DISTRIBUTION RESULTS FOR LOW-WEIGHT BINARY REPRESENTATIONS FOR PAIRS OF INTEGERS

PETER J. GRABNER[†], CLEMENS HEUBERGER[‡], AND HELMUT PRODINGER[*]

Abstract. We discuss an optimal method for the computation of linear combinations of elements of Abelian groups, which uses signed digit expansions. This has applications in elliptic curve cryptography. We compute the expected number of operations asymptotically (including a periodically oscillating second order term) and prove a central limit theorem. Apart from the usual right-to-left (i.e., least significant digit first) approach we also discuss a left-to-right computation of the expansions. This exhibits fractal structures that are studied in some detail.

1. Introduction

In several well-known cryptosystems the essential operation is the computation of multiples and linear combinations in an Abelian group law. We discuss the second operation in a context, where subtraction and addition are equally costly. The most prominent example for this situation is the group law on an elliptic curve.

The standard method to compute a multiple nP is the *binary method*, see [16]. It uses the operations double and add P. If one writes n in binary notation, the ones correspond to these addition operations. In our context the subtraction of P is not more costly than the addition of P. This leads to the concept of redundant expansions. Now, the possible digits are $\{0, \pm 1\}$, and -1 corresponds to a subtraction of P, see, e.g., [12]. The representation is no longer unique, and the goal is to find a representation with as many zeros as possible, in order to have low complexity. This *"Canonical Sparse Form"* was independently discovered by many authors, and we refer to [11] for a historic account. It is sometimes called nonadjacent form (NAF), since it may be characterized by the fact that from two adjacent digits at least one must be a zero. Only about $\frac{1}{3}$ of the digits are non-zero in contrast to $\frac{1}{2}$ in ordinary binary expansion. The number of non-zero digits in the NAF of n is called the *Hamming weight* of n.

In [13] Solinas discusses the problem of computing $mP + nQ$. Instead of computing mP and nQ separately, one can proceed as follows. An approach using unsigned digit expansions would use the doubling operations and occasional additions of P, Q, or $P + Q$.

Date: January 30, 2003.

2000 *Mathematics Subject Classification.* Primary: 11A63; Secondary: 28A80 94A60.

Key words and phrases. Elliptic curve cryptography, joint sparse form, signed digit expansions, fractals.

† This author is supported by the START-project Y96-MAT of the Austrian Science Fund.

‡ This author is supported by the grant S8307-MAT of the Austrian Science Fund.

* This author is supported by the grant NRF 2053748 of the South African National Research Foundation.

Now, in instances where subtractions are no obstacles, one can allow additions of P, Q, $-P$, $-Q$, $P+Q$, $P-Q$, $-P+Q$, and $-P-Q$. If one has an expansion with digits $\{0, \pm 1\}$, for both numbers m and n, then a $\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$ corresponds to an addition of $P+Q$, a $\left(\begin{smallmatrix}-1\\0\end{smallmatrix}\right)$ to an addition of $-P$, etc. To keep the complexity low, the goal is to create as many double zeros $\left(\begin{smallmatrix}0\\0\end{smallmatrix}\right)$ in the joint expansion as possible. Solinas found a canonical joint expansion, called *Joint Sparse Form*, which has about $\frac{1}{2}$ of the double digits being a double zero $\left(\begin{smallmatrix}0\\0\end{smallmatrix}\right)$. Again, the number of double digits different from $\left(\begin{smallmatrix}0\\0\end{smallmatrix}\right)$ is called the joint Hamming weight. This Joint Sparse Form has minimal joint Hamming weight among all joint expansions of two numbers $\left(\begin{smallmatrix}m\\n\end{smallmatrix}\right)$.

In this paper, we want to gain a better understanding of the Joint Sparse Form. We start by considering another joint representation that we call *Simple Joint Sparse Form*. It has always the same Hamming weight as the Joint Sparse Form (even more: the double zeros are in the same positions). As the name suggests, this form is simpler, and created in a less elaborate way than the Joint Sparse Form. In Section 2 we give an algorithm for its computation and characterize it in a syntactic way. Since the joint Hamming weight is the same, we use the Simple Joint Sparse Form exclusively throughout this paper.

In Section 3, we are interested in geometric and topological properties of the Simple Joint Sparse Form. We construct a transducer with 9 (essential) states that produces the Simple Joint Sparse Form from the binary expansions of two numbers x and y. Now each of these 9 states corresponds to a certain area in the unit square, and we thus find a decomposition of the unit square into 9 regions of fractal type. It can be seen in Figure 2 as any of the four subsquares (ignore the different hatchings for the moment). It is proved that these regions are connected; their respective areas are computed, as well as the Hausdorff dimension of the boundaries ($= 1.21\ldots$). Pairs of numbers on the boundaries have usually two different representations, but eight numbers have even three! The coordinates of these eight points are computed.

The regions correspond to digits, and a fortiori to the Hamming weight of a pair of numbers m, n. Five regions contribute one to the Hamming weight $h(m,n)$, while the remaining four (of total area $\frac{1}{2}$) contribute zero to it. In Section 4 we prove that $\sum_{m,n<N} h(m,n) \sim \frac{N^2}{2}\log_2 N$. Intuitively, that is not surprising, since there are about $N^2 \log_2 N$ possible positions, and about half of them are non-zero. The obtained formula is more precise, as it exhibits a periodic oscillation of order N^2, and an error term that depends on the Hausdorff dimension mentioned before. Such a periodicity phenomenon is not uncommon in digit counting problems. Our approach follows the elegant and elementary method of Delange [5].

Section 5 exhibits a *central limit theorem* for the Hamming weight $h(m,n)$. It uses the analytic machinery developed in [10]. With these methods, asymptotic expansions for expectation and variance can also be achieved, but the oscillating term mentioned before would be less explicit in this way.

The last Section 6 briefly discusses higher dimensions. Solinas [13] remarks that a generalization would *require a higher-order analogue of the Joint Sparse Form*. The lack of such an analogue is also regretted by Avanzi [1]. While it might be less obvious to obtain

such a higher dimensional Joint Sparse Form, based on the description given by Solinas, it is completely natural when starting from the ideas of the Simple Joint Sparse Form, introduced and studied in the present paper. And, indeed, we get an algorithm for it, show that it has minimal Hamming weight, and characterize it syntactically. The NAF has at least a zero in two consecutive digits, and the (Simple) Joint Sparse Form at least a double zero in three consecutive double digits. Now the d-dimensional Simple Joint Sparse Form guarantees a multiple zero among any consecutive $d+1$ multiple digits.

2. Sparse Forms

2.1. **Joint Sparse Form.** Solinas [13] calls an expansion $\binom{x_\ell \cdots x_0}{y_\ell \quad y_0}$ of integers $\binom{x}{y}$ their *Joint Sparse Form*, if

(2.1) Of any three consecutive positions, at least one is a double zero,

(2.2) Adjacent terms do not have opposite signs, i.e., $x_j x_{j+1} \neq -1$ and $y_j y_{j+1} \neq -1$,

(2.3) If $x_j x_{j+1} \neq 0$, then $y_{j+1} = \pm 1$ and $y_j = 0$,

(2.4) If $y_j y_{j+1} \neq 0$, then $x_{j+1} = \pm 1$ and $x_j = 0$.

He proves the following result:

Theorem 1 (Solinas)**.** *Every pair of integers* $\binom{x}{y}$ *has a unique Joint Sparse Form. This Joint Sparse Form minimizes the joint Hamming weight amongst all joint expansions of* $\binom{x}{y}$*.*

Solinas also gives an algorithm to compute the Joint Sparse Form for given integers or for given binary expansions as input. His algorithm also accepts reduced signed binary expansions, where reduced means that (2.2) is satisfied. We note that Solinas' Algorithm has to know x and y modulo 8 to calculate the least significant pair of digits of the Joint Sparse Form, which means a look-ahead of two positions. The algorithm can be described by a transducer which translates a reduced signed binary expansion into the Joint Sparse Form from right to left.

2.2. **Simple Joint Sparse Form.** We describe a simple procedure to obtain a joint expansion of low weight; it will turn out that this form has the same (i.e., minimal) Hamming weight as the Joint Sparse Form.

The key observation is that an odd integer can be represented as $x = (x_\ell \dots x_1 x_0)$ with digits $x_j \in \{0, \pm 1\}$ where the parity of x_1 can be prescribed by replacing x_0 by $-x_0$ if necessary.

We are given two integers x and y. If both are even, then we have no choice and have to output $\binom{0}{0}$. If both numbers are odd, we choose $\binom{x_0}{y_0}$ appropriately so that both, $(x - x_0)/2$ and $(y - y_0)/2$ are even, so that a $\binom{0}{0}$ will be written the next step. If, say, x is odd and y is even, then we choose x_0 in such a way that $(x - x_0)/2 \equiv (y - 0)/2 \pmod 2$. This either leads to $\binom{0}{0}$ immediately in the next step or in the following step. This procedure generates a pair $\binom{0}{0}$ after at most 3 steps. It is summarized in Algorithm 1.

Algorithm 1 Simple Joint Sparse Form

Input: x and y integers
Output: $\left(\begin{smallmatrix} x_\ell & \cdots & x_0 \\ y_\ell & & y_0 \end{smallmatrix}\right)$ Simple Joint Sparse Form

```
j ← 0
while x ≠ 0 or y ≠ 0 do
  x_j ← x mod 2, y_j ← y mod 2
  if (x_j, y_j) = (1, 1) then
    if (x − x_j)/2 ≡ 1 (mod 2) then
      x_j ← −x_j
    end if
    if (y − y_j)/2 ≡ 1 (mod 2) then
      y_j ← −y_j
    end if
  else if x_j ≠ y_j then
    if (x − x_j)/2 ≢ (y − y_j)/2 (mod 2) then
      x_j ← −x_j, y_j ← −y_j
    end if
  end if
  x ← (x − x_j)/2, y ← (y − y_j)/2
  j ← j + 1
end while
```

It is clear that Algorithm 1 yields a joint expansion $\left(\begin{smallmatrix} x_\ell & \cdots & x_0 \\ y_\ell & & y_0 \end{smallmatrix}\right)$ which satisfies the following syntactical rules:

$$\text{If } |x_j| \neq |y_j|, \text{ then } |x_{j+1}| = |y_{j+1}|, \tag{2.5}$$

$$\text{If } |x_j| = |y_j| = 1, \text{ then } x_{j+1} = y_{j+1} = 0. \tag{2.6}$$

We call any joint expansion of x and y with digits $\{0, \pm 1\}$, which satisfies these two rules a *Simple Joint Sparse Form of x and y*. Surprisingly, it turns out that these rules are strong enough to determine a unique joint expansion.

Theorem 2. *Let x and y be integers. Then there is a unique (up to leading $\left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right)$) joint expansion $\left(\begin{smallmatrix} x_\ell & \cdots & x_0 \\ y_\ell & & y_0 \end{smallmatrix}\right)$ with digits 0, ± 1 which satisfies the rules* (2.5) *and* (2.6).

Furthermore, the Simple Joint Sparse Form has the same joint Hamming weight as the Joint Sparse Form. Therefore, its joint Hamming weight is minimal amongst all joint expansions.

Proof. The existence is proved by Algorithm 1.

Assume that $\left(\begin{smallmatrix} x_\ell & \cdots & x_0 \\ y_\ell & & y_0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} x'_\ell & \cdots & x'_0 \\ y'_\ell & & y'_0 \end{smallmatrix}\right)$ represent the same pair of integers $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$. Without loss of generality, $\min\{|x|, |y|\}$ is minimal among all pairs of integers with at least two expansions. Then minimality ensures that $\left(\begin{smallmatrix} x_0 \\ y_0 \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} x'_0 \\ y'_0 \end{smallmatrix}\right)$. Without loss of generality, $x_0 = -x'_0 \neq 0$. This implies $x_1 \not\equiv x'_1 \pmod 2$. If $2 \mid y$, then $y_0 = y'_0 = 0$, and (2.5) implies

$x_1 \equiv y_1 \equiv y_1' \equiv x_1' \pmod 2$, a contradiction. Therefore, $2 \nmid y$. Then (2.6) yields $\binom{x_1}{y_1} = \binom{0}{0}$ and $\binom{x_1'}{y_1'} = \binom{0}{0}$. This is a contradiction to $x_1 \not\equiv x_1' \pmod 2$.

We already observed that (2.5) and (2.6) imply (2.1). It is clear that (2.3) and (2.4) are fulfilled also. However in general, (2.2) is not satisfied by a Simple Joint Sparse Form. Nevertheless, if $x_{j+1}x_j = -1$, our rules (2.5) and (2.6) imply that $|y_{j+1}| = 1$ and $y_j = 0$. Therefore, replacing $x_{j+1}x_j$ by $0x_{j+1}$ does not change the joint Hamming weight. A finite number of these simple operations transforms a Simple Joint Sparse Form into the Joint Sparse Form without changing the position (and therefore their number) of $\binom{0}{0}$. Minimality follows from the minimality of the Joint Sparse Form. □

We emphasize that the computation needs information modulo 4 only. It is therefore no more a surprise that it can be realized by a transducer with look-ahead of *one* only. This motivates the epitheton *simple*. We now construct this transducer which reads the binary expansion of $\binom{x}{y}$ from right to left and outputs their Simple Joint Sparse Form. Although in principle, we could admit arbitrary signed expansions as input, we refrain from doing so since this would lead to an automaton with 26 states. At any stage, the following information has to be available: the previously read pair of digits and the current pair of digits and information about a possible carry, since a 1 may have been replaced by -1. Since the carry is added to the previously read pair anyway, we represent states by the sum of the previously read pair and the pair of carries. This yields 9 states representing $\{0,1,2\} \times \{0,1,2\}$. From some initial state, there is an edge into the appropriate state which reads the first pair of digits but does not output anything. It is understood that we read some leading pairs of zeros until no further carries are left, i.e., we reach state $\binom{0}{0}$. We attach integer labels to states in a more or less arbitrary fashion since we will consider adjacency matrices. The correspondence between these labels and the pairs of carries plus digits is as follows:

label	1	2	3	4	5	6	7	8	9
state	$\binom{0}{0}$	$\binom{1}{1}$	$\binom{2}{2}$	$\binom{1}{0}$	$\binom{2}{0}$	$\binom{2}{1}$	$\binom{0}{1}$	$\binom{0}{2}$	$\binom{1}{2}$

The resulting transducer is shown in Figure 1.

3. The Geometry of the Simple Joint Sparse Form

The aim of this section is to understand the Simple Joint Sparse Form from left to right. We are interested to "know" in which state we are after k steps. Figure 2 shows the situation for $k = 11$ and all pairs of integers $0 \le x, y \le 2^{12} - 1$.

Figure 2 suggests that there is an underlying fractal structure. This structure will be studied in this section. We will prove

Theorem 3. *There exist* 9 *disjoint open connected subsets of* $[0,1]^2$*,* $A_1, \ldots, A_9$*, such that the pair of digits* (x_k, y_k) *of the simple Joint Sparse Form of the pair of integers* (x, y) *can be computed from the index* i *for which* $(\{x2^{-k-1}\}, \{y2^{-k-1}\}) \in A_i$ *and the pair of digits* (ξ_{k+1}, η_{k+1}) *in the (classical) binary expansion of* (x, y)*. The union of the sets* A_i *has Lebesgue measure* 1*, and their boundaries have Hausdorff-dimension* 1.2107605332 ....

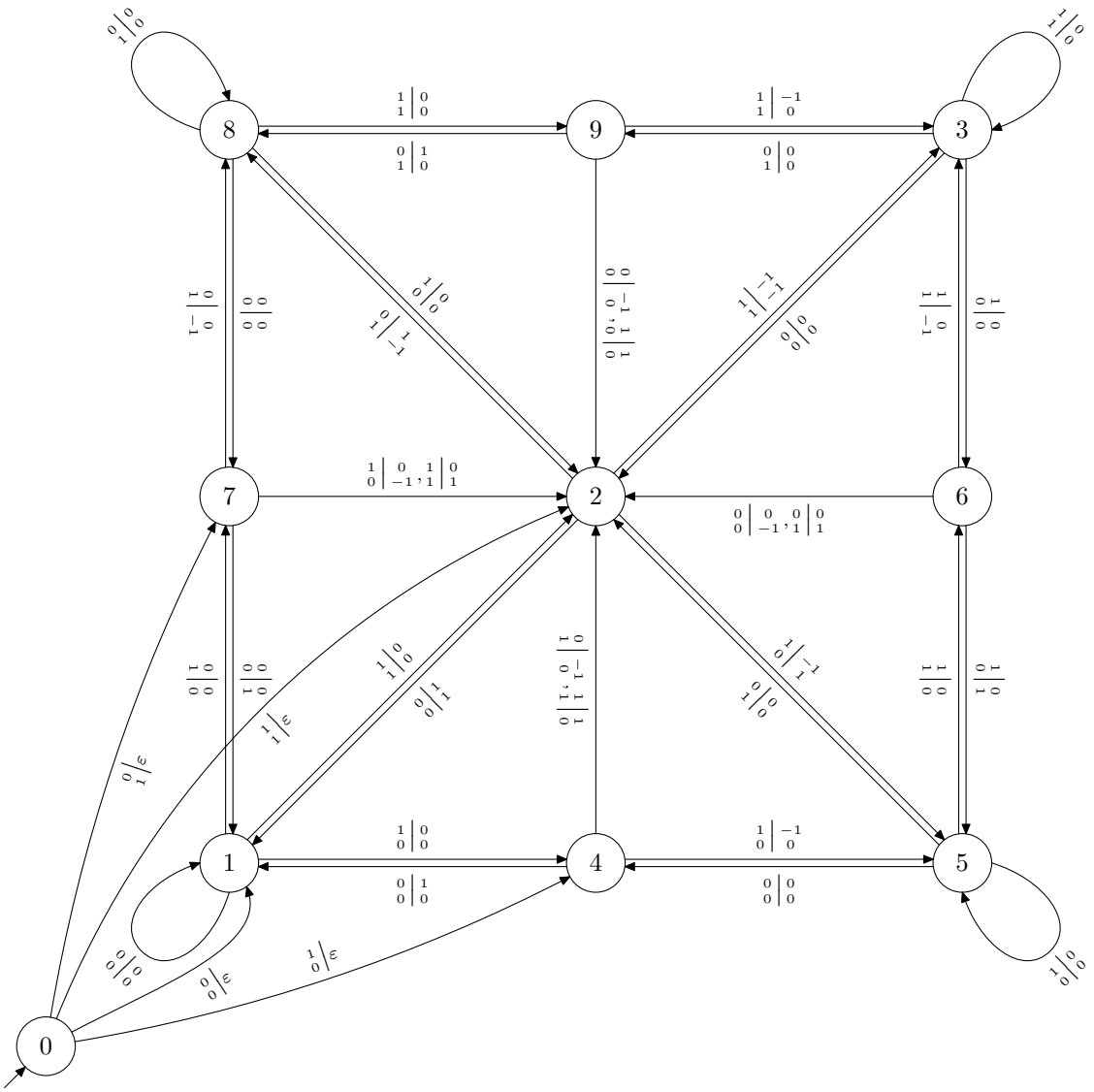

FIGURE 1. Automaton for calculating the Simple Joint Sparse Form from the binary expansion from right to left. The symbol ε denotes the empty word.

Furthermore, the index i decides on the Hamming weight of the output, and the measure of the union of those A_i, which yield positive Hamming weight, equals $\frac{1}{2}$.

It is clear that the k-th state when reading $\binom{x}{y}$ in their classical binary expansions

$$x = \sum_{j=0}^{J} \xi_j 2^j, \quad y = \sum_{j=0}^{J} \eta_j 2^j$$

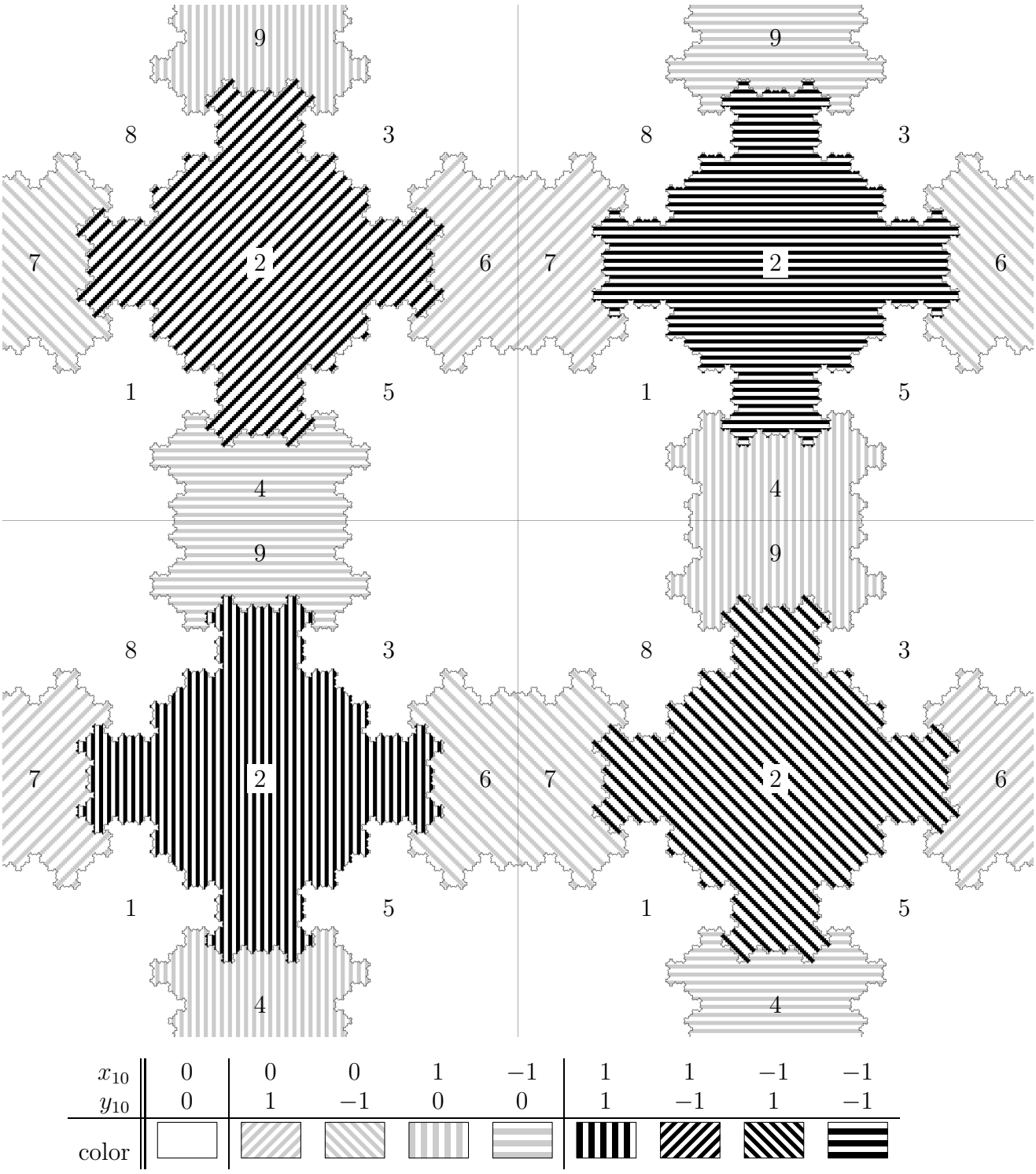

FIGURE 2. 11^{th} state and output digits $\frac{x_{10}}{y_{10}}$ when reading all pairs of integers up to $2^{12} - 1$.

depends on the k least significant digits, i.e., $\binom{x}{y} \bmod 2^k$ only. The output digits (x_{k-1}, y_{k-1}) in the Simple Joint Sparse Form

$$x = \sum_{j=0}^{J+2} x_j 2^j, \quad y = \sum_{j=0}^{J+2} y_j 2^j$$

depend on the $k+1$ least significant digits, or equivalently, on the k-th state and on (ξ_k, η_k). Since the state is the interesting information to be found, we renormalize pairs of integers less than 2^k by dividing through 2^k, which yields points in the unit square. The above mentioned fractal would then result from letting k tend to infinity. In order to prove convergence we define functions Φ_k on pairs of words of digits $\{0,1\}$ of length k as follows

$$\Phi_k \binom{\delta_1\, \delta_2 \cdots \delta_k}{\varepsilon_1\, \varepsilon_2 \quad\; \varepsilon_k} = \binom{\delta_1\, \delta_2 \cdots \delta_k}{\varepsilon_1\, \varepsilon_2 \quad\; \varepsilon_k} \cdot \{1, \dots, 9\},$$

where the expression on the right means application of the pair of words to all states of the automaton in Figure 1. Thus the image of Φ_k is a set of states. Furthermore,

$$\Phi_{k+1} \binom{\delta_1\, \delta_2 \cdots \delta_{k+1}}{\varepsilon_1\, \varepsilon_2 \quad\; \varepsilon_{k+1}} \subseteq \Phi_k \binom{\delta_1\, \delta_2 \cdots \delta_k}{\varepsilon_1\, \varepsilon_2 \quad\; \varepsilon_k},$$

which implies existence of the limit

$$\Phi \binom{\delta_1\, \delta_2 \cdots}{\varepsilon_1\, \varepsilon_2 \cdots} = \lim_{k\to\infty} \Phi_k \binom{\delta_1\, \delta_2 \cdots \delta_k}{\varepsilon_1\, \varepsilon_2 \quad\; \varepsilon_k}. \tag{3.1}$$

The function Φ defined on $(\{0,1\} \times \{0,1\})^{\mathbb{N}}$ is continuous in all points which have a singleton image.

Remark. In the above description the sequence Φ_k is calculated by the automaton in Figure 1 by reading digits from right to left. Certainly, it would be more desirable to have a description of Φ_k in terms of the digits in "natural" order, i.e., from left to right. This is indeed possible: We construct an automaton with set of states (a subset of) the set $\{1, \dots, 9\}^{\{1,\dots,9\}}$. The transition from state g by the pair of digits $\binom{\delta}{\varepsilon}$ will be denoted by $g \diamond \binom{\delta}{\varepsilon}$ in order to avoid any confusion. It is given by

$$\left(g \diamond \binom{\delta}{\varepsilon}\right)(i) := g\left(\binom{\delta}{\varepsilon} \cdot i\right).$$

The initial state is the identity map. It turns out that 750 states are actually reached. If we reach a constant map $g(i) = j$ after reading $\binom{\delta_1 \cdots \delta_k}{\varepsilon_1 \quad\; \varepsilon_k}$, we have $\Phi \binom{\delta_1 \cdots \delta_k \cdots}{\varepsilon_1 \quad\; \varepsilon_k \quad\;\; \cdots} = \{j\}$.

We now want to prove that Φ descends to a function on $[0,1]^2$ by

$$\Phi\left(\sum_{n=1}^{\infty} \delta_n 2^{-n}, \sum_{n=1}^{\infty} \varepsilon_n 2^{-n}\right) = \Phi \binom{\delta_1\, \delta_2 \cdots}{\varepsilon_1\, \varepsilon_2 \cdots}.$$

For this purpose we note the simple facts that

$$\binom{\delta\, \delta}{\varepsilon\, \varepsilon} \cdot \{1, \dots, 9\} \quad \text{is a singleton } (\delta, \varepsilon \in \{0,1\}) \tag{3.2}$$

and

$$\begin{pmatrix}\delta\,\delta\\ 0\,1\end{pmatrix}^k \cdot i = \begin{pmatrix}\delta\,\delta\\ 0\,1\end{pmatrix}^2 \cdot i \quad (\delta,\varepsilon\in\{0,1\}) \tag{3.3}$$

for all $k\geq 2$ and all $i\in\{1,\ldots,9\}$. In order to prove that

$$\Phi_{k+\ell}\begin{pmatrix}\delta_1 & \cdots & \delta_k & 1 & 0 & 0 & \cdots & 0\\ \varepsilon_1 & & \varepsilon_k & \varepsilon_{k+1} & \varepsilon_{k+2} & \varepsilon_{k+3} & & \varepsilon_{k+\ell}\end{pmatrix} = \Phi_{k+\ell}\begin{pmatrix}\delta_1 & \cdots & \delta_k & 0 & 1 & 1 & \cdots & 1\\ \varepsilon_1 & & \varepsilon_k & \varepsilon_{k+1} & \varepsilon_{k+2} & \varepsilon_{k+3} & & \varepsilon_{k+\ell}\end{pmatrix}$$

for $\ell\geq 9$ it is sufficient by (3.2) and (3.3) to check

$$\begin{pmatrix}1 & 0 & \cdots & 0\\ \varepsilon_1 & \varepsilon_2 & & \varepsilon_9\end{pmatrix}\cdot\{1,\ldots,9\} = \begin{pmatrix}0 & 1 & \cdots & 1\\ \varepsilon_1 & \varepsilon_2 & & \varepsilon_9\end{pmatrix}\cdot\{1,\ldots,9\}$$

for all choices of $(\varepsilon_1,\ldots,\varepsilon_9)$. The same proof applies if the first and second coordinate are interchanged. Thus Φ is well-defined on $[0,1]^2$ and continuous in all points which have a singleton image.

We want to describe the sets

$$A_j = \{(x,y)\in[0,1]^2 \mid \Phi(x,y)=\{j\}\},$$
$$V_j = \{(x,y)\in[0,1]^2 \mid j\in\Phi(x,y)\}$$

topologically. The sets A_j are open by the continuity properties of Φ. For a point $(x,y)\in V_j$ and any k the suffix after k digits of the digital expansions of (x,y) can be altered to $(\tilde{x},\tilde{y})$ so that $\Phi(\tilde{x},\tilde{y})=\{j\}$. This implies $A_j\subseteq V_j\subseteq\overline{A_j}$. On the other hand for a point $(x,y)\notin V_j$ by a similar argument a neighbourhood of this point is in the complement of V_j. Thus $V_j=\overline{A_j}$.

Any neighbourhood of a point (x,y) with $\{i,j\}\subseteq\Phi(x,y)$ contains points $(x',y')\in A_i$ and $(x'',y'')\in A_j$ by the above arguments. This implies that $(x,y)\in\partial V_j$ and $\operatorname{int}(V_j)\subseteq A_j\subseteq V_j$, which yields $\operatorname{int}(V_j)=A_j$.

We now want to characterize the sets A_j and V_j in the language of *graph directed* sets as introduced in [8]. For this purpose we introduce the maps

$$f_{\delta,\varepsilon}(x,y)=\left(\frac{x+\delta}{2},\frac{y+\varepsilon}{2}\right).$$

It is clear from the definition that

$$\Phi(f_{\delta,\varepsilon}(x,y)) = \begin{pmatrix}\delta\\ \varepsilon\end{pmatrix}\cdot\Phi(x,y). \tag{3.4}$$

Equation (3.4) leads us to the definition

$$F(S_1,\ldots,S_9) = (F_1(S_1,\ldots,S_9),\ldots,F_9(S_1,\ldots,S_9)), \tag{3.5}$$

where

$$F_i(S_1,\ldots,S_9) = \bigcup_{\substack{j,\delta,\varepsilon\\ i=(\delta,\varepsilon)\cdot j}} f_{\delta,\varepsilon}(S_j),$$

where $S_k \subseteq [0,1]^2$. Since F acts as a contraction on the compact subsets of $[0,1]^2$, there exist unique compact sets $K_1, \dots, K_9$, such that $F(K_1, \dots, K_9) = (K_1, \dots, K_9)$. These sets can be obtained as the limits of iterates of F of any 9-tuple of compact sets. From (3.4) we conclude that

$$F_i(A_1, \dots, A_9) \subseteq A_i, \tag{3.6}$$

$$F_i(V_1, \dots, V_9) = V_i \tag{3.7}$$

and therefore $V_i = K_i$ for $i = 1, \dots, 9$.

Next we want to prove that the sets A_j are connected. We introduce the open sets

$$O_j = \operatorname{int}\left(\bigcup_{\Phi_4\left(\begin{smallmatrix}\delta_1 & \dots & \delta_4\\ \varepsilon_1 & & \varepsilon_4\end{smallmatrix}\right)=\{j\}} \left(\frac{\delta_1}{2} + \dots + \frac{\delta_4}{16}, \frac{\varepsilon_1}{2} + \dots + \frac{\varepsilon_4}{16} \right) + \left[0, \frac{1}{16}\right]^2 \right).$$

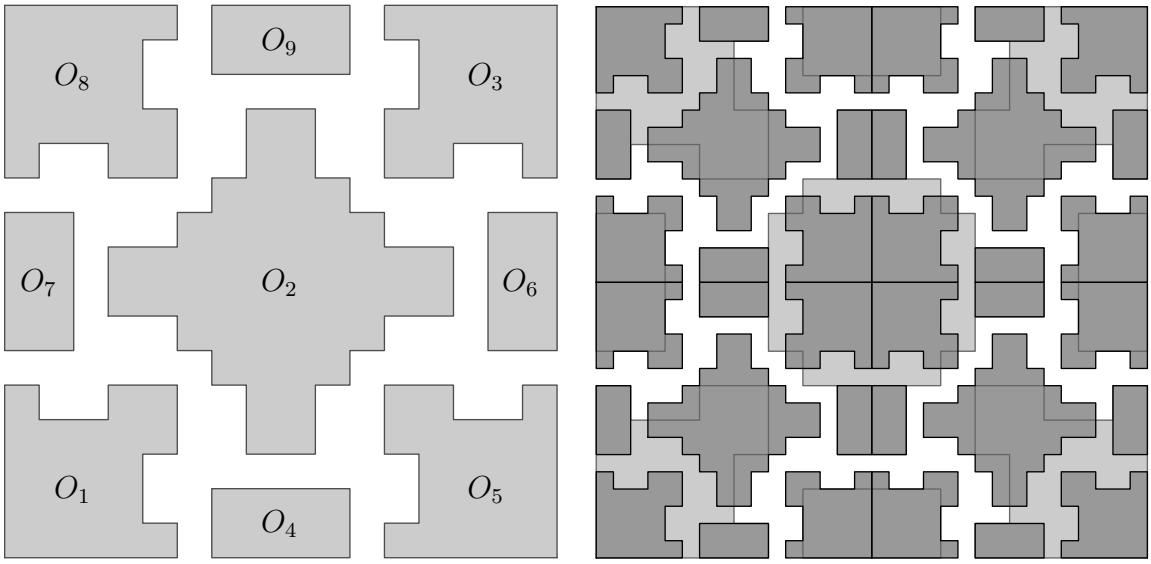

FIGURE 3. Left: the sets O_i.
Right: The dark gray areas represent the left image after one application of the functions $f_{\delta,\varepsilon}$.

These sets are shown in the left image of Figure 3. The sets O_j are connected and

$$O_j \subset V_j.$$

The right image in Figure 3 shows that

$$O_i \cap F_i(O_1, \dots, O_9) \neq \emptyset \quad \text{and therefore } O_i \cup F_i(O_1, \dots, O_9) \text{ is connected.}$$

From this it follows by induction that the sets

$$B_i = \bigcup_{\ell=0}^{\infty} \left(F^\ell(O_1, \dots, O_9)\right)_i$$

are connected. Furthermore, B_i is a dense open subset of V_i, since

$$(V_1, \dots, V_9) = \lim_{k\to\infty} F^k(\overline{O_1}, \dots, \overline{O_9}).$$

Therefore the sets $A_i = \operatorname{int}(V_i)$ are connected.

In the following we want to study intersections of two or three sets V_j. Clearly, we have for pairwise distinct i, j, k

$$\begin{aligned} V_{\{i,j\}} &:= V_i \cap V_j = \left\{(x,y) \in [0,1]^2 \mid \{i,j\} \subseteq \Phi(x,y)\right\}, \\ V_{\{i,j,k\}} &:= V_i \cap V_j \cap V_k = \left\{(x,y) \in [0,1]^2 \mid \{i,j,k\} \subseteq \Phi(x,y)\right\}. \end{aligned} \tag{3.8}$$

These sets can be generated by the automata in Figure 4 and Figure 5. These automata have the two (resp. 3) element subsets of $\{1, \dots, 9\}$ as their states (only those which correspond to non-empty intersections are drawn) and the obvious transition functions. In order to generate a point in $V_{\{i,j\}}$ we start in the state labeled with i, j and follow the arcs in the reverse direction. The triple intersections are singleton sets, which will be called "three country borders":

$$\left\{\left(\frac{1}{5}, \frac{2}{5}\right)\right\} = V_{\{1,2,7\}}, \left\{\left(\frac{1}{5}, \frac{3}{5}\right)\right\} = V_{\{2,7,8\}}, \left\{\left(\frac{2}{5}, \frac{1}{5}\right)\right\} = V_{\{1,2,4\}}, \left\{\left(\frac{2}{5}, \frac{4}{5}\right)\right\} = V_{\{2,8,9\}},$$
$$\left\{\left(\frac{3}{5}, \frac{1}{5}\right)\right\} = V_{\{2,4,5\}}, \left\{\left(\frac{3}{5}, \frac{4}{5}\right)\right\} = V_{\{2,3,9\}}, \left\{\left(\frac{4}{5}, \frac{2}{5}\right)\right\} = V_{\{2,5,6\}}, \left\{\left(\frac{4}{5}, \frac{3}{5}\right)\right\} = V_{\{2,3,6\}}.$$

Now, we want to compute the measures of the sets V_i and the Hausdorff-dimension of ∂V_i. It is an immediate consequence of the definition that

$$\bigcup_{i=1}^{9} V_i = [0,1]^2.$$

Furthermore, from (3.7) we can conclude

$$\lambda(V_i) \le \frac{1}{4} \sum_{\substack{j,\delta,\varepsilon \\ (\delta,\varepsilon)\cdot j = i}} \lambda(V_j). \tag{3.9}$$

Summing these inequalities for $j = 1, \dots, 9$ we obtain

$$\sum_{j=1}^{9} \lambda(V_i) \le \sum_{j=1}^{9} \lambda(V_i),$$

which implies that equality has to hold in (3.9) for all $j = 1, \dots, 9$. Since

$$\lambda(V_i) = \frac{1}{4}\left(\sum_{\substack{j,\delta,\varepsilon \\ (\delta,\varepsilon)\cdot j = i}} \lambda(V_j) - \sum_{\substack{j<k,\delta_1,\delta_2,\varepsilon_1,\varepsilon_2 \\ (\delta_1,\varepsilon_1)\cdot j = i \\ (\delta_2,\varepsilon_2)\cdot k = i}} \lambda(V_j \cap V_k) + \text{triple intersections} \right),$$

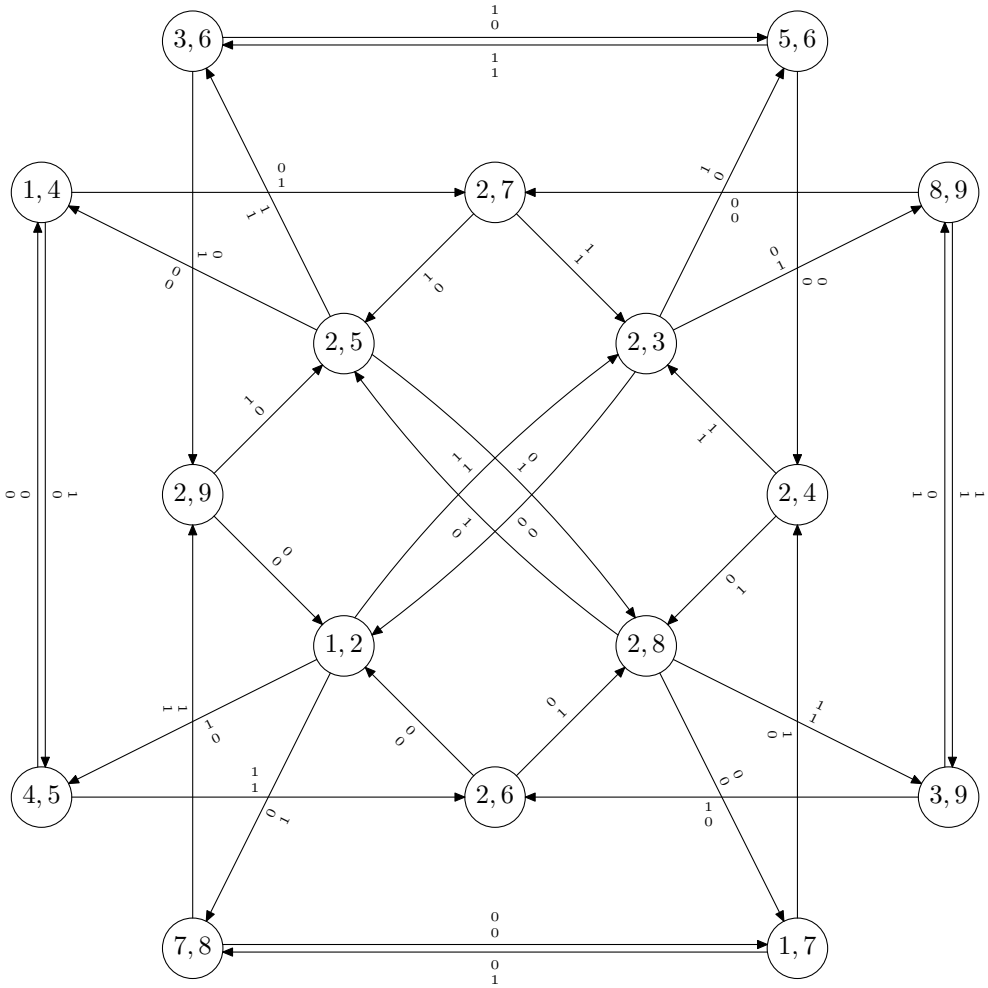

FIGURE 4. The automaton generating the points in the sets $V_{\{i,j\}}$.

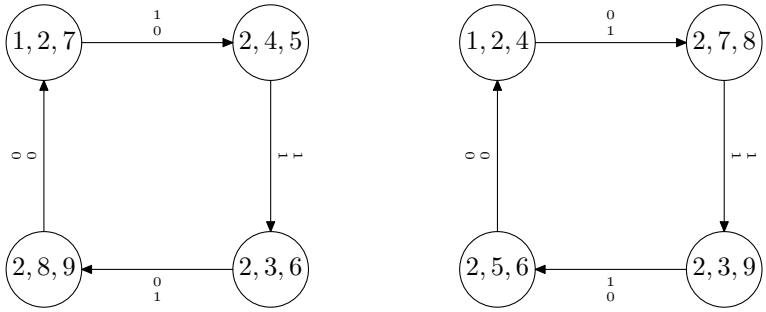

FIGURE 5. The automaton generating the "three country borders" $V_{\{i,j,k\}}$.

and we know that the triple intersections consist of single points only, we can conclude that $\lambda(V_j \cap V_k) = 0$ for $j \neq k$, and therefore the boundaries of the sets V_j have measure 0. Furthermore, we have $\sum_i \lambda(V_i) = 1$, which yields

$$\lambda(V_1) = \lambda(V_3) = \lambda(V_5) = \lambda(V_8) = \frac{1}{8}, \quad \lambda(V_4) = \lambda(V_6) = \lambda(V_7) = \lambda(V_9) = \frac{1}{16}, \quad \lambda(V_2) = \frac{1}{4}.$$

For computing the Hausdorff-dimension of the boundaries of the sets V_j we notice that the sets $V_{\{i,j\}}$ defined in (3.8) satisfy the relation

$$V_{\{i,j\}} = \bigcup_{\substack{\delta,\varepsilon,\{k,\ell\} \\ (\delta,\varepsilon)\cdot\{k,\ell\}=\{i,j\}}} f_{\delta,\varepsilon}(V_{\{k,\ell\}}). \tag{3.10}$$

This observation brings us in the context of *graph directed* sets as introduced in [8]. The box-dimension can be computed from the dominating eigenvalue of the adjacency matrix of the "boundary automaton" given in Figure 4. This eigenvalue is the positive root λ of the equation

$$x^3 - 2x^2 + x - 4 = 0. \tag{3.11}$$

This yields

$$\dim_B(\partial A_j) = \alpha = \frac{\log \lambda}{\log 2} = 1.2107605332885233950\ldots. \tag{3.12}$$

For technical reasons we introduce the set $V_{10} = \partial[0,1]^2$. Then the open sets

$$A_{\{i,j\}} = \Big\{(x,y) \in \operatorname{int}(V_i \cup V_j) \mid \forall k \in \{1,\ldots,10\} \setminus \{i,j\} : d((x,y), V_{\{i,j\}}) < d((x,y), V_k)\Big\}$$

satisfy

$$\bigcup_{\substack{\delta,\varepsilon,\{k,\ell\} \\ (\delta,\varepsilon)\cdot\{k,\ell\}=\{i,j\}}} f_{\delta,\varepsilon}(A_{\{k,\ell\}}) \subseteq A_{\{i,j\}} \tag{3.13}$$

with the union being disjoint. This is the open set condition which by [7, Theorem 9.2] implies that the Hausdorff-dimension of $V_{\{i,j\}}$ equals its box-dimension. Thus we have

$$\dim_H(\partial A_j) = \frac{\log \lambda}{\log 2} = 1.2107605332885233950\ldots. \tag{3.14}$$

Figure 2 exhibits a rotational structure which has not been discussed yet. This is a natural property of the underlying problem on elliptic curves: since there is a symmetry in the algorithm described in the introduction between the pairs of points (P, Q) and $(P + Q, P - Q)$ the map $(x, y) \mapsto (x + y, x - y)$ should preserve the structure of the sets A_i. We will prove now that this is indeed the case. For this purpose we introduce the map

$T : (x, y) \mapsto (x + y \mod 1, x - y \mod 1)$. This map satisfies

$$T(A_2) \subseteq A_1 \cup A_3 \cup A_5 \cup A_8, \tag{3.15}$$
$$T(A_4 \cup A_6 \cup A_7 \cup A_9) \subseteq A_2,$$
$$T((A_1 \cap f_{00}(A_2)) \cup (A_3 \cap f_{11}(A_2)) \cup (A_5 \cap f_{10}(A_2)) \cup (A_8 \cap f_{01}(A_2))) \subseteq A_4 \cup A_6 \cup A_7 \cup A_9,$$
$$T((A_1 \setminus f_{00}(A_2)) \cup (A_3 \setminus f_{11}(A_2)) \cup (A_5 \setminus f_{10}(A_2)) \cup (A_8 \setminus f_{01}(A_2))) \subseteq A_1 \cup A_3 \cup A_5 \cup A_8.$$

Adding or subtracting two numbers given in their Simple Joint Sparse Form is digit-wise addition (or subtraction) and subsequent correction by the rule $(0, \pm 2) \mapsto (\pm 1, 0)$ by (2.6). We demonstrate relation (3.15); the proof of the other relations is similar: let (x, y) be given in its Simple Joint Sparse Form. The condition $(x, y) \in A_2$ is equivalent to

$$\begin{matrix} x \\ y \end{matrix} = \begin{pmatrix} 0\,.\,1\,\delta\,* \\ 0\,.\,1\,\varepsilon\,* \end{pmatrix} \cdots \quad \text{(in Simple Joint Sparse Form!)},$$

since 2 is the unique state which produces two non-zero digits as output (cf. Figure 2). Since $\delta\varepsilon = 0$ we have

$$\begin{matrix} x + y \\ x - y \end{matrix} = \begin{pmatrix} 1\,.\,0\,* \\ 0\,.\,0\,* \end{pmatrix} \cdots \quad \text{(in Simple Joint Sparse Form)}.$$

Therefore, $T(x, y) \in A_i$ for a state i, which produces the output $\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}$, i.e., $i \in \{1, 3, 5, 8\}$.

4. Geometric Approach for Estimating the Joint Hamming Weight

In this section we give a derivation for an asymptotic formula for the mean of the Hamming weight of the Joint Sparse Form. The proof follows the ideas used by H. Delange in [5].

Theorem 4. *The Hamming weight of the Joint Sparse Form of two positive integers satisfies the following asymptotic formula*

$$S(N) = \sum_{m,n<N} h(m, n) = \frac{N^2}{2} \log_2 N + N^2 \psi_1(\log_2 N) + \mathcal{O}(N^\alpha), \tag{4.1}$$

where ψ_1 is a continuous periodic function of period 1 and α is given by (3.12).

Proof. Theorem 3 states that the contribution of the pair of digits (x_k, y_k) to the Hamming weight of the Joint Sparse Form of the pair (m, n) equals

$$\mathbb{1}_H \left(\left\{ \frac{m}{2^{k+1}} \right\}, \left\{ \frac{n}{2^{k+1}} \right\} \right), \quad \text{where } H = \operatorname{int}(V_2 \cup V_4 \cup V_6 \cup V_7 \cup V_9).$$

Notice that $\lambda_2(H) = \frac{1}{2}$. It follows immediately that

$$S(N) = \sum_{k=0}^{K} \sum_{m,n<N} \mathbb{1}_H \left(\left\{ \frac{m}{2^{k+1}} \right\}, \left\{ \frac{n}{2^{k+1}} \right\} \right) = \sum_{k=0}^{K} \sum_{m,n<N} \mathbb{1}_{H_k} \left(\left\{ \frac{m}{2^{k+1}} \right\}, \left\{ \frac{n}{2^{k+1}} \right\} \right) \tag{4.2}$$

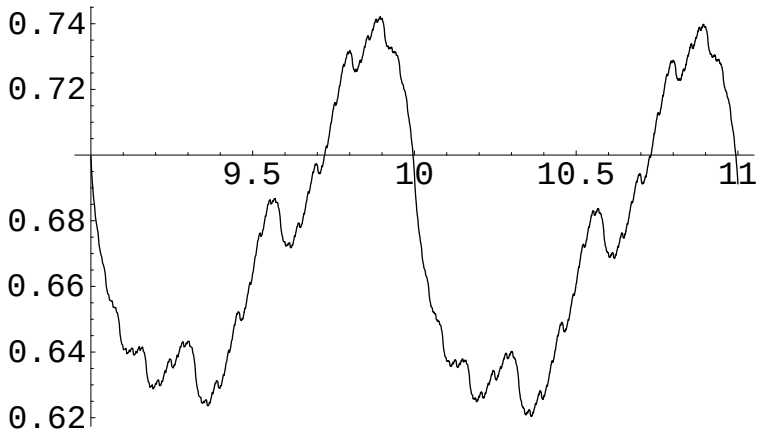

FIGURE 6. Plot of $S(N)/N^2 - \frac{1}{2}\log_2 N$ over $\log_2 N$ for $N = 512, \ldots, 2048$.

with $K = \lfloor \log_2 N \rfloor + 2$ and

$$H_k = \bigcup_{(m,n)\in 2^{k+1}H\cap\mathbb{Z}^2} [m2^{-k-1}, (m+1)2^{-k-1}) \times [n2^{-k-1}, (n+1)2^{-k-1}). \tag{4.3}$$

This enables us to rewrite the sum as an integral

$$S(N) = \sum_{k=0}^{K} \iint_{[0,N]^2} \mathbb{1}_{H_k}\left(\left\{\frac{m}{2^{k+1}}\right\}, \left\{\frac{n}{2^{k+1}}\right\}\right) dm\, dn. \tag{4.4}$$

Setting $t = N2^{-K} \in [\frac{1}{4}, \frac{1}{2})$, substituting $m = 2^K x$ and $n = 2^K y$ in the integrals, and reversing the order of summation yields

$$S(N) = 4^K \sum_{k=0}^{K} \iint_{[0,t]^2} \mathbb{1}_{H_{K-k}}\left(\left\{2^{k-1}x\right\}, \left\{2^{k-1}y\right\}\right) dx\, dy.$$

We rewrite this as

$$\begin{aligned} S(N) = \frac{1}{2}(K+1)(t2^K)^2 &+ 4^K \sum_{k=0}^{K} \iint_{[0,t]^2} \left(\mathbb{1}_H\left(\left\{2^{k-1}x\right\}, \left\{2^{k-1}y\right\}\right) - \frac{1}{2}\right) dx\, dy \\ &+ 4^K \sum_{k=0}^{K} \iint_{[0,t]^2} \left(\mathbb{1}_{H_{K-k}} - \mathbb{1}_H\right)\left(\left\{2^{k-1}x\right\}, \left\{2^{k-1}y\right\}\right) dx\, dy. \end{aligned} \tag{4.5}$$

We remark that t is a rational number with denominator 2^K and therefore the integral

$$\iint_{[0,t]^2} \left(\mathbb{1}_H\left(\left\{2^{k-1}x\right\}, \left\{2^{k-1}y\right\}\right) - \frac{1}{2}\right) dx\, dy = 0 \quad \text{for } k > K,$$

since $\lambda_2(H) = \frac{1}{2}$. Thus we can extend the second summand in (4.5) to an infinite sum without changing its value. It is natural to define the continuous function

$$\Psi(t) = \sum_{k=0}^{\infty} \iint_{[0,t]^2} \left(\mathbb{1}_H \left(\left\{2^{k-1}x\right\}, \left\{2^{k-1}y\right\} \right) - \frac{1}{2} \right) dx\, dy.$$

Simple computations yield $\Psi(\frac{1}{4}) = -\frac{1}{16}$ and $\Psi(\frac{1}{2}) = -\frac{1}{8}$.

We now treat the third summand in (4.5). For this purpose we have to estimate the integral

$$\begin{aligned} (4.6)\quad & \iint_{[0,t]^2} \left(\mathbb{1}_{H_\ell} - \mathbb{1}_H\right) \left(\left\{2^{k-1}x\right\}, \left\{2^{k-1}y\right\} \right) dx\, dy \\ &= \iint_{[0,2^{-k+1}\lfloor 2^{k-1}t \rfloor]^2} \left(\mathbb{1}_{H_\ell} - \mathbb{1}_H\right) \left(\left\{2^{k-1}x\right\}, \left\{2^{k-1}y\right\} \right) dx\, dy + \iint_{[0,t]^2 \setminus [0,2^{-k+1}\lfloor 2^{k-1}t \rfloor]^2} \cdots dx\, dy. \end{aligned}$$

We set

$$\beta_\ell = \iint_{[0,1]^2} \left(\mathbb{1}_{H_\ell} - \mathbb{1}_H\right)(x,y)\, dx\, dy$$

and remark that by the definition of the box dimension and the arguments given in Section 3 we have $\beta_\ell = \mathcal{O}((\lambda/4)^\ell)$, where λ is given by (3.11). Thus the first integral in (4.6) equals $\beta_\ell(2^{-k+1}\lfloor 2^{k-1}t \rfloor)^2$; the second integral is $\mathcal{O}((\lambda/4)^\ell 2^{-k})$, since it can be written as a sum over $\mathcal{O}(2^k)$ integrals over squares of side-length 2^{-k+1}, and each integral gives a contribution of $\mathcal{O}((\lambda/4)^\ell)$.

Summing up we obtain

$$(4.7)\quad S(N) = \frac{N^2}{2}(K+1) + 4^K \Psi(t) + 4^K \sum_{k=0}^{K} \left(\frac{\lfloor 2^{k-1}t \rfloor}{2^{k-1}} \right)^2 \beta_{K-k} + 4^K \sum_{k=0}^{K} \mathcal{O}\left(\left(\frac{\lambda}{4} \right)^{K-k} 2^{-k} \right).$$

Rewriting this and observing that the last summand is $\mathcal{O}(\lambda^K) = \mathcal{O}(N^\alpha)$ we obtain

$$\begin{aligned} (4.8)\quad S(N) &= \frac{N^2}{2}(K+1) + 4^K \Psi(t) + 4^K t^2 \sum_{k=0}^{K} \beta_{K-k} \\ &\quad - 2 \cdot 4^K t \sum_{k=0}^{K} \frac{\{2^{k-1}t\}}{2^{k-1}} \beta_{K-k} + 4^K \sum_{k=0}^{K} \frac{\{2^{k-1}t\}^2}{4^k} \beta_{K-k} + \mathcal{O}(N^\alpha) \\ &= \frac{N^2}{2}(K+1) + 4^K \Psi(t) + N^2 \sum_{k=0}^{\infty} \beta_k + \mathcal{O}(N^\alpha), \end{aligned}$$

where we have used that $\beta_k = \mathcal{O}((\lambda/4)^k)$. Inserting $K = \log_2 N - \{\log_2 N\} + 2$ and using $t = 2^{\{\log_2 N\}-2}$ we obtain

(4.9)
$$S(N) = \frac{N^2}{2}\log_2 N + N^2\left(\frac{3}{2} - \frac{1}{2}\{\log_2 N\} + 4^{2-\{\log_2 N\}}\Psi\left(2^{\{\log_2 N\}-2}\right) + \sum_{k=0}^{\infty}\beta_k\right) + \mathcal{O}(N^\alpha).$$

We notice here that a simple computation involving the adjacency matrix of the automaton in Figure 1 proves that

$$\sum_{k=0}^{\infty}\beta_k = \frac{3}{16}.$$

The function

$$\psi_1(x) = \frac{27}{16} - \frac{1}{2}\{x\} + 4^{2-\{x\}}\Psi\left(2^{\{x\}-2}\right)$$

is a periodic function with period 1, which is trivially continuous in $[0,1)$. Furthermore, $\psi_1(0) = \lim_{x\to 1-}\psi_1(x) = \frac{11}{16}$. Thus the theorem is proved. □

5. Exponential sums and Central Limit Theorem

In this section we will prove a central limit theorem for the Hamming weight of the Joint Sparse Form.

Theorem 5. *The following equation holds uniformly for all $x \in \mathbb{R}$ and any $\varepsilon > 0$*

(5.1)
$$\frac{1}{N^2}\#\left\{m,n<N \mid \frac{h(m,n)-\frac{1}{2}\log_2 N}{\frac{1}{4}\sqrt{\log_2 N}} < x\right\} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-\frac{t^2}{2}}\,dt + \mathcal{O}\left((\log N)^{-\frac{1}{6}+\varepsilon}\right).$$

The automaton for calculating the Simple Joint Sparse Form given in Figure 1 can also be used to compute the Hamming weight of the representation (simply map any output different from $\binom{0}{0}$ to 1). Furthermore, the Hamming weight which results from a transition from i to j depends on i only, cf. Figure 2. Therefore, there is no look-ahead needed for calculating the Hamming weight.

For the proof of Theorem 5 we use exponential sums. For this purpose we calculate

$$f(m,n) = e^{ith(m,n)}$$

in terms of the binary digits of m and n. For each pair of digits (δ,ε) we define a matrix $M_{\delta,\varepsilon}$ in the following way: its (k,ℓ)-th entry equals e^{ith}, if the automaton reads (δ,ε) and

writes h while going from state k to state ℓ and 0 otherwise ($z = e^{it}$)

$$M_{0,0} = \begin{pmatrix} 1&0&0&0&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0&0&0\\ 0&z&0&0&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0&0&0\\ 0&0&0&z&0&0&0&0&0&0\\ 0&z&0&0&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&z&0&0&0\\ 0&z&0&0&0&0&0&0&0&0 \end{pmatrix}, \qquad M_{0,1} = \begin{pmatrix} 0&0&0&0&0&0&z&0&0&0\\ 0&0&0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0&0&z\\ 0&z&0&0&0&0&0&0&0&0\\ 0&z&0&0&0&0&0&0&0&0\\ 0&z&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0&1&0 \end{pmatrix},$$

$$M_{1,0} = \begin{pmatrix} 0&0&0&z&0&0&0&0&0&0\\ 0&0&0&0&1&0&0&0&0&0\\ 0&0&0&0&0&z&0&0&0&0\\ 0&0&0&0&1&0&0&0&0&0\\ 0&0&0&0&1&0&0&0&0&0\\ 0&0&0&0&1&0&0&0&0&0\\ 0&z&0&0&0&0&0&0&0&0\\ 0&z&0&0&0&0&0&0&0&0\\ 0&z&0&0&0&0&0&0&0&0 \end{pmatrix}, \qquad M_{1,1} = \begin{pmatrix} 0&z&0&0&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0&0&0\\ 0&z&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&z&0&0&0\\ 0&0&1&0&0&0&0&0&0&0\\ 0&z&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&z\\ 0&0&1&0&0&0&0&0&0&0 \end{pmatrix}.$$

Then it is an immediate consequence of the definition of the matrices $M_{\delta,\varepsilon}$ that

$$f(m,n) = \vec{v}^T \prod_{\ell=0}^{L} M_{m_\ell,n_\ell} M_{0,0}^2 \vec{v}, \tag{5.2}$$

for

$$m = \sum_{\ell=0}^{L} m_\ell 2^\ell, \quad n = \sum_{\ell=0}^{L} n_\ell 2^\ell$$

and

$$\vec{v}^T = (1,0,0,0,0,0,0,0,0,0).$$

The factor $M_{0,0}^2$ adds two leading 0s to the expansions of m and n to output the possible carries that could still occur.

The function $f(m,n)$ can be expressed in terms of the "bivariate 2-multiplicative matrix function" (cf. [2])

$$M(m,n) = \prod_{\ell=0}^{L} M_{m_\ell,n_\ell}. \tag{5.3}$$

We recall here that a (scalar) function φ is 2-multiplicative (cf. [4]), if

$$\varphi\left(\sum_{\ell=0}^{L} \varepsilon_\ell 2^\ell\right) = \prod_{\ell=0}^{L} \varphi(\varepsilon_\ell).$$

We now study the summatory functions

$$E(N) = \sum_{m,n<N} e^{ith(m,n)},$$

$$F(N) = \sum_{m,n<N} M(m,n).$$

The function F satisfies the relations

$$F(2N) = \sum_{\delta,\varepsilon=0}^{1} \sum_{\substack{2m+\delta<2N\\ 2n+\varepsilon<2N}} M(2m+\delta, 2n+\varepsilon) = \sum_{\delta,\varepsilon=0}^{1} M_{\delta,\varepsilon} F(N)$$

and

$$\begin{aligned} F(2N+1) &= \sum_{\delta,\varepsilon=0}^{1} \sum_{\substack{2m+\delta<2N+1\\ 2n+\varepsilon<2N+1}} M(2m+\delta, 2n+\varepsilon) \\ &= \sum_{\delta,\varepsilon=0}^{1} M_{\delta,\varepsilon} F(N) + \sum_{n<2N} M(2N,n) + \sum_{m<2N} M(m,2N) + M(2N,2N). \end{aligned}$$

Setting $A = \sum_{\delta,\varepsilon=0}^{1} M_{\delta,\varepsilon}$ and

$$G_1(N) = \sum_{n<N} M(N,n), \quad G_2(N) = \sum_{m<N} M(m,N) \tag{5.4}$$

we can rewrite this as

$$\begin{aligned} F(2N) &= AF(N) \\ F(2N+1) &= AF(N) + B_{1,0}G_1(N) + B_{2,0}G_2(N) + M_{0,0}M(N,N), \end{aligned} \tag{5.5}$$

where $B_{1,0} = M_{0,0} + M_{0,1}$ and $B_{2,0} = M_{0,0} + M_{1,0}$.

The functions G_1 and G_2 satisfy the recurrence relations

$$\begin{aligned} G_i(2N) &= B_{i,0}G_i(N) \\ G_i(2N+1) &= B_{i,1}G_i(N) + C_i M(N,N) \end{aligned} \qquad i = 1,2, \tag{5.6}$$

where $B_{1,1} = M_{1,0} + M_{1,1}$, $B_{2,1} = M_{0,1} + M_{1,1}$, $C_1 = M_{1,0}$, and $C_2 = M_{0,1}$. Iterating (5.6) yields

$$G_i\left(\sum_{\ell=0}^{L} \varepsilon_\ell 2^\ell\right) = \sum_{\ell=0}^{L} \varepsilon_\ell \prod_{j=0}^{\ell-1} B_{i,\varepsilon_j} C_i \prod_{j=\ell+1}^{L} M_{\varepsilon_j,\varepsilon_j}. \tag{5.7}$$

Inserting (5.7) into (5.5) and iterating yields $F(N) = F_0(N) + F_1(N) + F_2(N)$ with $(i = 1, 2)$

$$\begin{aligned} F_0\left(\sum_{\ell=0}^{L} \varepsilon_\ell 2^\ell\right) &= \sum_{\ell=0}^{L} \varepsilon_\ell A^\ell M_{0,0} \prod_{p=\ell+1}^{L} M_{\varepsilon_p,\varepsilon_p}, \\ F_i\left(\sum_{\ell=0}^{L} \varepsilon_\ell 2^\ell\right) &= \sum_{\ell=0}^{L} \varepsilon_\ell A^\ell B_{i,0} \sum_{j=\ell+1}^{L} \varepsilon_j \prod_{k=\ell+1}^{j-1} B_{i,\varepsilon_k} C_i \prod_{k=j+1}^{L} M_{\varepsilon_k,\varepsilon_k}. \end{aligned} \tag{5.8}$$

The matrices $M_{\delta,\varepsilon}$ only have eigenvalues 0 and 1. The matrices $B_{i,\varepsilon}$ have the characteristic polynomial

$$x^6 (x-1) \left(x^2 - x - 2e^{it}\right),$$

where the roots of the last factor are less than 2 in modulus. The characteristic polynomial of the matrix A is

$$x (x-1) \left(x^2 - x - 2e^{it}\right)^2 \left(x^3 - x^2 - 8e^{it}x - 16e^{2it}\right).$$

The dominating eigenvalue $\lambda(t)$ is a root of the fourth factor and has the following Taylor expansion around $t = 0$

$$\lambda(t) = 4 + 2it - \frac{5t^2}{8} - \frac{25it^3}{192} + \frac{131t^4}{6144} + \mathcal{O}(t^5), \tag{5.9}$$

furthermore, $|\lambda(t)| \le 4$. We will denote the modulus of the second largest eigenvalue by $\beta(t)$. Numerical studies show that $2 = \beta(0) \le \beta(t) \le \beta(\pi) = 3.04276\ldots$.

Since the arguments follow the same lines as in [10], we only give a sketch of the proof. We split the sums in (5.8) into the contribution which comes from the dominating eigenvalue and a remainder term, which originates from the other eigenvalues. Let $T^{-1}AT = \operatorname{diag}(\lambda(t), \ldots)$ be the diagonalization of A and $\Lambda = T \operatorname{diag}(\lambda(t)^{-1}, 0, \ldots, 0)T^{-1}$. We define

$$\begin{aligned}
\Psi_0\left((x_0, x_1, \ldots)\right) &= \sum_{\ell=0}^{\infty} x_\ell \Lambda^\ell M_{0,0} \coprod_{p=0}^{\ell-1} M_{x_p,x_p} \\
\Psi_i\left((x_0, x_1, \ldots)\right) &= \sum_{\ell=0}^{\infty} x_\ell \Lambda^\ell B_{i,0} \sum_{j=0}^{\ell-1} x_j \coprod_{k=j+1}^{\ell-1} B_{i,x_k} C_i \coprod_{k=0}^{j-1} M_{x_k,x_k},
\end{aligned} \tag{5.10}$$

where $\coprod_{j=a}^{b} z_j = z_b z_{b-1} \cdots z_a$. Furthermore, we set $\Psi = \vec{v}^T(\Psi_0 + \Psi_1 + \Psi_2)M_{0,0}^2\vec{v}$. The function Ψ is continuous on the infinite product space $\{0,1\}^{\mathbb{N}_0}$. Using this notation we can write

$$E(N) = \lambda(t)^{\log_2 N} \lambda(t)^{-\{\log_2 N\}} \Psi((\varepsilon_L, \varepsilon_{L-1}, \ldots, \varepsilon_0, 0^{(\infty)})) + \mathcal{O}(N \log N).$$

Since $E(N+1) - E(N) = \mathcal{O}(N)$ by definition, Ψ descends to a continuous function on $[1, 2]$ by a general argument given in [14]. See also [9].

Thus we have for $|t| = o(\log^{-\frac{1}{3}} N)$

$$\sum_{m,n<N} e^{ith(m,n)} = N^{2+\frac{it}{2\log 2} - \frac{t^2}{32\log 2} + \mathcal{O}(t^3)} \psi(t, \log_2 N) + \mathcal{O}\left(N^{\log_2 \beta(t)}\right) \tag{5.11}$$

for the continuous periodic function $\psi(t, \log_2 N) = \lambda(t)^{-\{\log_2 N\}} \Psi(2^{\{\log_2 N\}})$. Differentiation with respect to t and inserting $t = 0$ yields a second proof for Theorem 4 (the justification that this procedure really exhibits the asymptotic expansion uses the same argument as given in [2]). We notice here that this "analytic" approach gives better error terms than the "geometric" approach in Section 3. Nevertheless, we included the geometric proof, since it gives more insight.

Differentiating twice yields

$$\sum_{m,n<N} h(m,n)^2 = \frac{1}{4}N^2 \log_2^2 N + \frac{1}{16}N^2 \log_2 N + N^2(\log_2 N)\psi_1(\log_2 N) + N^2\psi_2(\log_2 N) + \mathcal{O}(N \log N),$$

where ψ_1 and ψ_2 are continuous periodic functions related to the derivatives of $\psi(t,\cdot)$. From this we compute the "variance"

$$\frac{1}{N^2}\sum_{m,n<N} h(m,n)^2 - \left(\frac{1}{N^2}\sum_{m,n<N} h(m,n)\right)^2 = \frac{1}{16}\log_2 N + \psi_2(\log_2 N) - \psi_1^2(\log_2 N) + o(1).$$

We now use a procedure which is totally similar to the proof of the central limit theorem [10, Theorem 3]. From (5.11) we derive

$$\frac{1}{N^2}\sum_{m,n<N} \exp\left(it\frac{h(m,n)-\frac{1}{2}\log_2 N}{\frac{1}{4}\sqrt{\log_2 N}}\right) = e^{-\frac{t^2}{2}}\left(1+\mathcal{O}(|t|^3\log^{-\frac{1}{2}} N)\right). \tag{5.12}$$

An application of the Berry-Esseen inequality (cf. [3, 6, 15]) to (5.12) yields (5.1).

6. Higher Dimensions

It is now natural to ask whether it is possible to extend the notion of Joint Sparse Form to higher dimensions. In this section we will generalize the syntactic results obtained in Section 2.2. It is clear that the other methods have such a generalization, too.

Let $x^{(1)}, \ldots, x^{(d)}$ be integers, $d \geq 1$. A *joint expansion* of $x^{(1)}, \ldots, x^{(d)}$ is a matrix $(x_j^{(k)})_{\substack{1\leq k\leq d\\ 0\leq j\leq \ell}}$ with entries $0, \pm 1$ such that $x^{(k)} = \sum_{j=0}^{\ell} x_j^{(k)} 2^j$ for $1 \leq k \leq d$. Its *joint Hamming weight* is the number of $0 \leq j \leq \ell$ such that there is a $1 \leq k \leq d$ with $x_j^{(k)} \neq 0$. We want to find a joint expansion of the given integers with minimum joint Hamming weight.

We will now describe a method for transforming a joint expansion into a minimal joint expansion. For a joint expansion $X = (x_j^{(k)})$, we set

$$A_j(X) := \{1 \leq k \leq d \mid x_j^{(k)} \neq 0\}.$$

Let now X be a given joint expansion of $x^{(1)}, \ldots, x^{(d)}$. If $A_0(X) = \emptyset$, there is no choice, and the column of zeros is written. If $A_1(X) \subseteq A_0(X)$, we replace $x_0^{(k)}$ by $-x_0^{(k)}$ for $k \in A_1(X)$, which yields a new joint expansion X' with $A_1(X') = \emptyset$, i.e., the next column will be a zero column. However, if $A_1(X) \setminus A_0(X) \neq \emptyset$, it is impossible to have a zero column in the first two steps. Therefore, we replace $x_0^{(k)}$ by $-x_0^{(k)}$ for all $k \in A_0(X) \setminus A_1(X)$. This new expansion X' has $A_1(X') = A_1(X) \cup A_0(X)$, which is good since it may allow a zero column in the third step. This procedure is summarized in Algorithm 2.

It is clear that Algorithm 2 yields a joint expansion X which satisfies the following syntactical rule:

$$A_{j+1}(X) \supsetneqq A_j(X) \text{ or } A_{j+1}(X) = \emptyset, \qquad j \geq 0. \tag{6.1}$$

We call any joint expansion of $x^{(1)}, \ldots, x^{(d)}$ which satisfies this rule a *Simple Joint Sparse Form* of $x^{(1)}, \ldots, x^{(d)}$. It is clear that this notion is a generalization of the non-adjacent form (for $d = 1$) and the Simple Joint Sparse Form for $d = 2$.

Algorithm 2 d-dimensional Simple Joint Sparse Form

Input: $x^{(1)}, \dots, x^{(d)}$ integers
Output: $(x_j^{(k)})_{\substack{1\le k\le d\\ 0\le j\le \ell}}$ Simple Joint Sparse Form of $x^{(1)}, \dots, x^{(d)}$

```
j ← 0
A_0 ← {k | x^(k) odd}
while ∃k : x^(k) ≠ 0 do
  x_j^(k) ← x^(k) mod 2, 1 ≤ k ≤ d
  A_{j+1} ← {k | (x^(k) − x_j^(k))/2 ≡ 1 (mod 2)}
  if A_{j+1} ⊆ A_j then
    for all k ∈ A_{j+1} do
      x_j^(k) ← −x_j^(k)
    end for
    A_{j+1} ← ∅
  else
    for all k ∈ A_j \ A_{j+1} do
      x_j^(k) ← −x_j^(k)
    end for
    A_{j+1} ← A_j ∪ A_{j+1}
  end if
  x^(k) ← (x^(k) − x_j^(k))/2, 1 ≤ k ≤ d
  j ← j + 1
end while
```

Theorem 6. *Let $d \ge 1$ and $x^{(1)}, \dots, x^{(d)}$ be integers. Then there is a unique joint expansion which satisfies* (6.1).

Furthermore, the joint Hamming weight of the Simple Joint Sparse Form is minimal amongst all joint expansions.

Proof. The existence of the Simple Joint Sparse Form is proved by Algorithm (6.1).

We now prove uniqueness. Let $X = (x_j^{(k)})_{\substack{1\le k\le d\\ 0\le j\le \ell}}$ and $Y = (y_j^{(k)})_{\substack{1\le k\le d\\ 0\le j\le \ell}}$ be Simple Joint Sparse Forms of the same integers $x^{(1)}, \dots, x^{(d)}$. Without loss of generality, we may assume that there is a $1 \le k \le d$ such that $x_0^{(k)} \ne y_0^{(k)}$. Since $2x_1^{(k)} + x_0^{(k)} \equiv 2y_1^{(k)} + y_0^{(k)} \pmod 4$, we get $x_1^{(k)} \not\equiv y_1^{(k)} \pmod 2$. Without loss of generality, we assume $x_1^{(k)} = \pm 1$. Since $A_1(X) \ne \emptyset$, there is a $k' \in A_1(X) \setminus A_0(X)$ by (6.1). We have $x_0^{(k')} = y_0^{(k')} = 0$ and $x_1^{(k')} \equiv y_1^{(k')} \pmod 2$. Therefore, $A_1(Y) \ne \emptyset$, which implies by (6.1) that $k \in A_0(Y) \subsetneq A_1(Y)$, hence $y_1^{(k)} \ne 0$, a contradiction.

We now prove minimality. Let X be a joint expansion of $x^{(1)}, \dots, x^{(d)}$ of minimal Hamming weight. For $j \ge 0$ we set $h_j(X) := 1$ if $A_j(X) \ne \emptyset$ and $h_j(X) := 0$ otherwise. for $j \ge 0$. Without loss of generality, we may assume that $(h_0(X), h_1(X), \dots)$ is lexicographically minimal amongst all minimal joint expansions. Moreover, we may assume

that

$$A_{j+1}(X) \supseteq A_j(X) \text{ or } A_{j+1} = \emptyset, \qquad j \geq 0.$$

This may be achieved by replacing $(x_{j+1}^{(k)}, x_j^{(k)}) = (0, x_j^{(k)})$ by $({x'_{j+1}}^{(k)}, {x'_j}^{(k)}) = (x_j^{(k)}, -x_j^{(k)})$ where necessary.

Assume now that $\emptyset \neq A_j(X) = A_{j+1}(X)$. Let $m = \min\{i \geq j : A_i(X) = \emptyset\}$ and set $m^{(k)} = \min\{i \geq j : x_i^{(k)} \neq x_j^{(k)}\}$ for $k \in A_j(X)$. By definition, $j+1 \leq m^{(k)} \leq m$. We now replace $\left(x_{m^{(k)}}^{(k)}, \ldots, x_j^{(k)}\right)$ by $\left((x_{m^{(k)}}^{(k)} + x_j^{(k)}), 0, \ldots, 0, -x_j^{(k)}\right)$ for $k \in A_j(X)$ and call the new expansion X'. By construction, it is a joint expansion (with digits $0, \pm 1$). For any $k \in A_j(X)$, we have ${x'}_{j+1}^{(k)} = 0$: If $m^{(k)} > j+1$, this is clear, if $m^{(k)} = j+1$, we have $x_{j+1}^{(k)} = -x_j^{(k)}$ and therefore ${x'}_{j+1}^{(k)} = x_{j+1}^{(k)} + x_j^{(k)} = 0$. This implies $A_{j+1}(X') = \emptyset$. On the other hand, by minimality of X, we have $A_m(X') \neq \emptyset$. Thus we have constructed an expansion of the same joint Hamming weight which has smaller $(h_0(X'), h_1(X'), \ldots)$, a contradiction to our assumptions on X. Therefore, X is the Simple Joint Sparse Form. □

Acknowledgment. The authors are indebted to Jörg M. Thuswaldner for suggesting a simplified proof for the connectivity of A_j in Section 3.

References

1. R. Avanzi, *On multi-exponentiation in cryptography*, 2003, manuscript, available at `http://citeseer.nj.nec.com/545130.html`.
2. G. Barat and P. J. Grabner, *Digital functions and distribution of binomial coefficients*, J. London Math. Soc. **64** (2001), 523–547.
3. A. C. Berry, *The accuracy of the Gaussian approximation to the sum of independent variates*, Trans. Amer. Math. Soc **49** (1941), 122–136.
4. H. Delange, *Sur les fonctions q-additive ou q-multiplicatives*, Acta Arith. **21** (1972), 285–298.
5. ———, *Sur la fonction sommatoire de la fonction "somme des chiffres"*, l'Enseignement Math.(2) **21** (1975), 31–47.
6. C. G. Esseen, *Fourier analysis of distribution functions. A mathematical study of the Laplace-Gaussian law*, Acta Math. **77** (1945), 1–125.
7. K. Falconer, *Fractal geometry*, John Wiley & Sons Ltd., Chichester, 1990, Mathematical foundations and applications.
8. ———, *Techniques in fractal geometry*, John Wiley & Sons Ltd., Chichester, 1997.
9. P. J. Grabner and M. Rigo, *Additive functions with respect to numeration systems on regular languages*, Monatsh. Math. (2003), to appear.
10. P. J. Grabner and J. M. Thuswaldner, *On the sum of digits function for number systems with negative bases*, Ramanujan J. **4** (2000), 201–220.
11. C. Heuberger and H. Prodinger, *On minimal expansions in redundant number systems: algorithms and quantitative analysis*, Computing **66** (2001), 377–393.
12. F. Morain and J. Olivos, *Speeding up the computations on an elliptic curve using addition-subtraction chains*, RAIRO Inform. Théor. Appl. **24** (1990), 531–543.
13. J. A. Solinas, *Low-weight binary representations for pairs of integers*, Tech. Report CORR 2001-41, University of Waterloo, 2001, manuscript, available at `http://www.cacr.math.uwaterloo.ca/techreports/2001/corr2001-41.ps`.
14. G. Tenenbaum, *Sur la non-dérivabilité de fonctions périodiques associées à certaines formules sommatoires*, The Mathematics of Paul Erdős (R. L. Graham and J. Nešetřil., eds.), Algorithms Comb., vol. 13, Springer, Berlin, 1997.

15. J. D. Vaaler, *Some extremal functions in Fourier analysis*, Bull. Amer. Math. Soc. **12** (1985), 183–216.
16. J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge University Press, New York, 1999.

(P. Grabner) Institut für Mathematik A, Technische Universität Graz, Steyrergasse 30, 8010 Graz, Austria
E-mail address: peter.grabner@tugraz.at

(C. Heuberger) Institut für Mathematik B, Technische Universität Graz, Steyrergasse 30, 8010 Graz, Austria
E-mail address: clemens.heuberger@tugraz.at

(H. Prodinger) The John Knopfmacher Centre for Applicable Analysis and Number Theory, School of Mathematics, University of the Witwatersrand, P. O. Wits, 2050 Johannesburg, South Africa
E-mail address: helmut@staff.ms.wits.ac.za