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 (possibly 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

\[
(a \downarrow b)_{2j} = a_j \quad \text{for} \quad j = 1, \ldots, m
\]

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

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:

![Natural Binary Tree](image)

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

Remark 1.5 If \( g : \mathbb{N} + 1 \rightarrow X \) 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 \( \mathcal{L}(\ast, k) = \mathcal{L}(\text{id}, k) \), where \( \text{id} : \mathbb{N} + 1 \rightarrow \mathbb{N} + 1 \) is the identity function, and the NBT can be written as \( \mathcal{L}(\ast) \). More explicitly one has
1. Preliminaries

\[ \mathcal{L}(\ast, k) = (2^k, 2^k + 1, \ldots, 2^{k+1} - 1) \]
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 \(L(g, k, i)\). Hence

\[ L(g, k, i) := g(2^k + i - 1) \]

**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 \(#\text{binary}(n)\) - 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

\[ A(n) = \frac{2j + 1}{2^{k+1}} \]

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

**Definition 1.8** Let \(g : \mathbb{N} + 1 \rightarrow X\) 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 \(E(g, S) := (g(s_1), \ldots, g(s_m))\) 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 \(\mathbb{N}(k) := \{n \in \mathbb{N} + 1 \mid n < 2^{k+1}\}\) be the full initial triangle up to level \(k\) of the
NBT. Then we can form the series of sequences

\[ E(g, 0) := E(g, N(0)) = (g(1)) \]
\[ E(g, 1) := E(g, N(1)) = (g(2), g(1), g(3)) \]
\[ E(g, 2) := E(g, N(2)) = (g(4), g(2), g(5), g(1), g(6), g(3), g(7)) \]

\[ \ldots \]

which is called the binary evolution scheme of \( g \) and will be denoted by \( E(g) \).

We define \( E(g, -1) \) as the void sequence.

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

\[ E(g, k, i) = g(E(*, k, i)) \]

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

\[ E(g, k) = E(g, k - 1) \downarrow L(g, k) \]

From Definition 1.3 we have the recursion formulas

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

which in particular imply that

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

**Remark 1.10** The evolution scheme \( E(*) \) is interesting and well known:
1. Preliminaries

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

```
     1
  2       3
4  5  6  7
  8  9 10 11
12 13 14 15
16 17 18 19
```

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

Concatenating the vectors $E(\ast, k)$ to an infinite sequence $E(\ast, 0)E(\ast, 1) \cdots$, 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 $E(\ast, h)$ 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
```

**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 $\text{odd}(n) := u$ and call it the odd part of $n$. Furthermore $|n|_2 := 2^{-m}$ is the 2-adic absolute value of $n$.

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

1. If $n > 0$, then $\text{odd}(n)$ is odd.
2. $n$ is odd iff $\text{odd}(n) = n$.
3. $|n|_2 = 1$ iff $n$ is odd. In particular $|1|_2 = 1$.
4. $\text{odd}(n) = 1$ iff $n = 0$ or $n$ is a power of 2.
5. If $n > 0$, then $n \cdot |n|_2 = \text{odd}(n)$.

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

$$E(\ast, k, i) = 2^k |i|_2 + \frac{\text{odd}(i) - 1}{2}$$
1. Preliminaries

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

$$E(*, k, i) = E(*, k - m, \text{odd}(i)) = E(*, k - m, 2j + 1)$$

$$= 2^{k-m} + j = 2^{k-m} + \frac{\text{odd}(i) - 1}{2}$$

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

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

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

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

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

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

$$= 2^k |2^k + j|_2 + \frac{(2^k + j)|2^k + j|_2 - 1}{2}$$

$$= 2^k |j|_2 + \frac{(2^k + j)|j|_2 - 1}{2} = \frac{2^{k+1} + 2^k + j}{2} |j|_2 - \frac{1}{2}$$

(2) This is a special case of (1) or also of Remark 1.9. □

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

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

Proof. Immediate from Remark 1.9. □

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 $E(*)$ 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
1. Preliminaries

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

(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

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

\[ \square \]

Remark 1.17 (A very general method).

1. Let \((M, \prec)\) be totally ordered set and \( g : M \to X \) 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

\[ n \prec m \iff A(n) < A(m) \]

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 $\varepsilon$ 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 $N := \mathbb{N} \cup \{1/2\}$.

We extend now the function $A$ of Remark 1.7 to a function $\mathbb{N} \rightarrow [0, 1]$ 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 $L(\ast, -1) := (0, 1/2)$.

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

$$ E(g, k) := g(0)E(g, k)g(1/2) $$

and, as usual, $E(\ast, k) := E(id, k)$.

We shall not use the expressions $E(g, k, i)$, but define instead

$$ E(g, k, 0) := g(0) $$

$$ E(g, k, 2^k+1) := g(1/2) $$

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

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

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

$$ A : \mathbb{N} \rightarrow \overline{D} $$

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 $A(E(\ast, k, i)) = \frac{i}{2^{k+1}}$.

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

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

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

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

**Proof.** (1) Consider first the case \(0 < a < 2^k\). Then \(a \frac{2^k}{2^k} = A(\mathcal{E}(\ast, k-1, a))\), hence
\[
A^{-1} \left( \frac{a}{2k} \right) = \mathcal{E}(\ast, k-1, a) \frac{2^{k-1} |a|_2 + \frac{\text{odd}(a) - 1}{2}}{2}
\]

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

**Proposition 2.6** Let \(k \in \mathbb{N}\) and \(1 \leq i < 2^{k+1}\). If \(i\) is odd, then
\[
\mathcal{E}(\ast, k, i) \geq 2 \cdot \mathcal{E}(\ast, k, i-1) + 1
\]
\[
\mathcal{E}(\ast, k, i) \geq 2 \cdot \mathcal{E}(\ast, k, i+1)
\]

**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 \(e_j := \mathcal{E}(\ast, k, j)\) (for fixed \(k\)), from Theorem 1.13 now follow
\[
e_i = 2^k |i|_2 + \frac{\text{odd}(i) - 1}{2} = \frac{2^{k+1}}{2}
\]
\[
e_{i-1} = 2^k |i - 1|_2 + \frac{\text{odd}(i - 1) - 1}{2} \leq \frac{2^k + \frac{i-1}{2} - 1}{2}
\]
\[
= \frac{2^{k+1} + i - 1}{4} - \frac{1}{2} = \frac{e_i - 1}{2}
\]
\[
e_{i+1} = 2^k |i + 1|_2 + \frac{\text{odd}(i + 1) - 1}{2} \leq \frac{2^k + \frac{i+1}{2} - 1}{2}
\]
\[
= \frac{2^{k+1} + i - 1}{4} = \frac{e_i}{2}
\]
\(\square\)

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

\[
0 \ 8 \ 4 \ 9 \ 2 \ 10 \ 5 \ 11 \ 1 \ 12 \ 6 \ 13 \ 3 \ 14 \ 7 \ 15 \ 1/2
\]

The elements of \(\mathcal{L}(\ast, 3)\) are shown in boldface type. Similarly for every \(k \in \mathbb{N}\) each number \(n \in \mathcal{L}(\ast, k)\) has a left and a right neighbor in \(\mathcal{E}(\ast, k)\), which belong to levels \(< k\) and are called the **left support** \(Ls(n)\) and the **right support** \(Rs(n)\) of \(n\) respectively.
It is also clear (by the very construction of $A$ in Remark 1.7) that
\[
A(Ls(n)) = A(n) - \frac{1}{2^{k+1}}
\]
\[
A(Rs(n)) = A(n) + \frac{1}{2^{k+1}}
\]

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:

\[
\begin{align*}
Ls(2n) &= Ls(n) & \text{if } n > 0 \\
Ls(2n+1) &= n \\
Rs(2n) &= n & \text{if } n > 0 \\
Rs(2n+1) &= Rs(n) & \text{if } n > 0 \\
Rs(n) &= Ls(n+1) & \text{if } n+1 \text{ is not a power of 2}
\end{align*}
\]

(2) Moreover:

\[
\begin{align*}
Ls(2^k) &= 0 & \text{for } k \in \mathbb{N} \\
Rs(2^k-1) &= 1/2 & \text{for } k \in \mathbb{N} + 1
\end{align*}
\]

(3) In particular $Ls(1) = 0$ and $Rs(1) = 1/2$.

**Proof.** This is clear from the NBT.

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

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

\[
Ls(n) = Ls(2i + 1) = i = \frac{\text{odd}(n) - 1}{2}
\]

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

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

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

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

\[
Ls(n) \leq \frac{\text{odd}(n)-1}{2} \leq \frac{n-1}{4} = \frac{n-1}{2}
\]

thus

\[
\frac{n}{4} \geq Ls(n) + \frac{1}{2} > Ls(n)
\]

(2) From Remark 2.8 we know that $Ls(n) = \frac{n-1}{2}$.

Suppose first that $n + 1$ is not a power of 2. Then

\[
Rs(n) = Ls(n+1) = \frac{\text{odd}(n+1)-1}{2} \leq \frac{n+1-1}{4} = \frac{n-1}{4}
\]
2. Generalized Stern-Brocot trees

hence
\[ \frac{n}{4} \geq \text{Rs}(n) + \frac{1}{4} > \text{Rs}(n) \]

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

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

\[
\begin{align*}
g(0) &:= a \\
g(1/2) &:= b \\
g(n) &:= f(g(\text{Ls}(n)), g(\text{Rs}(n))) \quad \text{for } n \in \mathbb{N} + 1
\end{align*}
\]

Since for \( n \in \mathbb{N} + 1 \) the levels of \( \text{Ls}(n) \) and \( \text{Rs}(n) \) 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 \( g : \mathbb{N} \rightarrow X \) be a function and \( k \in \mathbb{N} \). Then

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

*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 \( \text{Ls}(n) \) and \( \text{Rs}(n) \) are the left and right neighbors of \( n \) in \( \mathcal{E}(*, k) \) and thus are neighbors of each other in \( \mathcal{E}(*, k - 1) \).

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

If follows that, if now \( f : X \times X \rightarrow X \), \( a, b \in X \) and \( g := f_{ab} \), then \( g(n) \) is the value of \( f \) evaluated on the left and right neighbors of \( g(n) \) in \( \mathcal{E}(g, k) \) (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 \( \mathcal{E}(f_{ab}, k) \) is obtained from \( x := \mathcal{E}(f_{ab}, k - 1) \) 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 \( f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \) 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 \(n \in \mathbb{N}\).

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

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

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

\(k - 1 \rightarrow k\): If \(n\) is even, then \(Rs(n) = \frac{n}{2} > Ls(n)\), hence

\[g(n) = f(g(Ls(n)), g(n/2)) \stackrel{\text{IND}}{=} f(Ls(n), n/2) = 2 \frac{n}{2} = n\]

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

\[g(n) = f(g((n-1)/2), g(Rs(n))) \stackrel{\text{IND}}{=} f((n-1)/2, Rs(n)) = n\] \(\square\)

**Definition 2.15** Let \(f : X \times X \rightarrow X\) be a mapping, and \(a, b \in X\). Then we may construct a mapping \(f_{ab} : \mathbb{N} \rightarrow X\) 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 \(f : X \times X \rightarrow X\) be mapping and \(a, b \in X\). For \(k \in \mathbb{N}\) then the sequence \(E(f_{ab}, k) = (x_1, \ldots, x_{2^{k+1} - 1})\) 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 which we describe in Pari/GP and which justifies the name **dichotomic generator**:

```pari
\} \text{Example:}
f(x,y) = (3x+5*y+2)%7
p=2^101; q=2^94
v=[dicho(f,n,0,p,0,1) | n<-[q..q+40]]
to_q(v,60,"")
```

Notice that we may use this algorithm for calculating far away elements of the sequence \(E(f_{ab}, k)\), 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.
2. Generalized Stern-Brocot trees

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

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

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 \( g : \mathbb{N} + 1 \rightarrow X \) be a mapping.

We shall then consider the sequences \( E(g, k) \) 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 \( E(g, k) \) for different \( k \) can be rather unrelated. For theoretical investigations, however, also the case that \( E(g, k + 1) \) is always a continuation of \( E(g, k) \), i.e., that \( E(g, k) \) is always a prefix of \( E(g, k + 1) \), 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 \( g : \mathbb{N} + 1 \rightarrow X \) be a mapping. We define an infinite sequence \( E(g, \infty) : \mathbb{N} + 1 \rightarrow X \) by setting

\[
E(g, \infty, n) := E(g, k, n)
\]

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

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

The bold numbers themselves represent the sequence \( E(\ast, \infty) \).

The sequence \( E(g, \infty) \), always defined, is of course interesting only if \( E(g, k + 1) \) is a continuaton of \( E(g, k) \) for every \( k \in \mathbb{N} \).

In this case the mapping \( g \) is called continuutive.

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 \( 2j + 1 \in L(\ast, k) \) iff \( j \in L(\ast, k - 1) \), the recursion formulas of Remark 1.9 become now

\[
\begin{align*}
E(g, \infty, 1) &= g(1) \\
E(g, \infty, 2j) &= E(g, \infty, j) & \text{for } j \in \mathbb{N} + 1 \\
E(g, \infty, 2j + 1) &= g(2^k + j) & \text{for } k \in \mathbb{N} \text{ and } 2^{k-1} \leq j < 2^k
\end{align*}
\]

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

1. \( g \) is continuative.
2. \( g \) is constant on each column of \( E(\ast) \).
3. \( g \) is constant on each column of \( L(\ast) \).
4. \( E(g, \infty, 2j + 1) = g(2^k + j) \) for every \( k, j \in \mathbb{N} \) with \( j < 2^k \).
3. Continuative Mappings

(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 \(E(\ast)\) were represented in Remark 1.10, those of \(L(\ast)\) in Remark 1.16.

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

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

(2) \(\iff\) (3): We observed in Remark 1.16 that \(L(\ast)\) and \(E(\ast)\) have the same columns - which in \(L(\ast)\) appear only once, in \(E(\ast)\) infinitely often.

(5) \(\iff\) (6): Clear. \(\Box\)

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

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

where the dot denotes concatenation of words.

Proof. Clear. \(\Box\)

Lemma 3.6 Let \(f : X \times X \to X\) 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 \(E(f_{ab}, k) = E(f_{ac}, k)\) for every \(a \in X\) and every \(k \in \mathbb{N}\).

\(k = 0:\) Applying the hypothesis to \(x = a\) we have \(f(a,b) = f(a,c)\), hence

\[ E(f_{ab}, 0) = (f(a,b)) = (f(a,c)) = E(f_{ac}, 0) \]

\(k \to k + 1:\) One has

\[
E(f_{ab}, k + 1) \overset{3 \& 5}{=} E(f_{a, f(a,b)}, k) \cdot f(a,b) \cdot E(f_{f(a,b),b}, k)
= E(f_{a, f(a,c)}, k) \cdot f(a,c) \cdot E(f_{f(a,c),b}, k)
\overset{IND}{=} E(f_{a, f(a,c)}, k) \cdot f(a,c) \cdot E(f_{f(a,c),c}, k) = E(f_{ac}, k + 1)
\]
where we used again that \( f(a, b) = f(ac) \), applying in \( \text{IN} \) the induction hypothesis on \( f(a, c) \) instead of \( a \).

**Proposition 3.7** Let \( f : X \times X \to X \) 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
\[
E(f_{ab}, k + 1) \leq E(f_{a, f(a,b)}, k) \cdot f(a, b) \cdot E(f_{f(a,b), b}, k)
\]

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 \( E(f_{ab}, k) = E(f_{a, f(a,b)}, k) \) is a prefix of \( E(f_{ab}, k + 1) \).

**Corollary 3.8** Let \( f : X \times X \to X \) be a mapping and \( a, b \in X \).

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

**Remark 3.9** Let \( g : \mathbb{N} \to X \) be a mapping and set \( a := g(0), b := g(1/2) \).

Consider the sequences \( E(g, k) \):

\[
\begin{array}{cccccccc}
\text{a} & g(1) & b \\
\text{a} & g(2) & g(1) & g(3) & b \\
\text{a} & g(4) & g(2) & g(5) & g(1) & g(3) & g(7) & b \\
\ldots
\end{array}
\]

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

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

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

**Proof.** (1) \( \iff \) (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 $\phi: X \to X$ 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 $\phi: X \to X$ be a mapping and $a \in X$. We define a mapping $g: \mathbb{N} \to X$ in the following way:

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

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

On its domain of definition $\phi_a$ 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 $(\phi, a)$ or, for short, the mapping $\phi_a$ itself, a one-sided generator.

Proposition 4.6 Let $\phi: X \to X$ 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

\[
\phi_a(2j) = \phi(\phi_a(Ls(2j))) \overset{2 \&}{=} \phi(\phi_a(Ls(j))) = \phi_a(j).
\]

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

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

\[
aE(\phi_a, \infty) = \phi_a
\]

or, equivalently,

\[
E(\phi_a, \infty, n) = \phi_a(n)
\]

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

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

(1) We show that $u$ satisfies the same recursion rules as $\phi_a$, i.e., that
4. One-sided generators

\[ u_1 = \phi(a) \]
\[ u_{2j} = u_j \]
\[ u_{2j+1} = \phi(u_j) \]

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

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

\[ u_1 = \phi_a(1) = \phi(a) \]
\[ u_j = \phi(u_j) \text{ for } j \in \mathbb{N} + 1 \]
\[ u_{2j+1} = \phi_a(2^k + j) \text{ for every } k, j \in \mathbb{N} \text{ with } j < 2^k \]

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

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

\[ k-1 \rightarrow k: \text{ Assume } 0 \leq j < 2^k. \]

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

\[ u_{2^k+1} = \phi(\phi_a(Ls(2^k + j))) \]
\[ = \phi\left( \phi\left( 2^k + j - \frac{1}{2} \right) \right) = \phi(u_j) \]

since \( 0 \leq j - \frac{1}{2} < 2^{k-1} \).

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.

\[ u_{2^k+1} = \phi_a(2^k + j) = \phi_a(2^m (2^{k-m} + r)) = \phi(u_j) \]

\[ \square \]

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:

\[ g=f_{\{1,6\}} : 6 6 5 6 5 3 2 6 5 3 2 7 2 2 1 6 5 3 2 7 2 2 1 7 2 4 7 2 \ldots \]
\[ E(g,\text{infinite}) : 6 6 5 6 3 5 2 6 7 3 2 5 2 2 1 6 7 7 2 3 4 2 7 5 2 2 1 2 \ldots \]

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 \( \phi : X \rightarrow X \) the following statements are equivalent:

(1) \( u = \phi_a \).

(2) \( u = aE(\phi_a, \infty) \).

(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.
4. One-sided generators

**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 \( \beta := \biguplus_{n} n + 1 : \mathbb{N} \to \mathbb{N} \) and define \( h := \beta_0 : \mathbb{N} \to \mathbb{N} \) in accordance with Definition 4.5 by
\[
h(0) := 0
\]
\[
h(n) := h(Ls(n)) + 1 \quad \text{for } n \in \mathbb{N} + 1
\]
Then by Theorem 4.7
\[
h = 0^\mathcal{E}(h, \infty) = 01121223122323341223233423 \ldots
\]
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 \( \phi : X \to X \) 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 \( n \).
\[
\begin{align*}
n &= 0: & \phi_0(a) &= \phi^{h(0)}(a) = a = \phi_a(0) \smallskip
\hline
n - 1 \to n: & \text{Now } n > 0 \text{ and we may write } n = 2^m r \text{ with } r \text{ odd.}
\end{align*}
\]
By Proposition 2.9 \( Ls(n) = \frac{r - 1}{2} \), hence \( h(n) = h\left( \frac{r - 1}{2} \right) + 1 \). Further
\[
\phi_a(n) = \phi_a(2^m r) = \phi^4 \phi_a(r) = \phi \left( \phi_a \left( \frac{r - 1}{2} \right) \right)
\]
\[
\overset{IND}{=} \phi \left( \phi^{h\left( \frac{r - 1}{2} \right)}(a) \right) = \phi^{h\left( \frac{r - 1}{2} \right) + 1}(a) = \phi^{h(n)}(a) \quad \Box
\]
5. Examples

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

For every generator are first indicated the function \( f : X \times X \rightarrow X \) (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 \( \mu \) 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

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

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:

\begin{itemize}
  \item \texttt{runs .................. run test} (cf. Bassham a.o. [1], Maurer [10] and Fisz [5])
  \item \texttt{freq .................. frequency test} (cf. Bassham a.o. [1])
  \item \texttt{cusum ................. cumulative sum test} (cf. Bassham a.o. [1])
  \item \texttt{blocks ............. blocks test} (cf. Fisz [5])
  \item \texttt{autocorr .......... auto-correlation test} (cf. Bassham a.o. [1])
  \item \texttt{longrun ............ longrun test} (cf. Guibas & Odlyzko [6] p. 252-253])
  \item \texttt{2bits ................ 2-bit test} (cf. Fisz [5] page 399] and Bassham a.o. [1])
  \item \texttt{ks_discrete ...... discrete Kolmogorov-Smirnov test} (cf. Kuipers & Niederreiter [9] p. 90-92] and Fisz [5])
\end{itemize}
5. Examples

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

\[ f(x, y) = (x + y + 1) \mod 7 \]

\[ a = 3, b = 5 \]
Example 5.4

\[ f(x, y) = (x + 3y + 3) \mod 4 \]

\[ a = 3, b = 2 \]
5. Examples

Example 5.5

\[ f(x, y) = (3x + 5y + 2) \mod 7 \]

\[ a = 3, \ b = 4 \]
5. Examples

Example 5.6

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

\[ a = 2, b = 3 \]

8
185
0138452
504113880435728
7580745121138878207443550732185
676548201724353162012113887837081250172484435515801773220138452
2677168564681250418732344355237146525041620121138878370853474058616 \ldots
422677578146284556447628616275807451383773228314844355157823834781547 \ldots
3402422677576507086154765218043515564484271652188611465267654820172 \ldots
831410823042226775765071685801740588611056427168572013820744355310 \ldots
1853715451705812831410823402422677576507168580178146284548204187241 \ldots
0138452347810564353187402548616218537154517058128314108234024226775 \ldots
5. Examples

Example 5.7

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

\[ a = 2, b = 5 \]
Example 5.8

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

\[ a = 1, b = 8 \]
5. Examples

Example 5.9

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

\[ a = 1, \quad b = 4 \]
5. Examples

Example 5.10

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

\[ a = 3, \ b = 4 \]

8
687
7638172
271643682167321
0247611624837638227116572302712
100214071681011662147803271643682252476101163577323310024761321
514040027124508761163821405101167627124070860730247611624837638226 \ldots
6511245054002476132144570681716810116436822712450351140510116571 \ldots
7635110132144570355445705450400214071681530271246445774016382167611 \ldots
2716436511014051530271246445774073652554644577403554457054504002712 \ldots
024761162483763511101405124503511115631002476132142624644577372450872 \ldots
1002140716810116621478032716436511014051245035113214457073651101011 \ldots

runs: 0.1227
freq: 0.0546
casum: 0.0813
blocks: 0.9708
autocorr: 0.1418
longrun: 0.3880
2bits: 0.0145
ks_discrete: 0.0697
DTF: 0.4624
Maurer: 0.9151

29
5. Examples

Example 5.11

\[ f(x, y) = (\text{altsum}(31x + 35y + 47)) \mod 9 \]

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

\[ a = 18, b = 11 \]

\[ 0, 203, 4210738, 848211804763287, 5864082211316870040716831248172, 857816357757157870615226784307157757157721057757157801267864815 \]

\[ \ldots, 8578163577571578706152267843071577571577210577574211802577571578014 \]

\[ 8565775801268375775715772105775817004641056632263577157801267864815 \]

\[ \ldots, 8578163577571578706152267843071577571577210577574211802577571578014 \]

| runs: | 0.0000 |
|-------|--------|
| freq: | 0.0028 |
| csum: | 0.0061 |
| blocks: | 0.0010 |
| autocorr: | 0.0000 |
| longrun: | 1.0000 |
| 2bits: | 0.0000 |
| ks_discrete: | 0.0000 |
| DTV: | 0.3069 |
| Maurer: | 0.8097 |
Example 5.12

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

\[ a = 3, \ b = 4 \]

1
313
7331331
474373313373313
141714134743733133734743733133
31343117113431331417141347437331337347431471413474373313373313
7331331413311711313314133133733134311711343131417141347437331337...
474373313373314313373313311711331337331343133733134313373313473313...
1417141347437331337347437331334171413474373313373474373313373313...
3134311711343133141714134743733133734743733141714134743733133733...
73313314133117113133141331337331343117113431331417141347437331337...
474373313373314313373313331331171134313331337331343133733133734743733...

...
Example 5.13

\[ f(x, y) = \left( \left\lfloor \frac{x^2}{y+1} \right\rfloor + 3 \right) \mod 10 \]

\[ a = 3, \ b = 4 \]
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
22324322140322321144103232232432211212211441411441121441
2232432214032232114410323223243221121441411403232232432214032232112 \ldots
2232432214032232114410323223243221121441411403232232432214032232112 \ldots
2232432214032232114410323223243221121441411403232232432214032232112 \ldots
2232432214032232114410323223243221121441411403232232432214032232112 \ldots
2232432214032232114410323223243221121441411403232232432214032232112 \ldots

\begin{figure}
\centering
\includegraphics[width=\textwidth]{chart.png}
\caption{Graphical representation of the sequence.}
\end{figure}
Example 5.15

\[ f(x, y) = |x - y + 1| \]

\[ a = 2, b = 7 \]
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.