mu_k)_k$ and $(\nu_k)_k$ tend to the same limiting measure μ.

In order to compute the characteristic function of ν_k we consider the weighted adjacency matrix of $\mathcal{M}_{U,\Sigma}$,

$$A_{U,\Sigma}(t) = \sum_{z\in\Sigma} e(zt)\, A_{U,z},$$

where we use the notation $e(t) = e^{2\pi i t}$. Then we have

$$\widehat{\nu}_k(t) = \frac{1}{M_k} \sum_{z\in L_U\cap\Sigma^k} e\big(g(z)t\big) = \frac{1}{M_k}\mathbf{v}_1 A_{U,\Sigma}\big(e(t\beta^{-1})\big) A_{U,\Sigma}\big(e(t\beta^{-2})\big)\cdots A_{U,\Sigma}\big(e(t\beta^{-k})\big)\mathbf{v}_2,$$

where $\mathbf{v}_1$ is the indicator (row) vector of the initial state of $\mathcal{M}_{U,\Sigma}$ and $\mathbf{v}_2$ is the indicator (column) vector of the terminal states of $\mathcal{M}_{U,\Sigma}$.

Lemma 3.1. *The adjacency matrix $A_{U,\Sigma} = A_{U,\Sigma}(0)$ of the automaton $\mathcal{M}_{U,\Sigma}$ has a unique dominating eigenvalue α, which is positive and of multiplicity* 1.

Proof. By Proposition 2.7, every non-zero eigenvalue of $A_{U,\Sigma}$ is an eigenvalue of $A_{\beta,\Sigma}$, with the same multiplicity. Therefore, the lemma follows from Proposition 2.6 and the Perron-Frobenius theorem. □

By Lemma 3.1, there exists a positive constant C such that

$$M_k = \mathbf{v}_1 A_{U,\Sigma}^k \mathbf{v}_2 = C\alpha^k + \mathcal{O}\big((|\alpha_2|+\varepsilon)^k\big) \tag{3.3}$$

for every $\varepsilon > 0$, where α and α_2 are the largest and second largest roots of the characteristic polynomial of $A_{U,\Sigma}$.

Lemma 3.2. *Let A be a $n\times n$-matrix with complex entries. There exists a matrix norm $\|\cdot\|$ satisfying $\|A\| = \rho(A)$ (the spectral radius) if and only if for all eigenvalues λ of A with $|\lambda| = \rho(A)$ the algebraic and geometric multiplicity are equal.*

Proof. Assume that for all λ with $|\lambda| = \rho(A)$ the algebraic and geometric multiplicities are equal. Then there exists a non-singular matrix S, such that

$$SAS^{-1} = \begin{pmatrix} \lambda_1 & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & \lambda_2 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & \ddots & 0 & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_r & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & & & \\ \vdots & \vdots & \ddots & \vdots & & B & \\ 0 & 0 & \dots & 0 & & & \end{pmatrix},$$

with $|\lambda_1| = \cdots = |\lambda_r| = \rho(A)$ and $\rho(B) < \rho(A)$. Then by [HJ85, Lemma 5.6.10 and Theorem 5.6.26] there is a norm $\|\cdot\|_{n-r}$ on $\mathbb{C}^{n-r}$ such that the induced norm on matrices satisfies $\|B\| < \rho(A)$. Define the norm on $\mathbb{C}^n$ by

$$\|\mathbf{x}\| = \|\mathrm{pr}_1 S\mathbf{x}\|_r + \|\mathrm{pr}_2 S\mathbf{x}\|_{n-r},$$

where pr_1 denotes the projection to the first r coordinates and pr_2 the projection to the $n-r$ last coordinates; $\|\cdot\|_r$ is just the ℓ^1-norm on $\mathbb{C}^r$. Then we have

$$\frac{\|A\mathbf{x}\|}{\|\mathbf{x}\|} = \frac{\rho(A)\|\mathrm{pr}_1 S\mathbf{x}\|_r + \|B\mathrm{pr}_2 S\mathbf{x}\|_{n-r}}{\|\mathrm{pr}_1 S\mathbf{x}\|_r + \|\mathrm{pr}_2 S\mathbf{x}\|_{n-r}} \le \rho(A)$$

and therefore $\|A\| = \rho(A)$ by the fact that $\|A\| \ge \rho(A)$ for all norms. Here we have used $\mathrm{pr}_2 SAS^{-1} = B\mathrm{pr}_2$.

If on the other hand A is not diagonalisable for some λ with $|\lambda| = \rho(A)$, then there exist two vectors $\mathbf{e}_1$ and $\mathbf{e}_2$ such that

$$A\mathbf{e}_1 = \lambda\mathbf{e}_1 + \mathbf{e}_2 \quad \text{and } A\mathbf{e_2} = \lambda\mathbf{e}_2.$$

Then we have

$$A^k\mathbf{e}_1 = \lambda^k\mathbf{e}_1 + k\lambda^{k-1}\mathbf{e}_2.$$

Let $\|\cdot\|$ be any norm on $\mathbf{C}^n$. Then

$$\|\lambda^{-k}A^k\mathbf{e}_1\| = \|\mathbf{e}_1 + k\lambda^{-1}\mathbf{e}_2\| \ge k|\lambda|^{-1}\|\mathbf{e}_1\| - \|\mathbf{e}_2\|$$

shows that $\|\lambda^{-k}A^k\mathbf{e}_1\|$ is unbounded, whereas $\|A\| = \rho(A)$ would imply that this sequence is bounded by $\|\mathbf{e}_1\|$. Thus there is no induced matrix norm with $\|A\| = \rho(A)$. Since by [HJ85, Theorem 5.6.26] for every norm there is an induced norm, which is smaller, there cannot exist a matrix norm with $\|A\| = \rho(A)$. □

By Lemma 3.2 there exists a norm on $\mathbb{C}^{\#\text{ states of }\mathcal{M}_{U,\Sigma}}$ such that the induced norm on matrices satisfies $\|A_{U,\Sigma}(0)\| = \rho(A_{U,\Sigma}(0)) = \alpha$. From now on we use this norm. By differentiability of the entries of $A_{U,\Sigma}(t)$ and the fact that the norm $\|\cdot\|$ is comparable to the ℓ^1-norm, there exists a positive constant C such that

$$\big\|A_{U,\Sigma}(t) - A_{U,\Sigma}(0)\big\| \le C|t|.$$

We will prove that $(\nu_k)_k$ (and therefore $(\mu_k)_k$) weakly tends to a limit measure by showing that $(\widehat{\nu}_k(t))_k$ tends to a limit $\widehat{\nu}(t) = \widehat{\mu}(t)$.

Lemma 3.3. *The sequence of measures $(\mu_k)_k$ defined by (3.1) converges weakly to a probability measure μ. The characteristic functions satisfy the inequality*

$$\big|\widehat{\mu}_k(t) - \widehat{\mu}(t)\big| = \begin{cases} \mathcal{O}\big(|t|\,\beta^{-\eta k}\big) & \text{for } |t| \le 1, \\ \mathcal{O}\big(|t|^{\eta}\beta^{-\eta k}\big) & \text{for } |t| \ge 1, \end{cases} \tag{3.4}$$

with

$$\eta = \frac{\log\alpha - \log(|\alpha_2| + \varepsilon)}{\log\beta + \log\alpha - \log(|\alpha_2| + \varepsilon)} \tag{3.5}$$

for any $\varepsilon > 0$. The constants implied by the $\mathcal{O}$-symbol depend only on ε.

Proof. We study the product

$$P_k(t) = \alpha^{-k}\prod_{j=1}^{k} A(t\beta^{-j}),$$

with $A = A_{U,\Sigma}$. For $|t| \le 1$ we estimate

$$\begin{aligned}
\big\|P_k(t) - P_k(0)\big\| &= \alpha^{-k} \left\| \prod_{j=1}^{k} \Big(A(0) + \big(A(t\beta^{-j}) - A(0)\big)\Big) - A(0)^k \right\| \\
&\le \alpha^{-k} \sum_{\ell=1}^{k} \big\|A(0)\big\|^{k-\ell} \sum_{1\le j_1<j_2<\cdots<j_\ell\le k} \big\|A(t\beta^{-j_1}) - A(0)\big\| \cdot \big\|A(t\beta^{-j_2}) - A(0)\big\| \cdots \big\|A(t\beta^{-j_\ell}) - A(0)\big\| \\
&\le \sum_{\ell=1}^{k} \alpha^{-\ell} \sum_{1\le j_1<j_2<\cdots<j_\ell\le k} C^\ell |t|^\ell \beta^{-(j_1+\cdots+j_\ell)} \\
&\le \sum_{\ell=1}^{k} \frac{1}{\ell!} \alpha^{-\ell} C^\ell |t|^\ell \bigg(\sum_{j=1}^{k} \beta^{-j} \bigg)^\ell \le \exp\left(\frac{C|t|}{\alpha(\beta-1)}\right) - 1 = \mathcal{O}(|t|).
\end{aligned}$$

Furthermore, we have for $j > k > \ell$ and $1 \le |t| \le \beta^\ell$

$$\begin{aligned}
&\big\|P_k(t) - P_j(t)\big\| = \big\|P_{k-\ell}(t\beta^{-\ell})P_\ell(t) - P_{j-\ell}(t\beta^{-\ell})P_\ell(t)\big\| \\
&\le \big\|P_\ell(t)\big\| \Big(\big\|P_{k-\ell}(t\beta^{-\ell}) - P_{k-\ell}(0)\big\| + \big\|P_{j-\ell}(t\beta^{-\ell}) - P_{j-\ell}(0)\big\| + \big\|P_{k-\ell}(0) - P_{j-\ell}(0)\big\| \Big) \\
&\qquad = \mathcal{O}\big(|t|\beta^{-\ell}\big) + \mathcal{O}\bigg(\bigg(\frac{|\alpha_2| + \varepsilon}{\alpha} \bigg)^{k-\ell} \bigg) = \mathcal{O}\big(|t|^\eta \beta^{-\eta k}\big).
\end{aligned}$$

Here we have used the fact that $\|P_\ell(t)\|$ is uniformly bounded for all $\ell \in \mathbb{N}$ and all $t \in \mathbb{R}$, since all entries of $P_\ell(t)$ are bounded by the entries of $\alpha^{-\ell} A(0)^\ell$ and the entries of this matrix converge. In the last step we have set $\ell = \lceil (1-\eta)\log_\beta |t| + \eta k \rceil$. The inequality is valid for $j > k > \log_\beta |t|$.

We now assume that $|t| \le 1$ and $j > k > \ell$. Then we have

$$\begin{aligned}
\big|\widehat{\nu}_k(t) - \widehat{\nu}_j(t)\big| &= \left| \frac{\alpha^k}{M_k} \mathbf{v}_1 P_k(t) \mathbf{v}_2 - \frac{\alpha^j}{M_j} \mathbf{v}_1 P_j(t) \mathbf{v}_2 \right| \\
&= \left| \frac{\alpha^k}{M_k} \mathbf{v}_1 P_{k-\ell}(t\beta^{-\ell}) P_\ell(t) \mathbf{v}_2 - \frac{\alpha^j}{M_j} \mathbf{v}_1 P_{j-\ell}(t\beta^{-\ell}) P_\ell(t) \mathbf{v}_2 \right| \\
&\le \left| \frac{\alpha^k}{M_k} \mathbf{v}_1 P_{k-\ell}(0) P_\ell(t) \mathbf{v}_2 - \frac{\alpha^j}{M_j} \mathbf{v}_1 P_{j-\ell}(0) P_\ell(t) \mathbf{v}_2 \right| + \mathcal{O}\big(|t|\beta^{-\ell}\big) \\
&= \left| \frac{\alpha^k}{M_k} \mathbf{v}_1 P_{k-\ell}(0) \big(P_\ell(t) - P_\ell(0)\big) \mathbf{v}_2 - \frac{\alpha^j}{M_j} \mathbf{v}_1 P_{j-\ell}(0) \big(P_\ell(t) - P_\ell(0)\big) \mathbf{v}_2 \right| + \mathcal{O}\big(|t|\beta^{-\ell}\big) \\
&= |t|\, \mathcal{O}\bigg(\beta^{-\ell} + \bigg(\frac{|\alpha_2| + \varepsilon}{\alpha} \bigg)^{k-\ell} \bigg),
\end{aligned}$$

where we have used $\frac{\alpha^k}{M_k} \mathbf{v}_1 P_k(0) \mathbf{v}_2 = 1$ in the fourth line. Setting $\ell = \lfloor \eta k \rfloor$ gives

$$\big|\widehat{\nu}_k(t) - \widehat{\nu}_j(t)\big| = \mathcal{O}\big(|t|\beta^{-\eta k}\big).$$

Thus $\widehat{\nu}_k(t)$ converges uniformly on compact subsets of $\mathbb{R}$ to a continuous limit $\widehat{\mu}(t)$, and the measures ν_k tend to a measure μ weakly. From this together with (3.2) the two inequalities (3.4) are immediate. □

Lemma 3.4. *There exists a positive real number $\gamma < \alpha$ such that*

$$\max_{x\in\mathbb{Z}[\beta]} \#\big\{ z_{k-1}\cdots z_0 \in L_\beta \cap \Sigma^k : \ \textstyle\sum_{j=0}^{k-1} z_j\beta^j = x\big\} \ = \ \mathcal{O}(\gamma^k).$$

Proof. Similarly to (3.3), we have

$$\#(L_\beta \cap \Sigma^k) = \mathbf{v}_1' \, A_{\beta,\Sigma}^k \, \mathbf{v}_2' = \mathcal{O}(\alpha^k),$$

where $\mathbf{v}_1'$ is the indicator (row) vector of the initial state of $\mathcal{M}_{\beta,\Sigma}$ and $\mathbf{v}_2' = (1,\dots,1)^T$ is the indicator (column) vector of the terminal states of $\mathcal{M}_{\beta,\Sigma}$. We show that there exists some $\ell \ge 1$ and a matrix $\tilde{A}$ with $\tilde{A} < A_{\beta,\Sigma}^\ell$ (entrywise) such that

$$\#\big\{ z_{k-1}\cdots z_0 \in L_\beta \cap \Sigma^k : \ \textstyle\sum_{j=0}^{k-1} z_j\beta^j = x\big\} \le \mathbf{v}_1' \, \tilde{A}^{\lfloor k/\ell \rfloor} \, A_{\beta,\Sigma}^{k-\lfloor k/\ell\rfloor \ell} \, \mathbf{v}_2' \tag{3.6}$$

for all $x \in \mathbb{Z}[\beta]$, $k \ge 0$.

Each entry in $A_{\beta,\Sigma}^\ell$ counts the number of paths of length ℓ in $\mathcal{M}_{\beta,\Sigma}$ between two states q and q'. By the proof of Proposition 2.6, there exists $k_1 \ge 0$ such that the path labelled by 0^{k_1} leads from every state to the initial state. Let $k_2 \ge 0$ be such that $1\,0^{k_2}$ leads from the initial state to itself, k_3 be the maximal distance of a state from the initial state, and $\ell = k_1 + k_2 + k_3 + 1$. Then, for any two states q, q', there exists a $z' \in \Sigma^{k_3}$ such that paths labelled by $0^{k_1}\,1\,0^{k_2}\,z'$ and by $0^{k_1+1+k_2}\,z'$ (of length ℓ) run from q to q'. It is well known that the words $(z_{k-1}\cdots z_0, y_{k-1}\cdots y_0)$ with $\sum_{j=0}^{k-1} z_j\beta^j = \sum_{j=0}^{k-1} y_j\beta^j$ are recognised by a finite automaton with transitions of the form $s \overset{(a,b)}{\to} \beta s + b - a$, see e.g. [FS08]. For sufficiently large k_1 and k_2, there is no path labelled by $(0^{k_1}\,1\,0^{k_2}, 0^{k_1+1+k_2})$ in this automaton. Therefore, for any fixed $x \in \mathbb{Z}[\beta]$, any word $z_{k-1}\cdots z_j$, $\ell \le j \le k$, leading to the state q in $\mathcal{M}_{\beta,\Sigma}$ cannot be prolonged by all labels of paths of length ℓ between q and q' when we want to obtain a word $z_{k-1}\cdots z_0 \in L_\beta \cap \Sigma^k$ with $\sum_{j=0}^{k-1} z_j\beta^j = x$.

This means that, for sufficiently large ℓ, (3.6) holds with $\tilde{A}$ taken as the matrix with every entry being one smaller than that of $A_{\beta,\Sigma}^\ell$. Let $\tilde{\alpha}$ be the dominant eigenvalue of $\tilde{A}$, then $\tilde{\alpha} < \alpha^\ell$ and the lemma holds with $\gamma = \tilde{\alpha}^{1/\ell}$. □

Corollary 3.5. *The counting function f satisfies $f(n) = \mathcal{O}(|n|^{\log_\beta \gamma})$ for some $\gamma < \alpha$.*

Proposition 3.6. *Let γ be as in Lemma 3.4. Then the measure μ satisfies*

$$\mu\big([x,y]\big) = \mathcal{O}\big((y-x)^\theta\big) \tag{3.7}$$

with

$$\theta = \frac{\log\alpha - \log\gamma}{\log\beta}. \tag{3.8}$$

Proof. Let $x < y$, and $\ell = \lfloor -\log_\beta(y-x) \rfloor$. Recall that

$$\mu\big([x,y]\big) = \lim_{k\to\infty} \frac{1}{M_k} \sum_{z\in L_U\cap\Sigma^k:\, g(z)\in[x,y]} \delta_{g(z)}. \tag{3.9}$$

Let $z = z_{k-1}\cdots z_0 \in L_U\cap\Sigma^k$. By Proposition 2.7, we have $z_{k-1}\cdots z_{k-\ell} \in L_\beta$ for sufficiently large k. If $g(z)\in[x,y]$, then

$$\sum_{j=0}^{\ell-1} z_{j+k-\ell}\beta^j \in \beta^\ell[x,y] - \left[\frac{\min\Sigma}{\beta-1}, \frac{\max\Sigma}{\beta-1}\right].$$

Since $y-x \le \beta^{-\ell}$, this implies that $\sum_{j=0}^{\ell-1} z_{j+k-\ell}\beta^j$ lies in an interval of bounded size. For all conjugates $\beta_i \ne \beta$, we have $\big|\sum_{j=0}^{\ell-1} z_{j+k-\ell}\beta_i^j\big| \le \max_{a\in\Sigma}|a|/(1-|\beta_i|)$, thus $\sum_{j=0}^{\ell-1} z_{j+k-\ell}\beta^j$ can take only a bounded number of values in $\mathbb{Z}[\beta]$. (The bound does not depend on the choice of $[x,y]$.) Then $z_{k-\ell-1}\cdots z_0 \in L_U\cap\Sigma^{k-\ell}$ and Lemma 3.4 yield that

$$\mu\big([x,y]\big) = \mathcal{O}\bigg(\gamma^\ell \lim_{k\to\infty}\frac{M_{k-\ell}}{M_k}\bigg) = \mathcal{O}\bigg(\bigg(\frac{\gamma}{\alpha}\bigg)^\ell\bigg).$$

Combining this with $\ell = -\log_\beta(y-x)+\mathcal{O}(1)$ gives (3.7). □

We use Proposition 3.6 and the following lemma to establish purity of the measure μ.

Lemma 3.7 ([JW35, Theorem 35], [Ell79, Lemma 1.22 (ii)])**.** *Let $Q = \prod_{k=0}^\infty Q_k$ be an infinite product of discrete spaces equipped with a measure κ, which satisfies Kolmogorov's 0-1-law (i.e., every tail event has either measure 0 or 1). Furthermore, let X_k be a sequence of random variables defined on the spaces Q_k, such that the series $X = \sum_{k=0}^\infty X_k$ converges κ-almost everywhere. Then the distribution of X is either purely discrete, or purely singular continuous, or absolutely continuous with respect to Lebesgue measure.*

Proposition 3.8. *The measure μ is pure, i.e., it is either absolutely continuous or purely singular continuous.*

Proof. We equip the shift space

$$\mathcal{K} = \big\{(z_k)_{k\ge0} :\ z_k z_{k-1}\cdots z_0 \in L_\beta\cap\Sigma^* \text{ for all } k\ge0\big\}$$

associated to the automaton $\mathcal{M}_{\beta,\Sigma}$ with the measure

$$\begin{aligned}\kappa\big([z_0,z_1,\dots,z_{\ell-1}]\big) &= \lim_{k\to\infty}\frac{1}{M_k}\#\big\{y_{k-1}\cdots y_0\in L_\beta :\ y_{\ell-1}\cdots y_0 = z_{\ell-1}\cdots z_0\big\}\\ &= \lim_{k\to\infty}\frac{1}{\mathbf{v}_1' A_{\beta,\Sigma}^k \mathbf{v}_2'}\mathbf{v}_1' A_{\beta,\Sigma}^{k-\ell} A_{\beta,z_{\ell-1}}\cdots A_{\beta,z_0}\mathbf{v}_2\end{aligned}$$

given on the cylinder set

$$[z_0,z_1,\dots,z_{\ell-1}] = \big\{(y_k)_{k\ge0}\in\mathcal{K} :\ y_{\ell-1}\cdots y_0 = z_{\ell-1}\cdots z_0\big\}.$$

Then κ can be written in terms of the transition matrices

$$\kappa\big([z_0, z_1, \dots, z_{\ell-1}]\big) = \frac{1}{\mathbf{v}\mathbf{v}_2'} \alpha^{-\ell} \mathbf{v} A_{\beta, z_{\ell-1}} \cdots A_{\beta, z_0} \mathbf{v}_2',$$

where $\mathbf{v}$ is the left Perron-Frobenius eigenvector of the matrix $A_{\beta,\Sigma}$. Let $\mathbf{w}$ denote the right Perron-Frobenius eigenvalue of the matrix $A_{\beta,\Sigma}$ with $\mathbf{v}\mathbf{w} = 1$. Then by positivity of all entries of $\mathbf{w}$ and $\mathbf{v}_2'$ the measure $\tilde{\kappa}$ given by

$$\tilde{\kappa}\big([z_0, z_1, \dots, z_{\ell-1}]\big) = \alpha^{-\ell} \mathbf{v} A_{\beta, z_{\ell-1}} \cdots A_{\beta, z_0} \mathbf{w}$$

is equivalent to κ.

The measure $\tilde{\kappa}$ is strongly mixing and therefore ergodic with respect to the shift. Thus $\tilde{\kappa}$ and κ satisfy the hypotheses of Lemma 3.7.

The continuity of μ is an immediate consequence of Proposition 3.6. □

In order to give an error bound for the rate of convergence of the measures μ_k to the measure μ, we will use the following version of the Berry-Esseen inequality, which was proved in [Gra97].

Proposition 3.9. *Let μ_1 and μ_2 be two probability measures with their Fourier transforms defined by*

$$\widehat{\mu}_k(t) = \int_{-\infty}^{\infty} e^{2\pi i t x} \, d\mu_k(x), \quad k = 1, 2.$$

Suppose that $\big(\widehat{\mu}_1(t) - \widehat{\mu}_2(t)\big)\, t^{-1}$ is integrable on a neighbourhood of zero and μ_2 satisfies

$$\mu\big((x, y)\big) \le c\, |x - y|^{\theta}$$

for some $0 < \theta < 1$. Then the following inequality holds for all real x and all $T > 0$:

$$\begin{aligned}\Big|\mu_1\big((-\infty, x)\big) - \mu_2\big((-\infty, x)\big)\Big| \le{}& \left| \int_{-T}^{T} \hat{J}(T^{-1}t)\, (2\pi i t)^{-1} \big(\widehat{\mu}_1(t) - \widehat{\mu}_2(t)\big)\, e^{-2\pi i x t}\, dt \right| \\ &+ \left(c + \frac{1}{\pi^2}\right) T^{-\frac{2\theta}{2+\theta}} + \left| \frac{1}{2T} \int_{-T}^{T} \left(1 - \frac{|t|}{T}\right) \big(\widehat{\mu}_1(t) - \widehat{\mu}_2(t)\big)\, e^{-2\pi i x t}\, dt \right|,\end{aligned}$$

where

$$\hat{J}(t) = \pi t (1 - |t|) \cot \pi t + |t|.$$

Lemma 3.10. *The measures μ_k satisfy*

$$\big|\mu_k\big((x, y)\big) - \mu\big((x, y)\big)\big| = \mathcal{O}\big(\beta^{-\zeta k}\big) \tag{3.10}$$

uniformly for all $x, y \in \mathbb{R}$ with $\zeta = \frac{2\theta\eta}{\eta(\theta+2)+2\theta}$.

Proof. We apply Proposition 3.9 to the measures μ_k and μ. For this purpose we use the inequalities (3.4) to obtain

$$\begin{aligned}\big|\mu_k\big((-\infty,x)\big)-\mu\big((-\infty,x)\big)\big| &= \mathcal{O}\bigg(\beta^{-\eta k}\int_{-1}^{1} dt\bigg)+\mathcal{O}\bigg(\beta^{-\eta k}\int_{1\le|t|\le T}|t|^{\eta-1}\,dt\bigg)+\mathcal{O}\Big(T^{-\frac{2\theta}{2+\theta}}\Big)\\ &\quad+\mathcal{O}\bigg(\beta^{-\eta k}\frac{1}{T}\int_{-1}^{1}|t|\,dt\bigg)+\mathcal{O}\bigg(\beta^{-\eta k}\frac{1}{T}\int_{1\le|t|\le T}|t|^{\eta}\,dt\bigg)=\mathcal{O}\big(\beta^{-\zeta n}\big)\end{aligned}$$

by choosing $T=\beta^{\zeta\frac{2+\theta}{2\theta}k}$. □

Now the statement of the asymptotic behaviour of the average $\frac{1}{2N-1}\sum_{|n|<N} f(n)$ is a consequence of the preceding discussion of the properties of μ. Combining Lemma 3.3, Proposition 3.6, and Lemma 3.10 we obtain the following theorem.

Theorem 3.11. *The summatory function of the number of representations of n with minimal weight satisfies*

$$\sum_{|n|<N} f(n) = N^{\log_\beta \alpha}\,\Phi(\log_\beta N)+\mathcal{O}(N^{\lambda}), \tag{3.11}$$

where Φ denotes a continuous periodic function of period 1 and

$$\lambda=\frac{\log\alpha}{\log\beta}-\frac{2\theta\eta}{\eta(\theta+2)+2\theta},$$

η given by (3.5), and θ given by (3.8).

Proof. Using the definition of μ_k in (3.1) and the value m given by Lemma 2.8 we have

$$\sum_{|n|<N} f(n) = M_k\,\mu_k\big((-N/U_k, N/U_k)\big),$$

where we choose $k=\lfloor\log_\beta N\rfloor+m$. Replacing μ_k by μ, using $U_k=C\beta^k+\mathcal{O}(|\beta_2|^k)$, $M_k=D\alpha^k+\mathcal{O}((|\alpha_2|+\varepsilon)^k)$ and taking all error terms into account yields

$$\begin{aligned}\sum_{|n|<N} f(n) &= D\,\alpha^{\lfloor\log_\beta N\rfloor+m}\,\mu\big(\big(-\beta^{\log_\beta N-\lfloor\log_\beta N\rfloor-m}/C,\,\beta^{\log_\beta N-\lfloor\log_\beta N\rfloor-m}/C\big)\big)\\ &\quad+\mathcal{O}\big(\alpha^k\beta^{-\zeta k}\big)+\mathcal{O}\bigg(\alpha^k\bigg(\frac{|\beta_2|}{\beta}\bigg)^{\theta k}\bigg)+\mathcal{O}\big((|\alpha_2|+\varepsilon)^k\big),\end{aligned}$$

with ζ as in Lemma 3.10. Defining

$$\Phi(t)=D\,\alpha^{m+\lfloor t\rfloor-t}\,\mu\big(\big(-\beta^{t-\lfloor t\rfloor-m}/C,\,\beta^{t-\lfloor t\rfloor-m}/C\big)\big)$$

for $t\ge 0$ yields (3.11). The periodicity of Φ follows from the definition. The continuity of Φ in non-integer points follows from the continuity of μ. The fact that $\Phi(0)=\lim_{t\to 1-}\Phi(t)$

is a consequence of the self-similarity of the measure μ

$$\mu(\beta^{-1}A) = \alpha^{-1}\mu(A) \text{ for } A \subset [-\beta^{-m}, \beta^{-m}];$$

this follows from (3.9) by the observation that multiplication by β^{-1} corresponds to adding a prefix 0 in the representation and reading a leading zero does not change the state of the automaton. □

4. Exact number of representations

To obtain the exact number of U-expansions of minimal weight representing an integer n, we choose one of these expansions and look at the transducer which transforms any other expansion into it. One way of choosing a output language of such a transducer is to take the set of greedy U-expansions (for positive numbers) and their symmetric counterparts (to represent negative numbers). A possible deficiency of this language is that it is not contained in L_U. In the following, we describe a regular language $G_U \subseteq L_U$ such that, for every $n \in \mathbb{Z}$, there is, up to leading zeros, a unique word $z \in G_U$ with $z \sim_U n$.

We call a word $z = z_k \cdots z_0 \in L_U$ *greedy U-expansion of minimal weight* if

$$0^{\min(\ell-k,0)}\,|z_k| \cdots |z_0| \geq 0^{\min(k-\ell,0)}\,|y_\ell| \cdots |y_0| \quad \text{for all } y = y_\ell \cdots y_0 \in L_U \text{ with } z \sim_U y,$$

with respect to the lexicographical order. The set of all greedy U-expansions of minimal is denoted by G_U.

Lemma 4.1. *Let U be as in Theorem 2.1. For any $n \in \mathbb{Z}$, there is, up to leading zeros, a unique word $z \in G_U$ with $z \sim_U n$.*

Proof. Let $n \in \mathbb{Z}$. First note that by Lemma 2.8 there are, up to leading zeros, only finitely many words $z \in G_U$ with $z \sim_U n$. Therefore there exists a greedy U-expansion of minimal weight $z = z_k \cdots z_0$ with $z \sim_U n$.

Let $y = y_\ell \cdots y_0$ be another word in G_U with $y \sim_U n$. Then we have $0^{\min(\ell-k,0)}|z_k| \cdots |z_0| = 0^{\min(k-\ell,0)}|y_\ell| \cdots |y_0|$. Neglecting leading zeros, we can assume w.l.o.g. that $k = \ell$. We have $\frac{y_k+z_k}{2} \cdots \frac{y_0+z_0}{2} \in \mathbb{Z}^*$ because $\frac{y_j+z_j}{2} = z_j$ in case $y_j = z_j$, $\frac{y_j+z_j}{2} = 0$ in case $y_j = -z_j$; and $\frac{y_k+z_k}{2} \cdots \frac{y_0+z_0}{2} \sim_U n$. If we had $y_j \neq z_j$ for some j, then $\frac{y_k+z_k}{2} \cdots \frac{y_0+z_0}{2}$ would have smaller weight than z, contradicting $z \in L_U$. Therefore, z and y differ only by leading zeros. □

Theorem 4.2. *Let U be as in Theorem 2.1. Then G_U is recognised by a finite automaton.*

Proof. It suffices to show that $L_U \setminus G_U$ is a regular language. Since the complement of a regular language is regular, see e.g. [FS08, Lemma 3.9], this implies that G_U is regular.

Let $z = z_k \cdots z_0 \in L_U \setminus G_U$. Then there exists a $y = y_\ell \cdots y_0 \in L_U$ with $y \sim_U z$ and $0^{\min(\ell-k,0)}\,|z_k| \cdots |z_0| < 0^{\min(k-\ell,0)}\,|y_\ell| \cdots |y_0|$. Since L_U is a regular language, the product $\{(z_k \cdots z_0, y_k \cdots y_0) \mid z_k \cdots z_0, y_k \cdots y_0 \in L_U,\, k \geq 0\}$ is recognised by a finite automaton. One can construct a finite automaton recognising the lexicographic relation $|z_k| \cdots |z_0| < |y_k| \cdots |y_0|$. By Proposition 2.4, the same holds for $z_k \cdots z_0 \sim_U y_k \cdots y_0$. Therefore, there exists a finite automaton which recognises the set of pairs $(z_k \cdots z_0, y_k \cdots y_0) \in L_U \times L_U$ such that $z_k \cdots z_0 \sim_U y_k \cdots y_0$ and $|z_k| \cdots |z_0| < |y_k| \cdots |y_0|$. Let H be the projection of this set to the first coordinate, then H is regular. Moreover, $L_U \setminus G_U$ is the set of words which

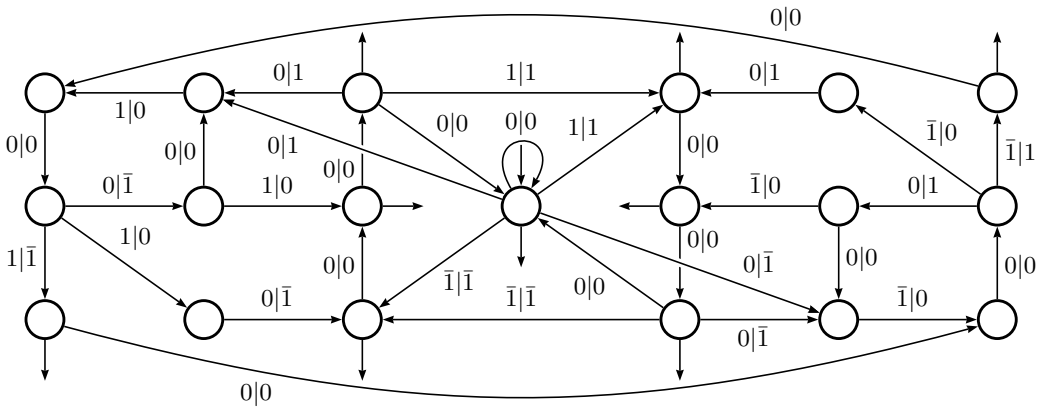

FIGURE 2. Transducer $\mathcal{N}_{F,\{-1,0,1\}}$ normalising F-expansions of minimal weight in $\{-1,0,1\}^*$. Here $a \mid b$ stands for (a,b) in the transition labels.

are obtained from words in H by removing or appending initial zeros. This language is regular as well. By the remarks at the beginning of the proof, this proves the lemma. □

Proposition 4.3. *Let U be as in Theorem 2.1. Then there exists a finite letter-to-letter transducer recognising the pairs $(z_k \cdots z_0, y_k \cdots y_0) \in L_U \times G_U$ with $z_k \cdots z_0 \sim_U y_k \cdots y_0$.*

Proof. Similarly to the proof of Theorem 4.2, this follows from the regularity of L_U and G_U, and from Proposition 2.4. □

Note that in Proposition 4.3 the input and output must have the same length. In particular, the input must be as least as long as the corresponding word in G_U without leading zeros. By Lemma 2.8, the difference between any two words in L_U without leading zeros with the same value as U-expansions is bounded. Therefore, there exists a *transducer with initial function* which computes, for every word in L_U without leading zeros, the corresponding word in G_U without leading zeros, see [Fro92].

We have the following corollary of Proposition 4.3, where $\mathcal{N}_{U,\Sigma}$ denotes the trim minimal letter-to-letter transducer of Proposition 4.3.

Corollary 4.4. *Let U, Σ, f be as in Section 3, $n \in \mathbb{Z}$ and $y \in G_U$ with $y \sim_U n$. Then $f(n)$ is given by the number of successful paths in $\mathcal{N}_{U,\Sigma}$ with y as output.*

It was shown in [FS08] that the transducer in Figure 2 transforms any F-expansion of minimal weight, after possible addition of a leading zero, into the corresponding F-expansion of minimal weight avoiding the factors 11, $1\bar{1}$, 101, $10\bar{1}$, 1001 and their opposites. Here, we write $\bar{1}$ instead of 1, and opposite means that 1's and $\bar{1}$'s are exchanged. This transducer shows that the set of outputs is G_F, thus this transducer is equal to $\mathcal{N}_{F,\{-1,0,1\}}$.

Now we can relate the growth of $f(n)$ to the *joint spectral radius* of the set $\{R_{U,a} : a \in \Sigma\}$, where $R_{U,a}$ denotes the adjacency matrix of the transitions with output a in $\mathcal{N}_{U,\Sigma}$. The joint spectral radius is defined by

$$\rho\big(\{R_{U,a} : a \in \Sigma\}\big) = \lim_{k\to\infty} \max\big\{\|R_{U,z_{k-1}} \cdots R_{U,z_0}\|^{1/k} \mid z_{k-1} \cdots z_0 \in \Sigma^k\big\},$$

where $\|\cdot\|$ is any matrix norm. The definition of the joint spectral radius is due to [RS60]; an overview of its properties and its calculation can be found in [Jun09].

Theorem 4.5. *Let U, Σ, f be as in Section 3. For any $\varepsilon > 0$, we have $f(n) = \mathcal{O}(|n|^{\log_\beta(\gamma+\varepsilon)})$, where γ is the joint spectral radius of the set of matrices $\{R_{U,a} : a \in \Sigma\}$.*

Proof. For any non-zero $n \in \mathbb{Z}$, the length of the word $y \in G_U$ with $y \sim_U n$ and without leading zeros is $\log_\beta |n| + \mathcal{O}(1)$. By Corollary 4.4, the number of successful paths in $\mathcal{N}_{U,\Sigma}$ with output $y_{k-1} \cdots y_0$ is $\mathbf{v} R_{U,y_{k-1}} \cdots R_{U,y_0} \mathbf{w}$ for vectors $\mathbf{v}, \mathbf{w}$ corresponding to the initial and the terminal states of $\mathcal{N}_{U,\Sigma}$, thus $f(n) = \mathcal{O}((\gamma+\varepsilon)^{\log_\beta |n|})$. □

For $U = F$ and $\Sigma = \{-1, 0, 1\}$, we have an explicit formula for the maximal number of elements of $L_F \cap \{-1, 0, 1\}^k$ with the same value.

Theorem 4.6. *Let $U = F$ and $\Sigma = \{-1, 0, 1\}$. For every $k \geq 1$, we have*

$$\max_{n \in \mathbb{Z}} f_k(n) = 2^{\lfloor (k-1)/3 \rfloor}.$$

Proof. First we show that

$$\max_{y \in \Sigma^k} \mathbf{v} R_{F,y} \mathbf{w} = 2^{\lfloor (k-1)/3 \rfloor}, \tag{4.1}$$

where $R_{F,y_{k-1}\cdots y_0} = R_{F,y_{k-1}} \cdots R_{F,y_0}$, and $\mathbf{v}, \mathbf{w}$ are as in the proof of Theorem 4.5. From the structure of G_F, it is clear that $R_{F,y} = 0$ if y contains a factor $11, 1\bar{1}, 101, 10\bar{1}, 1001$ or its opposite. We have the following entrywise relations between matrices:

$$R_{F,10^7} \leq R_{F,100\bar{1}0000},\ R_{F,1000\bar{1}0} \leq R_{F,100\bar{1}0},\ R_{F,10^k\bar{1}} \leq R_{F,100\bar{1}} \quad \text{for all } k \geq 4,$$
$$R_{F,100001} \leq \widetilde{R}_{F,1000\bar{1}},\ R_{F,10^k1} \leq \widetilde{R}_{F,100\bar{1}} \quad \text{for } k = 3 \text{ and all } k \geq 5.$$

Here, $\widetilde{R}_{F,y}$ denotes the matrix which is obtained from $R_{F,y}$ by exchanging each column with its symmetric counterpart. Since $R_{F,y}\mathbf{w} = R_{F,y0}\mathbf{w}$ for all $y \in \Sigma^*$, we obtain that $R_{F,y}\mathbf{w}$ is maximal for y with period $100\bar{1}00$. For $y = (100\bar{1}00)^{k/6}$, where a fractional power $(z_1 \cdots z_6)^{k/6}$ denotes as usual the word $(z_1 \cdots z_6)^{\lfloor k/6 \rfloor} z_1 \cdots z_{k-6\lfloor k/6 \rfloor}$, we have $\mathbf{v} R_{F,y} \mathbf{w} = 2^{\lfloor (k-1)/3 \rfloor}$, thus (4.1) holds. By Corollary 4.4, this means that $f_k(n) = 2^{\lfloor (k-1)/3 \rfloor}$ for $n \sim_F (100\bar{1}00)^{k/6}$, and $f_k(n) \leq 2^{\lfloor (k-1)/3 \rfloor}$ for all n with greedy F-expansion of minimal weight of length at most k.

It remains to consider $f_k(n)$ for those n whose greedy F-expansion of minimal weight (without leading zeros) is longer than k. The transducer $\mathcal{N}_{F,\{-1,0,1\}}$ shows that any F-expansion of minimal weight in $\{-1, 0, 1\}^*$ is at most 1 shorter than the corresponding greedy F-expansion of minimal weight. Thus we have to consider $n \sim_F y_k y_{k-1} \cdots y_0 \in G_F$, where we assume w.l.o.g. $y_k = 1$. For such an n, we have $f_k(n) = \mathbf{v}' R_{F,y_{k-1}\cdots y_0} \mathbf{w}$, where $\mathbf{v}'$ is the indicator vector of the state which is reached from the initial state by the transition labeled by $(1, 0)$. Now, equations and inequalities such as $\mathbf{v}' R_{F,00\bar{1}001} = \mathbf{v} R_{F,00\bar{1}001}$ and $\mathbf{v}' R_{F,000\bar{1}} \leq \mathbf{v} R_{F,\bar{1}}$ show that $f_k(n) \leq \max_{y \in \Sigma^k} \mathbf{v} R_{F,y} \mathbf{w} = 2^{\lfloor (k-1)/3 \rfloor}$. □

References

[BR10] V. Berthé and M. Rigo (eds.), *Combinatorics, Automata and Number Theory*, Encyclopedia of Mathematics and Its Applications, no. 135, Cambridge University Press, Cambridge, 2010.

[CFA+06] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren (eds.), *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006.

[DG10] M. Drmota and P. J. Grabner, *Analysis of digital functions and applications*, ch. 9, pp. 452–504, in Berthé and Rigo [BR10], 2010.

[Doc06] C. Doche, *Exponentiation*, ch. 9, pp. 145–168, in Cohen et al. [CFA+06], 2006.

[Ell79] P. D. T. A. Elliott, *Probabilistic Number Theory. I*, Grundlehren der Mathematischen Wissenschaften, vol. 239, Springer-Verlag, New York, 1979, Mean-value theorems.

[Erd39] P. Erdős, *On a family of symmetric Bernoulli convolutions*, Amer. J. Math. **61** (1939), 974–976.

[Fro89] C. Frougny, *Linear numeration systems, θ-developments and finite automata*, STACS 89 (Paderborn, 1989), Lecture Notes in Comput. Sci., vol. 349, Springer, Berlin, 1989, pp. 144–155.

[Fro92] C. Frougny, *Representation of numbers and finite automata*, Math. Systems Theory **25** (1992), 37–60.

[Fro02] ———, *Numeration systems*, Algebraic Combinatorics on Words (M. Lothaire, ed.), Encyclopedia of Mathematics and its Applications, vol. 90, Cambridge University Press, 2002, pp. 230–268.

[FS08] C. Frougny and W. Steiner, *Minimal weight expansions in Pisot bases*, J. Math. Cryptol. **2** (2008), no. 4, 365–392.

[FS10] C. Frougny and J. Sakarovitch, *Number representations and finite automata*, ch. 2, pp. 34–107, in Berthé and Rigo [BR10], 2010.

[GH06] P. J. Grabner and C. Heuberger, *On the number of optimal base 2 representations of integers*, Des. Codes Cryptogr. **40** (2006), 25–39.

[Gra97] P. J. Grabner, *Functional iterations and stopping times for Brownian motion on the Sierpiński gasket*, Mathematika **44** (1997), 374–400.

[HJ85] R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press, Cambridge, 1985.

[Jun09] R. Jungers, *The joint spectral radius*, Lecture Notes in Control and Information Sciences, vol. 385, Springer-Verlag, Berlin, 2009.

[JW35] B. Jessen and A. Wintner, *Distribution functions and the Riemann zeta function*, Trans. Amer. Math. Soc. **38** (1935), no. 1, 48–88.

[LM95] D. Lind and B. Marcus, *An Introduction to Symbolic Dynamics and Coding*, Cambridge University Press, Cambridge, 1995.

[PT89] A. Pethő and R. F. Tichy, *On digit expansions with respect to linear recurrences*, J. Number Theory **33** (1989), no. 2, 243–256.

[Rei60] G. W. Reitwiesner, *Binary arithmetic*, Advances in computers, Vol. 1, Academic Press, New York, 1960, pp. 231–308.

[RS60] G.-C. Rota and G. Strang, *A note on the joint spectral radius*, Nederl. Akad. Wetensch. Proc. Ser. A 63 = Indag. Math. **22** (1960), 379–381.

[Sak09] J. Sakarovitch, *Elements of automata theory*, Cambridge University Press, Cambridge, 2009, Translated from the 2003 French original by Reuben Thomas.

[vzGG99] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge University Press, New York, 1999.

(P. Grabner) Institut für Analysis und Computational Number Theory, Technische Universität Graz, Steyrergasse 30, 8010 Graz, Austria
E-mail address: peter.grabner@tugraz.at

(W. Steiner) LIAFA, CNRS, Université Paris Diderot – Paris 7, Case 7014, 75205 Paris Cedex 13, France
E-mail address: steiner@liafa.jussieu.fr