REVISTA DE LA UNIÓN MATEMÁTICA ARGENTINA
Vol. 67, No. 1, 2024, Pages 229–244
Published online: May 15, 2024
https://doi.org/10.33044/revuma.3076

# MODULAR AUTOMATA

THOMAS N. HIBBARD†, CAMILO A. JADUR, AND JORGE F. YAZLLE

Abstract. Let $M$ and $b$ be integers greater than 1, and let $\mathbf{p}$ be a positive probability vector for the alphabet $\mathcal{A}_b = \{0, \dots, b-1\}$. Let us consider a random sequence $w_0, w_1, \dots, w_j$ over $\mathcal{A}_b$, where the $w_i$'s are independent and identically distributed according to $\mathbf{p}$. Such a sequence represents, in base $b$, the number $n = \sum_{i=0}^{j} w_i b^{j-i}$. In this paper, we explore the asymptotic distribution of $n$ mod $M$, the remainder of $n$ divided by $M$. In particular, by using the theory of Markov chains, we show that if $M$ and $b$ are coprime, then $n$ mod $M$ exhibits an asymptotic discrete uniform distribution, independent of $\mathbf{p}$; on the other hand, when $M$ and $b$ are not coprime, $n$ mod $M$ does not necessarily have a uniform distribution, and we obtain an explicit expression for this limiting distribution.

## 1. Introduction

In this work we deal with non-negative integer numbers (represented in some fixed integer base $b > 1$) whose digits are randomly generated step by step; we are interested in the distribution of such numbers modulo a given integer $M > 1$. More precisely, the set $\{0, \dots, b-1\}$ of all digits for such representations is endowed with a strictly positive probability vector $\mathbf{p}$. Suppose that, according to $\mathbf{p}$, we produce a random sequence of independent and identically distributed digits $w_0, w_1, \dots, w_j$. Such a sequence represents, in base $b$, the number $n = \sum_{i=0}^{j} w_i b^{j-i}$. In this context, and especially for $j$ larger and larger, the distribution of the remainder of $n$ divided by $M$ is of natural interest: Given $r \in \{0, \dots, M-1\}$, what is the probability that $n$ mod $M$ is precisely $r$? At first glance, one could be tempted to think that, in all cases, this probability depends on $r$ and also on $\mathbf{p}$, since endowing a particular digit with a high probability could favor some of the possible residues.

For $b = 2$, simulation trials show that a long sequence of 0's and 1's in which 0 occurs with probability $p \in (0, 1)$ (that is, $\mathbf{p} = (p, 1-p)$) seems to have a steady state probability $1/M$ of being the binary representation of a multiple of a given odd number $M$, independently of $p$. Tables 1 and 2 below show outcomes of such simulations for $M = 9$ and $M = 11$, respectively (bar charts are given in Figure 1);

2020 *Mathematics Subject Classification.* 37H05, 60J10.
*Key words and phrases.* Random $b$-ary expressions, stochastic automata, Markov chains.
Work supported with funds from projects #2380 and #2728 – C.I.U.N.Sa.
†Deceased, 2016.

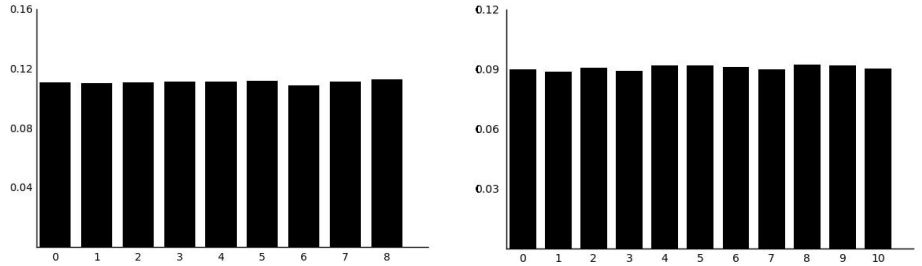
in each case, three different schemes for **p** were chosen, and, for each one, 50,000 trials with 100-bit random numbers were executed; we registered the frequency of having residue 0 and, additionally, the frequency of all the other possible residues for each case.

| **p** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| (0.3,0.7) | 0.111 | 0.110 | 0.113 | 0.111 | 0.109 | 0.110 | 0.111 | 0.112 | 0.113 |
| (0.1,0.9) | 0.113 | 0.110 | 0.113 | 0.111 | 0.111 | 0.108 | 0.111 | 0.112 | 0.111 |
| (0.95,0.05) | 0.113 | 0.114 | 0.110 | 0.110 | 0.110 | 0.111 | 0.107 | 0.114 | 0.111 |

TABLE 1. $b = 2$, $M = 9$.

| **p** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| (0.3,0.7) | 0.091 | 0.091 | 0.090 | 0.090 | 0.091 | 0.091 | 0.092 | 0.092 | 0.088 | 0.092 | 0.092 |
| (0.1,0.9) | 0.091 | 0.093 | 0.089 | 0.090 | 0.092 | 0.091 | 0.090 | 0.091 | 0.092 | 0.091 | 0.090 |
| (0.95,0.05) | 0.094 | 0.089 | 0.091 | 0.091 | 0.092 | 0.089 | 0.092 | 0.091 | 0.090 | 0.090 | 0.091 |

TABLE 2. $b = 2$, $M = 11$.



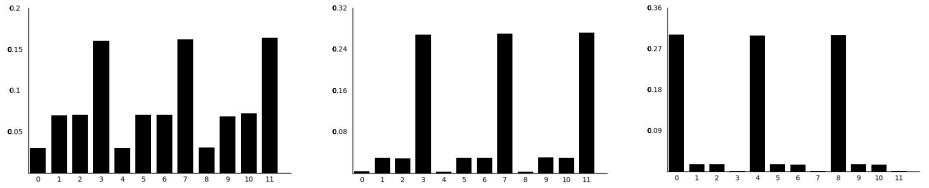

$M = 9$ $M = 11$

FIGURE 1. $b = 2$.

In fact, the same trials show that not only 0, but all the possible residues modulo $M$ of the numbers represented by such sequences, seem to have the same probability $1/M$, not depending on $p$.

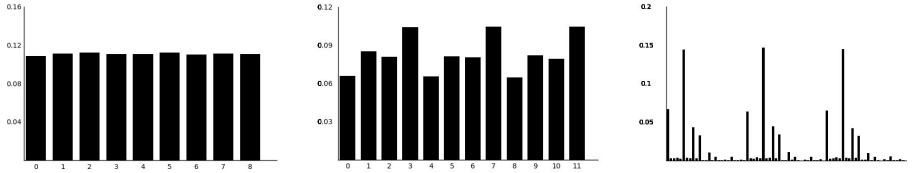
Still in the binary case $b = 2$, but now taking $M$ even, simulation shows that, in general, the residues have no longer all the same probability $1/M$. Moreover, for fixed $M$, **p** has a strong influence on the results. Figure 2 shows some outcomes for the case $M = 12$.

When $b > 2$, and depending on whether $M$ is (or is not) coprime with $b$, trials reveal similar situations. For instance, taking $b = 10$, Figure 3 shows outcomes for $M = 9$, $M = 12$ and $M = 75$.



$\mathbf{p} = (0.3, 0.7)$ $\mathbf{p} = (0.1, 0.9)$ $\mathbf{p} = (0.95, 0.05)$

FIGURE 2. $b = 2$, $M = 12$.



(a) $M = 9$ (b) $M = 12$ (c) $M = 75$

FIGURE 3. $b = 10$, $\mathbf{p} = (0.24, 0.01, 0.01, 0.01, 0.01, 0.52, 0.01, 0.01, 0.17, 0.01)$.

Calling $X_k = \sum_{i=0}^{k} w_i b^{k-i} \bmod M$, the problem can be seen as that of the evolution of the random variable $X_k$ recursively generated under the stochastic recurrence $X_k = (bX_{k-1} + w_k) \bmod M$, where $w_k$ is the randomly generated $k$th digit. Our simulations suggest that coprimality between $b$ and $M$ plays a central role in the asymptotic distribution for $X_k$.

We mention that, as an antecedent, deterministic recursive formulas of the form $X_k = (aX_{k-1} + c) \bmod m$, for $a, c, m$ fixed positive integers, have been studied as pseudo-random number generators (see, for instance, [7]). Of course, the choice of values for the parameters affects how good the generator is. Usually, $m$ has many repeated prime factors and is coprime with $c$; in addition, $a - 1$ is divisible by any prime factor of $m$, and if $m$ is a multiple of 4, so is $a - 1$. In such cases, $X_k$ has the uniform limiting distribution. In order to produce pseudo-random numbers, programming languages use such deterministic recursions, each with its own set of parameters (for instance, Borland C++ takes $a = 22695477$, $c = 1$, $m = 2^{32}$).

In the case we propose to study here, randomness is added, since the independent coefficient in the recursion varies in some random way, and our aim is to describe how this randomness influences the asymptotic distribution for $X_k$ in our stochastic recursion. To do so, we consider a special class of stochastic automata which we call *modular automata*, whose definition and basic properties are given in Section 3. Then, applying to modular automata the theory of Markov chains—thus giving a dynamical flavor to our problem—in Section 4 we will show that $X_k$ has uniform asymptotic distribution (that is, all the possible remainders have the same steady state probability $1/M$) whenever $M$ is coprime with $b$, regardless of the probability

vector $\mathbf{p}$. Based on this result, in Section 5 we obtain an explicit expression for the asymptotic distribution of $X_k$ (in terms of $M$, $b$ and $\mathbf{p}$) for arbitrary positive integer values of $M$ and $b$. We start by presenting, in Section 2, the necessary formal definitions, also recalling some well-known facts which will be useful in what follows.

*Note from authors Jadur and Yazlle.* Dr. Thomas Hibbard passed away in 2016. We wish to justify his inclusion as an author of this paper. In 2011, Dr. Hibbard commented on his observations (obtained by simulation) about an unexpected regularity of the residues (modulo an odd number) of randomly generated binary sequences. We worked with Dr. Hibbard on this counter-intuitive problem, obtaining significant advances for such binary sequences and odd moduli, and sharing preliminary results in some scientific meetings. By 2014, he devised a strategy to also handle the case of even moduli, which by the end of 2015 allowed us to obtain a formula for the stationary distribution of residues modulo any positive integer, in the case of binary sequences. This was the state of our joint research when unfortunately Dr. Hibbard passed away. In 2019, we started working again on the problem, and submitted the paper in 2022. It is clear to us that Dr. Hibbard merits being an author of the present work.

## 2. Formal definitions

We begin with a couple of classical results in number theory. The reader is referred to [5] for proofs and a thorough presentation.

By a *natural number* we mean a non-negative integer. When $n$ and $M$ are integers with $M > 0$, by $n$ mod $M$ we mean the remainder of $n$ divided by $M$. We will use $\equiv_M$ to denote the classical equivalence relation congruence modulo $M$ between integers, and $\mathbb{Z}_M$ for $\mathbb{Z}/\langle M\rangle$, identifying $[r]$ with $r$ for $0 \leq r < M$. Thus, we consider $\mathbb{Z}_M = \{0, \ldots, M-1\}$, endowed with the operations of addition and multiplication modulo $M$.

**Proposition 2.1.** *For $p$ and $q$ coprime numbers, $n \equiv_{pq} r$ if and only if $n \equiv_p r$ and $n \equiv_q r$.*

For $M$ prime, $\mathbb{Z}_M$ is a field, thus providing unique solutions for equations $b \times x = c$ when $b \neq 0$. More generally, we have the following result.

**Proposition 2.2.** *For any $\mathbb{Z}_M$, given $b$ coprime with $M$ and $c \in \mathbb{Z}_M$, there is a unique solution for the equation $b \times x = c$.*

2.1. **$b$-ary expressions.** An *alphabet* is a finite set $\mathcal{A}$ of *symbols*, or *letters*. A *word on $\mathcal{A}$* is a finite sequence of letters[1]; in particular, $\epsilon$ represents the empty sequence, or *empty word*. The *length* of a word $w$, denoted by $|w|$, is the length of the corresponding sequence. We denote by $\mathcal{A}^*$ the set of all words on $\mathcal{A}$. $\mathcal{A}^*$ is endowed with the *concatenation* operation, consisting of joining words end-to-end. Given a natural number $b > 1$, by a *representation* of a natural number $n$ *in base $b$* we

[1]By default, nonempty sequences will start from index 0.

mean a word $w$ on the alphabet $\{0,\dots,b-1\}$ such that $n=\sum_{i=0}^{|w|-1} w_i b^{|w|-1-i}$ (the empty sequence representing the number 0). In such a case, we also say that $w$ is a *$b$-ary expression* of $n$. The symbols $0,\dots,b-1$ are also called *digits* and, except when it is likely to lead to confusion, $b$-ary expressions are written down without any special characters between the digits. Note that the representation in base $b$ of a number is unique except for leading 0's (in our application here we need them).

**Remark 2.3.** There are connections between certain arithmetic operations and manipulation of $b$-ary expressions:

- Multiplication by $b^k$ corresponds to appending $k$ 0's at the right.
- The last $k$ digits of a $b$-ary expression correspond to the remainder of the division by $b^k$; deleting those last $k$ digits, we obtain the integer part of such division. Consequently, two sequences in base $b$ represent numbers equivalent mod $b^k$ if and only if they coincide in the last $k$ digits.

There are a lot of very nice and comprehensive treatments of number representations (see, for instance, [2] or [3]).

2.2. **Markov chains.** Next, we present a classical formalism which will allow us to consider and solve our problem within the framework of dynamical systems. We include just a very basic summary of the theory, suited strictly for our purposes (for a general treatment, see, for instance, [4] or [9]).

A *discrete-time finite-state homogeneous Markov chain* is a sequence $\{X_n\}_{n\in\mathbb{N}}$ of random variables on a finite *state space* $K$ whose conditional probabilities satisfy the *homogeneous Markov property*:

$$\mathbb{P}\left(X_{n+1}=r \,|\, X_n=q,\, X_{n-1}=s_{n-1},\dots,X_0=s_0\right)=\mathbb{P}\left(X_1=r \,|\, X_0=q\right)$$

for any $n\in\mathbb{N}$ and any $q,r,s_0,\dots,s_{n-1}\in K$.

From now on, discrete-time finite-state homogeneous Markov chains will be referred to as simply *Markov chains*, or *Markov processes*.

$\mathbb{P}\left(X_1=r \,|\, X_0=q\right)$ is the *one-step transition probability from state $q$ to state $r$*, and is denoted by $\mathcal{P}_{q,r}$. The whole 2-dimensional array $\mathcal{P}=\left(\mathcal{P}_{q,r}\right)_{q,r\in K}$ is called the *transition matrix* of the chain, and completely characterizes the chain (up to a renaming of the states).

It is well known that $\mathbb{P}\left(X_n=r \,|\, X_0=q\right)$, the *$n$-step transition probability from state $q$ to state $r$*, is the $(q,r)$-entry of the $n$th power of $\mathcal{P}$, that is, $\left(\mathcal{P}^n\right)_{q,r}$.

The Markov chain is called *irreducible* if each pair $q,r\in K$ admits $n\in\mathbb{N}$ such that $\left(\mathcal{P}^n\right)_{q,r}>0$.

The *period* of a state $q$, denoted by $\mathrm{per}(q)$, is

$$\mathrm{per}(q)=\gcd\left\{n>0:\left(\mathcal{P}^n\right)_{q,q}>0\right\}.$$

A state having period 1 is said to be *aperiodic*. The Markov process is called *aperiodic* when all its states are aperiodic.

A known fact about any irreducible Markov process is that all its states have the same period.

A Markov chain which is both irreducible and aperiodic is said to be *ergodic*.

A fundamental question about the transition matrix of a Markov chain is the existence of an *invariant vector*, that is, a probability vector $\mathbf{v}$ for the states such that $\mathbf{v}\mathcal{P} = \mathbf{v}$, and whether such $\mathbf{v}$ is unique. A known deep result about Markov processes, which is of fundamental importance in this work, is that the transition matrix of any ergodic Markov chain possesses exactly one invariant vector, and the asymptotic probability that the process is in a given state is the corresponding entry of such vector. In [4, p. 208] there is a proof of this result (in a more general setting, for arbitrary Markov chains) which we state as follows:

**Lemma 2.4** ([4, Theorem 6.4 (3)])**.** *Let $\{X_n\}_{n\in\mathbb{N}}$ be an ergodic Markov chain with transition matrix $\mathcal{P}$. Then, there exists a unique vector $\mathbf{v}$ such that $\mathbf{v}\mathcal{P} = \mathbf{v}$. Moreover, for any state $r$, we have that $\lim_{n\to\infty} \mathbb{P}(X_n = r) = \mathbf{v}_r$.*

2.3. **Stochastic automata.** Markov chains have a graphical and intuitive counterpart, which we will introduce now (see [8] for a general treatment).

**Definition 2.5.** A *stochastic automaton* is a 4-tuple $(K, \mathcal{A}, \delta, \mathbf{p})$, where $K$ is a finite set of *states*, $\mathcal{A}$ is a finite *input alphabet*, $\delta$ is the *next state function* from $K \times \mathcal{A}$ to $K$, and $\mathbf{p}$ is a strictly positive probability vector for $\mathcal{A}$, that is, $0 < \mathbf{p}_a < 1$ for each $a \in \mathcal{A}$ and $\sum_{a\in\mathcal{A}} \mathbf{p}_a = 1$.

In other words, a stochastic automaton is a standard deterministic finite-state automaton (without indication of initial and final states) together with a positive probability function for its input alphabet. A classical presentation of finite-state automata is given in [6].

It is customary to represent the stochastic automaton as a directed arc-labeled graph having $K$ as its vertex set, and whose edge set is as follows: from vertex $q$ there is an edge labeled "$a : \mathbf{p}_a$" to vertex $r$ if and only if $\delta(q, a) = r$.

We extend inductively $\delta$ to $K \times \mathcal{A}^*$ the way we do for finite automata, that is,

- $\delta(q, \epsilon) = q$ for each $q \in K$;
- $\delta(q, va) = \delta(\delta(q, v), a)$ for each $q \in K$, $v \in \mathcal{A}^*$ and $a \in \mathcal{A}$.

Similarly, the probability distribution $\mathbf{p}$ for $\mathcal{A}$ is extended to $\mathcal{A}^*$ in the natural way: $\mathbf{p}(\epsilon) = 1$ and $\mathbf{p}(t_0 \dots t_j) = \mathbf{p}_{t_0} \cdots \mathbf{p}_{t_j}$. In particular, such extension of $\mathbf{p}$ defines a positive probability for each path (of any length) in the graph.

Stochastic automata can be regarded as Markov processes. The stochastic automaton $(K, \mathcal{A}, \delta, \mathbf{p})$ corresponds to the Markov chain having state space $K$, with the one-step transition probability from state $q$ to state $r$ being the sum of the probabilities of all the edges from $q$ to $r$ in the automaton; i.e., the transition matrix $\mathcal{P}$ of the chain (which we will also call the *transition matrix of the automaton*) is defined by

$$\mathcal{P}_{q,r} = \sum_{a\in\mathcal{A}:\delta(q,a)=r} \mathbf{p}_a. \tag{2.1}$$

**Definition 2.6.** A stochastic automaton is said to be *irreducible* (resp., *aperiodic*, *ergodic*) when its corresponding Markov chain is irreducible (resp., aperiodic, ergodic).

With $\mathcal{P}$ as defined in (2.1), the $(q,r)$-entry of $\mathcal{P}^n$ contains the sum of the probabilities of all the paths of length $n$ in the graph going from state $q$ to state $r$. Having this in mind, we can check ergodicity of the chain in terms of paths and cycles in the graph, as follows:

- For $q, r \in K$ and $n \in \mathbb{N}$, we have that $(\mathcal{P}^n)_{q,r} > 0$ if and only if there exists some path of length $n$ going from $q$ to $r$ in the graph. Hence, irreducibility of the chain is equivalent to having at least one path (of any length) from each vertex to each other.
- For $q \in K$ and $n > 0$, $(\mathcal{P}^n)_{q,q} > 0$ if and only if there exists a cycle of length $n$ on $q$. Hence, the period of state $q$ is the greatest common divisor of the lengths of all nonempty cycles on $q$, i.e., $\mathrm{per}(q) = \gcd\{|w| : w \neq \epsilon, \delta(q,w) = q\}$. In particular, a state with a loop is aperiodic.

Observe that the sum of all the entries in row $q$ of $\mathcal{P}$ equals the sum of the probabilities of all the edges in the automaton starting at state $q$; since $\delta$ is a function with domain $K \times \mathcal{A}$, we have that $\sum_{r\in K} \mathcal{P}_{q,r} = \sum_{a\in\mathcal{A}} \mathbf{p}_a = 1$, that is, each row of $\mathcal{P}$ is a probability vector for $K$. Concerning the columns of $\mathcal{P}$, the sum of all the entries in column $r$ equals the sum of the probabilities of all the edges in the automaton arriving at state $r$ (but this sum is not always 1). Note that $\mathcal{P}_{q,r} = 0$ if there is no $a \in \mathcal{A}$ such that $\delta(q,a) = r$.

## 3. Modular automata

In this section, we define a subclass of the family of stochastic automata, which will be very useful for our purposes.

For the rest of this work, $b > 1$ will represent an integer base, $\mathcal{A}_b = \{0, \ldots, b-1\}$ will be the set of digits for $b$-ary expressions and $\mathbf{p}$ will represent a strictly positive probability vector for $\mathcal{A}_b$.

**Definition 3.1.** Let $M$ be an integer greater than 1. The $(b, M, \mathbf{p})$-*modular automaton* is the stochastic automaton $(\mathbb{Z}_M, \mathcal{A}_b, \delta, \mathbf{p})$, where $\delta(q,a) = (qb+a) \bmod M$ for each $q \in K$ and $a \in \mathcal{A}_b$.

**Example 3.2.** The $(2, 3, (0.1, 0.9))$-modular automaton has states $\mathbb{Z}_3 = \{0,1,2\}$, input alphabet $\mathcal{A}_2 = \{0,1\}$ and function $\delta$ as specified in Figure 4 (in the table at left, rows correspond to members of $\mathbb{Z}_3$ and columns to members of $\mathcal{A}_2$; at right, the picture of the corresponding graph).

The finite automaton underlying a $(b, M, \mathbf{p})$-modular automaton is a classical example in the framework of finite-state automata (see, for instance, [3]). It allows a very easy computation of $n \bmod M$ provided we have a $b$-ary expression $w$ of the number $n$: in the graph which represents the automaton, start at state 0 and

| $\delta$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 2 | 0 |
| 2 | 1 | 2 |

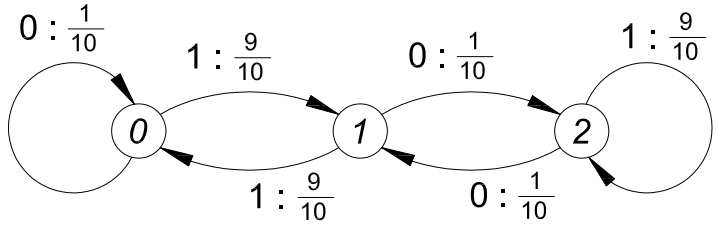



FIGURE 4. $(2, 3, (0.1, 0.9))$-modular automaton.

follow the unique labeled path corresponding to the sequence of symbols in $w$; the final vertex of this path is $n \bmod M$. More generally, we have the following result.

**Proposition 3.3.** *Consider any $(b, M, \mathbf{p})$-modular automaton. For every state $q \in \mathbb{Z}_M$ and every word $w$ in $\mathcal{A}_b^*$, if $w$ is a $b$-ary expression of a number $n$, then $\delta(q, w) = \left(b^{|w|}q + n\right) \bmod M$.*

*Proof.* Let $q$ be any state in $\mathbb{Z}_M$. We will proceed by induction on $|w|$, the length of $w$:

- $|w| = 0$: then $w = \epsilon$, so $n = 0$. Hence $\left(b^0 q + 0\right) \bmod M = q = \delta(q, \epsilon)$, as desired.
- Let us suppose the statement valid for any word of length $k$, and let $w$ be a word of length $k + 1$. Hence $w = va$ for some $v \in \mathcal{A}_b^*$ of length $k$ and $a \in \mathcal{A}_b$. Let $n, m$ be the numbers whose $b$-ary expressions are respectively $w$ and $v$. Observe that $n = mb + a$.

  From the definition of $\delta$ (and its extension to $K \times \mathcal{A}_b^*$), we have $\delta(q, w) = \delta(q, va) = \delta(\delta(q, v), a) = (\delta(q, v)b + a) \bmod M$. But $|v| = k$, so from the induction hypotesis we have $\delta(q, v) = \left(b^{|v|}q + m\right) \bmod M$. Hence

$$\delta(q, w) = \left(\left(\left(b^{|v|}q + m\right) \bmod M\right) b + a\right) \bmod M.$$

  The value of the right-hand side does not change if we ignore the first 'mod $M$' and take mod $M$ just once at the end. Therefore,

$$\delta(q, w) = \left(b^{|v|+1}q + mb + a\right) \bmod M = \left(b^{|w|}q + n\right) \bmod M,$$

  and the inductive step is established.

□

**Remark 3.4.** From our previous result, observe that, as a particular case in any $(b, M, \mathbf{p})$-modular automaton, if $w$ is the representation of $n$ in base $b$, then $\delta(0, w) = n \bmod M$, according to our comment before Proposition 3.3.

Intuitively, it is clear that any sequence of digits can be extended to a $b$-ary representation of a number whose remainder modulo $M$ is any desired value. Just for the sake of completeness, we include here a proof of this fact in our next result.

**Lemma 3.5.** *Every modular automaton is irreducible.*

*Proof.* Let us consider any $(b, M, \mathbf{p})$-modular automaton, and let $q, r$ be states with $q \neq r$. Take any integer $k$ with $b^k \geq M$. Put $n = \left(r - qb^k\right) \bmod M$, and let $w$ be a word of length $k$ which represents $n$ in base $b$ (note that $0 \leq n < M \leq b^k$, so there is a word of length at most $k$ which represents $n$ in base $b$; by appending 0's at left of this word if necessary, we obtain such $w$). From Proposition 3.3, we have that $\delta(q, w) = (qb^k + n) \bmod M = r$, as desired. □

We have the following even stronger property of modular automata.

**Lemma 3.6.** *Every modular automaton is ergodic.*

*Proof.* Let $\mathcal{M}$ be a modular automaton. We have that $\delta(0, 0) = 0$, so state 0 has a loop. Then, $\mathrm{per}(0) = 1$, that is, 0 is aperiodic. From Lemma 3.5, we know that $\mathcal{M}$ is irreducible, and consequently all its states have the same period 1, so $\mathcal{M}$ itself is aperiodic. Since $\mathcal{M}$ is irreducible and aperiodic, we have the result. □

Due to Lemma 3.6, and having in mind Lemma 2.4 and Remark 3.4, we can solve our problem of finding the asymptotic distribution of the number represented by a random $b$-ary expression, modulo $M$, by obtaining the unique invariant vector of the corresponding ergodic $(b, M, \mathbf{p})$-modular automaton. In the next section, we do so for the case that $\gcd(b, M) = 1$, and in Section 5 we obtain the invariant vector for the general case.

## 4. The case $b$ and $M$ coprime

Throughout the present section, $M > 1$ will represent an integer coprime with $b$, and $\mathcal{P}$ will be the transition matrix of the $(b, M, \mathbf{p})$-modular automaton.

Suppose that a long sequence $w = w_0 w_1 \dots w_j$ of digits from the base is generated digit by digit, in such a way that each $w_i$ is $a$ with probability $\mathbf{p}_a$, independently of the other terms of the sequence. Such $w$ is a $b$-ary expression of a number $n$. As announced in Section 1, we will now prove that, for any $r \in \{0, \dots, M-1\}$, in the steady state the event $n \bmod M = r$ has probability $1/M$, independently of $r$ and $\mathbf{p}$. That is, in the steady state the distribution of $n \bmod M$ is the discrete uniform vector $\left(\frac{1}{M}\right)_{r \in \{0,\dots,M-1\}}$. In order to achieve this result, we will consider the $(b, M, \mathbf{p})$-modular automaton.

Given a state $r \in \mathbb{Z}_M$ and a digit $a \in \mathcal{A}_b$, we ask how many edges labeled "$a : \mathbf{p}_a$" end at $r$ in the corresponding graph. As we will see in our next result, due to the coprimality between $b$ and $M$ there is one, and only one, such edge.

**Lemma 4.1.** *Let $r \in \mathbb{Z}_M$ and $a \in \mathcal{A}_b$. Then, there is exactly one state $q_a \in \mathbb{Z}_M$ such that $\delta(q_a, a) = r$*

*Proof.* According to Definition 3.1, for any state $q \in \mathbb{Z}_M$, we have $\delta(q, a) = (bq + a) \bmod M$, so the condition $\delta(q, a) = r$ is met exactly for all those $q$ such that $bq + a \equiv_M r$. As $b$ and $M$ are coprime numbers, from Proposition 2.2 there exists exactly one state $q_a \in \mathbb{Z}_M$ such that $bq_a \equiv_M r - a$. That is, $\delta(q_a, a) = r$, and for all $q \neq q_a$, we have $\delta(q, a) \neq r$. □

Given states $q$ and $r$, it will be useful to have a notation for the set of digits corresponding to edges from $q$ to $r$ in the modular automaton. Concretely, for $q, r \in \mathbb{Z}_M$, we set $E_{q,r} = \{a \in \mathcal{A}_b : \delta(q, a) = r\}$.

For instance, concerning Example 3.2, $E_{1,0} = \{1\}$ and $E_{2,0} = \emptyset$.

Fixed $r \in \mathbb{Z}_M$, it turns out that $\{E_{q,r} : q \in \mathbb{Z}_M\}$ is a pairwise disjoint family whose union is $\mathcal{A}_b$, as we will see next.

**Lemma 4.2.** *Let $r \in \mathbb{Z}_M$. Then, $\mathcal{A}_b = \bigcup_{q\in\mathbb{Z}_M} E_{q,r}$, where the union is pairwise disjoint.*

*Proof.* First let us see the equality. $\bigcup_{q\in\mathbb{Z}_M} E_{q,r} \subset \mathcal{A}_b$ is trivial, since each $E_{q,r}$ is a subset of $\mathcal{A}_b$. For the other inclusion, let $a \in \mathcal{A}_b$. From Lemma 4.1, there is a unique $q_a \in \mathbb{Z}_M$ such that $\delta(q_a, a) = r$. Then $a \in E_{q_a,r}$, which is a subset of $\bigcup_{q\in\mathbb{Z}_M} E_{q,r}$, so we have $\mathcal{A}_b \subset \bigcup_{q\in\mathbb{Z}_M} E_{q,r}$.

Now let $q_1, q_2 \in \mathbb{Z}_M$, and suppose that there is $a \in E_{q_1,r} \cap E_{q_2,r}$. This means that $\delta(q_1, a) = r$ and $\delta(q_2, a) = r$. But again from Lemma 4.1, we have that $q_1 = q_2$. That is, the family $\{E_{q,r} : q \in \mathbb{Z}_M\}$ is pairwise disjoint. □

Our previous result has an important consequence for the column vectors of $\mathcal{P}$: all of them are probability vectors.

**Proposition 4.3.** *Let $r \in \mathbb{Z}_M$. Then, $\sum_{q\in\mathbb{Z}_M} \mathcal{P}_{q,r} = 1$.*

*Proof.* Recall that, for any $q \in \mathbb{Z}_M$, we have

$$\mathcal{P}_{q,r} = \sum_{a\in\mathcal{A}_b:\delta(q,a)=r} \mathbf{p}_a.$$

According to the definition of $E_{q,r}$, the righ-hand member is $\sum_{a\in E_{q,r}} \mathbf{p}_a$. Adding up over $q \in \mathbb{Z}_M$, and applying Lemma 4.2, we have

$$\sum_{q\in\mathbb{Z}_M} \mathcal{P}_{q,r} = \sum_{q\in\mathbb{Z}_M} \sum_{a\in E_{q,r}} \mathbf{p}_a = \sum_{a\in\bigcup_{q\in\mathbb{Z}_M} E_{q,r}} \mathbf{p}_a = \sum_{a\in\mathcal{A}_b} \mathbf{p}_a = 1,$$

and the result is established. □

From this, we arrive to our first main result.

**Theorem 4.4.** *Let $\mathbf{u}$ be the uniform vector for $\mathbb{Z}_M$, that is, $\mathbf{u}_q = 1/M$ for each $q \in \mathbb{Z}_M$. Then, $\mathbf{u}$ is the unique invariant vector of $\mathcal{P}$.*

*Proof.* From Lemmas 2.4 and 3.6, we know that $\mathcal{P}$ has a unique invariant vector, so all we have to do is check that $\mathbf{u}$ is invariant under multiplication by $\mathcal{P}$. Let $r \in \mathbb{Z}_M$. We have that

$$(\mathbf{u}\mathcal{P})_r = \sum_{q\in\mathbb{Z}_M} \mathbf{u}_q \mathcal{P}_{q,r} = \sum_{q\in\mathbb{Z}_M} \frac{1}{M} \mathcal{P}_{q,r} = \frac{1}{M} \sum_{q\in\mathbb{Z}_M} \mathcal{P}_{q,r} = \frac{1}{M} = \mathbf{u}_r,$$

where we have applied Proposition 4.3. Since $(\mathbf{u}\mathcal{P})_r = \mathbf{u}_r$ for any $r \in \mathbb{Z}_M$, we have $\mathbf{u}\mathcal{P} = \mathbf{u}$, and the result is established. □

Theorem 4.4 is an explanation for the results of simulations shown in Figures 1 and 3 (a) concerning the frequencies of residues modulo an $M$ coprime with the base: in the long term (here, this means long sequences of digits from the base), the Markov chain is in any state with probability $1/M$, and by virtue of Remark 3.4 and Lemma 2.4, this is equivalent to saying that any possible residue has probability $1/M$.

## 5. The invariant vector for the general case

In this section we will consider the case that the modulo $M > 1$ is not necessarily coprime with $b$.

From Lemma 3.6 we know that, even in this case, the Markov process has still an invariant vector $\mathbf{v}$, whose entries indicate the steady state frequencies of each possible remainder. One (tedious) way to get such $\mathbf{v}$ is to solve the system of equations implicit in $\mathbf{v}\mathcal{P} = \mathbf{v}$ and $\sum \mathbf{v}_r = 1$. In order to get some insight about the shape of the entries of $\mathbf{v}$, we considered the case of binary representations ($b = 2$), taking the probability $p$ of digit 0 as a parameter (hence being $1 - p$ the probability of digit 1). By using a mathematical software to solve the above system, we obtained the invariant vector $\mathbf{v}$ for the cases $M = 2$, 4, 6, 8, 10, 12, as seen in Table 3 below.

| $M$ | $\mathbf{v}$ |
|---|---|
| 2 | $(p, 1-p)$ |
| 4 | $\left(p^2, p(1-p), p(1-p), (1-p)^2\right)$ |
| 6 | $\left(\frac{p}{3}, \frac{1-p}{3}, \frac{p}{3}, \frac{1-p}{3}, \frac{p}{3}, \frac{1-p}{3}\right)$ |
| 8 | $\left(p^3, p^2(1-p), p^2(1-p), p(1-p)^2, p^2(1-p), p(1-p)^2, p(1-p)^2, (1-p)^3\right)$ |
| 10 | $\left(\frac{p}{5}, \frac{1-p}{5}, \frac{p}{5}, \frac{1-p}{5}, \frac{p}{5}, \frac{1-p}{5}, \frac{p}{5}, \frac{1-p}{5}, \frac{p}{5}, \frac{1-p}{5}\right)$ |
| 12 | $\left(\frac{p^2}{3}, \frac{p(1-p)}{3}, \frac{p(1-p)}{3}, \frac{(1-p)^2}{3}, \frac{p^2}{3}, \frac{p(1-p)}{3}, \frac{p(1-p)}{3}, \frac{(1-p)^2}{3}, \frac{p^2}{3}, \frac{p(1-p)}{3}, \frac{p(1-p)}{3}, \frac{(1-p)^2}{3}\right)$ |

Table 3. Invariant vector for $b = 2$, $\mathbf{p} = (p, 1-p)$ and $M \leq 12$, $M$ even.

The result obtained left us with the conjecture that, in the case of binary representations and $M$ even, all $\mathbf{v}_r$ have the form $\frac{p^i(1-p)^j}{m}$ with $i + j = s$ for some integers $s, m$. In fact, we seem to be dealing with the probabilities of all the $s$-digit binary sequences, weighted by some factor $1/m$. It is indeed the case for $b = 2$,

and the explanation for this is encompassed in our next considerations, where we will obtain explicit formulas for $\mathbf{v}_r$ in terms of $b$, $M$, $\mathbf{p}$ and $r$.

For the rest of this section, we fix the following notation:

- $m$ will represent the greatest factor of $M$ which is coprime with $b$.
- $k$ will be the positive integer such that $M = km$.

From the above definitions, two facts follow easily.

**Lemma 5.1.** *$k$ and $m$ are coprime numbers.*

*Proof.* Suppose that $k$ and $m$ had a common prime factor $q$. Since $m$ and $b$ are coprime, $q$ could not divide $b$, so $\gcd(q, b) = 1$. Being also $\gcd(m, b) = 1$, $qm$ would result a divisor of $M$ coprime with $b$, contradicting the maximality of $m$. Hence, $k$ and $m$ cannot have common prime factors. □

**Lemma 5.2.** *Let $q$ be any prime factor of $k$. Then, $q$ is also a factor of $b$.*

*Proof.* If $q$ were not a divisor of $b$, then we would have $\gcd(q, b) = 1$ and $\gcd(m, b) = 1$, and therefore $qm$ would be a divisor of $M$ coprime with $b$, contradicting the maximality of $m$. Hence, $q$ is necessarily a factor of $b$. □

As a consequence, some power of $b$ is divisible by $k$, as we see next.

**Lemma 5.3.** *There exists a natural number $s$ such that $k$ is a factor of $b^s$.*

*Proof.* If $k = 1$, take $s = 0$ and we are done.

If $k > 1$, let $q_1^{s_1} \cdots q_l^{s_l}$ be the prime factorization of $k$ (that is, all the $q_i$ are primes different from each other, and all the $s_i$ are positive integers), and take $s = \max\{s_1, \ldots, s_l\}$. From Lemma 5.2, we have that each $q_i^{s_i}$ is a factor of $b^{s_i}$, which in turn divides $b^s$. Since $\gcd\left(q_i^{s_i}, q_j^{s_j}\right) = 1$ for $i \neq j$, we have that $k$ divides $b^s$. □

Observe that the number $s$ produced in the previous proof is actually the least natural number with the property that $k$ is a factor of $b^s$. From now on, $s$ will represent this minimal value.

For the rest of our work, it will be handy to introduce two new notations. The first one, for the set of all the $s$-digit $b$-ary expressions which represent a number congruent modulo $k$ with a given $r \in \mathbb{Z}_M$. Specifically, for $r \in \mathbb{Z}_M$, we put $T_r = \left\{t_0 \ldots t_{s-1} \in \mathcal{A}_b^* : \sum_{i=0}^{s-1} t_i b^{s-1-i} \equiv_k r\right\}$. For instance, taking $b = 10$, $k = 25$ and $s = 2$, and representing sequences of digits as quoted text, we have $T_0 = \{\text{‘00’}, \text{‘25’}, \text{‘50’}, \text{‘75’}\}$.

The second notation is addresed to represent the number of times that a given digit appears in a $b$-ary expression.

**Definition 5.4.** Let $a \in \mathcal{A}_b$ and $t \in \mathcal{A}_b^*$. The *number of occurrences of $a$ in $t$*, denoted by $\#_a(t)$, is defined to be 0 if $t = \epsilon$, and, for $t = t_0 t_1 \ldots t_j$ (with each $t_i \in \mathcal{A}_b$), $\#_a(t) = \#\{i : t_i = a\}$.

Recall that we have extended $\mathbf{p}$ to $\mathcal{A}_b^*$ by letting $\mathbf{p}(t) = \mathbf{p}_{t_0} \cdots \mathbf{p}_{t_j}$ whenever $t = t_0 t_1 \dots t_j$ with $t_i \in \mathcal{A}_b$. Grouping factors corresponding to identical digits, and considering that $\mathbf{p}_a^{\#_a(t)} = 1$ whenever $a$ does not appear in $t$, we have that $\mathbf{p}(t) = \prod_{a=0}^{b-1} \mathbf{p}_a^{\#_a(t)}$.

Now we are in a position to state our main result, which gives an explicit formula for the entries of the invariant vector $\mathbf{v}$ we are looking for.

**Theorem 5.5.** *Let $w_0 w_1 \dots w_j$ be a random sequence of digits from $\mathcal{A}_b$, representing in base $b$ the number $n$. Then, for any $r \in \mathbb{Z}_M$, the steady state probability that $r = n \bmod M$ is given by*

$$\mathbf{v}_r = \frac{1}{m} \sum_{t \in T_r} \prod_{a=0}^{b-1} \mathbf{p}_a^{\#_a(t)}$$

*with $T_r$ and $\#_a(t)$ as defined above.*

*Proof.* Let $L$ and $R$ be the numbers represented in base $b$ by $w_0 \dots w_{j-s}$ and $w_{j-s+1} \dots w_j$, respectively. That is, $R$ is the number represented in base $b$ by the last $s$ digits of $w$, and $L$ is the number represented by the previous digits:

$$w = \overbrace{w_0 w_1 \cdots w_{j-s}}^{L} \overbrace{w_{j-s+1} \cdots w_j}^{R}.$$

Hence we have $n = Lb^s + R$.

Let $r$ be a given number in $\mathbb{Z}_M$. Since $M = km$ with $\gcd(k, m) = 1$ (Lemma 5.1), from Proposition 2.1 we have that $n \equiv_M r$ is equivalent to having, simultaneously, $Lb^s + R \equiv_m r$ and $Lb^s + R \equiv_k r$. The former condition requires that $L \equiv_m (r - R)\left(b^s\right)^{-1}$. Hence, as $m$ is coprime with $b$, from Theorem 4.4 we have that the first congruence has probability $1/m$.

Concerning the second congruence, and since $k$ is a factor of $b^s$ (Lemma 5.3), we need to have simply $R \equiv_k r$. This congruence occurs with a probability given by the sum of the probabilities of all the $b$-ary expressions of length $s$ representing in base $b$ a number congruent modulo $k$ with $r$. That is to say, $R \equiv_k r$ has probability $\sum_{t \in T_r} \mathbf{p}(t)$, or $\sum_{t \in T_r} \prod_{a=0}^{b-1} \mathbf{p}_a^{\#_a(t)}$.

Since the events corresponding to each congruence are independent, we conclude that the probability that $n \equiv_M r$ is

$$\mathbf{v}_r = \frac{1}{m} \sum_{t \in T_r} \prod_{a=0}^{b-1} \mathbf{p}_a^{\#_a(t)},$$

and the result is established. □

Observe that Theorem 5.5 is in fact a generalization of Theorem 4.4: if $M$ is coprime with $b$, then $m = M$ and $k = 1$, so $s = 0$, and in such a case $T_r$ is nothing but the singleton $\{\epsilon\}$, and thus $\sum_{t \in T_r} \prod_{a=0}^{b-1} \mathbf{p}_a^{\#_a(t)} = \prod_{a=0}^{b-1} \mathbf{p}_a^{\#_a(\epsilon)} = 1$; hence, according to Theorem 5.5, for $\gcd(b, M) = 1$, we have $\mathbf{v}_r = 1/m = 1/M$ for any $r$, which agrees with Theorem 4.4.

Let us illustrate the statement in Theorem 5.5 with some examples.

**Example 5.6.** Take $b = 10$, $M = 18$, and suppose that digit 0 has probability 24/100, 5 has probability 52/100, 8 has probability 17/100 and each other decimal digit has probability 1/100. That is,

$$\mathbf{p} = (0.24, 0.01, 0.01, 0.01, 0.01, 0.52, 0.01, 0.01, 0.17, 0.01)\,.$$

In this case, we have $m = 9$, $k = 2^1$ and $s = 1$.

Using the notation given in the theorem, we have, for instance, $T_4 = \{\text{'0'}, \text{'2'}, \text{'4'}, \text{'6'}, \text{'8'}\}$, so the probability for $n \equiv_{18} 4$ is $\mathbf{v}_4 = \frac{1}{9}(\mathbf{p}_0 + \mathbf{p}_2 + \mathbf{p}_4 + \mathbf{p}_6 + \mathbf{p}_8) = \frac{44}{900}$. This is the same value of $\mathbf{v}_r$ for any $r$ even. Similarly, for any odd $r$, we have $T_r = \{\text{'1'}, \text{'3'}, \text{'5'}, \text{'7'}, \text{'9'}\}$, and therefore $\mathbf{v}_r = \frac{1}{9}(\mathbf{p}_1 + \mathbf{p}_3 + \mathbf{p}_5 + \mathbf{p}_7 + \mathbf{p}_9) = \frac{56}{900}$.

**Example 5.7.** Let $b = 10$, $M = 75$ and let $\mathbf{p}$ be as in Example 5.6. Now we have $m = 3$, $k = 5^2$ and $s = 2$. Let us calculate the probability of having a multiple of 75. We have $T_0 = \{\text{'00'}, \text{'25'}, \text{'50'}, \text{'75'}\}$, so the probability for $n \equiv_{75} 0$ is

$$\mathbf{v}_0 = \frac{1}{3}\left(\mathbf{p}_0^2 + \mathbf{p}_2\mathbf{p}_5 + \mathbf{p}_5\mathbf{p}_0 + \mathbf{p}_7\mathbf{p}_5\right) = \frac{1928}{30000} \simeq 0.064,$$

which agrees with the value for the first bar in the simulation shown in Figure 3 (c).

**Example 5.8.** For $b = 2$, $M = 12$, $\mathbf{p} = (p, 1-p)$ (where $p$ is a parameter in the open interval $(0, 1)$), we have $m = 3$, $k = 2^2$, $s = 2$. Consider $r = 3$. We have $T_3 = \{\text{'11'}\}$, so $\mathbf{v}_3 = \frac{1}{3}\mathbf{p}_1^2 = \frac{(1-p)^2}{3}$. This is in accordance with the entry for 3 at the last row in Table 3.

**Remark 5.9.** In Example 5.8, we have $k = b^s$. Whenever the values of $b$ and $M$ lead to this condition, for any $r \in \mathbb{Z}_M$, the set $T_r$ is a singleton consisting solely of the sequence of the last $s$ digits of the $b$-ary expression of $r$ (left-padded with 0 if necessary); so, calling $t$ this $s$-digit sequence, the formula in Theorem 5.5 reduces to

$$\mathbf{v}_r = \frac{1}{m}\mathbf{p}_0^{\#_0(t)}\mathbf{p}_1^{\#_1(t)}\cdots\mathbf{p}_{b-1}^{\#_{b-1}(t)}.$$

In particular, for $b = 2$, we have $M = m2^s$ for $m$ odd and $s$ natural, so, for any $r \in \mathbb{Z}_M$,

$$\mathbf{v}_r = \frac{1}{m}\mathbf{p}_0^{\#_0(t)}\mathbf{p}_1^{\#_1(t)},$$

where $t$ is the word formed by the last $s$ bits in the binary expression of $r$. The above expression for $\mathbf{v}_r$ is consistent with the results shown in Table 3.

## 6. Conclusions and perspectives

Given $b$ and $M$ integers greater than 1, together with a strictly positive probability vector $\mathbf{p}$ for the digits in the base $b$, and for $r \in \mathbb{Z}_M$ fixed, in this paper we have obtained the formula for the probability that a randomly generated long enough $b$-ary expression represents a number congruent modulo $M$ with $r$ (in particular, when $\gcd(b, M) = 1$, we have shown the counter-intuitive fact that this probability is equal to $1/M$ regardless of $r$ and $\mathbf{p}$). The case of $b$-ary representations is then

almost completely understood whenever we consider integer bases, leaving just the study of the convergence rate towards the asymptotic distribution.

A future research line, suggested by Fabien Durand at UPJV (Amiens, France), is based on considering noninteger bases, for instance, Fibonacci representations. Let $\{f_i\}_{i\in\mathbb{N}}$ be the (shifted) classical Fibonacci sequence $\{1, 2, 3, 5, 8, \ldots\}$, which satisfies the recurrence $f_k = f_{k-1} + f_{k-2}$. It is well known that every positive integer number $n$ can be associated with a unique finite binary sequence $w = w_0 w_1 \cdots w_j$ with $w_j = 1$ and not containing two consecutive 1's, in such a way that $n = w_0 f_0 + w_1 f_1 + \cdots + w_j f_j$. Fixed the probability $p$ of digit 0 (so $1 - p$ is the probability of 1), and given an integer $M$ greater than 1 and any $r \in \mathbb{Z}_M$, it would be interesting to obtain the probability that a random sequence of independently generated bits (according to $p$), not containing 11, be the Fibonacci representation of a number $n$ congruent modulo $M$ with $r$. Simulation induces the conjecture that, in the steady state, this is always $1/M$ regardless of $r$ and $p$. Although the situation seems to be quite similar to that of integer bases, attacking the problem via Markov chains can produce a stochastic automaton which is not ergodic, so probably other tools and considerations are required to solve the raised conjecture. This problem can be generalized by considering any sequence $\{f_i\}_{i\in\mathbb{N}}$ defined by a high-order linear recurrence, in such a way that every positive integer can be represented by a unique finite binary sequence as above.

## Acknowledgments

We thank the reviewers for their valuable contributions, and Valérie Berthé, Alejandro Maass, Fabien Durand and Fréderic Pacaut for reading earlier versions. All this led to improving a lot the presentation of our results.

All the simulations in this work were performed using the *SageMath* software system [1].

## References

[1] *SageMath, the Sage Mathematics Software System* (Version 9.2), The Sage Developers, 2020. Available at https://sagemath.org.

[2] G. Barat, V. Berthé, P. Liardet, and J. Thuswaldner, Dynamical directions in numeration, *Ann. Inst. Fourier (Grenoble)* **56** no. 7 (2006), 1987–2092. DOI MR Zbl

[3] C. Frougny and J. Sakarovitch, Number representation and finite automata, in *Combinatorics, automata and number theory*, Encyclopedia Math. Appl. 135, Cambridge Univ. Press, Cambridge, 2010, pp. 34–107. DOI MR Zbl

[4] G. R. Grimmett and D. R. Stirzaker, *Probability and random processes*, third ed., Oxford University Press, New York, 2001. MR Zbl

[5] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, fourth ed., Oxford, at the Clarendon Press, 1960. MR Zbl

[6] J. E. Hopcroft and J. D. Ullman, *Introduction to automata theory, languages, and computation*, Addison-Wesley Series in Computer Science, Addison-Wesley, Reading, MA, 1979. MR Zbl

[7] D. E. Knuth, *The art of computer programming. Vol. 2: Seminumerical algorithms*, second ed., Addison-Wesley Series in Computer Science and Information Processing, Addison-Wesley, Reading, MA, 1981. MR Zbl

[8] M. O. Rabin, Probabilistic automata, *Inf. Control* **6** no. 3 (1963), 230–245. DOI Zbl

[9] S. M. Ross, *Stochastic processes*, second ed., Wiley Series in Probability and Statistics, John Wiley & Sons, New York, 1996. MR Zbl

*Thomas N. Hibbard*
Departamento de Matemática, Universidad Nacional de Salta, Argentina

*Camilo A. Jadur*
Departamento de Matemática, Universidad Nacional de Salta, Argentina
jadur@unsa.edu.ar

*Jorge F. Yazlle* ✉
Departamento de Matemática, Universidad Nacional de Salta, Argentina
yazlle@unsa.edu.ar

*Received: December 13, 2021*
*Accepted: October 14, 2022*