

UNIVERZA V LJUBLJANI  
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 1. stopnja

Program dvojne diplome iz matematike  
z Univerzo v Trstu

Carlo Lanzi Luciani  
**Automatne grupe**

Delo diplomskega seminarja

Mentorja: izr. prof. dr. Ganna Kudryavtseva  
prof. Alessandro Logar

Ljubljana, 2020

UNIVERSITÀ DEGLI STUDI DI TRIESTE  
DIPARTIMENTO DI MATEMATICA  
E GEOSCIENZE

UNIVERZA V LJUBLJANI  
FAKULTETA ZA MATEMATIKO IN FIZIKO

Programma di doppio titolo  
in Matematica

Program dvojne diplome  
iz matematike

Double Degree Program in Mathematics

**Carlo Lanzi Luciani**

**Gruppi di automi**

**Automatne grupe**

Tesi finale

Delo diplomskega seminarja

**Groups of automata**

Final Thesis

Supervisor/Mentorja/Supervisors

izr. prof. dr. Ganna Kudryavtseva

prof. Alessandro Logar

2020

## CONTENTS

Add TABLE of  
CONTENTS

# Groups of automata

## ABSTRACT

In this bachelor thesis we present some interesting examples and results on groups generated by Mealy automata.

In the first section we introduce the input and output of an automaton as sequences of symbols from an alphabet  $\mathbf{X}$ , and we discuss their properties. In particular we present the set  $\mathbf{X}^*$  of finite sequences as the set of vertices of a rooted tree. Then we go on to the formal definition of a finite deterministic Mealy automaton (we will simply call it an automaton)  $\mathcal{A}$ , and we provide some examples of automata given by Moore diagrams (graph representations of automata). We define the concept of an initial automaton  $\mathcal{A}_{q_0}$  and its action  $\bar{\lambda}_{q_0}$ .

In the second section we give an abstract characterization of actions of automata; the notion of a synchronous automatic transformation  $f : \mathbf{X}^* \rightarrow \mathbf{X}^*$ . We give a special attention to invertible automata. Then we provide the definition of a group generated by an automaton. pay

In the third section we describe some algebraic structures that arise in connection to groups of automata. We first revise the notions of left and right actions of a group on a set and on a group, the semidirect product construction and finally the wreath product construction. We then show the relationship of these notions with automata. study

In the fourth section we present the classification of groups generated by 2-state-automata over a 2-letter-alphabet ([4, 6]). Before formulating the result we introduce two important groups that arise in this theorem, i.e., the infinite dihedral group and the lamplighter group. This group can be realized as a wreath product of the infinite cyclic group  $\mathbb{Z}$  and the two-element group  $\mathbb{Z}_2$ . Then we define an automatic function, called the adding machine, ~~which will be needed later~~. Finally we present a detailed account of a part of the proof. It is based on careful case consideration.

Try to avoid using references in the abstract.  
The latter of the classification theorem.

**Math. Subj. Class. (2010):** 68Q45, 68Q70, 20E07, 20E22, 20E08, 18B20, 20M05

**Keywords:** automaton, finite automaton, word space, Moore diagram, wreath product, semidirect product, wreath product, recursion, infinite lamplighter group, infinite dihedral group, adding machine, groups acting on rooted trees

# Automatne grupe

## RAZŠIRJENI POVZETEK

V diplomskem delu predstavljamo nekaj zanimivih primerov z avtomati generiranih grup.

V prvem delu spoznamo osnove teorije avtomatov. Hevristično uvedemo avtomat kot računski model, tj. stroj, ki vsakemu vhodnemu podatku (input) priredi izhodnega (output). Input in output predstavimo z elementi končne množice  $\mathbf{X}$ , ki ji pravimo abeceda. Množico končnih zaporedij, imenovano končni slovar, razumemo kot monoid (glede operacije stikanja besed) ali kot množico vozlišč drevesa: vozlišče  $\mathbf{w}$  je potomec vozlišča  $\mathbf{v} \in \mathbf{X}^*$  natanko tedaj, ko velja  $\mathbf{w} = \mathbf{v}x$ , pri čemer  $x \in \mathbf{X}$ . Nato preidemo na definicijo Mealyjevega končnega determinističnega avtomata  $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$  in jo grafično prikažemo z Moorejevimi diagrami. Nato definiramo koncept začetnega avtomata  $\mathcal{A}_{q_0}$  in njegovega delovanja  $\bar{\lambda}_{q_0} : \mathbf{X}^* \rightarrow \mathbf{X}^*$ .

V drugem delu opišemo operacijo komponiranja avtomatov in analiziramo lastnosti množice  $\mathcal{FSA}(\mathbf{X})$ , tj. množice funkcij  $f : \mathbf{X}^* \rightarrow \mathbf{X}^*$ , imenovanih sinhrona avtomatna transformacija, ki jih lahko opišemo s kakim začetnim avtomatom. Tu spoznamo, da je zgornja množica v bijektivni korespondenci z množico homomorfizmov dreves  $f : \mathbf{X}^* \rightarrow \mathbf{X}^*$ . Nato se osredotočimo le na obrnljive avtomatne transformacije: bijektivne sinhrona transformacije, ki tvorijo grupo  $\mathcal{GA}(\mathbf{X})$  izomorfno  $\mathcal{AUT}_{tree}(\mathbf{X}^*)$ , oziroma množici avtomorfizmov drevesa  $\mathbf{X}^*$ . Preučimo še vpliv obrnljivosti avtomata na dostopnost njegovih stanj in podamo definicijo z avtomatom generirane grupe.

Tretji del opisuje vrsto algebraičnih orodij potrebnih pri analizi z avtomatom generiranih grup. Pričnemo z definicijo levega in desnega delovanja grupe  $G$  na množico  $\mathbf{X}$ . Predstavimo delovanje grupe  $H$  na grupo  $N$ , ki ohranja strukturo  $N$ , s ciljem uvedbe semidirektnega produkta  $H \ltimes N$  in navedemo nekaj praktičnih uporab slednjega, npr. diedersko grupo  $\mathbb{Z}_2 \ltimes \mathbb{Z}_n$ . S tema strukturama definiramo  $\wr$  produkt med grupo desnih permutacij  $(Y, B)$  in grupo  $A$ , pišemo  $B \wr A$ . V naslednjem razdelku ugotovimo, da je  $\mathcal{AUT}_{tree}(\mathbf{X}^*)$  izomorfna  $\mathcal{S}(\mathbf{X}) \wr \mathcal{AUT}_{tree}(\mathbf{X}^*)$ . Ker vemo, da je  $\mathcal{AUT}_{tree}(\mathbf{X}^*)$  izomorfna grupi bijektivnih sinhronih transformacij  $\mathcal{GA}(\mathbf{X})$ , lahko vsa delovanja  $f_i$  avtomata z  $n$  stanji nad abecedo s  $k$  simboli opišemo prek določenih rekurzivnih zvez.

V četrtem in zadnjem delu predstavimo rezultat iz [4]. Ta rezultat izrek v celoti klasificira grupe generirane z avtomati z dvema stanjema nad abecedo dveh črk. Preden izrek navedemo, predstavimo grupe, ki se pojavijo v rezultatu, začenši z neskončno diedersko grupo  $\mathbb{Z}_2 \ltimes \mathbb{Z}$ , torej grupo simetrij  $\mathbb{Z}$ . Sledi grupa svetilničarja (lamplighter group  $\mathbb{Z} \wr \mathbb{Z}_2$ ), in definicija posebne transformacije iz  $\mathcal{GA}(\mathbf{X})$ , imenovane adding machine. Zdaj lahko formuliramo klasifikacijski izrek.

Naj bo  $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$  avtomat. Naj bosta  $\mathbf{X} = \{0, 1\}$  in  $|\mathcal{Q}| = 2$ . Potem je grupa generirana z  $\mathcal{A}$  izomorfna eni izmed naslednjih grup:

- (1) Trivialna grupa  $\{1\}$ ,
- (2) Grupa z dvema elementoma  $\mathbb{Z}_2$ ,
- (3) Direktna vsota  $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ ,
- (4) Neskončna ciklična grupa  $\mathbb{Z}$ ,
- (5) Neskončna diedrska grupa  $\mathbb{Z}_2 \ltimes \mathbb{Z}$ ,
- (6) Grupa svetilničarja  $\mathbb{Z} \wr \mathbb{Z}_2$ .

VENČNI

kjer je

Nazadnje predstavimo del dokaza klasifikacijskega izreka, kjer si pomagamo z analizo primerov.

VENČNI

✓

**Ključne besede:** automat, končni avtomat, besedni prostor, Moorejev diagram, semidirektni produkt, venčni produkt, rekursivnost, grupa svetilničarja, neskončna diedrska grupa, stroj dodajanja, grupa delujoča na drevesih

# Gruppi di automi

## SINTESI ESTESA

In questa tesi triennale presentiamo alcuni interessanti esempi e risultati riguardanti i gruppi generati da automi.

Nella prima parte esploriamo le basi della teoria degli automi. Introduciamo euristicamente l'automata come modello di computazione, ovvero una macchina che per ogni dato immesso (input), ritorna un altro dato (output). Presentiamo input ed output con elementi dell'insieme  $\mathbf{X}$ , che chiamiamo alfabeto. Vediamo l'insieme delle sequenze finite, detto dizionario finito, come un monoide (rispetto all'operazione di composizione di parole) oppure come un grafo ad albero: un nodo  $\mathbf{w}$  è discendente di un altro  $\mathbf{v} \in \mathbf{X}^*$  se e solo se  $\mathbf{w} = \mathbf{v}x$ , per qualche  $x \in \mathbf{X}$ . Poi passiamo alla definizione di automa deterministico finito di Mealy  $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$  e ne diamo una rappresentazione con i diagrammi di Moore. Definiamo il concetto di automa iniziale  $\mathcal{A}_{q_0}$  e della sua azione  $\bar{\lambda}_{q_0} : \mathbf{X}^* \rightarrow \mathbf{X}^*$ .

Nella seconda parte descriviamo l'operazione di composizione di automi e analizziamo le proprietà dell'insieme  $\mathcal{FSA}(\mathbf{X})$ , ovvero l'insieme delle funzioni  $f : \mathbf{X}^* \rightarrow \mathbf{X}^*$ , dette trasformazioni automatiche sincrone, che possiamo descrivere con qualche automa iniziale. Qui scopriamo che quest'insieme è in biezione con l'insieme degli omomorfismi d'albero del dizionario finito  $\mathbf{X}^*$ . Quindi ci focalizziamo solamente sulle trasformazioni automatiche biettive, che formano il gruppo  $\mathcal{GA}(\mathbf{X})$  isomorfo a  $\mathcal{AUT}_{tree}(\mathbf{X}^*)$ , cioè l'insieme degli automorfismi d'albero su  $\mathbf{X}^*$ . Studiamo l'influenza dell'invertibilità di un automa sull'accessibilità dei suoi stati, ed infine diamo la definizione di gruppo generato da un automa.

La terza parte descrive una serie di strumenti algebrici necessari per l'analisi dei gruppi generati da automi. Partiamo dalle definizioni di azione destra e sinistra di un gruppo  $G$  su un insieme  $X$ . Presentiamo l'azione di un gruppo  $H$  su un altro gruppo  $N$  che conserva la struttura di  $N$ , al fine di introdurre il prodotto semidiretto  $H \ltimes N$ , e vediamo alcuni esempi pratici, e.g. il gruppo diedrale  $\mathbb{Z}_2 \ltimes \mathbb{Z}_n$ . Con queste due strutture definiamo il prodotto intrecciato di un gruppo di permutazioni destro  $(Y, B)$  e di un gruppo  $A$ , scritto  $B \wr A$ . Nella sezione seguente scopriamo che  $\mathcal{AUT}_{tree}(\mathbf{X}^*)$  è isomorfo a  $\mathcal{S}(\mathbf{X}) \wr \mathcal{AUT}_{tree}(\mathbf{X}^*)$ . Siccome sappiamo che  $\mathcal{AUT}_{tree}(\mathbf{X}^*)$  è isomorfo al gruppo delle trasformazioni sincrone biettive  $\mathcal{GA}(\mathbf{X})$ , possiamo descrivere tutte le azioni di un automa a  $n$  stati su un alfabeto a  $k$  simboli tramite formule ricorsive.

Nella quarta ed ultima parte presentiamo un risultato di [4]. Questo teorema classifica interamente i gruppi generati da automi a 2 stati su alfabeti a 2 lettere. Prima di enunciarlo presentiamo i gruppi che compaiono nel risultato, partendo dal gruppo diedrale infinito  $\mathbb{Z}_2 \ltimes \mathbb{Z}$ , cioè il gruppo delle simmetrie di  $\mathbb{Z}$ . Segue il gruppo del lampionaio (lamplighter group [6]),  $\mathbb{Z} \wr \mathbb{Z}_2$ , e la definizione di una speciale trasformazione in  $\mathcal{GA}(\mathbf{X})$ , detta macchina delle addizioni (adding machine). Ora possiamo formulare il teorema. Sia  $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$  un automa. Siano  $\mathbf{X} = \{0, 1\}$  e  $|\mathcal{Q}| = 2$ . Allora il gruppo generato da  $\mathcal{A}$  è isomorfo ad uno dei seguenti gruppi:

- (1) Il gruppo banale  $\{1\}$ ,
- (2) Il gruppo con due elementi  $\mathbb{Z}_2$ ,
- (3) La somma diretta  $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ ,
- (4) Il gruppo ciclico infinito  $\mathbb{Z}$ ,
- (5) Il gruppo diedrale infinito  $\mathbb{Z}_2 \ltimes \mathbb{Z}$ ,
- (6) Il gruppo del lampionaio  $\mathbb{Z} \wr \mathbb{Z}_2$ .

Infine presentiamo una parte delle dimostrazione del teorema di classificazione, dove ci aiutiamo con l'analisi dei casi.

**Parole chiave:** automi, automi finiti, spazi di parole, diagrammi di Moore, prodotti intrecciati, prodotti semidiretti, ricorsività, gruppo infinito del lampionaio, gruppo diedrale infinito, macchina delle addizioni, gruppi agenti su alberi



## Part 1. Introduction

The word *automaton* comes from greek (plural *automata* or *automatons*), and means "acting on one's self-will". Roughly speaking an automaton is a very specific *model of computation*. We can heuristically say that a model of computation is a machine which, for each input given, returns an output (Figure 1).



FIGURE 1. Model of computation

So we have a certain function  $f(input) = output$ . We will see later that such functions form groups.

### 1. WORDS SPACES AND ALPHABET TREES

We begin with the formalization of input and output.

**Definition 1.1.** An **alphabet**  $\mathbf{X}$  is a finite set of elements called **letters**.

**Definition 1.2.** The set  $\mathbf{X}^* := \{x_1 \dots x_n | n \in \mathbb{N} \cup \{0\}, x_i \in \mathbf{X}\}$  is called the **set of finite words** or **finite dictionary**, and its elements are called **words**. The element with no letters, written as  $\emptyset$ , is called the *empty word*.

**Definition 1.3.** Let  $\mathbf{w} = x_1 \dots x_n$  and  $\mathbf{u} = y_1 \dots y_m$  be words. The **length** of  $\mathbf{w}$ , written as  $|\mathbf{w}|$ , is  $n$ . The length of the empty word is 0. The **concatenation** of  $\mathbf{w}$  and  $\mathbf{u}$ , written as  $\mathbf{w} \circ \mathbf{u} = \mathbf{wu}$  is the word  $x_1 \dots x_n y_1 \dots y_m$ .

**Example 1.4.** Let  $\mathbf{X} = \{0, 1\}$ . Then  $0100 \circ 111 = 0100111$  and  $11 \circ 0101 = 110101$ . Let  $\mathbf{X} = \{0, j, 2\}$ . Then  $02j \circ 20j = 02j20j$  and  $j \circ 2j = j2j$ .  $\diamond$

**Proposition 1.5.**  $(\mathbf{X}^*, \circ)$  is a monoid, called the **free monoid on  $\mathbf{X}$**

*Proof.* The operation  $\circ$  is associative with  $\emptyset$  being an identity element.  $\square$

Let us define also words with an infinite length.

**Definition 1.6.** The **set of infinite words** or the **infinite dictionary** is the set  $\mathbf{X}^\omega := \{x_1 \dots x_i \dots | x_i \in \mathbf{X}\} = \mathbf{X}^{\mathbb{N} \cup \{0\}}$ .

**Remark 1.** Note that if  $\mathbf{u} = x_1 \dots x_n \in \mathbf{X}^*$  and  $\mathbf{v} = y_1 \dots y_i \dots \in \mathbf{X}^\omega$ , we can define  $\mathbf{u} \circ \mathbf{v} := x_1 \dots x_n y_1 \dots y_i \dots \in \mathbf{X}^\omega$ .

**Definition 1.7.** A word  $\mathbf{w} = x_1 \dots x_n$  is the **beginning** or the **prefix** of a word  $\mathbf{u} \in \mathbf{X}^*$  (or  $\mathbf{u} \in \mathbf{X}^\omega$ ) if  $\mathbf{u} = \mathbf{wv} = x_1 \dots x_n \mathbf{v}$  for some  $\mathbf{u} \in \mathbf{X}^*$  (or  $\in \mathbf{X}^\omega$ ). In this case we set  $\mathbf{v} = \mathbf{u} - \mathbf{w}$ .

Given  $A \subseteq \mathbf{X}^* \cup \mathbf{X}^\omega$ , we denote  $\mathcal{P}(A)$  the **longest common prefix of all the words from  $A$** . Note that  $\mathcal{P}(A)$  that is uniquely defined.

**1.1. Topology on infinite dictionaries.** We can endow the set  $\mathbf{X}^\omega$  with a metric, and consequently a topology.

Let  $\tilde{\lambda} = (\lambda_n)_{n \in \mathbb{N}}$  be an arbitrary *decreasing* sequence of *positive* numbers such that  $\lim_{n \rightarrow \infty} \lambda_n = 0$ . We define

$$(1) \quad d_{\tilde{\lambda}}(\mathbf{w}_1, \mathbf{w}_2) = \lambda_n$$

on  $\mathbf{X}^\omega$ , where  $n = |\mathcal{P}(\{\mathbf{w}_1, \mathbf{w}_2\})|$  is the lenght of the longest common prefix of the words  $\mathbf{w}_1$  and  $\mathbf{w}_2$ .

**Proposition 1.8.** *The function  $d_{\tilde{\lambda}}$  is a metric.*

*Proof.* We prove just the triangular inequality Let  $n = |\mathcal{P}(\{\mathbf{w}_1, \mathbf{w}_2\})|$ . Let  $\mathbf{w}_3 \in \mathbf{X}^\omega$ . We want to show that

$$d_{\tilde{\lambda}}(\mathbf{w}_1, \mathbf{w}_2) \leq d_{\tilde{\lambda}}(\mathbf{w}_1, \mathbf{w}_3) + d_{\tilde{\lambda}}(\mathbf{w}_3, \mathbf{w}_2)$$

Denote  $p := |\mathcal{P}(\{\mathbf{w}_1, \mathbf{w}_3\})|$  and  $q := |\mathcal{P}(\{\mathbf{w}_3, \mathbf{w}_2\})|$ . We need to show that  $\lambda_n \leq \lambda_p + \lambda_q$ . Suppose that  $p = \min\{p, q\}$  (if  $q = \min\{p, q\}$  the proof is symmetrical). If  $p \leq n$ , since  $\tilde{\lambda}$  is decreasing, we obtain  $\lambda_n \leq \lambda_p \leq \lambda_p + \lambda_q$ . Let us prove that  $p \leq n$  through reductio ad absurdum. Suppose that  $p > n$ . We denote the word  $\mathcal{P}(\{\mathbf{w}_1, \mathbf{w}_2\})$  by  $x_1 \dots x_n$ , the word  $\mathcal{P}(\{\mathbf{w}_1, \mathbf{w}_3\})$  by  $x_1 \dots x_n y_{n+1} \dots y_p$  and the word  $\mathcal{P}(\{\mathbf{w}_3, \mathbf{w}_2\})$  by  $x_1 \dots x_n z_{n+1} \dots z_p \dots z_q$ . But then  $x_1 \dots x_n y_{n+1} \dots y_p = x_1 \dots x_n z_{n+1} \dots z_p$  because they are of the same lenght and they are both prefixes of  $\mathbf{w}_3$ . Consequently the last word, of lenght  $p$ , is prefix both of  $\mathbf{w}_1$  and  $\mathbf{w}_2$ . Therefore it is a prefix of  $x_1 \dots x_n$ , so  $p \leq n$ , contradicting the assumption that  $p > n$ .  $\square$

Every set  $\mathbf{wX}^\omega := \{\mathbf{wu} | \mathbf{u} \in \mathbf{X}^\omega\}$  can be seen as a ball of radius  $\lambda_{|\mathbf{w}|}$  with the center in an arbitrary point  $\mathbf{u} \in \mathbf{wX}^\omega$ .

**Remark 2.** *It is often useful to set  $\tilde{\lambda} = (\frac{1}{n})_{n \in \mathbb{N}}$ .*

**1.2. Tree structure of dictionaries.** It is useful to represent  $\mathbf{X}^*$  in the form of a tree graph:  $\emptyset$  is the root and  $\mathbf{v} \in \mathbf{X}^*$  is a child of  $\mathbf{u} \in \mathbf{X}^*$  *if and only if*  $\mathbf{u} = \mathbf{v}x$  for some  $x \in \mathbf{X}$ . We call the resulting tree graph by **word tree** on  $\mathbf{X}$ . An example is given in [Figure 2](#).

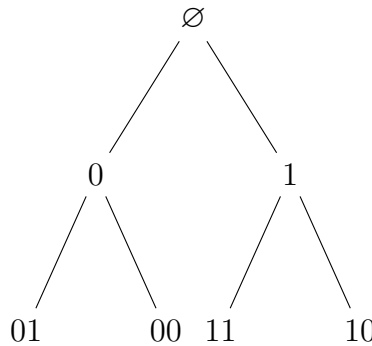


FIGURE 2. An example of the first three floors of the word tree on  $\mathbf{X} = \{0, 1\}$ .

**Convention 1.** *We will mostly use the alphabet  $\mathbf{X} = \{0, 1\}$ .*

The set  $X^n$  is called the *n-th floor* of  $\mathbf{X}^*$ .

Finally, we define the notion of an endomorphism of a tree and describe some of its properties.

**Definition 1.9.** Let  $A$  and  $B$  be word trees on some alphabet  $\mathbf{X}$  and  $f : A \rightarrow B$  be a function. It is called a **tree-homomorphism** if it preserves the root and the adjacency of the vertices, i. e.:

- (1) If  $a \in A$  is the root,  $f(a)$  is the root.
- (2) If  $(u, v)$  is an edge of  $A$ , then  $(f(u), f(v))$  is an edge of  $B$ .

If  $A = B$ ,  $f$  is called a **tree-endomorphism**. If  $A = B$  and  $f$  is bijective, we call it a **tree-automorphism**.

It can be verified that all tree-endomorphisms  $f : A \rightarrow A$  form a *semigroup* under the composition of functions, and all the tree-automorphisms  $f : A \rightarrow A$  form its subsemigroup which is also a *group*.

## 2. AUTOMATA AND INITIAL AUTOMATA

Now we will treat the formal definition of the very specific type of automaton which we need, the *deterministic finite (finite state) synchronous automaton*, or *finite Mealy automaton*, or *finite trasducer*. We will always call it simply an *automaton*, but the reader should know that this is a *very specific case*. A broader class of automata are treated in [3, 10].

**Definition 2.1.** An **automaton** is a 4-tuple  $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$  where:

- $\mathbf{X}$  is an alphabet, usually referred to as the **input** and/or **output alphabet**,
- $\mathcal{Q}$  is a set called the **set of internal states of the automaton**,
- $\pi : \mathbf{X} \times \mathcal{Q} \rightarrow \mathcal{Q}$  is a function called the **transition function**,
- $\lambda : \mathbf{X} \times \mathcal{Q} \rightarrow \mathbf{X}$  is a function called the **output function**.

We say that  $\mathcal{A}$  is a  $|\mathcal{Q}|$ -state automaton on  $\mathbf{X}$ .

This definition explains us how an automaton performs the action of transforming an input into an output. We can imagine that for every *input letter*  $x$  we plug in the machine, and for every *state*  $q$ , from which we decide to start, the machine moves to a state  $p = \pi(x, q) \in \mathcal{Q}$  and returns an *output letter*  $y = \lambda(x, q) \in \mathbf{X}$ .

**Definition 2.2.** Given an automaton  $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$  we define its **Moore diagram** as the oriented graph  $G = (\mathcal{Q}, \mathcal{E})$  where two states  $q_1$  and  $q_2$  are connected whenever  $\exists x \in \mathbf{X}$  s.t.  $\pi(x, q_1) = q_2$  and the label assigned to this edge is  $x|\lambda(x, q_1)$ .

An example of Moore diagram is given in Figure 3.

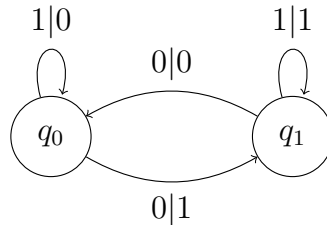


FIGURE 3. Example of the Moore diagram of a 2-state-automaton over the alphabet  $\mathbf{X} = \{0, 1\}$

We observe that for every automaton its Moore diagram has the following property:

- (2)  $\forall q \in \mathcal{Q}$  and  $\forall x \in \mathbf{X} \quad \exists! e \in \mathcal{E}$  such that the left-hand side of the label of  $e$  reads " $x$ ".

*determined their*

**Remark 3.** Automata are uniquely defined by Moore diagrams. So given  $\mathcal{M} := \{M \mid M \text{ is a Moore diagram}\}$ , there is a unique correspondence between  $\mathcal{M}$  and the set of all automata.

**Example 2.3.** In Figure 2, given the input  $\mathbf{w} = 0$  and the state  $q = q_0$ , we have  $\pi(\mathbf{w}, q) = q_1$  and  $\lambda(\mathbf{w}, q) = 1$ . If  $\mathbf{w} = 1$  and  $q = q_1$ , then  $\pi(\mathbf{w}, q) = q_1$  and  $\lambda(\mathbf{w}, q) = 1$ .  $\diamond$

**Definition 2.4.** We recursively extend the domain of  $\pi$  and  $\lambda$  from single letters in  $\mathbf{X}$  to words in  $\mathbf{X}^*$ . We define:

- $\bar{\pi} : \mathbf{X}^* \times \mathcal{Q} \longrightarrow \mathcal{Q} :$

$$\bar{\pi}(\emptyset, q) = q,$$

$$\bar{\pi}(x\mathbf{w}, q) = \bar{\pi}(\mathbf{w}, \bar{\pi}(x, q)).$$

- $\bar{\lambda} : \mathbf{X}^* \times \mathcal{Q} \longrightarrow \mathbf{X}^* :$

$$\bar{\lambda}(\emptyset, q) = \emptyset,$$

$$\bar{\lambda}(x\mathbf{w}, q) = \bar{\lambda}(x, q)\bar{\lambda}(\mathbf{w}, \bar{\pi}(x, q)).$$

**Remark 4.** The definitions (2.4) are equivalent to:

$$\bar{\pi}(\mathbf{w}x, q) = \bar{\pi}(x, \bar{\pi}(\mathbf{w}, q))$$

and

$$\bar{\lambda}(\mathbf{w}x, q) = \bar{\lambda}(\mathbf{w}, q)\bar{\lambda}(x, \bar{\pi}(\mathbf{w}, q)),$$

respectively.

**Example 2.5.** We can compute  $\bar{\pi}$  and  $\bar{\lambda}$  following the arrows on the Moore diagram of an automaton, and then making the composition of the single right-hand side of the labels. In the Figure 3, given the input  $\mathbf{w} = 0000$  and the state  $q = q_0$ , we have  $\bar{\pi}(q, \mathbf{w}) = q_0$  and  $\bar{\lambda}(q, \mathbf{w}) = 1010$ . If  $\mathbf{w} = 110$  and  $q = q_1$ , we have  $\bar{\pi}(q, \mathbf{w}) = q_0$  and  $\bar{\lambda}(q, \mathbf{w}) = 110$ .  $\diamond$

To effectively make an automaton a word-transducer, we need to specify an initial state. For example, in Figure 3 to get an output we need to feed the machine both with an input  $x$  and a state  $q$ . So let us fix  $q \in \mathcal{Q}$ .

**Definition 2.6.** If an automaton  $\mathcal{A}$  has a fixed state  $q_0$ , we call it an **initial automaton with the initial state**  $q_0$  and we write it as  $\mathcal{A}_{q_0}$ . Each  $\mathcal{A}_{q_0}$  naturally defines the map  $\bar{\lambda}_{q_0} : \mathbf{X}^* \longrightarrow \mathbf{X}^*$  with  $\bar{\lambda}_{q_0}(\mathbf{w}) := \bar{\lambda}(\mathbf{w}, q_0)$ , called the **action of the automaton**  $\mathcal{A}_{q_0}$ . Two initial automata are said to be **equivalent** if they define the same actions.

**Proposition 2.7.** The action  $\bar{\lambda}_{q_0}$  of an initial automaton preserves the length of words, i.e.  $|\bar{\lambda}_{q_0}(\mathbf{w})| = |\mathbf{w}|$ .

*Proof.* The statement can be easily verified by induction on  $n = |\mathbf{w}|$ .  $\square$

**Remark 5.** Given an initial automaton  $\mathcal{A}_{q_0}$ , we can define the infinite action  $\bar{\lambda}_{q_0} : \mathbf{X}^\omega \longrightarrow \mathbf{X}^\omega$  by similar recursive formulas, and we can consequently declare that two initial automata are  $\omega$ -equivalent if they determine the same infinite action. Two automata are equivalent if and only if they are  $\omega$ -equivalent ([4]).

**Example 2.8.** In Figure 4 we present the Moore diagrams of two equivalent initial automata.  $\diamond$

**Convention 2.** An initial automaton is usually drawn depicting the initial state with a double circle around ~~its~~ <sup>the respective</sup> vertex (Figure 4).

Let us stress once again that an automaton does not define any function, till we do not fix a state  $q_0$ .

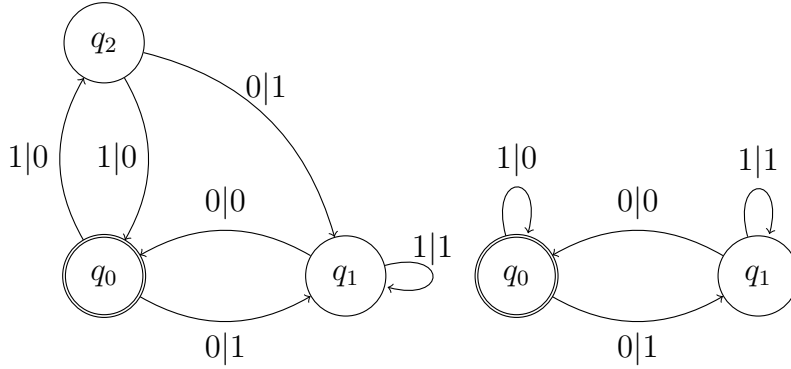


FIGURE 4. Two different initial automata which describe the same action. The double circle around  $q_0$  tells us  $q_0$  is the initial state.

## Part 2. The algebraic structures defined by automata

Here we will show how automata can define algebraic structures and how synchronous ~~functions~~ <sup>certain</sup> can be characterised.

*automatic transformation*

**Definition 2.9.** Given automata  $\mathcal{A}_1 = \langle X, \mathcal{Q}_1, \pi_1, \lambda_1 \rangle$  and  $\mathcal{A}_2 = \langle X, \mathcal{Q}_2, \pi_2, \lambda_2 \rangle$ , we define their *composition*  $\mathcal{B} := \mathcal{A}_1 * \mathcal{A}_2 = \langle X, \mathcal{Q}_1 \times \mathcal{Q}_2, \pi, \lambda \rangle$  with  $\pi$  and  $\lambda$  defined as follows:

- $\pi(x, (s_1, s_2)) = (\pi_1(x, s_1), \pi_2(\lambda_1(x, s_1), s_2))$ ,
- $\lambda(x, (s_1, s_2)) = \lambda_2(\lambda_1(x, s_1), s_2)$ ,

where  $x \in X$  and  $(s_1, s_2) \in \mathcal{Q}_1 \times \mathcal{Q}_2$ .

**Remark 6.** Let  $(\mathcal{A}_1)_{q_1}$  and  $(\mathcal{A}_2)_{q_2}$  be initial automata and let  $\bar{\lambda}_{q_1}^{\mathcal{A}_1}$  and  $\bar{\lambda}_{q_2}^{\mathcal{A}_2}$  be their actions. We can easily verify that

*it can be verified*

$$\bar{\lambda}_{q_2}^{\mathcal{A}_2} \circ \bar{\lambda}_{q_1}^{\mathcal{A}_1} = \bar{\lambda}_{(q_1, q_2)}^{\mathcal{A}_1 * \mathcal{A}_2} = \bar{\lambda}_{(q_1, q_2)}^{\mathcal{B}}$$

where  $\circ$  here denotes the operation of composition of functions and  $\bar{\lambda}^{\mathcal{A}_1 * \mathcal{A}_2} = \bar{\lambda}^{\mathcal{B}}$  is the action of  $\mathcal{A}_1 * \mathcal{A}_2 = \mathcal{B}$ . This means that the operation  $*$  on the set of automata gives rise to an operation  $*$ ' on the set of initial automata defined as  $(\mathcal{A}_1)_{q_1} *' (\mathcal{A}_2)_{q_2} := (\mathcal{A}_1 * \mathcal{A}_2)_{(q_1, q_2)}$ . With the operation  $*$ ' the set of all initial automata on an alphabet  $X$  becomes a semigroup.

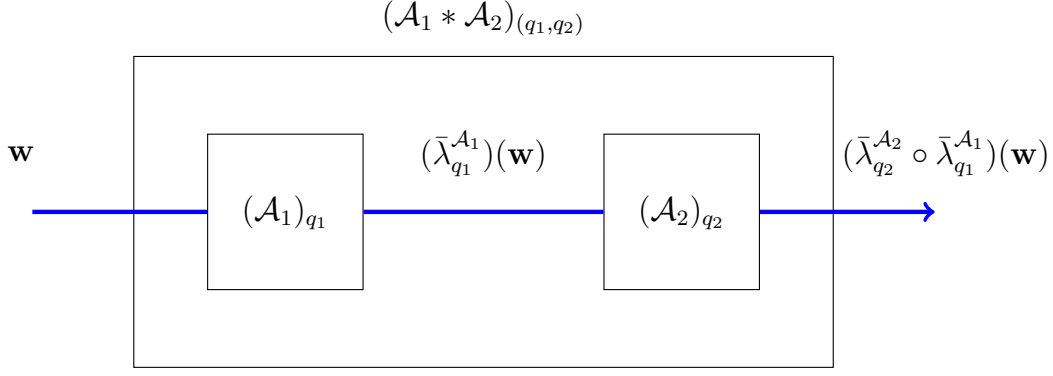


FIGURE 5. Concept of composition of initial automata.

### 3. SYNCHRONOUS AUTOMATIC TRANSFORMATIONS

In this section, given an action of an initial automaton, we describe and study its properties.

**Definition 3.1.** A transformation on  $\mathbf{X}^*$  (i.e. a function  $f : \mathbf{X}^* \rightarrow \mathbf{X}^*$ ) is called **finite synchronous automatic** if it is the (finite) action of some initial automaton  $\mathcal{A}_{q_0}$ , i.e. if  $f = \bar{\lambda}_{q_0}$ .

**Definition 3.2.** A transformation on  $\mathbf{X}^\omega$  (i.e. a function  $f : \mathbf{X}^\omega \rightarrow \mathbf{X}^\omega$ ) is called **infinite synchronous automatic** if it is the infinite action of some initial automaton.

**Proposition 3.3.** *The finite synchronous automatic transformations form a semigroup denoted by  $\mathcal{FSA}(X)$ .*

*Proof.* This arises from Remark 6. Let  $f_1 = \bar{\lambda}_{q_1}^{A_1}$  and  $f_2 = \bar{\lambda}_{q_2}^{A_2}$  be the actions of two initial automata  $(\mathcal{A}_1)_{q_1}$  and  $(\mathcal{A}_2)_{q_2}$  respectively. We have seen that

$$f_2 \circ f_1 = \bar{\lambda}_{q_2}^{A_2} \circ \bar{\lambda}_{q_1}^{A_1} = \bar{\lambda}_{(q_1, q_2)}^{A_1 * A_2},$$

hence  $f_2 \circ f_1$  is synchronous automatic. Therefore  $\mathcal{FSA}(X)$  is closed under composition of functions and consequently it is a semigroup.  $\square$

Now we provide an important characterization of synchronous automatic transformations:

**Proposition 3.4.** *A transformation  $f : \mathbf{X}^* \rightarrow \mathbf{X}^*$  is synchronous automatic if and only if  $f$  is a tree-endomorphism on  $\mathbf{X}^*$ .*

*Proof.* Just for the purpose of this proof, and just in the second part, we will use a more general definition of an automaton, allowing  $\mathcal{Q}$  to be infinite.

( $\Rightarrow$ ) Since  $f$  is synchronous automatic, there is an action  $\bar{\lambda}_{q_0}$  of some initial automaton such that  $f = \bar{\lambda}_{q_0}$ . We need to show that  $\bar{\lambda}_{q_0}$  (1) preserves the root and (2) preserves the adjacencies. By the definition  $f(\emptyset) = \bar{\lambda}_{q_0}(\emptyset) = \emptyset$ , thus (1) holds. Now we prove (2): if  $\mathbf{v}$  is a child of  $\mathbf{w}$  (i.e.  $\mathbf{v} = \mathbf{w}x$  for some  $x \in \mathbf{X}$ ), we show that  $f(\mathbf{v})$  is a child of  $f(\mathbf{w})$  (i.e.  $f(\mathbf{v}) = f(\mathbf{w})y$  for some  $y \in \mathbf{X}$ ). We have:

$$\begin{aligned} f(\mathbf{v}) &= f(\mathbf{w}x) = \bar{\lambda}_{q_0}(\mathbf{w}x) = \bar{\lambda}(\mathbf{w}x, q_0) = \\ &= \bar{\lambda}(\mathbf{w}, q_0) \bar{\lambda}(x, \bar{\pi}(q_0, \mathbf{w})) = f(\mathbf{w}) \bar{\lambda}(x, \bar{\pi}(q_0, \mathbf{w})). \end{aligned}$$

But  $|\bar{\lambda}(x, \bar{\pi}(q_0, \mathbf{w}))| = 1$  because every action is length-preserving, thus  $y = \bar{\lambda}(x, \bar{\pi}(q_0, \mathbf{w})) \in \mathbf{X}$ , so  $f(\mathbf{v}) = f(\mathbf{w}x) = f(\mathbf{w})y$ , hence (2) holds as well.

( $\Leftarrow$ ) Let  $f : \mathbf{X}^* \rightarrow \mathbf{X}^*$  be a tree-endomorphism. We must find an initial automaton such that its action is equal to  $f$ . We define  $\mathcal{A} = \langle X, \mathcal{Q}, \pi, \lambda \rangle := \langle X, \mathbf{X}^*, \pi, \lambda \rangle$  ( $\mathcal{Q} = \mathbf{X}^*$  is infinite) with  $\pi(\mathbf{q}, x) := \mathbf{q}x$  and  $\lambda(\mathbf{q}, x) := f(\mathbf{q}x) - f(\mathbf{q})$ .

First we show that the output function  $\lambda$  is well defined, i.e., the subtraction  $f(\mathbf{q}x) - f(\mathbf{q})$  is well defined. It is because  $f$  is a tree-endomorphism, so  $f(\mathbf{q}x)$  is a child of  $f(\mathbf{q})$ . Now we check if  $\bar{\lambda}_\emptyset$ , the action of  $\mathcal{A}_\emptyset$ , corresponds to the function  $f$ . We verify that  $\bar{\lambda}_\emptyset(\mathbf{w}) = f(\mathbf{w})$  by induction on  $n = |\mathbf{w}|$ .

(Case  $n = 0$ ) We have  $\bar{\lambda}(\emptyset, \emptyset) = \emptyset = f(\emptyset)$ .

(Case  $n \Rightarrow n + 1$ ) Given  $\mathbf{w} \in \mathbf{X}^* \setminus \{\emptyset\}$ , it can be written as  $\mathbf{v}x$ , with  $\mathbf{v} \in \mathbf{X}^*$  and  $x \in \mathbf{X}$ . Then  $\bar{\lambda}(\emptyset, \mathbf{v}x) = \bar{\lambda}(\emptyset, \mathbf{v})\bar{\lambda}(\bar{\pi}(\emptyset, \mathbf{v}), x) = f(\mathbf{v})\bar{\lambda}(\mathbf{v}, x) = f(\mathbf{v})[f(\mathbf{v}x) - f(\mathbf{v})]$  which finishes the proof. □

*tree-endomorphism?*

**Proposition 3.5.** *If  $f$  is an endomorphism on  $\mathbf{X}^*$ , then  $f(X^n) \subseteq X^n$ . In particular, if  $f$  is an automorphism, then  $f(\mathbf{X}^n) = \mathbf{X}^n$ , i.e. is a permutation on  $\mathbf{X}^n$ .*

*Proof.* This can be easily proved by induction on  $n$ . □

**Remark 7.** Proposition 3.5 provides a graph perspective on the length-preserving condition of actions of automata.

**Definition 3.6.** Let  $g : \mathbf{X}^* \rightarrow \mathbf{X}^*$  be a tree-endomorphism and  $\mathbf{v} \in \mathbf{X}^*$ . We define the **restriction of  $g$  in  $\mathbf{v}$**  as the function  $g|_{\mathbf{v}} : \mathbf{X}^* \rightarrow \mathbf{X}^*$  such that:

$$(3) \quad g(\mathbf{v}\mathbf{w}) = g(\mathbf{v})g|_{\mathbf{v}}(\mathbf{w}).$$

**Remark 8.** Since  $\mathbf{v}$  is a prefix of  $\mathbf{v}\mathbf{w}$ , and  $g$  is a tree-endomorphism, it can be proved by induction that  $g(\mathbf{v})$  is a prefix of  $g(\mathbf{v}\mathbf{w})$ . Therefore (3) is well defined.

**Proposition 3.7.** Let  $g, \mathbf{v}$  and  $g|_{\mathbf{v}}$  be as in Definition 3.6, then  $g|_{\mathbf{v}}(\mathbf{w}) = g(\mathbf{v}\mathbf{w}) - g(\mathbf{v})$ . Furthermore,  $g|_{\mathbf{v}}$  is a tree-endomorphism.

*Proof.* The first point is a direct consequence of Remark 8. Let us prove the second point. We have that  $g|_{\mathbf{v}}(\emptyset) = g(\mathbf{v}) - g(\mathbf{v}) = \emptyset$ , so  $g|_{\mathbf{v}}$  preserves the root. Furthermore, if  $x \in \mathbf{X}$ , then  $g|_{\mathbf{v}}(\mathbf{w}x) = g(\mathbf{v}\mathbf{w}x) - g(\mathbf{v}) = g(\mathbf{v}\mathbf{w})y - g(\mathbf{v})$  for some  $y \in \mathbf{X}$  (because  $g$  is a tree-endomorphism), and finally  $g(\mathbf{v}\mathbf{w})y - g(\mathbf{v}) = (g(\mathbf{v}\mathbf{w}) - g(\mathbf{v}))y = g|_{\mathbf{v}}(\mathbf{w})y$ , and therefore  $g|_{\mathbf{v}}$  is a tree-endomorphism. □

We give a description of the restriction  $g|_{\mathbf{v}}$  in terms of automata.

**Proposition 3.8.** If  $\bar{\lambda}_{q_0} : \mathbf{X}^* \rightarrow \mathbf{X}^*$  is the action of  $\mathcal{A}_{q_0}$ , then, for every  $\mathbf{v} \in \mathbf{X}^*$ , the action of  $\mathcal{A}_{\bar{\pi}(\mathbf{v}, q_0)}$  is given by  $(\bar{\lambda}_{q_0})|_{\mathbf{v}} = \bar{\lambda}_{\bar{\pi}(\mathbf{v}, q_0)}$ , i.e. the restriction of  $\bar{\lambda}_{q_0}$  in  $\mathbf{v}$ .

*Proof.* Given  $\mathbf{v}, \mathbf{w} \in \mathbf{X}^*$  we can easily prove by induction on  $n = |\mathbf{w}|$  that  $g(\mathbf{v}\mathbf{w}) := \bar{\lambda}_{q_0}(\mathbf{v}\mathbf{w}) = \bar{\lambda}_{q_0}(\mathbf{v})\bar{\lambda}_{\bar{\pi}(\mathbf{v}, q_0)}(\mathbf{w}) = g(\mathbf{v})\bar{\lambda}_{\bar{\pi}(\mathbf{v}, q_0)}(\mathbf{w})$ , consequently  $g|_{\mathbf{v}} = \bar{\lambda}_{\bar{\pi}(\mathbf{v}, q_0)}$ . □

#### 4. GROUPS GENERATED BY AUTOMATA

We start from the following definition.

**Definition 4.1.** Given an initial automaton  $\mathcal{A}_{q_0}$ , a state  $q$  is called **accessible** if there exists a word  $\mathbf{w} \in \mathbf{X}$  such that  $\bar{\pi}(\mathbf{w}, q_0) = q$ . We can also say that  $q$  is **accessible with respect to  $q_0$**  or **from  $q_0$** .



This means that in the Moore diagram there is a path from  $q_0$  to  $q$  for the vertex  $q \in \mathcal{Q}$ .

**Definition 4.2.** An initial automaton  $\mathcal{A}_{q_0}$  is called **accessible** if each  $q \in \mathcal{Q}$  is accessible with respect to  $q_0$ . An automaton is called **accessible** if each initial automaton defined by it is accessible.

**Proposition 4.3.** Given an automaton  $\mathcal{A} = \langle X, \mathcal{Q}, \pi, \lambda \rangle$  and a state  $q_0 \in \mathcal{Q}$ ,  $\bar{\lambda}_{q_0}$  is an invertible function if and only if for every accessible state  $q \in \mathcal{Q}$  (respect to  $q_0$ ) the function  $\lambda_q : \mathbf{X} \rightarrow \mathbf{X}$  is invertible.

*Proof.*  $(\Rightarrow)$  Suppose that  $\bar{\lambda}_{q_0}$  is an invertible function. Let us take an accessible state  $q \in \mathcal{Q}$  and a word  $\mathbf{w}$  such that  $\bar{\pi}_{q_0}(\mathbf{w}) = q$ . We check that  $\lambda_q$  is injective. Let  $x \neq y$ . From the converse we suppose that  $\lambda_q(x) = \lambda_q(y)$ . We would then have that

$$\bar{\lambda}_{q_0}(\mathbf{w}x) = \bar{\lambda}_{q_0}(\mathbf{w}) \underbrace{\bar{\lambda}_{\bar{\pi}(\mathbf{w}, q_0)}(x)} = \bar{\lambda}_{q_0}(\mathbf{w}) \underbrace{\lambda_q(x)} = \bar{\lambda}_{q_0}(\mathbf{w}) \lambda_q(y) = \bar{\lambda}_{q_0}(\mathbf{w}y).$$

Consequently, we would lose the injectivity of  $\bar{\lambda}_{q_0}$ , contradicting the hypothesis of its invertibility.

Analogously we can see that  $\lambda_q$  is surjective: let us take a word  $\mathbf{w} \in \mathbf{X}^*$  such that  $\bar{\pi}(\mathbf{w}, q_0) = q$  and  $y \in \mathbf{X}$ . We search an  $x \in \mathbf{X}$  such that  $\lambda_q(x) = y$ . Since  $\bar{\lambda}_{q_0}$  is invertible and synchronous automatic, the word  $\bar{\lambda}_{q_0}(\mathbf{w})y$  has a unique preimage, and it is of the form  $\mathbf{w}x$  for some  $x$ . Therefore:  $\bar{\lambda}_{q_0}(\mathbf{w})y = \bar{\lambda}_{q_0}(\mathbf{w}x) = \bar{\lambda}_{q_0}(\mathbf{w})\lambda_q(x)$ .

$(\Leftarrow)$  The transition function moves necessarily to an accessible state  $q$  for each  $\mathbf{w} \in \mathbf{X}^*$ . We know that  $\lambda_p : \mathbf{X} \rightarrow \mathbf{X}$  is invertible for each accessible  $p$ , including all the states on the path to  $q$ . Now we will prove that  $\bar{\lambda}_{q_0}$  is invertible on  $\mathbf{X}^n$  by induction on  $n$ , consequently it will be invertible on  $\bigcup_{n \in \mathbb{N}} \mathbf{X}^n = \mathbf{X}^*$ .

$(n = 1)$  On  $\mathbf{X}$  we have  $\bar{\lambda}_{q_0} = \lambda_{q_0}$ , therefore  $\bar{\lambda}_{q_0}$  is invertible by the hypothesis.

$(n \Rightarrow n + 1)$  Let us suppose that  $\bar{\lambda}_{q_0}$  is invertible on  $\mathbf{X}^n$ . If  $\mathbf{v} \in \mathbf{X}^{n+1}$  then  $\mathbf{v} = \mathbf{w}x \in \mathbf{X}^n \times \mathbf{X}$  with  $|\mathbf{w}| = n$ . Thus  $\bar{\lambda}_{q_0}(\mathbf{v}) = \bar{\lambda}_{q_0}(\mathbf{w}x) = \bar{\lambda}_{q_0}(\mathbf{w})\bar{\lambda}_{\bar{\pi}(\mathbf{w}, q_0)}(x) = \bar{\lambda}_{q_0}(\mathbf{w})\lambda_p(x)$  for some  $p$ . We observe now that if we change  $\mathbf{w}$  or  $x$ , we obtain a different image with respect to  $\bar{\lambda}_{q_0}$  on  $\mathbf{X}^n$  and with respect to  $\lambda_{q_0}$  on  $\mathbf{X}$  (injectivity). Furthermore, if we search for the preimage of a word  $\bar{\mathbf{w}}\bar{x} \in \mathbf{X}^{n+1}$ , we know that there exists a preimage  $\mathbf{w}$  of  $\bar{\mathbf{w}}$  through  $\bar{\lambda}_{q_0}$  and a preimage  $x$  of  $\bar{x}$  with respect to  $\lambda_{\bar{\pi}(\mathbf{w}, q_0)}$ . If we glue them together, we obtain:

$$\bar{\lambda}_{q_0}(\mathbf{w}x) = \bar{\lambda}_{q_0}(\mathbf{w})\lambda_{\bar{\pi}(\mathbf{w}, q_0)}(x) = \bar{\mathbf{w}}\bar{x}.$$

So surjectivity of  $\bar{\lambda}_{q_0}$  is proven. □

**Proposition 4.4.** The set  $\mathcal{GA}(X)$  of all bijective synchronous automatic transformations on an alphabet  $X$  is a group with respect to the composition operation. Furthermore, it is isomorphic to  $\mathcal{AUT}_{tree}(\mathbf{X}^*)$ , the group of all tree-automorphism of  $\mathbf{X}^*$ .

*Proof.* The set  $\mathcal{GA}(X)$  consists of all bijective elements of  $\mathcal{GA}(X)$ , hence it is a group. □



**Definition 4.5.** An initial automaton  $\mathcal{A}_{q_0}$  is called **invertible** if its action is invertible. An automaton  $\mathcal{A}$  is called **invertible** if  $\mathcal{A}_{q_0}$  is invertible for each  $q_0 \in \mathcal{Q}$ .

**Convention 3.** We introduce a different notation for Moore diagrams. Let  $q, p$  be vertices of a Moore diagram and  $q \rightarrow p$  an edge between them. Recalling Definition 2, this means there exists  $x, y \in \mathbf{X}$  such that  $\pi(x, q) = p$  and  $\lambda(x, q) = y$ . Then we label the arrow from  $q$  to  $p$  by the letter  $x$  and the vertex  $p$  by the function  $\lambda(\cdot, q) : \mathbf{X} \rightarrow \mathbf{X}$ . See Figure 6 for an example.

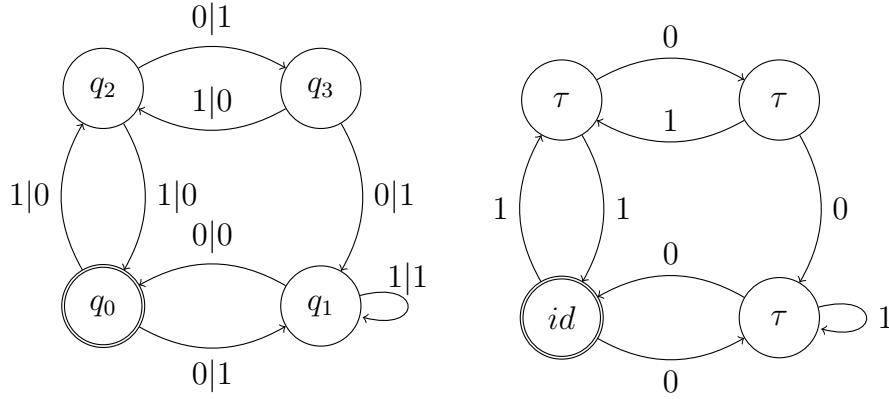


FIGURE 6. An example of the same initial automaton represented in two different ways. In the right figure  $\tau, id \in \mathcal{S}_2 := \mathcal{S}(\{0, 1\})$ , where,  $\tau$  inverts the elements in  $\{0, 1\}$  and  $id$  leaves them unchanged.

**Definition 4.6.** Given an automaton  $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$  we can define  $|\mathcal{Q}|$  initial automata, which define  $|\mathcal{Q}|$  actions  $\bar{\lambda}_q$  on  $\mathbf{X}^*$  inside  $\mathcal{FSA}(\mathbf{X})$ . By the **semigroup generated by  $\mathcal{A}$**  we mean the subsemigroup  $H(\mathcal{A})$  of  $\mathcal{FSA}(\mathbf{X})$  generated by all the actions  $\bar{\lambda}_q$  with  $q \in \mathcal{Q}$ :

$$H(\mathcal{A}) = \langle \{\bar{\lambda}_q : \mathbf{X}^* \rightarrow \mathbf{X}^* | q \in \mathcal{Q}\} \rangle,$$

where, for a set  $S$ ,  $\langle S \rangle$  means the semigroup generated by the elements of  $S$ , i.e. the smallest semigroup which contains all the elements of  $S$ .

**Remark 9.** *If  $\mathcal{A}$  is invertible then  $H(\mathcal{A})$  is the group generated by  $\mathcal{A}$ , and we have that  $H(\mathcal{A}) \subseteq \mathcal{GA}(\mathbf{X})$ .*

**Convention 4.** From now on by an automaton and by an initial automaton we mean an **invertible automaton** and an **invertible initial automaton**, respectively.

## Semidirect and wreath products

### Part 3. Group products and their applications in this context ?

#### 5. ACTIONS, SEMIDIRECT PRODUCTS AND WREATH PRODUCTS

Given a set  $X$ ,  $\mathcal{S}(X)$  denotes the **symmetric group on  $X$** , that is the group of all permutations  $\sigma : X \rightarrow X$ .

**Definition 5.1.** Let  $\circ$  be the composition of functions. We define  $f \cdot g := g \circ f$ .

### 5.1. Actions.

**Definition 5.2.** Given a group  $G$  and a set  $X$ , we call a **left  $G$ -action on  $X$**  or an **left action of  $G$  on  $X$**  an homomorphism of groups  $T_l : G \longrightarrow (\mathcal{S}(X), \circ)$ . We can also say that  $G$  **acts on  $X$  from the left by  $T_l$** . We say that  $G$  acts on  $X$  from the right by  $T_r$  if there exists an homomorphism  $T_r : G \longrightarrow (\mathcal{S}(X), \cdot)$ .

**Proposition 5.3.** *Let us take a group  $(G, *)$  and a set  $X$ . Then  $G$  is acting on  $X$  from the left if and only if exist a function  $\tau_l : G \times X \longrightarrow X$  such that:*

- $1x := \tau_l(1, x) = x$  for every  $x \in X$ ,
- $g(hx) := \tau_l(g, \tau_l(h, x)) = \tau_l(g * h, x) =: (g * h)x$  for every  $x \in X$  and  $g, h \in G$ .

Analogously  $G$  is acting on  $X$  from the right if and only if exist a function  $\tau_r : X \times G \longrightarrow X$  such that:

- $x1 := \tau_r(x, 1) = x$  for every  $x \in X$ ,
- $(xh)g := \tau_r(\tau_r(x, h), g) = \tau_r(x, h * g) =: x(h * g)$  for every  $x \in X$  and  $g, h \in G$ .

*Proof.* We prove just the case of left action.

- ( $\Leftarrow$ ) We define  $(T_l(g))(x) := \tau_l(g, x)$ , therefore we have  $T_l(g * h)(x) = \tau_l(g * h, x) = \tau_l(g, \tau_l(h, x)) = T_l(g)(\tau_l(h, x)) = (T_l(g) \circ T_l(h))(x)$  for every  $x \in X$ .
- ( $\Rightarrow$ ) This is similar. □

The main difference between acting from the left and from the right is the order in which we let the element of  $G$  act on  $X$ . Let us see some examples:

**Example 5.4.** The symmetric group  $(\mathcal{S}(X), \circ)$  on a set  $X$  acts on  $X$  from the left, in fact we can define  $T_l(\sigma)(x) = \sigma x := \sigma(x) \quad \forall \sigma \in \mathcal{S}(X)$  and  $\forall x \in X$ . Analogously we can define  $T_r(\sigma)(x) = x\sigma := \sigma(x)$ . Let  $X$  be such that  $|X| > 3$ , then  $\mathcal{S}(X)$  is not abelian. Let us take  $\sigma, \eta \in \mathcal{S}(X)$  such that  $\sigma \circ \eta \neq \eta \circ \sigma$ . Then there exists  $x$  such that  $x\sigma\eta \neq \sigma\eta x$ . This shows that  $\tau_l(\sigma\eta, x) \neq \tau_r(x, \sigma\eta)$ . ◇

**Example 5.5** (translations). Let  $A$  be an affine space, and let  $V$  be a vector space associated to it. Let  $T_l : V \longrightarrow \mathcal{S}(A)$  be a function such that  $T_l(\mathbf{v})(P) := P + \mathbf{v}$ , where  $P + \mathbf{v}$  is the translation of  $P \in A$  by the vector  $\mathbf{v} \in V$ . Then it is easy to see that  $T_l$  is a left action of  $V$  on  $A$ .

Let us now define the right action  $T_r(\mathbf{v})(P) = \mathbf{v} + P := P + \mathbf{v}$  and denote by  $+_V$  the operation of addition on  $V$ . We have an interesting consequence:

$$\begin{aligned} T_r(\mathbf{v} +_V \mathbf{w})(P) &= (\mathbf{v} +_V \mathbf{w}) + P = P + (\mathbf{v} +_V \mathbf{w}) = (P + \mathbf{v}) +_V \mathbf{w} = \\ &= \mathbf{w} + (P + \mathbf{v}) = (\mathbf{w} +_V \mathbf{v}) + P := P + (\mathbf{w} +_V \mathbf{v}) = T_l(\mathbf{w} +_V \mathbf{v})(P). \end{aligned}$$

This happens because  $V$  is abelian. ◇

**Example 5.6** (synchronous automatic bijective transformations). The group of all synchronous automatic bijective transformations  $(\mathcal{GA}(\mathbf{X}), \circ)$  acts from the left on  $\mathbf{X}^*$ :

- The identity of  $\mathcal{GA}(\mathbf{X})$  is  $id_{\mathcal{S}(\mathbf{X}^*)}$ , the identical function of  $\mathcal{S}(\mathbf{X}^*)$ . Therefore given  $\mathbf{v} \in \mathbf{X}^*$  we have that  $id_{\mathcal{S}(\mathbf{X}^*)}(\mathbf{w}) = \mathbf{w}$ .
  - Given  $f, g \in \mathcal{GA}(\mathbf{X})$  we have that  $(f \circ g)(\mathbf{w}) = f(g(\mathbf{w}))$ .
- ◇

**Definition 5.7.** Let  $G$  be a group acting from the right on  $X$  by  $T_r : G \rightarrow (\mathcal{S}(X), \cdot)$ . Then  $T_r$  is called **faithful** if it is **injective**. We then say that  $G$  acts **faithfully** on  $X$  by  $T_r$  from the right. In this case we say that  $(X, G)$  is a **right permutation group**.

Left permutation groups, denoted  $(G, X)$ , are defined analogously.

**Proposition 5.8.** A group  $G$  acts faithfully on a set  $X$  from the left if and only if for every  $h$  and  $g$  in  $G$  there exists  $x$  in  $X$  such that  $gx \neq hx$ .

A group  $G$  acts faithfully on a set  $X$  from the right if and only if for every  $h$  and  $g$  in  $G$  there exists  $x$  in  $X$  such that  $xg \neq xh$ .

*Proof.* It follows directly from Definition 5.7 and Proposition 5.3.  $\square$

**Proposition 5.9.** Let  $(\mathcal{S}(X), \circ)$  be the symmetric group on  $X$ . Then the function  $T_r : (\mathcal{S}(X), \circ) \rightarrow (\mathcal{S}(X), \cdot)$  defined by  $\sigma \mapsto \sigma^{-1}$  is a right action of  $(\mathcal{S}(X), \circ)$  on  $X$ .

*Proof.* We have that  $T_r(\eta^{-1} \circ \sigma^{-1})(x) = T_r((\sigma \circ \eta)^{-1})(x) = (\sigma \circ \eta)(x) = (\eta \cdot \sigma)(x) = T_r(\eta^{-1}) \cdot T_r(\sigma^{-1})(x)$ . Therefore  $T_r$  is an homomorphism.  $\square$

This motivates the introduction of ~~this~~ notation:

**Convention 5.** We denote  $T_r(\sigma\eta)(x)$  by  $x\eta\sigma$ . From now on whenever we will encounter  $(X, \mathcal{S}(X))$ , we will assume that  $\mathcal{S}(X)$  is endowed with the operation  $\circ$ , and that  $(\mathcal{S}(X), \circ)$  acts on  $X$  from the right as in Proposition 5.9.

**Remark 10.** If  $B$  is a group, we can consider  $(B, B)$  as a right permutation group, with  $B$  acting on itself by right multiplication.

Till now we have considered right actions  $T : G \rightarrow (\mathcal{S}(X), \cdot)$ . If the set  $N := X$  is also a group we consider right actions such that  $T(G) \subseteq \text{AUT}(N)$ , where  $\text{AUT}(N)$  is the group of automorphisms of  $N$ . In other words, given a group  $G$  we consider actions on  $N$  so that:

$$(n *_N n') g = n g *_N n' g$$

for all  $g \in G$  and all  $n, n' \in N$ .

**Remark 11.** Note that  $\text{AUT}(N) \subset \mathcal{S}(N)$ .

**5.2. Semidirect products.** We will define semidirect products using actions from the right. There is a possible definition also with actions from the left.

**Definition 5.10.** Let  $H, N$  be groups, with operations  $*_H$  and  $*_N$ , where  $H$  acts on  $N$  from the right by  $\varphi : H \rightarrow (\text{AUT}(N), \cdot)$ . On  $H \times N$  we define the following operation:

$$\star_\varphi : ((h_2, n_2), (h_1, n_1)) \mapsto (h_2 *_H h_1, \varphi(h_1)(n_2) *_N n_1) = (h_2 h_1, (n_2 h_1) *_N n_1)$$

We call  $(H \times N, \star_\varphi)$  the **semidirect product**  $H \ltimes_\varphi N$  of  $H$  and  $N$  relative to  $\varphi$  and we denote it by  $H \ltimes_\varphi N$ . We can also refer to  $\varphi$  as the **underlying homomorphism** of the semidirect product  $H \ltimes_\varphi N$ .

The open side of  $\ltimes$  points towards the group acted upon.

**Proposition 5.11.** The semidirect product  $H \ltimes_\varphi N$  is a group, where the identity element is  $(1_H, 1_N)$  and  $(h^{-1}, \varphi(h^{-1}))(n^{-1})$  is the inverse for  $(h, n)$ .

*Proof.* We prove just the associativity. The rest of the proof is an easier verification. Let  $(h'', n''), (h', n'), (h, n)$  be elements of  $H \rtimes_{\varphi} N$ . Then:

$$\begin{aligned}
 ((h'', n'') *_{\varphi} (h', n')) *_{\varphi} (h, n) &= (h''h', \varphi(h')(n'') * n') *_{\varphi} (h, n) = \\
 &= (h''h'h, (\varphi(h)((\varphi(h')(n'')) * n') * n) = \\
 &= (h''h'h, (\varphi(h) \circ \varphi(h'))(n'') * \varphi(h)(n') * n) = \\
 &= (h''h'h, (\varphi(h') \cdot \varphi(h))(n'') * \varphi(h)(n') * n) = \\
 &= (h''h'h, \varphi(h'h)(n'') * \varphi(h)(n') * n) = \\
 &= (h'', n'') *_{\varphi} (h'h, \varphi(h)(n') * n) = \\
 &= (h'', n'') *_{\varphi} ((h', n') *_{\varphi} (h, n)). \bullet
 \end{aligned}$$

□

**Example 5.12** (dihedral groups). Given a geometrical object  $A$  one can consider the set of all bijective geometrical transformations which leave  $A$  unchanged. By their definition, the composition of two ~~such~~ transformations also ~~has~~ leaves  $A$  unchanged. This set forms a group called the group of symmetries of  $A$ .

Let  $A$  be a regular polygon with  $n$  sides. The group of symmetries of this figure is  $\mathcal{D}_n$ , the so called  **$n$ -dihedral group**. There are two types of transformations in it, the rotation of  $\frac{k\pi}{n}$  degrees around the centre of the polygon, and the reflection with respect to one of the  $n$  axes of symmetry.



FIGURE 7. All the possible symmetries of an octagon visualised using a sign of STOP. The upper ones are all the rotations (elements  $(0, k)$ ), and the lowest one all the reflections (elements  $(1, k)$ ). The image has been taken from [Wikipedia](#).

It turns out that the group  $\mathcal{D}_n$  is isomorphic to the semidirect product  $\mathbb{Z}_2 \rtimes_{\varphi} \mathbb{Z}_n$ , where the action of  $\mathbb{Z}_2$  on  $\mathbb{Z}_n$  is given by  $\varphi(0)(z) := id_{\mathbb{Z}_n}(z) = z$  and  $\varphi(1)(z) := inv_{\mathbb{Z}_n}(z) := -z(mod\ n)$ . For example,  $\mathbb{Z}_2 \rtimes_{\varphi} \mathbb{Z}_n \ni (h_2, n_2) * (0, n_1) = (h_2 + 0, n_1 + n_2)$  and  $(h_2, n_2) * (1, n_1) = (h_2, n_1 - n_2)$ . We can notice that  $(h, k) = (h, 0) * (0, k)$ . The transformation  $(0, k)$  is necessarily always a rotation, while  $(h, 0)$  is the identity or the reflection through the central axis, depending if  $h = 0$  or  $h = 1$ . In other words, if we have  $(h, k) \in \mathbb{Z}_2 \rtimes_{\varphi} \mathbb{Z}_n$ ,  $h$  encodes the reflection and  $k$  the rotation.  $\diamond$

**5.3. Wreath products.** We follow [9].

**Definition 5.13.** Given a group  $A$  and a set  $Y$ , we define the **direct product**  $A^Y$  as:

$$A^Y := \prod_{\omega \in Y} A := \{\bar{a} = (a_{\omega})_{\omega \in Y} : a_{\omega} \in A\}$$

and the **direct sum**  $A^{(Y)}$  as:

$$A^{(Y)} := \bigoplus_{\omega \in Y} A_{\omega} := \{\tilde{a} = (a_{\omega})_{\omega \in Y} : a_{\omega} \in A \text{ and } a_{\omega} \neq 1_A \text{ only for a finite number of } \omega\}$$

If  $|Y|$  is finite, we have  $A^Y = A^{(Y)}$ .

**Remark 12.** If  $A$  is a group we can extend its operation  $*_A$  to  $A^Y$  and  $A^{(Y)}$  component-wise.

Now let  $(Y, B)$  be a right permutation group and  $A$  be a group. The group  $B$  acts faithfully from the right on  $A^Y$  permuting the indices  $Y$ , so we have an injective homomorphism  $\Phi : B \rightarrow (\mathcal{S}(A^Y), \cdot)$ . If we prove that  $\Phi(B) \subseteq \mathcal{AUT}(A^Y)$  we have everything we need to construct  $B \ltimes_{\Phi} A^Y$ . ~~The same can be done substituting  $A^Y$  with  $A^{(Y)}$ .~~ Let us formalise this:

**Proposition 5.14.** Let  $(Y, B)$  be a right permutation group with action given by  $(y, \beta) \mapsto y\beta$  and let  $A$  be a group. Then  $\Phi : B \rightarrow (\mathcal{S}(A^Y), \cdot)$  defined as

$$\Phi(\beta)((a_y)_{y \in Y}) = (a_{y\beta})_{y \in Y}$$

is a faithful right action of  $B$  on  $A^Y$  and consequently  $(A^Y, B)$  is a right permutation group. In addition we have that  $\Phi(B) \subseteq \mathcal{AUT}(A^Y)$ , where  $A^Y$  is equipped with the component-wise operation on  $A$ .

~~The same can be done substituting  $A^Y$  with  $A^{(Y)}$ .~~

A similar statement holds also is replaced

Proof. Let  $\beta \in B$  and  $\bar{a} \in A^Y$ . We have:

$$\Phi_{\beta}(\bar{a}) = \bar{a}\beta = (a_y)_{y \in Y}\beta := (a_{y\beta})_{y \in Y} = (a_y)_{y\beta^{-1} \in Y}$$

- (1) We must prove that  $\Phi(\beta)$  is bijective for every  $\beta \in B$ . Let us prove first the injectivity. Let  $\bar{a}, \bar{x} \in A^Y$  and let us consider  $\Phi(\beta)(\bar{a}) = (a_{y\beta})_{y \in Y} = (x_{y\beta})_{y \in Y} = \Phi(\beta)(\bar{x})$ . Then  $a_y = a_{y\beta\beta^{-1}} = x_{y\beta\beta^{-1}} = x_y$  for every  $y \in Y$ , and so  $\bar{a} = \bar{x}$ , hence  $\Phi(\beta)$  is injective. The surjectivity is very simple: if we have  $(a_y)_{y \in Y}$ , the element  $(a_{y\beta^{-1}})_{y \in Y}$  is its inverse image.
- (2) We now prove that  $\Phi(B) \subseteq \mathcal{AUT}(A^Y)$ , i.e. that  $\Phi_{\beta}$  is an automorphism:  $\Phi_{\beta}(\bar{a} \star \bar{x}) = \Phi_{\beta}((a_y \star x_y)_{y \in Y}) = (a_{y\beta} \star x_{y\beta})_{y \in Y} = (a_{y\beta})_{y \in Y} \star (x_{y\beta})_{y \in Y} = \Phi_{\beta}(\bar{a}) \star \Phi_{\beta}(\bar{x})$ .
- (3) We must prove that  $\Phi$  is ~~X~~ faithful, i.e., that if  $\Phi_{\beta} = \Phi_{\theta}$  then  $\beta = \theta$ . Let us suppose that  $\Phi_{\beta} = \Phi_{\theta}$ . We have, for every  $(a_y)_{y \in Y} \in A^Y$ , that  $(a_{y\beta})_{y \in Y} = \Phi_{\beta}((a_y)_{y \in Y}) = \Phi_{\theta}((a_y)_{y \in Y}) = (a_{y\theta})_{y \in Y}$ . It follows that  $y\beta = y\theta$  for every  $y \in Y$ . Since the action of  $B$  on  $Y$ , given by  $(y, \beta) \mapsto y\beta$ , is faithful, we have that  $\beta = \theta$ . ~~And so~~ the proof is finished.

For If we take  $A^{(Y)}$ , the proof is similar because if  $(a_y)_{y \in Y}$  has only a finite number of indices different from  $1_A$ , so does  $(a_{y\beta})_{y \in Y}$  for every  $\beta \in B$ .  $\square$

**Definition 5.15.** Let  $(Y, B)$  be a right permutation group and let  $A$  be a group. Suppose that we have a right action  $\Phi : B \rightarrow (\mathcal{AUT}(A^Y), \cdot)$  defined as in Proposition 5.14.

- We call  $B \ltimes_{\Phi} A^Y$  the **unrestricted wreath product**  $B \wr A$  of  $B$  and  $A$  and we denote it by  $B \wr A$ .
- We call  $B \ltimes_{\Phi} A^{(Y)}$  the **restricted wreath product**  $B \wr A$  of  $B$  and  $A$  and we denote it by  $B \wr A$ .

Therefore, having  $(\beta, \bar{p}), (\theta, \bar{q})$  in  $B \times A^Y$  (or in  $B \times A^{(Y)}$ ), their product in the group  $(B \rtimes_{\Phi} A^Y, *_\Phi)$  (or in the group  $(B \times A^{(Y)}, *_\Phi)$ ) is:

$$\begin{aligned} (\beta, \bar{p}) *_\Phi (\theta, \bar{q}) &= (\beta, (p_y)_{y \in Y}) *_\Phi (\theta, (q_y)_{y \in Y}) := \\ &= (\beta *_B \theta, (\Phi(\theta))(\bar{p}) *_A \bar{q}) = (\beta *_B \theta, (p_{y\theta} *_A q_y)_{y \in Y}) = (\beta\theta, (p_{y\theta}q_y)_{y \in Y}). \end{aligned}$$

If we take ~~two~~ groups  $B, A$  we can construct their wreath product  $B \wr A$  considering  $(B, B)$  a right permutation group, where  $B$  acts faithfully on itself by right multiplication.

From the context it will be clear if we are considering unrestricted or restricted wreath products. If  $Y$  is finite there is no difference between the two, and a more precise notation is used:

**Convention 6.** Let  $(B, Y), A, B \wr A = B \rtimes_{\Phi} A^Y$  be as previously defined, and let  $Y = \{y_1, \dots, y_k\}$ . Then  $\bar{a} \in A^Y$  is uniquely written as  $(a_1, \dots, a_k)$ . We denote  $(\beta, \bar{a}) \in B \wr A$  by  $\beta(a_1, \dots, a_k)$ . With this convention, given  $\beta(a_1, \dots, a_k)$  and  $\theta(g_1, \dots, g_k)$  in  $B \wr A$ , the multiplication rule  $*_{\Phi}$  becomes:

$$\begin{aligned} \beta(a_1, \dots, a_k) *_\Phi \theta(g_1, \dots, g_k) &= \beta\theta((a_1\theta, \dots, a_k\theta) *_A (g_1, \dots, g_k)) = \\ &= \beta\theta(a_1\theta g_1, \dots, a_k\theta g_k) \end{aligned}$$

and the inverse of  $\beta(a_1, \dots, a_k)$  is:

$$\beta^{-1}((g_1\beta^{-1})^{-1}, \dots, (g_k\beta^{-1})^{-1}).$$

**Remark 13.** Semidirect and wreath products arise often in mathematics. Interesting examples involve groups used to understand and solve sudoku or the Rubik's cube.

delete or provide source!

## 6. APPLICATIONS TO AUTOMATA

We will see the wreath product construction in the context of automata. First we will need to gather all the ingredients.

**Convention 7.** From now on the operation of composition of words will be denoted by the dot ".".

**Proposition 6.1.** Let  $\mathbf{X}$  be an alphabet. Denote by  $\mathcal{AUT}_{tree}(\mathbf{X}^*)$  the group of tree-automorphisms on  $\mathbf{X}^*$ . Then there exists a left  $\mathcal{AUT}_{tree}(\mathbf{X}^*)$ -action  $T$  on  $\mathbf{X}$  as a set  $(T : (\mathcal{AUT}_{tree}(\mathbf{X}^*), \circ) \longrightarrow (\mathcal{S}(\mathbf{X}), \circ))$  defined by  $T(f)(x) := f(x)$ .

*Proof.* The function  $f$  is a tree-automorphism, so by Proposition 3.5,  $f(\mathbf{X}) = (\mathbf{X})$ , therefore  $T(f)$  is a bijection on the alphabet  $\mathbf{X}$ . Furthermore we have that  $T(f \circ g)(x) = (f \circ g)(x) = f(g(x)) = T(f)(g(x)) = (T(f) \circ T(g))(x)$ , consequently  $T(f \circ g) = T(f) \circ T(g)$ , and so  $T$  is an homomorphism.  $\square$

We now take the right permutation group  $(\mathbf{X}, \mathcal{S}(\mathbf{X}))$  and the group  $\mathcal{AUT}_{tree}(\mathbf{X}^*)$ , where both  $\mathcal{S}(\mathbf{X})$  and  $\mathcal{AUT}(\mathbf{X}^*)$  are provided with the composition of functions denoted by  $\circ$  as their operation. We have so a right action of  $\mathcal{S}(\mathbf{X})$  on  $\mathcal{AUT}_{tree}(\mathbf{X}^*)^{\mathbf{X}}$  defined by  $\Phi(\sigma)(f_{x_1}, \dots, f_{x_k}) = (f_{x_1\sigma}, \dots, f_{x_k\sigma})$ , where  $x_i\sigma$  is the element  $\sigma(x_i) \in \mathbf{X}$ , and  $f_{x_i}$  is the restriction of  $f$  in  $x_i$  as defined in (3).

**Proposition 6.2.** Let  $\mathbf{X} = \{x_1, \dots, x_k\}$  and let  $T$  be as in the previous proposition. Let us take a right permutation group  $(\mathbf{X}, \mathcal{S}(\mathbf{X}))$ , where  $\mathcal{S}(\mathbf{X})$  acts as a group from



the right on  $\mathcal{AUT}_{tree}(\mathbf{X}^*)^{\mathbf{X}}$  by  $\Phi(\sigma)(f_{x_1}, \dots, f_{x_k}) = (f_{x_1\sigma}, \dots, f_{x_k\sigma})$ . Let us define  $\psi : (\mathcal{AUT}_{tree}(\mathbf{X}^*), \circ) \longrightarrow (\mathcal{S}(\mathbf{X}), \circ) \wr (\mathcal{AUT}_{tree}(\mathbf{X}^*), \circ) = \mathcal{S}(\mathbf{X}) \ltimes_{\Phi} \mathcal{AUT}_{tree}(\mathbf{X}^*)^{\mathbf{X}}$  as

$$\psi(f) = T(f)(f|_{x_1}, \dots, f|_{x_k})$$

where  $f|_{x_k}$  is the restriction of  $f$  in  $x_k$  as defined in 3.6. Then  $\psi$  is an isomorphism of groups.

*Proof.* • We prove that  $\psi$  is an homomorphism. Let  $f, g \in \mathcal{AUT}_{tree}(\mathbf{X}^*)$ . Then:

$$\begin{aligned} \psi(f)\psi(g) &= T(f)(f|_{x_1}, \dots, f|_{x_k}) *_{\Phi} T(g)(g|_{x_1}, \dots, g|_{x_k}) = \\ &= T(f)T(g)(f|_{x_1 T(g)} g|_{x_1}, \dots, f|_{x_k T(g)} g|_{x_k}) = \\ &= T(fg)((fg)|_{x_1}, \dots, (fg)|_{x_k}) = \\ &= \psi(fg) \end{aligned}$$

- We prove that  $\psi$  is ~~an~~ injective. If  $T(f)(f|_{x_1}, \dots, f|_{x_k}) = \psi(f) = \psi(g) = T(g)(g|_{x_1}, \dots, g|_{x_k})$  we have that  $f(x) = T(f)(x) = T(g)(x) = g(x)$  for every  $x \in \mathbf{X}$ . And since  $f|_{x_i} = g|_{x_i}$  for every  $x_i \in \mathbf{X}$ , it follows that  $f(x\mathbf{v}) = f(x)f|_x(\mathbf{v}) = g(x)g|_x(\mathbf{v}) = g(x\mathbf{v})$ . Consequently  $f = g$ , and  $\psi$  is one-to-one.
- We prove that  $\psi$  is ~~an~~ surjective. Let  $\beta(a_1, \dots, a_k)$  be an element of  $\mathcal{S}(\mathbf{X}) \wr \mathcal{AUT}_{tree}(\mathbf{X}^*)$ . Let us denote  $(a_1, \dots, a_k)$  by  $(a_{x_1}, \dots, a_{x_k})$ . Given  $\mathbf{w} = w_1 \dots w_n \in \mathbf{X}^*$  with  $n > 0$  we define  $f(\mathbf{w}) := \beta(w_1).a_{w_1}(w_2 \dots w_n)$  and  $f(\emptyset) := \emptyset$ . It is easy to verify that  $f$  is a tree-automorphism and that  $\psi(f) = \beta(a_{x_1}, \dots, a_{x_k})$ . □

The consequences of this result are very important: since by Proposition 4.4  $\mathcal{GA}(\mathbf{X})$ , the set of synchronous automatic transformations on  $\mathbf{X}$ , can be identified with  $\mathcal{AUT}_{tree}(\mathbf{X}^*)$ , the set of tree-automorphisms on  $\mathbf{X}^*$ , we have that every element in  $\mathcal{GA}(\mathbf{X})$  can be identified with some element  $\beta(a_1, \dots, a_k)$  in  $\mathcal{S}(\mathbf{X}) \wr \mathcal{AUT}_{tree}(\mathbf{X}^*)$  and viceversa. This leads to the following result.

**Proposition 6.3.** *The group  $\mathcal{S}(\mathbf{X}) \wr \mathcal{AUT}_{tree}(\mathbf{X}^*)$  acts **faithfully** on  $\mathbf{X}^*$  as a set from the left by:*

$$\beta(a_{x_1}, \dots, a_{x_k})(w_1 w_2 \dots w_n) = \beta(w_1).a_{w_1}(w_2 \dots w_n)$$

*Proof.* The group  $\mathcal{S}(\mathbf{X}) \wr \mathcal{AUT}_{tree}(\mathbf{X}^*)$  is isomorphic to  $\mathcal{AUT}_{tree}(\mathbf{X}^*)$  by  ~~$\psi^{-1}$  defined as in~~ Proposition 6.2. The group  $\mathcal{AUT}_{tree}(\mathbf{X}^*)$  acts faithfully from the left on  $\mathbf{X}^*$  by the identity function  $id : \mathcal{AUT}_{tree}(\mathbf{X}^*) \longrightarrow \mathcal{AUT}_{tree}(\mathbf{X}^*)$  because it is a subgroup of  $\mathcal{S}(\mathbf{X}^*)$ . Thus the group  $\mathcal{S}(\mathbf{X}) \wr \mathcal{AUT}_{tree}(\mathbf{X}^*)$  acts faithfully from the left by  $id \circ \psi^{-1} : \mathcal{S}(\mathbf{X}) \wr \mathcal{AUT}_{tree}(\mathbf{X}^*) \longrightarrow \mathcal{AUT}_{tree}(\mathbf{X}^*) \subseteq \mathcal{S}(\mathbf{X}^*)$  because  $id$  and  $\psi^{-1}$  are isomorphisms. Let  $\beta(a_{x_1}, \dots, a_{x_k}) \in \mathcal{S}(\mathbf{X}) \wr \mathcal{AUT}_{tree}(\mathbf{X}^*)$  and  $w_1 w_2 \dots w_n \in \mathbf{X}^*$ . There exists  $f \in \mathcal{AUT}_{tree}(\mathbf{X}^*)$  such that  $\psi(f) = \beta(a_{x_1}, \dots, a_{x_k})$ . Thus we have that:

$$\begin{aligned} id \circ \psi^{-1}(\beta(a_{x_1}, \dots, a_{x_k}))(w_1 w_2 \dots w_n) &= f(w_1 w_2 \dots w_n) = f(w_1)f|_{w_1}(w_2 \dots w_n) = \\ &= T(f)(w_1).a_{w_1}(w_2 \dots w_n) = \\ &= \beta(w_1).a_{w_1}(w_2 \dots w_n). \end{aligned}$$

*Proof.* let  $\varphi$  be the isomorphism from prop. 6.2. □  
The action of  $\varphi$  coincides with the action of  $\varphi(f)$ . Thus the

action  $v \neq f(f)$  is faithful. The statement follows  
 for any  $f \in \text{Aut tree}(X^*)$

**Proposition 6.4.** Let  $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$  be an automaton such that  $\mathcal{Q} = \{q_1, \dots, q_n\}$  and  $\mathbf{X} = \{x_1, \dots, x_k\}$ . Then the set of all the actions  $\bar{\lambda}_{q_l}$  defined by  $\mathcal{A}$  can be described with  $n$  recurrent formulas

$$(4) \quad \begin{aligned} f_{q_1} &= \beta_{q_1}(h_{x_1, q_1}, \dots, h_{x_k, q_1}), \\ f_{q_2} &= \beta_{q_2}(h_{x_1, q_2}, \dots, h_{x_k, q_2}), \\ &\dots \\ f_{q_n} &= \beta_{q_n}(h_{x_1, q_n}, \dots, h_{x_k, q_n}), \end{aligned}$$

EGA(X)

where each  $h_{x_i, q_j}$  is equal to some  $f_{q_l}$  and each  $\beta_{q_j}$  is a permutation of the alphabet. Conversely, Let  $S$  be a system of type (4), where each  $h_{x_i, q_j}$  is equal to some  $f_{q_l}$  and each  $\beta_j$  is a permutation of the alphabet. Then  $S$  defines uniquely an automaton  $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$  such that  $\bar{\lambda}_{q_l} = f_{q_l}$  for every  $q_l \in \mathcal{Q}$ .

*Proof.* Let  $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$  be an automaton. Each initial automaton  $\mathcal{A}_{q_l}$  defines a transformation  $\lambda_{q_l}$  in  $\mathcal{GA}(\mathbf{X})$ . By Proposition 3.8 we have that the restriction  $\bar{\lambda}_{q_l}|_x$  is equal to  $\bar{\lambda}_{\pi(x, q_l)} = \bar{\lambda}_p$  for some  $p \in \mathcal{Q}$ . Therefore  $\psi(\bar{\lambda}_{q_l}) = T(\bar{\lambda}_{q_l})(\bar{\lambda}_{\pi(x_1, q_l)}, \dots, \bar{\lambda}_{\pi(x_k, q_l)}) = \lambda_{q_l}(\bar{\lambda}_{\pi(x_1, q_l)}, \dots, \bar{\lambda}_{\pi(x_k, q_l)})$ , where  $\psi$  is defined as in Proposition 6.2 and  $\lambda_{q_l}$  is a permutation of  $\mathbf{X}$  because  $\mathcal{A}$  is invertible. Hence we obtain:

$$(5) \quad \begin{aligned} \bar{\lambda}_{q_1} &= \lambda_{q_1}(\bar{\lambda}_{\pi(x_1, q_1)}, \dots, \bar{\lambda}_{\pi(x_n, q_1)}), \\ \bar{\lambda}_{q_2} &= \lambda_{q_2}(\bar{\lambda}_{\pi(x_1, q_2)}, \dots, \bar{\lambda}_{\pi(x_n, q_2)}), \\ &\dots \\ \bar{\lambda}_{q_n} &= \lambda_{q_n}(\bar{\lambda}_{\pi(x_1, q_n)}, \dots, \bar{\lambda}_{\pi(x_n, q_n)}), \end{aligned}$$

where each  $\bar{\lambda}_{\pi(x_i, q_j)}$  is equal to  $\bar{\lambda}_{q_l}$  for  $\pi(x_i, q_j) = q_l \in \{q_1, \dots, q_n\}$ , and each  $\lambda_{q_j}$  is a permutation of the alphabet  $\mathbf{X}$ .

From the converse let us take a system  $S$  of the type (4). We have that each  $h_{x_i, q_j}$  is equal to some  $f_{q_l}$ . Let us define:

$$\begin{aligned} \pi(x_i, q_j) &= q_l, \\ \lambda(x_i, q_j) &= \beta_{q_j}(x_i). \end{aligned}$$

Then  $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$  is an automaton because each  $\lambda_{q_j}$  is a permutation of  $\mathbf{X}$ . We have that  $\bar{\lambda}_{\pi(x_i, q_j)}(\mathbf{w}) = \bar{\lambda}_{q_l}(\mathbf{w})$  for every  $\mathbf{w} \in \mathbf{X}^*$ . It follows that, given  $x_i \in \mathbf{X}$ ,  $\bar{\lambda}_{q_j}(x_i w_2 \dots w_n) = \lambda_{q_j}(x_i) \cdot \bar{\lambda}_{\pi(x_i, q_j)}(w_2 \dots w_n) = \beta_{q_j}(x_i) \cdot f_{q_l}(w_2 \dots w_n)$ . Since this is valid for every  $x_i \in \mathbf{X}$ , we have  $\bar{\lambda}_{q_j} = f_{q_j}$  for every  $q_j \in \mathcal{Q}$ .  $\square$

## Part 4. The classification theorem

In this section we present a result discovered by Grigorchuk and Zuk in [6], which describes all groups generated by 2-state-automata on a 2-letter-alphabet. Our demonstration here follows [4].

### 7. PROPEDEUTICS

We introduce some of the objects that arise in the formulation and in the proof of the classification theorem.

Prerequisites for preliminaries



**7.1. The infinite dihedral group.** We have seen that in the *finite* case the dihedral group  $\mathbb{Z}_2 \rtimes_{\varphi} \mathbb{Z}_n$  (5.12) is given as the symmetry group of the regular polygon with  $n$  sides. We now generalise it. *this*

**Definition 7.1.** The group  $\mathbb{Z}_2 \rtimes_{\varphi} \mathbb{Z}$  is called the **infinite dihedral group** and is denoted by  $\mathcal{D}_{\infty}$ . *think  $\mathbb{Z}$*

~~We find an object identifiable with  $\mathbb{Z}$ . We help ourselves thinking of it as the infinite line of integers.~~ *of*

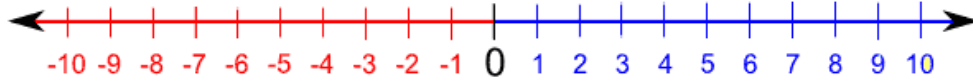


FIGURE 8. The line of integers (image taken from **Math Only Math**).

Then we can describe the action of the element  $(0, k)$  on this figure as a shift to the right by  $k$  positions, and the element  $(1, 0)$  as the reflection around the origin ( $z \mapsto -z$ ). Therefore the infinite dihedral group is the group of symmetries of  $\mathbb{Z}$ , that we represent as a line.

**7.2. The lamplighter group.** According to [11] the first reference to this algebraic object was anonymously made in [7] in 1983 and remained unnoticed for many years.

**Definition 7.2.** The **lamplighter group**  $\mathcal{L}$  is the *restricted* wreath product  $\mathbb{Z} \wr \mathbb{Z}_2 = \mathbb{Z} \ltimes \mathbb{Z}_2^{(\mathbb{Z})}$ .

*So* the elements of  $\mathcal{L}$  are of the form  $(z, (h_i)_{i \in \mathbb{Z}})$  with  $z \in \mathbb{Z}$  and  $h_i \in \mathbb{Z}_2$ , and just a finite number of  $h_i$  are different from  $0_{\mathbb{Z}_2}$ . Each  $(z, (h_i)_{i \in \mathbb{Z}})$  can be imagined as an infinite dark road ( $\mathbb{Z}$ ), with lampions every 10 meter ( $h_i$ ), and just a finite number of them turned on (the indices  $i$  for which  $h_i \neq 0_{\mathbb{Z}_2}$ ). *And* in a specific position  $z$ , near some lampion, we can see a man, the lamplighter.

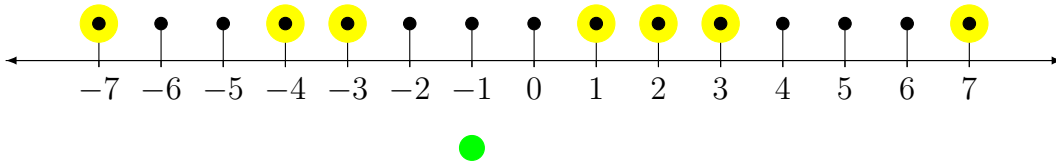


FIGURE 9. A representation of an **element**  $(-1, (h_i)_{i \in \mathbb{Z}})$  in  $\mathcal{L}$ . The green circle represent the coordinate  $-1$  of the lamplighter, while the yellow circles represent the lit on lampions at positions  $\{-7, -4, -3, 1, 2, 3, 7\}$ , i.e., the position  $i$  for which  $h_i \neq 0_{\mathbb{Z}_2}$ .

The product of two elements of  $\mathcal{L}$  is:

$$(z_2, (h_i)_{i \in \mathbb{Z}}) * (z_1, (k_i)_{i \in \mathbb{Z}}) = (z_1 + z_2, (h_{i+z_1} +_{\mathbb{Z}_2} k_i)_{i \in \mathbb{Z}}).$$

The inverse of  $(z, (h_i)_{i \in \mathbb{Z}})$  is  $(-z, (h_{i-z})_{i \in \mathbb{Z}_2})$ .

**7.3. The adding machine.**

**Definition 7.3.** Let  $\mathbf{X} = \{0, 1\}$ . The **adding machine** is the synchronous automatic transformation  $f = \tau(id_{\mathcal{G}\mathcal{A}(\mathbf{X})}, f) : \mathbf{X}^* \longrightarrow \mathbf{X}^*$ , where  $\tau$  is the transposition of  $\mathcal{S}(\mathbf{X})$ .

We call it adding machine because of the way it acts on  $\mathbf{X}^n$ .

$$(6) \quad \begin{aligned} f(0y_2 \dots y_n) &= \tau(0).id_{\mathcal{GA}(\mathbf{X})}(y_2 \dots y_n) = 1y_2 \dots y_n \\ f(1y_2 \dots y_n) &= \tau(1).f(y_2 \dots y_n) = 0.f(y_2 \dots y_n) \end{aligned}$$

Let us define the function  $t_n : \mathbf{X}^n \longrightarrow \mathbb{Z}/2^n\mathbb{Z} = \mathbb{Z}_{2^n}$  by:

$$(7) \quad t_n(y_1 \dots y_k \dots y_n) = y_1 + y_2 2 + \dots + y_k 2^{k-1} + \dots + y_n 2^{n-1}.$$

It easy to prove that  $t_n$  is bijective, and thus we can ~~so~~ translate the action of  $f$  to  $\mathbb{Z}_{2^n}$  by  $t_n$ .

The equations (6) tells us that if  $x_1 \dots x_k \dots x_n = \mathbf{w}_1 x_k \mathbf{w}_2 = \mathbf{w}_1 0 \mathbf{w}_2$  is a sequence, where  $\mathbf{w}_1$  is a sequence of 1s, while at position  $k$  there is the **first element**  $x_k = 0$ , then  $f(\mathbf{w}_1 x_k \mathbf{w}_2) = f(\mathbf{w}_1 0 \mathbf{w}_2) = \mathbf{v}_1.f(0 \mathbf{w}_2) = \mathbf{v}_1.\tau(0).id(\mathbf{w}_2) = \mathbf{v}_1 1 \mathbf{w}_2$ , where  $\mathbf{v}_1$  is a sequence of 0s. Then (7) yields:

$$\begin{aligned} (f \circ t_n^{-1})(t_n(x_1 \dots x_k \dots x_n)) &= \\ &= (f \circ t_n^{-1})(x_1 + x_2 2 + \dots + x_{k-1} 2^{k-2} + x_k 2^{k-1} + x_{k+1} 2^k \dots + x_n 2^{n-1}) = \text{why?} \\ &= (f \circ t_n^{-1})(1 + 1 \cdot 2 + \dots + 1 \cdot 2^{k-2} + 0 \cdot 2^{k-1} + x_{k+1} 2^k \dots + x_n 2^{n-1}) \leftarrow \text{why?} \\ &= t_n^{-1}(0 + 0 \cdot 2 + \dots + 0 \cdot 2^{k-2} + (t_{n-k} \circ f \circ t_{n-k}^{-1})(0 \cdot 2^{k-1} + x_{k+1} 2^k \dots + x_n 2^{n-1})) = \\ &= t_n^{-1}(0 + 0 \cdot 2 + \dots + 0 \cdot 2^{k-2} + 1 \cdot 2^{k-1} + id(x_{k+1} 2^k \dots + x_n 2^{n-1})) = \\ &= t_n^{-1}(0 + 0 \cdot 2 + \dots + 0 \cdot 2^{k-2} + 1 \cdot 2^{k-1} + x_{k+1} 2^k \dots + x_n 2^{n-1}) = \\ &= t_n^{-1}(t_n(x_1 \dots x_k \dots x_n) + 1). \end{aligned}$$

If instead  $x_1 \dots x_k \dots x_n = 1 \dots 1$  is the sequence without 0s, we have that:

$$\begin{aligned} (f \circ t_n^{-1})(t_n(x_1 \dots x_k \dots x_n)) &= \\ &= (f \circ t_n^{-1})(1 + 1 \cdot 2 + \dots + 1 \cdot 2^{n-1}) = (f \circ t_n^{-1})(2^n - 1) = \text{why?} \\ &= t_n^{-1}(0 + 0 \cdot 2 + \dots + 0 \cdot 2^{k-2} + (f \circ t_{n-k}^{-1})(1 \cdot 2^{k-1} + 1 \cdot 2^k \dots + 1 \cdot 2^{n-1})) = \\ &= t_n^{-1}(0 + 0 \cdot 2 + \dots + 0 \cdot 2^{k-2} + 0 \cdot 2^{n-1}) = \\ &= t_n^{-1}(1 + 1 \cdot 2 + \dots + 1 \cdot 2^{n-1} + 1) = t_n^{-1}(t_n(x_1 \dots x_k \dots x_n) + 1) = t_n^{-1}(2^n) = t_n^{-1}(0). \end{aligned}$$

This means that  $t_n \circ f$  adds 1 to each number in  $\mathbb{Z}_{2^n}$ .

Let us now focus on  $\langle f \rangle$ . In order to study it we need to look closer to a particular property of the function  $f$ .

**Definition 7.4.** A left action of  $G$  on  $X$  is said to be **transitive** if, for each  $x, y \in X$ , there exists an element  $g \in G$  such that  $gx = y$ .

**Definition 7.5.** A synchronous transformation  $s : \mathbf{X}^* \longrightarrow \mathbf{X}^*$  is called **spherically transitive** if  $\langle s \rangle$  acts transitively on  $\mathbf{X}^n$  for each  $n$ .

**Proposition 7.6.** If a synchronous transformation  $s : \mathbf{X}^* \longrightarrow \mathbf{X}^*$  is spherically transitive, then  $\langle s \rangle$  is infinite.

*Proof.* Let  $n \in \mathbb{N}$  and  $\mathbf{w}$  be an element of  $\mathbf{X}^n$ . Then, for each  $\mathbf{v} \in \mathbf{X}^n$ , there exists  $g_{\mathbf{v}} \in G$  such that  $g_{\mathbf{v}} \mathbf{w} = \mathbf{v}$ . This yields  $|G| \geq n$ , so  $G$  is infinite.  $\square$

**Proposition 7.7.** Let  $f$  be the adding machine. Then  $\langle f \rangle$  is spherically transitive and isomorphic to  $\mathbb{Z}$ .

*Proof.* Let  $\mathbf{y} = y_1 y_2 \dots y_n$ ,  $\mathbf{x} = x_1 x_2 \dots x_n$  be two sequences in  $\mathbf{X}^n$ . As in (7) let us consider  $t_n(\mathbf{y})$  and  $t_n(\mathbf{x})$  in  $\mathbb{Z}_{2^n}$ . We define  $m \in \mathbb{N} \cup \{0\}$  such that  $m = t_n(\mathbf{y}) - t_n(\mathbf{x}) \pmod{2^n}$ . Let us consider  $f^m \in \langle f \rangle$ . Then we have that:

$$t_n(f^m(\mathbf{x})) = t_n(\mathbf{x}) + m = t_n(\mathbf{x}) + (t_n(\mathbf{y}) - t_n(\mathbf{x})) = t_n(\mathbf{y}) \pmod{2^n},$$

which yields  $f^m(\mathbf{x}) = \mathbf{y}$  because  $t_n$  is bijective. Therefore  $f$  is spherically transitive and infinite. We define:

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow \langle f \rangle \\ m &\longmapsto f^m. \end{aligned}$$

We have that  $m_1 + m_2 \mapsto f^{m_1+m_2} = f^{m_1} \circ f^{m_2}$  so  $\phi$  is an homomorphism which is obviously surjective. Finally let  $k$  be the smallest element in  $\mathbb{Z}$  such that  $\phi(k) = f^0 = id$ . If  $k \neq 0$  we would have that  $|\langle f \rangle| = k$ , which is not possible because  $\langle f \rangle$  is infinite. Therefore the kernel of  $\phi$  is trivial, hence  $\phi$  is an isomorphism.  $\square$

## 8. THE THEOREM

**Theorem 8.1.** *Let  $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$  be an automaton. Let  $\mathbf{X} = \{0, 1\}$  and  $|\mathcal{Q}| = 2$ . Then the group generated by  $\mathcal{A}$  is isomorphic to one of the following groups:*

- (1) *The trivial group  $\{1\}$ ,*
- (2) *The 2nd order group  $(\mathbb{Z}_2, +)$ ,*
- (3) *The direct sum  $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ ,*
- (4) *The infinite cyclic group  $\mathbb{Z}$ ,*
- (5) *The infinite dihedral group  $\mathcal{D}_\infty$ ,*
- (6) *The lamplighter group  $\mathcal{L}$ .*

I would like to stress the beauty of this theorem, which shows us that also such complex groups as the last three ones can arise from such simple model of machines.

## 9. PROOF

We follow the proof in [4]. We provide only a part of the proof.

**9.1. Define the cases.** To prove Theorem 8.1 we need to examine case by case groups defined by each possible automaton  $\mathcal{A}$ . Let us verify in how many ways we can define the functions  $\pi$  and  $\lambda$ .

- ( $\pi$ ) Graphically, from each state there exit two possible arrows, and each can arrive to one of the two states. Algebraically, the function  $\pi$  has domain  $\mathbf{X} \times \mathcal{Q}$  and codomain  $\mathcal{Q}$ , so for its definition there are  $|\mathcal{Q}|^{|\mathbf{X} \times \mathcal{Q}|} = 2^{2 \cdot 2} = 16$  possibilities.
- ( $\lambda$ ) We can define the output function by its restrictions  $\lambda(\cdot, q)$ . For each  $q \in \mathcal{Q}$  the function  $\lambda(\cdot, q) : \mathbf{X} \longrightarrow \mathbf{X}$ , must be a permutation of the alphabet  $\mathbf{X}$ . Since  $\mathbf{X} = \{0, 1\}$ , there are only two possible permutations: the transposition  $\tau$ , which exchanges the two symbols, and the identity  $id$ , which leaves them unchanged. So there are 2 possibilities for  $\lambda(\cdot, q)$  and there are 2 states  $q$  in  $\mathcal{Q}$ . This means there are  $2 \cdot 2 = 4$  possible ways to define  $\lambda$ .

Overall this means  $16 \cdot 4 = 64$  possible ways to define  $\mathcal{A}$ .

Let  $\{q, s\}$  be the states of the automaton  $\mathcal{A}$ . Consequently the group is generated by the actions  $a = \bar{\lambda}_q$  and  $b = \bar{\lambda}_s$ . As we have seen in Proposition 6.4, we can define  $\mathcal{A}$  by the recursive formulas:

$$(8) \quad \begin{aligned} a &= \sigma^{i_1}(x_{11}, x_{12}), \\ b &= \sigma^{i_2}(x_{21}, x_{22}), \end{aligned}$$

where  $\sigma^{i_1}, \sigma^{i_2}$  are elements of  $\mathcal{S}_2 := \mathcal{S}(\mathbf{X}) = \mathcal{S}(\{0, 1\})$  and  $x_{ij} \in \{a, b\}$  (notice that we have two possibilities for each variable of the equation, so  $2^6 = 64$  cases as seen before). We suppose that  $i_1, i_2 \in \{0, 1\}$  and  $\sigma^0 := id_{\mathcal{S}(2)}$ , while  $\sigma^1 = \tau$  is the other element of  $\mathcal{S}_2$ , the transposition.

**Remark 14.** Recall that  $\mathcal{GA}(\mathbf{X})$  acts **faithfully** on  $\mathbf{X}^*$ , therefore two elements  $c, d$  of  $\mathcal{GA}(\mathbf{X})$  act in the same way on  $\mathbf{X}^*$  ( $c\mathbf{w} = d\mathbf{w}$  for every  $\mathbf{w}$ ) if and only if  $c = d$ .

**Convention 8.** From now on  $id$  will stand for the identity permutation of some **group set**, usually  $\mathcal{GA}(\mathbf{X})$  or  $\mathcal{S}(\mathbf{X})$  and it will be clear from the context which specific **group set** is being considered.

**9.2. Refinement of case analysis.** If  $\sigma^{i_1} = \sigma^{i_2} = id_{\mathcal{S}_2} = id$ , then  $a = b = id_{\mathcal{GA}(\mathbf{X})}$ , so we obtain the trivial group  $\{1\}$ . So we no longer need to consider the 16 cases where

$$\begin{aligned} a &= id(x_{11}, x_{12}) = id, \\ b &= id(x_{21}, x_{22}) = id. \end{aligned}$$

We need to consider just the cases where at least one between  $\sigma^{i_1}$  and  $\sigma^{i_2}$  acts non trivially on  $\mathbf{X}$ . ~~Denoting by  $\tau$  the transposition of  $\mathcal{S}_2$ ,~~ we notice that each case:

$$(9) \quad \begin{aligned} a &= \tau(x_{11}, x_{12}), \\ b &= \sigma^{i_2}(x_{21}, x_{22}), \end{aligned}$$

generates the same group as the case:

$$\begin{aligned} a &= \sigma^{i_2}(x_{21}, x_{22}), \\ b &= \tau(x_{11}, x_{12}). \end{aligned}$$

This means that we can analyse just the  $2^5 = 32$  cases (each non-fixed variable has two possible definitions) of the system (9) to see every possible group generated.

Let us define  $f : \mathcal{GA}(\mathbf{X}) \rightarrow \mathcal{GA}(\mathbf{X})$  by

$$(10) \quad \sigma(c|_0, c|_1) \mapsto \sigma(c|_1, c|_0).$$

We have that:

$$\begin{aligned} f(\gamma(c|_0, c|_1)\sigma(d|_0, d|_1)) &= f(\gamma\sigma(c|_{0\sigma}d|_0, c|_{1\sigma}d|_1)) = \gamma\sigma(c|_{1\sigma}d|_1, c|_{0\sigma}d|_0) = \\ &= \gamma(c|_1, c|_0)\sigma(d|_1, d|_0) = f(\gamma(c|_0, c|_1))f(\sigma(d|_0, d|_1)), \end{aligned}$$

so  $f$  is an homomorphism. It is easy to verify it is bijective. If  $p \in \langle a, b \rangle = G$ , then  $p = x_1x_2 \dots x_n$  with  $x_i \in \{a, b, a^{-1}, b^{-1}\}$  and  $f(p) = f(x_1x_2 \dots x_n) = f(x_1)f(x_2) \dots f(x_n) \in \langle f(a), f(b) \rangle$ . This means that  $G$  is isomorphic to  $f(G) = \langle f(a), f(b) \rangle$ . This tells us that the case

$$\begin{aligned} a &= \tau(a, b), \\ b &= \sigma^{i_2}(x_{21}, x_{22}) \end{aligned}$$

generates a group isomorphic to the one generated by the case

$$\begin{aligned} a &= \tau(b, a), \\ b &= \sigma^{i_2}(x_{22}, x_{21}). \end{aligned}$$

It follows that we can treat only the 24 cases where  $a \in \{\tau(a, a), \tau(a, b), \tau(b, b)\}$ .

**9.3. The cases with  $a = \tau(a, a)$ .** If we have  $a = \tau(a, a) = \tau(a|_0, a|_1)$ , then:

$$\begin{aligned} a^2 &= \tau(a|_0, a|_1) * \tau(a|_0, a|_1) = \\ &= \tau\tau(a|_0, a|_0, a|_1, a|_1) = \\ &= id(a^2, a^2). \end{aligned}$$

Therefore  $a^2 = id(a^2, a^2) = id_{\mathcal{GA}(\mathbf{X})}$ . This means  $a$  acts on  $\mathbf{X}^*$  changing each letter in a word to its opposite ( $\mathbf{X}$  has just two letters), and has order 2. Now we look at  $b$ .

- (1.1) If  $b = id(b, b)$ ,  $b = a^2$  acts on  $\mathbf{X}^*$  as the identity, then  $\langle a, b \rangle$  is isomorphic to  $(\mathbb{Z}_2, +)$  by  $a \mapsto 1$  and  $b \mapsto 0$ .
- (1.2) If  $b = \tau(a, a)$ , then  $b = a$  and  $\langle a, b \rangle = \langle a \rangle = \{id, a\}$ . Since  $a$  has order 2,  $\langle a \rangle$  is isomorphic to  $\mathbb{Z}_2$ .
- (1.3) If  $b = \tau(b, b)$ ,  $b$  acts on  $\mathbf{X}^*$  changing each letter in a word to its opposite, so  $b = a$  (recall Remark 14) and so  $\langle a, b \rangle = \langle a \rangle$  is again isomorphic to  $\mathbb{Z}_2$ .
- (1.4) If  $b = id(a, a)$ , then  $b$  acts on  $\mathbf{X}^*$  by changing each letter but the first one, so  $b^2 = id_{\mathcal{GA}(\mathbf{X})}$ . Furthermore,  $ab$  acts by changing just the first letter, and the same does  $ba$ , so recalling Remark 14, since they acts in the same way on  $\mathbf{X}^*$ ,  $ba = ab$ . It follows that  $\langle a, b \rangle = \{id = a^2, a, b, ab\}$  is isomorphic to  $(\mathbb{Z}_2 \oplus \mathbb{Z}_2, +)$  by the maps

$$\begin{aligned} a^2 = b^2 &\mapsto (0, 0), \\ a &\mapsto (1, 1), \\ b &\mapsto (0, 1), \\ ab = ba &\mapsto (1, 0). \end{aligned}$$

- (1.5) If  $b = \tau(a, b) = \tau(b|_0, b|_1)$  then:

$$ba^{-1} = ba = \tau(a, b)\tau(a, a) = \tau\tau(ba, aa) = id(ba, aa) = id_{\mathcal{S}_2}(ba, id_{\mathcal{GA}(\mathbf{X})}).$$

Therefore,  $ba$  acts by leaving the first letter unchanged, and if the second letter is 0 acts again, otherwise  $a^2 = id_{\mathcal{GA}(\mathbf{X})}$  acts on the rest of the word. So  $ba$  leaves each word unchanged:  $ba = id$ . So  $b = a^{-1} = a$ , because  $a$  has order 2. So again we have an isomorphism to  $\mathbb{Z}_2$ .

- (1.6) If  $b = id(a, b)$  we obtain the infinite dihedral group. The proof is omitted.
- (1.7) If  $b = \tau(b, a)$ , with the homomorphism  $f$  defined in (10), we have that  $\langle a, b \rangle = \langle \tau(a, a), \tau(b, a) \rangle$  is isomorphic to the group of case (1.5)  $\langle f(a), f(b) \rangle = \langle \tau(a, a), \tau(a, b) \rangle$ .
- (1.8) If  $b = id(b, a)$  the group  $\langle a, b \rangle = \langle \tau(a, a), id(b, a) \rangle$  is isomorphic to  $\langle f(a), f(b) \rangle = \langle \tau(a, a), id(a, b) \rangle$ , i.e., case (1.6).

**9.4. The cases with  $a = \tau(b, a)$ .** Let  $a = \tau(b, a) = \tau(a|_0, a|_1)$ .

- (2.1) If  $b = \tau(b, a) = \tau(b|_0, b|_1)$  then  $a = b$ , therefore  $a = \tau(a, a) = b = \tau(a, a)$  and so  $\langle a, b \rangle$ , as in case (1.2), is isomorphic to  $\mathbb{Z}_2$ .

(2.2) If  $b = \tau(a, b) = \tau(b|_0, b|_1)$  then:

$$\begin{aligned} ba^{-1} &= \tau(b|_0, b|_1) \tau(a|_1^{-1}, a|_0^{-1}) = \tau\tau(b|_1 a|_1^{-1}, b|_0 a|_0^{-1}) = \\ &= id(ba^{-1}, ab^{-1}), \\ ab^{-1} &= \tau(a|_0, a|_1) \tau(b|_1^{-1}, b|_0^{-1}) = id(a|_1 b|_1^{-1}, a|_0 b|_0^{-1}) = \\ &= id(ab^{-1}, ba^{-1}). \end{aligned}$$

This yields that if  $c := ba^{-1}$  and  $d := ab^{-1}$ , then:

$$\begin{aligned} c &= id(c, d), \\ d &= id(d, c). \end{aligned}$$

So  $c = d = id_{\mathcal{GA}(\mathbf{X})}$ , because they both leave each word unchanged. This gives us the equality  $id_{\mathcal{GA}(\mathbf{X})} = c = ba^{-1}$  which leads to  $a = b = \tau(a, b) = \tau(b, b)$ , and consequently to  $a^2 = id(a^2, a^2) = id_{\mathcal{GA}(\mathbf{X})}$ . So  $\langle a, b \rangle = \langle a \rangle = \{id_{\mathcal{GA}(\mathbf{X})}, a\}$ , which is isomorphic to  $\mathbb{Z}_2$ .

(2.3) If  $b = \tau(b, b)$ , then denoting  $b' := a$  and  $a' := b$ , we get  $a' = \tau(a', a')$  and  $b' = \tau(a', b')$  and we see again the case (1.5), so isomorphism with  $\mathbb{Z}_2$ .

(2.4) If  $b = \tau(a, a)$  we have:

$$\begin{aligned} ba^{-1} &= \tau(a, a) \tau(a^{-1}, b^{-1}) = id(id, ab^{-1}), \\ ab^{-1} &= \tau(b, a) \tau(a^{-1}, a^{-1}) = id(id, ba^{-1}). \end{aligned}$$

Then defining  $c := ba^{-1}$  and  $d := ab^{-1}$ , we get the same conclusion as in case (2.2), isomorphism with  $\mathbb{Z}_2$ .

(2.5) If  $b = id(b, b)$ , then  $b = id_{\mathcal{GA}(\mathbf{X})}$ , and  $a = \tau(id_{\mathcal{GA}(\mathbf{X})}, a)$ . Here  $a$  acts as the adding machine. Therefore  $\langle a, b \rangle = \langle a \rangle$  is isomorphic to  $\mathbb{Z}$ .

(2.6) If  $b = id(a, a)$ , the group  $G := \langle a, b \rangle$  is isomorphic to  $\mathbb{Z}$ . To arrive to this result we shall prove that  $G$  is cyclic, i.e., is generated by one element. We omit the proof that its cardinality is infinite. Then  $G$ , being infinite and cyclic, it is isomorphic to  $\mathbb{Z}$ . We prove that  $G$  is cyclic:

$$\begin{aligned} ba &= id(a, a) \tau(b, a) = \tau(ab, a^2), \\ ab &= \tau(b, a) id(a, a) = \tau(ba, a^2), \end{aligned}$$

which yields  $ba = ab$ , that is  $\langle a, b \rangle$  is abelian. Furthermore,


$$ba^2 = ba a = \tau(ba, a^2) \tau(b, a) = id(a^2 b, a^2 b).$$

Consequently,  $ba^2 = 1$ . We claim that  $G := \langle a, b \rangle = \langle ab \rangle$ . In fact  $ab$  generates  $b$  by  $(ab)^2 = abab = b(ba^2) = b$ , and  $ab$  and  $b$  generate  $a$  by  $abb^{-1} = a$ . Therefore  $G$  is cyclic generated by  $ab$ .

(2.7) If  $b = id(b, a)$  then  $\langle a, b \rangle = \mathcal{L}$  is the lamplighter group  $\mathcal{L}$ , but we are going to skip the proof.

(2.8) If  $b = id(a, b)$ , we can reach the symmetric case of the (2.7). Let us take  $b^{-1} = id(a^{-1}, b^{-1})$ ,  $a^{-1} = \tau(a^{-1}, b^{-1})$ . In general, since  $a^{-1}, b^{-1} \in \langle a, b \rangle$ , and consequently  $a, b \in \langle a^{-1}, b^{-1} \rangle$ , we have that  $\langle a, b \rangle = \langle a^{-1}, b^{-1} \rangle$ . So we can observe the group generated by  $a^{-1}, b^{-1}$ . Let us now take a generic element  $d = \tau(d, d) \in \mathcal{GA}(\mathbf{X})$ . Then:

$$\begin{aligned} (b^{-1})^d &= d^{-1} b^{-1} d = \tau(d^{-1}, d^{-1}) id(a^{-1}, b^{-1}) \tau(d, d) = id((b^{-1})^d, (a^{-1})^d), \\ (a^{-1})^d &= d^{-1} a^{-1} d = \tau(d^{-1}, d^{-1}) \tau(a^{-1}, b^{-1}) \tau(d, d) = \tau((b^{-1})^d, (a^{-1})^d). \end{aligned}$$

Let us call  $b' := b^{-1}$  and  $a' = a^{-1}$ . We showed that we can study the group generated by  $a', b'$ . Let us take the generic element  $x_1 x_2 \dots x_k$  with  $x_i \in \{a', b'\}$ . We observe that its conjugate by  $d$ ,  $(x_1 x_2 \dots x_k)^d$ , is the same as  $(x_1)^d (x_2)^d \dots (x_k)^d$ . This tells us that the each element in  $\langle a'^d, b'^d \rangle$  is conjugate to some element of  $\langle a', b' \rangle$  and viceversa. So the conjugate of the group  $\langle a', b' \rangle$  is  $\langle a'^d, b'^d \rangle$ , therefore they are isomorphic. So again, with another jump, we can define  $b'' := (b^{-1})^d = b'^d$  and  $a'' := (a^{-1})^d = a'^d$  and focus on  $\langle a'', b'' \rangle$  that is isomorphic to  $\langle a, b \rangle$ . For the equations above we have that 

$$\begin{aligned} a'' &= \tau(b'', a''), \\ b'' &= id(b'', a''). \end{aligned}$$

That is the case (2.7).

**9.5. The cases with  $a = \tau(b, b)$ .** Let  $a = \tau(b, b)$ .

- (3.1)-(3.2) The case  $b = \tau(a, b)$  is analogous to (2.4), while the case  $b = \tau(b, a)$  is symmetrical to (2.4), both leading to  $\mathbb{Z}_2$ .
- (3.3)-(3.4) If  $b = \tau(b, b)$  then  $b = a = \tau(a, a)$ , and we have the case (1.2) with  $\mathbb{Z}_2$ . If  $b = \tau(a, a)$  we arrive to the same conclusion.
- (3.5) If  $b = (b, b)$  then  $b = id$  and  $a = \tau(id, id)$ , so  $\langle a \rangle = \{id, a\}$  is isomorphic to  $\mathbb{Z}_2$ .
- (3.6)-(3.7) These cases lead to the infinite dihedral group. The proof is omitted.
- (3.8) If  $b = id(a, a)$ , then:

$$\begin{aligned} a^2 &= id(b^2, b^2), \\ b^2 &= id(a^2, a^2), \\ ba &= \tau(ab, ab), \\ ab &= \tau(ba, ba). \end{aligned}$$

This yields  $a^2 = b^2 = id$  and to  $ab = ba = \tau(ab, ab)$  (abelian group). For this reason we can see each possible word  $x_1 x_2 \dots x_k$  with  $x_i \in \{a, b, a^{-1}, b^{-1}\} = \{a, b\}$  as  $a^n b^m$  where  $n + m = k$ . In addition, we know that  $a^n = a^{n \pmod{2}}$  and  $b^m = b^{m \pmod{2}}$ , so each possible composition of  $a$  and  $b$  is an element  $a^i b^j$ , where  $i, j \in \{0, 1\}$ . So the group  $\langle a, b \rangle = \{id, a, b, ab\}$  is isomorphic to  $\mathbb{Z}_2 \oplus \mathbb{Z}_2$  by:

$$\begin{aligned} id &\longmapsto (0, 0), \\ a &\longmapsto (1, 0), \\ b &\longmapsto (0, 1), \\ ba &\longmapsto (1, 1), \end{aligned}$$

□

## CONCLUDING REMARKS

In this thesis we have gone through just a part of the theory of automata. We considered just finite deterministic Mealy automata, but if instead the reader may want to explore a broader class of objects, [3] is a very good source where to start



from. Otherwise for some more practical application of the theory there is the book [10]. The book [8] explores in the details the structures of subsection 5.3.

If the reader is interested to know more about the lamplighter group, I can recommend [1] for an approach which requires just the knowledge of an undergraduate, and [11] for an analysis in the case we take a finite version of this object.

For more examples of automata in connection to groups I recommend [2], where can be found the complete classification of 3-state-automata over a 2-letter-alphabet. can be found. The book [9] is another very good source, and the article [12] shows 5 algebraic problems which can be solved with the group generated by some specific automaton. The most notable example in the latter class is the first Grigorchuk group, analysed in 1984 in [5].

## ACKNOWLEDGEMENTS

I would like to thank both my Supervisors prof. Alessandro Logar and izr. prof. Ganna Kudryavtseva, and in particular the latter one, for all the time she spent helping me and for her infinite patience with my clumsiness. Then I would like to thank prof. Valentina Beorchia and prof. Marko Petkovšek thanks to whom I could participate in this exchange program. Without them this would not have even started. I need to thank also prof. Sašo Strle, who managed to follow me and other tens of students in the completion of the bachelor thesis. Finally I would like to thank my beloved ones, who managed to bear me during the last period.

## REFERENCES

- [1] Bonanome M.C., Dean M.H., Dean J.P. (2018) The L lamplighter group L2. In: *A sampling of remarkable groups*. Compact Textbooks in Mathematics. Birkhäuser, Cham. [https://doi.org/10.1007/978-3-030-01978-5\\_4](https://doi.org/10.1007/978-3-030-01978-5_4).
- [2] Bondarenko I., Grigorchuk R., Kravchenko R., Muntyan Y., Nekrashevych V., Savchuk D., Sunic Z., *Classification of groups generated by 3-state automata over a 2-letter alphabet*, 2008, 0803.3555, arXiv, math.GR.
- [3] Eilenberg S., Pure and applied mathematics, Elsevier, Volume 59, Part A, 1974, Page iii, ISSN 0079-8169, ISBN 9780122340017, [https://doi.org/10.1016/S0079-8169\(08\)60872-7](https://doi.org/10.1016/S0079-8169(08)60872-7). (<https://www.sciencedirect.com/science/article/pii/S0079816908608727>).
- [4] Grigorchuk R. I., Nekrashevych V. V., Sushchanskii V. I., “Automata, dynamical systems, and groups”, *Dynamical systems, automata, and infinite groups*, Collected papers, Tr. Mat. Inst. Steklova, **231**, Nauka, MAIK «Nauka/Inteperiodika», M., 2000, 134–214; Proc. Steklov Inst. Math., **231** (2000), 128–203.
- [5] Grigorchuk R.I., Machí A., *An example of an indexed language of intermediate growth*, Theoretical Computer Science, Volume 215, Issues 1–2, 1999, Pages 325–327, [https://doi.org/10.1016/S0304-3975\(98\)00161-3](https://doi.org/10.1016/S0304-3975(98)00161-3). (<https://www.sciencedirect.com/science/article/pii/S0304397598001613>).
- [6] Grigorchuk, R.I., Żuk, A., *The lamplighter group as a group generated by a 2-state automaton, and its spectrum*. Geometriae Dedicata 87, 209–244 (2001). <https://doi.org/10.1023/A:1012061801279>.
- [7] Kaimanovich, V. A.; Vershik, A. M., *Random walks on discrete groups: Boundary and entropy*. Ann. Probab. 11 (1983), no. 3, 457–490. <https://projecteuclid.org/euclid.aop/1176993497>.
- [8] Meldrum J. D. P. (1995), *Wreath products of groups and semigroups*, Longman [UK] / Wiley [US].
- [9] Nekrashevych V. V., *Self-similar groups*, volume 117 of Mathematical Surveys and Monographs. Amer. Math. Soc., Providence, RI, 2005.
- [10] Rhodes, John and Nehaniv, Chrystopher L and Hirsch, Morris W, *Applications of automata theory and algebra*, World Scientific Publishing Co. Pte. Ltd. , 2009, <https://doi.org/10.1007/978-1-4020-9000-0>.





[www.worldscientific.com/doi/abs/10.1142/7107](http://www.worldscientific.com/doi/abs/10.1142/7107) (<https://www.worldscientific.com/doi/pdf/10.1142/7107>).

- [11] Siehler J. A. (2012) *The finite lamplighter groups: A guided tour*, The College Mathematics Journal, 43:3, 203–211, DOI: 10.4169/college.math.j.43.3.203.
- [12] Zuk A., *Automata groups* - Topics in noncommutative geometry, 165–196, Clay Math. Proc., 16, Amer. Math. Soc., Providence, RI, 2012.