*J. Aust. Math. Soc.* **114** (2023), 78–109
doi:10.1017/S1446788722000027

# SOLENOIDAL MAPS, AUTOMATIC SEQUENCES, VAN DER PUT SERIES, AND MEALY AUTOMATA

**ROSTISLAV GRIGORCHUK and DMYTRO SAVCHUK**

(Received 24 October 2020; accepted 3 October 2021; first published online 6 April 2022)

Communicated by Ben Martin

**Abstract**

The ring $\mathbb{Z}_d$ of $d$-adic integers has a natural interpretation as the boundary of a rooted $d$-ary tree $T_d$. Endomorphisms of this tree (that is, solenoidal maps) are in one-to-one correspondence with 1-Lipschitz mappings from $\mathbb{Z}_d$ to itself. In the case when $d = p$ is prime, Anashin ['Automata finiteness criterion in terms of van der Put series of automata functions', *p-Adic Numbers Ultrametric Anal. Appl.* **4**(2) (2012), 151–160] showed that $f \in \mathrm{Lip}^1(\mathbb{Z}_p)$ is defined by a finite Mealy automaton if and only if the reduced coefficients of its van der Put series constitute a $p$-automatic sequence over a finite subset of $\mathbb{Z}_p \cap \mathbb{Q}$. We generalize this result to arbitrary integers $d \geq 2$ and describe the explicit connection between the Moore automaton producing such a sequence and the Mealy automaton inducing the corresponding endomorphism of a rooted tree. We also produce two algorithms converting one automaton to the other and *vice versa*. As a demonstration, we apply our algorithms to the Thue–Morse sequence and to one of the generators of the lamplighter group acting on the binary rooted tree.

2020 *Mathematics subject classification*: primary 68Q70; secondary 20M35, 20E08.

*Keywords*: Mealy automata, Moore automata, automatic sequence, van der Put series, $p$-adic analysis, solenoidal maps.

## 1. Introduction

Continuous self-maps of the ring $\mathbb{Z}_p$ of $p$-adic integers are the objects of study of $p$-adic analysis and $p$-adic dynamics. Among all continuous functions $\mathbb{Z}_p \to \mathbb{Z}_p$, there is an natural subclass of 1-Lipschitz functions that do not increase the distances between points of $\mathbb{Z}_p$. These functions appear in many contexts and have various names in the literature. For example, Bernstein and Lagarias in the paper devoted to

The first author graciously acknowledges support from the Simons Foundation through Collaboration Grant No. 527814 and is also supported by the mega-grant of the Russian Federation Government (N14.W03.31.0030). He also gratefully acknowledges support of the Swiss National Science Foundation. The second author greatly appreciates the support of the Simons Foundation through Collaboration Grant No. 317198.

the Collatz '$3n + 1$' conjecture call them solenoidal maps [10], Anashin in [3] (see also [5]) studied the conditions under which these functions act ergodically on $\mathbb{Z}_p$. For us, such functions are especially important because they act on regular rooted trees by endomorphisms (or automorphisms in the invertible case). Topologically, $\mathbb{Z}_p$ is homeomorphic to the Cantor set which, in turn, can be identified with the boundary $X^\infty$ of a rooted $p$-ary tree $X^*$, whose vertices are finite words over the alphabet $X = \{0, 1, \dots, p-1\}$. Namely, we identify a $p$-adic number $x_0 + x_1 p + x_2 p^2 + \cdots$ with the point $x_0 x_1 x_2 \ldots \in X^\infty$. (For the language of rooted trees and group actions on them, see [17, 23].)

Under this identification Nekrashevych, Sushchansky, and the first author [23, Proposition 3.7] showed that a continuous map from $\mathbb{Z}_p$ to itself induces a (graph) endomorphism of the tree $X^*$ precisely when it is 1-Lipschitz. Furthermore, it is an easy but not so well-known observation that the group $\mathrm{Isom}(\mathbb{Z}_p)$ of isometries of $\mathbb{Z}_p$ is naturally isomorphic to the group $\mathrm{Aut}(X^*)$ of automorphisms of a rooted $p$-ary tree. As such, the groups $\mathrm{Isom}(\mathbb{Z}_p)$ contain many exotic groups that provide counterexamples to several long standing conjectures and problems in group theory [20–22, 25] and have connections to other areas of mathematics, such as holomorphic dynamics [8, 33], combinatorics [19], analysis on graphs [18], computer science [11, 29, 30], cryptography [13, 31, 32, 35], and coding theory [12, 19]. In a similar way, one can characterize the group $\mathrm{Isom}(\mathbb{Q}_p)$ of isometries of the field $\mathbb{Q}_p$ of $p$-adic numbers as the group of automorphisms of a regular (not rooted) $(p+1)$-ary tree that fix the pointwise one selected end of this tree.

To describe important subgroups of $\mathrm{Isom}(\mathbb{Z}_p)$ and establish their properties, the languages of self-similar groups and semigroups initiated in [20] and developed in the last four decades (see survey papers [6, 23] and the book [33]), and Mealy automata have proved to be very effective. However, these tools were not widely used by researchers studying $p$-adic analysis and $p$-adic dynamics. There are only a few papers that build bridges between the two worlds. The first realization of an affine transformation of $\mathbb{Z}_p$ by a finite Mealy automaton was constructed by Bartholdi and Šunić in [9]. Ahmed and the second author in [1] described automata defining polynomial functions $x \mapsto f(x)$ on $\mathbb{Z}_d$, where $f \in \mathbb{Z}[x]$, and using the language of groups acting on rooted trees, deduced conditions for ergodicity of the action of $f$ on $\mathbb{Z}_2$ obtained by completely different methods by Larin [27]. In [4], Anashin proved an excellent result relating finiteness of the Mealy automaton generating an endomorphism of the $p$-ary tree to automaticity of the sequence of reduced van der Put coefficients of the induced functions on $\mathbb{Z}_p$, which are discussed below in detail. Automatic sequences represent an important area at the conjunction of computer science and mathematics. Some of the famous examples of automatic sequences include the Thue–Morse sequence and Rudin–Shapiro sequence defining space filling curves. We refer the reader to [2] for details. Recent applications of automatic sequences in group theory include [15, 16].

As in the real analysis, one of the effective ways to study functions $\mathbb{Z}_p \to \mathbb{Z}_p$ is to decompose them into series with respect to some natural basis in the space of continuous functions $C(\mathbb{Z}_p)$ from $\mathbb{Z}_p$ to itself. Two of the most widely used bases of this space are the Mahler basis and the van der Put basis [28, 36]. In the more general settings of the spaces of continuous functions from $\mathbb{Z}_p$ to a field, several other bases have been used in the literature: Walsh basis [38]; Haar basis (used in group theory context, for example, in [7]); Kaloujnine basis [16]. In this paper, we deal with the van der Put basis, which is made of functions $\chi_n(x)$, $n \geq 0$ that are characteristic functions of cylindrical subsets of $\mathbb{Z}_p$ consisting of all elements that have the $p$-adic expansion of $n$ as a prefix. Each continuous function $f \in C(\mathbb{Z}_p)$ can be decomposed uniquely as

$$f(x) = \sum_{n\geq 0} B_n^f \chi_n(x),$$

where the coefficients $B_n^f$ are elements of $\mathbb{Z}_p$ which we call van der Put coefficients. A function $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is 1-Lipschitz if and only if its van der Put coefficients can be represented as $B_n^f = b_n^f d^{\lfloor \log_d n \rfloor}$ for all $n > 0$, where $b_n^f \in \mathbb{Z}_p$ [5]. We call $b_n^f$ the *reduced van der Put coefficients* (see Section 3 for details).

The main results of the present paper are the following two theorems, in which $d \geq 2$ is an arbitrary (not necessarily prime) integer.

THEOREM 1.1. *Let $g \in \mathrm{End}(X^*)$ be an endomorphism of the rooted tree $X^*$, where $X = \{0, 1, \ldots, d-1\}$. Then $g$ is finite state if and only if the following two conditions hold for the transformation $\hat{g}$ of $\mathbb{Z}_d$ induced by $g$:*

(a) *the sequence $(b_n^{\hat{g}})_{n\geq 1}$ of reduced van der Put coefficients of $\hat{g}$ consists of finitely many eventually periodic elements from $\mathbb{Z}_d$;*
(b) *$(b_n^{\hat{g}})_{n\geq 1}$ is $d$-automatic.*

For the case of prime $d = p$, Theorem 1.1 was proved by Anashin in [4] using a completely different method from our approach. The proof from [4] does not provide a direct connection between the Mealy automaton of an endomorphism of $X^*$ and the Moore automaton of the corresponding sequence of its reduced van der Put coefficients. Our considerations are based on understanding the connection between the reduced van der Put coefficients of an endomorphism and of its sections at vertices of the rooted tree via the geometric notion of a portrait. This connection, summarized in the next theorem, bears a distinct geometric flavor and provides a way to effectively relate the corresponding Mealy and Moore automata.

THEOREM 1.2. *Let $X = \{0, 1, \ldots, d-1\}$ be a finite alphabet identified with $\mathbb{Z}/d\mathbb{Z}$.*

(a) *Given an endomorphism $g$ of the tree $X^*$, defined by the finite Mealy automaton, there is an explicit algorithmic procedure given by Theorem 7.1 and Algorithm 7.3 that constructs the finite Moore automaton generating the sequence $(b_n^g)_{n\geq 0}$ of reduced van der Put coefficients of $g$.*
(b) *Conversely, given a finite Moore automaton generating the sequence $(c_n)_{n\geq 0}$ of eventually periodic $d$-adic integers, there is an explicit algorithmic procedure given by Theorem 7.7 and Algorithm 7.8 that constructs the finite Mealy*

*automaton of an endomorphism $g$ whose reduced van der Put coefficients satisfy $b^g_n = c_n$ for all $n \geq 0$.*

(c) *Both constructions are dual to each other in a sense that the automata produced by them cover the input automata as labeled graphs (see Section 7 for the exact definition).*

Theorem 1.2 opens up a new approach to study automatic sequences by means of (semi)groups acting on rooted trees, and *vice versa*, to study endomorphisms of rooted trees via the language of Moore automata. Note that in this context, unlike in the $p$-adic analysis, the fact that the size of the alphabet can be chosen to be not necessarily prime plays an important role since there are important automatic sequences over such alphabets, as well as interesting endomorphisms of $d$-regular rooted trees, where $d$ is not a prime number.

In [4], Anashin, using Christol's famous characterization of $p$-automatic sequences in terms of algebraicity of the corresponding power series, suggested another version of the main result of his paper (that is, of Theorem 1.1 in the case of prime $d$). The authors are not aware of the existence of an analog of Christol's theorem in the situation of $d$-automaticity when $d$ is not prime. The first question that arises is how to define the algebraicity of a function when the field $\mathbb{Q}_p$ is replaced by the ring $\mathbb{Q}_d$ of $d$-adic numbers. The authors do not exclude that the extension of Christol's theorem is possible and leave this question for the future.

The paper is organized as follows. Section 2 introduces necessary notions related to Mealy automata and actions on rooted trees. Section 3 recalls how to represent a continuous function $\mathbb{Z}_d \to \mathbb{Z}_d$ by a van der Put series. We consider automatic sequences and define their portraits and sections in Section 4. The crucial argument relating van der Put coefficients of endomorphisms and their sections is given in Section 5. Section 6 contains the proof of Theorem 1.1. The algorithms relating Mealy and Moore automata associated with an endomorphism of $X^*$ and constituting the proof of Theorem 1.2, are given in Section 7. Finally, two examples are worked out in full detail in Section 8 to conclude the paper.

## 2. Mealy automata and endomorphisms of rooted trees

We start this section by introducing the notions and terminology of endomorphisms and automorphisms of regular rooted trees and transformations generated by Mealy automata. For more details, the reader is referred to [23].

Let $X = \{0, 1, \ldots, d-1\}$ be a finite alphabet with $d \geq 2$ elements (called letters) and let $X^*$ denote the set of all finite words over $X$. The set $X^*$ can be equipped with the structure of a rooted $d$-ary tree by declaring that $v$ is adjacent to $vx$ for every $v \in X^*$ and $x \in X$. Thus finite words over $X$ serve as vertices of the tree. The empty word corresponds to the root of the tree and for each positive integer $n$, the set $X^n$ corresponds to the $n$th level of the tree. Also, the set $X^\infty$ of infinite words over $X$ can be identified with the *boundary* of the tree $X^*$, which consists of all infinite paths in the tree, without backtracking, initiating at the root. We consider endomorphisms and

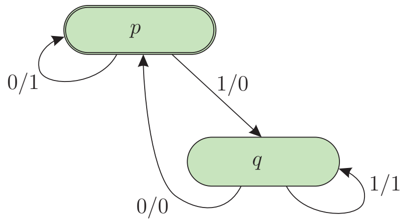


FIGURE 1. Mealy automaton generating the lamplighter group $\mathcal{L}$.

automorphisms of the tree $X^*$ (that is, the maps and bijections of $X^*$ that preserve the root and the adjacency of vertices). We sometimes denote the tree $X^*$ as $T_d$. The semigroup of all endomorphisms of $T_d$ is denoted by $\mathrm{End}(T_d)$ and the group of all automorphisms of $T_d$ is denoted by $\mathrm{Aut}(T_d)$. To operate with such objects, we use the language of Mealy automata.

DEFINITION 2.1. A *Mealy automaton* (or simply *automaton*) is a 4-tuple

$$(Q, X, \delta, \lambda),$$

where

- $Q$ is a set of states;
- $X$ is a finite alphabet (not necessarily $\{0, 1, \ldots, d-1\}$);
- $\delta\colon Q \times X \to Q$ is the *transition function*;
- $\lambda\colon Q \times X \to X$ is the *output function*.

If the set of states $Q$ is finite, the automaton is called *finite*. If for every state $q \in Q$ the output function $\lambda_q(x) = \lambda(q, x)$ induces a permutation of $X$, the automaton $\mathcal{A}$ is called *invertible*. Selecting a state $q \in Q$ produces an *initial automaton* $\mathcal{A}_q$, which formally is a 5-tuple $(Q, X, \delta, \lambda, q)$.

Here we consider automata with the same input and output alphabets.

Automata are often represented by their *Moore diagrams*. The Moore diagram of automaton $\mathcal{A} = (Q, X, \delta, \lambda)$ is a directed graph in which the vertices are in bijection with the states of $Q$ and the edges have the form $q \xrightarrow{x|\lambda(q,x)} \delta(q, x)$ for $q \in Q$ and $x \in X$. Figure 1 shows the Moore diagram of the automaton $\mathcal{A}$ that, as is explained later, generates the lamplighter group $\mathcal{L} = (\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}$.

Every initial automaton $\mathcal{A}_q$ induces an endomorphism of $X^*$, which is also denoted by $\mathcal{A}_q$, defined as follows. Given a word $v = x_1x_2x_3 \ldots x_n \in X^*$, it scans the first letter $x_1$ and outputs $\lambda(q, x_1)$. The rest of the word is handled similarly by the initial automaton $\mathcal{A}_{\delta(q,x_1)}$. So we can actually extend the functions $\delta$ and $\lambda$ to $\delta\colon Q \times X^* \to Q$ and $\lambda\colon Q \times X^* \to X^*$ via the equations

$$\delta(q, x_1x_2 \ldots x_n) = \delta(\delta(q, x_1), x_2x_3 \ldots x_n),$$
$$\lambda(q, x_1x_2 \ldots x_n) = \lambda(q, x_1)\lambda(\delta(q, x_1), x_2x_3 \ldots x_n).$$

https://doi.org/10.1017/S1446788722000027 Published online by Cambridge University Press

The boundary $X^\infty$ of the tree is endowed with a natural topology in which two infinite words are close if they have a large common prefix. With this topology, $X^\infty$ is homeomorphic to the Cantor set. Each endomorphism (respectively automorphism) of $X^*$ naturally induces a continuous transformation (respectively homeomorphism) of $X^\infty$.

DEFINITION 2.2. The semigroup (group) generated by all states of an automaton $\mathcal{A}$ viewed as endomorphisms (automorphisms) of the rooted tree $X^*$ under the operation of composition is called an *automaton semigroup (group)* and is denoted by $\mathbb{S}(\mathcal{A})$ (respectively $\mathbb{G}(\mathcal{A})$).

In the definition of the automaton, we do not require the set $Q$ of states to be finite. With this convention, the notion of an automaton group is equivalent to the notions of a *self-similar group* [33] and *state-closed group* [34]. However, most of the interesting examples of automaton (semi)groups are finitely generated (semi)groups defined by finite automata.

Let $g \in \mathrm{End}(X^*)$ and $x \in X$. For any $v \in X^*$, we can write

$$g(xv) = g(x)v'$$

for some $v' \in X^*$. Then the map $g|_x \colon X^* \to X^*$ given by

$$g|_x(v) = v'$$

defines an endomorphism of $X^*$ which we call the *state* (or *section*) of $g$ at vertex $x$. We can inductively extend the definition of a section at a letter $x \in X$ to a section at any vertex $x_1x_2 \ldots x_n \in X^*$ as follows:

$$g|_{x_1x_2\ldots x_n} = g|_{x_1}|_{x_2} \cdots |_{x_n}.$$

We adopt the following convention throughout the paper. If $g$ and $h$ are elements of some (semi)group acting on a set $Y$ and $y \in Y$, then

$$gh(y) = h(g(y)).$$

Hence, the state $g|_v$ at $v \in X^*$ of any product $g = g_1g_2 \cdots g_n$, where $g_i \in \mathrm{Aut}(X^*)$ for $1 \le i \le n$, can be computed as follows:

$$g|_v = g_1|_v g_2|_{g_1(v)} \cdots g_n|_{g_1g_2\cdots g_{n-1}(v)}.$$

Also, we use the language of wreath recursions. For each automaton semigroup $G$, there is a natural embedding

$$G \hookrightarrow G \wr \mathrm{Tr}(X),$$

where $\mathrm{Tr}(X)$ denotes the semigroup of all selfmaps of set $X$. This embedding is given by

$$G \ni g \mapsto (g_0, g_1, \ldots, g_{d-1})\sigma_g \in G \wr \mathrm{Tr}(X), \tag{2-1}$$

where $g_0, g_1, \ldots, g_{d-1}$ are the states of $g$ at the vertices of the first level and $\sigma_g$ is the transformation of $X$ induced by the action of $g$ on the first level of the tree. If

https://doi.org/10.1017/S1446788722000027 Published online by Cambridge University Press

$\sigma_g$ is the trivial transformation, it is customary to omit it in Equation (2-1). We call $(g_0, g_1, \ldots, g_{d-1})\sigma_g$ the *decomposition of $g$ at the first level* (or the *wreath recursion of $g$*). When this does not cause any confusion, we identify $g$ with its wreath recursion and write simply

$$g = (g_0, g_1, \ldots, g_{d-1})\sigma_g.$$

In the case of the automaton group $G = \mathbb{G}(\mathcal{A})$, the embedding Equation (2-1) is actually the embedding into the group $G \wr \mathrm{Sym}(X)$.

The decomposition at the first level of all generators $\mathcal{A}_q$ of an automaton semigroup $\mathbb{S}(\mathcal{A})$ under the embedding Equation (2-1) is called the *wreath recursion defining the semigroup*. Such a decomposition is especially convenient for computing the states of semigroup elements. Indeed, the products endomorphisms and inverses of automorphisms can be found as follows. If $g = (g_0, g_1, \ldots, g_{d-1})\sigma_g$ and $h = (h_0, h_1, \ldots, h_{d-1})\sigma_h$ are two elements of $\mathrm{End}(X^*)$, then

$$gh = (g_0 h_{\sigma_g(0)}, g_1 h_{\sigma_g(1)}, \ldots, g_{d-1} h_{\sigma_g(d-1)})\sigma_g\sigma_h$$

and in the case when $g$ is an automorphism, the wreath recursion of $g^{-1}$ is

$$g^{-1} = (g^{-1}_{\sigma_g^{-1}(0)}, g^{-1}_{\sigma_g^{-1}(1)}, \ldots, g^{-1}_{\sigma_g^{-1}(d-1)})\sigma_g^{-1}.$$

## 3. Continuous maps from $\mathbb{Z}_d$ to $\mathbb{Z}_d$

In this section, we recall how to represent every continuous function $f\colon \mathbb{Z}_d \to \mathbb{Z}_d$ by its van der Put series. For details when $d = p$ is prime, we refer the reader to Schikhof's book [36] and for needed facts about the ring of $d$-adic integers, we recommend [14, Section 4.2] and [26]. Here we relate the coefficients of these series to the vertices of the rooted $d$-ary tree, whose boundary is identified with $\mathbb{Z}_d$.

First, we recall that the ring of $d$-adic integers $\mathbb{Z}_d$ for arbitrary (not necessarily prime) $d$ is defined as the set of all formal sums

$$\mathbb{Z}_d = \{a_0 + a_1 d + a_2 d^2 + \cdots : a_i \in \{0, 1, \ldots, d-1\} = \mathbb{Z}/d\mathbb{Z}, i \geq 0\},$$

where addition and multiplication are defined in the same way as in $\mathbb{Z}_p$ for prime $p$ taking into account the carry over. Also, the ring $\mathbb{Q}_d$ of $d$-adic numbers can be defined as the full ring of fractions of $\mathbb{Z}_d$, but we only need to use elements of $\mathbb{Z}_d$ below. Algebraically, if $d = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ is the decomposition of $d$ into the product of primes, then

$$\mathbb{Z}_d = \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_k} \quad \text{and} \quad \mathbb{Q}_d = \mathbb{Q}_{p_1} \times \mathbb{Q}_{p_2} \times \cdots \times \mathbb{Q}_{p_k}.$$

As stated in the introduction, for the alphabet $X = \{0, 1, \ldots, d-1\}$, we identify $\mathbb{Z}_d$ with the boundary $X^\infty$ of the rooted $d$-ary regular tree $X^*$ in a natural way, viewing a $d$-adic number $x_0 + x_1 d + x_2 d^2 + \cdots$ as a point $x_0 x_1 x_2 \ldots \in X^\infty$. This identification gives rise to an embedding of $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ into $X^*$ via $n \mapsto [n]_d$, where $[n]_d$ denotes the word over $X$ representing the expansion of $n$ in base $d$ written backwards (so that, for example, $[6]_2 = 011$). There are two standard ways to define the image $[0]_d$ of

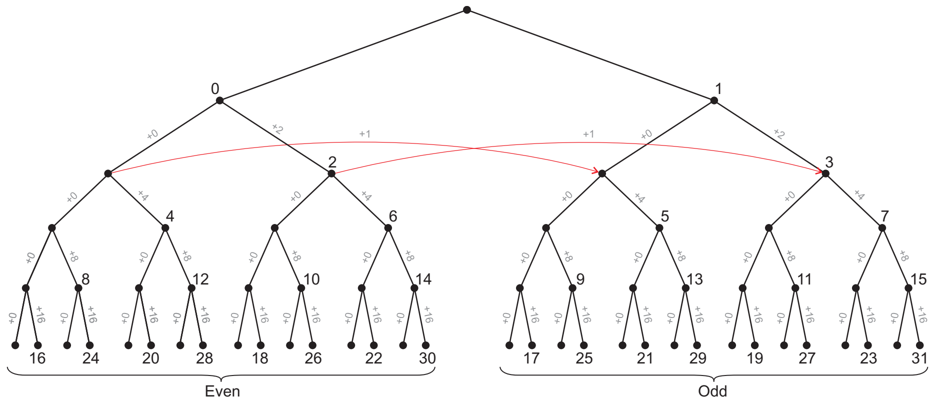


FIGURE 2. Labeling of vertices of a binary tree by elements of $\mathbb{N}_0$.

$0 \in \mathbb{N}_0$: one can define it to be either the empty word $\varepsilon$ over $X$ of length 0 or a word 0 of length 1. These two choices give rise later to two similar versions of the van der Put bases in the space of continuous functions from $\mathbb{Z}_d$ to $\mathbb{Z}_d$ that we call Mahler and Schikhof versions. Throughout the paper, we use Mahler's version and, unless otherwise stated, we define $[0]_d = 0$ (the word of length 1). However, we state some of the results for Schikhof's version as well. Note that the image of $\mathbb{N} \cup \{0\}$ consists of all vertices of $X^*$ that do not end with 0, and the vertex 0 itself. We call these vertices *labeled*. For example, the labeling of the binary tree is shown in Figure 2. The inverse of this embedding, with a slight abuse of notation as the notation does not explicitly mention $d$, we denote by bar $^{-}$. In other words, if $u = u_0 u_1 \dots u_n \in X^*$, then $\overline{u} = u_0 + u_1 d + \cdots + u_n d^n \in \mathbb{N}_0$. We note that the operation $u \mapsto \overline{u}$ is not injective as $\overline{u} = \overline{u0^k}$ for all $k \geq 0$.

Under this notation, we can also define for each $n \geq 0$ a cylindrical subset $[n]_d X^\infty \subset \mathbb{Z}_d$ that consists of all $d$-adic integers that have $[n]_d$ as a prefix. Geometrically, this set can be envisioned as the boundary of the subtree of $X^*$ hanging down from the vertex $[n]_d$.

For $n > 0$ with the $d$-ary expansion $n = x_0 + x_1 d + \cdots + x_k d^k$, $x_k \neq 0$, we define $n\_ = n - x_k d^k$. Geometrically, $n\_$ is the label of the labeled vertex in $X^*$ closest to $n$ along the unique path from $n$ to the root of the tree. For example, for $n = 22$, we have $[n]_2 = 01101$, so $[n\_]_2 = 011$ and $n\_ = 6$.

We are ready to define the decomposition of a continuous function $f : \mathbb{Z}_d \to \mathbb{Z}_d$ into a van der Put series. For each such function, there is a unique sequence $(B_n^f)_{n\geq 0}$, $B_n^f \in \mathbb{Z}_d$ of $d$-adic integers such that for each $x \in \mathbb{Z}_d$, the following expansion:

$$f(x) = \sum_{n\geq 0} B_n^f \chi_n(x) \tag{3-1}$$

holds, where $\chi_n(x)$ is the characteristic function of the cylindrical set $[n]_d X^\infty$ with values in $\mathbb{Z}_d$. The coefficients $B_n^f$ are called the *van der Put coefficients* of $f$ and are computed as follows:

$$B_n^f = \begin{cases} f(n) & \text{if } 0 \le n < d, \\ f(n) - f(n\_) & \text{if } n \ge d. \end{cases} \tag{3-2}$$

This is the decomposition with respect to the orthonormal van der Put basis $\{\chi_n(x)\colon n \ge 0\}$ of the space $C(\mathbb{Z}_d)$ of continuous functions from $\mathbb{Z}_d$ (as a $\mathbb{Z}_d$-module) to itself, as given in Mahler's book [28], and also used in [5]. In the literature, this basis is considered only when $d = p$ is a prime number, and is, in fact, an orthonormal basis of a larger space $C(\mathbb{Z}_p \to K)$ of continuous functions from $\mathbb{Z}_p$ to a normed field $K$ containing the field of $p$-adic rationals $\mathbb{Q}_p$. However, the given decomposition works in our context with all the proofs identical to the 'field' case.

To avoid possible confusion, we note that there is another standard version of the van der Put basis $\{\tilde{\chi}_n(x)\colon n \ge 0\}$ used, for example, in Schikhof's book [36]. We call this version of a basis Schikhof's version. In this basis, $\tilde{\chi}_n = \chi_n$ for $n > 0$, and $\tilde{\chi}_0$ is the characteristic function of the whole space $\mathbb{Z}_d$ (while $\chi_0$ is the characteristic function of $d\mathbb{Z}_d = 0X^\infty$). This difference corresponds to two ways of defining $[0]_d$ as mentioned earlier, since $\chi_n$ is defined as the characteristic function of $[n]_d X_\infty$. The definition of $\chi 0$ clearly depends on the choice we make for $[0]_d$. If $[0]_d = 0$, we obtain the version of basis used by Mahler, and defining $[0]_d = \varepsilon$ (the empty word) yields the basis used by Schikhof. This difference does not change much the results and the proofs, and we give formulations of some of our results for both bases. In particular, the decomposition Equation (3-1) is transformed into

$$f(x) = \sum_{n \ge 0} \tilde{B}_n^f \tilde{\chi}_n(x),$$

where Schikhof's versions of the van der Put coefficients $\tilde{B}_n^f$ are computed as

$$\tilde{B}_n^f = \begin{cases} f(0) & \text{if } n = 0, \\ f(n) - f(n\_) & \text{if } n > 0. \end{cases}$$

Among all continuous functions $\mathbb{Z}_d \to \mathbb{Z}_d$, we are interested in those that define endomorphisms of $X^*$ (viewed as a tree). We use the following useful characterization of these maps in terms of the coefficients of their van der Put series (which works for both versions of the van der Put basis). In the case of prime $d$, this easy fact is given in [5]. The proof in the general case is basically the same and we omit it.

THEOREM 3.1. *A function $\mathbb{Z}_d \to \mathbb{Z}_d$ is 1-Lipschitz if and only if it can be represented as*

$$f(x) = \sum_{n \ge 0} b_n^f d^{\lfloor \log_d n \rfloor} \chi_n(x), \tag{3-3}$$

*where $b_n^f \in \mathbb{Z}_d$ for all $n \ge 0$, and*

$$\lfloor \log_d n \rfloor = (\textit{the number of digits in the base-}d \textit{ expansion of } n) - 1.$$

https://doi.org/10.1017/S1446788722000027 Published online by Cambridge University Press

We call the coefficients $b_n^f$ from Theorem 3.1 the *reduced van der Put coefficients*. It follows from Equation (3-2) that these coefficients are computed as

$$b_n^f = B_n^f d^{-\lfloor \log_d n \rfloor} = \begin{cases} f(n) & \text{if } 0 \le n < d, \\ \dfrac{f(n) - f(n\_)}{d^{\lfloor \log_d n \rfloor}} & \text{if } n \ge d. \end{cases} \tag{3-4}$$

For Schikhof's version of the van der Put basis, Equation (3-3) has to be replaced with

$$f(x) = \sum_{n \ge 0} \tilde{b}_n^f d^{\lfloor \log_d n \rfloor} \chi_n(x)$$

and the corresponding reduced van der Put coefficients are computed as

$$\tilde{b}_n^f = \tilde{B}_n^f d^{-\lfloor \log_d n \rfloor} = \begin{cases} f(0) & \text{if } n = 0, \\ \dfrac{f(n) - f(n\_)}{d^{\lfloor \log_d n \rfloor}} & \text{if } n > 0. \end{cases}$$

In particular, $\tilde{b}_n^f = b_n^f$ for all $n \ge d$.

We note that since Schikhof's reduced van der Put coefficients $\tilde{b}_n^f$ differ from $b_n^f$ only for $n < d$, the claim of Theorem 1.1 clearly remains true for Schikhof's van der Put series as well.

## 4. Automatic sequences

There are several equivalent ways to define $d$-automatic sequences. We refer the reader to Allouche–Shallit's book [2] for details. Informally, a sequence $(a_n)_{n \ge 0}$ is called $d$-automatic if one can compute $a_n$ by feeding a deterministic finite automaton with output (DFAO) as the base-$d$ representation of $n$, and then applying the output mapping $\tau$ to the last state reached. We first recall the definition of the (Moore) DFAO and then give the formal definition of automatic sequences.

DEFINITION 4.1. A *deterministic finite automaton with output* (or a *Moore* automaton) is defined to be a 6-tuple

$$\mathcal{B} = (Q, X, \delta, q_0, A, \tau),$$

where

- $Q$ is a finite *set of states*;
- $X$ is the finite *input alphabet*;
- $\delta\colon Q \times X \to Q$ is the *transition function*;
- $q_0 \in Q$ is the *initial state*;
- $A$ is the *output alphabet*;
- $\tau\colon Q \to A$ is the *output function*.

https://doi.org/10.1017/S1446788722000027 Published online by Cambridge University Press

In the case when the input alphabet is $X = \{0, 1, \ldots, d-1\}$, we call the corresponding automaton a $d$-DFAO.

Similar to the case of Mealy automata, we extend the transition function $\delta$ to $\delta\colon Q \times X^* \to Q$. With this convention, a $d$-DFAO defines a function $f_M\colon X^* \to A$ by $f_M(w) = \tau(\delta(q_0, w))$.

Note that Moore automata can also be viewed as transducers as well by recording the values of the output function at every state while reading the input word. This way, each word over $X$ is transformed into a word over $A$ of the same length. This model of calculations is equivalent to Mealy automata (in the more general case when the output alphabet is allowed to be different from the input alphabet) in the sense that for each Moore automaton, there exists a Mealy automaton that defines the same transformation from $X^*$ to $A^*$ and *vice versa* (see [37] for details).

Recall that for a word $w = x_0x_1 \ldots x_n \in X^*$, we write $\overline{w} = x_0 + x_1d + \cdots + x_nd^n \in \mathbb{N}_0$ for the label of the labeled vertex in $X^*$ closest to $w$ along the unique path from $w$ to the root of the tree.

DEFINITION 4.2 [2]. We say that a sequence $(a_n)_{n\geq 0}$ over a finite alphabet $A$ is *$d$-automatic* if there exists a $d$-DFAO $\mathcal{B} = (Q, X, \delta, q_0, A, \tau)$ such that $a_n = \tau(\delta(q_0, w))$ for all $n \geq 0$ and $w \in X^*$ with $\overline{w} = n$.

For us, it is more convenient to use the alternative characterization of automatic sequences (for the proof, see for instance [2]).

THEOREM 4.3. *A sequence $(a_n)_{n\geq 0}$ over an alphabet $A$ is $d$ -automatic if and only if the collection of its subsequences of the form $\{(a_{j+n\cdot d^i})_{n\geq 0} \mid i \geq 0, 0 \leq j < d^i\}$, called the $d$-kernel, is finite.*

We recall the connection between the $d$-DFAO defining a $d$-automatic sequence $(a_n)_{n\geq 0}$ and the $d$-kernel of this sequence (see Theorem 6.6.2 in [2]). For that, we define the section of a sequence $(a_n)_{n\geq 0}$ at a word $v$ over $X = \{0, 1, \ldots, d-1\}$ recursively as follows.

DEFINITION 4.4. Let $(a_n)_{n\geq 0}$ be a sequence over alphabet $A$. Its *$d$-section* $(a_n)_{n\geq 0}|_x$ *at* $x \in X = \{0, 1, \ldots, d-1\}$ is a subsequence $(a_{x+nd})_{n\geq 0}$. For a word $v = x_1x_2 \ldots x_k$ over $X$, we further define the *$d$-section* $(a_n)_{n\geq 0}|_v$ *at* $v$ to be either $(a_n)_{n\geq 0}$ itself if $v$ is the empty word or $(a_n)_{n\geq 0}|_{x_1}|_{x_2} \cdots |_{x_k}$ otherwise.

We often omit $d$ in the term $d$-section when $d$ is clear from the context. The $d$-kernel of a sequence consists exactly of $d$-sections and the $d$-automaticity of a sequence can be reformulated as follows.

PROPOSITION 4.5. *A sequence $(a_n)_{n\geq 0}$ over an alphabet $A$ is $d$-automatic if and only if the set $\{(a_n)_{n\geq 0}|_v : v \in X^*\}$ is finite.*

The subsequences involved in the definition of the $d$-kernel can be plotted on the $d$-ary rooted tree $X^*$, where the vertex $v \in X^*$ is labeled with the subsequence $(a_n)|_v$. For $d = 2$, such a tree is shown in Figure 3.

https://doi.org/10.1017/S1446788722000027 Published online by Cambridge University Press

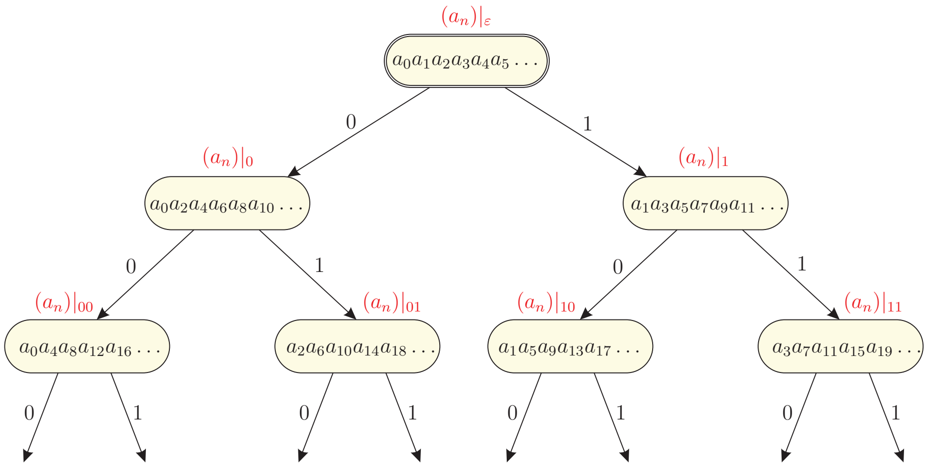


FIGURE 3. Tree of subsequences of $(a_n)_{n\geq 0}$ constituting its $d$-kernel (for $d = 2$).

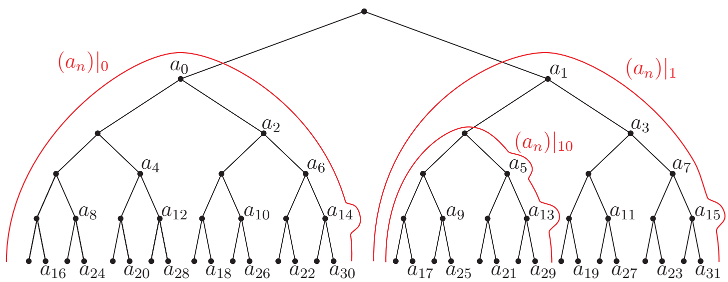


FIGURE 4. The 2-portrait of the sequence $(a_n)_{n\geq 0}$.

A convenient way to represent sections of a sequence and understand $d$-automaticity is to put the terms of this sequence on a $d$-ary tree. Recall that in the previous section, we have constructed an embedding of $\mathbb{N}_0$ into $X^*$ via $n \mapsto [n]_d$. Under this embedding, we call the image of $n \in \mathbb{N} \cup \{0\}$ the vertex $n$ of $X^*$.

DEFINITION 4.6. The *$d$-portrait* of a sequence $(a_n)_{n\geq 0}$ over an alphabet $A$ is a $d$-ary rooted tree $X^*$, where the vertex $n$ is labeled by $a_n$ and other vertices are unlabeled.

In other words, we label each vertex $v = x_0x_1 \ldots x_k$ with $x_k \neq 0$ or $v = 0$ by $a_{\overline{v}} = a_{x_0+x_1d+\cdots+x_kd^k}$. For example, Figure 4 represents the 2-portrait of the sequence $(a_n)_{n\geq 0}$.

To simplify the exposition, we write simply *portrait* for $d$-portrait when the value of $d$ is clear from the context. In particular, unless otherwise stated, $X$ denotes an alphabet $\{0, 1, \ldots, d-1\}$ of cardinality $d$ and a portrait means a $d$-portrait.

There is a simple connection between the portrait of a sequence and the portrait of its section at vertex $v \in X^*$ that takes into account that the subtree $vX^*$ of $X^*$ hanging down from vertex $v$ is canonically isomorphic to $X^*$ itself via $vu \leftrightarrow u$ for each $u \in X^*$.

https://doi.org/10.1017/S1446788722000027 Published online by Cambridge University Press

PROPOSITION 4.7. *For a sequence $(a_n)_{n\geq 0}$ over an alphabet $A$ with a portrait $P$ and a vertex $v = x_0x_1 \dots x_k$, $k \geq 0$ of $X^*$, the portrait of the section $(a_n)_{n\geq 0}|_v$ is obtained from the portrait of $(a_n)_{n\geq 0}$ by taking the (labeled) subtree of $P$ hanging down from vertex $v$, removing, if $v$ ends with $x_k \neq 0$ and $k > 0$, the label at its root vertex, and labeling the vertex 0 by $a_{\overline{v}} = a_{x_0+x_1d+\dots+x_kd^k}$, which is the label of the labeled vertex in $P$ closest to $v0$ on the unique path connecting $v0$ to the root.*

The proof of the above proposition follows immediately from the definitions of portrait and section.

In other words, as shown in Figure 4, you can see the portrait of a section of a sequence $(a_n)_{n\geq 0}$ at vertex $v \in X^*$ just by looking at the subtree hanging down in the portrait of $(a_n)_{n\geq 0}$ from vertex $v$ (modulo the minor technical issue of labeling the vertex 0 of this subtree and possibly removing the label of the root vertex). Therefore, a sequence is automatic if and only if its portrait has a finite number of 'subportraits' hanging down from its vertices. This way of interpreting automaticity now corresponds naturally to the condition of an automaton endomorphism being finite state.

Note that the formulation of the previous proposition would be simpler had we defined portraits by labeling each vertex $v = x_0x_1 \dots x_k$ of the tree by $a_{x_0+x_1d+\cdots x_kd^k}$ instead of only numbered ones, but we intentionally opt not to do that, to simplify our notation in the next section.

Now it is easy to see that the $d$-DFAO defining a $d$-automatic sequence $(a_n)_{n\geq 0}$ over an alphabet $A$ with the $d$-kernel $K$ can be built as follows.

PROPOSITION 4.8. *Suppose $(a_n)_{n\geq 0}$ is a $d$-automatic sequence over an alphabet $A$ with the $d$-kernel $K$. Then a $d$-DFAO $\mathcal{B} = (K, X, \delta, q_0, A, \tau)$, where*

$$\begin{aligned} \delta((a_n)_{n\geq 0}|_v, x) &= (a_n)_{n\geq 0}|_{vx}, \\ \tau((a_n)_{n\geq 0}|_v) &= a_{\overline{v}} \text{ (the first term of the sequence } (a_n)_{n\geq 0}|_v), \\ q_0 &= (a_n)_{n\geq 0}|_\varepsilon = (a_n)_{n\geq 0} \end{aligned} \tag{4-1}$$

*defines the sequence $(a_n)_{n\geq 0}$.*

Informally, we build the automaton $M$ by following the edges of the tree $X^*$ from the root, labeling these edges by the corresponding elements of $X$, and identifying the vertices that correspond to the same sections of $(a_n)_{n\geq 0}$ into one state of $M$ that is labeled by the 0 th term of the corresponding section.

## 5. Portraits of sequences of reduced van der Put coefficients and their sections

It turns out that there is a natural relation between the (portraits of the sequences of) reduced van der Put coefficients of an endomorphism $g$ and of its sections. Denote by $\sigma\colon \mathbb{Z}_d \to \mathbb{Z}_d$ the map $\sigma(a) = (a - (a \bmod d))/d$. This map corresponds to the shift map on $\mathbb{Z}_d$ that deletes the first letter of $a$. That is, if $a = x_0x_1x_2 \dots \in \mathbb{Z}_d$, then $\sigma(a) = x_1x_2x_3 \dots \in \mathbb{Z}_d$.

THEOREM 5.1. *Suppose $g \in \operatorname{End} X^*$ has sections $g|_x$, $x = 0, 1, \ldots, n-1$ at the vertices of the first level of $X^*$. Then the reduced van der Put coefficients $b_n^{g|_x}$ of the section $g|_x$ satisfy:*

$$b_n^{g|_x} = \begin{cases} \sigma(b_x^g) & n = 0, \\ b_{x+nd}^g + \sigma(b_x^g) & 0 < n < d, \\ b_{x+nd}^g & n \geq d, \end{cases} \tag{5-1}$$

*where for $b \in \mathbb{Z}_d$, we denote by $\sigma(b) = (b - (b \bmod d))/d$ the shift map on $\mathbb{Z}_d$.*

PROOF. First we consider the case $n = 0$. By Equation (3-4), the reduced van der Put coefficients are computed as follows:

$$b_0^{g|_x} = g|_x(0^\infty) = \frac{g(x0^\infty) - (g(x0^\infty) \bmod d)}{d} = \sigma(g(x0^\infty)) = \sigma(b_x^g).$$

Similarly for $0 < n < d$, we obtain

$$\begin{aligned} b_n^{g|_x} &= g|_x(n0^\infty) = \frac{g(xn0^\infty) - (g(xn0^\infty) \bmod d)}{d} \\ &= \frac{g(xn0^\infty) - (g(x0^\infty) \bmod d)}{d} + \frac{g(x0^\infty) - (g(xn0^\infty) \bmod d)}{d} \\ &= b_{x+nd}^g + \frac{g(x0^\infty) - (g(x0^\infty) \bmod d)}{d} = b_{x+nd}^g + \sigma(b_x^g). \end{aligned}$$

Finally, for $n > d$, we derive

$$\begin{aligned} b_n^{g|_x} &= d^{-\lfloor \log_d n \rfloor}(g|_x([n]_d 0^\infty) - g|_x([n\_]_d 0^\infty)) \\ &= d^{-\lfloor \log_d n \rfloor}\bigg( \frac{g(x[n]_d 0^\infty) - (g(x[n]_d 0^\infty) \bmod d)}{d} \\ &\qquad - \frac{g(x[n\_]_d 0^\infty) - (g(x[n\_]_d 0^\infty) \bmod d)}{d} \bigg) \\ &= d^{-\lfloor \log_d n \rfloor - 1}(g(x[n]_d 0^\infty) - g(x[n\_]_d 0^\infty)) \\ &= d^{-\lfloor \log_d (x+nd) \rfloor}(g([x+nd]_d 0^\infty) - g([(x+nd)\_]_d 0^\infty)) = b_{x+nd}^g, \end{aligned}$$

where in the last line, we used that for $x < d$, we have $x + (n\_)d = (x + nd)\_$ and

$$\lfloor \log_d(n) \rfloor + 1 = \lfloor \log_d(n) + 1 \rfloor = \lfloor \log_d(nd) \rfloor = \lfloor \log_d(x + nd) \rfloor. \qquad \square$$

In the case of Schikhof's version of the van der Put basis, we can similarly prove the following.

THEOREM 5.2. *Suppose $g \in \operatorname{End} X^*$ has sections $g|_x$, $x = 0, 1, \ldots, n-1$ at the vertices of the first level of $X^*$. Then the reduced van der Put coefficients with respect to*

https://doi.org/10.1017/S1446788722000027 Published online by Cambridge University Press

*Schikhof's version of the van der Put basis of the section $g|_x$ satisfy:*

$$\tilde{b}_n^{g|_x} = \begin{cases} ll\sigma(\tilde{b}_0^g) & n = 0, x = 0, \\ \sigma(\tilde{b}_x^g + b_0^g) & n = 0, 0 < x < d, \\ \tilde{b}_{x+nd}^g & n > 0. \end{cases}$$

There is a more visual way to state the third case in Equation (5-1) using the $^{\overline{\phantom{x}}}$ notation.

COROLLARY 5.3. *Let $x_0x_1\ldots x_k \in X^*$ be a word of length $k+1 \geq 3$ with $x_k \neq 0$. Then,*

$$b^g_{\overline{x_0x_1\ldots x_k}} = b^{g|_{x_0}}_{\overline{x_1\ldots x_k}}.$$

PROOF. Follows from Equation (5-1) and the fact that if $\overline{x_1x_2\ldots x_k} = n$, then $\overline{x_0x_1x_2\ldots x_k} = x_0 + nd$. □

The next corollary is used in the calculations in Section 8.

COROLLARY 5.4. *Let $v, w \in X^*$ with $w$ of length at least 2 and ending in a nonzero element of $X$. Then,*

$$b^g_{\overline{vw}} = b^{g|_v}_{\overline{w}}.$$

PROOF. When $v$ is the empty word, the claim is trivial. The general case now follows by induction on $|v|$ from Corollary 5.3 as for each $x \in X$, we have

$$b^g_{\overline{xvw}} = b^{g|_x}_{\overline{vw}} = b^{(g|_x)|_v}_{\overline{w}} = b^{g|_{xv}}_{\overline{w}}. \qquad \square$$

COROLLARY 5.5. *Let $g \in \mathrm{End}(X^*)$ be an endomorphism of $X^*$ and $v \in X^*$ be an arbitrary vertex. Then the sequences $(b_n^{g|_v})_{n\geq 0}$ and $(b_n^g)_{n\geq 0}|_v$ coincide starting from term $d$.*

PROOF. For any $n \geq d$, we have that $[n]_d = xw$ for some $x \in X$ and $w \in X^*$ of length at least 1 that ends with a nonzero element of $X$. So we have by Corollary 5.4,

$$b_n^{g|_v} = b^{g|_v}_{\overline{xw}} = b^g_{\overline{vxw}}.$$

However, $b^g_{\overline{vxw}}$ is exactly the term of the sequence $(b_n^g)_{n\geq 0}|_v$ with index $n = \overline{xw}$. □

Now, taking into account Proposition 4.7, there is a geometric way to look at the previous theorem. Namely, the third subcase in Equation (5-1) yields the following proposition.

COROLLARY 5.6. *Let $v \in X^*$ be an arbitrary vertex of $X^*$. The labels of the portrait of the sequence $(b_n^{g|_v})_{n\geq 0}$ coincide at levels 2 and below with the corresponding labels of the restriction of the portrait of $(b_n^g)_{n\geq 0}$ to the subtree hanging down from vertex $v \in X$.*

We illustrate by Figure 5 this fact for $v = x \in X$ of length one, where the portraits of $(b_n^{g|_0})_{n\geq 0}$ and $(b_n^{g|_1})_{n\geq 0}$ are drawn on the left and right subtrees of the portrait of $(b_n^g)_{n\geq 0}$. Figure 5 demonstrates that the labels of the portraits of sections coincide with the labels of the portrait of $(b_n^g)_{n\geq 0}$ below the dashed line. The first two subcases of Equation (5-1) give labels of the portraits of $(b_n^{g|_x})_{n\geq 0}, x \in X$ on the first level.

https://doi.org/10.1017/S1446788722000027 Published online by Cambridge University Press

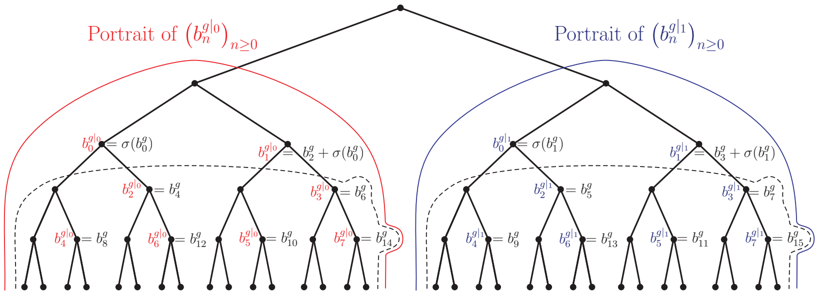


FIGURE 5. Correspondence between portraits of $(b_n^{g|x})_{n\geq 0}$ and $(b_n^g)_{n\geq 0}$.

## 6. Proof of the Theorem 1.1

In this section, we prove Theorem 1.1. In the arguments below, we work with eventually periodic elements of $\mathbb{Z}_d$, that is, elements of the form $a_0 + a_1 d + a_2 d^2 + \cdots$ with eventually periodic sequences $(a_i)_{i\geq 0}$ of coefficients. As shown in [14, Theorem 4.2.4], this set of $d$-adic integers can be identified with the subset $\mathbb{Z}_{d,0}$ of $\mathbb{Q}$ consisting of all rational numbers $a/b \in \mathbb{Q}$ such that $b$ is relatively prime to $d$. Algebraically, it can be defined as $\mathbb{Z}_{d,0} = D^{-1}\mathbb{Z}$, where $D$ is the multiplicative set $\{b \in \mathbb{Z} : \gcd(b, d) = 1\}$. We denote the corresponding inclusion $\mathbb{Z}_{d,0} \hookrightarrow \mathbb{Z}_d$ by $\psi$. The following inclusions then take place:

$$\begin{array}{ccccccc} \mathbb{Z} & \subset & \mathbb{Z}_{d,0} & \overset{\psi}{\hookrightarrow} & \mathbb{Z}_d & \subset & \mathbb{Q}_d \\ & & \cap & & & & \\ & & \mathbb{Q} & & & & \end{array}$$

We do not need the definition of $\psi$ which can be constructed using lemma 4.2.2 in [14], but rather need the definition of $\psi^{-1} : \psi(\mathbb{Z}_{d,0}) \to \mathbb{Z}_{d,0}$. The map is defined as follows. Suppose $uv^\infty \in \mathbb{Z}_d$ is an arbitrary eventually periodic element for some $u, v \in X^*$. Then we define

$$\psi^{-1}(uv^\infty) = \overline{u} + \frac{\overline{v} \cdot d^{|u|}}{1 - d^{|v|}} \in \mathbb{Z}_{d,0}.$$

LEMMA 6.1. *The preimage under $\psi$ of the set $\{v^\infty : v \in X^m\}$ of all periodic elements of $\mathbb{Z}_d$ whose periods have lengths dividing $m \geq 0$ is the set*

$$P^{0,m} = \left\{ \frac{j}{1 - d^m} : 0 \leq j < d^m \right\},$$

*which is a subset of the interval* $[-1, 0] \subset \mathbb{R}$.

PROOF. It follows from the definition of $\psi^{-1}$ that

$$\psi^{-1}(v^\infty) = \frac{\overline{v}}{1 - d^{|v|}}.$$

https://doi.org/10.1017/S1446788722000027 Published online by Cambridge University Press

Recall that for $v = x_0x_1 \dots x_{m-1}$, we have $\overline{v} = x_0 + x_1d + \cdots + x_{m-1}d^{m-1}$. This implies that $0 \le \overline{v} \le d^m - 1$ and, henceforth, $-1 \le \psi^{-1}(v^\infty) \le 0$. Moreover, as $v$ runs over all words in $X^m$, $\overline{v}$ runs over all integer numbers from 0 to $d^m - 1$ as we simply list the $d$-ary expansions of all these numbers. □

LEMMA 6.2. *The preimage under $\psi$ of the set $\{uv^\infty : u \in X^l, v \in X^m\}$ of all eventually periodic elements of $\mathbb{Z}_d$ with preperiods of length at most $l \ge 0$ and periods of lengths dividing $m \ge 1$ is the set*

$$P^{l,m} = \Big\{i + \frac{j \cdot d^l}{1 - d^m} : 0 \le i < d^l, 0 \le j < d^m\Big\},$$

*which is a subset of the interval $[-d^l, d^l - 1] \subset \mathbb{R}$.*

PROOF. We have

$$\begin{aligned}
\psi^{-1}(\{uv^\infty : u \in X^l, v \in X^m\}) &= \{\psi^{-1}(uv^\infty) : u \in X^l, v \in X^m\}\\
&= \{\psi^{-1}(u0^\infty) + \psi^{-1}(0^l v^\infty) : u \in X^l, v \in X^m\}\\
&= \{\overline{u} + d^l \cdot \psi^{-1}(v^\infty) : u \in X^l, v \in X^m\}\\
&= \{i + d^l\psi^{-1}(v^\infty) : 0 \le i < d^l, v \in X^m\} = \bigcup_{0 \le i < d^l} (i + d^l P^{0,m}).
\end{aligned}$$

The set $d^l P^{0,m}$ by Lemma 6.1 is a subset of $[-d^l, 0]$. Therefore, since $P^{l,m} \subset \mathbb{Q}$ is obtained as the union of all shifts of $d^l P^{0,m}$ by all integers $0 \le i < d^l$, we obtain that $P^{l,m} \subset [-d^l, d^l - 1]$. □

To obtain the condition of finiteness of Mealy automata in the proof of Theorem 1.1, we also need the following technical lemma. Define a sequence of subsets $A_i^{l,m}$ recursively by $A_0^{l,m} = P^{l,m}$, and

$$A_{i+1}^{l,m} = \sigma(A_i^{l,m}) + P^{l,m}. \tag{6-1}$$

$A_i^{l,m}$ is used later to describe the possible sets of states of an automaton defined by a transformation with a given automatic sequence of reduced van der Put coefficients.

LEMMA 6.3. *The set $A^{l,m} = \bigcup_{i \ge 0} A_i^{l,m}$ is finite.*

PROOF. First, we remark that the denominators of the fractions in $A_i^{l,m}$ are divisors of $d^m - 1$. Therefore, it is enough to prove by induction on $i$ that $A_i^{l,m} \subset [-z, z]$ for $z = (d^{l+1} + d - 1)/(d - 1)$. For $i = 0$, the statement is true since $A_0^{l,m} \subset [-d^l, d^l - 1]$ by Lemma 6.1, and

$$z = \frac{d^{l+1} + d - 1}{d - 1} > \frac{d^{l+1} + d - 1}{d} = d^l + \frac{d - 1}{d} > d^l.$$

Assume that the statement is true for a given $i \ge 0$. Any element of $A_{i+1}^{l,m}$ is equal to $\sigma(x) + b$ for some $x \in A_{i+1}^{l,m} \subset [-z, z]$ and $b \in P^{l,m} \subset [-d^l, d^l - 1]$. Since $\sigma(x) =$

https://doi.org/10.1017/S1446788722000027 Published online by Cambridge University Press

$(x - x \bmod d)/d$, we immediately obtain

$$\sigma(x) + b \le \frac{x}{d} + b \le \frac{z}{d} + d^l - 1 = \frac{(d^{l+1} + d - 1)}{d(d-1)} + d^l - 1$$
$$= \frac{d^l + 1 + (d^l - 1)(d-1)}{d-1} = \frac{d^{l+1} - d + 2}{d-1} < z.$$

For the lower bound, we obtain

$$\sigma(x) + b \ge \frac{x - d + 1}{d} + b \ge \frac{-z - d + 1}{d} - d^l = \frac{-\frac{d^{l+1}+d-1}{d-1} - d + 1}{d} - d^l$$
$$= \frac{-d^l - d + 1}{d-1} - d^l = -\frac{d^{l+1} + d - 1}{d-1} = -z. \qquad \square$$

We are ready to proceed to the main result of this section.

PROOF OF THEOREM 1.1. First, assume that $g \in \mathrm{End}(X^*)$ is defined by a finite Mealy automaton $\mathcal{A}$ with the set of states $Q$. To prove that $(b_n^g)_{n\ge 0}$ is automatic, by Proposition 4.5, we need to show that it has finitely many sections at vertices of $X^*$.

Assume that $v \in X^*$ is of length at least 2, $v = v'xy$ for some $v' \in X^*$ and $x, y \in X$. Then the section $(b_n^g)|_v$ is a sequence that can be completely identified by a pair

$$(b_{\overline{v}}^g, \sigma((b_n^g)|_v)), \tag{6-2}$$

where $b_{\overline{v}}^g$ is its zero term, and $\sigma((b_n^g)|_v)$ is the subsequence made of all other terms.

Since by Corollary 5.6

$$\sigma((b_n^g)|_v) = \sigma((b_n^g)|_{v'xy}) = \sigma((b_n^{g|_{v'}})|_{xy}),$$

the number of possible choices for the second component in Equation (6-2) is bounded above by $|Q| \cdot |X|^2$ (as we have $|Q|$ choices for $g|_{v'}$ and $|X|^2$ choices for $xy \in X^2$).

Further, if $\overline{v} < d$ (that is, $v = z0^k$ for some $z \in X$), then the number of choices for the first component $b_{\overline{v}}^g$ of Equation (6-2) is bounded above by $|Q| \cdot |X|$. Otherwise, $v' = v''x'y'$ for some $v'' \in X^*$, $x', y' \in X$ with $y' \ne 0$. In this case, $b_{\overline{v}}^g = b_{\overline{x'y'}}^{g|_{v''}}$, so the number of possible choices for $b_{\overline{v}}^g$ is again bounded above by $|Q| \cdot |X|^2$. Thus, the sequence $(b_n^g)_{n\ge 0}$ has finitely many sections.

To prove the first condition asserting that all $b_n^g$ are in $\mathbb{Z}_d \cap \mathbb{Q}$, or, equivalently, eventually periodic, it is enough to mention that by Equation (3-4) $b_n^g$ must be eventually periodic for $n \ge d$ as a shifted difference of two eventually periodic words $g(n) = g([n]_d 0^\infty)$ and $g(n\_) = g([n\_]_d 0^\infty)$. The latter two words are eventually periodic as they are the images of eventually periodic words $[n]_d 0^\infty$ and $[n\_]_d 0^\infty$ under a finite

https://doi.org/10.1017/S1446788722000027 Published online by Cambridge University Press

automaton transformation. A similar argument works for $n < d$, in which case there is no need to take a difference.

Now we prove the converse direction. Assume that for an endomorphism $g \in \mathrm{End}(X^*)$ of $X^*$, the sequence $(b_n^g)_{n\geq 0}$ is automatic and consists of eventually periodic elements of $\mathbb{Z}_d$. Then automaticity implies that $\{b_n^g : n \geq 0\}$ is finite as a set. Let $l$ be the maximal length among the preperiods of all $b_n^g$ and let $m$ be the least common multiple of the lengths of all periods of $b_n^g$. Then clearly $b_n^g \in \psi(P^{l,m})$ for all $n \geq 0$ by the definition of $P^{l,m}$ given in Lemma 6.2.

Our aim is to show that the set $\{g|_v : v \in X^*\}$ is finite. We show that there are only finitely many portraits $(b_n^{g|_v})_{n\geq 0}$. Let $v \in X^*$. By Corollary 5.6, the part of the portrait of $(b_n^{g|_v})_{n\geq 0}$ below level one coincides with the part below level one of the restriction of the portrait of $(b_n^g)_{n\geq 0}$ on the subtree hanging down from vertex $v$. However, according to Propositions 4.5 and 4.7, since $(b_n^g)_{n\geq 0}$ is automatic, there is only a finite number of such restrictions as the set of all sections $\{(b_n^g)|_v : v \in X^*\}$ is finite.

Hence, we only need to check that there is a finite number of choices for the van der Put coefficients of the first level of $g|_v$ for $v \in X^*$. To do that, we prove by induction on $|v|$ that $b_i^{g|_v} \in \psi(A_{|v|}^{l,m})$ for $0 \leq i < d$. The claim is trivial for $|v| = 0$ by definition of $A^{l,m}$ and the choice of $l$ and $m$. Assume that the claim is true for all words $v$ of length $k$, and let $vx$ be a word of length $k + 1$ for some $x \in X$. Then by assumption, $b_x^{g|_v} \in \psi(A_{|v|}^{l,m})$ and additionally $b_{x+d\cdot i}^{g|_v} \in P^{l,m}$ for $1 \leq i < d$, as these coefficients of $g$ on the second level of its portrait coincide with the corresponding coefficients of $g$. Now by Theorem 5.1, we obtain

$$b_i^{g|_{vx}} = b_i^{(g|_v)|_x} = \begin{cases} \sigma(b_x^{g|_v}) & i = 0, \\ b_{x+d\cdot i}^{g|_v} + \sigma(b_x^{g|_v}) & 0 < i < d. \end{cases}$$

In both cases, we get that $b_i^{g|_{vx}} \in A_{|vx|}^{l,m}$ by definition of $A_{|vx|}^{l,m}$ from Equation (6-1). Finally, Lemma 6.3 now guarantees that $g$ has finitely many sections and completes the proof. □

## 7. Mealy and Moore automata associated with an endomorphism of $X^*$

The above proof of Theorem 1.1 allows us to build algorithms that construct the Moore automaton of the automatic sequence of reduced van der Put coefficients of a transformation of $\mathbb{Z}_d$ defined by a finite state Mealy automaton, and *vice versa*.

We start from constructing the Moore automaton generating the sequence of reduced van der Put coefficients of an endomorphism $g$ from the finite Mealy automaton defining $g$.

THEOREM 7.1. *Let $g \in \mathrm{End}(X^*)$ be an endomorphism of $X^*$ defined by a finite initial Mealy automaton $\mathcal{A}$ with the set of states $Q_{\mathcal{A}} = \{g|_v : v \in X^*\}$. Let also $(b_n^g)_{n\geq 0}$ be the sequence of reduced van der Put coefficients of the map $\mathbb{Z}_d \to \mathbb{Z}_d$ induced by $g$. Then the Moore automaton $\mathcal{B} = (Q_{\mathcal{B}}, X, \delta, q, \mathbb{Z}_d, \tau)$, where*

https://doi.org/10.1017/S1446788722000027 Published online by Cambridge University Press

- *the set of states is* $Q_{\mathcal{B}} = \{(g|_v, (b^g_{\overline{vy}})_{y\in X})\colon v \in X^*\}$;
- *the transition and output functions are*

$$\begin{aligned}\delta((g|_v, (b^g_{\overline{vy}})_{y\in X}), x) &= (g|_{vx}, (b^g_{\overline{vxy}})_{y\in X}),\\ \tau((g|_v, (b^g_{\overline{vy}})_{y\in X})) &= b^g_{\overline{v}};\end{aligned} \tag{7-1}$$

- *the initial state is* $q = (g, (b^g_{\overline{y}})_{y\in X})$,

*is finite, and generates the sequence* $(b^g_n)_{n\geq 0}$.

PROOF. According to Proposition 4.8, one can construct an automaton $\mathcal{B}'$ generating $(b^g_n)_{n\geq 0}$ as follows. The states of $\mathcal{B}'$ are the sections of $(b^g_n)_{n\geq 0}$ at the vertices of $X^*$ (that is, the $d$-kernel of $(b^g_n)_{n\geq 0}$) with the initial state being the whole sequence $(b^g_n)_{n\geq 0}$, and transition and output functions defined by Equation (4-1). Let $v \in X^*$ be an arbitrary vertex. By Corollary 5.6, the labels of the portrait of $(b^g_n)_{n\geq 0}|_v$ at level 2 and below coincide with the corresponding labels of the portrait of $(b^{g|_v}_n)_{n\geq 0}$. Therefore, each state $(b^g_n)_{n\geq 0}|_v$ of $\mathcal{B}'$ can be completely defined by a pair, called the *label* of this state:

$$l((b^g_n)_{n\geq 0}|_v) = (g|_v, (b^g_{\overline{vy}})_{y\in X}), \tag{7-2}$$

where $(b^g_{\overline{vy}})_{y\in X}$ is the $d$-tuple of the first $d$ terms of $(b^g_n)_{n\geq 0}|_v$ that correspond to the labels of the first level of the portrait of this sequence. The first component of this pair defines the terms of $(b^{g|_v}_n)_{n\geq 0}$ at level 2 and below, and the second component consists of terms of the first level. It is possible that different labels define the same state of $\mathcal{B}'$, but clearly the automaton $\mathcal{B}$ from the statement of the theorem also generates $(b^g_n)_{n\geq 0}$ since its minimization coincides with $\mathcal{B}'$. Indeed, the set of states of $\mathcal{B}$ is the set of labels of states of $\mathcal{B}'$ and the transitions in $\mathcal{B}$ are obtained from the transitions in $\mathcal{B}'$ defined in Proposition 4.8, and the definition of labels.

Finally, the finiteness of $Q_{\mathcal{B}}$ follows from our proof of Theorem 1.1 since the set $\{g|_v\colon v \in X^*\}$ (coinciding with $Q_{\mathcal{A}}$) is finite, and the set $\{b^g_{\overline{vy}}\colon v \in X^*, y \in X\}$ is a subset of the finite set $\{b^{g'}_{\overline{w}}\colon g' \in Q_{\mathcal{A}}, w \in X \cup X^2\}$. □

For the algorithmic procedure that, given a finite state $g \in \mathrm{End}(X^*)$, constructs a Moore automaton generating the sequence $(b^g_n)_{n\geq 0}$ of its reduced van der Put coefficients, we need the following lemma.

LEMMA 7.2. *Given a finite state endomorphism* $g \in G$ *acting on* $X^*$ *with* $|X| = d$, *its first* $d^2$ *reduced van der Put coefficients* $b^g_{\overline{v}}$, $v \in X^*$ *of length at most* 2, *are eventually periodic elements of* $\mathbb{Z}_d$ *that can be algorithmically computed.*

PROOF. Suppose $g$ has $q$ states. If $\overline{v} = i < d$, then by definition, $b^g_i = g(i0^\infty)$ is the image of an eventually periodic word under a finite automaton transformation. Thus, it is also eventually periodic with the period of length at most $q$ and the preperiod of length at most $q+1$. Clearly, both the period and preperiod can be computed effectively. Further, if $d \leq \overline{v} < d^2$, then $v = xy$ for $x, y \in X$ with $y \neq 0$. In this case, $b^g_{\overline{v}} = (g(xy0^\infty) - g(x0^\infty))/d$ is eventually periodic as a shifted difference of two eventually

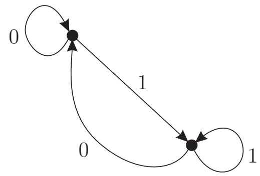


FIGURE 6. Underlying graph for Mealy automaton from Figure 1 and Moore automaton from Figure 8.

periodic words $g(xy0^\infty)$ and $g(x0^\infty)$. The latter two words are eventually periodic as they are the images of eventually periodic words $xy0^\infty$ and $x0^\infty$ under a finite automaton transformation that can be effectively computed. □

ALGORITHM 7.3 (construction of Moore automaton from Mealy automaton). Suppose an endomorphism $g$ of $X^*$ is defined by a finite state Mealy automaton A with the set of states $Q_{\mathrm{A}}$. To construct a Moore automaton B defining the sequence of reduced van der Put coefficients $(b^g_n)_{n\geq 0}$, complete the following steps.

Step 1. Compute $b^{g'}_{\overline{w}}$ for each $g' \in Q_{\mathrm{A}}$ and $w \in X \cup X^2$.
Step 2. Start building the set of states of B from its initial state $q = (g, (b^g_{\overline{y}})_{y\in X})$ with $\tau(q) = b^g_0$. Define $Q_0 = \{q\}$.
Step 3. To build $Q_{i+1}$ from $Q_i$ for $i \geq 1$, start from the empty set and for each state $q = (g|_v, (b^g_{\overline{vy}})_{y\in X}) \in Q_i$ and each $x \in X$, add the state $q_x = (g|_{vx}, (b^g_{\overline{vxy}})_{y\in X})$ to $Q_{i+1}$ unless it belongs to $Q_j$ for some $j \leq i$ or is already in $Q_{i+1}$. Use Corollary 5.4 to identify $b^g_{\overline{vxy}}$ with one of the elements computed in Step 1. Extend the transition function by $\delta(q, x) = q_x$ and the output function by $\tau(q_x) = b^g_{\overline{vx}}$.
Step 4. Repeat Step 3 until $Q_{i+1} = \emptyset$.
Step 5. The set of states of the Moore automaton B is $\bigcup_{i\geq 0} Q_i$, where the transition and output functions are defined in Step 3.

A particular connection between the constructed Moore automaton $\mathcal{B}$ and the original Mealy automaton $\mathcal{A}$ can be seen at the level of the underlying oriented graphs as explained below.

DEFINITION 7.4. For a Mealy automaton $\mathcal{A} = (Q, X, \delta, \lambda)$, we define its *underlying oriented graph* $\Gamma(\mathcal{A})$ to be the oriented labeled graph whose set of vertices is the set $Q$ of states of $\mathcal{A}$, and whose edges correspond to the transitions of $\mathcal{A}$ and are labeled by the input letters of the corresponding transitions. That is, there is an oriented edge from $q \in Q$ to $q' \in Q$ labeled by $x \in X$ if and only if $\delta(q, x) = q'$.

In other words, the underlying oriented graph of a Mealy automaton $\mathcal{A}$ can be obtained from the Moore diagram of $\mathcal{A}$ by removing the second components of the edge labels. For example, Figure 6 depicts the underlying graph of a Mealy automaton from Figure 1 generating the lamplighter group $\mathcal{L}$. Similarly, we construct underlying oriented graph of a Moore automaton.

https://doi.org/10.1017/S1446788722000027 Published online by Cambridge University Press

DEFINITION 7.5. For a Moore automaton $\mathcal{B} = (Q, X, \delta, q_0, A, \tau)$, we define its *underlying oriented graph* $\Gamma(\mathcal{B})$ to be the oriented labeled graph whose set of vertices is the set $Q$ of states of $\mathcal{B}$ and whose edges correspond to the transitions of $\mathcal{B}$ and are labeled by the input letters of the corresponding transitions. That is, there is an oriented edge from $q \in Q$ to $q' \in Q$ labeled by $x \in X$ if and only if $\delta(q, x) = q'$.

Figure 6 depicts also the underlying graph of a Moore automaton from Figure 8 generating the Thue–Morse sequence.

We finally define a *covering* of such oriented labeled graphs to be a surjective (both on vertices and edges) graph homomorphism that preserves the labels of the edges.

COROLLARY 7.6. *Let $g \in \mathrm{End}(X^*)$ be an endomorphism of $X^*$ defined by a finite Mealy automaton $\mathcal{A}$. Let also $(b_n^g)_{n\geq 0}$ be the (automatic) sequence of the reduced van der Put coefficients of a transformation $\mathbb{Z}_d \to \mathbb{Z}_d$ induced by $g$. Then the underlying oriented graph $\Gamma(\mathcal{B})$ of the Moore automaton $\mathcal{B}$ defining $(b_n^g)_{n\geq 0}$ obtained from $\mathcal{A}$ by Algorithm 7.3 covers the underlying oriented graph $\Gamma(\mathcal{A})$.*

PROOF. Since the transitions in the original Mealy automaton $\mathcal{A}$ defining $g$ are defined by $\delta(g|_v, x) = g|_{vx}$, we immediately get that the map from the set of vertices of the underlying oriented graph of $\mathcal{B}$ to the set of vertices of the underlying oriented graph of $\mathcal{A}$ defined by

$$(g|_v, (b^g_{\overline{vy}})_{y\in X}) \mapsto g|_v, v \in X^*$$

is a graph covering. □

Now we describe the procedure that constructs a Mealy automaton of an endomorphism defined by an automatic sequence generated by a given Moore automaton.

THEOREM 7.7. *Let $g \in \mathrm{End}(X^*)$ be an endomorphism of $X^*$ induced by a transformation of $\mathbb{Z}_d$ for which the sequence of reduced van der Put coefficients $(b_n^g)_{n\geq 0} \subset \mathbb{Z}_d$ is generated by a finite Moore automaton $\mathcal{B}$ with the set of states $Q_{\mathcal{B}} = \{(b_n^g)_{n\geq 0}|_v : v \in X^*\}$. Then the Mealy automaton $\mathcal{A} = (Q_{\mathcal{A}}, X, \delta, \lambda, q)$, where*

- *the set of states is $Q_{\mathcal{A}} = \{((b_n^g)_{n\geq 0}|_v, (b_i^{g|_v})_{i=0,1,\dots,d-1}) : v \in X^*\}$;*
- *the transition and output functions are*

$$\begin{aligned} \delta(((b_n^g)_{n\geq 0}|_v, (b_i^{g|_v})_{i=0,1,\dots,d-1}), x) &= ((b_n^g)_{n\geq 0}|_{vx}, (b_i^{g|_{vx}})_{i=0,1,\dots,d-1}), \\ \lambda(((b_n^g)_{n\geq 0}|_v, (b_i^{g|_v})_{i=0,1,\dots,d-1}), x) &= b_{\overline{x}}^{g|_v} \bmod d; \end{aligned} \tag{7-3}$$

- *the initial state is $q = ((b_n^g)_{n\geq 0}, (b_i^g)_{i=0,1,\dots,d-1})$,*

*is finite, and defines the endomorphism $g$.*

https://doi.org/10.1017/S1446788722000027 Published online by Cambridge University Press

PROOF. The initial Mealy automaton $\mathcal{A}'$ defining $g$ has set of states $Q' = \{g|_v : v \in X^*\}$, transition and output functions defined as

$$\delta'(g|_v, x) = g|_{vx},$$
$$\lambda'(g|_v, x) = g_v(x),$$

and the initial state $g = g|_\epsilon$.

Since each endomorphism of $X^*$ is uniquely defined by the sequence of its reduced van der Put coefficients, we can identify $Q'$ with the set

$$\{(b_n^{g|_v})_{n\geq 0} : v \in X^*\}.$$

By Corollary 5.5, the sequence $(b_n^{g|_v})_{n\geq 0}$ of the reduced van der Put coefficients that defines $g|_v$ coincides starting from term $d$ with $(b_n^g)_{n\geq 0}|_v$. Therefore, each state $g|_v$ of $\mathcal{A}'$ can be completely defined by a pair, called the *label* of this state:

$$l(g|_v) = ((b_n^g)_{n\geq 0}|_v, (b_i^{g|_v})_{i=0,1,\ldots,d-1}),$$

where $(b_i^{g|_v})_{i=0,1,\ldots,d-1}$ is the $d$-tuple of the first $d$ terms of $(b_n^{g|_v})_{n\geq 0}$ that corresponds to the labels of the first level of the portrait of this sequence. As in (7-2), the first component of this pair defines the terms of $(b_n^{g|_v})_{n\geq 0}$ at level 2 and below, and the second component consists of terms of the first level.

Similarly to the case of Theorem 7.1, it is possible that different labels define the same state of $\mathcal{A}'$, but clearly the automaton $\mathcal{A}$ from the statement of the theorem also generates $g$ since its minimization coincides with $\mathcal{A}'$. Indeed, the set of states of $\mathcal{A}$ is the set of labels of states of $\mathcal{A}'$ and the transition and output functions in $\mathcal{A}$ are obtained from the corresponding functions in $\mathcal{A}'$ and the definition of labels.

Finally, the finiteness of $Q$ follows from the above proof of Theorem 1.1 since the set $\{(b_n^g)_{n\geq 0}|_v : v \in X^*\}$ (coinciding with $Q_{\mathcal{B}}$) is finite, and the set $\{b_i^{g|_v} : v \in X^*, i = 0, 1, \ldots, d-1\}$ is finite as well, which follows from Lemma 6.3. □

We conclude with the description of the algorithm for building the Mealy automaton of an endomorphism of $X^*$ from a Moore automaton defining the sequence of its reduced van der Put coefficients.

ALGORITHM 7.8 (construction of Mealy automaton from Moore automaton). Let $g \in \mathrm{End}(X^*)$ be an endomorphism of $X^*$ induced by a transformation of $\mathbb{Z}_d$ for which the sequence of reduced van der Put coefficients $(b_n{}^g)_{n\geq 0}$, $b_n{}^g \in \mathbb{Z}_d$ is defined by a finite Moore automaton B with the set of states $Q_{\mathrm{B}} = \{(b_n{}^g)_{n\geq 0}|_v : v \in X^*\}$. To construct a Mealy automaton A $= (Q, X, \delta, \lambda, q)$ defining endomorphism $g$, complete the following steps.

Step 1. Start building the set of states of A from its initial state $q = ((b_n^g)_{n\geq 0}, (b_i^g)_{i=0,1,\ldots,d-1})$ with $\tau(q) = b_0{}^g$. Define $Q_0 = \{q\}$.

Step 2. To build $Q_{i+1}$ from $Q_i$ for $i \geq 1$, start from the empty set and for each state $q = ((b_n^g)_{n\geq 0}|_v, (b_i^{g|_v})_{i=0,1,\ldots,d-1}) \in Q_i$ and each $x \in X$, add state $q_x = ((b_n{}^g)_{n\geq 0}|_{vx}, (b_i{}^{g|_{vx}})_{i=0,\,1,\,\ldots,\,d-1})$ to $Q_{i+1}$ unless it belongs to $Q_j$ for some $j \leq i$ or is already

https://doi.org/10.1017/S1446788722000027 Published online by Cambridge University Press

in $Q_{i+1}$. Use the second case in Equation (5-1) to calculate $b_i^{g|_{vx}}$ from the coefficients $b_j^g$, which are the values of the output function of the given Moore automaton. Extend the transition function by $\delta(q, x) = q_x$ and the output function by $\lambda(q, x) = b_{x\subset}^{g|_v} \bmod d$.

Step 3. Repeat Step 2 until $Q_{i+1} = \varnothing$.

Step 4. The set of states of Mealy automaton A is $\bigcup_{i\geq 0} Q_i$, where the transition and output functions are defined in Step 2.

COROLLARY 7.9. *Let $g \in \mathrm{End}(X^*)$ be an endomorphism of $X^*$ induced by a selfmap of $\mathbb{Z}_d$ with the sequence of reduced van der Put coefficients defined by finite Moore automaton $\mathcal{B}$. Then the underlying oriented graph $\Gamma(\mathcal{A})$ of the Mealy automaton $\mathcal{A}$ obtained from $\mathcal{B}$ by Algorithm 7.8 covers the underlying oriented graph of $\mathcal{B}$.*

PROOF. Since the transitions in the original Moore automaton $\mathcal{B}$ defining $g$ are defined by $\delta((b_n^g)_{n\geq 0}|_v, x) = (b_n^g)_{n\geq 0}|_{vx}$, we immediately get that the map from the underlying oriented graph of $\mathcal{A}$ to the underlying oriented graph of $\mathcal{B}$ defined by

$$((b_n^g)_{n\geq 0}|_v, (b_i^{g|_v})_{i=0,1,\dots,d-1}) \mapsto (b_n^g)_{n\geq 0}|_v, v \in X^*$$

is a graph covering. □

## 8. Examples

**8.1. Moore automaton from Mealy automaton.** We first give an example of the construction of a Moore automaton from Mealy automaton. Consider the lamplighter group $\mathcal{L} = (\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}$ generated by the 2-state Mealy automaton $\mathcal{A}$ over the 2-letter alphabet $X = \{0, 1\}$ from [24] shown in Figure 1 and defined by the following wreath recursion:

$$p = (p, q)(01),$$
$$q = (p, q).$$

PROPOSITION 8.1. *The Moore automaton $\mathcal{B}_p$ generating the sequence of reduced van der Put coefficients of the transformation of $\mathbb{Z}_2$ induced by automorphism p is shown in Figure 7, where the initial state is on top, and the value of the output function $\tau$ of $\mathcal{B}_p$ at a given state is equal to the first component of the pair of d-adic integers in its label.*

PROOF. We apply Algorithm 7.3 and construct the sections of $(b_n^p)_{n\geq 0}$ at the vertices of $X^*$ in the form of (7-1). It may be useful to refer to Figure 7 to understand better the calculations that follow.

The label of the initial state $(b_n^p)_{n\geq 0}|_\varepsilon$ of $\mathcal{B}_p$ is $(p|_\varepsilon, (b_0^p, b_1^p))$. By (3-4), we get:

$$b_0^p = p(0^\infty) = 1^\infty \quad \text{and} \quad b_1^p = p(10^\infty) = 001^\infty.$$

https://doi.org/10.1017/S1446788722000027 Published online by Cambridge University Press

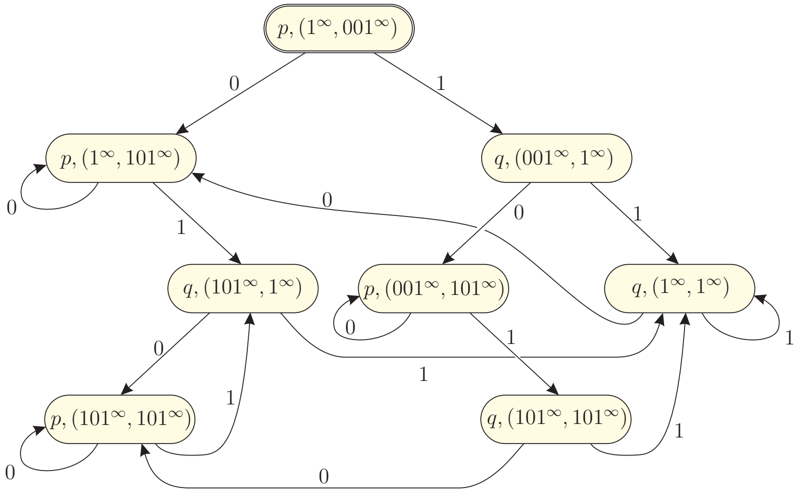


FIGURE 7. Moore automaton $\mathcal{B}_p$ generating the sequence $(b_n^p)_{n\geq 0}$ of reduced van der Put coefficients of the generator $p$ of the lamplighter group $\mathcal{L}$.

Therefore, the initial state of $\mathcal{B}_p$ is labeled by

$$l((b_n^p)_{n\geq 0}|_\varepsilon) = (p,(1^\infty,001^\infty)).$$

We proceed with the states corresponding to the vertices of the first level of $X^*$. We calculate:

$$b_2^p = \frac{p(010^\infty)-p(0^\infty)}{2} = \frac{1001^\infty - 1^\infty}{2} = 101^\infty,$$

$$b_3^p = \frac{p(110^\infty)-p(10^\infty)}{2} = \frac{0101^\infty - 001^\infty}{2} = 1^\infty.$$

Therefore, we get the labels of two more states in $\mathcal{B}_p$:

$$l((b_n^p)_{n\geq 0}|_0) = (p|_0,(b_0^p,b_2^p)) = (p,(1^\infty,101^\infty)),$$

$$l((b_n^p)_{n\geq 0}|_1) = (p|_1,(b_1^p,b_3^p)) = (q,(001^\infty,1^\infty)).$$

To obtain labels of the states at the vertices of deeper levels, we use Corollary 5.4. Namely, for $n>3$, we have that $[n]_2 = vx1 \in X^*$ for some $v\in X^*$ and $x\in X$. Therefore, by Corollary 5.4,

$$b_n^p = b^p_{\overline{vx1}} = b^{p|_v}_{\overline{x1}} = b^{p|_v}_{n \bmod 4}.$$

Therefore, it is enough to compute the first four values of $(b_n^{p|_v})_{n\geq 0}$ for all states $p|_v$ of an automaton $\mathcal{A}$. Since there are only two states in $\mathcal{A}$ and we have computed the first

https://doi.org/10.1017/S1446788722000027 Published online by Cambridge University Press

four values of $(b_n^p)_{n\geq 0}$, we proceed to $(b_n^p)_{n\geq 0}$:

$$\begin{aligned}
b_0^q &= q(0^\infty) = 01^\infty,\\
b_1^q &= q(10^\infty) = 101^\infty,\\
b_2^q &= \frac{q(010^\infty) - q(0^\infty)}{2} = \frac{0001^\infty - 01^\infty}{2} = 101^\infty,\\
b_3^q &= \frac{q(110^\infty) - q(10^\infty)}{2} = \frac{1101^\infty - 101^\infty}{2} = 1^\infty.
\end{aligned}$$

Now, by Corollary 5.5, we have that

$$\begin{aligned}
b_4^p &= b^p_{\overline{001}} = b^{p|_0}_{\overline{01}} = b^p_{\overline{01}} = b_2^p = 101^\infty,\\
b_6^p &= b^p_{\overline{011}} = b^{p|_0}_{\overline{11}} = b^p_{\overline{11}} = b_3^p = 1^\infty,\\
b_5^p &= b^p_{\overline{101}} = b^{p|_1}_{\overline{01}} = b^q_{\overline{01}} = b_2^q = 101^\infty,\\
b_7^p &= b^p_{\overline{111}} = b^{p|_1}_{\overline{11}} = b^q_{\overline{11}} = b_3^q = 1^\infty.
\end{aligned}$$

Thus, the states at the second level have the following labels:

$$\begin{aligned}
l((b_n^p)_{n\geq 0}|_{00}) &= (p|_{00}, (b^p_{\overline{000}}, b^p_{\overline{001}})) = (p, (b_0^p, b_4^p)) = (p, (1^\infty, 101^\infty)),\\
l((b_n^p)_{n\geq 0}|_{01}) &= (p|_{01}, (b^p_{\overline{010}}, b^p_{\overline{011}})) = (q, (b_2^p, b_6^p)) = (q, (101^\infty, 1^\infty)),\\
l((b_n^p)_{n\geq 0}|_{10}) &= (p|_{10}, (b^p_{\overline{100}}, b^p_{\overline{101}})) = (p, (b_1^p, b_5^p)) = (p, (001^\infty, 101^\infty)),\\
l((b_n^p)_{n\geq 0}|_{11}) &= (p|_{11}, (b^p_{\overline{110}}, b^p_{\overline{111}})) = (q, (b_3^p, b_7^p)) = (q, (1^\infty, 1^\infty)).
\end{aligned}$$

Since $l((b_n^p)_{n\geq 0}|_{00}) = l((b_n^p)_{n\geq 0}|_0)$, we can stop calculations along this branch. For other branches, we compute similarly on the next level. We start from branch 01:

$$l((b_n^p)_{n\geq 0}|_{010}) = (p|_{010}, (b^p_{\overline{0100}}, b^p_{\overline{0101}})) = (p, (b_2^p, b^{p|_{01}}_{\overline{01}})) = (p, (b_2^p, b_2^q)) = (p, (101^\infty, 101^\infty)),$$

and

$$\begin{aligned}
l((b_n^p)_{n\geq 0}|_{011}) &= (p|_{011}, (b^p_{\overline{0110}}, b^p_{\overline{0111}})) = (q, (b^{p|_0}_{\overline{11}}, b^{p|_{01}}_{\overline{11}}))\\
&= (q, (b_3^p, b_3^q)) = (q, (1^\infty, 1^\infty)) = l((b_n^p)_{n\geq 0}|_{11}).
\end{aligned}$$

For branch 10, we obtain

$$\begin{aligned}
l((b_n^p)_{n\geq 0}|_{100}) &= (p|_{100}, (b^p_{\overline{1000}}, b^p_{\overline{1001}})) = (p, (b_1^p, b^{p|_{10}}_{\overline{01}}))\\
&= (p, (b_1^p, b_2^p)) = (p, (001^\infty, 101^\infty)) = l((b_n^p)_{n\geq 0}|_{10})
\end{aligned}$$

and

$$l((b_n^p)_{n\geq 0}|_{101}) = (p|_{101}, (b^p_{\overline{1010}}, b^p_{\overline{1011}})) = (q, (b^{p|_1}_{\overline{01}}, b^{p|_{10}}_{\overline{11}})) = (q, (b_2^q, b_2^p)) = (q, (101^\infty, 101^\infty)).$$

For branch 11, we get

$$\begin{aligned} l((b_n^p)_{n\geq 0}|_{110}) &= (p|_{110}, (b^p_{\overline{1100}}, b^p_{\overline{1101}})) = (p, (b_3^p, b^{p|_{11}}_{\overline{01}})) \\ &= (p, (b_3^p, b_2^q)) = (p, (1^\infty, 101^\infty)) = l((b_n^p)_{n\geq 0}|_0) \end{aligned}$$

and

$$\begin{aligned} l((b_n^p)_{n\geq 0}|_{111}) &= (p|_{111}, (b^p_{\overline{1110}}, b^p_{\overline{1111}})) = (q, (b^{p|_1}_{\overline{11}}, b^{p|_{11}}_{\overline{11}})) \\ &= (q, (b_3^q, b_3^q)) = (q, (1^\infty, 1^\infty)) = l((b_n^p)_{n\geq 0}|_{11}). \end{aligned}$$

At this moment, we have two unfinished branches: 010 and 101. For 010, we have

$$\begin{aligned} l((b_n^p)_{n\geq 0}|_{0100}) &= (p|_{0100}, (b^p_{\overline{01000}}, b^p_{\overline{01001}})) = (p, (b_2^p, b^{p|_{010}}_{\overline{01}})) \\ &= (p, (b_2^p, b_2^p)) = (p, (101^\infty, 101^\infty)) = l((b_n^p)_{n\geq 0}|_{010}) \end{aligned}$$

and

$$\begin{aligned} l((b_n^p)_{n\geq 0}|_{0101}) &= (p|_{0101}, (b^p_{\overline{01010}}, b^p_{\overline{01011}})) = (q, (b^{p|_{01}}_{\overline{01}}, b^{p|_{010}}_{\overline{11}})) \\ &= (q, (b_2^q, b_3^p)) = (q, (101^\infty, 1^\infty)) = l((b_n^p)_{n\geq 0}|_{01}). \end{aligned}$$

Finally, for branch 101, we compute

$$\begin{aligned} l((b_n^p)_{n\geq 0}|_{1010}) &= (p|_{1010}, (b^p_{\overline{10100}}, b^p_{\overline{10101}})) = (p, (b^{p|_1}_{\overline{01}}, b^{p|_{101}}_{\overline{01}})) \\ &= (p, (b_2^q, b_2^q)) = (p, (101^\infty, 101^\infty)) = l((b_n^p)_{n\geq 0}|_{010}) \end{aligned}$$

and

$$\begin{aligned} l((b_n^p)_{n\geq 0}|_{1011}) &= (p|_{1011}, (b^p_{\overline{10110}}, b^p_{\overline{10111}})) = (q, (b^{p|_{10}}_{\overline{11}}, b^{p|_{101}}_{\overline{11}})) \\ &= (q, (b_3^p, b_3^q)) = (q, (1^\infty, 1^\infty)) = l((b_n^p)_{n\geq 0}|_{11}). \end{aligned}$$

We have completed all the branches and constructed all the transitions in the automaton $\mathcal{B}_p$. □

**8.2. Mealy automaton from Moore automaton.** In this subsection, we provide an example of the converse construction. Namely, we construct the finite state endomorphism of $\{0, 1\}^*$ that induces a transformation of $\mathbb{Z}_2$ with the Thue–Morse sequence of reduced van der Put coefficients, where we treat 0 as $0^\infty$ and 1 as $10^\infty$ according to the standard embedding of $\mathbb{Z}$ into $\mathbb{Z}_2$.

Recall that the Thue–Morse sequence $(t_n)_{n\geq 0}$ is the binary sequence defined by a Moore automaton shown in Figure 8. It can be obtained by starting with 0 and successively appending the Boolean complement of the sequence obtained thus far. The first 32 values of this sequence are shown in Table 1.

PROPOSITION 8.2. *The endomorphism $t$ of $X^*$ inducing a transformation of $\mathbb{Z}_2$ with the Thue–Morse sequence $(b_n^t)_{n\geq 0} = (t_n)_{n\geq 0}$ of the reduced van der Put coefficients is defined by the 2-state Mealy automaton $\mathcal{A}_t$ shown in Figure 9 with the following wreath*

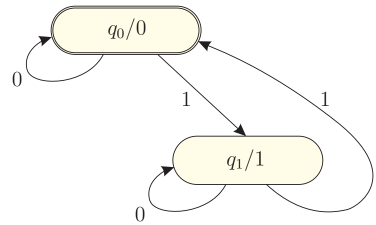


FIGURE 8. Moore automaton $\mathcal{B}$ generating the Thue–Morse sequence.

TABLE 1. First 32 values of the Thue–Morse sequence.

| $n$ | $[n]_2$ | $t_n$ | $n$ | $[n]_2$ | $t_n$ | $n$ | $[n]_2$ | $t_n$ | $n$ | $[n]_2$ | $t_n$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 8 | 0001 | 1 | 16 | 00001 | 1 | 24 | 00011 | 0 |
| 1 | 1 | 1 | 9 | 1001 | 0 | 17 | 10001 | 0 | 25 | 10011 | 1 |
| 2 | 01 | 1 | 10 | 0101 | 0 | 18 | 01001 | 0 | 26 | 01011 | 1 |
| 3 | 11 | 0 | 11 | 1101 | 1 | 19 | 11001 | 1 | 27 | 11011 | 0 |
| 4 | 001 | 1 | 12 | 0011 | 0 | 20 | 00101 | 0 | 28 | 00111 | 1 |
| 5 | 101 | 0 | 13 | 1011 | 1 | 21 | 10101 | 1 | 29 | 10111 | 0 |
| 6 | 011 | 0 | 14 | 0111 | 1 | 22 | 01101 | 1 | 30 | 01111 | 0 |
| 7 | 111 | 1 | 15 | 1111 | 0 | 23 | 11101 | 0 | 31 | 11111 | 1 |

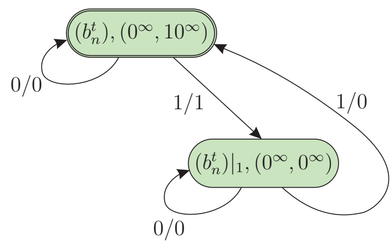


FIGURE 9. Mealy automaton $\mathcal{A}_t$ defining a transformation of $\mathbb{Z}_2$ whose sequence of reduced van der Put coefficients is the Thue–Morse sequence.

*recursion:*

$$t = (t, s),$$
$$s = (s, t)\begin{pmatrix} 01 \\ 00 \end{pmatrix},$$

*where* $\binom{01}{00}$ *denotes the selfmap of* $\{0, 1\}$ *sending both of its elements to* 0.

PROOF. We follow Algorithm 7.8, according to which the states of $\mathcal{A}_t$ are the pairs of the form

$$l(t|_v) = ((b_n^t)_{n\geq 0}|_v, (b_0^{t|_v}, b_1^{t|_v})).$$

https://doi.org/10.1017/S1446788722000027 Published online by Cambridge University Press

Below we suppress the subscript $n \geq 0$ in the notation for sequences to simplify the exposition. For example, we write simply $(b^t_n)$ for $(b^t_n)_{n\geq 0}$.

The initial state $t$ has a label

$$l(t) = l(t|_\varepsilon) = ((b^t_n), (b^t_0, b^t_1)) = ((b^t_n), (0^\infty, 10^\infty)).$$

We proceed to calculate the labels of the sections at the vertices of the first level. Using Theorem 5.1 (namely, the first two cases in Equation (5-1)) and the values $b^t_n = t_n$ of the Thue–Morse sequence from Table 1, we obtain:

$$\begin{aligned} l(t|_0) &= ((b^t_n)|_0, (b^{t|_0}_0, b^{t|_0}_1)) = ((b^t_n), (\sigma(b^t_0), b^t_2 + \sigma(b^t_0))) \\ &= ((b^t_n), (\sigma(0^\infty), 10^\infty + \sigma(0^\infty))) = ((b^t_n), (0^\infty, 10^\infty)) = l(t). \end{aligned}$$

We also use above the fact that $(b^t_n)|_0 = (b^t_n)$, which follows from the structure of automaton $\mathcal{B}$. Therefore, we can stop developing the branch that starts with 0 and move to the branch starting from 1. Similarly, we get

$$\begin{aligned} l(t|_1) &= ((b^t_n)|_1, (b^{t|_1}_0, b^{t|_1}_1)) = ((b^t_n)|_1, (\sigma(b^t_1), b^t_3 + \sigma(b^t_1))) \\ &= ((b^t_n)|_1, (\sigma(10^\infty), 0^\infty + \sigma(10^\infty))) = ((b^t_n)|_1, (0^\infty, 0^\infty)), \end{aligned} \tag{8-1}$$

so we obtain a new section. We compute the sections at the vertices of the second level using Figure 5, keeping in mind that according to Equation (8-1), $b^{t|_1}_0 = 0^\infty$:

$$\begin{aligned} l(t|_{10}) &= ((b^t_n)|_{10}, (b^{t|_{10}}_0, b^{t|_{10}}_1)) = ((b^t_n)|_1, (b^{(t|_1)|_0}_0, b^{(t|_1)|_0}_1)) \\ &= ((b^t_n)|_1, (\sigma(b^{t|_1}_0), b^{t|_1}_2 + \sigma(b^{t|_1}_0))) = ((b^t_n)|_1, (\sigma(0^\infty), b^t_5 + \sigma(0^\infty))) \\ &= ((b^t_n)|_1, (0^\infty, 0^\infty + 0^\infty)) = ((b^t_n)|_1, (0^\infty, 0^\infty)) = l(t|_1). \end{aligned}$$

Finally, since according to Equation (8-1) $b^{t|_1}_1 = 0^\infty$, we calculate the last section at 11:

$$\begin{aligned} l(t|_{11}) &= ((b^t_n)|_{11}, (b^{t|_{11}}_0, b^{t|_{11}}_1)) = ((b^t_n), (b^{(t|_1)|_1}_0, b^{(t|_1)|_1}_1)) \\ &= ((b^t_n), (\sigma(b^{t|_1}_1), b^{t|_1}_3 + \sigma(b^{t|_1}_1))) = ((b^t_n), (\sigma(0^\infty), b^t_7 + \sigma(0^\infty))) \\ &= ((b^t_n), (0^\infty, 10^\infty + 0^\infty)) = ((b^t_n), (0^\infty, 10^\infty)) = l(t). \end{aligned}$$

We have completed all the branches and constructed all the transitions in the automaton $\mathcal{A}_t$. We only need now to compute the values of the output function. By Equation (7-3), we get

$$\begin{aligned} \lambda(((b^t_n), (0^\infty, 10^\infty)), 0) &= 0^\infty \bmod 2 = 0, \\ \lambda(((b^t_n), (0^\infty, 10^\infty)), 1) &= 10^\infty \bmod 2 = 1, \\ \lambda(((b^t_n)|_1, (0^\infty, 0^\infty)), 0) &= 0^\infty \bmod 2 = 0, \\ \lambda(((b^t_n)|_1, (0^\infty, 0^\infty)), 1) &= 0^\infty \bmod 2 = 0, \end{aligned}$$

which completes the proof of the proposition. □

https://doi.org/10.1017/S1446788722000027 Published online by Cambridge University Press

## Acknowledgements

The authors are thankful to Zoran Šuníc and Svetlana Katok for enlightening conversations on the subject of the paper. The work on this project was partially conducted during the authors' visits to the American Institute of Mathematics SQuaRE program; they thank the institute for their hospitality and support. Finally, the authors are grateful to the anonymous referee for useful suggestions that improved the quality of the paper.

## References

[1] E. Ahmed and D. Savchuk, 'Endomorphisms of regular rooted trees induced by the action of polynomials on the ring $\mathbb{Z}_d$ of $d$-adic integers', *J. Algebra Appl.* **19** (2020), 2050154.
[2] J.-P. Allouche and J. Shallit, *Automatic Sequences: Theory, Applications, Generalizations* (Cambridge University Press, Cambridge, 2003).
[3] V. Anashin, 'Ergodic transformations in the space of $p$-adic integers', in: *p-Adic Mathematical Physics*, AIP Conference Proceedings, 826 (eds. Yu. Khrennikov, Z. Rakić and I.Volovich) (American Institute of Physics, Melville, NY, 2006), 3–24.
[4] V. Anashin, 'Automata finiteness criterion in terms of van der Put series of automata functions', *p-Adic Numbers Ultrametric Anal. Appl.* **4**(2) (2012), 151–160.
[5] V. S. Anashin, A. Y. Khrennikov and E. I. Yurova, 'Characterization of ergodic $p$-adic dynamical systems in terms of the van der Put basis', *Dokl. Akad. Nauk* **438**(2) (2011), 151–153 [English translation: *Dokl. Math.* **83**(3) (2011), 306–308].
[6] L. Bartholdi, R. Grigorchuk and V. Nekrashevych, 'From fractal groups to fractal sets', in: *Fractals in Graz 2001*, Trends in Mathematics (eds P. Grabner and W. Woess) (Birkhäuser, Basel, 2003), 25–118.
[7] L. Bartholdi and R. I. Grigorchuk, 'On the spectrum of Hecke type operators related to some fractal groups', *Tr. Mat. Inst. Steklova* **231**(Din. Sist., Avtom. i Beskon. Gruppy) (2000), 5–45.
[8] L. I. Bartholdi and V. V. Nekrashevych, 'Thurston equivalence of topological polynomials', *Acta Math.* **197**(1) (2006), 1–51.
[9] L. I. Bartholdi and Z. Šunik, 'Some solvable automaton groups', in: *Topological and Asymptotic Aspects of Group Theory*, Contemporary Mathematics, 394 (eds. R. Grigorchuk, M. Mihalik, M. Sapir and Z. Šunik) (American Mathematical Society, Providence, RI, 2006), 11–29.
[10] D. J. Bernstein and J. C. Lagarias, 'The $3x + 1$ conjugacy map', *Canad. J. Math.* **48**(6) (1996), 1154–1169.
[11] A. J. Cain, 'Automaton semigroups', *Theoret. Comput. Sci.* **410**(47–49) (2009), 5022–5038.
[12] P. Cull and I. Nelson, 'Error-correcting codes on the towers of Hanoi graphs', *Discrete Math.* **208/209** (1999), 157–175. Combinatorics (Assisi, 1996).
[13] M. Garzon and Y. Zalcstein, 'The complexity of Grigorchuk groups with application to cryptography,' *Theoret. Comput. Sci.* **88**(1) (1991), 83–98.
[14] M. Goresky and A. Klapper, *Algebraic Shift Register Sequences* (Cambridge University Press, Cambridge, 2012).
[15] R. Grigorchuk, D. Lenz and T. Nagnibeda, 'Spectra of Schreier graphs of Grigorchuk's group and Schroedinger operators with aperiodic order', *Math. Ann.* **370**(3–4) (2018), 1607–1637.
[16] R. Grigorchuk, Y. Leonov, V. Nekrashevych and V. Sushchansky, 'Self-similar groups, automatic sequences, and unitriangular representations', *Bull. Math. Sci.* **6**(2) (2016), 231–285.
[17] R. Grigorchuk and Z. Šunić, 'Self-similarity and branching in group theory', in: *Groups St. Andrews 2005, I*, London Mathematical Society Lecture Note Series, 339 (eds. C. M. Campbell,

https://doi.org/10.1017/S1446788722000027 Published online by Cambridge University Press

M. R. Quick, E. F. Robertson and G. C. Smith) (Cambridge University Press, Cambridge, 2007), 36–95.

[18] R. Grigorchuk and Z. Šunić, 'Schreier spectrum of the Hanoi Towers group on three pegs', in: *Analysis on Graphs and Its Applications*, Proceedings of Symposia in Pure Mathematics, 77 (eds P. Exner, J. Keating, P. Kuchment, T. Sunada and A. Teplyaev) (American Mathematical Society, Providence, RI, 2008), 183–198.

[19] R. Grigorchuk and Z. Šunik̀, 'Asymptotic aspects of Schreier graphs and Hanoi Towers groups', *C. R. Math. Acad. Sci. Paris* **342**(8) (2006), 545–550.

[20] R. I. Grigorchuk, 'On Burnside's problem on periodic groups', *Funktsional. Anal. i Prilozhen.* **14**(1) (1980), 53–54.

[21] R. I. Grigorchuk, 'On the Milnor problem of group growth', *Dokl. Akad. Nauk SSSR* **271**(1) (1983), 30–33.

[22] R. I. Grigorchuk, P. Linnell, T. Schick and A. Żuk, 'On a question of Atiyah', *C. R. Acad. Sci. Paris Sér. I Math.* **331**(9) (2000), 663–668.

[23] R. I. Grigorchuk, V. V. Nekrashevich and V. I. Sushchanskiĭ, 'Automata, dynamical systems, and groups', *Tr. Mat. Inst. Steklova* **231**(Din. Sist., Avtom. i Beskon. Gruppy) (2000), 134–214.

[24] R. I. Grigorchuk and A. Żuk, 'The lamplighter group as a group generated by a 2-state automaton, and its spectrum', *Geom. Dedicata* **87**(1–3) (2001), 209–244.

[25] R. I. Grigorchuk and A. Żuk, 'On a torsion-free weakly branch group defined by a three state automaton', *Internat. J. Algebra Comput.* **12**(1–2) (2002), 223–246.

[26] S. Katok, *p-Adic Analysis Compared with Real*, Student Mathematical Library, 37 (American Mathematical Society, Providence, RI; Mathematics Advanced Study Semesters, University Park, PA, 2007).

[27] M. V. Larin, 'Transitive polynomial transformations of residue rings', *Diskret. Mat.* **14**(2) (2002), 20–32.

[28] K. Mahler, *p-Adic Numbers and Their Functions*, 2nd edn, Cambridge Tracts in Mathematics, 76 (Cambridge University Press, Cambridge–New York, 1981).

[29] A. Miasnikov and D. Savchuk, 'An example of an automatic graph of intermediate growth', *Ann. Pure Appl. Logic* **166**(10) (2015), 1037–1048.

[30] A. Miasnikov and Z. Šunić, 'Cayley graph automatic groups are not necessarily Cayley graph biautomatic', in: *Language and Automata Theory and Applications*, Lecture Notes in Computer Science, 7183 (eds A.-H. Dediu and C. Martín-Vide) (Springer, Heidelberg, 2012), 401–407.

[31] A. Myasnikov, V. Shpilrain and A. Ushakov, *Non-Commutative Cryptography and Complexity of Group-Theoretic Problems*, Mathematical Surveys and Monographs, 177 (American Mathematical Society, Providence, RI, 2011). With an appendix by Natalia Mosina.

[32] A. G. Myasnikov and A. Ushakov, 'Random subgroups and analysis of the length-based and quotient attacks', *J. Math. Cryptol.* **2**(1) (2008), 29–61.

[33] V. Nekrashevych, *Self-Similar Groups*, Mathematical Surveys and Monographs, 117 (American Mathematical Society, Providence, RI, 2005).

[34] V. Nekrashevych and S. Sidki, 'Automorphisms of the binary tree: state-closed subgroups and dynamics of 1/2-endomorphisms', in: *Groups: Topological, Combinatorial and Arithmetic Aspects*, London Mathematical Society Lecture Note Series, 311 (ed. T. Müller) (Cambridge University Press, Cambridge, 2004), 375–404.

[35] G. Petrides, 'Cryptanalysis of the public key cryptosystem based on the word problem on the Grigorchuk groups', in: *Cryptography and Coding*, Lecture Notes in Computer Science, 2898 (ed. K. Paterson) (Springer, Berlin, 2003), 234–244.

[36] W. H. Schikhof. *Ultrametric Calculus: An Introduction to p-Adic Analysis*, Cambridge Studies in Advanced Mathematics, 4 (Cambridge University Press, Cambridge, 1984).

[37] L. A. Sholomov, *Foundations of the Theory of Discrete Logical and Computational Devices* (in Russian) (Nauka, Moscow, 1980).

[38] J. L. Walsh, 'A closed set of normal orthogonal functions', *Amer. J. Math.* **45**(1) (1923), 5–24.

ROSTISLAV GRIGORCHUK, Department of Mathematics, Texas A&M University,
College Station, TX 77843-3368, USA
e-mail: grigorch@math.tamu.edu

DMYTRO SAVCHUK, Department of Mathematics and Statistics,
University of South Florida, 4202 E Fowler Ave, Tampa, FL 33620-5700, USA
e-mail: savchuk@usf.edu