COUNTING OPTIMAL JOINT DIGIT EXPANSIONS

Peter J. Grabner[1]
Institut für Mathematik A, Technische Universität Graz, Steyrergasse 30, 8010 Graz, Austria
peter.grabner@tugraz.at

Clemens Heuberger[2]
Institut für Mathematik B, Technische Universität Graz, Steyrergasse 30, 8010 Graz, Austria
clemens.heuberger@tugraz.at

Helmut Prodinger[3]
Department of Mathematics, University of Stellenbosch, Stellenbosch 7600, South Africa
hproding@sun.ac.za

Received: 1/19/05, Revised: 5/17/05, Accepted: 8/12/05, Published: 9/8/05

Abstract

This paper deals with pairs of integers, written in base two expansions using digits $0, \pm 1$. Representations with minimal Hamming weight (number of non-zero pairs of digits) are of special importance because of applications in Cryptography. The interest here is to count the number of such optimal representations.

1. Introduction

In many public key cryptosystems, raising elements of a given group to large powers is an important issue. Let P be an element of a given group, whose operation will be written additively. We need to form nP for large integers n in a short amount of time. A classical way to do this is the *binary method*, which uses the operations "doubling" and "adding P." If n is written in its binary representation, the number of doublings is $\lfloor \log_2 n \rfloor$ and an addition corresponds to an occurrence of the digit 1, so the cost of the multiplication depends on the length and number of ones in the binary representation. If addition and subtraction are equally costly in the underlying group, it makes sense to consider *signed binary representations*, which additionally use the digit -1. Clearly, such a digit -1 corresponds to a subtraction. In general, there are many representations of n with digits $\{0, \pm 1\}$, and

[1]This author is supported by the START-project Y96-MAT of the Austrian Science Fund.
[2]This author is supported by the grant S8307-MAT of the Austrian Science Fund.
[3]This author is supported by the grant NRF 2053748 of the South African National Research Foundation

thus one is interested in those with a low "Hamming weight" (number of nonzero digits), as it leads to low costs. A prominent representation achieving this is the non-adjacent form (NAF), which was rediscovered many times. It is characterized by the fact that $x_j x_{j+1} = 0$ holds for all j (of two adjacent digits, at least one is zero). On average, only about 1/3 of the digits are non-zero (as opposed to 1/2 in standard binary representations).

The enumeration of representations with digits $\{0, \pm1\}$ of minimal Hamming weight was addressed in [4]; without going into technicalities, what came out of that analysis is that "most numbers have many optimal representations." (Numbers like 2^n have only one optimal representation, but are extremely rare.)

These ideas apply also *mutatis mutandis* to the computation of $n_1P + n_2Q$; instead of computing n_1P and n_2Q separately, one can use doublings and occasional additions of P, Q, or $P + Q$. Given two integers n_1 and n_2, a *joint expansion* of $\mathbf{n} = \binom{n_1}{n_2}$ is a sequence of digit vectors $\boldsymbol{\varepsilon}_\ell \boldsymbol{\varepsilon}_{\ell-1} \cdots \boldsymbol{\varepsilon}_0$ with $\boldsymbol{\varepsilon}_j = \binom{x_j}{y_j} \in \{0, \pm1\}^2$ and

$$\mathbf{n} = \mathsf{value}(\boldsymbol{\varepsilon}_\ell \boldsymbol{\varepsilon}_{\ell-1} \cdots \boldsymbol{\varepsilon}_0) = \sum_{j=0}^{\ell} 2^j \boldsymbol{\varepsilon}_j.$$

Its *(joint) Hamming weight* is the number of nonzero digit vectors $\left\{ j \mid \boldsymbol{\varepsilon}_j \neq \binom{0}{0} \right\}$. This leads to a linear combination algorithm which performs doublings and occasional additions of $\pm P$, $\pm Q$, $\pm P \pm Q$ (which are precomputed values). Clearly now one is interested in representations leading to as little additions as possible (i.e. low Hamming weight). On average, about 1/2 of the pairs of digits are $\substack{0\\0}$ and thus require no extra addition. The reader is invited to consult the paper [5] and the references therein.

As indicated, representations of minimal Hamming weight are of interest. In [5], a special representation, termed *Simple Joint Sparse Form*, was introduced. It can be described e.g., by the two syntactic rules

- if $|x_j| \neq |y_j|$ then $|x_{j+1}| = |y_{j+1}|$,
- if $|x_j| = |y_j| = 1$ then $x_{j+1} = y_{j+1} = 0$.

Earlier, Solinas [14] had introduced the so called *Joint Sparse Form* (that is less simple) and characterised by another set of syntactic rules:

- of any three consecutive positions, at least one is double zero,
- if $x_j x_{j+1} \neq 0$ then $y_{j+1} = \pm1$ and $y_j = 0$,
- if $y_j y_{j+1} \neq 0$ then $x_{j+1} = \pm1$ and $x_j = 0$.

Both representations are minimal with respect to their Hamming weight. Another representation of minimal Hamming weight was introduced in the paper [6]. We will not repeat its definition here but only stress the important fact that it can be constructed from left-to-right by a transducer. This representation as well as the simple joint sparse form can be extended in a straight-forward way to d dimensions (instead of 2); details are given in [5]. Such representations can be used to compute *linear combinations* $n_1P_1+\cdots+n_dP_d$. In general, all these minimal representations are different, and there exist other ones. Thus, a natural question is to determine the *number of minimal representations*. The present article is devoted to the enumeration of optimal joint representations. Again, loosely speaking, it will turn out that most pairs of integers have many optimal representations. Precise formulations will come later in the paper.

Throughout the paper the norm $\|\cdot\|$ is the maximum norm.

2. Recognising minimum weight expansions

In [5] we gave an algorithm for computing the "Simple Joint Sparse Form" of an integer vector. This is a joint expansion of minimal weight. It can be implemented as a transducer automaton, which converts any signed binary expansions of two integers into this joint expansion (the transducer shown in [5] gives only the conversion from ordinary binary expansion, but can be extended). The general procedure described in [9, Remark 20] can be used to obtain an automaton recognising expansions of minimal weight. This procedure relies on the fact that optimal expansions correspond to shortest paths in the conversion transducer with edge-weights corresponding to the improvement of the Hamming weight. The resulting automaton is shown in Figure 1. We call expansions of $\mathbf{n}$ which minimise the Hamming weight over all possible expansions of $\mathbf{n}$ *minimal joint expansions* of $\mathbf{n}$.

We define the transition matrices $A^{(\boldsymbol{\varepsilon})}=(a_{i,j}^{(\boldsymbol{\varepsilon})})_{1\le i,j\le 21}$ with $\boldsymbol{\varepsilon}\in\{0,\pm1\}^2$ by setting

$$a_{i,j}^{(\boldsymbol{\varepsilon})}=\begin{cases}1, & \text{if there is a transition from state } i \text{ to state } j \text{ labelled with } \boldsymbol{\varepsilon},\\ 0, & \text{otherwise.}\end{cases}$$

By construction (cf. also Figure 1), these matrices satisfy the relation

$$A^{(\boldsymbol{\varepsilon})}\cdot(1,1,\ldots,1)^T\le(1,1,\ldots,1)^T, \tag{2.1}$$

where this inequality has to be interpreted component-wise.

The following fact will be used later.

Lemma 1 *Let $(\boldsymbol{\varepsilon}_L\cdots\boldsymbol{\varepsilon}_0)$ be a minimal joint expansion and $L\ge K\ge 0$. Then $(\boldsymbol{\varepsilon}_L\cdots\boldsymbol{\varepsilon}_K)$ and $(\boldsymbol{\varepsilon}_{K-1}\cdots\boldsymbol{\varepsilon}_0)$ are minimal joint expansions.*

Proof. Since $(\boldsymbol{\varepsilon}_L\cdots\boldsymbol{\varepsilon}_0)$ is a minimal joint expansion, there is a path in the automaton in Figure 1 from state 1 with this label. Since there is a path from every state to state 1 with

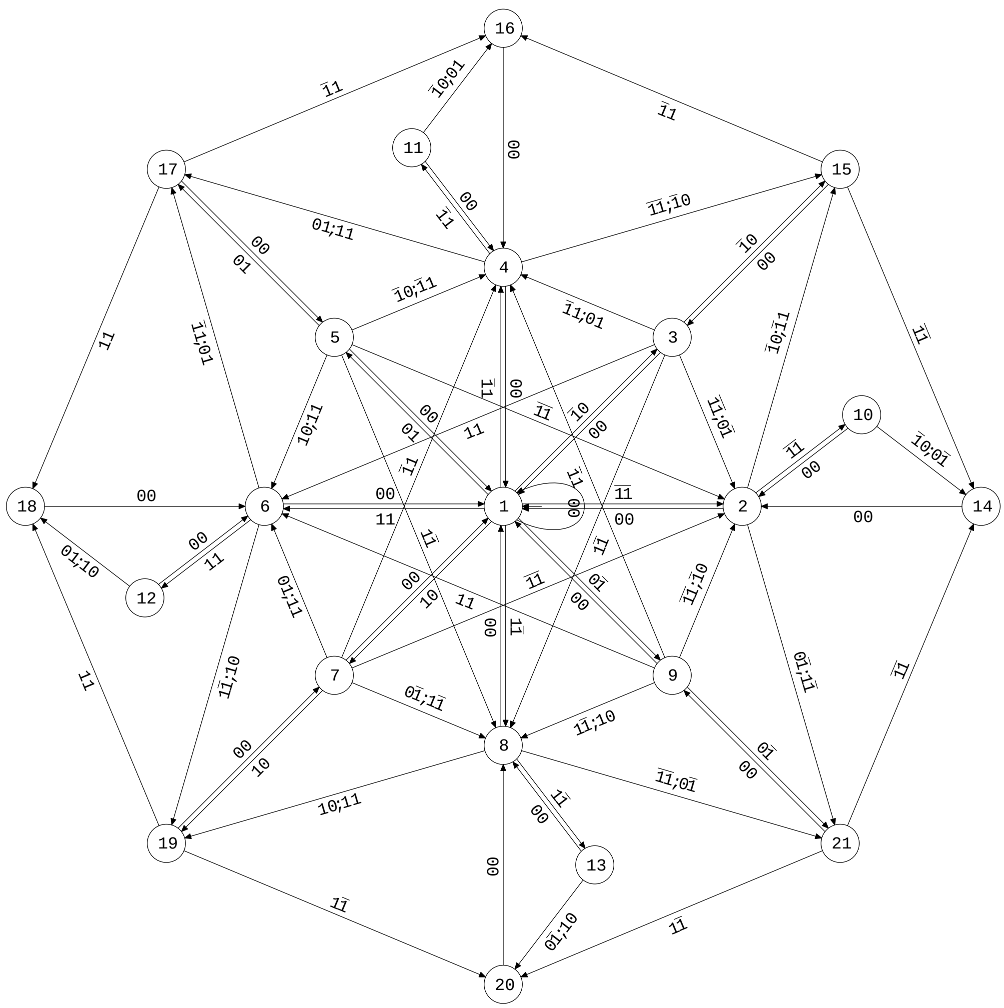

Figure 1: Automaton recognising joint expansions of minimum weight (initial state 1).

label $\mathbf{000}$, there is a path from state 1 to state 1 with input label $(\mathbf{000}\boldsymbol{\varepsilon}_{K-1}\cdots\boldsymbol{\varepsilon}_0)$, hence $(\boldsymbol{\varepsilon}_{K-1}\cdots\boldsymbol{\varepsilon}_0)$ is a minimal joint expansion.

Let $\mathbf{n} = \mathsf{value}(\boldsymbol{\varepsilon}_L\cdots\boldsymbol{\varepsilon}_K)$. If $(\boldsymbol{\varepsilon}_L\cdots\boldsymbol{\varepsilon}_K)$ was not a minimal joint expansion, then there would be a joint expansion $(\boldsymbol{\eta}_{L'}\cdots\boldsymbol{\eta}_K)$ of $\mathbf{n}$ of smaller Hamming weight. But this would imply that $(\boldsymbol{\eta}_{L'}\cdots\boldsymbol{\eta}_K\boldsymbol{\varepsilon}_{K-1}\cdots\boldsymbol{\varepsilon}_0)$ is a joint expansion of $\mathsf{value}(\boldsymbol{\varepsilon}_L\cdots\boldsymbol{\varepsilon}_0)$ of smaller joint Hamming weight than $(\boldsymbol{\varepsilon}_L\cdots\boldsymbol{\varepsilon}_0)$, which is a contradiction to the minimality of $(\boldsymbol{\varepsilon}_L\cdots\boldsymbol{\varepsilon}_0)$. Thus $(\boldsymbol{\varepsilon}_L\cdots\boldsymbol{\varepsilon}_K)$ is a minimal joint expansion, too. ☐

Lemma 2 *Let $\mathbf{n}\in\mathbb{Z}^2$ and $(\boldsymbol{\varepsilon}_K,\ldots,\boldsymbol{\varepsilon}_0)$ ($\boldsymbol{\varepsilon}_K\neq\mathbf{0}$) be an optimal expansion of $\mathbf{n}$. Then $K\in\{\lfloor\log_2\|\mathbf{n}\|\rfloor, \lfloor\log_2\|\mathbf{n}\|\rfloor+1\}$.*

Proof. We have

$$\|\mathbf{n}\| = \left\|\sum_{\ell=0}^{K}\boldsymbol{\varepsilon}_\ell 2^\ell\right\| \le \sum_{\ell=0}^{K}\|\boldsymbol{\varepsilon}_\ell\|2^\ell < 2^{K+1},$$

which yields $K\ge\lfloor\log_2\|\mathbf{n}\|\rfloor$.

For the opposite inequality we choose $L=\lfloor\log_2\|\mathbf{n}\|\rfloor$, set $\boldsymbol{\varepsilon}_\ell=0$ for $\ell>K$, and consider

$$\left\|\sum_{\ell=L+1}^{\infty}\boldsymbol{\varepsilon}_\ell 2^\ell\right\| \le \left\|\sum_{\ell=L+1}^{\infty}\boldsymbol{\varepsilon}_\ell 2^\ell - \mathbf{n}\right\| + \|\mathbf{n}\| < 2^{L+2}.$$

We conclude that $(\boldsymbol{\varepsilon}_K,\ldots,\boldsymbol{\varepsilon}_{L+1})$ is an optimal joint expansion of an integer vector $\mathbf{m}$ with $\|\mathbf{m}\|<2$. All these vectors have a joint expansion of weight at most 1, which is clearly optimal. If $\mathbf{m}\neq\mathbf{0}$ the non-zero column must be $\boldsymbol{\varepsilon}_{L+1}$. ☐

3. Counting frequencies

For an integer vector $\mathbf{n}$ the number of representations of minimal weight is denoted by $p(\mathbf{n})$. In the following we will study this quantity in detail. For technical purposes we define the functions $p_j(\mathbf{n})$ (for $j=1,\ldots,21$) as the number of paths in the automaton in Figure 1 from state j to state 1 with label $\boldsymbol{\varepsilon}_L\boldsymbol{\varepsilon}_{L-1}\cdots\boldsymbol{\varepsilon}_0$, with the additional requirement that $\mathbf{n}=\mathsf{value}(\boldsymbol{\varepsilon}_L\boldsymbol{\varepsilon}_{L-1}\cdots\boldsymbol{\varepsilon}_0)$. By construction of the automaton we have $p(\mathbf{n})=p_1(\mathbf{n})$.

From the definition of $p_j(\mathbf{n})$ and the transition matrices $A^{(\boldsymbol{\varepsilon})}$ we obtain the set of recurrence equations ($j = 1, \ldots, 21$)

$$\begin{aligned} p_j(2n_1, 2n_2) &= \sum_{\ell=1}^{21} a_{j,\ell}^{(0,0)} p_\ell(n_1, n_2) \\ p_j(2n_1+1, 2n_2) &= \sum_{\ell=1}^{21} a_{j,\ell}^{(1,0)} p_\ell(n_1, n_2) + \sum_{\ell=1}^{21} a_{j,\ell}^{(-1,0)} p_\ell(n_1+1, n_2) \\ p_j(2n_1, 2n_2+1) &= \sum_{\ell=1}^{21} a_{j,\ell}^{(0,1)} p_\ell(n_1, n_2) + \sum_{\ell=1}^{21} a_{j,\ell}^{(0,-1)} p_\ell(n_1, n_2+1) \\ p_j(2n_1+1, 2n_2+1) &= \sum_{\ell=1}^{21} a_{j,\ell}^{(1,1)} p_\ell(n_1, n_2) + \sum_{\ell=1}^{21} a_{j,\ell}^{(-1,1)} p_\ell(n_1+1, n_2) \\ &\quad + \sum_{\ell=1}^{21} a_{j,\ell}^{(1,-1)} p_\ell(n_1, n_2+1) + \sum_{\ell=1}^{21} a_{j,\ell}^{(-1,-1)} p_\ell(n_1+1, n_2+1). \end{aligned} \tag{3.1}$$

Note that by (2.1) all the sums $\sum_{\ell=1}^{21}$ in the above equations actually have only one non-zero term.

The following Lemma is of some interest on its own. We state without making further use of it.

Lemma 3 *Let* $\mathbf{n} \in \mathbb{Z}^2$ *and* $1 \le j \le 21$ *with* $p_j(\mathbf{n}) \neq 0$. *Then* $p_j(\mathbf{n}) = p_1(\mathbf{n})$.

Proof. Let $(\boldsymbol{\varepsilon}_L \cdots \boldsymbol{\varepsilon}_0)$ be the label of a path from state j to state 1 in the automaton in Figure 1 with $\mathsf{value}(\boldsymbol{\varepsilon}_L \cdots \boldsymbol{\varepsilon}_0) = \mathbf{n}$.

Since the automaton is strongly connected, there is a path from state 1 to state j with input label $(\boldsymbol{\eta}_K \cdots \boldsymbol{\eta}_0)$, say. Thus $(\boldsymbol{\varepsilon}_L \cdots \boldsymbol{\varepsilon}_0 \boldsymbol{\eta}_K \cdots \boldsymbol{\eta}_0)$ is the label of a path from state 1 to state 1 in the automaton, which implies that $(\boldsymbol{\varepsilon}_L \cdots \boldsymbol{\varepsilon}_0 \boldsymbol{\eta}_K \cdots \boldsymbol{\eta}_0)$ is a minimal joint expansion. From Lemma 1 we see that $(\boldsymbol{\varepsilon}_L \cdots \boldsymbol{\varepsilon}_0)$ is the label of a path from state 1 in the automaton. We conclude that $p_j(\mathbf{n}) \le p_1(\mathbf{n})$ and that $(\boldsymbol{\varepsilon}_L \cdots \boldsymbol{\varepsilon}_0)$ is a minimal joint expansion of $\mathbf{n}$.

Let now $(\boldsymbol{\varepsilon}'_{L'} \cdots \boldsymbol{\varepsilon}'_0)$ be some minimal joint expansion of $\mathbf{n}$, hence the joint Hamming weight of $(\boldsymbol{\varepsilon}'_{L'} \cdots \boldsymbol{\varepsilon}'_0)$ equals that of $(\boldsymbol{\varepsilon}_L \cdots \boldsymbol{\varepsilon}_0)$. This implies that $(\boldsymbol{\varepsilon}'_{L'} \cdots \boldsymbol{\varepsilon}'_0 \boldsymbol{\eta}_K \cdots \boldsymbol{\eta}_0)$ is a joint expansion of $\mathsf{value}(\boldsymbol{\varepsilon}_L \cdots \boldsymbol{\varepsilon}_0 \boldsymbol{\eta}_K \cdots \boldsymbol{\eta}_0)$ with the same joint Hamming weight as $(\boldsymbol{\varepsilon}_L \cdots \boldsymbol{\varepsilon}_0 \boldsymbol{\eta}_K \cdots \boldsymbol{\eta}_0)$. Thus $(\boldsymbol{\varepsilon}'_{L'} \cdots \boldsymbol{\varepsilon}'_0 \boldsymbol{\eta}_K \cdots \boldsymbol{\eta}_0)$ is the label of a path from state 1 too, which implies that $(\boldsymbol{\varepsilon}'_{L'} \cdots \boldsymbol{\varepsilon}'_0)$ is the label of a path from state j in the automaton. This shows that $p_1(\mathbf{n}) \le p_j(\mathbf{n})$ and finishes the proof of the lemma. □

Lemma 4 *The counting function of minimal expansions satisfies*

$$p(\mathbf{n}) = \mathcal{O}(\|\mathbf{n}\|^\gamma) \tag{3.2}$$

for $\gamma = \frac{1}{3}\log_2 \theta = 0.70555605477920029626\ldots$, *where* θ *is the positive root of the equation* $\theta^3 - 4\theta^2 - \theta - 2 = 0$. *The exponent* γ *is best possible.*

Proof. The proof will make use of the *Simple Joint Sparse Form* introduced in [5]. Here we only use its syntactic properties recalled in the introduction: every pair of integers $\mathbf{n}$ has a unique joint expansion satisfying the regular expression W^* with

$$W = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 & \pm 1 \\ 0 & \pm 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 & 0 \\ 0 & \pm 1 & \pm 1 \end{pmatrix} \right\},$$

where all signs can be chosen independently ($|W| = 25$). This representation allows to reduce the 84 functions $p_j(\mathbf{n} + \boldsymbol{\delta})$ occurring in (3.1) to the 9 functions contained in the vector

$$\begin{aligned} \mathbf{q}(\mathbf{n}) = \big(p_1(\mathbf{n}), p_{10}(\mathbf{n} + \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)), p_{11}(\mathbf{n} + \left(\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right)), p_{12}(\mathbf{n} + \left(\begin{smallmatrix} -1 \\ -1 \end{smallmatrix}\right)), p_{13}(\mathbf{n} + \left(\begin{smallmatrix} -1 \\ 1 \end{smallmatrix}\right)), \\ p_{15}(\mathbf{n} + \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)), p_{17}(\mathbf{n} + \left(\begin{smallmatrix} 0 \\ -1 \end{smallmatrix}\right)), p_{19}(\mathbf{n} + \left(\begin{smallmatrix} -1 \\ 0 \end{smallmatrix}\right)), p_{21}(\mathbf{n} + \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right))\big)^T. \end{aligned}$$

Indeed, for any $\mathbf{w} \in W$, there is a matrix $M_{\mathbf{w}}$ such that

$$\mathbf{q}(2^{|\mathbf{w}|}\mathbf{n} + \mathsf{value}(\mathbf{w})) = M_{\mathbf{w}}\mathbf{q}(\mathbf{n});$$

the matrices $M_{\mathbf{w}}$ can be computed using (3.1). Here, $|\mathbf{w}|$ denotes the length of the word $\mathbf{w}$. For instance, we have

$$M_{\left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 1 & -1 \end{smallmatrix}\right)} = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 & 3 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 2 \end{pmatrix}.$$

We note that $\mathbf{q}(\mathbf{0}) = \mathbf{v} = (1, 0, 0, 0, 0, 0, 0, 0, 0)^T$. From this observation it follows that

$$\mathbf{q}(\mathsf{value}(\mathbf{w}_L \mathbf{w}_{L-1} \cdots \mathbf{w}_0)) = M_{\mathbf{w}_L} M_{\mathbf{w}_{L-1}} \cdots M_{\mathbf{w}_0} \mathbf{v}.$$

It turns out that the matrices $M_{\mathbf{w}}$ lie in five orbits under the action of the group of permutation matrices. We write the matrices $M_{\mathbf{w}} = P_{\mathbf{w}} S_{R(\mathbf{w})} Q_{\mathbf{w}}^{-1}$ with certain permutation matrices $P_{\mathbf{w}}$ and $Q_{\mathbf{w}}$. The function R is given by

$$\begin{aligned} R\left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right) &= 0, \\ R\left(\begin{smallmatrix} 0 & -1 \\ 0 & 0 \end{smallmatrix}\right) = R\left(\begin{smallmatrix} 0 & 0 \\ 0 & -1 \end{smallmatrix}\right) = R\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) = R\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) &= 1, \\ R\left(\begin{smallmatrix} 0 & -1 \\ 0 & -1 \end{smallmatrix}\right) = R\left(\begin{smallmatrix} 0 & -1 \\ 0 & 1 \end{smallmatrix}\right) = R\left(\begin{smallmatrix} 0 & 1 \\ 0 & -1 \end{smallmatrix}\right) = R\left(\begin{smallmatrix} 0 & 1 \\ 0 & 1 \end{smallmatrix}\right) &= 2, \\ R\left(\begin{smallmatrix} 0 & -1 & -1 \\ 0 & -1 & 0 \end{smallmatrix}\right) = R\left(\begin{smallmatrix} 0 & -1 & 0 \\ 0 & -1 & -1 \end{smallmatrix}\right) = R\left(\begin{smallmatrix} 0 & -1 & -1 \\ 0 & 1 & 0 \end{smallmatrix}\right) = R\left(\begin{smallmatrix} 0 & -1 & 0 \\ 0 & 1 & 1 \end{smallmatrix}\right) &= 3, \\ R\left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & -1 & -1 \end{smallmatrix}\right) = R\left(\begin{smallmatrix} 0 & 1 & 1 \\ 0 & -1 & 0 \end{smallmatrix}\right) = R\left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \end{smallmatrix}\right) = R\left(\begin{smallmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right) &= 3, \\ R\left(\begin{smallmatrix} 0 & -1 & 0 \\ 0 & -1 & 1 \end{smallmatrix}\right) = R\left(\begin{smallmatrix} 0 & -1 & 1 \\ 0 & -1 & 0 \end{smallmatrix}\right) = R\left(\begin{smallmatrix} 0 & -1 & 0 \\ 0 & 1 & -1 \end{smallmatrix}\right) = R\left(\begin{smallmatrix} 0 & -1 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right) &= 4, \\ R\left(\begin{smallmatrix} 0 & 1 & -1 \\ 0 & -1 & 0 \end{smallmatrix}\right) = R\left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & -1 & 1 \end{smallmatrix}\right) = R\left(\begin{smallmatrix} 0 & 1 & -1 \\ 0 & 1 & 0 \end{smallmatrix}\right) = R\left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 1 & -1 \end{smallmatrix}\right) &= 4, \end{aligned}$$

and the matrices S_j are defined as

$$S_0 = \begin{pmatrix} 1&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0 \end{pmatrix}, \qquad S_1 = \begin{pmatrix} 1&0&0&0&0&0&0&1&0\\ 1&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0 \end{pmatrix}, \qquad S_2 = \begin{pmatrix} 1&1&0&0&0&2&0&2&0\\ 1&0&0&0&0&0&0&0&0\\ 0&1&0&0&0&1&0&1&0\\ 0&0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0 \end{pmatrix},$$

$$S_3 = \begin{pmatrix} 1&4&0&3&0&0&0&2&0\\ 1&2&0&2&0&0&0&1&0\\ 0&2&0&1&0&0&0&1&0\\ 0&1&0&1&0&0&0&1&0\\ 0&1&0&0&0&0&0&0&0\\ 0&1&0&1&0&0&0&1&0\\ 0&1&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0 \end{pmatrix}, \qquad S_4 = \begin{pmatrix} 2&3&0&2&0&0&0&1&0\\ 1&2&0&2&0&0&0&1&0\\ 1&1&0&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0 \end{pmatrix}.$$

Note that the characteristic polynomial of S_4 is $x^3 - 4x^2 - x - 2$ and θ is its dominant eigenvalue. Furthermore, we can choose the permutation matrices $P_{\mathbf{w}}$ and $Q_{\mathbf{w}}$ so that

$$\begin{aligned} &Q_{\left(\begin{smallmatrix}0&-1&0\\0&-1&1\end{smallmatrix}\right)} = P_{\left(\begin{smallmatrix}0&-1&1\\0&1&0\end{smallmatrix}\right)}, Q_{\left(\begin{smallmatrix}0&-1&1\\0&1&0\end{smallmatrix}\right)} = P_{\left(\begin{smallmatrix}0&1&0\\0&1&-1\end{smallmatrix}\right)}, Q_{\left(\begin{smallmatrix}0&1&0\\0&1&-1\end{smallmatrix}\right)} = P_{\left(\begin{smallmatrix}0&1&-1\\0&-1&0\end{smallmatrix}\right)}, Q_{\left(\begin{smallmatrix}0&1&-1\\0&-1&0\end{smallmatrix}\right)} = P_{\left(\begin{smallmatrix}0&-1&0\\0&-1&1\end{smallmatrix}\right)},\\ &Q_{\left(\begin{smallmatrix}0&-1&1\\0&-1&0\end{smallmatrix}\right)} = P_{\left(\begin{smallmatrix}0&1&0\\0&-1&1\end{smallmatrix}\right)}, Q_{\left(\begin{smallmatrix}0&1&0\\0&-1&1\end{smallmatrix}\right)} = P_{\left(\begin{smallmatrix}0&1&-1\\0&1&0\end{smallmatrix}\right)}, Q_{\left(\begin{smallmatrix}0&1&-1\\0&1&0\end{smallmatrix}\right)} = P_{\left(\begin{smallmatrix}0&-1&0\\0&1&-1\end{smallmatrix}\right)}, Q_{\left(\begin{smallmatrix}0&-1&0\\0&1&-1\end{smallmatrix}\right)} = P_{\left(\begin{smallmatrix}0&-1&1\\0&-1&0\end{smallmatrix}\right)}. \end{aligned}$$

This shows that

$$\mathbf{r}_k = \mathbf{q}\left(\mathsf{value}\left(\left(\begin{smallmatrix}0&-1&0&0&-1&1&0&1&0&0&1&-1\\0&-1&1&0&1&0&0&1&-1&0&-1&0\end{smallmatrix}\right)^k\right)\right) = P_{\left(\begin{smallmatrix}0&-1&0\\0&-1&1\end{smallmatrix}\right)} S_4^{4k} Q^{-1}_{\left(\begin{smallmatrix}0&1&-1\\0&-1&0\end{smallmatrix}\right)} \mathbf{v},$$

from which we deduce that $\|\mathbf{r}_k\| \gg \theta^{4k}$ and $\limsup_{\|\mathbf{n}\|\to\infty} p(\mathbf{n})\|\mathbf{n}\|^{-\gamma} > 0$.

For the upper bound we proceed by induction. For any $\mathbf{w} \in W^*$ we prove that for at least one of three consecutive values of ℓ the component-wise inequality

$$\mathbf{q}(\mathsf{value}(\mathbf{w}_\ell \mathbf{w}_{\ell-1} \cdots \mathbf{w}_0)) \leq C(\mathbf{w}_\ell)\theta^{|\mathbf{w}_\ell|+\cdots+|\mathbf{w}_0|} P^{-1}_{\mathbf{w}_\ell} \mathbf{v}_\theta$$

holds. Here $\mathbf{v}_\theta$ is the (Perron-Frobenius) eigenvector (with first component 1) associated to the eigenvalue θ of the matrix S_4 and

$$C(\mathbf{w}_\ell) = \begin{cases} \frac{9}{10} & \text{if } R(\mathbf{w}_\ell) = 1, \\ 1 & \text{otherwise.} \end{cases}$$

The proof of the induction step was performed by studying 4700 cases with `Mathematica`. This verification took 11 seconds. Certainly, this implies $p(\mathbf{n}) = \mathcal{O}(\|\mathbf{n}\|^\gamma)$. □

4. Construction of a measure

We define a sequence of measures, which reflect the distribution of $p(\mathbf{n})$. It turns out that it is easier to study a modified version of $p(\mathbf{n})$. We define $p^{(K)}(\mathbf{n})$ to be the number of joint expansions of minimal weight of $\mathbf{n}$ of length at most K. Lemma 2 implies that $p(\mathbf{n}) = p^{(K)}(\mathbf{n})$ for $K > \log_2 \|\mathbf{n}\| + 1$ and $p^{(K)}(\mathbf{n}) = 0$ for $K < \log_2 \|\mathbf{n}\|$.

$$\mu_K = \frac{1}{M_K} \sum_{\mathbf{n}\in\mathbb{Z}^2} p^{(K)}(\mathbf{n}) \delta_{2^{-K}\mathbf{n}}, \tag{4.1}$$

where $\delta_{\mathbf{x}}$ denotes the unit point mass concentrated in $\mathbf{x}$ and M_K is chosen such that μ_K has total mass 1. Note that the support of μ_K is contained in $[-1,1]^2$.

In order to derive an expression for the Fourier transform of μ_K, we introduce the matrix $A(\mathbf{t})$ by

$$A(\mathbf{t}) = \sum_{\boldsymbol{\varepsilon}\in\{0,\pm1\}^2} e\left(\langle \boldsymbol{\varepsilon}, \mathbf{t}\rangle\right) A^{(\boldsymbol{\varepsilon})},$$

where $e(x) = e^{2\pi i x}$ for $x \in \mathbb{R}$. Obviously, $A := A(\mathbf{0})$ is the adjacency matrix of the directed multigraph (cf. [1]) depicted in Figure 1. Furthermore, we observe that A is primitive. From this it follows immediately that

$$M_K = (1,0,\ldots,0)A^K(1,1,\ldots,1)^T = C\lambda^K + \mathcal{O}(|\lambda_2|^K), \tag{4.2}$$

where λ denotes the dominating and λ_2 the second largest eigenvalue of the matrix A. The characteristic polynomial factors as

$$(x-1)(x+1)(x^2-2x-1)^2(x^3-x-2)(x^3+2x^2+3x-2)^2(x^6-x^5-10x^4-56x^3+27x^2+33x-2).$$

The two largest eigenvalues are zeros of the sextic factor. Numerically, we have

$$\lambda = 4.98676981078412784 41\ldots, \quad |\lambda_2| = 3.46535078299054406 13\ldots. \tag{4.3}$$

The Fourier transform of μ_K is given by

$$\widehat{\mu}_K(\mathbf{t}) = \int_{\mathbb{R}^2} e\left(\langle \mathbf{x}, \mathbf{t}\rangle\right) d\mu_K(\mathbf{x}) = \frac{1}{M_K} \sum_{\mathbf{n}\in\mathbb{Z}^2} p^{(K)}(\mathbf{n}) e\left(2^{-K}\langle \mathbf{n}, \mathbf{t}\rangle\right). \tag{4.4}$$

Since $p^{(K)}(\mathbf{n})$ is the number of paths in the automaton of length K labelled with minimal representations of $\mathbf{n}$, we have

$$\widehat{\mu}_K(\mathbf{t}) = \frac{1}{M_K}(1,0,\ldots,0)A(2^{-K}\mathbf{t})A(2^{-(K-1)}\mathbf{t})\cdots A(2^{-1}\mathbf{t})(1,1,\ldots,1)^T. \tag{4.5}$$

Lemma 5 *Let $B(\mathbf{t})$ be a matrix function mapping real vectors $\mathbf{t}$ to square matrices satisfying*

$$\|B(\mathbf{t}) - B\| \le C\|\mathbf{t}\| \text{ for } \|t\| \le T, \tag{4.6}$$

$$|B_{i,j}(\mathbf{t})| \le B_{i,j} \text{ for all } i,j \tag{4.7}$$

for some $C, T > 0$, some non-negative matrix B, and the matrix norm $\|\cdot\|$ induced by the maximum norm on the vector space. Assume that B has a simple dominating eigenvalue 1 *and denote by ρ the modulus of the second largest eigenvalue and by r the size of the largest Jordan-block associated to an eigenvalue of modulus ρ. Then the sequence of matrices*

$$P_K(\mathbf{t}) = B(2^{-K}\mathbf{t})B(2^{-(K-1)}\mathbf{t})\cdots B(2^{-1}\mathbf{t})$$

converges to a limit $P(\mathbf{t})$ for all $\mathbf{t}$ and

$$\begin{aligned} \|P_K(\mathbf{t}) - P_K(\mathbf{0})\| &\ll \|\mathbf{t}\| \text{ for } \|\mathbf{t}\| \le 2T, \\ \|P(\mathbf{t}) - P_K(\mathbf{t})\| &\ll (1+\|\mathbf{t}\|)^\eta K^{r-1}2^{-\eta K} \text{ for all } \mathbf{t}, \end{aligned} \tag{4.8}$$

where $\eta = -\frac{\log\rho}{\log 2 - \log\rho}$.

Proof. By our assumptions on B there exists a constant $C_2 > 0$ such that $\|B^\ell\| \le C_2$ for all $\ell \ge 0$. For $\|\mathbf{t}\| \le 2T$ we have (setting $j_0 = K+1$)

$$\begin{aligned} \|P_K(\mathbf{t}) - P_K(\mathbf{0})\| &= \left\|(B + (B(2^{-K}\mathbf{t}) - B))\cdots(B + (B(2^{-1}\mathbf{t}) - B)) - B^K\right\| \\ &= \left\| \sum_{\ell=1}^{K} \sum_{K \ge j_1 > \cdots > j_\ell \ge 1} \left(\prod_{k=1}^{\ell} B^{j_{k-1}-j_k-1}(B(2^{-j_k}\mathbf{t}) - B) \right) B^{j_\ell - 1} \right\| \\ &\le \sum_{\ell=1}^{K} \sum_{K \ge j_1 > \cdots > j_\ell \ge 1} C_2^{\ell+1} C^\ell \|\mathbf{t}\|^\ell \prod_{k=1}^{\ell} 2^{-j_k} \\ &\le C_2 \sum_{\ell=1}^{K} \frac{1}{\ell!}(CC_2\|\mathbf{t}\|)^\ell \left(\sum_{j=1}^{K} 2^{-j} \right)^\ell \\ &\le C_2\left(\exp(CC_2\|\mathbf{t}\|) - 1\right) \le CC_2^2 \exp(2CC_2T)\|\mathbf{t}\|. \end{aligned}$$

Let $\|\mathbf{t}\| \le 2^{\ell+1}T$ and observe that (4.7) implies $\|P_\ell(\mathbf{t})\| \le \|B^\ell\| \le C_2$. Then we have for $K > L > \ell$

$$\begin{aligned} \|P_K(\mathbf{t}) - P_L(\mathbf{t})\| &= \|P_{K-\ell}(2^{-\ell}\mathbf{t})P_\ell(\mathbf{t}) - P_{L-\ell}(2^{-\ell}\mathbf{t})P_\ell(\mathbf{t})\| \\ &\le \|B^\ell\|\left(\|P_{K-\ell}(2^{-\ell}\mathbf{t}) - P_{K-\ell}(\mathbf{0})\| + \|P_{K-\ell}(\mathbf{0}) - P_{L-\ell}(\mathbf{0})\| + \|P_{L-\ell}(2^{-\ell}\mathbf{t}) - P_{L-\ell}(\mathbf{0})\|\right) \\ &\le C_2\left(2CC_2^2\exp(2CC_2T)\,2^{-\ell}\|\mathbf{t}\| + C_3L^{r-1}\rho^{L-\ell}\right), \end{aligned} \tag{4.9}$$

where C_3 is a suitable constant coming from the Jordan decomposition of B. Choosing $\ell = \lceil \eta L \rceil$ we get

$$\|P_K(\mathbf{t}) - P_L(\mathbf{t})\| \ll (1+\|\mathbf{t}\|)2^{-\eta L}L^{r-1}. \tag{4.10}$$

Therefore, the sequence $(P_K(\mathbf{t}))_K$ converges uniformly on compact subsets.

For $\|\mathbf{t}\| \ge 1$ we choose $\ell = \lceil (1-\eta)\log_2\|\mathbf{t}\| + \eta L \rceil$ in (4.9) to obtain

$$\|P_K(\mathbf{t}) - P_L(\mathbf{t})\| \ll \|\mathbf{t}\|^\eta L^{r-1}2^{-\eta L}. \tag{4.11}$$

Combining this with (4.10) gives (4.8).

□

Lemma 6 *The sequence of measures μ_K defined by (4.1) converges weakly to a probability measure μ. The characteristic functions satisfy the estimate*

$$|\widehat{\mu}_K(\mathbf{t}) - \widehat{\mu}(\mathbf{t})| = \mathcal{O}(\|\mathbf{t}\|^{\eta} 2^{-\eta K}) \tag{4.12}$$

with

$$\eta = \frac{\log \lambda - \log |\lambda_2|}{\log 2 + \log \lambda - \log |\lambda_2|} = 0.3443071023441693011\ldots.$$

The constants implied by the $\mathcal{O}$-symbol are absolute.

Proof. We apply Lemma 5 to $B(\mathbf{t}) = \frac{1}{\lambda} A(\mathbf{t})$ and $T = 1$. From (4.2), (4.5), and (4.8) we obtain for $L > K$ and $\|\mathbf{t}\| \geq 1$ that

$$|\widehat{\mu}_K(\mathbf{t}) - \widehat{\mu}_L(\mathbf{t})| \ll \|\mathbf{t}\|^{\eta} 2^{-\eta K} + \left(\frac{|\lambda_2|}{\lambda}\right)^K \ll \|\mathbf{t}\|^{\eta} 2^{-\eta K}.$$

For $L > K > \ell$, $\|\mathbf{t}\| \leq 1$, $v_1 = (1, 0, \ldots, 0)^T$, and $v_2 = (1, 1, \ldots, 1)^T$ we have by (4.2) and (4.8)

$$\begin{aligned}
|\widehat{\mu}_K(\mathbf{t}) - \widehat{\mu}_L(\mathbf{t})| &= \left| \frac{\lambda^K}{M_K} v_1^T P_{K-\ell}(2^{-\ell}\mathbf{t}) P_\ell(\mathbf{t}) v_2 - \frac{\lambda^L}{M_L} v_1^T P_{L-\ell}(2^{-\ell}\mathbf{t}) P_\ell(\mathbf{t}) v_2 \right| \\
&\ll \left| \frac{\lambda^K}{M_K} v_1^T P_{K-\ell}(\mathbf{0}) P_\ell(\mathbf{t}) v_2 - \frac{\lambda^L}{M_L} v_1^T P_{L-\ell}(\mathbf{0}) P_\ell(\mathbf{t}) v_2 \right| + 2^{-\ell}\|\mathbf{t}\| \\
&= \left| \frac{\lambda^K}{M_K} v_1^T P_{K-\ell}(\mathbf{0}) (P_\ell(\mathbf{t}) - P_\ell(\mathbf{0})) v_2 - \frac{\lambda^L}{M_L} v_1^T P_{L-\ell}(\mathbf{0}) (P_\ell(\mathbf{t}) - P_\ell(\mathbf{0})) v_2 \right| \qquad (4.13) \\
&\qquad + 2^{-\ell}\|\mathbf{t}\| \\
&\ll \|\mathbf{t}\| \left(\left(\frac{|\lambda_2|}{\lambda} \right)^{K-\ell} + 2^{-\ell} \right) \ll \|\mathbf{t}\| 2^{-\eta K},
\end{aligned}$$

where we used the fact $\widehat{\mu}_K(0) = \widehat{\mu}_L(0) = 1$ in (4.13) and we chose $\ell = \lceil \eta K \rceil$. Thus $\widehat{\mu}_K(\mathbf{t})$ converges uniformly on compact subsets of $\mathbb{R}^2$ to a continuous limit $\widehat{\mu}(\mathbf{t})$, and the measures μ_K tend to a measure μ weakly. □

Lemma 7 *For $\mathbf{x} \leq \mathbf{y}$ the measure μ satisfies*

$$\mu([\mathbf{x}, \mathbf{y}]) = \mathcal{O}(\|\mathbf{y} - \mathbf{x}\|^{\beta}), \tag{4.14}$$

where $\beta = \log_2 \lambda - \gamma = 1.6125495549804366828\ldots$, where $\gamma = 0.705556\ldots$ is defined in Lemma 4. (as usual $[\mathbf{x}, \mathbf{y}]$ denotes the rectangle with lower left corner $\mathbf{x}$ and upper right corner $\mathbf{y}$.)

Proof. Without loss of generality, we may assume that $\|\mathbf{y}-\mathbf{x}\| < 1/2$ and $\|\mathbf{x}\|, \|\mathbf{y}\| \leq 1$. We choose $n \in \mathbb{N}$ such that

$$2^{-n-1} \leq \|\mathbf{y}-\mathbf{x}\| < 2^{-n}. \tag{4.15}$$

Then $[\mathbf{x}, \mathbf{y}]$ can be covered by 4 squares of the type $[2^{-n}\mathbf{a}, 2^{-n}(\mathbf{a}+\mathbf{1})]$, where $\mathbf{a} \in \mathbb{Z}^2$ and $\mathbf{1} = (1,1)^T$. For $K > n$ we obtain

$$\mu_K([2^{-n}\mathbf{a}, 2^{-n}(\mathbf{a}+\mathbf{1})]) = \frac{1}{M_K} \sum_{\mathbf{0}\leq\mathbf{k}\leq 2^{K-n}\mathbf{1}} p^{(K)}(2^{K-n}\mathbf{a}+\mathbf{k}).$$

If $\sum_{\ell=0}^{L} 2^\ell \boldsymbol{\varepsilon}_\ell$ is a minimal joint expansion of $2^{K-n}\mathbf{a}+\mathbf{k}$ then there is a $\boldsymbol{\delta} \in \{0, \pm 1\}^2$ such that $\sum_{\ell=0}^{K-n-1} 2^\ell \boldsymbol{\varepsilon}_\ell$ is a minimal expansion of $\mathbf{k} - 2^{K-n}\boldsymbol{\delta}$ and $\sum_{\ell=0}^{L-K+n} 2^\ell \boldsymbol{\varepsilon}_{\ell+K-n}$ is a minimal expansion of $\mathbf{a}+\boldsymbol{\delta}$ by Lemma 1. Therefore we have

$$\begin{aligned}\mu_K([2^{-n}\mathbf{a}, 2^{-n}(\mathbf{a}+\mathbf{1})]) &\leq \frac{1}{M_K} \sum_{\boldsymbol{\delta}\in\{0,\pm1\}^2} p(\mathbf{a}+\boldsymbol{\delta}) \sum_{\mathbf{0}\leq\mathbf{k}\leq 2^{K-n}\mathbf{1}} p(\mathbf{k}-2^{K-n}\boldsymbol{\delta}) \\ &\ll \|\mathbf{a}\|^\gamma \frac{1}{M_K} \sum_{-2^{K-n}\mathbf{1}\leq\mathbf{k}\leq 2^{K+1-n}\mathbf{1}} p(\mathbf{k}) \ll \|\mathbf{a}\|^\gamma \frac{M_{K-n+2}}{M_K} \ll \left(\frac{2^\gamma}{\lambda}\right)^n.\end{aligned}$$

A standard argument allows the limit $K \to \infty$. Combining this with (4.15) gives the assertion of the lemma. □

Lemma 8 *Let $B(\mathbf{0}, r)$ denote the Euclidean ball of radius r centred at the origin. Then*

$$\mu(B(\mathbf{0}, r+\varepsilon) \setminus B(\mathbf{0}, r)) \ll (r+\varepsilon)\varepsilon^{\beta-1}. \tag{4.16}$$

Proof. We need at most 4^n times the area of the annulus $B(\mathbf{0}, r+\varepsilon+\sqrt{2}\cdot 2^{-n}) \setminus B(\mathbf{0}, r-\sqrt{2}\cdot 2^{-n})$ squares of side-length 2^{-n} to cover the annulus $B(\mathbf{0}, r+\varepsilon) \setminus B(\mathbf{0}, r)$. From (4.14) we get

$$\mu(B(\mathbf{0}, r+\varepsilon) \setminus B(\mathbf{0}, r)) \ll 2^{-n\beta} 4^n \pi (2r+\varepsilon)(\varepsilon + 2\sqrt{2}\cdot 2^{-n}).$$

Choosing $n = -\lceil \log_2 \varepsilon \rceil$ we get

$$\mu(B(\mathbf{0}, r+\varepsilon) \setminus B(\mathbf{0}, r)) \ll 2^{(2-\beta)n}(r+\varepsilon)\varepsilon \ll (r+\varepsilon)\varepsilon^{\beta-1}.$$

□

As a first consequence of the weak convergence of the measures μ_K (Lemma 6) and the estimate for the measure-dimension (Lemma 7) we formulate the following theorem. In Section 6 we will give an explicit estimate for the error term, if $V = B(\mathbf{0}, 1)$.

Theorem 1 *Let V be a bounded measurable subset of $\mathbb{R}^2$ with $\mu(\partial(t\cdot V)) = 0$ for all $t \in \mathbb{R}^+$. Assume further that $t \mapsto \mu(t\cdot V)$ is monotonically increasing and there exists a $T > 0$ such that $[-1,1]^2 \subset t\cdot V$ for $t > T$. Then*

$$\sum_{\mathbf{n}\in N\cdot V} p(\mathbf{n}) = N^{\log_2 \lambda} F_V(\log_2 N)(1+o(1)), \tag{4.17}$$

where F_V *is a continuous periodic function of period* 1 *depending on the set* V *and* $\lambda = 4.9867698107841278441\ldots$ *is the largest root of*

$$x^6 - x^5 - 10x^4 - 56x^3 + 27x^2 + 33x - 2 = 0.$$

Remark 1 Examples for sets satisfying the first hypothesis of Theorem 1 are sets whose boundary has Hausdorff dimension $< \beta = 1.6125\ldots$ (cf. 7), for instance convex sets. The second condition is satisfied, if $t_1 \cdot V \subset t_2 \cdot V$ for $t_1 < t_2$. The third condition is satisfied, if V contains a neighbourhood of the origin.

Proof. The proof uses standard arguments from the theory of uniform distribution, especially the notion of discrepancy, as discussed in the classical book [12, Chapters 2,3].

By weak convergence of the measures μ_K to the limit μ and our assertions on the set V, we have for every fixed $t \in \mathbb{R}^+$

$$\lim_{K\to\infty} \mu_K(t \cdot V) = \mu(t \cdot V).$$

We need uniformity in t in this limit relation. By our assumptions on V the function $\mu(t\cdot V)$ is continuous. For a fixed positive integer m there exist $t_k \in \mathbb{R}^+$ $(k = 0, \ldots, m)$ such that $\mu(t_k \cdot V) = \frac{k}{m}$. There exists a K_0 such that

$$\left(1 - \frac{1}{m}\right) \mu(t_k \cdot V) \le \mu_K(t_k \cdot V) \le \left(1 + \frac{1}{m}\right) \mu(t_k \cdot V)$$

for all $K \ge K_0$ and $k = 1, \ldots, m$. Let $t \in \mathbb{R}^+$ then there exists an integer k such that $t_k \le t < t_{k+1}$ (or $\mu(t \cdot V) = 1$). Then we have

$$\left(1 - \frac{1}{m}\right) \mu(t_k \cdot V) \le \mu_K(t \cdot V) \le \left(1 + \frac{1}{m}\right) \mu(t_{k+1} \cdot V)$$

and therefore $|\mu_K(t \cdot V) - \mu(t \cdot V)| \le \frac{3}{m}$ for $K \ge K_0$. Thus $\mu_K(t \cdot V)$ tends to $\mu(t \cdot V)$ uniformly in t.

We conclude the proof by writing

$$\sum_{\mathbf{n}\in N\cdot V} p(\mathbf{n}) = M_K \mu_K(2^{-K} N \cdot V) = C\lambda^K (1 + o(1))(\mu(2^{-K} N \cdot V) + o(1))$$

for $K = \lfloor \log_2 N \rfloor + R$, where the integer R is chosen large enough to ensure $2^{-R} \cdot V \subset [-\frac{1}{2}, \frac{1}{2}]$. Setting

$$F_V(t) = C\lambda^{R-t} \mu(2^{t-R} \cdot V) \text{ for } 0 \le t < 1$$

and extending F_V periodically we obtain (4.17). $\square$

5. Berry-Esseen bounds

This section is devoted to a precise study of the error term in Theorem 1 for $V = B(\mathbf{0}, 1)$. We use the notation $\mathbf{c}(\phi) = (\cos\phi, \sin\phi)^T$.

Proposition 1 *Let ν_1 and ν_2 be two probability measures in $\mathbb{R}^2$ with their Fourier transforms defined by*

$$\widehat{\nu}_k(\mathbf{t}) = \int_{\mathbb{R}^2} e\left(\langle \mathbf{x}, \mathbf{t}\rangle\right) d\nu_k(\mathbf{x}).$$

Suppose that ν_2 satisfies

$$\nu_2\left(B(\mathbf{0}, r+\varepsilon) \setminus B(\mathbf{0}, r)\right) \ll \varepsilon^\theta \tag{5.1}$$

for some $0 < \theta < 1$ and all $r \geq 0$. Then the following inequality holds for all $r \geq 0$ and $T > 0$

$$|\nu_1(B(\mathbf{0}, r)) - \nu_2(B(\mathbf{0}, r))| \ll \int_0^T \int_0^{2\pi} K_r(t, T) \left|\widehat{\nu}_1(t\mathbf{c}(\phi)) - \widehat{\nu}_2(t\mathbf{c}(\phi))\right| t \, d\phi \, dt + T^{-\frac{2\theta}{\theta+2}}, \tag{5.2}$$

where the kernel function $K_r(t, T)$ satisfies

$$K_r(t, T) \ll \frac{1}{T^2} + \min\left(r^2, \frac{r^{\frac{1}{2}}}{t^{\frac{3}{2}}}\right).$$

The implied constant in (5.2) depends only on the implied constant in (5.1).

Proof. The proof makes use of ideas developed in [10] as an extension of the Beurling-Selberg extremal functions. We will use a more explicit version as given in [7].

From [7, Lemma 2] we infer the existence of two even entire functions G_1 and G_2 of exponential type T, which satisfy

$$G_1(x) \leq \chi_{[-r,r]}(x) \leq G_2(x) \text{ and } G_2(x) - G_1(x) \ll \min\left(1, T^{-2}|x - r|^{-2}\right) \tag{5.3}$$

for all $x \in \mathbb{R}$. By the Paley-Wiener theorem the Fourier transform of $U_j(\mathbf{x}) = G_j(\|\mathbf{x}\|_2)$ $(j = 1, 2)$ is supported on the ball of radius T. Furthermore, by [7, (3.8)] we have

$$\widehat{U}_j(\mathbf{t}) \ll \left(\frac{1}{T^2} + \min\left(r^2, \frac{r^{\frac{1}{2}}}{\|\mathbf{t}\|_2^{\frac{3}{2}}}\right)\right).$$

We use the functions U_j to estimate

$$\begin{aligned}
\nu_2(B(\mathbf{0}, r)) - \nu_1(B(\mathbf{0}, r)) &= \chi_{B(\mathbf{0},r)} \star \nu_2(\mathbf{0}) - \chi_{B(\mathbf{0},r)} \star \nu_1(\mathbf{0}) \leq U_2 \star \nu_2(\mathbf{0}) - U_1 \star \nu_1(\mathbf{0}) \\
&= U_1 \star (\nu_2 - \nu_1)(\mathbf{0}) + (U_2 - U_1) \star \nu_2(\mathbf{0}) \\
&= \int_{\|\mathbf{t}\|_2 \leq T} \widehat{U}_1(\mathbf{t})(\widehat{\nu}_2(\mathbf{t}) - \widehat{\nu}_1(\mathbf{t})) \, d\mathcal{L}(\mathbf{t}) + \int_{\mathbb{R}^2} (U_2(\mathbf{x}) - U_1(\mathbf{x})) \, d\nu_2(\mathbf{x}),
\end{aligned}$$

where $\star$ is the convolution on $\mathbb{R}^2$ and $\mathcal{L}$ denotes the two-dimensional Lebesgue measure. Analogously the inequality

$$\nu_2(B(\mathbf{0},r)) - \nu_1(B(\mathbf{0},r)) \geq \int\limits_{\|\mathbf{t}\|_2\leq T} \widehat{U}_2(\mathbf{t})(\widehat{\nu}_2(\mathbf{t}) - \widehat{\nu}_1(\mathbf{t}))\, d\mathcal{L}(\mathbf{t}) - \int\limits_{\mathbb{R}^2} (U_2(\mathbf{x}) - U_1(\mathbf{x}))\, d\nu_2(\mathbf{x})$$

Setting $K_r(\|\mathbf{t}\|_2, T) = \max(|\widehat{U}_1(\mathbf{t})|, |\widehat{U}_2(\mathbf{t})|)$ (notice that $\widehat{U}_j$ only depends on $\|\mathbf{t}\|_2$) and transforming the integral to polar coordinates yields the first summand in (5.2).

We now estimate the integral $\int_{\mathbb{R}^2}(U_2(\mathbf{x}) - U_1(\mathbf{x}))\, d\nu_2(\mathbf{x})$ by applying (5.3). This yields

$$\begin{aligned}
&\int_{\mathbb{R}^2} (U_2(\mathbf{x}) - U_1(\mathbf{x}))\, d\nu_2(\mathbf{x}) \\
&\ll \int\limits_{B(\mathbf{0},r+\varepsilon)\setminus B(\mathbf{0},r-\varepsilon)} d\nu_2(\mathbf{x}) + \int\limits_{\|\mathbf{x}\|_2\leq r-\varepsilon} \frac{1}{T^2(r-\|\mathbf{x}\|_2)^2}\, d\nu_2(\mathbf{x}) + \int\limits_{\|\mathbf{x}\|_2\geq r+\varepsilon} \frac{1}{T^2(\|\mathbf{x}\|_2-r)^2}\, d\nu_2(\mathbf{x}) \\
&\ll \varepsilon^\theta + \frac{1}{T^2\varepsilon^2}.
\end{aligned}$$

Choosing $\varepsilon = T^{-\frac{2}{\theta+2}}$ gives the second summand in (5.2). □

6. Average frequency in large circles

In this section we prove

Theorem 2 *Let $p(\mathbf{n})$ denote the number of joint expansions of minimal weight of $\mathbf{n} \in \mathbb{Z}^2$. Then the following asymptotic formula holds*

$$\sum_{\|\mathbf{n}\|_2<N} p(\mathbf{n}) = N^{\log_2 \lambda} F(\log_2 N) + \mathcal{O}(N^{\log_2 \lambda - 0.1229}), \tag{6.1}$$

where $\lambda = 4.9867698107841278441\ldots$ is the largest root of

$$x^6 - x^5 - 10x^4 - 56x^3 + 27x^2 + 33x - 2 = 0$$

and F is a continuous periodic function of period 1.

Proof. By Lemma 2 and the definition of the measures μ_K we write

$$\sum_{\|\mathbf{n}\|_2<N} p(\mathbf{n}) = M_K \mu_K(B(\mathbf{0}, N2^{-K})) \tag{6.2}$$

for $N < 2^{K-1}$.

Applying Proposition 1 to the measures μ_K and μ and using Lemmas 6 and 8 we get for $r < 1$

$$|\mu_K(B(\mathbf{0},r)) - \mu(B(\mathbf{0},r))| \ll \int_0^T K_r(t,T)t^\eta 2^{-\eta K} t\,dt + T^{-2\frac{\beta-1}{\beta+1}}.$$

Choosing

$$\log_2 T = \frac{\eta}{\eta + \frac{1}{2} + \frac{2(\beta-1)}{\beta+1}} K$$

yields

$$|\mu_K(B(\mathbf{0},r)) - \mu(B(\mathbf{0},r))| \ll 2^{-\xi K} \tag{6.3}$$

with

$$\xi = \frac{4\eta(\beta-1)}{2\eta\beta + 2\eta + 5\beta - 2} = 0.1229447532612942498\ldots.$$

Inserting (6.3) and (4.2) into (6.2) yields

$$\sum_{\|\mathbf{n}\|_2 < N} p(\mathbf{n}) = C\lambda^K \mu(B(\mathbf{0}, N2^{-K})) + \mathcal{O}(\lambda_2^K) + \mathcal{O}(\lambda^K 2^{-\xi K}).$$

Setting $K = \lfloor \log_2 N \rfloor + 2$ and $F(t) = C\lambda^{2-t}\mu(B(\mathbf{0}, 2^{t-2}))$ we obtain the assertion of the theorem. □

7. Purity of the measure

In this section we study the measure μ introduced in Section 4 in further detail. In particular, we show that it is purely singular continuous. As it is the case for Bernoulli convolutions (cf. [3]) the measure turns out to be pure as a consequence of the Jessen-Wintner theorem.

Lemma 9 ([11, Theorem 35], [2, Lemma 1.22 (ii)]) *Let $Q = \prod_{n=0}^\infty Q_n$ be an infinite product of discrete spaces equipped with a measure ν, which satisfies Kolmogorov's* 0-1-*law (i.e. every tail event has either measure* 0 *or* 1*). Furthermore, let X_n be a sequence of random variables defined on the spaces Q_n, such that the series $X = \sum_{n=0}^\infty X_n$ converges ν-almost everywhere. Then the distribution of X is either purely discrete, or purely singular continuous, or absolutely continuous with respect to Lebesgue measure.*

Remark 2 We notice that in [2] and [11] the additional assumption of mutual independence of the random variables X_n is made in the statement of the result instead of the 0-1-law. The proofs however only depend on the 0-1-law.

We define the measure ν on the space

$$\mathcal{K} = \left\{(\mathbf{x}_1, \mathbf{x}_2, \ldots) \in (\{0, \pm 1\}^2)^{\mathbb{N}} \mid \forall n \in \mathbb{N} : (\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n) \text{ is an optimal expansion}\right\}$$

by

$$\nu([\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_n]) = \lim_{k\to\infty}\frac{1}{M_k}\#\left(\{(\mathbf{x}_1,\ldots,\mathbf{x}_k)\text{ is optimal}\}\cap[\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_n]\right),$$

where

$$[\boldsymbol{\varepsilon}_1,\ldots,\boldsymbol{\varepsilon}_n] = \{(\mathbf{x}_1,\mathbf{x}_2,\ldots)\in\mathcal{K}\mid \mathbf{x}_1=\boldsymbol{\varepsilon}_1,\ldots,\mathbf{x}_n=\boldsymbol{\varepsilon}_n\}.$$

We notice that the measure μ studied in Section 4 is the image of ν under the map $(\mathbf{x}_1,\mathbf{x}_2,\ldots)\mapsto\sum_{n=1}^{\infty}2^{-n}\mathbf{x}_n$. Furthermore, the same arguments as used in [4] show that $(\mathbf{x}_n)_{n\in\mathbb{N}}$ form a mixing sequence of random variables and ν therefore satisfies a 0-1-law. Thus the measure μ is pure by Lemma 9 and by Lemma 7 it is continuous.

In order to compute $\widehat{\mu}(2^k(1,1))$, we identify the constants C, C_2 and C_3 for our special choice of B in the proof of Lemma 5:

$$C = 76,\quad C_2 = C_3 = 23.1.$$

Inserting $T = 2^{-10}$, $\ell = 100$ and $L = 200$ into (4.9) we obtain

$$\|P(1,1) - P_{200}(1,1)\| \le 10^{-10}.$$

As in [4] we observe that

$$\widehat{\mu}(2^k(1,1)) = \lim_{n\to\infty} v_1^T\frac{\lambda^n}{M_n}P_n(2^k(1,1))v_2 = \lim_{n\to\infty} v_1^T\frac{\lambda^{n-k}}{M_n}P_{n-k}(1,1)A(\mathbf{0})^k v_2.$$

Since $\lim_{n\to\infty}P_{n-k}(1,1)$ can be computed by the above estimate, and $\lim_{k\to\infty}\lambda^{-k}A(\mathbf{0})^k$ can be computed by an eigenvector computation, we are able to compute

$$\lim_{k\to\infty}\widehat{\mu}(2^k(1,1)) = -0.0393555\ldots,$$

which shows that μ is not absolutely continuous. Thus we have proved the following theorem.

Theorem 3 *The measure μ defined in Lemma 6 is purely singular continuous.*

8. Higher dimensions

Specific higher dimensional joint expansions of minimal weight have been introduced and studied in [5, 8, 13]. The arguments and methods used in the present paper could also be used for dimensions $d \ge 3$:

- the automata can be produced by the same algorithm; for $d = 3$ the automaton has 109 states and maximal eigenvalue $11.9496\ldots$, for $d = 4$ it has 577 states and maximal eigenvalue 29.379.
- Lemmas 1, 2, and 3, are still true in higher dimensions.

- an analogue to Lemma 4 can be given by the same arguments; however, the computational effort can be expected to be immense. The value of γ cannot be predicted.

- Assuming the strong connectivity of the automaton the construction of the measures μ_K as well as their weak convergence to a limit μ can be carried out as in Section 4. If the value of the exponent γ in Lemma 4 is small enough and therefore β in Lemma 7 is large enough, the arguments in Section 6 can be used to compute the average frequency in large Euclidean balls.

References

[1] R. Diestel, *Graph theory*, second ed., Graduate Texts in Mathematics, vol. 173, Springer-Verlag, New York, 2000.

[2] P. D. T. A. Elliott, *Probabilistic number theory. I, mean-value theorems*, Grundlehren der Mathematischen Wissenschaften, vol. 239, Springer-Verlag, New York, 1979.

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

[4] P. J. Grabner and C. Heuberger, *On the number of optimal base 2 representations of integers*, submitted, available at `http://www.opt.math.tu-graz.ac.at/~cheub/publications/countminimal.pdf`, 2005.

[5] P. J. Grabner, C. Heuberger, and H. Prodinger, *Distribution results for low-weight binary representations for pairs of integers*, Theor. Comput. Sci. **319** (2004), 307–331.

[6] P. J. Grabner, C. Heuberger, H. Prodinger, and J. Thuswaldner, *Analysis of linear combination algorithms in cryptography*, Transactions on Algorithms, to appear.

[7] G. Harman, *On the Erdős-Turán inequality for balls*, Acta Arith. **85** (1998), 389–396.

[8] C. Heuberger, R. Katti, H. Prodinger, and X. Ruan, *The alternating greedy expansion and applications to left-to-right algorithms in cryptography*, Preprint, available at `http://www.opt.math.tu-graz.ac.at/~cheub/publications/alg1.pdf`, 2004.

[9] C. Heuberger and H. Prodinger, *Analysis of alternative digit sets for nonadjacent representations*, Preprint, available at `http://www.opt.math.tu-graz.ac.at/~cheub/publications/dnaf-1.pdf`.

[10] J. J. Holt and J. D. Vaaler, *The Beurling-Selberg extremal functions for a ball in Euclidean space*, Duke Math. J. **83** (1996), 202–248.

[11] B. Jessen and A. Wintner, *Distribution functions and the Riemann zeta function*, Trans. Amer. Math. Soc. **38** (1935), 48–88.

[12] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley-Interscience, New York, 1974.

[13] J. Proos, *Joint sparse forms and generating zero columns when combing*, Tech. Report CORR 2003-23, Centre for Applied Cryptographic Research, 2003, available at `http://www.cacr.math.uwaterloo.ca/techreports/2003/corr2003-23.ps`.

[14] J. A. Solinas, *Low-weight binary representations for pairs of integers*, Tech. Report CORR 2001-41, University of Waterloo, 2001, available at `http://www.cacr.math.uwaterloo.ca/techreports/2001/corr2001-41.ps`.