October 2018

Groups Generated by Automata Arising from Transformations of the Boundaries of Rooted Trees

Elsayed Ahmed
University of South Florida, sayed.mathematics@gmail.com

Groups Generated by Automata Arising from Transformations of the Boundaries of Rooted Trees

by

Elsayed Ahmed

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
Department of Mathematics and Statistics
College of Arts and Sciences
University of South Florida

Major Professor: Dmytro Savchuk, Ph.D.
Chairman: Paul Rosen, Ph.D.
Nataša Jonoska, Ph.D.
Jean-François Biasse, Ph.D.
Milé Krajčevski, Ph.D.

Date of Approval:
October 5, 2018

Keywords: Mealy Automata, Ergodicity, Permutational Polynomials, Lamplighter Group, Bireversible Automata

Dedication

To my wife Zeinab and my little son Saad

Acknowledgments

I would like to express my deep gratitude to my advisor Dr. Dmytro Savchuk for his great help and guidance. But for him, I would not have been able to come up with this dissertation. I am lucky to have him as my advisor. I am also indebted to Dr. Nataša Jonoska, Dr. Jean-François Biasse and Dr. Milé Krajčevski for their willingness to serve on my supervisory committee

Table of Contents

List of Figures

Abstract

In this dissertation we study groups of automorphisms of rooted trees arising from the transformations of the boundaries of these trees. The boundary of every regular rooted tree can be endowed with various algebraic structures. The transformations of these algebraic structures under certain conditions induce endomorphisms or automorphisms of the tree itself that can be described using the language of Mealy automata. This connection can be used to study boundary transformations using the properties of the induced endomorphisms, or vice versa.

We concentrate on two ways to interpret the boundary of the rooted d-regular tree. In the first approach discussed in detail in Chapter 3 we treat it as the ring $\mathbb{Z}_d$ of d-adic integers. This is achieved by naturally identifying the n^{th} level of the rooted d-ary tree with the ring $\mathbb{Z}/(d^n\mathbb{Z})$. Under this interpretation we study transformations of $\mathbb{Z}_d$ induced by polynomials in $\mathbb{Z}[x]$. We show that they always induce endomorphisms of the tree, completely describe these endomorphisms using the language of automata and show that all of their sections are again induced by polynomials in $\mathbb{Z}[x]$ of the same degree. In the case of permutational polynomials acting on $\mathbb{Z}_d$ by bijections the induced endomorphisms are automorphisms of the tree. For $d = 2$ such polynomials were completely characterized by Rivest in [Riv01]. As our main application we utilize the result of Rivest to derive the conditions on the coefficients of a permutational polynomial $f(x) \in \mathbb{Z}[x]$ that are necessary and sufficient for f to induce a level transitive automorphism of the binary tree, which is equivalent to the ergodicity of the action of $f(x)$ on $\mathbb{Z}_2$ with respect to the normalized Haar measure. Such polynomials have applications in cryptography and are used in certain generators of random numbers.

In the second approach, to be discussed in Chapter 4, we treat the boundary of the rooted binary tree as the ring $(\mathbb{Z}/2\mathbb{Z})[[t]]$ of formal power series over $\mathbb{Z}/2\mathbb{Z}$. This view allowed us to completely describe the structure of a certain group generated by a 4-state 2-letter bireversible automaton. Namely, we show that it is isomorphic to the lamplighter group $(\mathbb{Z}/2\mathbb{Z})^2 \wr \mathbb{Z}$ of rank two. We show that the action of the generators of this group on the boundary of the tree can be induced by affine transformations of $(\mathbb{Z}/2\mathbb{Z})[[t]]$. To our best knowledge, this is the first realization of the rank 2 lamplighter group by a bireversible automaton.

Chapter 1
Introduction

1.1 Groups Generated by Automata

The first appearance of groups generated by automata goes back to the beginning of 1960's [Glu61, Hoř63] but it took more than 20 years to realize their importance and utility. Now this is a rich theory with connections to holomorphic dynamics [Nek05], combinatorics [GŠ06], analysis [GLSŻ00], dynamical systems [GS16], computer science [MS15], and many other areas. We refer the reader to the survey article [GNS00] for history and references.

It was not until the 1970's and the beginning of the 1980's that the first influential results of this theory came up when it was shown in [Ale72, Sus79, Gri80, GS83] that automaton groups provide examples of finitely generated infinite torsion groups. This made a contribution to one of the most famous problems in algebra, namely the General Burnside Problem. This problem was first solved by E.S. Golod in [Gol64] using the Golod-Shafarevich theorem.

There are actually two other versions of Burnside problem. The first, which was also originally introduced by Burnside, is the bounded Burnside problem. It asks for the existence of infinite finitely generated groups of bounded exponent (a group has bounded exponent n if g^n is trivial for all elements g of the group). This problem merely reduces to the question of finiteness of free Burnside groups $B(m, n)$ with m generators and exponent n. The problem was positively solved by Novikov and Adian [NA68, NA68, NA68]. Namely, they have shown that $B(m, n)$ is infinite for any odd $n \geq 4381$ and $m > 1$. Later Adian in [Adi79] improved the bound for n to 665. The question for the even exponent remained open until Ivanov [Iva94] and Lysenok [Lys96] obtained independently proofs for exponents

$\geq 2^{48}$ and ≥ 8000 correspondingly.

The third version of Burnside problem is called the restricted Burnside problem which asks if there is, for any given m and n, an m-generated finite group with exponent n of maximal order. Obviously if the free Burnside group $B(m,n)$ is finite, this group would be such a maximal group. Unfortunately this is not always the case as mentioned above. For prime exponents Kostrikin in 1950s answered this question affirmatively. The complete positive solution of the restricted Burnside problem was obtained by Zelmanov [Zel91b,Zel90,Zel91a]. For more information on the three versions of the problem, we refer the reader to [Adi79, Gol68, Gup89, Kos90, Zel91b, GL02]).

Indeed, the possible relation of groups generated by automata to the General Burnside problem was first suggested by Glushkov in [Glu61, p.46]. Investigating the methods used to study the properties of the examples from [Ale72, Sus79, Gri80], we can see that they are quite different. For example, the methods used in [Ale72] are typical for the theory of finite automata. The exposition in [Sus79] is based on Kaloujnine's tableaux which comes from his theory of iterated wreath products of cyclic groups of prime order p. The approach in [Gri80] is mainly based on the notions of self-similarity and contraction (The contraction property here means that the length of the elements contracts by a factor bounded away from 1 when one passes to sections). An essential tool introduced in the beginning of the 1980's was the language of actions on rooted trees which was first suggested by Gupta and Sidki in [GS83]. It tremendously helped in bringing geometric insight to the subject.

The importance of automaton groups was again emphasized when it was shown that some of these groups provided the first examples of groups of intermediate growth [Gri83, Gri84, Gri85]. This answered the question of J.Milnor [Mil68] about the existence of such groups as well as M. Day's problem [Day57] on the existence of amenable but not elementary amenable groups. So far all known examples of groups of intermediate growth and non-elementary amenable groups are based on automaton groups or groups acting on trees.

In this dissertation we will study endomorphisms of rooted trees arising from transformations of the boundaries of those trees. Using the theory of automaton groups, we can

describe the action of such endomorphisms. Before we go on, we briefly introduce the structure of rooted trees and their boundaries and give different views to look at their vertices and elements. The set of vertices of a rooted d-ary tree can be naturally identified with the set X^* of all finite words over an alphabet $X = \{0, 1, \ldots, d-1\}$. The boundary of the tree consisting of all infinite paths without backtracking initiating at the root, which is usually denoted by X^∞, can be interpreted in many ways. Different ways of looking at X^∞ lead to different approaches to study its transformations and automorphisms of the tree X^* induced by these transformations.

One way to proceed is to give the n-th level of X^* the structure of $\mathbb{Z}/(d^n\mathbb{Z})$ by identifying $x_0x_1\ldots x_{n-1} \in X^n$ with $x_0 + d \cdot x_1 + \cdots + d^{n-1} \cdot x_{n-1} \in \mathbb{Z}/(d^n\mathbb{Z})$. The boundary of X^* is then identified with the ring $\mathbb{Z}_d$ of d-adic integers. So every 1-Lipschitz mapping f over $\mathbb{Z}_d$ (the boundary of X^*) naturally induces a well-defined mapping $f_k = f \pmod{d^k}$ of the residue ring $\mathbb{Z}/(d^n\mathbb{Z})$ (the n^{th} level of X^*) by letting $f_k(x) = f(x) \pmod{d^k}$. In [Ana02] Anashin showed that a 1-Lipschitz function on $\mathbb{Z}_p$ (for a prime p) is measure-preserving (or, accordingly, ergodic) if and only if it is bijective (accordingly, transitive) modulo p^k for all $k = 1, 2, 3, \ldots$. This result is a restatement of Theorem 6.5 in [GNS00] in the language of transformations of p-adic integers.

The boundary X^∞ can also be interpreted as the ring $(\mathbb{Z}/d\mathbb{Z})[[t]]$ of formal power series over $\mathbb{Z}/d\mathbb{Z}$. Each infinite word $a_0a_1a_2\ldots \in X^\infty$ can be represented as an element $a_0 + a_1t + \cdots + a_it^i + \cdots$ of $(\mathbb{Z}/d\mathbb{Z})[[t]]$. It was shown in [SS16] that affine transformations of $(\mathbb{Z}/d\mathbb{Z})[[t]]$ induce automorphisms of X^*. Another approach to identify the boundary X^* that will be also used in this dissertation is to interpret it as an infinite dimensional free $(\mathbb{Z}/d\mathbb{Z})$-module $(\mathbb{Z}/d\mathbb{Z})^\infty$ (which is a vector space over $\mathbb{Z}/d\mathbb{Z}$ in the case of prime d).

1.2 Action of Polynomials over $\mathbb{Z}$ on the Rooted Trees

For a fixed integer $d \geq 2$ every polynomial $f(x) \in \mathbb{Z}[x]$ naturally induces mappings $f_n \colon \mathbb{Z}/(d^n\mathbb{Z}) \to \mathbb{Z}/(d^n\mathbb{Z})$ for all positive integers n. Equivalently, these mappings are induced by the action of f on the ring of d-adic integers $\mathbb{Z}_d$. These two equivalent approaches

to study polynomials in $\mathbb{Z}[x]$ have been used in different contexts during the last several decades. One of the first motivations came from the constructions of the generators for pseudo-random sequences and goes back to Knuth [Knu81, Ana98, Lar02a]. In this and most of the other applications it is crucial to consider polynomials acting by permutations on $\mathbb{Z}/(d^n\mathbb{Z})$. Such polynomials are generally called permutational polynomials, however it is important to emphasize the distinction of these polynomials from the class of permutation polynomials that permute elements of finite fields $\mathbb{F}_{p^n}$ (see [LN83, Chapter 7] for a survey). In many cases a stronger condition of transitivity of this action is required. Another type of applications come from cryptography. Rivest in [Riv01] completely characterized polynomials that act by permutations on $\mathbb{Z}/(2^n\mathbb{Z})$ for all $n \geq 1$ and pointed out the use of one of them (namely, $f(x) = 2x^2 + x$) in the symmetric block cipher RC6 [RRSY] that was one of the five finalists of the AES competition. The questions of ergodicity of the action of permutational polynomials have been studied in the context of dynamical systems on $\mathbb{Z}_p$ by Anashin [Ana06]. We refer the reader to a nice survey paper [Fan15] for a background and history in polynomial dynamics on $\mathbb{Z}/(d^n\mathbb{Z})$.

In this dissertation (Chapter 3), we offer another view on the polynomials acting on $\mathbb{Z}_d$ and on $\mathbb{Z}/(d^n\mathbb{Z})$. Namely, we use the tools from the theory of groups acting on rooted trees by automorphisms and groups generated by Mealy automata. The key idea in many of the arguments in this theory is understanding automorphisms of rooted trees by describing their *sections* (terms *states* and *restrictions* are also widely used) at the subtrees hanging down from vertices of the original rooted tree. If the original tree was regular (i.e., every vertex has the same number of children), these subtrees are canonically isomorphic to the original tree, and these sections can be treated as the automorphisms of the original tree as well. We utilize this approach to analyze the action of polynomials on $\mathbb{Z}_d$.

Note that the connection between the functions on the boundary of the tree induced by automata and 1-Lipschitz functions on $\mathbb{Z}_d$ was also established by Anashin in [Ana12], where a criterion for finiteness of the corresponding automaton in terms of the van der Put series of the function was developed. This criterion provided an application of the p-adic analysis

to the theory of automata. Here we suggest a converse application.

Identifying the n-th level of X^* with $\mathbb{Z}/(d^n\mathbb{Z})$ and the boundary of X^* with the ring $\mathbb{Z}_d$ of d-adic integers as discussed in Section 3.2, we show in Proposition 3.2.1 that each polynomial in $\mathbb{Z}[x]$ induces an endomorphism of the tree X^*, while each permutational polynomial induces an automorphism. Our first result describes the structure of these endomorphisms.

Theorem 3.2.3. Given a polynomial $f(x) = a_0 + a_1x + \cdots + a_tx^t \in \mathbb{Z}[x]$ inducing an endomorphism of X^*, the image of a vertex $x_0 \in X$ under f is $f(x_0) \pmod d$ and the section of f at x_0 is again induced by a polynomial given by the equation:

$$f|_{x_0}(x) = \Big(f(x_0) \text{ div } d\Big) + \sum_{i=1}^{t} \frac{f^{(i)}(x_0)}{i!} d^{i-1}x^i,$$

where $f^{(i)}$ denotes the i^{th} derivative of a polynomial f, and $f(x_0)$ div d is the quotient of $f(x_0)$ and d.

Note that the case of linear polynomials was partially considered by Bartholdi and Šuníc in [BŠ06].

Our main application here deals with permutational polynomials acting transitively on $\mathbb{Z}/(2^n\mathbb{Z})$ for all n. In terms of the action on the tree this condition is equivalent to being level transitive. Equivalently, $f \in \mathbb{Z}[x]$ induces a level transitive automorphism if and only if the corresponding dynamical system $(\mathbb{Z}_2, f)$ is minimal (i.e., the orbit of each element of $\mathbb{Z}_2$ under f is dense in $\mathbb{Z}_2$), or ergodic with respect to the Haar measure on $\mathbb{Z}_2$ (coinciding with the uniform Bernoulli measure on $\mathbb{Z}_2$ viewed as a Cantor set) [GNS00, Proposition 6.5], [Ana06].

In order to state our main result, we first review the history of the problem. The following theorem proved by Larin in [Lar02a] gives the conditions that f has to satisfy in order to be transitive mod 2^n for each positive integer n.

Theorem 3.3.10 ([Lar02a])**.** A polynomial $f(x) = a_0 + a_1x + \cdots + a_tx^t \in \mathbb{Z}[x]$ is transitive mod 2^n for every positive integer n if and only if it satisfies the following conditions:

(i) $a_0 \equiv 1 \pmod 2$

(ii) $a_1 \equiv 1 \pmod 2$

(iii) $a_3 + a_5 + a_7 + \cdots \equiv 2a_2 \pmod 4$

(iv) $a_4 + a_6 + a_8 + \cdots \equiv a_1 + a_2 - 1 \pmod 4$

Rivest in [Riv01] (see an alternative proof in [MŠG10]) derived the following conditions that are necessary and sufficient for a polynomial $f \in \mathbb{Z}[x]$ to induce a permutation of each level of $\{0,1\}^*$ and hence an automorphism of the tree.

Theorem 3.2.11 ([Riv01])**.** A polynomial $f(x) = a_0 + a_1x + \cdots + a_tx^t$ in $\mathbb{Z}[x]$ induces a permutation of $\mathbb{Z}/(2^n\mathbb{Z})$ for each positive integer n if and only if it satisfies the following conditions:

(i) $a_1 \equiv 1 \pmod 2$

(ii) $a_2 + a_4 + a_6 + \cdots \equiv 0 \pmod 2$

(iii) $a_3 + a_5 + a_7 + \cdots \equiv 0 \pmod 2$

Using Theorem 3.2.3 we study level transitivity of a permutational polynomial f by counting the number of nontrivial actions of the sections of f in each level. In [BOERT96, Proposition (4.6)], it was shown that f acts level transitively on the rooted binary tree if and only if the number of nontrivial actions of the sections of f in each level of $\{0,1\}^*$ is odd. Using this fact, we determine the conditions that f has to meet in order to be level transitive. These conditions are summarized in the following theorem which is the main result of Chapter 3.

Theorem 3.3.9. Let $f(x) = a_0 + a_1x + \cdots + a_tx^t$ be a permutational polynomial acting on the rooted binary tree. Then this action is level transitive if and only if the following conditions hold:

(i) $a_0 \equiv 1 \pmod 2$

(ii) $2a_2 \equiv a_3 + a_5 + \cdots \pmod 4$

(iii) $a_2 + a_1 - 1 \equiv a_4 + a_6 + \cdots \pmod 4$

Combining the conditions of Theorems 3.2.11 and 3.3.9, we obtain the conditions of Theorem 3.3.10 using a completely different approach.

1.3 Lamplighter Groups Arising as Automaton Groups

The lamplighter group and its generalizations have been studied extensively during the last several decades. The simplest lamplighter group $\mathcal{L} = \mathcal{L}_{1,2}$ is defined as the restricted wreath product $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}$ or, equivalently, as $\oplus_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}$, where $\mathbb{Z}$ acts on $\oplus_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z})$ by shifting the index. More generally, higher rank lamplighter groups $\mathcal{L}_{n,d}$ are defined similarly as $(\mathbb{Z}/d\mathbb{Z})^n \wr \mathbb{Z}$.

All of the groups in this class are metabelian groups of exponential growth that, despite seemingly simple algebraic structure, possess extraordinary properties, connect different areas of mathematics, and serve as counterexamples to several conjectures. To start with, this is one of the simplest examples of finitely generated but not finitely presented groups.

Especially fruitful from historical perspective was the discovery that the lamplighter group (of rank 1) $\mathcal{L}$ is one of the 6 nonisomorphic groups generated by 2-state 2-letter invertible Mealy automata [GNS00]. Every group generated by a d-letter automaton naturally acts on the regular d-ary tree, whose set of vertices can be identified with the set X^* of all finite words over a d-letter alphabet $X = \{0, 1, \ldots, d-1\}$ as we mentioned earlier. The automaton realization of $\mathcal{L}$ has eventually led to the construction of counterexamples to various versions of Atiyah conjecture on l^2-Betti numbers [Ati76] in [GLSŻ00, DS02, Aus13, LW13, Gra14] and more recently [Gra16]. The striking property of $\mathcal{L}$ behind the first construction in [GLSŻ00] is that the spectrum of the Laplace operator on the Cayley graph of $\mathcal{L}$ (with respect to a special system of generators) is pure point spectrum [GŻ01], which was obtained via the action of $\mathcal{L}$ on the boundary X^∞ of the rooted binary tree X^* induced by its automaton realization.

The lamplighter type groups play also an important role in the theory of random walks on groups [KmV83, LPP96, PSC02, BTZ17]. The subgroup structure of $\mathcal{L}_{n,p}$ was explicitly described by Grigorchuk and Kravchenko in [GK14]. Further, the lamplighter groups happen to be one of the first examples of scale-invariant groups that are not virtually nilpotent [NP11], thus giving a counterexample to a conjecture by Benjamini. Here by scale-invariant group we mean finitely generated infinite group G that possess a nested sequence of finite index

subgroups G_n that are all isomorphic to G and whose intersection is a finite group. And again, the automaton realization of lamplighter groups played an important role in this construction. In particular, it is proved in [GS14] that each self-replicating automaton group acting essentially freely on the boundary of a tree (i.e., in such a way that for every nontrivial element of the group the measure of the fixed point set of this element under the action of the group on the boundary of the rooted tree is zero) is scale-invariant. Many lamplighter type groups happen to act essentially freely on the boundary.

Below we survey some of a history of generating lamplighter type groups by automata. But before proceeding, we first informally recall the classes of reversible and bireversible automata (the formal treatment is given in Section 2.2). For every invertible n-state m-letter automaton $\mathcal{A}$ one can define an m-state n-letter *dual* automaton $\partial\mathcal{A}$ by "swapping the roles" of letters of the alphabet and the states of an automaton. I.e., there is a transition $q \xrightarrow{x/y} w$ in $\mathcal{A}$ for states q, w of $\mathcal{A}$ and letters x, y from the alphabet if and only if there is a transition $x \xrightarrow{q/w} y$ in $\partial\mathcal{A}$. An automaton $\mathcal{A}$ is called *reversible* if its dual $\partial\mathcal{A}$ is invertible, and it is called *bireversible* if $\mathcal{A}$, ∂A and $\partial(A^{-1})$ are all invertible. Bireversible automata constitute a very interesting class. The groups that they generate are often hard to analyze by the standard methods based on various contraction properties. For example, several families of bireversible automata studied in [GM05, VV07, VV10, SVV11, SV11] generate free nonabelian groups or free products of finite number of copies of $\mathbb{Z}/2\mathbb{Z}$. But the proof behind the main break through construction in [VV07] that answered 20 year old question by Sidki is rather technical and involved.

In Chapter 4 we will prove the following theorem. Indeed this is the main result of this chapter.

Theorem 4.4.12. The group $\mathcal{G} = \langle a = (b, d)\sigma, b = (d, b)\sigma, c = (a, c), d = (c, a)\rangle$ is generated by a 4-state 2-letter bireversible automaton (depicted in Figure 13) and is isomorphic to the rank 2 lamplighter group $\mathcal{L}_{2,2} \cong (\mathbb{Z}/2\mathbb{Z})^2 \wr \mathbb{Z}$.

With the result above in mind, we proceed to surveying the history of the topic to motivate our interest in the group $\mathcal{G}$. After the original realization of $\mathcal{L}_{1,2}$ in [GNS00, GŻ01] by a 2-

state 2-letter automaton, Silva and Steinberg in [SS05] have constructed a family of n^d-state n^d-letter reset automata generating $\mathcal{L}_{n,d}$. Thus, the group $\mathcal{L}_{2,2}$ in this family is generated by 4-state 4-letter automaton.

In [BŠ06] Bartholdi and Šuníc have constructed a large family of lamplighter groups $\mathcal{L}_{n,p}$ parametrized by monic polynomials over $\mathbb{Z}_p$ that are invertible in the ring $\mathbb{Z}_p[[t]]$ of formal power series over $\mathbb{Z}_p$. There are two automata in this family generating $\mathcal{L}_{2,2}$: these automata correspond to polynomials t^2+t+1 and t^2+1. Both of these automata are 4-state 2-letter automata, but none of them is bireversible (however, their inverses are reversible). Another reincarnation of $\mathcal{L}_{2,2}$ was discovered in [GS14], where it was shown that a 3-state 2-letter automaton (not reversible) generates an index 2 extension of $\mathcal{L}_{2,2}$.

The first examples of bireversible automata generating lamplighter type groups were constructed in [BDR16] and [SS16]. Bondarenko, D'Angeli, and Rodaro in [BDR16] presented a 3-state 3-letter self-dual bireversible automaton generating $\mathcal{L}_{1,3} \cong \mathbb{Z}_3 \wr \mathbb{Z}$. The second automaton was a 4-state 2-letter automaton generating an index 2 extension of $\mathcal{L}_{2,2}$. It appeared as the main example in the paper by Sidki and the second author [SS16] whose main goal was to understand the action of lamplighter type groups on rooted trees. In a very recent preprint [SS18] Skipper and Steinberg, using affine transformations of power series rings with coefficients in a finite commutative ring, have constructed families of bireversible automata generating $A \wr \mathbb{Z}$ for a finite abelian group A such that the 2-Sylow subgroup of A has no multiplicity one summands in its expression as a direct sum of cyclic groups of order a power of 2.

In most cases when lamplighter group is generated by finite automaton acting on a binary tree, the base group $\oplus_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z})$, which is generated by infinite number of commuting involutions, consists of spherically homogeneous automorphisms (an automorphism in called spherically homogeneous provided that for each level its states at the vertices of this level all coincide). Thus the whole group usually lies in the normalizer of the group $\mathrm{SHAut}(X^*)$ of all spherically homogeneous automorphisms inside the group $\mathrm{Aut}(X^*)$ of all automorphisms of X^*. It was shown in [SS16] that this normalizer consists of affine automorphisms of X^*

coming from the affine actions on the boundary X^∞ of the tree viewed as uncountable infinite dimensional vector space over $\mathbb{Z}/2\mathbb{Z}$. Moreover, it was shown that every realization of lamplighter group as an automaton group acting on the binary tree is conjugate to the one coming from affine actions. The group $\mathcal{G}$ is not an exception, but it turns out that elements of $\mathcal{G}$ sit in a more narrow class of automorphisms induced by the affine transformations of the boundary of X^* viewed as the ring $(\mathbb{Z}/2\mathbb{Z})[[t]]$. For $f, g \in (\mathbb{Z}/2\mathbb{Z})[[t]]$ let $\tau_{f,g}$ denote the automorphism of the X^* sending $h(t)$ to $h(t)\cdot f(t)+g(t)$. The group of all such automorphisms is denoted by $\mathrm{Aff}_{[[t]]}(X^*)$.

Theorem 4.4.4. The generators a, b, c and d of $\mathcal{G}$ all lie in $\mathrm{Aff}_{[[t]]}(X^*)$ and are induced by the affine transformations of the form

$$a = \tau_{\frac{t^2+t+1}{t^2+1},\frac{1}{(t+1)^3}}, \qquad b = \tau_{\frac{t^2+t+1}{t^2+1},\frac{t^2+t+1}{(t+1)^3}},$$
$$c = \tau_{\frac{t^2+t+1}{t^2+1},\frac{t}{(t+1)^3}}, \qquad d = \tau_{\frac{t^2+t+1}{t^2+1},\frac{t^2}{(t+1)^3}}.$$

There is another motivation to study the group $\mathcal{G}$ from Theorem 4.4.12. It was initially one of the six groups among those generated by 7421 non-minimally symmetric 4-state invertible automata over 2-letter alphabet studied in [Cap14], for which the existence of elements of infinite order could not be easily established by the standard known methods. Note that very recently Gillibert [Gil18] has shown that the order problem is undecidable in the class of automaton groups, so there is no hope to have a unified algorithm working in all cases. Moreover, slightly later Bartholdi and Mitrofanov showed that, perhaps, quite surprisingly, the problem remains undecidable even in the class of contracting automaton groups [BM17]. In [KPS16] many elements of infinite order in two of these six groups were found using a new technique of orbit automata. And the mentioned example from [SS16] was one of these two groups. We use a similar approach to study the structure of the group $\mathcal{G}$, but our proof is somewhat simpler and the automaton that we study generates exactly $\mathcal{L}_{2,2}$, and not its index 2 extension like in [SS16].

Chapter 2
Definitions and notations

In this chapter we introduce the notions and terminology to be used in the dissertation.

2.1 Rooted Trees

We will study the action of certain polynomials on regular rooted trees as well as groups generated by automorphisms of regular rooted trees. So we start with the definition of a tree and some related terminology.

Definition 2.1.1. A *tree* is a connected graph with no cycles. A *rooted tree* is a tree with one vertex selected to be the root.

In any connected graph, a metric (called combinatorial metric) can be defined such that the distance between any pair of vertices is the number of edges in a shortest path (geodesic) connecting them. The n^{th} level of a rooted tree is defined as the set of vertices whose distance from the root is n. Since the tree has no cycles, for each vertex v of the n^{th} level there is only one path from the root to v. The vertex u in this path that lies in level $n-1$ is called the parent of v. The vertex v is called a child of u. Hence every vertex except for the root has exactly one parent and may have some children.

Definition 2.1.2. A rooted tree is said to be *d-regular* or *d-ary* if there exists some positive integer d such that each vertex of the tree has exactly d children.

In a d-ary tree the n^{th} level has d^n vertices. Definition 2.1.2 asserts that all these trees have infinitely many levels. In case $d = 2$, such a tree is called a *rooted binary tree* which

represents our main interest in this dissertation. We will always visualize regular rooted trees such that they grow from top to bottom. So the root is the highest vertex and the children of each vertex v are located right under v.

We will label the vertices of a rooted d-ary tree by finite words over a finite alphabet $X = \{0, 1, \ldots, d-1\}$. Equivalently the set X^* of all finite words over X can be given the structure of a rooted d-ary tree by declaring that v is adjacent to vx for each $v \in X^*$ and $x \in X$. Thus the empty word corresponds to the root and for each positive integer n the set X^n corresponds to the n^{th} level of the tree. The example of the rooted binary tree is shown in Figure 7.

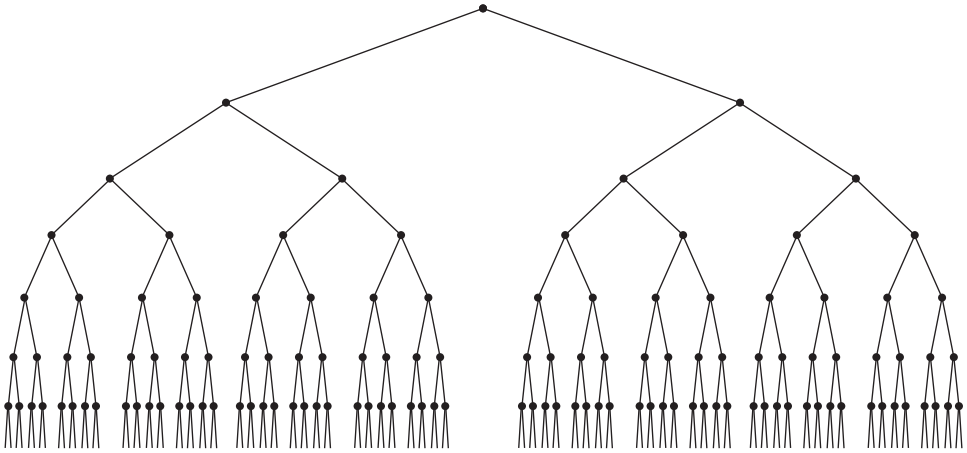

Figure 1.: Binary Tree

The set X^∞ of all infinite words over X can be identified with the *boundary* of the tree X^* consisting of all infinite paths in the tree without backtracking initiating at the root. An ultrametric can be defined on X^∞ as follows. The distance between two infinite words $x_1x_2x_3\ldots$ and $y_1y_2y_3\ldots$ in X^∞ is defined as 2^{-n}, where n is the length of the longest common prefix of these two words. Thus two words are closer if their common prefix is longer. Topologically X^∞ is homeomorphic to the Cantor set.

We are interested in groups of automorphisms of regular rooted trees. So we first define what these automorphisms are.

Definition 2.1.3. An *endomorphism* of a tree X^* is a map from the set of vertices of X^* to itself which preserves the adjacency relation. If such a map is bijective, it is called an automorphism of X^*.

An automorphism of X^* preserves the degree of each vertex as well as the distance from each vertex to the root. Since the root is the only vertex with degree d, it is invariant under all the tree automorphisms. Also the levels of the tree are invariant under automorphisms since the distance is preserved. The group of all automorphisms of X^* is denoted by $\operatorname{Aut} X^*$.

2.2 Mealy Automata

A convenient language to describe endomorphisms of regular rooted trees is the language of mealy automata.

Definition 2.2.1. A *Mealy automaton* (or simply *automaton*) is a tuple (Q, X, π, λ), where Q is a set (the set of states), X is a finite alphabet, $\pi\colon Q \times X \to Q$ is the *transition function* and $\lambda\colon Q \times X \to X$ 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* $\mathcal{A}_q$.

Automata are often represented by their *Moore diagrams*. The Moore diagram of an automaton $\mathcal{A} = (Q, X, \pi, \lambda)$ is a directed graph in which the vertices are the states of Q and the edges have the form $q \xrightarrow{x|\lambda(q,x)} \pi(q, x)$ for $q \in Q$ and $x \in X$.

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

$$\pi(q, x_1x_2\dots x_n) = \pi(\pi(q, x_1), x_2x_3\dots x_n),$$
$$\lambda(q, x_1x_2\dots x_n) = \lambda(q, x_1)\lambda(\pi(q, x_1), x_2x_3\dots x_n).$$

Definition 2.2.2. The semigroup (group) generated by all states of an automaton $\mathcal{A}$ viewed as endomorphisms of the rooted tree X^* under the operation of composition is called an *automaton semigroup (group)* and denoted by $\mathbb{S}(\mathcal{A})$ (respectively $\mathbb{G}(\mathcal{A})$).

In the definition of an 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 *self-similar group* [Nek05] and *state-closed group* [NS04]. However, most of the interesting examples of automaton groups are finitely generated groups defined by finite automata.

We now introduce the notion of a *state* (also called *section*) of an endomorphism at a vertex of the tree which is one of the main concepts in automata theory.

Definition 2.2.3. Let g be an endomorphism of the tree X^* and $x \in X$. For any $v \in X^*$ we can write

$$g(xv) = g(x)v' \tag{2.1}$$

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* of g at vertex x. We can inductively extend the definition of a section to any finite word $x_1x_2 \dots x_n \in X^*$ as follows.

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

We notice that $h|_v$ is actually an endomorphism of the tree rooted at v which can be identified with X^* as shown in figure 2.

In fact, any endomorphism of X^* can be induced by an initial automaton. Given an endomorphism g of X^*, we construct an initial automaton $\mathcal{A}(g)$ whose action on X^* coincides with that of g as follows. The set of states of $\mathcal{A}(g)$ is the set $\{g|_v \colon v \in X^*\}$ of different states of g at the vertices of X^*. The transition and output functions are defined by

$$\pi(g|_v, x) = g|_{vx},$$
$$\lambda(g|_v, x) = g|_v(x).$$

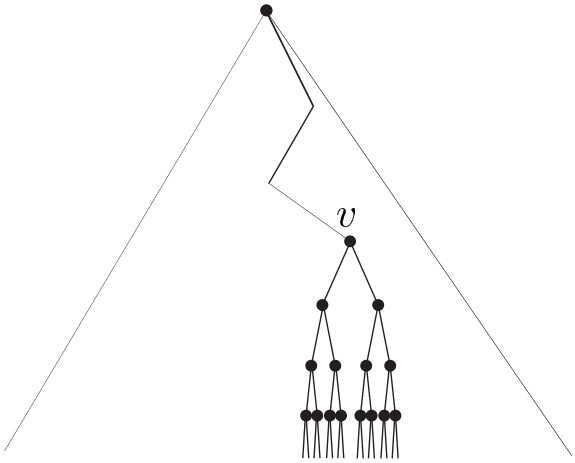

Figure 2.: Subtree rooted at v

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

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

Hence the states of any element of an automaton (semi)group can be computed as follows. If $g = g_1 g_2 \dots g_n$ and $v \in X^*$, then

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

Example 1. The automaton given by the Moore diagram in fig 3 has two states id and τ, where id is the identity automorphism of the rooted binary tree. This automaton generates a group $\langle \tau \rangle$ on $\{0,1\}^*$. The action of τ on the element $00000\dots$ of the boundary $\{0,1\}^\infty$ is as follows:

$$\begin{aligned}
\tau(00000\dots) &= 10000\dots, \\
\tau^2(00000\dots) &= 01000\dots, \\
\tau^3(00000\dots) &= 11000\dots, \\
\tau^4(00000\dots) &= 00100\dots, \\
\tau^5(00000\dots) &= 10100\dots
\end{aligned}$$

and so on. Identifying $\{0,1\}^\infty$ with the ring of dyadic integers (we will discuss this in detail in the next chapter), we see that the action of τ is just adding one to the input. That is

why τ is called the adding machine or the odometer. This asserts, in particular, that τ has infinite order so the group $\langle\tau\rangle$ is infinite cyclic.

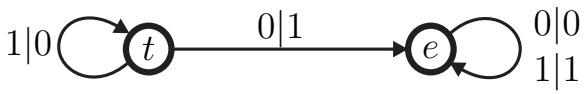

Figure 3.: Moore diagram of the adding machine automaton

Definition 2.2.4. Given an invertible automaton $\mathcal{A} = (Q, X, \pi, \lambda)$, we define its inverse as an automaton $\mathcal{A}^{-1} = (Q^{-1}, X, \tilde{\pi}, \tilde{\lambda})$, where

$$\tilde{\pi}(q^{-1}, x) = \pi(q, \lambda_q^{-1}(x)),$$
$$\tilde{\lambda}(q^{-1}, x) = \lambda_q^{-1}(x).$$

For Chapter 4 we will need the notions of reversible and bireversible automata that we introduce here.

For every finite automaton, we can construct a *dual automaton* by switching the states and the alphabet and switching the transition and output functions.

Definition 2.2.5. Given a finite automaton $\mathcal{A} = (Q, X, \pi, \lambda)$, its dual is a finite automaton $\partial\mathcal{A} = (X, Q, \hat{\lambda}, \hat{\pi})$, where

$$\hat{\lambda}(x, q) = \lambda(q, x),$$
$$\hat{\pi}(x, q) = \pi(q, x).$$

for every $x \in X$ and $q \in Q$.

It is easy to see that the dual of the dual of an automaton $\mathcal{A}$ coincides with $\mathcal{A}$. The semigroup $\mathbb{S}(\partial\mathcal{A})$ generated by $\partial\mathcal{A}$ acts on the free monoid Q^*. This induces the action on $\mathbb{S}(\mathcal{A})$. Similarly, $\mathbb{S}(\mathcal{A})$ acts on $\mathbb{S}(\partial\mathcal{A})$.

Definition 2.2.6. The semigroup $\mathbb{S}(\partial\mathcal{A})$ generated by the dual automaton $\partial\mathcal{A}$ is called the dual semigroup to the semigroup $\mathbb{S}(\mathcal{A})$ generated by $\mathcal{A}$.

Definition 2.2.7. An automaton $\mathcal{A}$ is called *bireversible* if it is invertible as well as its dual and the dual to $\mathcal{A}^{-1}$.

For a group G generated by a bireversible automaton $\mathcal{A}$, we can consider a dual group $\hat{G}$ generated by the dual automaton $\partial\mathcal{A}$.

2.3 Wreath Recursion and Portraits

For each automaton group G there is a natural embedding

$$G \hookrightarrow G \wr \mathrm{Sym}(X)$$

given by

$$G \ni g \mapsto (g_1, g_2, \ldots, g_d)\sigma_g \in G \wr \mathrm{Sym}(X), \tag{2.2}$$

where $g_1, g_2, \ldots, g_d$ are the states of g at the vertices of the first level, and σ_g is the permutation of X induced by the action of g on the first level of the tree. This is schematically shown in figure 4. If σ_g is the trivial permutation, it is customary to omit it in the notation. In the case of a binary rooted tree $\{0,1\}^*$, there is only one nontrivial permutation, namely the transposition (01), which is usually denoted simply by σ.

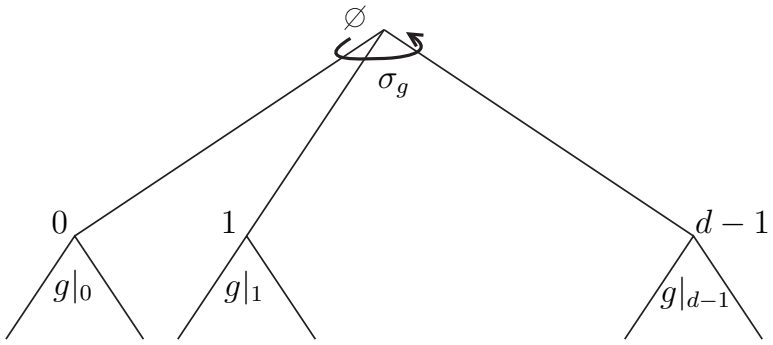

Figure 4.: Decomposition of an automorphism g of X^*

The decomposition of all generators of an automaton group under the embedding (2.2) is called the *wreath recursion* defining the group. It is a convenient language when doing

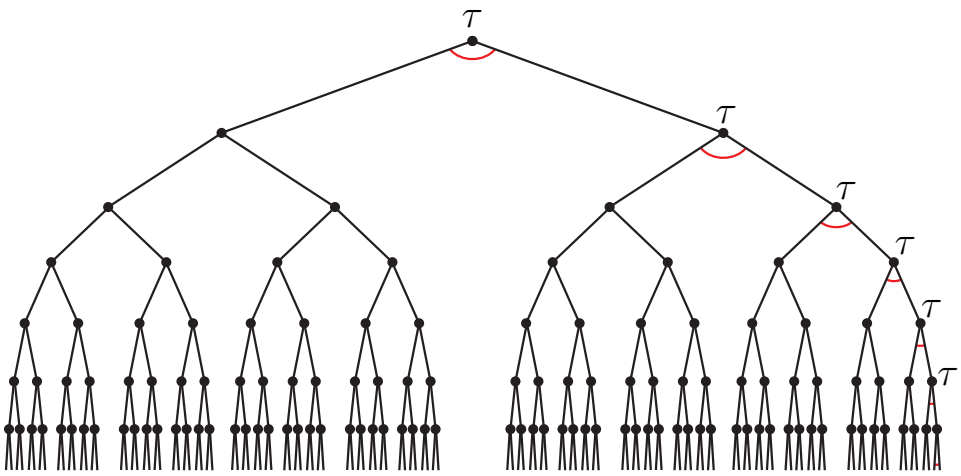

Figure 5.: The full portrait of the adding machine

computations involving the states of automorphisms. Indeed, products and inverses of automorphisms can be found as follows. If $g \mapsto (g_1, g_2, \ldots, g_d)\sigma_g$ and $h \mapsto (h_1, h_2, \ldots, h_d)\sigma_h$ are two elements of $\mathrm{Aut}(X^*)$, then

$$gh = (g_1 h_{\sigma_g(1)}, g_2 h_{\sigma_g(2)}, \ldots, g_d h_{\sigma_g(d)})\sigma_g\sigma_h$$

and

$$g^{-1} = (g^{-1}_{\sigma_g^{-1}(1)}, g^{-1}_{\sigma_g^{-1}(2)}, \cdots, g^{-1}_{\sigma_g^{-1}(d)})\sigma_g^{-1}$$

We can visualize the action of an automorphism g on the tree X^* using what is called the *full portrait* of g. The full portrait of g is a labeled infinite rooted d-ary tree with the root labeled by the name of the endomorphism g and each vertex v labeled by $g|_v$. Under each vertex v, we usually write the name of the mapping that $g|_v$ defines on the first level of the subtree rooted at v. In the case of a rooted binary tree, we draw a little arc (called switch) connecting the two edges hanging down from v if $g|_v$ acts nontrivially on the first level of the subtree rooted at v. If there is no switch, it means the action is trivial.

As an example, we again consider the adding machine τ which has the wreath recursion $\tau = (\tau, id)\sigma$. The full portrait of τ is shown in Figure 5.

2.4 Word Problem

The word problem is one of the three classical algorithmic problems in group theory formulated by Max Dehn in 1911 [Deh11]. It is stated as follows:

The word problem for a finitely generated group G is an algorithmic problem of deciding whether two given words over a symmetric generating set for G represent the same element of G.

The other two problems formulated by Dehn are the *conjugacy problem* (asking whether two given elements of a group are conjugate in it) and the *isomorphism problem* (asking whether there is an algorithm testing the isomorphism of groups from a given class).

The word problem has an easy solution in the class of groups generated by automata. The conjugacy problem was recently shown to be undecidable in groups generated by automata [ŠV12]. The question whether the isomorphism problem is decidable in this class is still open.

Not all groups admit an algorithm deciding the word problem. The first example of a finitely presented group with undecidable word problem was constructed by Novikov in 1955.

The algorithm of the word problem in groups generated by automata goes as follows. Let G be an automaton group generated by a finite automaton $\mathcal{A}$. Then the set S of states of $\mathcal{A}$ is the generating set for G. Suppose we need to check whether two words w and w' over $S \cup S^{-1}$ correspond to the same element of G. Since the equality $w = w'$ is equivalent to $w^{-1}w' = 1$, we can without loss of generality assume that w' is the trivial word. So we only need to check whether w corresponds to a nontrivial element of G or not.

In order to do this, we go over all possible sections of w and look either for a nontrivial action on the first level, or for repetitions of sections. Whenever we see a repetition, we stop going along this branch of the tree. Note that the set of sections of w is finite since every section is represented by a word of length not more than the length of w.

- If at some point we find a section that acts nontrivially on the first level, then $w \neq 1$.

- If we searched over all the sections (since w has only finite number of sections, the process will eventually terminate) and did not find a section acting nontrivially on the first level, we declare $w = 1$.

This algorithm is not so efficient as it requires an exponential (in terms of the length of the input word) running time and space in the worst case. This is because the sections of w are parametrized by words of lengths at most the length of w, but the size of this set obviously grows exponentially with the length of w.

However, there are some classes of automaton groups that admit polynomial time word problem algorithms. The most important of those is the class of *contracting groups*.

Calculations in groups generated by automata are often conceptually simple but usually technically difficult and time consuming. There are two packages that deal with the class of groups generated by automata: `AutomGrp` by Yevgen Muntyan and Dmytro Savchuk [MS16] and `FR` by Laurent Bartholdi [Bar15], both written for the `GAP` system [GAP15]. We will use mostly `AutomGrp` package and will try to hide as many technical details into computer calculations as the proofs will allow us.

Chapter 3

Endomorphisms of regular rooted trees induced by the action of polynomials on the ring $\mathbb{Z}_d$ of d-adic integers

The results of this chapter are presented in paper [AS17]. The structure of this chapter is as follows. In Section 3.1, we introduce an identification of the n^{th} level of the rooted d-ary tree X^* with the ring $\mathbb{Z}/(d^n\mathbb{Z})$ of integers modulo d^n. Also the notion of level transitivity is considered as well as the necessary and sufficient conditions that have to be met by an automorphism of the rooted binary tree $\{0,1\}^*$ in order to be level transitive. In Section 3.2, we show that every polynomial in $\mathbb{Z}[x]$ induces an endomorphism of X^* and show how to find the sections of this endomorphism. Then the class of permutational polynomials, which induce automorphisms of X^*, is considered. In Section 3.3, we prove the main theorem of this chapter which determines the necessary and sufficient conditions a 2-permutational polynomial has to meet in order to be level transitive.

3.1 Level Transitivity

We will identify the n^{th} level of X^* with the ring $\mathbb{Z}/(d^n\mathbb{Z})$ by identifying a vertex $x_0x_1\dots x_{n-1} \in X^n$ with $x_0 + dx_1 + \cdots + d^{n-1}x_{n-1} \in \mathbb{Z}/(d^n\mathbb{Z})$. For example, the vertices 00, 01, 10 and 11 of the second level of the rooted binary tree are identified with 0, 2, 1 and 3, respectively as shown in Figure 6. Moreover, the boundary of the tree can be naturally identified with the ring $\mathbb{Z}_d$ of d-adic integers.

The way we identified the n^{th} level of X^* with $\mathbb{Z}/(d^n\mathbb{Z})$ may not be the most natural way. A more natural way to do that is to identify a vertex $x_0x_1\dots x_{n-1}$ with its d-ary expansion $x_{n-1} + dx_{n-2} + \cdots + d^{n-1}x_0$. So the vertices 00, 01, 10 and 11 of the second level of the

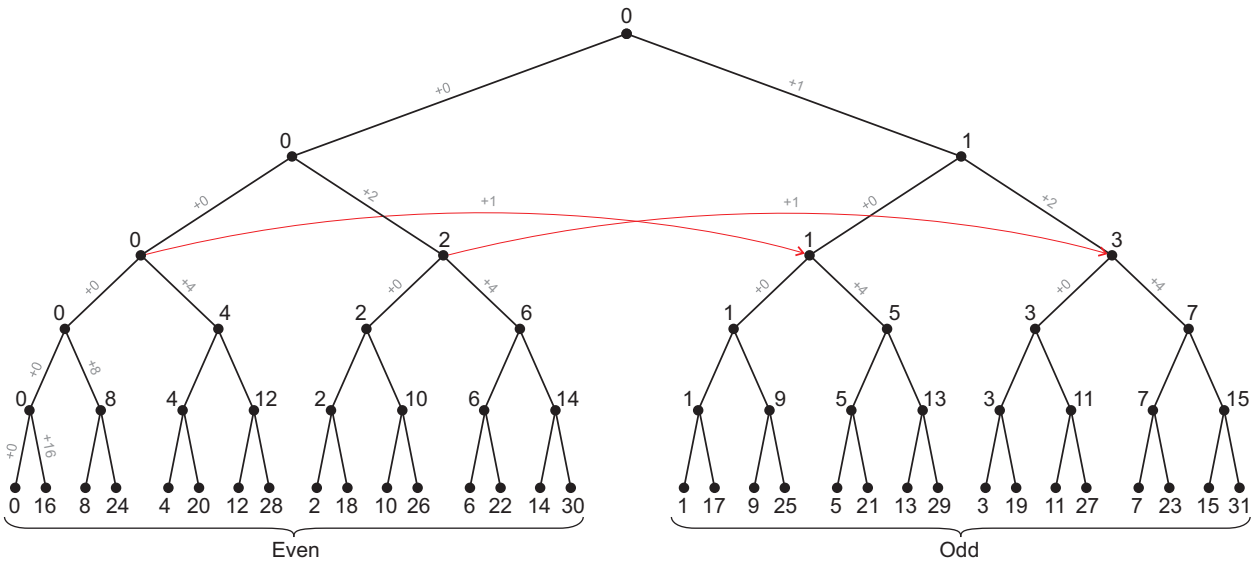

Figure 6.: Dyadic Numbering of vertices in the binary tree

binary tree are identified with 0, 1, 2 and 3, respectively, as shown in Figure 7. However, we adopt the first identification so that mappings induced by polynomials on X^* preserve the adjacency relation as we will see later.

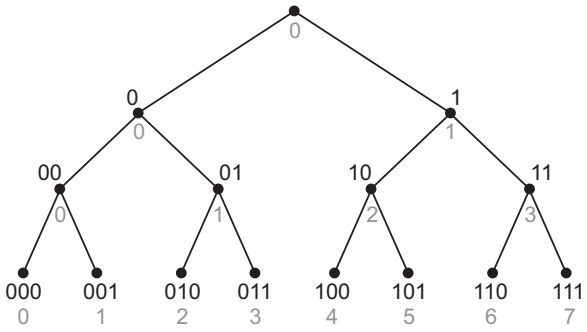

Figure 7.: Standard Numbering of vertices in the binary tree

The next definition introduces the notion of level transitivity which is the core concept of this chapter. Also a necessary and sufficient condition for an automorphism to act level transitively on a rooted binary tree is provided in the next proposition, that is a partial case of a more general result [BOERT96, Proposition (4.6)]. We give here an elementary proof

for this partial case.

Definition 3.1.1. An automorphism g of X^* is said to act *level transitively* on X^* if it acts transitively on each level of X^*.

Proposition 3.1.2. *Let g be an automorphism of the rooted binary tree $\{0,1\}^*$. Then g is level transitive if and only if the full portrait of g has an odd number of switches (nontrivial actions) in each level including the zeroth level.*

Proof. We first prove the sufficiency of the given condition using induction on level. Let g be an automorphism of $\{0,1\}^*$ whose full portrait has an odd number of switches in each level. So there is exactly one switch in the zeroth level and hence g acts transitively on the first level. Suppose that g acts transitively on the n^{th} level X^n and pick a random vertex $v \in X^{n+1}$. We want to show that the orbit of v by g is the whole level X^{n+1} which means that g acts transitively on the $(n+1)^{th}$ level X^{n+1}. Let $u \in X^n$ be the parent of v. It follows from the induction hypothesis that the orbit of u by g is the whole level X^n i.e., it has size 2^n. So $g(u), g^2(u), \ldots, g^{2^n}(u) = u$ are distinct. As such $g(v), g^2(v), \ldots, g^{2^n-1}(v)$ are distinct and different from v (because $g^r(u)$ is the parent of $g^r(v)$ for $r = 1, 2, \ldots$). Since there is an odd number of switches in the n^{th} level, it follows that $g^{2^n}(v)$ can not be v. Therefore $g^{2^n}(v)$ is the other child of u. For $k = 1, 2, \ldots, 2^n - 1$, we have $g^{2^n+k}(u) = g^k(u) \neq u$ which ensures that $g^{2^n+k}(v) \neq v$ for $k = 1, 2, \ldots, 2^n - 1$. We obviously have $g^{2^{n+1}}(v) = v$. Since g induces a permutation on X^{n+1}, the sets $\{g^k(v) \colon 0 \leq k < 2^n\}$ and $\{g^{2^n+k}(v) \colon 0 \leq k < 2^n\}$ of cardinality 2^n each are disjoint and their union forms the orbit of v by g of size 2^{n+1}, which means that it is the whole level X^{n+1}.

Now we prove the necessity of the condition. Let g be an automorphism of $\{0,1\}^*$ which does not satisfy the condition of the theorem. If there is no switch in the zeroth level, then g does not act transitively on the first level and we are done. So we assume that this is not the case and that X^n is the highest level (assuming the tree grows from top to bottom) with an even number of switches for some $n > 0$. Again we pick a vertex $v \in X^{n+1}$ and let $u \in X^n$ be the parent of v. From the sufficiency proof, we see that g acts transitively on X^n

and hence $g^{2n}(u) = u$. Since there is an even number of switches in the level X^n, we obtain that $g^{2n}(v) = v$. This means that g does not act transitively on X^{n+1}. □

Example 2. The adding machine τ has exactly one switch in each level. So the last theorem asserts that τ acts level transitively on the rooted binary tree.

3.2 Endomorphisms of Rooted Trees Arising from Polynomials over $\mathbb{Z}$

For a fixed integer $d \geq 2$, each polynomial $f(x) \in \mathbb{Z}[x]$ induces mappings $f_n \colon \mathbb{Z}/(d^n\mathbb{Z}) \to \mathbb{Z}/(d^n\mathbb{Z})$ for all positive integers n by taking the evaluation map modulo d^n. Identifying the n^{th} level of the rooted d-ary tree X^* with the ring $\mathbb{Z}/(d^n\mathbb{Z})$, the polynomial f gives rise to a mapping on the whole tree. In the next proposition, we show that this mapping is always an endomorphism of the rooted tree as it preserves the root and the adjacency relation. If for some d the mapping f_n is a bijection for each n, then f induces a permutation of each level of the rooted d-ary tree X^* and hence induces an automorphism of X^*. From now on, we will use the term *permutational polynomial* to denote a polynomial in $\mathbb{Z}[x]$ that induces an automorphism of X^* and to denote the automorphism it induces on X^* as well. The same letter will be used to refer to both functions and no confusion will arise.

Proposition 3.2.1. *Let $f(x) \in \mathbb{Z}[x]$. Then f induces an endomorphism on the rooted d-ary tree X^*. Moreover, different polynomials over $\mathbb{Z}$ induce different endomorphisms on X^*.*

Proof. We pick two adjacent vertices u and v of the tree such that u is the parent of v. So

$$u = x_0 + dx_1 + \cdots + d^{n-1}x_{n-1} \in X^n$$

and

$$v = x_0 + dx_1 + \cdots + d^{n-1}x_{n-1} + d^n x_n \in X^{n+1}$$

for some $x_0, \ldots, x_n \in \{0, 1, \ldots, d-1\}$ and $n \geq 0$. Let

$$f(u) = y_0 + dy_1 + \cdots + d^{n-1}y_{n-1}$$

and

$$f(v) = y_0' + dy_1' + \cdots + d^{n-1}y_{n-1}' + d^n y_n',$$

where $y_0, \ldots, y_{n-1}, y'_0, \ldots, y'_n \in \{0, 1, \ldots, d-1\}$. Since $u \equiv v \pmod{d^n}$, it follows that $f(u) \equiv f(v) \pmod{d^n}$. Thus

$$y_0 + dy_1 + \cdots + d^{n-1}y_{n-1} = y'_0 + dy'_1 + \cdots + d^{n-1}y'_{n-1}$$

By uniqueness of the d-ary expansion, we obtain $y_i = y'_i$ for $i = 0, \ldots, n-1$. Hence $f(u)$ is the parent of $f(v)$. This means that f preserves the adjacency relation so it is an endomorphism of X^*.

Now we consider two different polynomials $g, h \in \mathbb{Z}[x]$. We can find an integer k such that $g(k) \neq h(k)$. Let N be the smallest positive integer such that $g(k) \not\equiv h(k) \pmod{d^N}$. Then the actions of g and h on the N^{th} level of X^* are different. □

Our next goal is to completely describe endomorphisms induced by polynomials by explicitly describing their sections at all the vertices of X^*. Before we proceed to the next theorem, we need to introduce some basic notation to make our expressions less cumbersome.

Notation 3.2.2. Given two integers $d > 0$ and a, we can use the division algorithm to find two unique integers q and r such that $a = dq + r$ where $r \in \{0, 1, \ldots, d-1\}$. We will adopt the notation $Q_d(a) = q$ and $R_d(a) = r$ i.e., $Q_d(a) = a \operatorname{div} d$ and $R_d(a)$ is the remainder of a when divided by d. So for each integer a we always have

$$a = R_d(a) + dQ_d(a). \tag{3.1}$$

Theorem 3.2.3. *Given a polynomial $f(x) = a_0 + a_1x + \cdots + a_tx^t \in \mathbb{Z}[x]$ inducing an endomorphism of X^*, the image of a vertex $x_0 \in X$ under the induced endomorphism is $R_d(f(x_0))$ and the section of f at x_0 is again induced by a polynomial given by the equation:*

$$f|_{x_0}(x) = Q_d(f(x_0)) + \sum_{i=1}^{t} \frac{f^{(i)}(x_0)}{i!} d^{i-1}x^i \tag{3.2}$$

Proof. We pick a vertex $u = x_0 + dx_1 + d^2x_2 + \cdots + d^nx_n$ which has x_0 as a prefix. We can write u as $u = x_0 + d \cdot v$, where $v = x_1 + dx_2 + \cdots + d^{n-1}x_n$ corresponds to the suffix of the word u as in equation (2.2.3). Using the Taylor expansion of f about x_0 and the fact that

according to equality (3.1), $f(x_0) = R_d(f(x_0)) + dQ_d(f(x_0))$ we obtain

$$f(u) = f(x_0 + d \cdot v) = \sum_{i=0}^{t} \frac{f^{(i)}(x_0)}{i!} d^i v^i$$
$$= R_d(f(x_0)) + d \cdot \left(Q_d(f(x_0)) + \sum_{i=1}^{t} \frac{f^{(i)}(x_0)}{i!} d^{i-1} v^i \right)$$

Therefore,

$$f(x_0) = R_d(f(x_0 + d \cdot v)) = R_d(f(x_0)),$$

where with a slight abuse of notation in the left hand side x_0 and $f(x_0)$ denote vertices of the first level of X^*, and in the right hand side x_0 is an element of $\mathbb{Z}/(d\mathbb{Z})$. And finally,

$$f|_{x_0}(v) = Q_d(f(x_0 + d \cdot v)) = Q_d(f(x_0)) + \sum_{i=1}^{t} \frac{f^{(i)}(x_0)}{i!} d^{i-1} v^i$$

□

Remark 3.2.4. Equation (3.2) immediately implies that all the sections of f are polynomials of the same degree as the degree of f. Also since $f^{(t)}(x) = t! a_t$, all the sections of f at the same level n have the same leading coefficient $(d^{t-1})^n a_t$.

Example 3. The sections of the polynomial $f(x) = 1 + 3x + 2x^2$ at the vertices of the first three levels of the tree are depicted in Figure 8.

Proposition 3.2.5. *A polynomial f acting on X^* is finite-state (has finitely many distinct sections) if and only if it is linear.*

Proof. First we show that a linear polynomial $f(x) = ax + b$ acting on X^* has finitely many sections. From equation (3.2), we see that the section of f at a vertex $x_0 \in X$ is given by $f|_{x_0}(x) = ax + Q_d(b + x_0 a)$. Hence all the sections of f are linear polynomials with the same leading coefficient a. So the number of sections of f is bounded up by the number of distinct constant terms of these sections. Since the constant term can be written as $Q_d(b + a + \cdots + a)$ where we have exactly $x_0 \leq d-1$ summands equal to a, it is enough to notice that for any collection of integers $n_1, n_2, \ldots, n_d$ we have $|Q_d(n_1 + n_2 + \cdots + n_d)| \leq \max\{|n_1|, |n_2|, \ldots, |n_d|\}$. Therefore, any section of f has the form $ax + c$ where $|c| \leq \max\{|a|, |b|\}$.

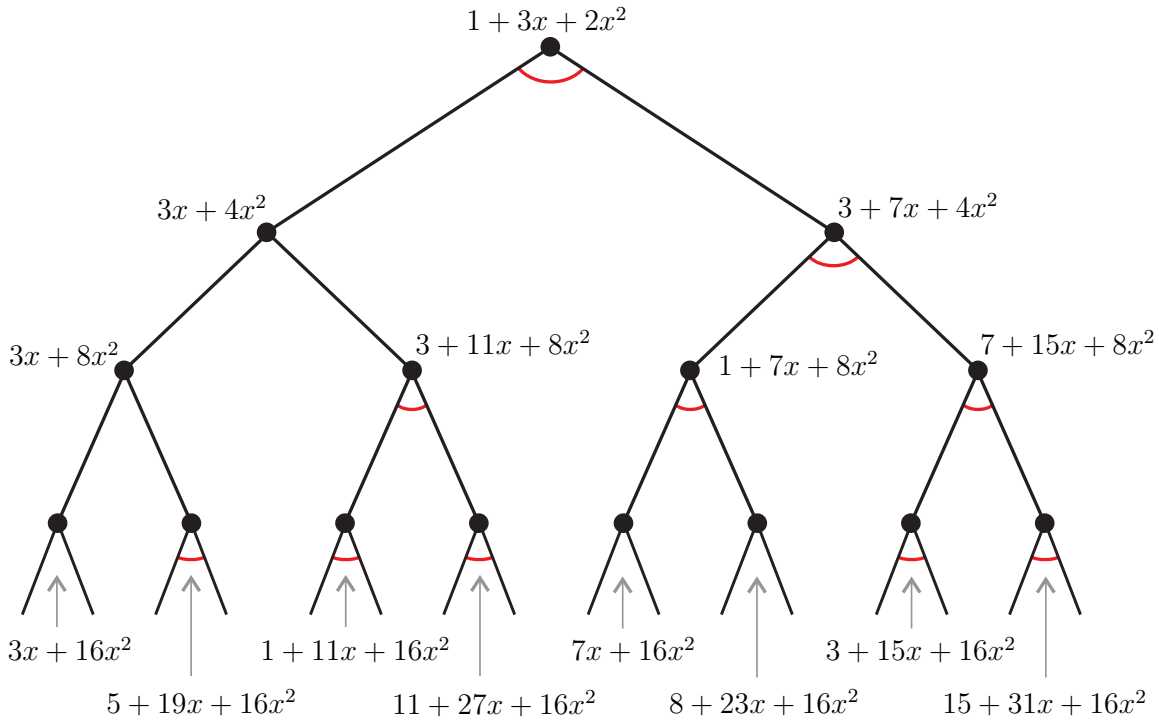

Figure 8.: Sections of an automorphism of $\{0,1\}^*$ induced by a polynomial $f(x) = 1 + 3x + 2x^2$

The fact that any nonlinear polynomial $f(x) = a_0 + a_1 x + \cdots + a_t x^t$ acting on X^* has infinitely many sections follows immediately from Remark 3.2.4 and Proposition 3.2.1. □

The next proposition deals with the characterization of the activity growth of endomorphisms induced by polynomials in the sense of Sidki [Sid00]. Recall that for an endomorphism g of X^* its activity growth function is defined as follows:

$$\theta_g(n) = |\{v \in X^n \colon g|_v \neq id\}| .$$

According to [Sid00] the activity growth function of a finite state automorphism (having finitely many distinct sections) may grow either polynomially or exponentially. These conditions have direct impact on the structure of the group generated by automorphisms of trees. For example, it has been shown in [Sid04] (see also [Nek10]) that there are no free subgroups in a group generated by finite state polynomially growing automorphisms. Additionally, it was proved in [BKN10, AAV13] that subgroups of Aut X^* generated by finite number of finite state automorphisms with up to linear growth are amenable. It is still an open question if the previous claim is still true when "linear" is replaced with "polynomial".

Proposition 3.2.6. *All polynomials $f(x) \in \mathbb{Z}[x]$ induce endomorphisms of X^* of exponential growth except polynomials of the form $f(x) = x + b$ which have bounded activity growth functions.*

Proof. Let $f(x)$ be a polynomial in $\mathbb{Z}[x]$ inducing an endomorphism of X^*. By Remark 3.2.4 all sections of f are induced by polynomials of the same degree as the one of f. Therefore, by Proposition 3.2.1, if f is nonlinear, it does not have any trivial sections and thus, its activity growth is exponential. For a linear polynomial of the form $f(x) = ax + b$ with $a \neq 1$, all its sections are linear polynomials with the same leading term and, therefore, nontrivial. Finally, every polynomial of the form $f(x) = x + b$ is simply a power of the adding machine $\tau(x) = x + 1$, which has bounded activity growth. Since the product of endomorphisms of bounded growth again has bounded growth, $f(x) = x + b = \tau^{(b)}(x)$ also has a bounded activity growth. □

Now we turn our attention to the permutational polynomials inducing automorphisms of X^*. First of all, we recall the definition.

Definition 3.2.7. A polynomial $f(x) \in \mathbb{Z}[x]$ is said to be *d-permutational* (or, simply, *permutational* if d is clear from the context) if for each $n \geq 1$ the mapping $f_n \colon \mathbb{Z}/(d^n\mathbb{Z}) \to \mathbb{Z}/(d^n\mathbb{Z})$ induced by the evaluation homomorphism is a permutation.

According to Proposition 3.2.1 each permutational polynomial induces an automorphism of the d-ary tree X^*. The following simple remark follows immediately from the definition.

Remark 3.2.8. The sections of a permutational polynomial acting on X^* are again permutational polynomials.

For each $d \geq 2$, the set of all linear d-permutational polynomials obviously forms a group under the operation of composition. However, the set of all d-permutational polynomials does not form a group as it is not closed under taking inverses. In fact, it has the structure of a cancellative monoid as shown in the next proposition.

Proposition 3.2.9. *For each $d \geq 2$, the set of all d-permutational polynomials forms a cancellative monoid under the operation of composition.*

Proof. It is clear that the composition of two d-permutational polynomials is again a permutational polynomial and that it induces an automorphism of the rooted d-ary tree X^*. The polynomial $\mathrm{id}(x) = x$ plays the role of the identity as it clearly induces the identity automorphism of the tree, so we have the structure of a monoid.

The inverse of an automorphism of X^* induced by a permutational polynomial always exists but it cannot always be induced by a polynomial. Although this is the case for linear permutational polynomials, the inverse of a nonlinear permutational polynomial cannot be induced by a polynomial. If this were true, we would have two polynomials not both linear acting on the ring $\mathbb{Z}_d$ (the boundary of X^*) with a trivial composition which is impossible. Still the existence of the inverse makes cancellation legitimate. □

Remark 3.2.10. If we consider the action of a d-permutational polynomial f on some specific level n, identified with $\mathbb{Z}/(d^n\mathbb{Z})$, the inverse of f on $\mathbb{Z}/(d^n\mathbb{Z})$ can always be induced by a permutational polynomial as shown in [MŠG10].

For the rest of the chapter, we will consider only permutational polynomials acting on the rooted binary tree $\{0,1\}^*$. The next theorem, proved by Rivest in [Riv01], determines the conditions under which a polynomial $f(x) \in \mathbb{Z}[x]$ induces a permutation of $\mathbb{Z}/(2^n\mathbb{Z})$ for each n and hence an automorphism of $\{0,1\}^*$ (i.e., is a 2-permutational polynomial).

Theorem 3.2.11 ([Riv01,MŠG10])**.** *A polynomial $f(x) = a_0+a_1x+\cdots+a_tx^t \in \mathbb{Z}[x]$ induces a permutation of $\mathbb{Z}/(2^n\mathbb{Z})$ for each n if and only if it satisfies the following conditions:*

(i) $a_1 \equiv 1 \pmod 2$

(ii) $a_2 + a_4 + a_6 + \cdots \equiv 0 \pmod 2$

(iii) $a_3 + a_5 + a_7 + \cdots \equiv 0 \pmod 2$

The theorem does not put any restriction on the constant term a_0 of the polynomial f. Assuming that f satisfies the conditions of the theorem i.e., it induces a permutation of $\mathbb{Z}/(2^n\mathbb{Z})$ and that a_0 is even (odd), all the evens of $\mathbb{Z}/(2^n\mathbb{Z})$ are mapped to evens (odds) and all the odds of $\mathbb{Z}/(2^n\mathbb{Z})$ are mapped to odds (evens). A special case of the theorem is when $f(x) = ax + b$ i.e., when f is linear. It defines a permutation of $\mathbb{Z}/(2^n\mathbb{Z})$ if and only if a is odd.

From now on, a permutational polynomial will always mean a 2-permutational polynomial. Also we will drop the 2 subscript in the notation of the function Q_2 and write $Q(a) = a \operatorname{div} 2$. According to equation (3.2), the sections of a permutational polynomial $f(x) = a_0 + a_1x + \cdots + a_tx^t$ acting on $\{0,1\}^*$ at the vertices 0 and 1 are given by the two equations:

$$f|_0(x) = Q(a_0) + a_1x + 2a_2x^2 + 2^2a_3x^3 + \cdots + 2^{t-1}a_tx^t \tag{3.3}$$

and

$$f|_1(x) = Q(a_0 + a_1 + \cdots + a_t) + (a_1 + 2a_2 + \cdots + ta_t)x \\ + \Big(2 \cdot 1a_2 + 3 \cdot 2a_3 + \cdots + t(t-1)a_t\Big)x^2 + 4\sum_{i=3}^{t} \frac{f^{(i)}(1)}{i!} 2^{i-3}x^i \quad (3.4)$$

In the case of a linear polynomial $f(x) = ax+b$, we have $f|_0(x) = ax+Q(b)$ and $f|_1(x) = ax+Q(a+b)$. For example, the adding machine τ can be represented by a linear permutational polynomial $\tau(x) = x + 1$. The sections of τ at 0 and 1 are respectively x and $x + 1$.

According to Theorem 3.2.11, the group of all linear 2-permutational polynomials is isomorphic to the group of matrices

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{Z},\ a \text{ odd} \right\}.$$

A generating set of this group is $\{p, q_{-1}, q_3, q_5, q_7, \ldots\}$, where $p(x) = x + 1$ and $q_m(x) = mx$ for $m = -1, 3, 5, 7, \ldots$. All the generators have infinite orders except for q_{-1} which is an involution. It was shown in [BŠ06] that for each $m = -1, 3, 5, 7, \ldots$, the subgroup generated by p and q_m is the Baumslag-Solitar group $BS(1, m) = \langle p, q_m \mid q_m p^m = pq_m \rangle$, where we adopt the convention that when the expression fg is used to denote the composition of two functions it means the function f acts first. In the same paper, Bartholdi and Šuníc considered sections of some linear polynomials acting on $\{0, 1\}^*$.

3.3 Level Transitivity of Permutational Polynomials

We start this section by presenting a couple of basic number theoretic facts that will be used many times in the proof of our main theorem. We introduce a bunch of lemmas without proofs. The proofs are straight forward so we leave them as simple exercises. The first lemma gives some properties of the function $Q(x)$ which was defined in section 3.2. Lemmas 3.3.2, 3.3.3 and 3.3.4 follow from the fact that for any positive integer n we have $ax \equiv x \pmod{n}$ if a and x are integers and $a \equiv 1 \pmod{n}$. We only list these results here in order to refer to them in the main proof later.

Lemma 3.3.1. *For any three integers x, m and n, we have:*

(i) $Q(x+2n) = Q(x) + n$

(ii) $Q(x) + Q(x+1) = x$

(iii) $Q(x) + Q(x+1+2n) = x+n$

(iv) $Q(x+4n) \equiv Q(x) \pmod 2$

(v) $Q(x) + Q(x+1+4n) \equiv x \pmod 2$

(vi) If $n \equiv m \pmod 4$, *then* $Q(x+n) \equiv Q(x+m) \pmod 2$

Lemma 3.3.2. *Let $a_1, a_2, \ldots, a_n$ be a collection of odd numbers. Then for any sequence of integers $x_1, x_2, \ldots, x_n$, we have* $a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv x_1 + x_2 + \cdots + x_n \pmod 2$ *i.e., $a_1x_1 + a_2x_2 + \cdots + a_nx_n$ has the same parity as $x_1 + x_2 + \cdots + x_n$.*

Lemma 3.3.3. *Let $a_1, a_2, \ldots, a_n$ and $x_1, x_2, \ldots, x_n$ be integers such that* $a_i \equiv 1 \pmod 4$ *for $i = 1, 2, \ldots, n$. Then* $a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv x_1 + x_2 + \cdots + x_n \pmod 4$.

Lemma 3.3.4. *Let $a_1, a_2, \ldots, a_n$ be a collection of odd numbers and $x_1, x_2, \ldots, x_n$ be any sequence of integers. Then* $a_1^2x_1 + a_2^2x_2 + \cdots + a_n^2x_n \equiv x_1 + x_2 + \cdots + x_n \pmod 4$.

The next notation and the two lemmas below will be used to simplify the proof of the main result.

Notation 3.3.5. If $f(x) = a_0 + a_1x + \cdots + a_tx^t \in \mathbb{Z}[x]$ is a permutational polynomial, then by Theorem 3.2.11 it uniquely defines integers k_f, m_f and n_f such that

$$\begin{aligned} a_1 &= 2k_f + 1, \\ a_2 + a_4 + \cdots &= 2m_f, \\ a_3 + a_5 + \cdots &= 2n_f. \end{aligned} \tag{3.5}$$

Further, for an arbitrary polynomial $g(x)$ we will denote by $a_i^{(g)}$ its coefficient at x^i.

The following lemma shows, in particular, that not every permutational polynomial can be a section of another permutational polynomial.

Lemma 3.3.6. *Let $f(x) = a_0 + a_1x + \cdots + a_tx^t$ be a permutational polynomial acting on the rooted binary tree $\{0,1\}^*$. Then for each non-root vertex $v \in \{0,1\}^*$, the permutational polynomial $f|_v(x) = b_0 + b_1x + \cdots + b_tx^t$ corresponding to the section of f at v, satisfies $n_{f|_v} \equiv 0 \pmod 2$ and $b_2 \equiv 0 \pmod 2$.*

Proof. Clearly, it is enough to check the conditions only for vertices of the first level. But this trivially follows from equations (3.3) and (3.4). We only have to notice that all the coefficients at x^i for $i \geq 3$ in both $f|_0$ and $f|_1$ are divisible by 4 and that the coefficients at x^2 in both $f|_0$ and $f|_1$ are divisible by 2. □

Lemma 3.3.7. *For every permutational polynomial $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_tx^t$ satisfying $n_g \equiv b_2 \pmod 2$, we have $(k_{g|_0} + k_{g|_1}) + (m_{g|_0} + m_{g|_1}) \equiv 0 \pmod 2$.*

Proof. First we have $a_1^{(g|_0)} + a_1^{(g|_1)} = 2k_{g|_0} + 1 + 2k_{g|_1} + 1$, thus from equations (3.3) and (3.4) we have

$$\begin{aligned} k_{g|_0} + k_{g|_1} &= \frac{a_1^{(g|_0)} + a_1^{(g|_1)}}{2} - 1 = \frac{b_1 + (b_1 + 2b_2 + \cdots + tb_t)}{2} - 1 \\ &= (b_1 - 1) + b_2 + (2b_4 + 3b_6 + 4b_8 + \cdots) + \frac{3b_3 + 5b_5 + \cdots}{2} \\ &= 2k_g + b_2 + (2b_4 + 4b_8 + \cdots) + (3b_6 + 5b_{10} + \cdots) + \frac{3b_3 + 5b_5 + \cdots}{2}. \end{aligned}$$

Using Lemma 3.3.2, we can write the sum modulo 2 as

$$k_{g|_0} + k_{g|_1} \equiv b_2 + (b_6 + b_{10} + \cdots) + \frac{3b_3 + 5b_5 + \cdots}{2} \pmod 2.$$

Again from equations (3.3) and (3.4), we can write $m_{g|_0} + m_{g|_1}$ modulo 2 as

$$\begin{aligned} m_{g|_0} + m_{g|_1} &\equiv b_2 + (b_2 + 3 \cdot 1b_3 + 2 \cdot 3b_4 + 5 \cdot 2b_5 + 3 \cdot 5b_6 + \cdots) \\ &\equiv 2b_2 + (2 \cdot 3b_4 + 5 \cdot 2b_5 + \cdots) + (3 \cdot 1b_3 + 3 \cdot 5b_6 + \cdots) \\ &\equiv b_3 + b_6 + b_7 + b_{10} + b_{11} + b_{14} + b_{15} + \cdots \pmod 2. \end{aligned}$$

The last congruence comes again from applying Lemma 3.3.2. Therefore the sum

$$(k_{g|_0} + k_{g|_1}) + (m_{g|_0} + m_{g|_1}) \equiv b_2 + (b_3 + b_7 + b_{11} + b_{15} + \cdots) + \frac{3b_3 + 5b_5 + \cdots}{2}$$
$$\equiv b_2 + \frac{5(b_3 + b_5) + 9(b_7 + b_9) + \cdots}{2} \pmod 2.$$

From Lemma 3.3.3, we have

$$5(b_3 + b_5) + 9(b_7 + b_9) + \cdots \equiv (b_3 + b_5) + (b_7 + b_9) + \cdots \equiv 2n_g \pmod 4$$

and thus

$$\frac{5(b_3 + b_5) + 9(b_7 + b_9) + \cdots}{2} \equiv n_g \pmod 2$$

. Therefore, $(k_{g|_0}+k_{g|_1})+(m_{g|_0}+m_{g|_1}) \equiv b_2+n_g \equiv 0 \pmod 2$. The proof is now complete. □

Now it is time to introduce our main theorem that determines the conditions under which a permutational polynomial acts level transitively on the rooted binary tree $\{0,1\}^*$. Obviously a permutational polynomial acts nontrivially on the first level of the tree if and only if its constant term is odd. Further, according to Proposition 3.1.2, a permutational polynomial f acts level transitively on $\{0,1\}^*$ if and only if in each level of the tree, the number of sections of f with odd constant terms is odd, or equivalently, the sum of these constant terms is odd.

The next proposition determines the conditions that a linear permutational polynomial has to meet in order to act level transitively on $\{0,1\}^*$. The general result is given by Theorem 3.3.9 which we prove by induction on level. The proof of the linear case is provided first so that the idea of the induction becomes clear and then the general case is considered. The proof given here is essentially different from the proofs of similar results introduced in [Ana06] and in [Lar02a].

Proposition 3.3.8. *Let $f(x) = ax + b$ be a permutational polynomial acting on the rooted binary tree $\{0,1\}^*$. Then this action is level transitive if and only if the following conditions hold:*

(i) $b \equiv 1 \pmod 2$

(ii) $a \equiv 1 \pmod 4$

Proof. We first show that the conditions are necessary. If condition (i) is not satisfied, then f does not act transitively on the first level. So we assume that condition (i) is satisfied but condition (ii) is not. We can also use the fact that a is odd since f is permutational. Thus we can write $b = 2s+1$ and $a = 2r+1$, where s and r are integers and r is odd. The sections of f at 0 and 1 are respectively

$$ax + Q(b) = ax + s$$

and

$$ax + Q(a + b) = ax + r + s + 1$$

. The sum of the two constant terms is $2s + r + 1$ which is even. Therefore, f does not act transitively on the second level.

To prove sufficiency of the conditions, we use induction on level. First we can write $a = 4k + 1$ for some integer k which follows from condition (ii). Since b is odd, f acts transitively on the first level. Now assume that the sections of f at some level $n \geq 0$ are respectively $ax+\alpha_1, \ldots, ax+\alpha_m$, where $m = 2^n$ and suppose that $\alpha_1+\cdots+\alpha_m \equiv 1 \pmod 2$, which serves as the induction hypothesis. The sections of f at level $n + 1$ are respectively

$$ax + \sigma_1, ax + \sigma_2, \ldots, ax + \sigma_{2m-1}, ax + \sigma_{2m}$$

, where

$$\sigma_1 = Q(\alpha_1),\ \sigma_2 = Q(\alpha_1 + 4k + 1),\ \ldots\ ,\ \sigma_{2m-1} = Q(\alpha_m),\ \sigma_{2m} = Q(\alpha_m + 4k + 1)$$

. Hence the sum of constant terms of the sections of level $n + 1$ is

$$(\sigma_1 + \sigma_2) + \cdots + (\sigma_{2m-1} + \sigma_{2m}) =$$

$$(Q(\alpha_1) + Q(\alpha_1 + 4k + 1)) + \cdots + (Q(\alpha_m) + Q(\alpha_m + 4k + 1)) \equiv \alpha_1 + \cdots + \alpha_m \equiv 1 \pmod 2$$

, where we have used Lemma 3.3.1 part (v). The proof is now complete. □

The adding machine $\tau(x) = x + 1$ as well as all its odd powers $\tau^r(x) = x + r$, where r is odd, satisfy the conditions of the last proposition. So they act level transitively on the rooted binary tree $\{0,1\}^*$.

Theorem 3.3.9. *Let $f(x) = a_0 + a_1x + \cdots + a_tx^t$ be a permutational polynomial acting on the rooted binary tree $\{0,1\}^*$. Then this action is level transitive if and only if the following conditions hold:*

(i) $a_0 \equiv 1 \pmod 2$

(ii) $2a_2 \equiv a_3 + a_5 + \cdots \pmod 4$

(iii) $a_2 + a_1 - 1 \equiv a_4 + a_6 + \cdots \pmod 4$

Proof. Before proceeding to the proof of the necessity and sufficiency of the conditions $(i) - (iii)$ we restate them taking into account that f is a permutational polynomial. Using Notation 3.3.5, we can write $a_1 = 2k_f + 1$, $a_2 + a_4 + \cdots = 2m_f$ and $a_3 + a_5 + \cdots = 2n_f$ for some integers k_f, m_f and n_f. To simplify notation, we will drop the lower index f and will write simply k, m, n for k_f, m_f and n_f below. Thus, the condition (ii) of our hypothesis is equivalent to the condition

(ii') $a_2 \equiv n \pmod 2$.

Further, by adding a_2 to both sides in the condition (iii) we obtain:

$$2a_2 + a_1 - 1 \equiv a_2 + a_4 + \cdots \equiv 2m \pmod 4.$$

Plugging $a_1 = 2k+1$ into the last congruence and dividing both sides by 2 yields the following equivalent to condition (iii):

(iii') $k + a_2 \equiv m \pmod 2$.

To show that the conditions $(i), (ii)'$ and $(iii)'$ are necessary, we first notice that if condition (i) is not satisfied then f does not act transitively on the first level. So we assume that condition (i) is satisfied and hence we can write $a_0 = 2s+1$ for some integer s. Equations (3.3)

and (3.4) tell us that the constant terms of the sections of f at 0 and 1 are respectively $Q(a_0)$ and $Q(a_0 + a_1 + \cdots + a_t)$. Their sum is

$$\begin{aligned} Q(a_0) + Q(a_0 + a_1 + \cdots + a_t) &= Q(a_0) + Q(a_0 + 2k + 1 + 2m + 2n) \\ &= a_0 + k + m + n = 2s + (k + n) + m + 1, \end{aligned}$$

where we have used Lemma 3.3.1 part (iii). For f to act transitively on the second level this sum must be odd, so we must have

$$(k + n) \equiv m \pmod 2. \tag{3.6}$$

If exactly one of the two conditions (ii') and (iii') is satisfied, then $(k + n) \not\equiv m \pmod 2$. However, if the two conditions are both not satisfied, we have $(k + n) \equiv m \pmod 2$ so f does act transitively on the second level. We will show that in the latter case, f does not act transitively on the third level by proving that the sum of constant terms of the sections of f at the second level is even.

From equations (3.3) and (3.4), we can infer that the constant terms of the sections of f at the vertices $00, 01, 10$ and 11 are respectively:

- $Q(Q(a_0)) = Q(s)$
- $Q(s + a_1 + 2a_2 + \cdots + 2^{t-1}a_t) = Q(s + 2k + 1 + 2a_2 + \cdots + 2^{t-1}a_t)$
- $Q(Q(a_0 + a_1 + \cdots + a_t)) = Q(Q(2s + 1 + 2k + 1 + 2m + 2n)) = Q(1 + s + k + m + n)$
- $Q((1+s+k+m+n)+(a_1+2a_2+\cdots+ta_t)+(2\cdot 1a_2+3\cdot 2a_3+\cdots+t(t-1)a_t)+4\sum_{i=3}^{t}\frac{f^{(i)}(1)}{i!}2^{i-3})$

The sum of these constant terms modulo 2 is

$$\begin{aligned} Q(s) + Q(s + 2k + 1 + 2a_2) + Q(1 + s + k + m + n) \\ + Q((1 + s + k + m + n) + a_1 + 2^2a_2 + 3^2a_3 + \cdots + t^2a_t), \end{aligned}$$

where we have used Lemma 3.3.1 part (iv). Using part (iii) of the same lemma and reusing part (iv) as well, the sum modulo 2 simplifies to

$$\begin{aligned}
&s+k+a_2+Q(1+s+k+m+n)\\
&\qquad +Q((1+s+k+m+n)+1+2k+(2^2a_2+4^2a_4+\cdots)+(3^2a_3+5^2a_5+\cdots))\\
&\equiv s+k+a_2+Q(1+s+k+m+n)+Q((1+s+k+m+n)+1+2k+(3^2a_3+5^2a_5+\cdots))\\
&\equiv s+k+a_2+Q(1+s+k+m+n)+Q((1+s+k+m+n)+1+2k+(a_3+a_5+\cdots))\\
&\equiv s+k+a_2+Q(1+s+k+m+n)+Q((1+s+k+m+n)+1+2k+2n) \pmod 2,
\end{aligned}$$

where we have used Lemma 3.3.4 to obtain $3^2a_3+5^2a_5+\cdots \equiv a_3+a_5+\cdots$. Again we apply part (iii) of Lemma 3.3.1 to have the sum modulo 2 as

$$s+k+a_2+(1+s+k+m+n)+k+n \equiv 2s+2k+(k+n)+m+(n+a_2+1)$$

$$\equiv ((k+n)+m)+(n+a_2+1) \equiv (k+n)+m \equiv 0 \pmod 2$$

where we have used the fact that the two conditions (ii') and (iii') are both not satisfied.

Now we prove the sufficiency of the conditions (i), $(ii)'$ and $(iii)'$. We will show that f acts transitively on the first and second levels and then use induction for other levels. Condition (i) guarantees transitivity on the first level. We deduced in the proof of necessity that the transitivity on the second level is equivalent to equality (3.6) which, in our case, is obtained by adding conditions $(ii)'$ and $(iii)'$.

Before we formulate the induction hypothesis, we recall that at each vertex v of $\{0,1\}^*$ the section $f|_v$ is induced by a permutational polynomial $f|_v(x)=a_0^{(f|_v)}+a_1^{(f|_v)}x+\cdots+a_t^{(f|_v)}x^t$, and integers $a_i^{(f|_v)}$, $k_{f|_v}$, $m_{f|_v}$, and $n_{f|_v}$ are defined as in Notation 3.3.5. Also if v is a non-root vertex, we have $n_{f|_v}\equiv 0 \pmod 2$ and $a_2^{(f|_v)}\equiv 0 \pmod 2$ by Lemma 3.3.6.

Let us assume that the sections of f at some level $l\geq 1$ of the tree are $\varphi_1,\ldots,\varphi_r$, where $r=2^l$. For our induction hypothesis we suppose that $a_0^{(\varphi_1)}+\cdots+a_0^{(\varphi_r)}\equiv 1 \pmod 2$. Let $\psi_1,\psi_2,\ldots,\psi_{2r-1},\psi_{2r}$ be the sections of f at level $l+1$. Then

$$\sum_{i=1}^{2r} a_0^{(\psi_i)} = \sum_{j=1}^{r} \left(a_0^{(\psi_{2j-1})} + a_0^{(\psi_{2j})} \right) = \sum_{j=1}^{r} \left(Q\left(a_0^{(\varphi_j)}\right) + Q\left(a_0^{(\varphi_j)} + a_1^{(\varphi_j)} + \cdots + a_t^{(\varphi_j)}\right) \right)$$

$$= \sum_{j=1}^{r} \left(Q\left(a_0^{(\varphi_j)}\right) + Q\left(a_0^{(\varphi_j)} + 2k_{\varphi_j} + 1 + 2m_{\varphi_j} + 2n_{\varphi_j}\right) \right) = \sum_{j=1}^{r} \left(a_0^{(\varphi_j)} + k_{\varphi_j} + m_{\varphi_j} + n_{\varphi_j} \right)$$

$$= \sum_{j=1}^{r} a_0^{(\varphi_j)} + \sum_{j=1}^{r} k_{\varphi_j} + \sum_{j=1}^{r} m_{\varphi_j} + \sum_{j=1}^{r} n_{\varphi_j} \equiv 1 + \sum_{j=1}^{r} k_{\varphi_j} + \sum_{j=1}^{r} m_{\varphi_j} \pmod 2$$

by induction hypothesis, where we have used Lemma 3.3.1 part (*iii*), then rearranged the terms, and finally exploited Lemma 3.3.6 at the last transition. To complete the proof we mention that $(k_{\varphi_i} + k_{\varphi_{i+1}}) + (m_{\varphi_i} + m_{\varphi_{i+1}}) \equiv 0 \pmod 2$ for $i = 1, 3, \ldots, r-1$ according to Lemma 3.3.7. Indeed, if $l = 1$, then φ_0 and φ_1 are the sections of f at the vertices of the first level. In this case the condition of Lemma 3.3.7 is just the condition $(ii)'$. When $l > 1$, φ_i and φ_{i+1} are sections at the vertices of the first level of a section of f at some non-root vertex. Thus the condition of Lemma 3.3.7 is again satisfied according to Lemma 3.3.6. □

If a mapping f acting on the rooted binary tree $\{0,1\}^*$ is level transitive, then the orbit of every element in the boundary of the tree $\mathbb{Z}_2$ under f is dense in $\mathbb{Z}_2$. Thus the dynamical system $(\mathbb{Z}_2, f)$ is minimal. Also Anashin proved in [Ana06] that a polynomial $f \in \mathbb{Z}[x]$ is ergodic with respect to the normalized Haar measure on $\mathbb{Z}_2$ if and only if f is transitive mod 2^n for every positive integer n. Combining Theorem 3.2.11 and Theorem 3.3.9, we thus obtain a new and more elementary proof of the result of Larin [Lar02a].

Theorem 3.3.10 ([Lar02a]). *Let $f(x) = a_0 + a_1 x + \cdots + a_t x^t \in \mathbb{Z}_2[x]$. Then the dynamical system $(\mathbb{Z}_2, f)$ is minimal, or equivalently, f is ergodic with respect to the normalized Haar measure of $\mathbb{Z}_2$ if and only if the following conditions are satisfied:*

(i) $a_0 \equiv 1 \pmod 2$

(ii) $a_1 \equiv 1 \pmod 2$

(iii) $2a_2 \equiv a_3 + a_5 + \cdots \pmod 4$

(iv) $a_2 + a_1 - 1 \equiv a_4 + a_6 + \cdots \pmod 4$

Chapter 4

The lamplighter group of rank two generated by a bireversible automaton

The results of this chapter are presented in paper [AS18]. The structure of this chapter is as follows. In Section 4.1, we consider the class of spherically homogeneous automorphisms. In Section 4.2, we consider the classes of affine automorphisms and affine shifts together with an intermediate class. We emphasize the relation between affine automorphisms and spherically homogeneous automorphisms. In Section 4.3, we introduce the lamplighter group $\mathcal{L}$ and give its presentation. In Section 4.4, we study the structure of the automaton group $\mathcal{G} = \langle a = (b, d)\sigma, b = (d, b)\sigma, c = (a, c), d = (c, a)\rangle$ and show that it is isomorphic to the rank 2 lamplighter group $\mathcal{L}_{2,2} \cong (\mathbb{Z}/2\mathbb{Z})^2 \wr \mathbb{Z}$.

4.1 Spherically Homogeneous Automorphisms

The notion of spherically homogeneous automorphisms is crucial in the study of some automaton groups including the group $\mathcal{G}$ to be considered in this chapter. We introduce this notion in the next definition.

Definition 4.1.1. An automorphism g of the tree X^* is called *spherically homogeneous* if for each level l the states of g at the vertices of X^l all coincide.

Each such automorphism has a form $a = (b, b, \ldots, b)\sigma_1$, $b = (c, c, \ldots, c)\sigma_2, \ldots$, where σ_i's are permutations of X. For example, automorphisms $a = (a, a)\sigma, b = (a, a)$ are spherically homogeneous automorphisms of the binary tree. Clearly, an automorphism g of X^* is spherically homogeneous if and only if for each level l of the tree X^* the states of g at all the vertices of X^l act identically on the first level.

Every spherically homogeneous automorphism can be fully defined by a sequence $\{\sigma_n\}_{n\geq 1}$ of permutations of X where σ_n describes the action of g on the n-th letter of the input word. Given a sequence $\{\sigma_n\}_{n\geq 1}$, we can denote the corresponding spherically homogeneous automorphism by $[\sigma_n]_{n\geq 1}$.

The set of all spherically homogeneous automorphisms of X^* forms an uncountable subgroup $\mathrm{SHAut}(X^*)$ of $\mathrm{Aut}(X^*)$ isomorphic to a direct product of countably many copies of $\mathrm{Sym}(|X|)$. Thus, in the case of the binary tree, this group is abelian. When $d \geq 3$, the group $\mathrm{SHAut}(X^*)$ contains an abelian subgroup consisting of automorphisms whose sections act on the first level as powers of some fixed long d-cycle.

In the case of a binary tree, there is a countably generated self-similar dense subgroup Δ in $\mathrm{SHAut}(X^*)$ defined below.

For an automorphism $g \in \mathrm{Aut}(X^*)$, we will denote by $g^{(n)}$ the automorphism of X^* acting trivially on the n-th level, and whose states at all vertices of X^n are equal to g. For example, $g^{(0)} = g$, $g^{(1)} = (g, g)$, etc. In particular, we will denote by $\sigma^{(n)}$, $n \geq 0$ the automorphism of X^* that acts on the $(n+1)$-st coordinate in the input word by the long cycle σ. So $\sigma^{(0)} = (1, 1)\sigma$, $\sigma^{(1)} = (\sigma^{(0)}, \sigma^{(0)})$, $\ldots$, $\sigma^{(n+1)} = (\sigma^{(n)}, \sigma^{(n)})$. Now define a group Δ as

$$\Delta = \langle \sigma^{(0)}, \sigma^{(1)}, \sigma^{(2)}, \ldots \rangle.$$

For a finite state automorphism g of X^*, it is algorithmically decidable whether g is spherically homogeneous or not. First we check if all the states of g at the vertices of the first level coincide. If not, then g is not spherically homogeneous. Otherwise, we repeat the procedure for the state $g|_0$ (note that $g|_0 = g|_1 = \cdots = g|_{d-1}$). Since g is finite state, this procedure will eventually terminate.

4.2 Affine Automorphisms

In this section we discuss the notion of affine automorphisms and a related notion of $(\mathbb{Z}/d\mathbb{Z})[[t]]$-affine automorphisms. As described above, one of the ways to define an automorphism of X^* is by using the language of automata. However, some automorphisms can

be defined also differently. Namely, if we endow the boundary X^∞ of the tree with some algebraic structure, then some natural transformations of X^∞ will induce automorphisms of X^*. For example, one can endow X^∞ with the structure of the ring of d-adic numbers and study the automorphisms induced by polynomials as we did in the last chapter. Here, we will use two other interpretations of the boundary X^∞ as the ring $(\mathbb{Z}/d\mathbb{Z})[[t]]$ of formal power series over $(\mathbb{Z}/d\mathbb{Z})$, and as an infinite dimensional free $\mathbb{Z}/d\mathbb{Z}$-module $(\mathbb{Z}/d\mathbb{Z})^\infty$ (which is a vector space over $(\mathbb{Z}/d\mathbb{Z})$ in the case of prime d).

Each infinite word $a_0a_1a_2\ldots \in X^\infty$ can be represented as an element $a_0+a_1t+\cdots+a_it^i+\cdots$ of $(\mathbb{Z}/d\mathbb{Z})[[t]]$. Let $f(t) = a_0 + a_1t + a_2t^2 + \ldots$ and $g(t) = b_0 + b_1t + b_2t^2 + \ldots$ be power series in $(\mathbb{Z}/d\mathbb{Z})[[t]]$ with a_0 being a unit in $\mathbb{Z}/d\mathbb{Z}$ (so that $f(t)$ is a unit in $(\mathbb{Z}/d\mathbb{Z})[[t]]$). We can define an affine transformation $\tau_{f,g}$ of $(\mathbb{Z}/d\mathbb{Z})[[t]]$ by

$$\Big(\tau_{f,g}(h)\Big)(t) = g(t) + h(t)\cdot f(t).$$

It is shown in [SS16] that this transformation induces an automorphism of X^* under the above identification of X^∞ with $(\mathbb{Z}/d\mathbb{Z})[[t]]$. With a slight abuse of notation we will also denote it by $\tau_{f,g}$. Such automorphisms are called $(\mathbb{Z}/d\mathbb{Z})[[t]]$-*affine automorphisms of* X^*.

For example, an automorphism of the form $\tau_{1,g(t)}$ is a spherically homogeneous automorphism of X^* that acts on the i-th letter of an input word by $(0, 1, \ldots, d-1)^{b_i} \in \mathrm{Sym}(X)$, where b_i is the coefficient at t^i in $g(t)$. In particular, the addition of t^n in $(\mathbb{Z}/d\mathbb{Z})[[t]]$ induces $\sigma^{(n)} \in \mathrm{SHAut}(X^*)$, and thus the group of automorphisms induced by addition of all possible polynomials in $(\mathbb{Z}/d\mathbb{Z})[[t]]$ is exactly Δ.

A more general class of affine automorphisms of X^* is obtained by viewing X^∞ as an infinite dimensional free $(\mathbb{Z}/d\mathbb{Z})$-module $(\mathbb{Z}/d\mathbb{Z})^\infty$, where we treat a word $a_0a_1a_2\ldots \in X^\infty$ as an infinite-dimensional row "vector" $[a_0, a_1, a_2, \ldots] \in (\mathbb{Z}/d\mathbb{Z})^\infty$. The set $\{\mathbf{e}_i\}_{i\geq 1}$, where $\mathbf{e}_i = [0, 0, \ldots, 0, 1, 0, \ldots]$ with 1 at position i, serves as a natural "basis" for $(\mathbb{Z}/d\mathbb{Z})^\infty$.

Let A be an infinite upper triangular matrix with entries from $\mathbb{Z}/d\mathbb{Z}$ whose diagonal entries are units in $\mathbb{Z}/d\mathbb{Z}$. We will denote the set of all such matrices by $U_\infty(\mathbb{Z}/d\mathbb{Z})$. Also let $\mathbf{b} \in (\mathbb{Z}/d\mathbb{Z})^\infty$ be a row vector. We define the transformation $\pi_{A,\mathbf{b}}\colon (\mathbb{Z}/d\mathbb{Z})^\infty \to (\mathbb{Z}/d\mathbb{Z})^\infty$

by

$$\pi_{A,\mathbf{b}}(\mathbf{x}) = \mathbf{b} + \mathbf{x} \cdot A.$$

which is always well-defined since A is upper triangular. As shown in [SS16] every such transformation induces an automorphism of the tree X^* which will be also denoted by $\pi_{A,\mathbf{b}}$ and called an *affine automorphism of* X^*.

The set $\mathrm{Aff}(X^*) = \{\pi_{A,\mathbf{b}} \in \mathrm{Aut}(X^*) \mid A \in U_\infty(\mathbb{Z}/d\mathbb{Z}),\ \mathbf{b} \in (\mathbb{Z}/d\mathbb{Z})^\infty\}$ forms a group which is called the *group of affine automorphisms of* X^*. Let I denote the infinite identity matrix over $\mathbb{Z}/d\mathbb{Z}$. Then the set $\mathrm{Aff}_I(X^*) = \{\pi_{I,\mathbf{b}}, \mathbf{b} \in (\mathbb{Z}/d\mathbb{Z})^\infty\}$ is a subgroup of $\mathrm{Aff}(X^*)$ which is called the group of *affine shifts*. Indeed, $\mathrm{Aff}_I(X^*)$ is the topological closure of the group Δ described above. Moreover, $\mathrm{Aff}_I(X^*)$ is a subgroup of the group $\mathrm{SHAut}(X^*)$ of spherically homogeneous automorphisms of X^*. They coincide when $d = 2$.

The following two results from [SS16] will be important in the proof of the main theorem in Section 4.4.

Proposition 4.2.1 ([SS16]). *Let* $f(t) = \sum_{n=0}^{\infty} a_n t^n, g(t) = \sum_{n=0}^{\infty} b_n t^n \in (\mathbb{Z}/d\mathbb{Z})[[t]]$ *be two power series with* a_0 *a unit in* $\mathbb{Z}/d\mathbb{Z}$. *Then the* $(\mathbb{Z}/d\mathbb{Z})[[t]]$*-affine automorphism* $\tau_{f,g}$ *coincides with the affine automorphism* $\pi_{A,\mathbf{b}}$ *for* $\mathbf{b} = [b_0, b_1, b_2, \ldots]$ *and*

$$A = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 & \ldots \\ 0 & a_0 & a_1 & a_2 & \ldots \\ 0 & 0 & a_0 & a_1 & \ldots \\ 0 & 0 & 0 & a_0 & \ldots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

Thus, the set $\mathrm{Aff}_{[[t]]}(X^*) = \{\tau_{f,g} \in \mathrm{Aut}(X^*) \mid f, g \in (\mathbb{Z}/d\mathbb{Z})[[t]], f(t)$ is a unit in $(\mathbb{Z}/d\mathbb{Z})[[t]]\}$ forms a proper subgroup of $\mathrm{Aff}(X^*)$ and is called the *group of* $(\mathbb{Z}/d\mathbb{Z})[[t]]$*-affine automorphisms of* X^*.

Theorem 4.2.2 ([SS16]). *The normalizer* N *of the group* $\mathrm{Aff}_I(X^*)$ *in* $\mathrm{Aut}(X^*)$ *coincides with the group* $\mathrm{Aff}(X^*)$ *of all affine automorphisms. In particular, in the case of the binary tree, the normalizer of* $\mathrm{SHAut}(\{0,1\}^*)$ *in* $\mathrm{Aut}(\{0,1\}^*)$ *is* $\mathrm{Aff}(\{0,1\}^*)$.

4.3 Lamplighter Groups

In this section we introduce the lamplighter group and give a presentation of it with two generators and infinitely many relations. We show that it has the structure of a semidirect product, or more specifically, a restricted wreath product. First we give a motivation to the concept which makes it easy to obtain the generators and relations and to define multiplication. We do not provide complete proofs here. For a more detailed discussion on the topic, the reader is referred to [Eck12] and [Tab17].

Consider an infinite street lined with evenly spaced lampposts. A lamplighter can walk along the street in both directions lighting a finite number of lamps and then stop at one lamppost. We can view this infinite street as the number line and index the lampposts with integers. Thus each element of the lamplighter group $\mathcal{L}$ is determined by a finite set of integers (corresponding to the illuminated lamps) and a single integer corresponding to the final position of the lamplighter. An example of such element is shown in Figure 9 where the illuminated lamps are those indexed with $-2, -1, 2$ and 3 and the lamplighter stands at the lamp indexed with 1. This interpretation of the elements of the lamplighter group was initially given by Jim Cannon.

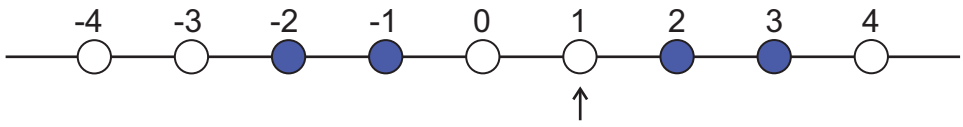

Figure 9.: An element of the lamplighter group

We can use the elements of the cyclic group $\mathbb{Z}/2\mathbb{Z}$ to refer to the two different states of a lamp. We simply let 0 indicate a lamp turned off and 1 indicate a lamp turned on. To list illuminated lamps corresponding to a certain element g of $\mathcal{L}$, we use the infinite direct sum $\oplus_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z})$ where each element in $\oplus_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z})$ has only finitely many nonzero entries indicating the illuminating lamps of g. Now we can set the underlying set of $\mathcal{L}$ as the direct product of $\oplus_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z})$ and $\mathbb{Z}$ where the first component lists illuminated lamps using an element of $\oplus_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z})$ and the second component determines the final position of the lamplighter

determined by an integer.

To create an element of $\mathcal{L}$ we need two actions which will be taken as the generators of the group. First the lamplighter must be able to move one step in either direction. Second the lamplighter must be able to change the state of the lamp at which it stands, that is, turn it on (off) if it is off (on). Let us formally define multiplication in $\mathcal{L}$ as follows. Let $l_1 = ((x_i), n)$ and $l_2 = ((y_i), m)$ be elements of $\mathcal{L}$, then

$$l_1 l_2 = ((z_i), n + m) \tag{4.1}$$

where $z_i = x_i + y_{i-n}$. It is easy to check that $e = (\mathbf{0}, 0)$, where $\mathbf{0}$ is the element of $\oplus_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z})$ whose entries are all zeros, is the identity of the group. The configuration of e is depicted in Figure 10. Let $t = (\mathbf{0}, 1)$ and $a = ((a_i), 0)$, where (a_i) has only one nonzero entry indexed with 0. Then multiplying an element $((x_i), n)$ by t from the right gives $((x_i), n+1)$, i.e. only the lamplighter is shifted one unit to the right. Also multiplying $((x_i), n)$ by a from the right gives $((x_i'), n)$, where $x_i' = x_i$ for all values of i except $i = n$, i.e. only the state of the lamp indexed with n is changed. The configurations of t and a are shown in Figure 11.

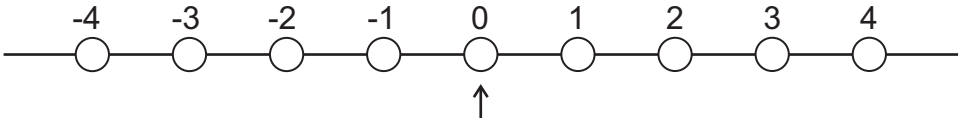

Figure 10.: The Identity of the lamplighter group

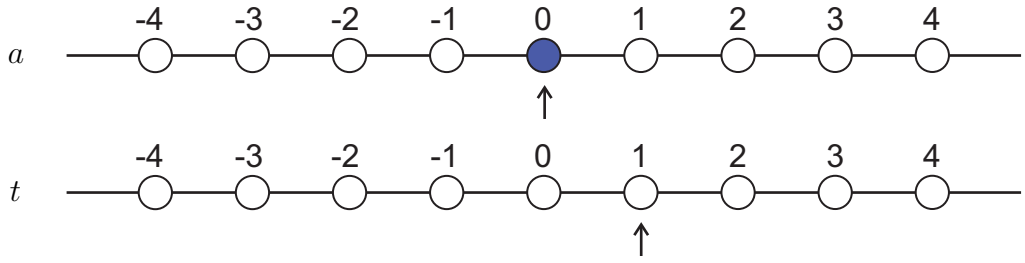

Figure 11.: The Generators of the lamplighter group

We can easily see that $a^2 = e$, i.e. a has order 2 and that t has an infinite order. So every

element in $\mathcal{L}$ can be written as a finite product in a, t and t^{-1}. For example the element shown in Figure 9 can be written as $t^2atat^{-4}at^{-1}at^3$. Actually to create this element, we start with e and do the following steps:

- Move two units to the right (given by t^2)
- Illuminate the lamp at 2 (given by a)
- Move one unit to the right (given by t)
- Illuminate the lamp at 3 (given by a)
- Move four units to the left (given by t^{-4})
- Illuminate the lamp at -1 (given by a)
- Move one unit to the left (given by t^{-1})
- Illuminate the lamp at -2 (given by a)
- Move three units to the right (given by t^3) to end at 1

Notice that in the expression $t^2atat^{-4}at^{-1}at^3$, each appearance of a indicates changing the state of the lamp indexed with λ where λ is the sum of the powers of t preceding this appearance of a.

We claim that the lamplighter group is given by the presentation

$$\mathcal{L} = \langle a, t \mid a^2, [a^{t^j}, a^{t^k}] \text{ for all } j, k \in \mathbb{Z} \rangle,$$

where $[x, y] = xyx^{-1}y^{-1}$ is the commutator of x and y and $a^x = x^{-1}ax$ is the conjugate of a by x. The relation a^2 is immediate. To show that $[a^{t^j}, a^{t^k}] = e$ for all $j, k \in \mathbb{Z}$, we give the following informal explanation. We start with e, move j units to the left, illuminate the lamp indexed with j and return to the origin (that is $t^{-j}at^j$). Then move k units to the left, illuminate the lamp indexed with k and return to the origin (that is $t^{-k}at^k$). The configuration we get (lamps indexed with j and k illuminated and the lamplighter stands at

0) can be also obtained by reversing the last two walks, i.e. the elements $t^{-j}at^j$ and $t^{-k}at^k$ commute. We will not prove here that these are the only relations of the group. Still we give a hint to this proof. For an element of $\mathcal{L}$ written as a product in a, t and t^{-1} to be trivial, it has to satisfy the following two conditions. First the sum of the powers of t has to be zero. Second for each appearance of a preceded by powers of t with sum λ there must be another appearance of a preceded by powers of t with sum $-\lambda$. The first condition guarantees that the final position of the lamplighter is at 0 and the second condition guarantees that all the lamps are off.

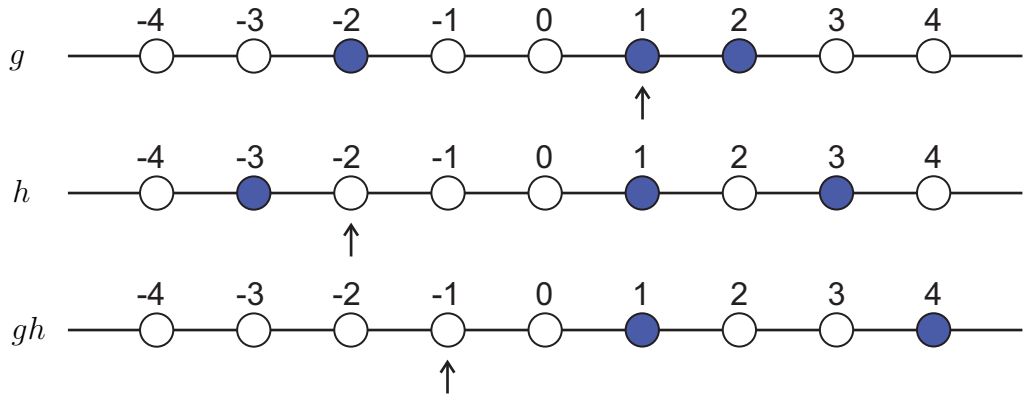

Figure 12.: Product of two elements in $\mathcal{L}$

In Figure 12 the product of two elements g and h in the group $\mathcal{L}$ is shown. This product can be obtained using equation (4.1). Alternatively, we can write $g = t^{-2}at^3atat^{-1}$ and $h = t^{-3}at^4at^2at^{-5}$. So we obtain

$$gh = t^{-2}at^3atat^{-1}t^{-3}at^4at^2at^{-5} = t^{-2}at^3atat^{-4}at^4at^2at^{-5} =$$

$$(t^{-2}at^2)(tat^{-1})(t^2at^{-2})(t^{-2}at^2)(t^2at^{-2})(t^4at^{-4})t^{-1} =$$

$$(tat^{-1})(t^4at^{-4})t^{-1} = tat^3at^{-5}$$

where we have used the fact that conjugates of a by the powers of t commute.

Equation (4.1) means that the lamplighter group $\mathcal{L}$ is defined as the restricted wreath product $(\mathbb{Z}/2\mathbb{Z})\wr\mathbb{Z}$ or, equivalently, as $\oplus_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z})\rtimes\mathbb{Z}$, where $\mathbb{Z}$ acts on $\oplus_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z})$ by shifting

the index. More generally, higher rank lamplighter groups $\mathcal{L}_{n,d}$ are defined similarly as $(\mathbb{Z}/d\mathbb{Z})^n \wr \mathbb{Z}$. To understand the structure of the group $(\mathbb{Z}/d\mathbb{Z})^n \wr \mathbb{Z}$, we again consider an infinite street lined with lampposts indexed with integers. A lamplighter can move along the street and change the states of lamps. Here each lamp has d^n different states corresponding to the elements of $(\mathbb{Z}/d\mathbb{Z})^n$. The group $\mathcal{L}$ we introduced in this section is actually the group $\mathcal{L}_{1,2}$. In the next section we will be interested in the group $\mathcal{L}_{2,2}$ which is defined similarly to $\mathcal{L}$ with the difference in the "brightness" settings of the lamps. Namely, in this group every lamp can have a brightness (or color) from the Klein group $(\mathbb{Z}/2\mathbb{Z})^2$. In other words, $\mathcal{L}_{2,2}$ is isomorphic to $\oplus_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}$ and has the presentation

$$\mathcal{L}_{2,2} = \langle a, b, t \mid a^2, b^2, (ab)^2, [x^{t^j}, y^{t^k}] \text{ for all } j, k \in \mathbb{Z}, x, y \in \{a, b\}\rangle.$$

4.4 The Structure of Group $\mathcal{G}$

In this section we will study the structure of the group $\mathcal{G}$ generated by the 4-state automaton $\mathcal{A}$ whose Moore diagram is shown in Figure 13. We will show that $\mathcal{G}$ is isomorphic to the rank 2 *lamplighter* group $\mathcal{L}_{2,2} \cong (\mathbb{Z}/2\mathbb{Z})^2 \wr \mathbb{Z}$. For that, we use the technique similar to the one developed in [SS16]. We also use a `GAP` package `Automgrp` [MS16] to perform and check most of the calculations here.

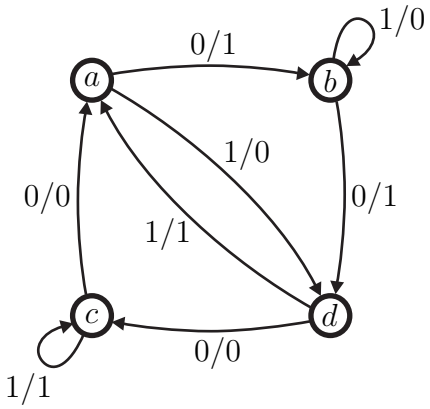

Figure 13.: The Automaton $\mathcal{A}$ generating the group $\mathcal{G}$.

Before we go to investigate the structure of $\mathcal{G}$, we emphasize that the automaton $\mathcal{A}$ gen-

erating $\mathcal{G}$ is bireversible.

Proposition 4.4.1. *The automaton $\mathcal{A}$ shown in Figure 13 generating the group $\mathcal{G}$ is bireversible.*

Proof. By construction the automaton $\mathcal{A}$ is invertible and its dual $\partial\mathcal{A}$ is given by the wreath recursion

$$\begin{aligned} \mathbb{O} &= (\mathbb{1},\mathbb{1},\mathbb{O},\mathbb{O})(abdc), \\ \mathbb{1} &= (\mathbb{O},\mathbb{O},\mathbb{1},\mathbb{1})(ad). \end{aligned}$$

So $\partial\mathcal{A}$ is invertible and $\mathcal{A}$ is reversible. Similarly one can check that the dual of $\mathcal{A}^{-1}$ is also invertible. Therefore, $\mathcal{A}$ is a bireversible automaton. □

The wreath recursion of $\mathcal{G}$ is given by:

$$\begin{aligned} a &= (b,d)\sigma, \\ b &= (d,b)\sigma, \\ c &= (a,c), \\ d &= (c,a). \end{aligned}$$

Let us put $x = ab^{-1}$, $y = ac^{-1}$ and $z = ad^{-1}$. It is straightforward to verify that the subgroup $\langle x,y,z\rangle$ is isomorphic to the 4-element Klein group $(\mathbb{Z}/2\mathbb{Z})^2$. In particular, we have $y = xz = zx$ and $x^2 = z^2 = 1$ (so $x^{-1} = x$ and $z^{-1} = z$). Therefore, $\mathcal{G} = \langle x,z,a\rangle$.

Observe, that the following relations hold in $\mathcal{G}$:

$$\begin{aligned} x &= ab^{-1} = ba^{-1} = dc^{-1} = cd^{-1}, \\ y &= ac^{-1} = ca^{-1} = bd^{-1} = db^{-1}, \\ z &= ad^{-1} = da^{-1} = bc^{-1} = cb^{-1}. \end{aligned} \tag{4.2}$$

The GAP calculations done so far are listed below.

```
gap> G := AutomatonGroup("a=(b,d)(1,2), b=(d,b)(1,2), c=(a,c), d=(c,a)");
< a, b, c, d >
gap> x := a*b^-1;; y := a*c^-1;; z := a*d^-1;;
gap> StructureDescription(Group([x,y,z]));
```

```
"C2 x C2"


gap> FindGroupRelations(G, 2);
(b*a^-1)^2
b*c^-1*d*a^-1
b*d^-1*c*a^-1
(c*a^-1)^2
c*b^-1*d*a^-1
c*d^-1*b*a^-1
(d*a^-1)^2
d*b^-1*c*a^-1
d*c^-1*b*a^-1
[ (b*a^-1)^2, b*c^-1*d*a^-1, b*d^-1*c*a^-1, (c*a^-1)^2, c*b^-1*d*a^-1,
  c*d^-1*b*a^-1, (d*a^-1)^2, d*b^-1*c*a^-1, d*c^-1*b*a^-1 ]
gap>
```

Since $x = ab^{-1} = (bd^{-1}, db^{-1})$, $y = ac^{-1} = (bc^{-1}, da^{-1})\sigma$, $z = ad^{-1} = (ba^{-1}, dc^{-1})\sigma$, using relations (4.2) and the notation introduced in the Section 4.1, we obtain

$$x = y^{(1)}, \quad y = z^{(1)}\sigma, \quad z = x^{(1)}\sigma.$$

So $x, y, z \in \mathrm{SHAut}(X^*)$.

Lemma 4.4.2. *The automorphism a lies in the normalizer of the group* $\mathrm{SHAut}(X^*)$.

Proof. Since $\Delta = \langle \sigma^{(0)}, \sigma^{(1)}, \ldots \rangle$ is dense in $\mathrm{SHAut}(X^*)$ in the case of binary tree, it suffices to show that $(\sigma^{(n)})^a, (\sigma^{(n)})^{a^{-1}} \in \mathrm{SHAut}(X^*)$ for $n = 0, 1, \ldots$ Direct calculations give

$$\begin{aligned}
&(\sigma^{(0)})^a = (d^{-1}, b^{-1})\sigma(1,1)\sigma(b,d)\sigma = (d^{-1}b, b^{-1}d)\sigma,\\
&d^{-1}b = b^{-1}d,\\
&d^{-1}b = (c^{-1}d, a^{-1}b)\sigma,\\
&c^{-1}d = a^{-1}b,\\
&c^{-1}d = (a^{-1}c, c^{-1}a).
\end{aligned}$$

Therefore, using again relations (4.2) we obtain $(\sigma^{(0)})^a \in \mathrm{SHAut}(X^*)$. It follows also by direct calculations that

$$\begin{aligned}(\sigma^{(n+1)})^a &= ((\sigma^{(n)})^d, (\sigma^{(n)})^b),\\ (\sigma^{(n+1)})^b &= ((\sigma^{(n)})^b, (\sigma^{(n)})^d),\\ (\sigma^{(n+1)})^c &= ((\sigma^{(n)})^a, (\sigma^{(n)})^c),\\ (\sigma^{(n+1)})^d &= ((\sigma^{(n)})^c, (\sigma^{(n)})^a)\end{aligned} \tag{4.3}$$

for $n = 0, 1, \ldots$. We claim that $(\sigma^{(n)})^a = (\sigma^{(n)})^b = (\sigma^{(n)})^c = (\sigma^{(n)})^d$ for $n = 0, 1, \ldots$. This can be proved by induction on n as follows. We have

$$\begin{aligned}(\sigma^{(0)})^a &= (d^{-1}, b^{-1})\sigma(1,1)\sigma(b,d)\sigma = (d^{-1}b, b^{-1}d)\sigma,\\ (\sigma^{(0)})^b &= (b^{-1}, d^{-1})\sigma(1,1)\sigma(d,b)\sigma = (b^{-1}d, d^{-1}b)\sigma,\\ (\sigma^{(0)})^c &= (a^{-1}, c^{-1})(1,1)\sigma(a,c) = (a^{-1}c, c^{-1}a)\sigma,\\ (\sigma^{(0)})^d &= (c^{-1}, a^{-1})(1,1)\sigma(c,a) = (c^{-1}a, a^{-1}c)\sigma.\end{aligned}$$

Hence $(\sigma^{(0)})^a = (\sigma^{(0)})^b = (\sigma^{(0)})^c = (\sigma^{(0)})^d$. Now equations (4.3) prove our claim. It follows immediately that $(\sigma^{(n)})^a \in \mathrm{SHAut}(X^*)$ for $n = 1, 2, \ldots$ Similarly we can show that $(\sigma^{(n)})^{a^{-1}} \in \mathrm{SHAut}(X^*)$ for $n = 0, 1, \ldots$ □

Lemma 4.4.2 together with Theorem 4.2.2 give the following corollary.

Corollary 4.4.3. *The automorphism a lies in $\mathrm{Aff}(X^*)$ and is equal to $\pi_{A,\mathbf{b}}$ for the matrix A with the i-th row $\mathbf{a}_i = [0^{i-1}, 1, (1,0)^\infty]$ (depicted in Figure 14) and $\mathbf{b} = [(1,1,0,0)^\infty]$.*

Proof. We can easily find $\mathbf{b}$ by computing $\mathbf{b} = \mathbf{b} + [0,0,0,\ldots] \cdot A = \pi_{A,\mathbf{b}}(0^\infty) = a(0^\infty)$. Let $\mathbf{e}_i = [0, 0, \ldots, 0, 1, 0, \ldots]$ be the i-th standard basis vector in $(\mathbb{Z}/2\mathbb{Z})^\infty$. Then we can compute the i-th row $\mathbf{a}_i$ of matrix A as follows. Since $a(\mathbf{e}_i) = \mathbf{b} + \mathbf{e}_i \cdot A = \mathbf{b} + \mathbf{a}_i$, we obtain $\mathbf{a}_i = a(\mathbf{e}_i) - \mathbf{b}$. We leave the computations for the reader as an exercise. □

As immediate corollary, we obtain the following theorem.

Theorem 4.4.4. *The generators a, b, c and d of $\mathcal{G}$ all lie in $\mathrm{Aff}_{[[t]]}(X^*)$ and are induced by the affine transformations of the form*

$$\begin{aligned}a &= \tau_{\frac{t^2+t+1}{t^2+1}, \frac{1}{(t+1)^3}}, \qquad & b &= \tau_{\frac{t^2+t+1}{t^2+1}, \frac{t^2+t+1}{(t+1)^3}},\\ c &= \tau_{\frac{t^2+t+1}{t^2+1}, \frac{t}{(t+1)^3}}, \qquad & d &= \tau_{\frac{t^2+t+1}{t^2+1}, \frac{t^2}{(t+1)^3}}.\end{aligned}$$

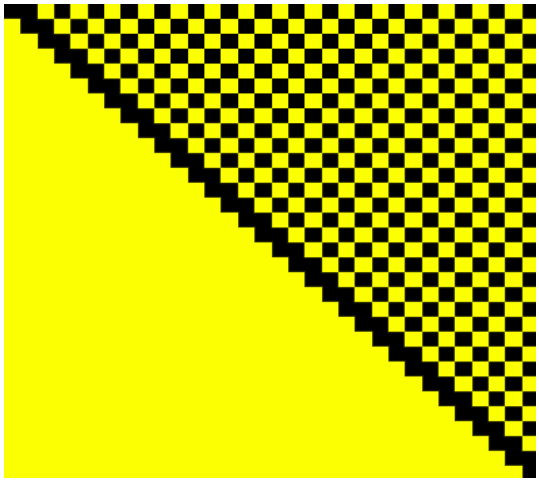

Figure 14.: A 32×32 minor of the matrix A corresponding to the affine automorphism a.

Proof. By Proposition 4.2.1, we obtain $a \in \mathrm{Aff}_{[[t]]}(X^*)$ with

$$f = 1 + t + t^3 + t^5 + \cdots = 1 + t(1 + t^2 + t^4 + \cdots) = 1 + \frac{t}{1+t^2} = \frac{t^2+t+1}{t^2+1},$$

and

$$\begin{aligned} g &= 1 + t + t^4 + t^5 + t^8 + t^9 + \cdots \\ &= (1 + t^4 + t^8 + \cdots) + t(1 + t^4 + t^8 + \cdots) = \frac{1+t}{1+t^4} = \frac{1}{(t+1)^3}, \end{aligned}$$

where for simplification in the last step we used the fact that calculations are performed in $\mathbb{Z}/2\mathbb{Z}$. By Corollary 2.6 in [SS16], we can find the section of an affine automorphism $\tau_{f,g}$ at a vertex $x \in X$ via the formula

$$\tau_{f,g}|_x = \tau_{f, x\sigma(f)+\sigma(g)},$$

where $\sigma(c_0 + c_1 t + c_2 t^2 + \cdots) = c_1 + c_2 t + c_3 t^2 + \cdots$ for every formal power series $c_0 + c_1 t + c_2 t^2 + \cdots$. Using this formula, we can find the transformations inducing the automorphisms b, c and d, where $b = a|_0$, $d = a|_1$ and $c = d|_0$. □

By Lemma 4.4.2, conjugates of any spherically homogeneous element $s \in \mathrm{SHAut}(X^*)$ by powers (possibly negative) of a are also spherically homogeneous, and hence commute.

Therefore the following notation is well-defined for any $i_j \in \mathbb{Z}$:

$$s^{a^{i_1}+a^{i_2}+\cdots+a^{i_n}} := s^{a^{i_1}} s^{a^{i_2}} \cdots s^{a^{i_n}}.$$

In particular, for each Laurent polynomial $p(a) \in (\mathbb{Z}/2\mathbb{Z})[a, a^{-1}]$ the elements $x^{p(a)}$ and $z^{p(a)}$ are defined. To show that $\langle x, z, a\rangle$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2 \wr \mathbb{Z}$ it suffices to show that for each pair of Laurent polynomials $p(a)$ and $q(a)$ not both trivial, the element $x^{p(a)}z^{q(a)}$ of $\mathcal{G}$ is nontrivial. Actually, if it happens that for a pair of Laurent polynomials $p(a)$ and $q(a)$ we have $x^{p(a)}z^{q(a)} = 1$, conjugating the last equation by a large enough power of a gives $x^{\tilde{p}(a)}z^{\tilde{q}(a)} = 1$ for some $\tilde{p}, \tilde{q} \in (\mathbb{Z}/2\mathbb{Z})[a]$. Therefore, it is enough to show that for each pair of polynomials $p, q \in (\mathbb{Z}/2\mathbb{Z})[a]$ not both trivial $x^{p(a)}z^{q(a)}$ is a nontrivial element of $\mathcal{G}$. The proof of this fact will be based on the following lemmas.

Lemma 4.4.5. *For any pair of polynomials $p, q \in (\mathbb{Z}/2\mathbb{Z})[a]$, we have*

$$((x^{p(a)}z^{q(a)})^{(1)})^a = (x^{p(a)a}z^{q(a)a})^{(1)},$$
$$((x^{p(a)}z^{q(a)})^{(1)}\sigma)^a = (x^{p(a)a+a}z^{q(a)a+a})^{(1)}\sigma.$$

Proof. We can write $a = (x^{-1}, z^{-1})(a, a)\sigma = (x, z)(a, a)\sigma$ and $a^{-1} = (z^a, x^a)(a^{-1}, a^{-1})\sigma$. Then using the fact that conjugates of x and z by powers of a commute and that $x^2 = z^2 = 1$, we obtain

$$((x^{p(a)}z^{q(a)})^{(1)})^a = (z^a, x^a)(a^{-1}, a^{-1})\sigma(x^{p(a)}z^{q(a)})^{(1)}(x, z)(a, a)\sigma =$$
$$(a^{-1}zx^{p(a)}z^{q(a)}za, a^{-1}xx^{p(a)}z^{q(a)}xa) = (a^{-1}x^{p(a)}z^{q(a)}a)^{(1)} = (x^{p(a)a}z^{q(a)a})^{(1)}$$

and

$$((x^{p(a)}z^{q(a)})^{(1)}\sigma)^a = (z^a, x^a)(a^{-1}, a^{-1})\sigma(x^{p(a)}z^{q(a)})^{(1)}\sigma(x, z)(a, a)\sigma =$$
$$(a^{-1}zx^{p(a)}z^{q(a)}xa, a^{-1}xx^{p(a)}z^{q(a)}za)\sigma = (a^{-1}x^{p(a)+1}z^{q(a)+1}a)^{(1)}\sigma = (x^{p(a)a+a}z^{q(a)a+a})^{(1)}\sigma$$

□

Lemma 4.4.6. *For each $n \geq 0$, we have $x^{a^n} = (x^{a^n}z^{a^n})^{(1)}$ and*

$$z^{a^n} = \begin{cases} (x)^{(1)}\sigma, & n = 0, \\ (z^a)^{(1)}\sigma, & n = 1, \\ (x^{a+a^2+\cdots+a^{n-1}}z^{a+a^2+\cdots+a^n})^{(1)}\sigma, & n > 1. \end{cases}$$

Proof. For $n = 0$ we have $x = x^{a^0} = (y)^{(1)} = (xz)^{(1)}$ and $z = z^{a^0} = (x)^{(1)}\sigma$. Using induction on n from Lemma 4.4.5, we immediately reach the statement of the lemma. □

Let us define

$$\phi_n(a) = \begin{cases} 0 & n = 0 \\ a + a^2 + \cdots + a^n & n > 0 \end{cases}$$

For each polynomial $q(a) = \sum_{i=0}^{n} c_i a^i \in (\mathbb{Z}/2\mathbb{Z})[a]$ we define

$$\psi_q(a) = \sum_{i=1}^{n} c_i \phi_{i-1}(a).$$

Lemma 4.4.7. *The functions ϕ_n and ψ_q have the following properties:*

(i) For each $n \geq 1$, we have $\phi_n(a) = a\phi_{n-1}(a) + a$.

(ii) If $\deg q \leq 1$, then $\psi_q = 0$.

(iii) If $\deg q \geq 2$, then $\deg \psi_q = \deg q - 1$.

(iv) The function ψ_q is linear in q.

Proof. The proof is straightforward and we leave it to the reader as an easy exercise. □

Lemma 4.4.8. *For each pair of polynomials $p, q \in (\mathbb{Z}/2\mathbb{Z})[a]$, the section of $x^{p(a)}z^{q(a)}$ at each vertex of the first level is $x^{p(a)+\psi_q(a)+q(0)}z^{p(a)+a\psi_q(a)+aq(1)+aq(0)}$.*

Proof. Assume $q(a) = \sum_{i=0}^{n} c_i a^i$. Then using the definition of the function ψ_q together with Lemma 4.4.6, we obtain the section of $z^{q(a)}$ at each vertex of the first level (say $z^{q(a)}|_0$) as

$$z^{q(a)}|_0 = \begin{cases} x^{c_1\phi_0(a)+c_2\phi_1(a)+\cdots+c_n\phi_{n-1}(a)}z^{c_1\phi_1(a)+c_2\phi_2(a)+\cdots+c_n\phi_n(a)}, & c_0 = 0, \\ x^{1+c_1\phi_0(a)+c_2\phi_1(a)+\cdots+c_n\phi_{n-1}(a)}z^{c_1\phi_1(a)+c_2\phi_2(a)+\cdots+c_n\phi_n(a)}, & c_0 = 1 \end{cases}$$

$$= \begin{cases} x^{\psi_q(a)}z^{a\psi_q(a)+a(c_1+c_2+\cdots+c_n)}, & c_0 = 0, \\ x^{1+\psi_q(a)}z^{a\psi_q(a)+a(c_1+c_2+\cdots+c_n)}, & c_0 = 1, \end{cases}$$

$$= x^{q(0)+\psi_q(a)}z^{a\psi_q(a)+a(q(1)-q(0))} = x^{q(0)+\psi_q(a)}z^{a\psi_q(a)+aq(1)+aq(0)},$$

where we have used Lemma 4.4.7(i) and the fact that $-1 = 1$ in $\mathbb{Z}/2\mathbb{Z}$. It is obvious from Lemma 4.4.6 that $x^{p(a)}|_0 = x^{p(a)}z^{p(a)}$. Now the statement of the lemma follows immediately from the fact that $x^{p(a)}z^{q(a)}$ is spherically homogeneous. □

Remark 4.4.9. Since z acts nontrivially on the first level, it is clear that the action of $z^{q(a)}$ on the first level is trivial if and only if $q(a)$ has an even number of terms which, in the case of $\mathbb{Z}/2\mathbb{Z}$, is equivalent to $q(1) = 0$. In other words, $z^{q(a)} = (x^{q(0)+\psi_q(a)} z^{a\psi_q(a)+aq(0)})^{(1)}$ if $q(1) = 0$ and $z^{q(a)} = (x^{q(0)+\psi_q(a)} z^{a\psi_q(a)+a+aq(0)})^{(1)}\sigma$ if $q(1) = 1$.

To simplify our notation, we will denote $x^{p(a)} z^{q(a)}$ by (p, q) for each pair of polynomials $p, q \in (\mathbb{Z}/2\mathbb{Z})[a]$. To say that the section of $x^{p(a)} z^{q(a)}$ at each vertex of the first level is $x^{p'(a)} z^{q'(a)}$, we use the notation $(p, q) \to (p', q')$. According to Lemma 4.4.8, we have $p' = p + \psi_q + q(0)$ and $q' = p + a\psi_q + aq(1) + aq(0)$.

Before we prove our main theorem, we need to introduce a remark and a lemma.

Remark 4.4.10. The leading coefficient of any nonzero polynomial in $(\mathbb{Z}/2\mathbb{Z})[a]$ is 1. So when we add two polynomials of the same degree, say n, the degree of the sum is less than n.

Lemma 4.4.11. *Let $q(a)$ be a polynomial in $(\mathbb{Z}/2\mathbb{Z})[a]$ with degree at least 2. Then* $\deg(\psi_q + \psi_{a\psi_q}) = \deg q - 2$.

Proof. Let $q(a) = c_0 + c_1 a + \cdots + c_n a^n$ with $n \geq 2$ and $c_n \neq 0$. Then

$$\psi_q(a) = a(c_2 + c_3 + \cdots + c_n) + a^2(c_3 + c_4 + \cdots + c_n) + \cdots + a^{n-2}(c_{n-1} + c_n) + a^{n-1}c_n.$$

Hence

$$a\psi_q(a) = a^2(c_2 + c_3 + \cdots + c_n) + a^3(c_3 + c_4 + \cdots + c_n) + \cdots + a^{n-1}(c_{n-1} + c_n) + a^n c_n.$$

So

$$\psi_{a\psi_q}(a) = a(c_2 + 2c_3 + 3c_4 + \cdots + (n-1)c_n) + a^2(c_3 + 2c_4 + 3c_5 + \cdots + (n-2)c_n) + \cdots$$

$$+a^{n-2}(c_{n-1} + 2c_n) + a^{n-1}c_n.$$

We finally obtain

$$\psi_q(a) + \psi_{a\psi_q}(a) = a(2c_2 + 3c_3 + \cdots + nc_n) + a^2(2c_3 + 3c_4 + \cdots + (n-1)c_n) + \cdots$$

$$+a^{n-2}(2c_{n-1}+3c_n)+a^{n-1}(2c_n)$$

$$=a(2c_2+3c_3+\cdots+nc_n)+a^2(2c_3+3c_4+\cdots+(n-1)c_n)+\cdots+a^{n-2}c_n.$$

Therefore, $\deg(\psi_q+\psi_{a\psi_q})=n-2=\deg q-2$. □

We are now ready to prove our main theorem.

Theorem 4.4.12. *The group $\mathcal{G}=\langle a=(b,d)\sigma, b=(d,b)\sigma, c=(a,c), d=(c,a)\rangle$ is isomorphic to the rank 2 lamplighter group $(\mathbb{Z}/2\mathbb{Z})^2\wr\mathbb{Z}$.*

Proof. From the paragraph preceding Lemma 4.4.5, we only need to show that for each pair of polynomials $p,q\in(\mathbb{Z}/2\mathbb{Z})[a]$ not both trivial the expression $x^{p(a)}z^{q(a)}$ is nontrivial. We will assume the theorem is incorrect and prove it by contradiction as follows. We pick two polynomials $p,q\in(\mathbb{Z}/2\mathbb{Z})[a]$ such that $x^{p(a)}z^{q(a)}$ is trivial with $\max\{\deg p,\deg q\}$ minimal. We will find a pair of polynomials $\tilde{p},\tilde{q}\in(\mathbb{Z}/2\mathbb{Z})[a]$ such that $x^{\tilde{p}}z^{\tilde{q}}$ is trivial and $\max\{\deg\tilde{p},\deg\tilde{q}\}<\max\{\deg p,\deg q\}$. To find these two polynomials, we use the fact that all the states of the trivial automorphism are trivial and so is the product of any two of them.

Using the notation introduced above, we start with a pair (p,q) corresponding to the trivial element of $\mathcal{G}$ with $\deg p=m$ and $\deg q=n$ such that $\max\{m,n\}$ is minimal. So $(p,q)\to(p',q')$ where

$$p'=p+\psi_q+q(0)\quad\text{and}\quad q'=p+a\psi_q+aq(0)$$

(Note that $q(1)=0$ by Remark 4.4.9). We consider four cases of what can happen with the degrees of polynomials and analyze the dynamics that arises when we compute the sections of corresponding elements.

Case I. $m>n$.

Using Lemma 4.4.7(iii), we obtain $\deg p'=\deg q'=m$, which constitutes Case II.

Case II. $m=n$.

If $m=n\leq 1$, then $\psi_q=0$. In such a case, we have only six values of the expression $x^{p(a)}z^{q(a)}$ to consider, namely $x^{a+1},x^a,x,x^{a+1}z^{a+1},x^az^{a+1}$ and xz^{a+1}, which are all nontrivial (keep in

mind that $q(1) = 0$). So we will assume in Case II that $m \geq 2$ (and also in Case I since we have checked all possible occurrences). Hence by Lemma 4.4.7(iii) and Remark 4.4.10, we have $\deg p' = m$ and $\deg q' < m$. Therefore we get back to Case I (which does not yet finish the proof, of course).

Case III. $m = n - 1$.

If $n = 1$ and $m = 0$, we have only two values of the expression $x^{p(a)}z^{q(a)}$ to consider, namely z^{a+1} and xz^{a+1} which are both nontrivial. So we will assume in Case III that $n \geq 2$. Hence again by Lemma 4.4.7(iii) and Remark 4.4.10, we have $\deg p' < n - 1$ and $\deg q' = n$, thus bringing us to Case IV.

Case IV. $m < n - 1$.

Here we always have $n \geq 2$. We obtain $\deg p' = n - 1$ and $\deg q' = n$. Which again brings us to Case III.

Let (p'', q'') be the state of (p, q) at any vertex of the second level (they are all equal), i.e. $(p, q) \to (p', q') \to (p'', q'')$. We claim that in Case I and Case IV above, $(p + p'', q + q'')$ is trivial (this is immediate) with $\max\{\deg(p + p''), \deg(q + q'')\} < \max\{\deg p, \deg q\}$ and the two polynomials $p + p''$ and $q + q''$ are not both trivial (we will show only that $p + p''$ is nontrivial). Since Case I leads to Case II in the first level and vice versa, and the same thing happens with Case III and Case IV, it is enough to consider only Case I and Case IV.

The polynomial p'' can be easily computed using Lemma 4.4.7(ii),(iv) and it is equal to

$$\begin{aligned} p'' = p' + \psi_{q'} + q'(0) &= (p + \psi_q + q(0)) + \psi_{p+a\psi_q+aq(0)} + p(0) \\ &= (p + \psi_q + q(0)) + \psi_p + \psi_{a\psi_q} + p(0) = p + \psi_q + \psi_p + \psi_{a\psi_q} + q(0) + p(0) \end{aligned}$$

and thus

$$p + p'' = \psi_q + \psi_p + \psi_{a\psi_q} + q(0) + p(0).$$

In Case I, we have $\deg q, \deg q'' < m$ so $\deg(q + q'') < m$. By Lemma 4.4.7(iii), $\deg(p + p'') = m - 1 < m$. Since $m \geq 2$, the polynomial $p + p''$ is nontrivial.

In Case IV, $\deg q = \deg q'' = n$. Hence by Remark 4.4.10, $\deg(q + q'') < n$. By Lemma 4.4.11, $\deg(p + p'') = n - 2 < n$. For $n \geq 3$, the polynomial $p + p''$ is nontrivial. We still have to check the case when $n = 2$ and $m = 0$ (keeping in mind that $q(1) = 0$).

There are four values of the expression $x^{p(a)}z^{q(a)}$ to consider, namely $x^{a^2}, x^{a^2+a}, x^{a^2+1}, x^{a^2+a+1}$, which are all nontrivial. The proof is now complete. □

The GAP calculations done through the proof of 4.4.12 are listed below.

```
gap> L1 := [x^a*x,x^a,x^a*x*z^a*z,x^a*z^a*z,x*z^a*z];
[ b^-1*a^2*b^-1, b^-1*a, b^-1*a^2*b^-1*d^-1*a^2*d^-1, b^-1*a*d^-1*a^2*d^-1,
  a*b^-1*d^-1*a^2*d^-1 ]
gap> List (L1, g -> IsOne(g));
[ false, false, false, false, false ]
gap> L2 := [z^a*z,x*z^a*z];
[ d^-1*a^2*d^-1, a*b^-1*d^-1*a^2*d^-1 ]
gap> List (L2, g -> IsOne(g));
[ false, false ]
gap> L3 := [x^(a^2),x^(a^2)*x^a,x^(a^2)*x,x^(a^2)*x^a*x];
[ a^-1*b^-1*a^2, a^-1*b^-1*a^2*b^-1*a, a^-1*b^-1*a^3*b^-1,
  a^-1*(b^-1*a^2)^2*b^-1 ]
gap> List (L3, g -> IsOne(g));
[ false, false, false, false ]
```

Chapter 5
Conclusions

5.1 Conclusions and Open Problems

In this chapter we summarize the results introduced in this dissertation and state some open problems and possible directions for further investigations.

In Chapter 3 we discussed the problem of level transitivity of permutational polynomials acting on the rooted binary tree. We first introduced a way to identify the n^{th} level of the rooted d-ary tree X^* with the ring $\mathbb{Z}/(d^n\mathbb{Z})$. With this identification, we showed in Proposition 3.2.1 that each polynomial $f(x) \in \mathbb{Z}[x]$ induces an endomorphism of X^*. Since the ring $\mathbb{Z}[x]$ is countable and we have uncountably many endomorphisms of X^*, not every such endomorphism can be induced by a polynomial over $\mathbb{Z}$. So we consider the ring $\mathbb{Z}[[x]]$ of formal power series over $\mathbb{Z}$ which is uncountable. Unlike the case of polynomials, not every formal power series over $\mathbb{Z}$ induces mappings of the levels $\mathbb{Z}/(d^n\mathbb{Z})$ of the tree X^*. This is simply a problem of convergence. We suggest the following necessary and sufficient condition on a formal power series over $\mathbb{Z}$ to induce a mapping of each level of X^* and hence an endomorphism of the whole tree. This condition guarantees a finite output for each vertex of the tree.

Proposition 5.1.1. *A formal power series $F(x) = a_0 + a_1x + a_2x^2 + \cdots \in \mathbb{Z}[[x]]$ induces an endomorphism of the rooted d-ary tree X^* if and only if $\lim_{n\to\infty} |a_n|_d = 0$, where $|a_n|_d$ is the d-adic norm of a_n.*

The endomorphisms induced by power series over $\mathbb{Z}$ with converging to zero in d-adic norm coefficients constitute a natural generalization of the endomorphisms induced by polynomials. For example, Theorem 3.2.3 about the sections of corresponding endomorphisms,

and Rivest's theorem 3.2.11 have natural extensions to this wider class. On the other hand, many basic questions still remain widely open. Below we list some of them.

Question 5.1.2. *Consider a random endomorphism ϕ of the regular rooted tree X^*. Can it be induced by a formal power series over $\mathbb{Z}$?*

In Proposition 3.2.9 we showed that for each $d \geq 2$, the set of all d-permutational polynomials forms a cancellative monoid under the operation of composition. Although the inverse of an automorphism induced by a d-permutational polynomial $f(x) \in \mathbb{Z}[x]$ always exists, it cannot be induced by a polynomial over $\mathbb{Z}$ unless f is linear. The following open question naturally arises.

Question 5.1.3. *Let ϕ be an automorphism of the regular rooted tree X^* induced by a polynomial $f(x) \in \mathbb{Z}[x]$. When can ϕ^{-1} be induced by a formal power series over $\mathbb{Z}$? and how can we compute the coefficients of this formal power series if it does exist?*

In Theorem 3.2.3 we derived a formula to evaluate the sections of an endomorphism of X^* induced by a polynomial over $\mathbb{Z}$ which turned out to be again polynomials of the same degree. Proposition 3.2.5 asserts that the only polynomials in $\mathbb{Z}[x]$ that induce finite-state endomorphisms of X^* are linear polynomials. Also Proposition 3.2.6 asserts that the only polynomials in $\mathbb{Z}[x]$ that induce endomorphisms of X^* of polynomial growth are the powers of the adding machine and that all the other polynomials induce endomorphisms of exponential growth.

Theorem 3.2.11 proved by Rivest gives the necessary and sufficient conditions for a polynomial $f(x) \in \mathbb{Z}[x]$ to be 2-permutational. The following two open problems naturally arise.

Problem 5.1.4. *Determine the necessary and sufficient conditions that a polynomial $f(x) \in \mathbb{Z}[x]$ has to meet to be d-permutational for $d > 2$.*

Problem 5.1.5. *Determine the necessary and sufficient conditions that a formal power series over $\mathbb{Z}$ satisfying the condition of Proposition 5.1.1 has to meet to be d-permutational for $d \geq 2$.*

In Theorem 3.3.9 we give the necessary the sufficient conditions that a 2-permutational polynomial has to meet to act level transitively on the rooted binary tree $\{0,1\}^*$. Again we consider two open problems.

Problem 5.1.6. *Determine the necessary and sufficient conditions that a d-permutational polynomial $f(x) \in \mathbb{Z}[x]$ has to meet to act level transitively on the rooted d-ary tree X^* for $d > 2$.*

Problem 5.1.7. *Determine the necessary and sufficient conditions that a d-permutational power series over $\mathbb{Z}$ has to meet to act level transitively on the rooted d-ary tree X^* for $d \geq 2$.*

In fact, Problem 5.1.6 was partially solved by Larin [Lar02b] and Knuth [Knu98] in the case when $f(x)$ is a quadratic polynomial and d is a prime.

In Chapter 4 we studied the structure of the group $\mathcal{G} = \langle a = (b,d)\sigma, b = (d,b)\sigma, c = (a,c), d = (c,a)\rangle$ where we proved in Theorem 4.4.12 that it is isomorphic to the rank 2 lamplighter group $(\mathbb{Z}/2\mathbb{Z})^2 \wr \mathbb{Z}$. The group $\mathcal{G}$ was initially one of the six groups among those generated by 7421 non-minimally symmetric 4-state invertible automata over 2-letter alphabet studied in [Cap14], for which the existence of elements of infinite order could not be easily established by the standard known methods. In [KPS16] many elements of infinite order in two of these six groups were found using a new technique of orbit automata. And in [SS16] the structure of one of them was completely described. There is only one group left with unknown structure, namely the group $\langle a = (b,d)\sigma, b = (d,c)\sigma, c = (c,b)\sigma, d = (a,a)\rangle$. In [Cap14], the following conjecture was suggested. This paves the way to an interesting research project to work on.

Conjecture 5.1.8. *The group $\langle a = (b,d)\sigma, b = (d,c)\sigma, c = (c,b)\sigma, d = (a,a)\rangle$ is isomorphic to the free group F_4 of rank 4 freely generated by $\{a,b,c,d\}$.*

References

[AAV13] Gideon Amir, Omer Angel, and Bálint Virág. Amenability of linear-activity automaton groups. *J. Eur. Math. Soc. (JEMS)*, 15(3):705–730, 2013.

[Adi79] S. I. Adian. *The Burnside problem and identities in groups*, volume 95 of *Ergebnisse der Mathematik und ihrer Grenzgebiete [Results in Mathematics and Related Areas]*. Springer-Verlag, Berlin, 1979.

[Ale72] S. V. Alešin. Finite automata and the Burnside problem for periodic groups. *Mat. Zametki*, 11:319–328, 1972.

[Ana98] V. S. Anashin. Uniformly distributed sequences in computer algebra or how to construct program generators of random numbers. *J. Math. Sci. (New York)*, 89(4):1355–1390, 1998. Computing mathematics and cybernetics, 2.

[Ana02] V. S. Anashin. Uniformly distributed sequences of p-adic integers. *Diskret. Mat.*, 14(4):3–64, 2002.

[Ana06] Vladimir Anashin. Ergodic transformations in the space of p-adic integers. In *p-adic mathematical physics*, volume 826 of *AIP Conf. Proc.*, pages 3–24. Amer. Inst. Phys., Melville, NY, 2006.

[Ana12] V. Anashin. Automata finiteness criterion in terms of van der Put series of automata functions. *p-Adic Numbers Ultrametric Anal. Appl.*, 4(2):151–160, 2012.

[AS17] Elsayed Ahmed and Dmytro Savchuk. Endomorphisms of regular rooted trees induced by the action of polynomials on the ring $\mathbb{Z}_d$ of d-adic integers. Preprint: arxiv:1711.06735, 2017.

[AS18] Elsayed Ahmed and Dmytro Savchuk. The lamplighter group of rank two generated by a bireversible automaton. Preprint: arxiv:1802.03695, 2018.

[Ati76] M. F. Atiyah. Elliptic operators, discrete groups and von Neumann algebras. In *Colloque "Analyse et Topologie" en l'Honneur de Henri Cartan (Orsay, 1974)*, pages 43–72. Astérisque, No. 32–33. Soc. Math. France, Paris, 1976.

[Aus13] Tim Austin. Rational group ring elements with kernels having irrational dimension. *Proc. Lond. Math. Soc. (3)*, 107(6):1424–1448, 2013.

[Bar15] Laurent Bartholdi. *FR – GAP package "Computations with functionally recursive groups", Version 2.2.1*, 2015. (available at *http://www.gap-system.org/Packages/fr.html*).

[BDR16] Ievgen Bondarenko, Daniele D'Angeli, and Emanuele Rodaro. The lamplighter group $\mathbb{Z}_3 \wr \mathbb{Z}$ generated by a bireversible automaton. *Comm. Algebra*, 44(12):5257–5268, 2016.

[BKN10] Laurent Bartholdi, Vadim Kaimanovich, and Volodymyr Nekrashevych. On amenability of automata groups. *Duke Mathematical Journal*, 154(3):575–598, 2010. available at *http://arxiv.org/abs/0802.2837*.

[BM17] Laurent Bartholdi and Ivan Mitrofanov. The word and order problems for self-similar and automata groups. Preprint: arxiv:1710.10109, 2017.

[BOERT96] Hyman Bass, Maria Victoria Otero-Espinar, Daniel Rockmore, and Charles Tresser. *Cyclic renormalization and automorphism groups of rooted trees*, volume 1621 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1996.

[BŠ06] Laurent I. Bartholdi and Zoran Šuniḱ. Some solvable automaton groups. In *Topological and Asymptotic Aspects of Group Theory*, volume 394 of *Contemp. Math.*, pages 11–29. Amer. Math. Soc., Providence, RI, 2006.

[BTZ17] Jérémie Brieussel, Ryokichi Tanaka, and Tianyi Zheng. Random walks on the discrete affine group. Preprint: arxiv:1703.07741, 2017.

[Cap14] Louis Caponi. On Classification of Groups Generated by Automata with 4 States over a 2-Letter Alphabet. Master's thesis, University of South Florida, Department of Mathematics and Statistics, Tampa, FL, 33620, USA, 2014.

[Day57] Mahlon M. Day. Amenable semigroups. *Illinois J. Math.*, 1:509–544, 1957.

[Deh11] M. Dehn. Über unendliche diskontinuierliche Gruppen. *Math. Ann.*, 71(1):116–144, 1911.

[DS02] Warren Dicks and Thomas Schick. The spectral measure of certain elements of the complex group ring of a wreath product. *Geom. Dedicata*, 93:121–137, 2002.

[Eck12] Scott Eckenthal. The lamplighter group, 2012. Bachelor's Thesis, Trinity College of Connecticut.

[Fan15] Ai-Hua Fan. p-adic polynomial dynamics, 2015. `https://cantorsalta2015.sciencesconf.org/conference/cantorsalta2015/Fan.pdf`.

[GAP15] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.7.8*, 2015.

[Gil18] Pierre Gillibert. An automaton group with undecidable order and Engel problems. *J. Algebra*, 497:363–392, 2018.

[GK14] R. Grigorchuk and R. Kravchenko. On the lattice of subgroups of the lamplighter group. *Internat. J. Algebra Comput.*, 24(6):837–877, 2014.

[GL02] Rostislav Grigorchuk and Igor Lysionok. Burnside problem. In Alexander V. Mikhalev and Günter F. Pilz, editors, *The concise handbook of algebra*, pages 111–115. Kluwer Academic Publishers, Dordrecht, 2002.

[GLSŻ00] Rostislav I. Grigorchuk, Peter Linnell, Thomas Schick, and Andrzej Żuk. On a question of Atiyah. *C. R. Acad. Sci. Paris Sér. I Math.*, 331(9):663–668, 2000.

[Glu61] V. M. Glushkov. Abstract theory of automata. *Uspekhi mat. nauk.*, 16(5):3–62, 1961. (in Russian).

[GM05] Yair Glasner and Shahar Mozes. Automata and square complexes. *Geom. Dedicata*, 111:43–64, 2005. (available at *http://arxiv.org/abs/math.GR/0306259*).

[GNS00] 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):134–214, 2000.

[Gol64] E. S. Golod. On nil-algebras and finitely approximable p-groups. *Izv. Akad. Nauk SSSR Ser. Mat.*, 28:273–276, 1964.

[Gol68] E. S. Golod. Some problems of Burnside type. In *Proc. Internat. Congr. Math. (Moscow, 1966)*, pages 284–289. Izdat. "Mir", Moscow, 1968.

[Gra14] Łukasz Grabowski. On Turing dynamical systems and the Atiyah problem. *Invent. Math.*, 198(1):27–69, 2014.

[Gra16] Łukasz Grabowski. Irrational l^2 invariants arising from the lamplighter group. *Groups Geom. Dyn.*, 10(2):795–817, 2016.

[Gri80] R. I. Grigorchuk. On Burnside's problem on periodic groups. *Funktsional. Anal. i Prilozhen.*, 14(1):53–54, 1980.

[Gri83] R. I. Grigorchuk. On the Milnor problem of group growth. *Dokl. Akad. Nauk SSSR*, 271(1):30–33, 1983.

[Gri84] R. I. Grigorchuk. Degrees of growth of finitely generated groups and the theory of invariant means. *Izv. Akad. Nauk SSSR Ser. Mat.*, 48(5):939–985, 1984.

[Gri85] R. I. Grigorchuk. Degrees of growth of p-groups and torsion-free groups. *Mat. Sb. (N.S.)*, 126(168)(2):194–214, 286, 1985.

[GS83] Narain Gupta and Said Sidki. On the Burnside problem for periodic groups. *Math. Z.*, 182(3):385–388, 1983.

[GŠ06] Rostislav Grigorchuk and Zoran Šunić. Asymptotic aspects of Schreier graphs and Hanoi Towers groups. *C. R. Math. Acad. Sci. Paris*, 342(8):545–550, 2006.

[GS14] Rostislav Grigorchuk and Dmytro Savchuk. Self-similar groups acting essentially freely on the boundary of the binary rooted tree. In *Group theory, combinatorics, and computing*, volume 611 of *Contemp. Math.*, pages 9–48. Amer. Math. Soc., Providence, RI, 2014.

[GS16] Rostislav Grigorchuk and Dmytro Savchuk. Ergodic decomposition of group actions on rooted trees. *Tr. Mat. Inst. Steklova*, 292(Algebra, Geometriya i Teoriya Chisel):100–117, 2016.

[Gup89] Narain Gupta. On groups in which every element has finite order. *Amer. Math. Monthly*, 96(4):297–308, 1989.

[GŻ01] Rostislav I. Grigorchuk and Andrzej Żuk. The lamplighter group as a group generated by a 2-state automaton, and its spectrum. *Geom. Dedicata*, 87(1-3):209–244, 2001.

[Hoř63] Jiří Hořejš. Transformations defined by finite automata. *Problemy Kibernet.*, 9:23–26, 1963.

[Iva94] Sergei V. Ivanov. The free Burnside groups of sufficiently large exponents. *Internat. J. Algebra Comput.*, 4(1-2):ii+308, 1994.

[KmV83] V. A. Kaĭ manovich and A. M. Vershik. Random walks on discrete groups: boundary and entropy. *Ann. Probab.*, 11(3):457–490, 1983.

[Knu81] Donald E. Knuth. *The art of computer programming. Vol. 2.* Addison-Wesley Publishing Co., Reading, Mass., second edition, 1981. Seminumerical algorithms, Addison-Wesley Series in Computer Science and Information Processing.

[Knu98] Donald E. Knuth. *The art of computer programming. Vol. 2.* Addison-Wesley, Reading, MA, 1998. Seminumerical algorithms, Third edition [of MR0286318].

[Kos90] A. I. Kostrikin. *Around Burnside*, volume 20 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990. Translated from the Russian and with a preface by James Wiegold.

[KPS16] Ines Klimann, Matthieu Picantin, and Dmytro Savchuk. Orbit automata as a new tool to attack the order problem in automaton groups. *J. Algebra*, 445:433–457, 2016.

[Lar02a] M. V. Larin. Transitive polynomial transformations of residue rings. *Diskret. Mat.*, 14(2):20–32, 2002.

[Lar02b] M. V. Larin. Transitive polynomial transformations of residue rings. *Diskret. Mat.*, 14(2):20–32, 2002.

[LN83] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1983. With a foreword by P. M. Cohn.

[LPP96] Russell Lyons, Robin Pemantle, and Yuval Peres. Random walks on the lamplighter group. *Ann. Probab.*, 24(4):1993–2006, 1996.

[LW13] Franz Lehner and Stephan Wagner. Free lamplighter groups and a question of Atiyah. *Amer. J. Math.*, 135(3):835–849, 2013.

[Lys96] I. G. Lysënok. Infinite Burnside groups of even period. *Izv. Ross. Akad. Nauk Ser. Mat.*, 60(3):3–224, 1996.

[Mil68] J. Milnor. Problem 5603. *Amer. Math. Monthly*, 75:685–686, 1968.

[MS15] Alexei Miasnikov and Dmytro Savchuk. An example of an automatic graph of intermediate growth. *Ann. Pure Appl. Logic*, 166(10):1037–1048, 2015.

[MS16] Y. Muntyan and D. Savchuk. *AutomGrp – GAP package for computations in self-similar groups and semigroups, Version 1.3*, 2016. Accepted GAP package (available at *http://www.gap-system.org/Packages/automgrp.html*).

[MŠG10] Smile Markovski, Zoran Šunić, and Danilo Gligoroski. Polynomial functions on the units of Z_{2^n}. *Quasigroups Related Systems*, 18(1):59–82, 2010.

[NA68] P. S. Novikov and S. I. Adjan. Infinite periodic groups. I. *Izv. Akad. Nauk SSSR Ser. Mat.*, 32:212–244, 1968.

[Nek05] Volodymyr Nekrashevych. *Self-similar groups*, volume 117 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2005.

[Nek10] Volodymyr Nekrashevych. Free subgroups in groups acting on rooted trees. *Groups Geom. Dyn.*, 4(4):847–862, 2010.

[NP11] Volodymyr Nekrashevych and Gábor Pete. Scale-invariant groups. *Groups Geom. Dyn.*, 5(1):139–167, 2011.

[NS04] V. Nekrashevych and S. Sidki. Automorphisms of the binary tree: state-closed subgroups and dynamics of 1/2-endomorphisms. volume 311 of *London Math. Soc. Lect. Note Ser.*, pages 375–404. Cambridge Univ. Press, 2004.

[PSC02] C. Pittet and L. Saloff-Coste. On random walks on wreath products. *Ann. Probab.*, 30(2):948–977, 2002.

[Riv01] Ronald L. Rivest. Permutation polynomials modulo 2^w. *Finite Fields Appl.*, 7(2):287–292, 2001.

[RRSY] Ronald L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Yin. The RC6 block cipher. Posted on the RC6 site of RSA Laboratories. Slides from NIST AES1 (1998-08-21) and AES3 (2000-04-14) conferences.

[Sid00] Said Sidki. Automorphisms of one-rooted trees: growth, circuit structure, and acyclicity. *J. Math. Sci. (New York)*, 100(1):1925–1943, 2000. Algebra, 12.

[Sid04] Said Sidki. Finite automata of polynomial growth do not generate a free group. *Geom. Dedicata*, 108:193–204, 2004.

[SS05] P. V. Silva and B. Steinberg. On a class of automata groups generalizing lamplighter groups. *Internat. J. Algebra Comput.*, 15(5-6):1213–1234, 2005.

[SS16] Dmytro M. Savchuk and Said N. Sidki. Affine automorphisms of rooted trees. *Geom. Dedicata*, 183:195–213, 2016.

[SS18] Rachel Skipper and Benjamin Steinberg. Lamplighter groups, bireversible automata and rational series over finite rings. Preprint: arxiv:1807.00433, 2018.

[Sus79] V. I. Sushchansky. Periodic permutation p-groups and the unrestricted Burnside problem. *DAN SSSR.*, 247(3):557–562, 1979. (in Russian).

[SV11] Dmytro Savchuk and Yaroslav Vorobets. Automata generating free products of groups of order 2. *J. Algebra*, 336(1):53–66, 2011.

[ŠV12] Zoran Šunić and Enric Ventura. The conjugacy problem in automaton groups is not solvable. *J. Algebra*, 364:148–154, 2012.

[SVV11] Benjamin Steinberg, Mariya Vorobets, and Yaroslav Vorobets. Automata over a binary alphabet generating free groups of even rank. *Internat. J. Algebra Comput.*, 21(1-2):329–354, 2011.

[Tab17] Jennifer Taback. Lamplighter groups. In *Office hours with a geometric group theorist*, pages 310–330. Princeton Univ. Press, Princeton, NJ, 2017.

[VV07] Mariya Vorobets and Yaroslav Vorobets. On a free group of transformations defined by an automaton. *Geom. Dedicata*, 124:237–249, 2007.

[VV10] Mariya Vorobets and Yaroslav Vorobets. On a series of finite automata defining free transformation groups. *Groups Geom. Dyn.*, 4(2):377–405, 2010.

[Zel90] E. I. Zel′manov. Solution of the restricted Burnside problem for groups of odd exponent. *Izv. Akad. Nauk SSSR Ser. Mat.*, 54(1):42–59, 221, 1990.

[Zel91a] E. I. Zel′manov. Solution of the restricted Burnside problem for 2-groups. *Mat. Sb.*, 182(4):568–592, 1991.

[Zel91b] Efim I. Zelmanov. On the restricted Burnside problem. In *Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990)*, pages 395–402, Tokyo, 1991. Math. Soc. Japan.

About the Author

Elsayed Ahmed was born in Gharbeya, Egypt in 1991. He received his B.S. degree in mathematics in July 2012 from Mansoura University, Mansoura, Egypt. He also received a PrePhD diploma in mathematics in August 2014 from the International Centre of Theoretical Physics (ICTP), Trieste, Italy. He has been working as a teaching assistant at the Department of Mathematics and Statistics, University of South Florida since August 2014 where he received his M.A. and Ph.D. in mathematics in May 2016 and December 2018, respectively. His current research interests include groups generated by automata and polynomial dynamics on the ring of d-adic integers. His permanent address is: Department of Mathematics and Statistics,University of South Florida, Tampa, FL, 33620, USA.