Dichotomic random number generators

Josef Eschgfäller and Andrea Scarpante

Università degli Studi di Ferrara

esg@unife.it & andrea.scarpante@student.unife.it

Abstract

We introduce several classes of pseudorandom sequences which represent a natural extension of classical methods in random number generation. The sequences are obtained from constructions on labeled binary trees, generalizing the well-known Stern-Brocot tree.

Keywords: Dichotomic random number generator, pseudorandom sequence, binary tree, Stern-Brocot tree, Pari/GP.

1. Preliminaries

Standing hypothesis 1.1 Let X be a non-empty set.

A *vector* is a finite (possibily void) sequence of elements of X. In the combinatorics of words a vector is also called a (finite) *word* and the set of all words is denoted by X^*. We shall use both terminologies.

The length of a word v is denoted by $|v|$.

Remark 1.2 For experiments, examples and graphical outputs we employed the computer algebra system Pari/GP, using a collection of functions we prepared which is available on *felix.unife.it*/++/*paritools*. The names of all functions in this collection begin with `t_`.

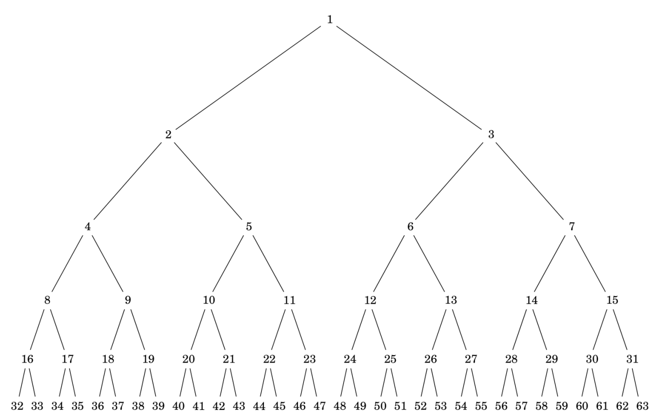
Definition 1.3 Let $a = (a_1, \ldots, a_m)$ and $b = (b_1, \ldots, b_{m+1})$ be two vectors with $|b| = |a| + 1$. Their *interleave* (or *shuffle*) $a \downarrow b$ is the vector

$(b_1, a_1, b_2, a_2, b_3, \ldots, b_m, a_m, b_{m+1})$

One has

$$(a \downarrow b)_{2j} = a_j \quad \text{for } j = 1, \ldots, m$$
$$(a \downarrow b)_{2j+1} = b_{j+1} \quad \text{for } j = 0, \ldots, m$$

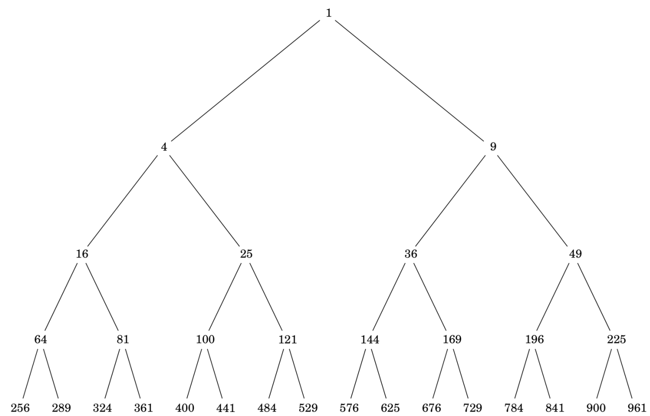
Definition 1.4 The *natural binary tree* (NBT) is the infinite binary tree labeled by the elements of $\mathbb{N} + 1$ as in the figure:



The rows (row vectors) of the tree are called its *levels*, the k-th level (beginning to count with 0) being denoted by $\mathcal{L}(*, k)$.

Remark 1.5 If $g : \mathbb{N} + 1 \longrightarrow X$ is a function, we obtain a labeled tree $\mathcal{L}(g)$ whose levels are denoted by $\mathcal{L}(g, k)$, as illustrated by the figure for $g(n) = n^2$.

Hence $\mathcal{L}(*, k) = \mathcal{L}(\mathrm{id}, k)$, where $\mathrm{id} : \mathbb{N} + 1 \longrightarrow \mathbb{N} + 1$ is the identity function, and the NBT can be written as $\mathcal{L}(*)$. More explicitly one has



$\mathcal{L}(*, k) = (2^k, 2^k + 1, \ldots, 2^{k+1} - 1)$

and therefore

$\mathcal{L}(g, k) = (g(2^k), g(2^k + 1), \ldots, g(2^{k+1} - 1))$

We count the elements in each row of the tree beginning with 1 and denote the i-th element of level k by $\mathcal{L}(g, k, i)$. Hence

$\mathcal{L}(g, k, i) := g(2^k + i - 1)$

Definition 1.6 Every $n \in \mathbb{N}+1$ belongs to a unique level k and has therefore a unique representation of the form

$n = 2^k + j$

with $k, j \in \mathbb{N}$ and $0 \leq j < 2^k$. In this case we write $n = 2^k \oplus j$.

We write also $L(n) := k$ for the level of n. Hence $j = n - 2^{L(n)}$.

In Pari/GP one obtains $L(n)$ as `#binary(n)-1`.

Remark 1.7 We project now the NBT to the unit interval $[0, 1]$ in such a way that for $n = 2^k \oplus j$ the abscissa $A(n)$ is given by

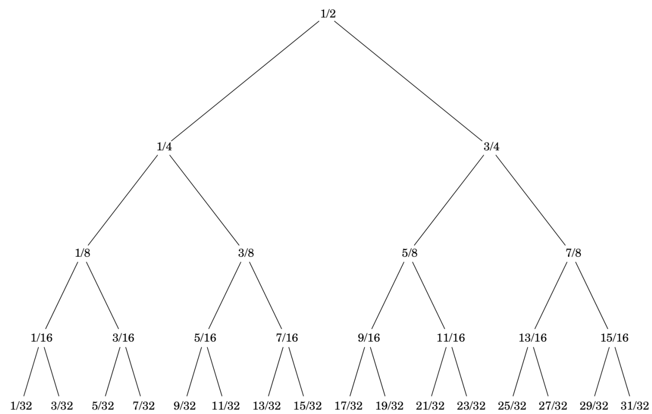
$A(n) = \dfrac{2j + 1}{2^{k+1}}$

We obtain then a new labeled tree $\mathcal{L}(A)$, which is called the *dyadic tree*. It contains every dyadic number $\dfrac{2j+1}{2^{k+1}}$ with $k, j \in \mathbb{N}$ and $0 \leq j < 2^k$ exactly once.

Definition 1.8 Let $g : \mathbb{N} + 1 \longrightarrow X$ be a function and S be a finite non-empty subset of $\mathbb{N} + 1$. Assume that S has exactly m elements. Since the abscissa function A of Remark 1.7 is injective, we can write $S = \{s_1, \ldots, s_m\}$ such that $A(s_1) < A(s_2) < \ldots < A(s_m)$. See also Remark 1.17.

The sequence $\mathcal{E}(g, S) := (g(s_1), \ldots, g(s_m))$ is then called the *binary evolution sequence* of g on S.

This is motivated by the following special case: For $k \in \mathbb{N}$ let $\mathbb{N}(k) := \left\{n \in \mathbb{N} + 1 \mid n < 2^{k+1}\right\}$ be the full initial triangle up to level k of the



NBT. Then we can form the series of sequences

$$
\begin{aligned}
&\mathcal{E}(g,0) := \mathcal{E}(g,\mathbb{N}(0)) = (g(1))\\
&\mathcal{E}(g,1) := \mathcal{E}(g,\mathbb{N}(1)) = (g(2),g(1),g(3))\\
&\mathcal{E}(g,2) := \mathcal{E}(g,\mathbb{N}(2)) = (g(4),g(2),g(5),g(1),g(6),g(3),g(7))\\
&\qquad \ldots
\end{aligned}
$$

which is called the *binary evolution scheme* of g and will be denoted by $\mathcal{E}(g)$.

We define $\mathcal{E}(g,-1)$ as the void sequence.

Again we write $\mathcal{E}(*,\ldots)$ for $\mathcal{E}(\mathrm{id},\ldots)$ and $\mathcal{E}(g,k,i)$ for the i-th element of $\mathcal{E}(g,k)$. Hence

$\mathcal{E}(g,k,i) = g(\mathcal{E}(*,k,i))$

Remark 1.9 In Def. 1.8 for every $k \in \mathbb{N}+1$ one has

$\mathcal{E}(g,k) = \mathcal{E}(g,k-1) \downarrow \mathcal{L}(g,k)$

From Definition 1.3 we have the recursion formulas

$$\mathcal{E}(*,k,2j) = \mathcal{E}(*,k-1,j) \quad \text{for } j = 1,\ldots,2^k-1$$

$$\mathcal{E}(*,k,2j+1) = 2^k + j = \mathcal{L}(*,k,j+1) \quad \text{for } j = 0,\ldots,2^k-1$$

which in particular imply that

$\mathcal{E}(*,k+\alpha,2^k) = 2^\alpha \quad$ for every $k,\alpha \in \mathbb{N}$

Remark 1.10 The evolution scheme $\mathcal{E}(*)$ is interesting and well known:

1																
2	1	3														
4	2	5	1	6	3	7										
8	4	9	2	10	5	11	1	12	6	13	3	14	7	15		
16	8	17	4	18	9	19	2	20	10	21	5	22	11	23	1	24 ...
32	16	33	8	34	17	35	4	36	18	37	9	38	19	39	2	40 ...
64	32	65	16	66	33	67	8	68	34	69	17	70	35	71	4	72 ...
128	64	129	32	130	65	131	16	132	66	133	33	134	67	135	8	136 ...
256	128	257	64	258	129	259	32	260	130	261	65	262	131	263	16	264 ...
512	256	513	128	514	257	515	64	516	258	517	129	518	259	519	32	520 ...

or, if we want to respect the positions of the elements on the tree:

```
                                        1
                  2                     1                     3
        4         2          5          1          6          3          7
   8    4    9    2    10    5    11    1    12    6    13    3    14    7    15
16 8 17 4 18 9 19 2 20 10 21 5 22 11 23 1 24 12 25 6 26 13 27 3 28 14 29 7 30 15 31
```

Notice that $\mathcal{E}(*, k)$ is always a permutation of $\mathbb{N}(k)$. This implies in particular that $\mathcal{E}(*, k)$ has length $|\mathbb{N}(k)| = 2^{k+1} - 1$.

Concatenating the vectors $\mathcal{E}(*, k)$ to an infinite sequence $\mathcal{E}(*, 0)\mathcal{E}(*, 1)\cdots$, we obtain the sequence

$$(1, 2, 1, 3, 4, 2, 5, 1, 6, 3, 7, 8, 4, 9, 2, 10, 5, 11, 1, 12, 6, 13, 3, 14, 7, 15, 16, \ldots)$$

which appears on OEIS as *A131987*. If one connects the same vectors by 0, beginning with (0), one obtains the sequence

$$u = (0, 0, 1, 0, 2, 1, 3, 0, 4, 2, 5, 1, 6, 3, 7, 0, 8, 4, 9, 2, 10, 5, 11, 1, 12, 6, 13, 3, \ldots)$$

known as *A025480*. It is described by the simple recursion

$$u_{2n} = n, \quad u_{2n+1} = u_n$$

beginning with $n = 0$.

Remark 1.11 We observe first that the position in $\mathcal{E}(*, h)$ of a number n which belongs to a level $\leq h$ is given by $A(n) \cdot 2^{h+1}$.

If in the second output of Remark 1.10 we write only the new elements of each level, we obtain a textual output of the NBT:

```
                                        1
                  2                                           3
        4                    5                     6                     7
   8         9         10         11         12         13         14         15
16   17   18   19   20    21   22    23   24    25   26    27   28    29   30    31
```

Definition 1.12 We recall the following terminology from number theory:

Let $n \in \mathbb{N}$. If $n > 0$, then there exists a unique representation of the form $n = u \cdot 2^m$ where u is odd. We write $\mathrm{odd}(n) := u$ and call it the *odd part* of n. Furthermore $|n|_2 := 2^{-m}$ is the 2-*adic absolute value* of n.

We define $\mathrm{odd}(0) := 1$ and $|0|_2 := 0$. Then:

(1) If $n > 0$, then $\mathrm{odd}(n)$ is odd.

(2) n is odd iff $\mathrm{odd}(n) = n$.

(3) $|n|_2 = 1$ iff n is odd. In particular $|1|_2 = 1$.

(4) $\mathrm{odd}(n) = 1$ iff $n = 0$ or n is a power of 2.

(5) If $n > 0$, then $n \cdot |n|_2 = \mathrm{odd}(n)$.

Theorem 1.13 *Let* $k \in \mathbb{N}$ *and* $0 \leq i < 2^{k+1}$. *Then*

$$\mathcal{E}(*, k, i) = 2^k |i|_2 + \frac{\mathrm{odd}(i) - 1}{2}$$

Proof. Write $i = 2^m \operatorname{odd}(i)$ and $\operatorname{odd}(i) = 2j+1$. Then $m \leq k$ and $0 \leq j < 2^k$, so that from Remark 1.9 we obtain

$$\begin{aligned}\mathcal{E}(*, k, i) &= \mathcal{E}(*, k-m, \operatorname{odd}(i)) = \mathcal{E}(*, k-m, 2j+1) \\ &= 2^{k-m} + j = 2^{k-m} + \frac{\operatorname{odd}(i) - 1}{2}\end{aligned}$$

Since $2^{-m} = |i|_2$, the theorem follows. $\square$

Corollary 1.14 *Let $k, j \in \mathbb{N}$ and $0 \leq j < 2^k$. Then:*

(1) $\mathcal{E}(*, k, 2^k + j) = \dfrac{2^{k+1} + 2^k + j}{2} |j|_2 - \dfrac{1}{2}$.

(2) If j is odd, then $\mathcal{E}(*, k, 2^k + j) = 2^k + 2^{k-1} + \dfrac{j-1}{2}$.

Proof. (1) The hypotheses on j and k imply that $|2^k + j|_2 = |j|_2$.
Since $2^k + j > 0$, from Theorem 1.13 we have

$$\begin{aligned}\mathcal{E}(*, k, 2^k + j) &= 2^k |2^k + j|_2 + \frac{\operatorname{odd}(2^k + j) - 1}{2} \\ &= 2^k |2^k + j|_2 + \frac{(2^k + j)|2^k + j|_2 - 1}{2} \\ &= 2^k |j|_2 + \frac{(2^k + j)|j|_2 - 1}{2} = \frac{2^{k+1} + 2^k + j}{2} |j|_2 - \frac{1}{2}\end{aligned}$$

(2) This is a special case of (1) or also of Remark 1.9. $\square$

Proposition 1.15 *Let $k, h \in \mathbb{N}$ with $h \geq k$ and $n = 2^k \oplus j \in \mathcal{L}(*, k)$. Then*

$n = \mathcal{E}(*, k, 2j+1) = \mathcal{E}(*, h, (2j+1) \cdot 2^{h-k})$

Proof. Immediate from Remark 1.9. $\square$

Remark 1.16 If we represent the NBT $\mathcal{L}(*)$ simply by its rows, we obtain the scheme

1																		
2	3																	
4	5	6	7															
8	9	10	11	12	13	14	15											
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31			
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	...
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	...
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	...
256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	...
512	513	514	515	516	517	518	519	520	521	522	523	524	525	526	527	528	529	...

The columns which appear in $\mathcal{L}(*)$ coincide with the columns which appear in the scheme $\mathcal{E}(*)$ shown in Remark 1.10.

Proof. This is immediate from Remark 1.9:

(1) Fix $i \in \mathbb{N} + 1$ and set $j := i - 1$. Then the i-th column in $\mathcal{L}(*)$ consists of the numbers $\mathcal{L}(*, k, i)$ with $k \in \mathbb{N}$ such that $i \leq 2^{k+1}$, i.e. $j < 2^{k+1}$. By Remark 1.9 we have

$\mathcal{L}(*, k, i) = \mathcal{L}(*, k, j+1) = \mathcal{E}(*, k, 2j+1) = \mathcal{E}(*, k, 2i-1)$

(2) Fix again $i \in \mathbb{N}+1$ and write $i = 2^m(2j+1)$ with $m, j \in \mathbb{N}$. As in the proof of Theorem 1.13 we have

$\mathcal{E}(*, k, i) = \mathcal{E}(*, k-m, 2j+1) = \mathcal{L}(*, k-m, j+1)$ □

Remark 1.17 (A very general method). 1. Let $(M, \prec)$ be totally ordered set and $g : M \longrightarrow X$ be a mapping. Then each finite non-empty subset $S \subset M$ can be written in the form $S = \{s_1, \ldots, s_m\}$ where $s_1 \prec s_2 \prec \ldots \prec s_m$, giving rise to the vector $(g(s_1), \ldots, g(s_m))$. In some cases one could consider this vector as a *pseudorandom* sequence.

2. We shall apply this idea to the case $M = \mathbb{N}+1$ and

$n \prec m \;\Leftrightarrow\; A(n) < A(m)$

where A is defined as in Remark 1.7. This order is known as *inorder* in computer science; cfr. Knuth [**7** p. 316-317]. The sets S will be often the sets $\mathbb{N}(k)$ - the sequences generated are then the rows $\mathcal{E}(g, k)$ of the binary evolution scheme of g.

3. It could be interesting also to work with other subsets $S \subset \mathbb{N}+1$.

2. Generalized Stern-Brocot trees

Standing hypothesis 2.1 Let X be a non-empty set. We use the standard notations from combinatorics of words:

$$X^* := \bigcup_{n=0}^{\infty} X^n$$

$$X^+ := X^* \setminus \varepsilon = \bigcup_{n=1}^{\infty} X^n$$

where ε is the empty word. Every $v \in X^*$ belongs to exactly one X^n and we define then the length of v as $|v| := n$. In particular $|\varepsilon| = 0$.

Definition 2.2 Let $\overline{\mathbb{N}} := \mathbb{N} \cup \{1/2\}$.

We extend now the function A of Remark 1.7 to a function $\overline{\mathbb{N}} \longrightarrow [0,1]$ by defining

$$A(0) := 0$$
$$A(1/2) := 1$$

The artificial elements 0 and $1/2$ belong, by definition, to level -1. We put therefore $\mathcal{L}(*,-1) := (0,1/2)$

Similarly we put, for any function $g : \overline{\mathbb{N}} \longrightarrow X$ and $k \in \mathbb{N}$

$\overline{\mathcal{E}(g,k)} := g(0)\mathcal{E}(g,k)g(1/2)$

and, as usual, $\overline{\mathcal{E}(*,k)} := \overline{\mathcal{E}(\mathrm{id},k)}$.

We shall not use the expressions $\overline{\mathcal{E}(g,k,i)}$, but define instead

$$\mathcal{E}(g,k,0) := g(0)$$
$$\mathcal{E}(g,k,2^{k+1}) := g(1/2)$$

Definition 2.3 Let $\mathcal{D} := \left\{ \dfrac{a}{2^k} \mid a,k \in \mathbb{N} \text{ with } 0 < a < 2^k \right\}$ be the set of dyadic numbers and put

$\overline{\mathcal{D}} := \mathcal{D} \cup \{0,1\} = \left\{ \dfrac{a}{2^k} \mid a,k \in \mathbb{N} \text{ with } 0 \leq a \leq 2^k \right\}$

The mapping A from Remark 1.7 can then be considered as a mapping:

$A : \overline{\mathbb{N}} \longrightarrow \overline{\mathcal{D}}$

with $A(0) := 0$ and $A(1/2) := 1$.

Notice that this mapping is bijective by construction.

Remark 2.4 Let $k \in \mathbb{N}$ and $0 \leq i < 2^{k+1}$. Then $A(\mathcal{E}(*,k,i)) = \dfrac{i}{2^{k+1}}$.

Proof. Clear, since the projections of the elements of $\mathbb{N}(k)$ are separated by intervals of length $\dfrac{1}{2^{k+1}}$.

Observe that the equation is true also for $i = 0$, since $\mathcal{E}(*,k,0) = 0$. □

Proposition 2.5 *Let $a,k \in \mathbb{N}$ with $a \leq 2^k$. Then*

$A^{-1}\left(\frac{a}{2^k}\right) = 2^{k-1}|a|_2 + \frac{\text{odd}(a)-1}{2}$

Proof. (1) Consider first the case $0 < a < 2^k$. Then $\frac{a}{2^k} \overset{2.4}{=} A(\mathcal{E}(*, k-1, a))$, hence

$A^{-1}\left(\frac{a}{2^k}\right) = \mathcal{E}(*, k-1, a) \overset{1.13}{=} 2^{k-1}|a|_2 + \frac{\text{odd}(a)-1}{2}$

(2) If $a = 0$, then $2^{k-1}|a|_2 + \frac{\text{odd}(a)-1}{2} = 0 = A^{-1}(0)$.

(3) If $a = 2^k$, then $2^{k-1}|a|_2 + \frac{\text{odd}(a)-1}{2} = \frac{1}{2} + 0 = \frac{1}{2} = A^{-1}(1)$. □

Proposition 2.6 *Let* $k \in \mathbb{N}$ *and* $1 \leq i < 2^{k+1}$. *If* i *is odd, then*

$$\mathcal{E}(*, k, i) \geq 2 \cdot \mathcal{E}(*, k, i-1) + 1$$
$$\mathcal{E}(*, k, i) \geq 2 \cdot \mathcal{E}(*, k, i+1)$$

Proof. Since i is odd, we have $|i|_2 = 1$ and $|i \pm 1|_2 \leq \frac{1}{2}$ and also $\text{odd}(i \pm 1) \leq \frac{i \pm 1}{2}$. Writing for the moment $e_j := \mathcal{E}(*, k, j)$ (for fixed k), from Theorem 1.13 now follow

$$\begin{aligned}
e_i &= 2^k|i|_2 + \frac{\text{odd}(i)-1}{2} = \frac{2^{k+1}}{2} \\
e_{i-1} &= 2^k|i-1|_2 + \frac{\text{odd}(i-1)-1}{2} \leq \frac{2^k + \frac{i-1}{2} - 1}{2} \\
&= \frac{2^{k+1} + i - 1}{4} - \frac{1}{2} = \frac{e_i - 1}{2} \\
e_{i+1} &= 2^k|i+1|_2 + \frac{\text{odd}(i+1)-1}{2} \leq \frac{2^k + \frac{i+1}{2} - 1}{2} \\
&= \frac{2^{k+1} + i - 1}{4} = \frac{e_i}{2}
\end{aligned}$$

□

Definition 2.7 For $k \in \mathbb{N}$, the sequence $\mathcal{E}(*, k)$ contains, as noticed in Remark 1.9, all elements of $\mathcal{L}(*, k)$ in their natural order, interspersed with the elements of $\mathcal{E}(*, k-1)$, these belonging to levels $< k$, as shown here for level $k = 3$, where we appended the two artificial elements on both extremities:

$$0 \quad \mathbf{8} \quad 4 \quad \mathbf{9} \quad 2 \quad \mathbf{10} \quad 5 \quad \mathbf{11} \quad 1 \quad \mathbf{12} \quad 6 \quad \mathbf{13} \quad 3 \quad \mathbf{14} \quad 7 \quad \mathbf{15} \quad 1/2$$

The elements of $\mathcal{L}(*, 3)$ are shown in boldface type. Similarly for every $k \in \mathbb{N}$ each number $n \in \mathcal{L}(*, k)$ has a left and a right neighbor in $\overline{\mathcal{E}(*, k)}$, which belong to levels $< k$ and are called the *left support* $\text{Ls}(n)$ and the *right support* $\text{Rs}(n)$ of n respectively.

It is also clear (by the very construction of A in Remark 1.7) that

$$A(\mathrm{Ls}(n)) = A(n) - \frac{1}{2^{k+1}}$$
$$A(\mathrm{Rs}(n)) = A(n) + \frac{1}{2^{k+1}}$$

Notice finally that, since every $n \in \mathbb{N}+1$ belongs to a unique level k, the left and the right support of n are well defined for every such n.

Remark 2.8 (1) For $n \in \mathbb{N}$ we have:

$$\begin{array}{rcll} \mathrm{Ls}(2n) & = & \mathrm{Ls}(n) & \text{if} \quad n > 0 \\ \mathrm{Ls}(2n+1) & = & n & \\ \mathrm{Rs}(2n) & = & n & \text{if} \quad n > 0 \\ \mathrm{Rs}(2n+1) & = & \mathrm{Rs}(n) & \text{if} \quad n > 0 \\ \mathrm{Rs}(n) & = & \mathrm{Ls}(n+1) & \text{if} \quad n+1 \text{ is not a power of } 2 \end{array}$$

(2) Moreover:

$$\begin{array}{rcll} \mathrm{Ls}(2^k) & = & 0 & \text{for} \quad k \in \mathbb{N} \\ \mathrm{Rs}(2^k - 1) & = & 1/2 & \text{for} \quad k \in \mathbb{N}+1 \end{array}$$

(3) In particular $\mathrm{Ls}(1) = 0$ and $\mathrm{Rs}(1) = 1/2$.

Proof. This is clear from the NBT. □

Proposition 2.9 *Let* $n \in \mathbb{N}+1$. *Then* $\mathrm{Ls}(n) = \dfrac{\mathrm{odd}(n) - 1}{2}$.

Proof. Write $n = 2^m \,\mathrm{odd}(n)$ with $\mathrm{odd}(n) = 2i + 1$. By Remark 2.8 then

$$\mathrm{Ls}(n) = \mathrm{Ls}(2i+1) = i = \frac{\mathrm{odd}(n) - 1}{2}$$ □

Remark 2.10 Let $n \in \mathbb{N}+1$.

(1) If n is even, then $\mathrm{Rs}(n) = \dfrac{n}{2} > 2\,\mathrm{Ls}(n)$, hence $n > 4\,\mathrm{Ls}(n)$.

(2) If n is odd > 1, then $\mathrm{Ls}(n) = \dfrac{n-1}{2} \geq 2\,\mathrm{Rs}(n)$, hence $n > 4\,\mathrm{Rs}(n)$.

Proof. (1) From Remark 2.8 we know that $\mathrm{Rs}(n) = \dfrac{n}{2}$. Now n is even, therefore $\mathrm{odd}(n) \leq \dfrac{n}{2}$. Hence

$$\mathrm{Ls}(n) \overset{2.9}{=} \frac{\mathrm{odd}(n) - 1}{2} \leq \frac{\frac{n}{2} - 1}{2} = \frac{n}{4} - \frac{1}{2}$$

thus

$$\frac{n}{4} \geq \mathrm{Ls}(n) + \frac{1}{2} > \mathrm{Ls}(n)$$

(2) From Remark 2.8 we know that $\mathrm{Ls}(n) = \dfrac{n-1}{2}$.
Suppose first that $n+1$ is not a power of 2. Then

$$\mathrm{Rs}(n) = \mathrm{Ls}(n+1) = \frac{\mathrm{odd}(n+1) - 1}{2} \leq \frac{\frac{n+1}{2} - 1}{2} = \frac{n-1}{4}$$

hence

$$\frac{n}{4} \geq \mathrm{Rs}(n) + \frac{1}{4} > \mathrm{Rs}(n)$$

Otherwise, if $n+1$ is a power of 2, then $\mathrm{Rs}(n) = \frac{1}{2} < \frac{3}{4} \leq \frac{n}{4}$, since $n \geq 3$ by hypothesis. □

Definition 2.11 Let $f : X \times X \longrightarrow X$ be a mapping and $a, b \in X$. Then we define a mapping $g := f_{ab} : \overline{\mathbb{N}} \longrightarrow X$ in the following way:

$$\begin{aligned} g(0) &:= a \\ g(1/2) &:= b \\ g(n) &:= f(g(\mathrm{Ls}(n)), g(\mathrm{Rs}(n))) \text{ for } n \in \mathbb{N}+1 \end{aligned}$$

Since for $n \in \mathbb{N}+1$ the levels of $\mathrm{Ls}(n)$ and $\mathrm{Rs}(n)$ are both strictly smaller than the level of n, the mapping f_{ab} is well defined.

Notice that always $g(1) = f(a, b)$.

Substituting each $n \in \mathbb{N}+1$ in the NBT by $f_{ab}(n)$, we obtain the labeled binary tree $\mathcal{L}(f_{ab})$ which can be considered as a *generalized Stern-Brocot* tree, as we shall see (Proposition 2.14).

Remark 2.12 Let $g : \overline{\mathbb{N}} \longrightarrow X$ be a function and $k \in \mathbb{N}$. Then

$$\overline{\mathcal{E}(g,k)} = \mathcal{L}(g,k) \downarrow \overline{\mathcal{E}(g,k-1)}$$

Proof. This follows from Remark 1.9, because appending one element on each side of the shorter sequence in Definition 1.3 corresponds to reversing the order of the two sequences around the $\downarrow$ symbol. □

Remark 2.13 Let $k \in \mathbb{N}$ and $n \in \mathcal{L}(*, k)$. Recall from Definition 2.7 that $\mathrm{Ls}(n)$ and $\mathrm{Rs}(n)$ are the left and right neighbors of n in $\overline{\mathcal{E}(*,k)}$ and thus are neighbors of each other in $\overline{\mathcal{E}(*,k-1)}$.

Consider now any function $g : \overline{\mathbb{N}} \longrightarrow X$. Then again $g(\mathrm{Ls}(n))$ and $g(\mathrm{Rs}(n))$ are neighbors of each other in $\overline{\mathcal{E}(g,k-1)}$ and $g(n)$ is inserted between them in $\overline{\mathcal{E}(g,k)}$.

If follows that, if now $f : X \times X \longrightarrow X$, $a, b \in X$ and $g := f_{ab}$, then $g(n)$ is the value of f evaluated on the left and right neighbors of $g(n)$ in $\overline{\mathcal{E}(g,k)}$ (taken in the position determined by n if it appears more than once), which both can be calculated on a lower level.

From Remark 2.12 we see that the sequence $\overline{\mathcal{E}(f_{ab},k)}$ is obtained from $x := \overline{\mathcal{E}(f_{ab},k-1)}$ by inserting between x_i and x_{i+1} the value $f(x_i, x_{i+1})$.

Proposition 2.14 *The NBT itself can be considered as a generalized Stern-Brocot tree.*

For this we define $f : \overline{\mathbb{N}} \times \overline{\mathbb{N}} \longrightarrow \overline{\mathbb{N}}$ *by*

$$f(x,y) := \begin{cases} 2y & \text{if } x < y \\ 2x+1 & \text{if } x > y \\ 0 & \text{otherwise} \end{cases}$$

and choose $a := 0$, $b := 1/2$.*Then* $f_{ab}(n) = n$ *for every* $n \in \overline{\mathbb{N}}$.

Proof. Let $g := f_{ab}$. By definition $g(0) = 0$, $g(1/2) = 1/2$.

Suppose $n \in \mathbb{N}+1$. Then $n \in \mathcal{L}(*, k)$ for some $k \in \mathbb{N}$. We use Remark 2.10 and show the proposition by induction on k.

$\underline{k=0}$: Then $n = 1$. But $g(1) = f(0, 1/2) = 2 \cdot \frac{1}{2} = 1$.

$\underline{k-1 \longrightarrow k}$: If n is even, then $\mathrm{Rs}(n) = \dfrac{n}{2} > \mathrm{Ls}(n)$, hence

$$g(n) = f(g(\mathrm{Ls}(n)), g(n/2)) \stackrel{IND}{=} f(\mathrm{Ls}(n), n/2) = 2\frac{n}{2} = n$$

If n is odd, then $\mathrm{Ls}(n) = \dfrac{n-1}{2} > \mathrm{Rs}(n)$, hence

$$g(n) = f(g((n-1)/2), g(\mathrm{Rs}(n))) \stackrel{IND}{=} f((n-1)/2, \mathrm{Rs}(n)) = n$$ □

Definition 2.15 Let $f : X \times X \longrightarrow X$ be a mapping, and $a, b \in X$.

Then we may construct a mapping $f_{ab} : \overline{\mathbb{N}} \longrightarrow X$ as in Definition 2.11.

The triple (f, a, b) is called a *dichotomic generator* or simply a generator (of random sequences).

Remark 2.16 Let $f : X \times X \longrightarrow X$ be mapping and $a, b \in X$.
For $k \in \mathbb{N}$ then the sequence $\mathcal{E}(f_{ab}, k) = (x_1, \ldots, x_{2^{k+1}-1})$ can be calculated by the general recursion formulas in Remark 1.9, but, as a consequence of Remark 2.13, also by the following algorithm wich we describe in Pari/GP and which justifies the name *dichotomic generator*:

```
dicho (f,n,i,j,a,b) = {my (m,x);
if (n==i,return(a), n==j, return(b)); m=(i+j)\2;
x=f(a,b); if (n==m,return(x));
if (n<m, dicho(f,n,i,m,a,x), dicho(f,n,m,j,x,b))}

\\ Example:
f (x,y) = (3*x+5*y+2)%7
p=2^101; q=2^94

v=[dicho(f,n,0,p,0,1) | n<-[q..q+40]]
t_to(v,60,,"")
\\ 06562615052102001446426543236352445110603
```

Notice that we may use this algorithm for calculating far away elements of the sequence $\mathcal{E}(f_{ab}, k)$, as we did in this example, where, for $f(x, y) = (3x + 5y + 2) \mod 7$, $a = 2$, $b = 3$, $k = 100$, the elements x_n are calculated for $n = 2^{94}, 2^{94}+1, \ldots, 2^{94}+40$. This calculation is done directly on these indices without the need for calculating the preceding elements.

Remark 2.17 Each finite sequence $x_0 = a, \ldots, x_m = b$ of distinct elements can be obtained by the method of Remark 2.16: We define $f(x_0, x_m) := x_{[m/2]}$ and similarly $f(x_i, x_j) := x_{[(i+j)/2]}$, wherever these indices appear; all other values of f can be chosen arbitrarily.

For example the sequence $(x_0, \ldots, x_{11})$ can be obtained as a dichotomic sequence if we define:

$$
\begin{aligned}
f(x_0, x_{11}) &:= x_5 \\
f(x_0, x_5) &:= x_2 \\
f(x_5, x_{11}) &:= x_8 \\
f(x_0, x_2) &:= x_1 \\
f(x_2, x_5) &:= x_3 \\
f(x_5, x_8) &:= x_6 \\
f(x_8, x_{11}) &:= x_9 \\
f(x_6, x_8) &:= x_7 \\
f(x_3, x_5) &:= x_4 \\
f(x_9, x_{11}) &:= x_{10}
\end{aligned}
$$

Remark 2.18 As far as we know, the idea of using Remark 2.13 for the generation of random sequences appears in Centrella [**2**] (written under the supervision of J. E.) and Kreindl [**8**].

3. Continuative Mappings

Remark 3.1 Let $g : \mathbb{N} + 1 \longrightarrow X$ be a mapping.

We shall then consider the sequences $\mathcal{E}(g, k)$ as (finite) random sequences, in the spirit of Remark 1.17.

For applications where unpredictability of the generated sequences is desired, as for example in cryptology, it may be a pleasing aspect of the method that the sequences $\mathcal{E}(g, k)$ for different k can be rather unrelated. For theoretical investigations, however, also the case that $\mathcal{E}(g, k+1)$ is always a continuation of $\mathcal{E}(g, k)$, i.e., that $\mathcal{E}(g, k)$ is always a prefix of $\mathcal{E}(g, k+1)$, will be interesting.

We shall now consider the question, when this happens, if g is of the form f_{ab} as in Definition 2.11.

Definition 3.2 Let $g : \mathbb{N} + 1 \longrightarrow X$ be a mapping. We define an infinite sequence $\mathcal{E}(g, \infty) : \mathbb{N} + 1 \longrightarrow X$ by setting

$\mathcal{E}(g, \infty, n) := \mathcal{E}(g, \infty)(n) := \mathcal{E}(g, k, n)$

if $n \in \mathcal{L}(*, k)$. This sequence consists of the values of g on the bold numbers in the following scheme (see Remark 1.10):

$$
\begin{array}{lllllllllllllllllllllllllllllll}
\mathbf{1} \\
2 & \mathbf{1} & \mathbf{3} \\
4 & 2 & 5 & \mathbf{1} & \mathbf{6} & \mathbf{3} & \mathbf{7} \\
8 & 4 & 9 & 2 & 10 & 5 & 11 & \mathbf{1} & \mathbf{12} & \mathbf{6} & \mathbf{13} & \mathbf{3} & \mathbf{14} & \mathbf{7} & \mathbf{15} \\
16 & 8 & 17 & 4 & 18 & 9 & 19 & 2 & 20 & 10 & 21 & 5 & 22 & 11 & 23 & \mathbf{1} & \mathbf{24} & \mathbf{12} & \mathbf{25} & \mathbf{6} & \mathbf{26} & \mathbf{13} & \mathbf{27} & \mathbf{3} & \mathbf{28} & \mathbf{14} & \mathbf{29} & \mathbf{7} & \mathbf{30} & \mathbf{15} & \mathbf{31}
\end{array}
$$

The bold numbers themselves represent the sequence $\mathcal{E}(*, \infty)$.

The sequence $\mathcal{E}(g, \infty)$, always defined, is of course interesting only if $\mathcal{E}(g, k+1)$ is a continuation of $\mathcal{E}(g, k)$ for every $k \in \mathbb{N}$.
In this case the mapping g is called *continuative*.

If g is defined on some set containing $\mathbb{N} + 1$ (usually on $\mathbb{N}$ or on $\overline{\mathbb{N}}$), this means, by convention, that the restriction $g_{|\mathbb{N}+1}$ is continuative.

Remark 3.3 Since for $k, j \in \mathbb{N} + 1$ one has $2j + 1 \in \mathcal{L}(*, k)$ iff $j \in \mathcal{L}(*, k-1)$, the recursion formulas of Remark 1.9 become now

$$
\begin{aligned}
\mathcal{E}(g, \infty, 1) &= g(1) \\
\mathcal{E}(g, \infty, 2j) &= \mathcal{E}(g, \infty, j) \quad \text{ for } j \in \mathbb{N} + 1 \\
\mathcal{E}(g, \infty, 2j+1) &= g(2^k + j) \quad \text{ for } k \in \mathbb{N} \text{ and } 2^{k-1} \le j < 2^k
\end{aligned}
$$

Proposition 3.4 *Let $g : \mathbb{N} + 1 \longrightarrow X$ be a mapping. Then the following statements are equivalent:*

(1) g is continuative.

(2) g is constant on each column of $\mathcal{E}(*)$.

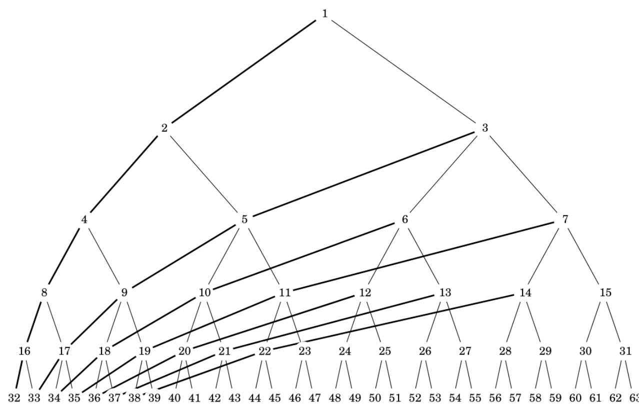
(3) g is constant on each column of $\mathcal{L}(*)$.

(4) $\mathcal{E}(g, \infty, 2j+1) = g(2^k + j)$ for every $k, j \in \mathbb{N}$ with $j < 2^k$.

(5) $g(2^k + j) = g(2^m + j)$ *for every* $k, m, j \in \mathbb{N}$ *such that* $j < 2^k \leq 2^m$.
(6) $g(n) = g(n + 2^{L(n)} \cdot (2^r - 1))$ *for every* $n \in \mathbb{N} + 1, r \in \mathbb{N}$.

Here $L(n)$ is the level of n as in Definition 1.6. The rows and columns of $\mathcal{E}(*)$ were represented in Remark 1.10, those of $\mathcal{L}(*)$ in Remark 1.16.

The columns of $\mathcal{L}(*)$ appear also as leftward diagonals in the tree-like representation (that is, in the NBT), as in the figure:



Proof. (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (4) $\Leftrightarrow$ (5): By definition.

(2) $\Leftrightarrow$ (3): We observed in Remark 1.16 that $\mathcal{L}(*)$ and $\mathcal{E}(*)$ have the same columns - which in $\mathcal{L}(*)$ appear only once, in $\mathcal{E}(*)$ infinitely often.

(5) $\Leftrightarrow$ (6): Clear. $\square$

Lemma 3.5 *Let* $f : X \times X \longrightarrow X$ *be a mapping and* $a, b \in X$. *For every* $k \in \mathbb{N}$ *then*

$\mathcal{E}(f_{ab}, k+1) = \mathcal{E}(f_{a,f(a,b)}, k) \cdot f(a,b) \cdot \mathcal{E}(f_{f(a,b),b}, k)$

where the dot denotes concatenation of words.

Proof. Clear. $\square$

Lemma 3.6 *Let* $f : X \times X \longrightarrow X$ *be a mapping and* $b, c \in X$. *Assume that* $f(x,b) = f(x,c)$ *for every* $x \in X$.
Then $f_{ab} = f_{ac}$ *for every* $a \in X$.

Proof. We show by induction on $k \in \mathbb{N}$ that $\mathcal{E}(f_{ab}, k) = \mathcal{E}(f_{ac}, k)$ for every $a \in X$ and every $k \in \mathbb{N}$.

$\underline{k = 0}$: Applying the hypothesis to $x = a$ we have $f(a,b) = f(a,c)$, hence
$\mathcal{E}(f_{ab}, 0) = (f(a,b)) = (f(a,c)) = \mathcal{E}(f_{ac}, 0)$

$\underline{k \longrightarrow k+1}$: One has

$$\begin{aligned}
\mathcal{E}(f_{ab}, k+1) &\overset{3.5}{=} \mathcal{E}(f_{a,f(a,b)}, k) \cdot f(a,b) \cdot \mathcal{E}(f_{f(a,b),b}, k) \\
&= \mathcal{E}(f_{a,f(a,c)}, k) \cdot f(a,c) \cdot \mathcal{E}(f_{f(a,c),b}, k) \\
&\overset{IND}{=} \mathcal{E}(f_{a,f(a,c)}, k) \cdot f(a,c) \cdot \mathcal{E}(f_{f(a,c),c}, k) = \mathcal{E}(f_{ac}, k+1)
\end{aligned}$$

where we used again that $f(a,b) = f(ac)$, applying in $\overset{IND}{=}$ the induction hypothesis on $f(a,c)$ instead of a. □

Proposition 3.7 *Let $f : X \times X \longrightarrow X$ be a mapping and $a, b \in X$. Assume that $f(x, f(a,b)) = f(x,b)$ for every $x \in X$.*

Then f_{ab} is continuative.

Proof. For every $k \in \mathbb{N}$ we have

$$\mathcal{E}(f_{ab}, k+1) \overset{3.5}{=} \mathcal{E}(f_{a,f(a,b)}, k) \cdot f(a,b) \cdot \mathcal{E}(f_{f(a,b),b}, k) \qquad (*)$$

The hypothesis $f(x,b) = f(x, f(a,b))$ for every $x \in X$ implies by Lemma 3.6 that $f_{a,f(a,b)} = f_{ab}$, hence (*) implies that $\mathcal{E}(f_{ab}, k) = \mathcal{E}(f_{a,f(a,b)}, k)$ is a prefix of $\mathcal{E}(f_{ab}, k+1)$. □

Corollary 3.8 *Let $f : X \times X \longrightarrow X$ be a mapping and $a, b \in X$.*

If $f(a,b) = b$, then f_{ab} is continuative.

Remark 3.9 Let $g : \overline{\mathbb{N}} \longrightarrow X$ be a mapping and set $a := g(0)$, $b := g(1/2)$. Consider the sequences $\overline{\mathcal{E}(g,k)}$:

$$\begin{array}{llllllllll} a & g(1) & b \\ a & g(2) & g(1) & g(3) & b \\ a & g(4) & g(2) & g(5) & g(1) & g(6) & g(3) & g(7) & b \\ \ldots \end{array}$$

Then, for any fixed $k \in \mathbb{N}$, $\overline{\mathcal{E}(g,k+1)}$ is a continuation of $\overline{\mathcal{E}(g,k)}$ iff $\mathcal{E}(g,k+1)$ is a continuation of $\mathcal{E}(g,k)$ and, in addition, $g(1) = b$.

Corollary 3.10 *Let $f : X \times X \longrightarrow X$ be a mapping and $a, b \in X$. The following statements are equivalent:*

(1) $\overline{\mathcal{E}(f_{ab}, k+1)}$ is a continuation of $\overline{\mathcal{E}(f_{ab}, k)}$ for every $k \in \mathbb{N}$.

(2) $\mathcal{E}(f_{ab}, k+1)$ is a continuation of $\mathcal{E}(f_{ab}, k)$ for every $k \in \mathbb{N}$ and, in addition, $f(a,b) = b$.

(3) $f(a,b) = b$.

Proof. (1) $\Leftrightarrow$ (2): Remark 3.9.

(2) $\Rightarrow$ (3): Clear.

(3) $\Rightarrow$ (2): Corollary 3.8.

We found this result first in Kreindl [**8**]. □

4. One-sided generators

Standing hypothesis 4.1 Let X be a non-empty set.

Definition 4.2 If P is a property defined for mappings, we say that the generator (f, a, b) has property P if the mapping f_{ab} has property P. Thus for example the generator (f, a, b) is called continuative, if the mapping f_{ab} is continuative.

Definition 4.3 A dichotomic generator (f, a, b) is called *one-sided*, if $f(x, y)$ depends only on x. In this case there exists a function $\phi : X \longrightarrow X$ such that $f(x, y) = \phi(x)$ for every $x, y \in X$.

Remark 4.4 Every one-sided generator is continuative.

Proof. Let (f, a, b) be a one-sided generator.

For every $x \in X$ then $f(x, f(a, b)) = f(x, b)$, since f does not depend on the second argument. Hence f_{ab} is continuative by Proposition 3.6. □

Definition 4.5 Let $\phi : X \longrightarrow X$ be a mapping and $a \in X$. We define a mapping $g : \mathbb{N} \longrightarrow X$ in the following way:

$$g(0) := a$$
$$g(n) := \phi(g(\mathrm{Ls}(n))) \quad \text{for } n \in \mathbb{N} + 1$$

and write also $\phi_a := g$. Since for $n > 0$ always $\mathrm{Ls}(n) < n$, the mapping is well defined.

On its domain of definition ϕ_a coincides obviously with f_{ab}, if we define $f(x, y) := \phi(x)$ and choose $b \in X$ arbitrarily. Therefore we shall also call the couple (ϕ, a) or, for short, the mapping ϕ_a itself, a one-sided generator.

Proposition 4.6 *Let $\phi : X \longrightarrow X$ be a mapping and $a \in X$. Then:*

$$\phi_a(2j) = \phi_a(j)$$
$$\phi_a(2j + 1) = \phi(\phi_a(j))$$

for every $j \in \mathbb{N}$. In particular $\phi_a(1) = \phi(a)$.

Proof. (1) This statement is trivial for $j = 0$. Assume $j > 0$. Then

$$\phi_a(2j) = \phi(\phi_a(\mathrm{Ls}(2j))) \overset{2.8}{=} \phi(\phi_a(\mathrm{Ls}(j))) = \phi_a(j).$$

(2) $\phi_a(2j + 1) = \phi(\phi_a(\mathrm{Ls}(2j + 1))) \overset{2.8}{=} \phi(\phi_a(j))$. □

Theorem 4.7 *Let $\phi : X \longrightarrow X$ be a mapping and $a \in X$. Then*

$$a\mathcal{E}(\phi_a, \infty) = \phi_a$$

or, equivalently,

$$\mathcal{E}(\phi_a, \infty, n) = \phi_a(n)$$

for every $n \in \mathbb{N} + 1$.

Proof. Let $u := a\mathcal{E}(\phi_a, \infty)$, hence $u_0 = a$ and $u_n = \mathcal{E}(\phi_a, \infty, n)$ for $n \in \mathbb{N} + 1$.

(1) We show that u satisfies the same recursion rules as ϕ_a, i.e., that

$$\begin{aligned} u_1 &= \phi(a) \\ u_{2j} &= u_j \\ u_{2j+1} &= \phi(u_j) \end{aligned}$$

for every $j \in \mathbb{N}+1$. This clearly implies $u = \phi_a$.

(2) Since by Remark 4.4 ϕ_a is continuative, from Proposition 3.4 we have

$$\begin{aligned} u_1 &= \phi_a(1) = \phi(a) \\ u_{2j} &= u_j \ \text{ for } j \in \mathbb{N}+1 \\ u_{2j+1} &= \phi_a(2^k + j) \ \text{ for every } k, j \in \mathbb{N} \text{ with } j < 2^k \end{aligned}$$

(3) We show by induction on $k \in \mathbb{N}$ the following statement:

If $0 \le j < 2^k$, then $u_{2j+1} = \phi(u_j)$.

$\underline{k=0}$: In this case $j = 0$ and we have to show that $u_1 = \phi(u_0) = \phi(a)$, and this is true.

$\underline{k-1 \longrightarrow k}$: Assume $0 \le j < 2^k$.

Suppose first that j is odd. Since now $k > 0$, also $2^k + j$ is odd, thus

$$\begin{aligned} u_{2j+1} &= \phi(\phi_a(\mathrm{Ls}(2^k + j))) \overset{2.8}{=} \phi\left(\phi_a\left(\frac{2^k + j - 1}{2}\right)\right) \\ &= \phi\left(\phi_a\left(2^{k-1} + \frac{j-1}{2}\right)\right) \overset{(2)}{=} \phi\left(u_{2\frac{j-1}{2}+1}\right) = \phi(u_j) \end{aligned}$$

since $0 \le \dfrac{j-1}{2} < 2^{k-1}$.

Suppose now that j is even. For $j = 0$ we have $u_1 = \phi(u_0) = \phi(a)$ as before. Otherwise write $j = 2^m r$ with r odd. Then $0 < m < k$ and

$$\begin{aligned} u_{2j+1} &\overset{(2)}{=} \phi_a(2^k + j) = \phi_a(2^m(2^{k-m} + r)) \overset{4.6}{=} \phi_a(2^{k-m} + r) \\ &\overset{(2)}{=} u_{2r+1} \overset{IND}{=} \phi(u_r) = \phi\left(u_{\frac{j}{2^m}}\right) \overset{(2)}{=} \phi(u_j) \end{aligned}$$

□

Remark 4.8 The conclusion in Theorem 4.7 is not more true for general continuative dichotomic generators, as the example $(f, 1, 6)$ with $f(x, y) = (3x + 2y + 7) \mod 8$ shows:

```
g=f_{1,6}      : 6 6 5 6 5 3 2 6 5 3 2 7 2 2 1 6 5 3 2 7 2 2 1 7 2 4 7 2 ...
E(g,infinite) : 6 6 5 6 3 5 2 6 7 3 2 5 2 2 1 6 7 7 2 3 4 2 7 5 2 2 1 2 ...
```

Remark 4.9 Since in the proof of Theorem 4.7 u is uniquely determined by the recursion rules (*), for a sequence $u \in X^{\mathbb{N}}$ with $a := u_0$ and a mapping $\phi : X \longrightarrow X$ the following statements are equivalent:

(1) $u = \phi_a$.

(2) $u = a\mathcal{E}(\phi_a, \infty)$.

(3) For every $j \in \mathbb{N}$ we have $u_{2j} = u_j$ and $u_{2j+1} = \phi(u_j)$.

The infinite sequences which obey a recursion rule of type (3) are therefore exactly the sequences obtained by a one-sided generator as in Theorem 4.7.

Example 4.10 Let u be the Thue-Morse sequence $u \in \{0,1\}^{\mathbb{N}}$ defined by $u_0 := 0, u_{2j} = u_j, u_{2j+1} = 1 - u_j$.

By Theorem 4.7 it can be obtained as $u = 0\mathcal{E}(\phi_0, \infty)$, where $\phi(x) := 1 - x$.

Example 4.11 Consider the function $\beta := \bigcirc_n n + 1 : \mathbb{N} \longrightarrow \mathbb{N}$ and define $h := \beta_0 : \mathbb{N} \longrightarrow \mathbb{N}$ in accordance with Definition 4.5 by

$$\begin{aligned} &h(0) := 0 \\ &h(n) := h(\mathrm{Ls}(n)) + 1 \quad \text{for } n \in \mathbb{N} + 1 \end{aligned}$$

Then by Theorem 4.7

$h = 0\mathcal{E}(h, \infty) = 0\ 1\ 1\ 2\ 1\ 2\ 2\ 3\ 1\ 2\ 2\ 3\ 2\ 3\ 3\ 4\ 1\ 2\ 2\ 3\ 2\ 3\ 3\ 4\ 2\ 3\ \ldots$

One can also show that $h(n)$ is equal to the Hamming weight of n, i.e. to the number of ones in the binary representation of n. This sequence is well known and listed as *A000120* in the OEIS.

Proposition 4.12 *Let $\phi : X \longrightarrow X$ be a mapping and $a \in X$.*
Define h as in Example 4.11. Then
$\phi_a(n) = \phi^{h(n)}(a)$
for every $n \in \mathbb{N}$.

Proof. We show the proposition by induction on n.

$\underline{n = 0}$: $\phi^{h(0)}(a) = \phi^0(a) = a = \phi_a(0)$.

$\underline{n - 1 \longrightarrow n}$: Now $n > 0$ and we may write $n = 2^m r$ with r odd.

By Proposition 2.9 $\mathrm{Ls}(n) = \dfrac{r-1}{2}$, hence $h(n) = h\left(\dfrac{r-1}{2}\right) + 1$. Further

$$\begin{aligned} \phi_a(n) &= \phi_a(2^m r) \overset{4.6}{=} \phi_a(r) = \phi\left(\phi_a\left(\frac{r-1}{2}\right)\right) \\ &\overset{IND}{=} \phi\left(\phi^{h\left(\frac{r-1}{2}\right)}(a)\right) = \phi^{h\left(\frac{r-1}{2}\right)+1}(a) = \phi^{h(n)}(a) \end{aligned}$$

□

5. Examples

Remark 5.1 In the following chapter we present examples of dichotomic generators.

For every generator are first indicated the function $f : X \times X \longrightarrow X$ (with X usually tacitly understood) and the initial values $a, b \in X$.

Then follows the beginning of the binary evolution scheme (Definition 1.8) of the function f_{ab}, from which the last row is selected. This vector of values is represented graphically in a bar diagram; by a similar bar diagram we represent also the absolute values of the discrete Fourier transform of the vector, with the origin centered.

Using the values $x_i - \mu$ as increments, where μ is the mean of the vector, we obtain a random walk which is given too.

On the left then we present a usually longer vector of the same level of the evolution scheme by points in the plane, which are calculated in the following manner: As for the discrete Kolmogorov-Smirnov test (cf. Centrella [**2**]) first the vector is decomposed in ordered non-overlapping blocks of length 10. Then the Ruffini-Horner method for powers of 2 is applied to each block giving us a vector of real numbers:

$u := (u_1, ..., u_r)$

where r is the number of blocks.
Finally each entry u_i of u is divided by 2^{10}, which gives the vector

$v := (v_1, ..., v_r)$ with $v_i := \frac{u_i}{2^{10}}$.

Now from the pairs (v_{2k}, v_{2k+1}) we obtain a 2-dimensional representation of the sequence.

Remark 5.2 Each time the numerical results of a battery of tests are given using the following shortcuts:

`runs` .... *run test* (cf. Bassham a.o. [**1**], Maurer [**10**] and Fisz [**5**])

`freq` .... *frequency test* (cf. Bassham a.o. [**1**])

`cusum` .... *cumulative sum test* (cf. Bassham a.o. [**1**])

`blocks` .... *blocks test* (cf. Fisz [**5**])

`autocorr` .... *auto-correlation test* (cf. Bassham a.o. [**1**])

`longrun` .... *longrun test* (cf. Guibas & Odlyzko [**6** p. 252-253])

`2bits` .... 2-*bit test* (cf. Fisz [**5** page 399] and Bassham a.o. [**1**])

`ks_discrete` .... *discrete Kolmogorov-Smirnov test* (cf. Kuipers & Niederreiter [**9** p. 90-92] and Fisz [**5**])

`DTF` .... *discrete Fourier transform test* (cf. Bassham a.o. [**1**])

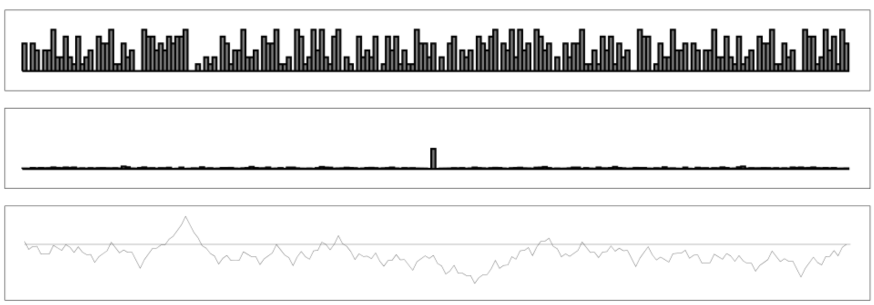
`Maurer` .... *Maurer's universal test* (cf. Maurer [**10**], Coron & Naccache [**3**], Doğanaksoy & Tezcan [**4**] and Bassham a.o. [**1**])

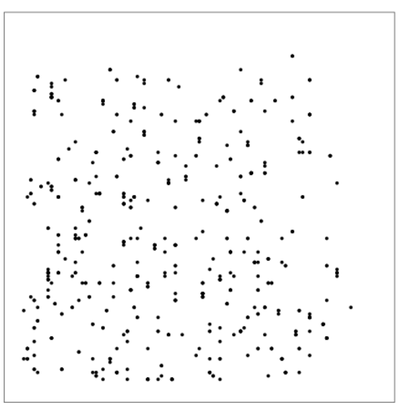
For every example we simply project the generate sequence onto $\mathbb{Z}/2\mathbb{Z}$ and we apply the above, most commonly used, bit tests, as described in the cited references.

Example 5.3

$$\boxed{\begin{array}{r} f(x,y) = (x+y+1) \mod 7 \\ a=3, b=5 \end{array}}$$

2
621
3622410
033622520461206
4043033622521512305446114230065
145054134043033622521512410501426340653424461131640263401006554
5164356065346153145054134043033622521512410501420461206560216402263 ...
2501164413255600065523144611052351643560653461531450541340430336225 ...
6215602131164424615362154556001010065545126351642446113120651263250 ...
3622410556003241535131164424020446110523362241053435455600102120212 ...
0336225204612065455600104362046105232501535131164424020450323054244 ...
4043033622521512305446114230065534354556001021205413362230544611206 ...



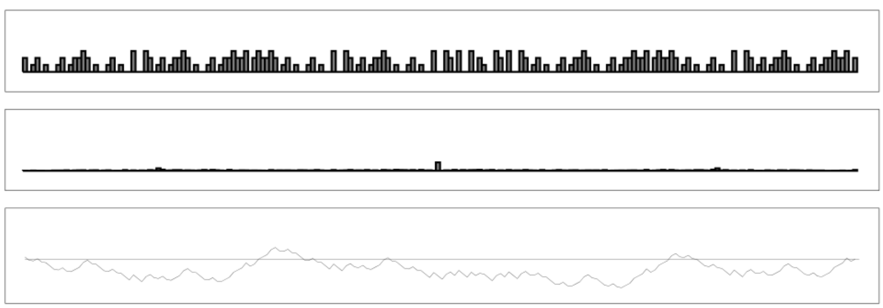


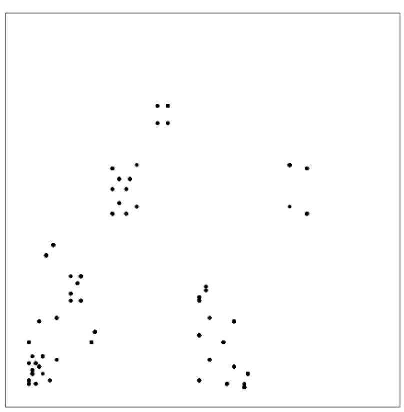
```
       runs: 0.1831
       freq: 0.0000
      cusum: 0.0000
     blocks: 0.3239
   autocorr: 0.8025
    longrun: 0.9692
      2bits: 0.0000
ks_discrete: 0.0000
        DTF: 0.0000
     Maurer: 0.9177
```

Example 5.4

$$\boxed{\begin{array}{r} f(x,y) = (x + 3y + 3) \mod 4 \\[1em] a = 3, b = 2 \end{array}}$$

```
0
201
0210212
201201001201223
0210212210210030212210212232230
201201001201223201001201003003201201223201001201223223023223201
0210212210210030212210212232230210210030212210210030032030030210212  ...
2012010012012232010012010030032012012232010012012232230232232012010  ...
0210212210210030212210212232230210210030212210210030032030030210212  ...
2012010012012232010012010030032012012232010012012232230232232012010  ...
0210212210210030212210212232230210210030212210210030032030030210212  ...
2012010012012232010012010030032012012232010012012232230232232012010  ...
```



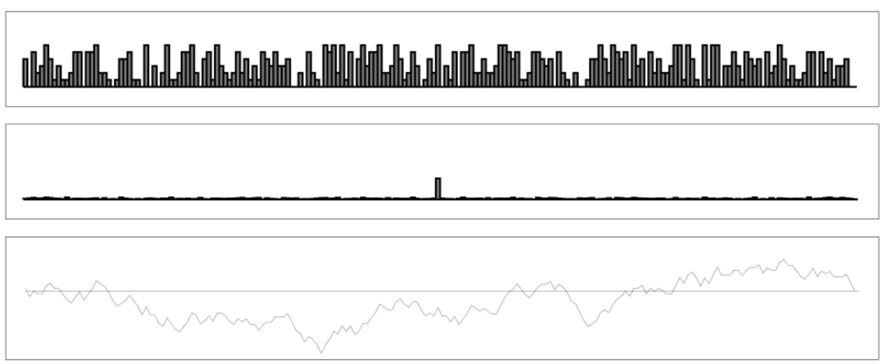


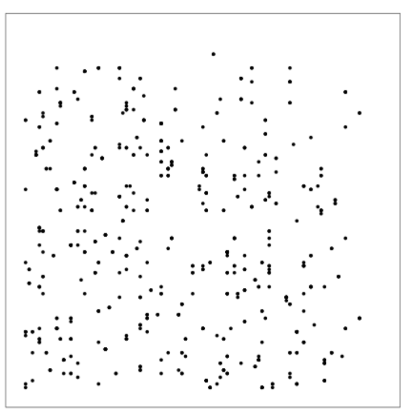
```
        runs: 0.0000
        freq: 0.0000
       cusum: 0.0000
      blocks: 0.0000
    autocorr: 0.0000
     longrun: 0.0000
       2bits: 0.0000
 ks_discrete: 0.0000
         DTF: 0.0000
      Maurer: 0.0217
```

Example 5.5

$$\boxed{\begin{array}{r} f(x,y) = (3x + 5y + 2) \mod 7 \\ a = 3, b = 4 \end{array}}$$

3
533
1543533
212524131543533
0261125562045163212524131543533
405236413112550556221014451106030261125562045163212524131543533
3400656223665451632131125505306505562242615001446445113150466033405 ...
5334002046355622422366163524451106030261632131125505306543404635306 ...
1543533400205210142603150556224204324223661641060315620464451131504 ...
2125241315435334002052106562615001443236603321253065055622420432101 ...
0261125562045163212524131543533400205210656261504635562236412530200 ...
4052364131125505562210144511060302611255620451632125241315435334002 ...





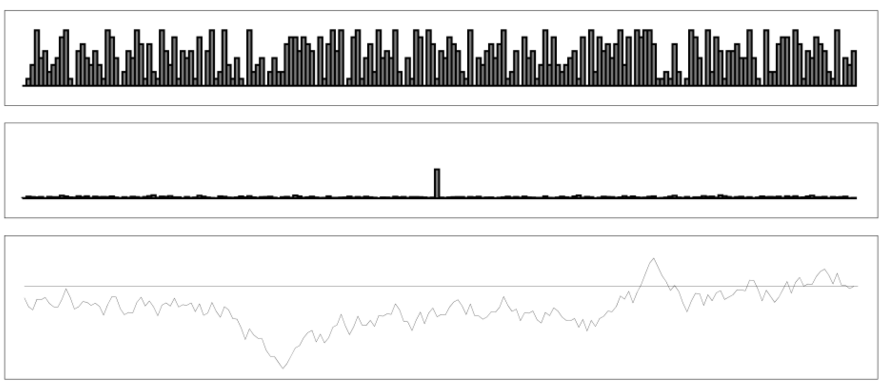
```
       runs: 0.8195
       freq: 0.0000
      cusum: 0.0000
     blocks: 0.1431
   autocorr: 0.2605
    longrun: 0.0000
      2bits: 0.0000
ks_discrete: 0.0000
        DTF: 0.0009
     Maurer: 0.9743
```

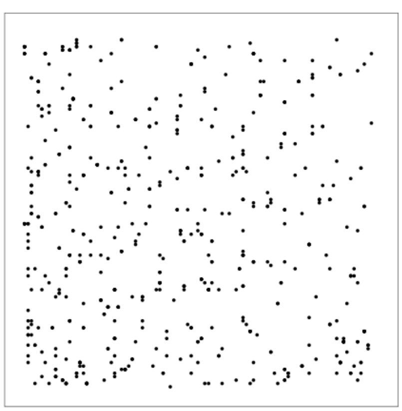
Example 5.6

$$f(x,y) = (7x + 4y) \mod 9$$

$$a = 2, b = 3$$

```
8
185
0138452
504113880435728
7580745121138878207443550732185
676548201724353162012113887837081250172484435515801773220138452
2677168564681250418732344355237146525041620121138878370853474058616 ...
4226775781462845564476286162758074513837732283148443551572834781547 ...
3402422677576507086154765218043515564484271652188611465267654820172 ...
8314108234024226775765071685801740588611056427168572013820744355310 ...
1853715451705812831410823402422677576507168580178146284548204187241 ...
0138452347810564353187402548616218537154517058128314108234024226775 ...
```





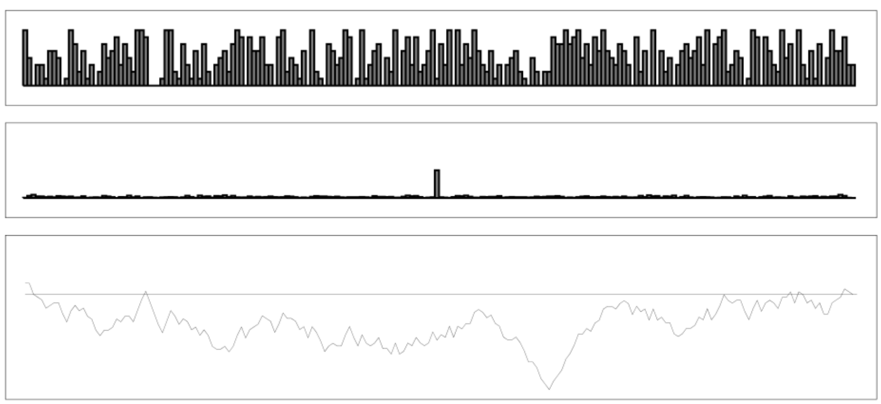
```
         runs: 0.6533
         freq: 0.0000
        cusum: 0.0000
       blocks: 0.9994
     autocorr: 0.4345
      longrun: 0.0183
        2bits: 0.0000
  ks_discrete: 0.0011
          DTF: 0.0093
       Maurer: 0.9867
```

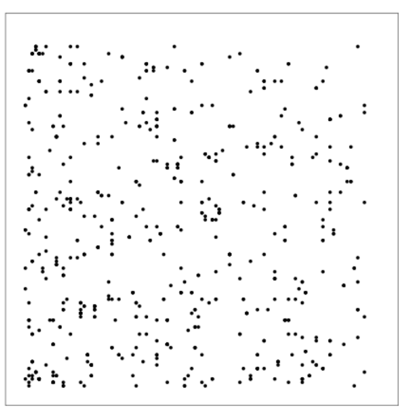
Example 5.7

$$f(x,y) = (7x + 4y + 5) \mod 9$$

$$a = 2, b = 5$$

```
3
431
8403315
685460832331556
7678052436201813724323315565164
276637587075328403561210018821630782840372432331556516458106048
0227668653072508870067257372685460831516612251305001883862510653806 ...
1042022766867846457380678235401838870050263782355733078276780524362 ...
5130345210420227668678463758543604855733487026375862431524600188134 ...
3581638083648532513034521042022766867846375854365307250805240356203 ...
4315082106534870181356042805737235816380836485325130345210420227668 ...
8403315540186251302645736428870001882163151620345268707557330782431 ...
```





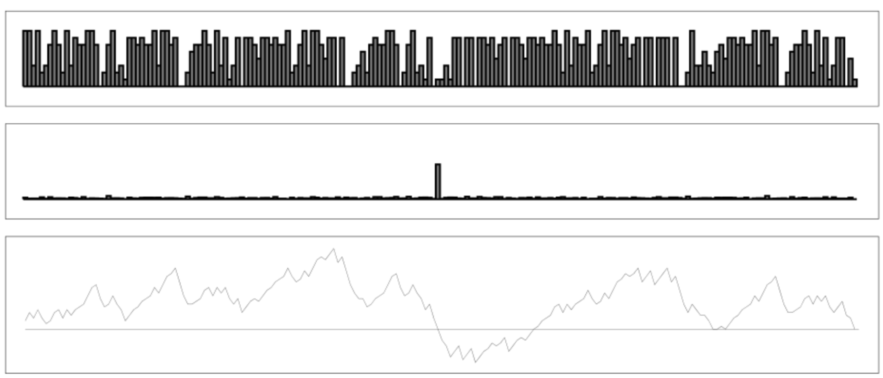
```
       runs: 0.2851
       freq: 0.0000
      cusum: 0.0000
     blocks: 0.0007
   autocorr: 0.3815
    longrun: 0.1354
      2bits: 0.0000
ks_discrete: 0.0000
        DTF: 0.0039
     Maurer: 0.9316
```

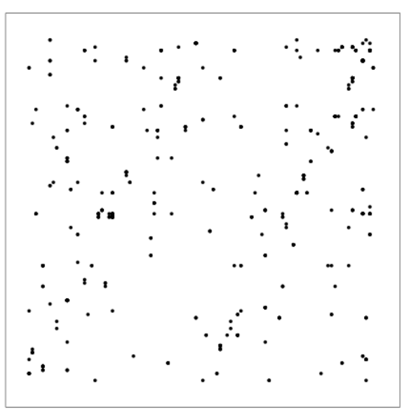
Example 5.8

$$f(x,y) = (x^3 + 2xy^2 + x^2y + 2y^3 + 5x^2 + 2xy + 7y^2 + 6x + 6y + 7) \mod 9$$

$$a = 1, b = 8$$

```
8
883
8838236
883823686283766
8838236862837668860268231776766
883823686283766886026823177676683886700256686283713707764776766
8838236862837668860268231776766838867002566862837137077647767668236 ...
8838236862837668860268231776766838867002566862837137077647767668236 ...
8838236862837668860268231776766838867002566862837137077647767668236 ...
8838236862837668860268231776766838867002566862837137077647767668236 ...
8838236862837668860268231776766838867002566862837137077647767668236 ...
8838236862837668860268231776766838867002566862837137077647767668236 ...
```





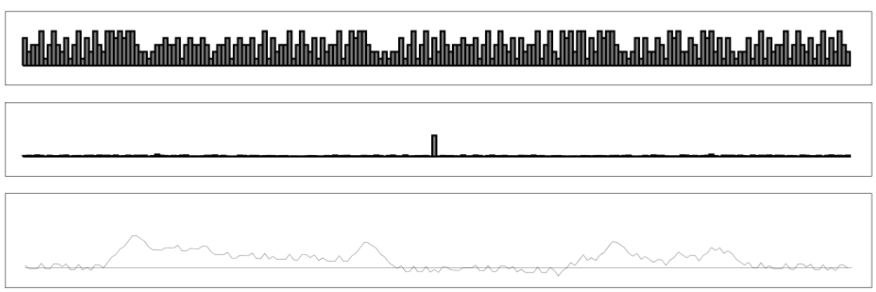
```
        runs: 0.7640
        freq: 0.0000
       cusum: 0.0000
      blocks: 0.0000
    autocorr: 0.9751
     longrun: 0.9922
       2bits: 0.0000
 ks_discrete: 0.0000
         DTF: 0.1106
      Maurer: 0.5568
```

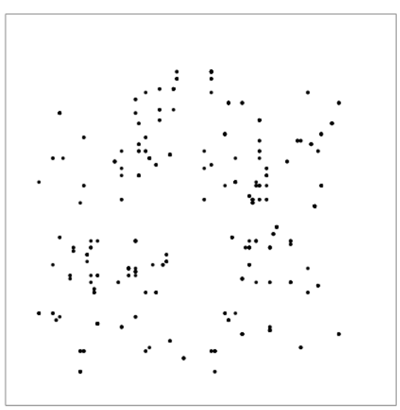
Example 5.9

$$f(x,y) = A^x_y, \quad \text{where } A = \begin{pmatrix} 1 & 4 & 2 & 5 & 3 \\ 4 & 1 & 3 & 2 & 5 \\ 5 & 2 & 4 & 3 & 1 \\ 3 & 5 & 1 & 4 & 2 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix}$$

$$a = 1, b = 4$$

```
5
351
2315215
423351353241351
5452334315212315532224312315215
351425323343341351353241423351354553221212241351423351353241351
2315215452555322334334134334312315212315532224315452334315212315142 ...
4233513532413514253255454553221233433413433431233413433413514233513 ...
5452334315212315532224312315215452555322554514251425455322124142334 ...
3514253233433413513532414233513545532212122413514233513532413514253 ...
2315215452555322334334134334312315212315532224315452334315212315142 ...
4233513532413514253255454553221233433413433431233413433413514233513 ...
```





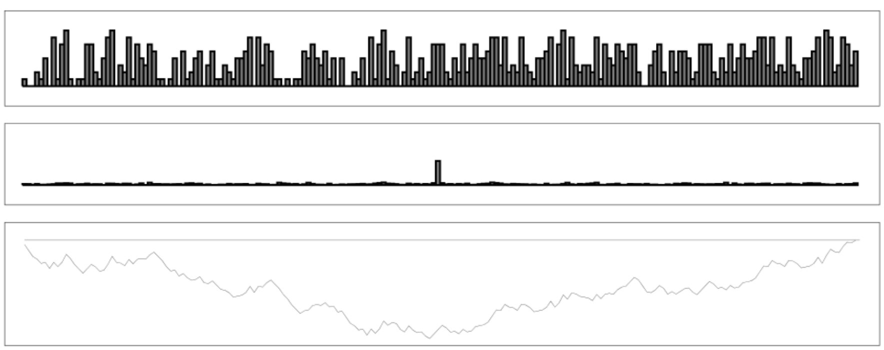
```
       runs: 0.0007
       freq: 0.0000
      cusum: 0.0000
     blocks: 0.0000
   autocorr: 0.5319
    longrun: 0.0183
      2bits: 0.0000
ks_discrete: 0.0000
        DTF: 0.2031
     Maurer: 0.7355
```

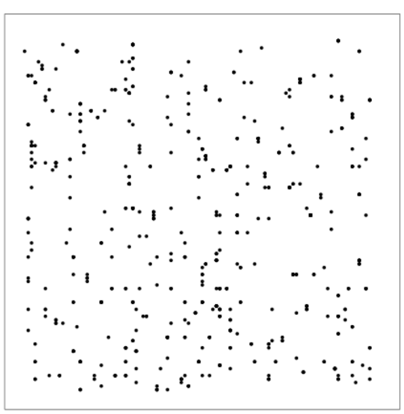
Example 5.10

$$f(x,y) = \begin{cases} (3x+4y+1) \mod 9 & \textbf{if } (x^2+y^3) \equiv 1 \mod 8 \\ (7x+7y+4) \mod 9 & \textbf{otherwise} \end{cases}$$

$$a = 3, b = 4$$

```
8
687
7638172
271643682167321
0247611624837638227116572302712
100214071681011662147803271643682252476101163577323310024761321
5140400271245087611638214051011676627124070860730247611624837638225 ...
6511245054504002476132144570681716810116436822712450351140510116571 ...
7635110132144570355445705450400214071681530271246445774016382167611 ...
2716436511014051530271246445774073652554644577403554457054504002712 ...
0247611624837635110140512450351115631002476132142624644577372450872 ...
1002140716810116621478032716436511014051245035113214457073651101011 ...
```





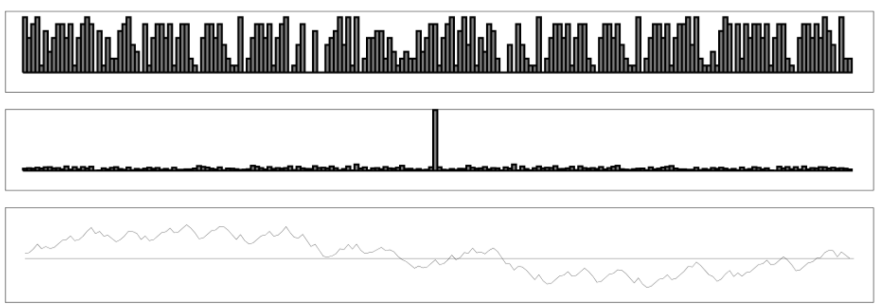
```
runs: 0.1227
freq: 0.0546
cusum: 0.0813
blocks: 0.9708
autocorr: 0.1418
longrun: 0.3680
2bits: 0.0145
ks_discrete: 0.0697
DTF: 0.4624
Maurer: 0.9151
```

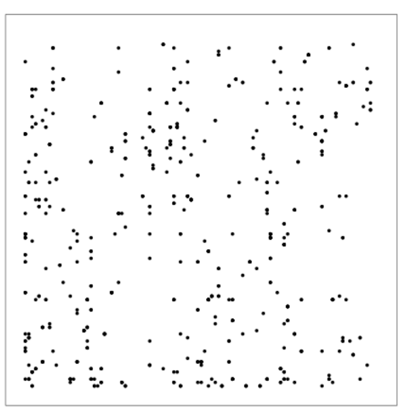
Example 5.11

$$\boxed{\begin{array}{r} f(x,y) = (\text{altsum}(31x + 35y + 47) \quad \text{mod } 9 \\ a = 18, b = 11 \end{array}}$$

where $\text{altsum}(n)$ is the alternating sum of decimal digits of n.

```
0
203
4210738
848211804763287
5864082211316870040716831248172
857816844088223211315381267817006004404721267843815274080147428
5865775801267864344088382232531211315381051328015226575801470060462 ...
8578163577571578706152265758168413343440883843282232531275138152113 ...
5865775801268375775715772105775817004641056232263577157801267864815 ...
8578163577571578706152267843071577571577210577574211802577571578014 ...
5865775801268375775715772105775817004641056232265758641360472105775 ...
8578163577571578706152267843071577571577210577574211802577571578014 ...
```





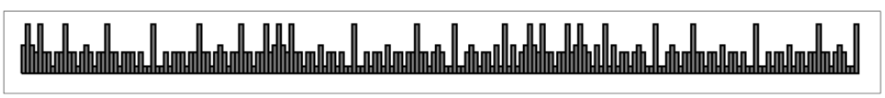
```
       runs: 0.0000
       freq: 0.0026
      cusum: 0.0051
     blocks: 0.0010
   autocorr: 0.0000
    longrun: 1.0000
      2bits: 0.0000
ks_discrete: 0.0000
        DTF: 0.3069
     Maurer: 0.8097
```

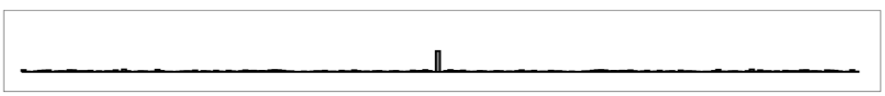
Example 5.12

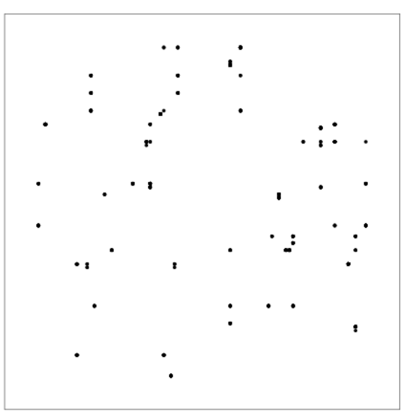
$$f(x,y) = \left(\left[\frac{x^2}{y} \right] + \left[\frac{y^2}{x} \right] \right) \mod 7 + 1$$

$$a = 3, b = 4$$

```
1
313
7331331
474373313373313
1417141347437331337347437331331
313431171134313314171413474373313373474314171413474373313373313
7331331413313117113133141331337331343117113431331417141347437331337 ...
4743733133733134313373313331311711313331337331343133733133734743733 ...
1417141347437331337347437331331413313373474373313373733133313117113 ...
3134311711343133141714134743733133734743141714134743733133733134313 ...
7331331413313117113133141331337331343117113431331417141347437331337 ...
4743733133733134313373313331311711313331337331343133733133734743733 ...
```





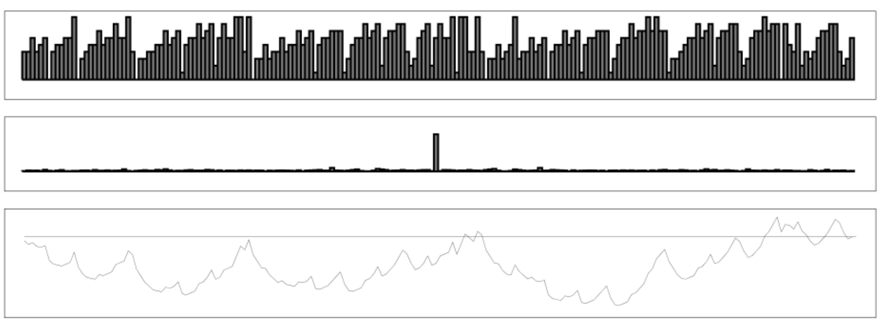


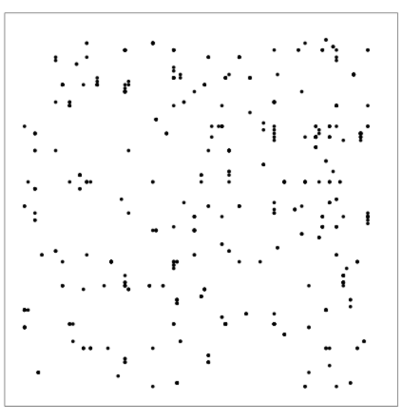
```
        runs: 0.0000
        freq: 0.0000
       cusum: 0.0000
      blocks: 0.0000
    autocorr: 0.0000
     longrun: 1.0000
       2bits: 0.0000
 ks_discrete: 0.0000
         DTF: 0.0000
      Maurer: 0.1154
```

Example 5.13

$$\boxed{f(x,y) = \left(\left[\frac{x^2}{y+1}\right] + 3\right) \mod 10 \qquad a = 3, b = 4}$$

```
4
446
4464560
446456045566903
4464560455669034557566866940334
446456045566903455756686694033445575671566867826866994903353446
4464560455669034557566866940334455756715668678268669949033534464557 ...
```



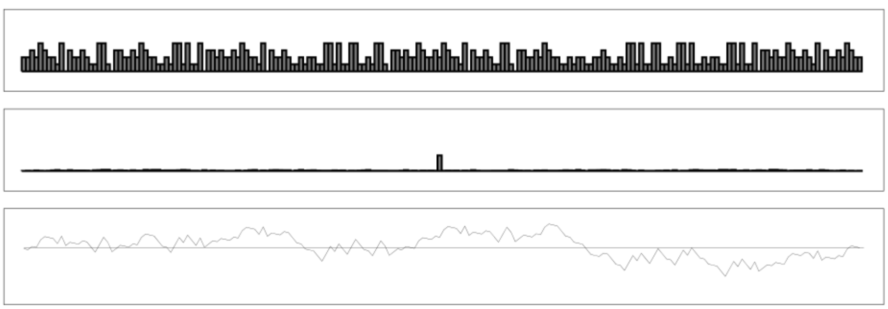


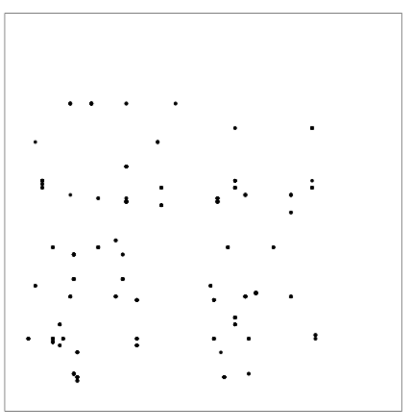
```
       runs: 0.0000
       freq: 0.0000
      cusum: 0.0000
     blocks: 0.0000
   autocorr: 0.0000
    longrun: 1.0000
      2bits: 0.0000
ks_discrete: 0.0000
        DTF: 0.0141
     Maurer: 0.5880
```

Example 5.14

$$f(x,y) = (\gcd(3x + 4y + 1, xy + y^2 + 4)) \mod 5$$
$$a = 3, b = 4$$

```
2
221
2232114
223243221121441
2232432214032232112122114414114
223243221403223211441033223243221121221122321121441411441121441
2232432214032232114410332232432211214414114033232232432214032232112 ...
2232432214032232114410332232432211214414114033232232432214032232112 ...
2232432214032232114410332232432211214414114033232232432214032232112 ...
2232432214032232114410332232432211214414114033232232432214032232112 ...
2232432214032232114410332232432211214414114033232232432214032232112 ...
2232432214032232114410332232432211214414114033232232432214032232112 ...
```



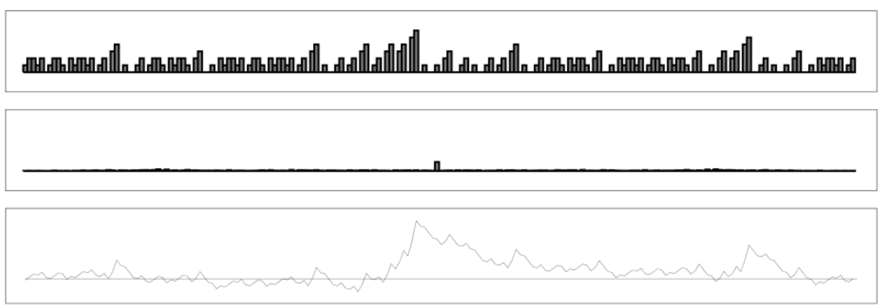


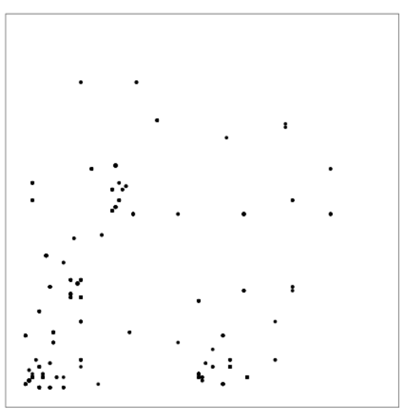
```
        runs: 0.0000
        freq: 0.0000
       cusum: 0.0000
      blocks: 0.9873
    autocorr: 0.0000
     longrun: 0.0000
       2bits: 0.0000
 ks_discrete: 0.0000
         DTF: 0.4845
      Maurer: 0.4318
```

Example 5.15

$$\boxed{\begin{array}{r} f(x,y) = |x - y + 1| \\ \\ a = 2, b = 7 \end{array}}$$

```
4
142
2124324
122102142322142
2102122120122124320322122124324
1221201221021221023001021221021423223023221221021221021423222142
2102122102300102122120122102122120120340100120122102122120122124320 ...
1221201221021221201203401001201221021221023001021221201221021221023 ...
2102122102300102122120122102122102300102302304500120100102300102122 ...
1221201221021221201203401001201221021221023001021221201221021221201 ...
2102122102300102122120122102122102300102302304500120100102300102122 ...
1221201221021221201203401001201221021221023001021221201221021221201 ...
```





```
       runs: 0.0000
       freq: 0.0000
      cusum: 0.0000
     blocks: 0.0000
   autocorr: 0.0000
    longrun: 0.0000
      2bits: 0.0000
ks_discrete: 0.0000
        DTF: 0.0000
     Maurer: 0.0217
```

References

[1] **L. Bassham a.o.:** *A statistical test suite for random and pseudorandom number generators for cryptographic applications*. NIST 2010.

[2] **R. Centrella:** *Numeri casuali - teoria e generatori dicotomici*. Tesi Univ. Roma 1997.

[3] **J. Coron/D. Naccache:** *An accurate evaluation of Maurer's universal test*. Springer LN CS 1556 (2002), 57-71.

[4] **A. Doğanaksoy/C. Tezcan:** *An alternative approach to Maurer's universal statistical test*. 3rd Inf. Sec. Crypt. Conference Ankara 2008.

[5] **M. Fisz:** *Wahrscheinlichkeitsrechnung und mathematische Statistik*. Deutscher Vlg. Wiss. 1989.

[6] **L. Guibas/A. Odlyzko:** *Long repetitive patterns in random sequences*. Zt. Wtheorie verw. Geb. 53 (1980), 241-262.

[7] **D. Knuth:** *The art of computer programming*. Volume 1. Addison-Wesley.

[8] **H. Kreindl:** *BUS-Theorie*. Internet ca. 2012.

[9] **L. Kuipers/H. Niederreiter:** *Uniform distribution of sequences*. Dover 2006.

[10] **U. Maurer:** *A universal statistical test for random bit generators*. J. Cryptology 5/2 (1992), 89-105.