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

Tesi finale

Automatne grupe

Delo diplomskega seminarja

Groups of automata

Final Thesis

Supervisori/Mentorja/Supervisors
izr. prof. dr. Ganna Kudryavtseva
prof. Alessandro Logar

2020

Contents

Groups of automata

Abstract

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

In the first part we introduce the input and output as sequences of symbols from an alphabet $\mathbf{X}$, and we show some structure on them. In particular we visualise the set $\mathbf{X}^*$ of the finite sequences as a rooted tree. Then we illustrate the formal definition of the finite deterministic Mealy automaton (we will simply call it automaton) $\mathcal{A}$, and we show some examples by Moore diagrams (graph representations of automata). Finally we derive the concept of initial automaton $\mathcal{A}_{q_0}$ and its action $\bar{\lambda}_{q_0}$.

In part number two we lift up the level of description of these machines, giving a more abstract characterization of their actions as transformations $f : \mathbf{X}^* \longrightarrow \mathbf{X}^*$, as tree-morphisms, and analysing their properties. We see the operation of composition of automata. We successively restrict our vision to invertible automata and study how does this manifest in terms of accessibility of states. Finally the reader see the definition of group generated by an automaton.

In the third part we describe some algebraic structures necessary to approach groups of automata. So the first step is to describe left and right actions of a group acting on a set, then right actions φ of a group G on a group N s.t. $\varphi(G) \subset \mathcal{AUT}(N)$ (where $\mathcal{AUT}(N)$ is the set of group automorphisms on N), the semidirect products and finally the wreath products. And at last we show why did we need to give this description applying these structures to automata.

In part number four we present a result of [5, 7]: the classification of groups generated by 2-state-automata over a 2-letter-alphabet. First we must introduce two important objects of the theorem, i.e., the infinite dihedral group and the lamplighter group. Then we illustrate a precise synchronous automatic function, called the adding machine, which will become useful later. And finally, we go through the proof of the result.

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 sledečem diplomskem delu predstavljamo nekaj zanimivih primerov z avtomati generiranih grup in z njimi povezanih rezultatov.

V prvem delu spoznamo osnove. Hevristično uvedemo avtomat kot računski model, tj. stroj, ki vsakemu vhodnemu podatku (input) priredi izhodnega (output). To nas motivira k formalizaciji inputa in outputa: gre za zaporedja simbolov, ki jih naš stroj lahko prebere in prepiše, torej zaporedja elementov končne množice $\mathbf{X}$, ki ji pravimo abeceda. Opazimo, da je množico končnih zaporedij, imenovano končni slovar, mogoče razumeti kot monoid (glede operacije stikanja besed) ali kot drevo: graf, v katerem je vozlišče $\mathbf{w}$ 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 dejansko definicijo Mealyjevega končnega determinističnega avtomata $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$ in jo grafično prikažemo z Moorejevimi diagrami. Od tod izpeljemo koncept začetnega avtomata $\mathcal{A}_{q_0}$ in njegovega delovanja $\bar{\lambda}_{q_0} : \mathbf{X}^* \longrightarrow \mathbf{X}^*$.

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

Tretji del je pretežno tehnične narave, saj opisuje vrsto algebraičnih orodij potrebnih pri analizi z avtomatom generiranih grup. Pričnemo z definicijo levega in desnega delovanja grupe G na množico X in specifičnega primera, ko grupa $S(X)$ (simetrična grupa nad X) z desne deluje na X - sledimo notaciji iz [4]. 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 produkt *wreath* med grupo desnih permutacij (Y, B) in grupo A, pišemo $B \wr A$. V naslednjem razdelku koncepte apliciramo na področje avtomatov in 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 avtomata n stanj na abecedo s k simboli opišemo prek rekurzivnih zvez:

$$\begin{aligned} f_1 &= \beta_1(h_{1,x_1}, \ldots, h_{1,x_k}), \\ f_2 &= \beta_2(h_{2,x_1}, \ldots, h_{2,x_k}), \\ &\ldots \\ f_n &= \beta_n(h_{n,x_1}, \ldots, h_{n,x_k}), \end{aligned}$$

kjer je vsak h_{j,x_i} enak nekemu f_j za nek $j \in \{1, \ldots, n\}$, in je vsak β_j permutacija iz $\mathcal{S}(\mathbf{X})$.

V četrtem in zadnjem delu predstavimo rezultat iz [5], na podlagi dokazov iz [6]. Dokazani izrek v celoti klasificira grupe generirane z avtomati dveh stanj nad abecedo dveh črk. Preden izrek navedemo predstavimo grupe, ki se pojavijo v rezultatu, in se bralcu verjetno manj znane, začenjši z neskončno diedersko grupo

because the abstract must be self-contained.

$\mathbb{Z}_2 \ltimes \mathbb{Z}$, torej množice simetrij $\mathbb{Z}$. Sledi grupa svetilničarja (lamplighter group), $\mathbb{Z} \wr \mathbb{Z}_2$, in uvedba posebne transformacije $\mathcal{GA}(\mathbf{X})$, imenovane adding machine, z nekaj nič nimi posebnimi lastnostmi. Nazadnje navedemo izrek in nastavimo štetje primerov s pomočjo rekurzivnih zvez:

$$a = \sigma^{i_1}(x_{11}, x_{12})$$
$$b = \sigma^{i_2}(x_{21}, x_{22})$$

kjer sta a, b delovanji, ki ju definira avtomat, σ^{i_1} in σ^{i_2} permutaciji iz $\mathcal{S}(\{0,1\})$ ter x_{ij} elementi iz $\{a, b\}$. Analiziramo vseh 64 možnih primerov.

grupe

[7]

definicija

Zdaj lahko formuliramo klasifikacijski izrek. [Provide here the formulation of the classification theorem]. Nazadnje predstavimo del dokaza klasifikacijskega izreka, kjer si pomagamo z analizo primerov.

Ključne besede: automat, končni avtomat, besedni prostor, Moorejev diagram, semidirektni produkt, krožni produkt, rekursivnost, neskončni vzigalnik grup, neskončni diedrski grup, stroj dodajanja, grupi delujujoči drevesom

na drevesih

grupa svetilničarja

krožni

Gruppi di automi

Sintesi Estesa

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

Nella prima parte prendiamo confidenza con gli oggetti principali. Introduciamo euristicamente gli automi come modelli di computazione, ovvero macchine che per ogni input dato, ritornano un output. Questo ci motiva a formalizzare input ed output, che vengono visti come sequenze di simboli che possono essere letti e trascritti dalla nostra macchina. Quindi sequenze di elementi di un insieme finito $\mathbf{X}$ detto alfabeto. Vediamo che l'insieme delle sequenze finite, detto dizionario finito, può essere visto o come un monoide rispetto all'operazione di composizione di parole oppure come un grafo ad albero, in cui un nodo $\mathbf{w}$ è discendente di un altro $\mathbf{v} \in \mathbf{X}^*$ se e solo se $\mathbf{w} = \mathbf{v}x$, con $x \in \mathbf{X}$. Poi passiamo alla definizione vera e propria di automa deterministico finito di Mealy $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$ e ne diamo una visualizzazione grafica tramite i diagrammi di Moore. Da qui deriviamo l'idea di automa iniziale $\mathcal{A}_{q_0}$ e della sua azione $\bar{\lambda}_{q_0} : \mathbf{X}^* \longrightarrow \mathbf{X}^*$.

Nella seconda parte invece ci spostiamo su un livello più astratto, descrivendo l'operazione di composizione di automi e analizzando le proprietà dell'insieme $\mathcal{FSA}(\mathbf{X})$, ovvero l'insieme delle funzioni $f : \mathbf{X}^* \longrightarrow \mathbf{X}^*$, dette trasformazioni sincrone, che possono essere descritte da qualche automa iniziale. Qui scopriamo che quest'insieme è in biezione con l'insieme degli omomorfismi d'albero del dizionario finito $\mathbf{X}^*$. Restringiamo poi lo sguardo solo sugli automi invertibili, e quindi sulle trasformazioni sincrone biettive, che formano il gruppo $\mathcal{GA}(\mathbf{X})$, che sarà quindi isomorfo a $\mathcal{AUT}_{tree}(\mathbf{X}^*)$, ovvero l'insieme degli automorfismi d'albero su $\mathbf{X}^*$. Studiamo come influisce l'invertibilità di un automa sull'accessibilità dei suoi stati, ed infine diamo a definizione di gruppo generato da un automa.

La parte numero tre è la più tecnica, perchè descrive una serie di strumenti algebrici necessari all'analisi dei gruppi generati da automi. Partiamo dalle definizioni di azione di un gruppo G su un insieme X, sia destra che sinistra, e del caso particolare in cui sia $\mathcal{S}(X)$ (gruppo simmetrico su X) ad agire su X da destra, usando la notazione introdotta in [4]. Successivamente vediamo 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 indicarne alcuni esempi pratici come il gruppo diedrale $\mathbb{Z}_2 \ltimes \mathbb{Z}_n$. Con queste due strutture definiamo infine il prodotto *wreath* di un gruppo di permutazioni destro (Y, B) e di un gruppo A, scritto $B \wr A$. Nella sezione seguente applichiamo questi concetti al campo degli automi, scoprendo 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 a $\mathcal{GA}(\mathbf{X})$, il gruppo delle trasformazioni sincrone biettive, possiamo descrivere tutte le azioni di un automa a n stati su un alfabeto a k simboli tramite formule ricorsive del tipo

$$\begin{aligned} f_1 &= \beta_1(h_{1,x_1}, \ldots, h_{1,x_k}), \\ f_2 &= \beta_2(h_{2,x_1}, \ldots, h_{2,x_k}), \\ &\ldots \\ f_n &= \beta_n(h_{n,x_1}, \ldots, h_{n,x_k}), \end{aligned}$$

dove ogni h_{j,x_i} è uguale a qualche f_j per qualche $j \in \{1, \ldots, n\}$, ed ogni β_j è una permutazione in $\mathcal{S}(\mathbf{X})$.

Nella quarta ed ultima parte presentiamo un risultato di [7], seguendo la dimostrazione di [5]. Il teorema in questione classifica completamente i gruppi generati da automi a 2 stati su alfabeti a 2 lettere. Prima di enunciarlo presentiamo i gruppi che potrebbero essere sconosciuti al lettore e che si trovano nel risultato, partendo dal gruppo diedrale infinito $\mathbb{Z}_2 \ltimes \mathbb{Z}$, cioè l'insieme delle simmetrie di $\mathbb{Z}$. Passiamo al lamplighter group, $\mathbb{Z} \wr \mathbb{Z}_2$, ed infine introduciamo una trasformazione particolare in $\mathcal{GA}(\mathbf{X})$, detta adding machine, ed alcune sue proprietà particolari. Enunciamo poi il teorema, e impostiamo il conteggio dei casi attraverso le formule ricorsive

$$a = \sigma^{i_1}(x_{11}, x_{12}),$$
$$b = \sigma^{i_2}(x_{21}, x_{22}),$$

dove a, b sono le due azioni definite dall'automa, $\sigma^{i_1}, \sigma^{i_2}$ sono permutationi in $\mathcal{S}(\{0,1\})$, e x_{ij} sono elementi in $\{a, b\}$. Da qui analizziamo ognuno dei 64 casi possibili.

Parole chiave: automi, automi finiti, spazi di parole, diagrammi di Moore, prodotti circolari, 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 *automat**A*** 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 discover later that the elements of the groups we will introduce are exactly these functions. But at this point we realise that to arrive there we must define and understand the structure of input and output.

1. WORDS SPACES AND ALPHABET TREES

Data given and received will be somehow written and read through some kind of symbols. Mathematically this means the following:

Definition 1.1. An **alphabet 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 $\varnothing$, 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 **lenght** of $\mathbf{w}$, written as $|\mathbf{w}|$, is n. The lenght 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 $j \circ 2j = j2j$. ♢

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

Proof. The operation $\circ$ is associative with $\varnothing$ being an identity element. □

Let us define also words with an infinite lenght.

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, that is uniquely defined.

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

Let $\widetilde{\lambda} = (\lambda_n)_{n\in\mathbb{N}}$ be an arbitrary *decreasing* sequence of *positive* numbers such that $\lim\limits_{n\to\infty} \lambda_n = 0$. So we can define

$$d_{\widetilde{\lambda}}(\mathbf{w_1}, \mathbf{w_2}) = \lambda_n \tag{1}$$

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 $d_{\widetilde{\lambda}}$ 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

$$d_{\widetilde{\lambda}}(\mathbf{w_1}, \mathbf{w_2}) \leq d_{\widetilde{\lambda}}(\mathbf{w_1}, \mathbf{w_3}) + d_{\widetilde{\lambda}}(\mathbf{w_3}, \mathbf{w_2}).$$

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 $p = \mathbf{min}\{p, q\}$ (if $q = \mathbf{min}\{p, q\}$ the proof is symmetrical). If $p \leq n$, since $\widetilde{\lambda}$ 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. Let $p > n$. 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 is prefix of $x_1 \dots x_n$, so $p \leq n$, contradicting the hypothesis $p > n$. □

Every $\mathbf{wX}^\omega := \{\mathbf{wu} | \mathbf{u} \in \mathbf{X}^\omega\}$ 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 $\widetilde{\lambda} = (\frac{1}{n})_{n\in\mathbb{N}}$.*

1.2. **Tree structure of the dictionaries.** It is useful to represent $\mathbf{X}^*$ in the form of a tree graph: the verteces will be the elements of $\mathbf{X}^*$ with $\varnothing$ as the root. An example is Figure 2. We then say that $\mathbf{v}$ is a child of $\mathbf{u}$ *if and only if* $\mathbf{u} = \mathbf{v}x$ for some $x \in \mathbf{X}$.

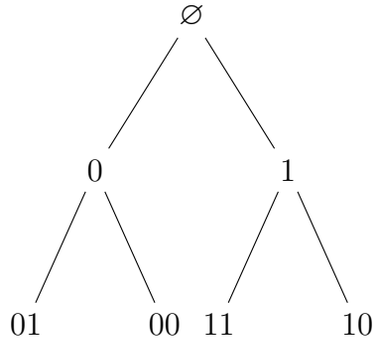


FIGURE 2. An example of the first three floors of the tree graph of $X = \{0, 1\}$.

Convention 1. *We will mostly use the alphabet $\mathbf{X} = \{0, 1\}$. The case with $|X| = n \in \mathbb{N}$ is often treated similarly.*

The set X^n is called the *the n-th floor of* 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 and $f : A \longrightarrow B$ be a function. It is called a **tree-morphism** (or a tree-homomorphism) if it preserves the root and the adjacency of the vertices, i. e.:

- If $a \in A$ is the root, $f(a)$ is the root.
- If (u, v) is an edge of A, then $(f(u), f(v))$ is an edge of B (that is, f *is a graph-homomorphism*).

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 the tree-homomorphisms form a *semigroup* under the composition of functions, and all the tree-automorphisms 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 *automaton*, but the reader should know that this is a *very specific* case. If you would like to explore a broader class of automata you can take a look at [4, 11].

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**,
- $\pi : \mathbf{X} \times \mathcal{Q} \longrightarrow \mathcal{Q}$ is a function called the **transition function**,
- $\lambda : \mathbf{X} \times \mathcal{Q} \longrightarrow \mathbf{X}$ is a function called the **output function**.

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

This technical description 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 $\exists x \in \mathbf{X} \quad s.t. \quad \pi(x, q_1) = q_2$ and the label assigned to this edge is $x|\lambda(x, q_1)$.

An example of Moore diagram is Figure 3.

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"

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.*

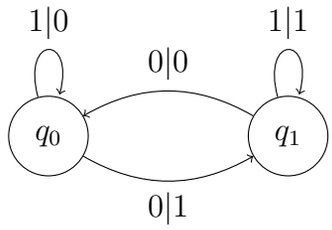


FIGURE 3. Example of the Moore diagram of a 2-state-automaton over the alphabet $\mathbf{X} = \{0, 1\}$

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 $\lambda(\mathbf{w}, q) = 1$. ♢

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

- $\bar{\pi} : \mathbf{X}^* \times \mathcal{Q} :\longrightarrow \mathcal{Q}$;
$$\bar{\pi}(\varnothing, q) = q \,,$$
$$\bar{\pi}(x\mathbf{w}, q) = \bar{\pi}(\mathbf{w}, \bar{\pi}(x, q)) \,.$$
- $\bar{\lambda} : \mathbf{X}^* \times \mathcal{Q} :\longrightarrow \mathbf{X}^*$;
$$\bar{\lambda}(\varnothing, q) = \varnothing \,,$$
$$\bar{\lambda}(x\mathbf{w}, q) = \bar{\lambda}(x, q)\bar{\lambda}(\mathbf{w}, \bar{\pi}(x, q)) \,.$$

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

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

and

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

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 $\bar{\lambda}(q, \mathbf{w}) = 110$. ♢

To effectively make an automaton a word-transducer we need to specify an initial state. In other words, 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 $q \in \mathcal{Q}$.

For example

Definition 2.6. If an automaton $\mathcal{A}$ has a fixed state q_0, we call it an **initial automaton with 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 lenght of words, i.e. $|\bar{\lambda}_{q_0}(\mathbf{w})| = |\mathbf{w}|$.*

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

Remark 5. *Given $\mathcal{A}_{q_0}$, we can define an 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 ω-equivalent if they determine the same infinite action. Two automata are equivalent if and only if they are ω-equivalent ([5]).*

Example 2.8. In Figure 4 we present two equivalent initial automata. ♢

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

Let us stress once again that an automaton doesn't define any function, till we don't fix a state q_0.

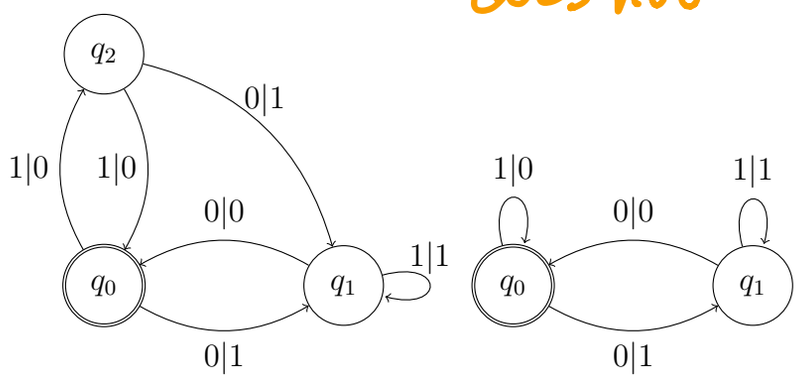


FIGURE 4. Two different initial automata which describe the same action. The double circle around q_0 tells us it is the initial state.

Part 2. ~~Automata, trees and~~ algebraic structures ~~they define~~

Here we will show how automata can define algebraic structures and how synchronous functions can be characterised.

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 π and λ 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*

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

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 the operation $*$ on the set of automata ~~returns~~ 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 $\mathbf{X}$ becomes a semigroup.

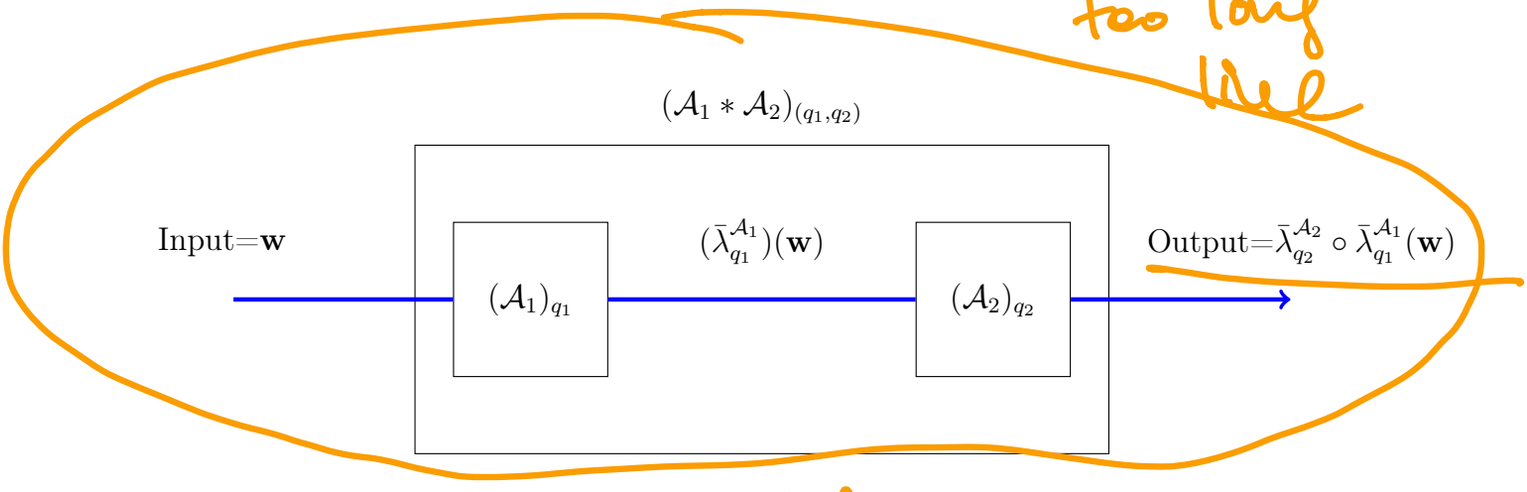


FIGURE 5. Concept of composition of automata in terms of initial automata.

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 $f : \mathbf{X}^* \longrightarrow \mathbf{X}^*$) 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 $f : \mathbf{X}^\omega \longrightarrow \mathbf{X}^\omega$) 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 $\mathcal{FSA}(X)$.*

Proof. The first point comes from the fact that the composition of *initial* automata is an *initial* automaton, therefore $\mathcal{FSA}(X)$ is closed under composition of functions. □

Now we provide an important characterization of synchronous automatic transformations:

Proposition 3.4. *A transformation $f : \mathbf{X}^* \longrightarrow \mathbf{X}^*$ 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) is a graph endomorphism. By the definition $f(\varnothing) = \bar{\lambda}_{q_0}(\varnothing) = \varnothing$, 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:

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

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

($\Leftarrow$) Let $f : \mathbf{X}^* \longrightarrow \mathbf{X}^*$ be a tree-endomorphism. We must find an initial automaton such that its action is exactly 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 need to show that the output function λ 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 need to check if $\bar{\lambda}_\varnothing$, the action of $\mathcal{A}_\varnothing$, corresponds to the function f. We verify that $\bar{\lambda}_\varnothing(\mathbf{w}) = f(\mathbf{w})$ by induction on $n = |\mathbf{w}|$.

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

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

□

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. It can be easily proved by induction on n. □

Remark 7. *The last proposition is a graph persepective on the lenght-preserving condition of actions of automata.*

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

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

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

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

Proof. The first point is a direct consequence of 8. Let us prove the second point. We have that $g|_\mathbf{v}(\varnothing) = g(\mathbf{v}) - g(\mathbf{v}) = \varnothing$, so $g|_\mathbf{v}$ preserves the root. Furthermore, if we have $x \in \mathbf{X}$, 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-morphism), 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-morphism. □

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

Proposition 3.8. *If $\bar{\lambda}_{q_0} : \mathbf{X}^* \longrightarrow \mathbf{X}^*$ 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 $g|_\mathbf{v} = \bar{\lambda}_{\bar{\pi}(\mathbf{v},q_0)}$. □

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.

~~Practically~~ 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) $\lambda_q : \mathbf{X} \longrightarrow \mathbf{X}$ 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 $\bar{\pi}_{q_0}(\mathbf{w}) = q$. ~~Let us consider $\lambda_q : \mathbf{X} \longrightarrow \mathbf{X}$.~~ We check that λ_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 λ_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 $\lambda_p : \mathbf{X} \longrightarrow \mathbf{X}$ 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 will obtain a different image with respect to $\bar{\lambda}_{q_0}$ on $\mathbf{X}^n$ and with respect to λ_{q_0} on $\mathbf{X}$ (injectivity). ~~And~~ 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 the surjectivity 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 set of all tree-automorphism of $\mathbf{X}^*$.*

Proof. Since $\mathcal{FSA}(X)$ is the semigroup of all tree endomorphisms on $\mathbf{X}^*$, $\mathcal{GA}(X)$ is the set of all bijective tree endomorphisms on $\mathbf{X}^*$, which 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 label-notation for the Moore diagrams. Given q, p vertices of a Moore diagram and $q \longrightarrow p$ an edge between them, on the label of the edge we write "x", and on the label of the vertex q we write the name of the application "$\lambda(\cdot, q) : \mathbf{X}^* \longrightarrow \mathbf{X}^*$". See Figure 6 for an example.*

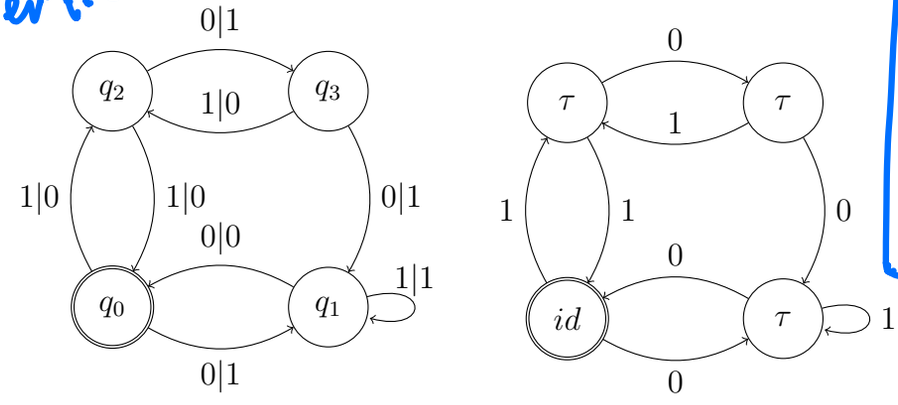


FIGURE 6. An example of the same initial automaton represented in two different ways. In the right figure $\tau, id \in \mathcal{S}_2 := \mathcal{S}(\{0,1\})$, where, τ inverts the elements in $\{0,1\}$ and id leaves them unchanged.

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 of $\mathcal{FSA}(\mathbf{X})$ generated by all the actions $\bar{\lambda}_q$ with $q \in \mathcal{Q}$:

$$\langle \{ \bar{\lambda}_q : \mathbf{X}^* \longrightarrow \mathbf{X}^* | q \in \mathcal{Q} \} \rangle,$$

where $\langle S \rangle$ for a set S 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 we speak about the **group generated by** $\mathcal{A}$, and we have that $\langle S \rangle \subseteq \mathcal{GA}(\mathbf{X})$.*

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

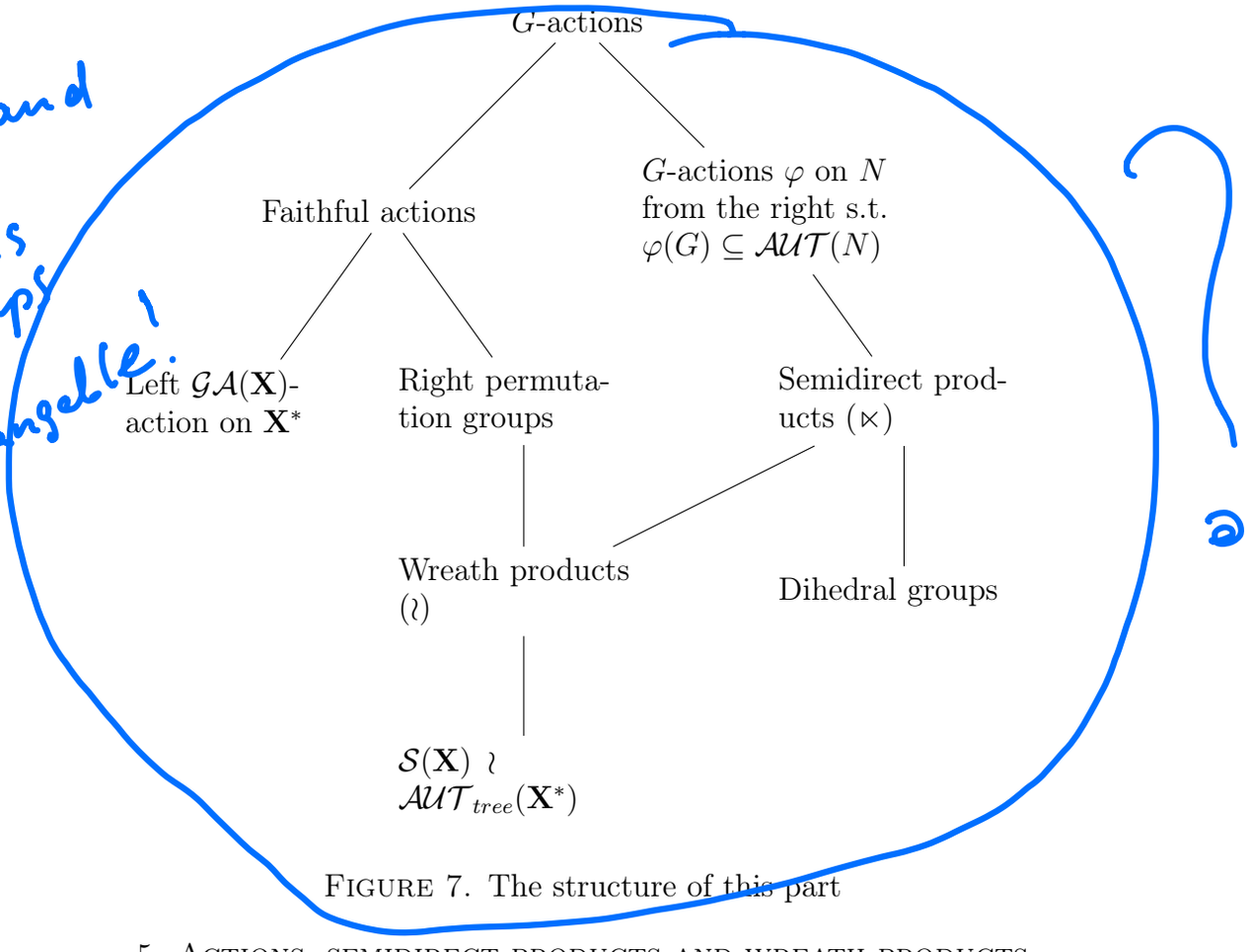


FIGURE 7. The structure of this part

5. Actions, semidirect products and wreath products

The quite complicated structures we are going to speak about arise naturally very often in algebra. This is particularly the case in environments involving some kind of recursion or selfsimilarity, as automata do.

Convention 5. *Given a set X, $\mathcal{S}(X)$ denotes the **symmetrical group on** X, that is the group of all permutations $\sigma : X \longrightarrow X$.*

Definition 5.1. Let $\circ$ be the composition of functions. We call the **product** of functions the operation "$\cdot$" defined as $f \cdot g := g \circ f$.

5.1. **Actions.** There are two equivalent definitions of an action. The purpose of the first one is to give a more abstract characterization, which is comfortable to work with. The second one helps us to visualise what we are doing as a strange "multiplication", and to write it more easily. Furthermore there are two different types of action: left and right. Right actions are needed to define the wreath product, while left actions explain us better the relation between $\mathcal{GA}(\mathbf{X})$ and $\mathbf{X}^*$.

The abstract definition is:

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

~~The more visualisable definition~~:

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* $g, h \in G$

We write $gx := \tau_l(g, x)$.

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

We write $xg := \tau_r(x, g)$.

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

(⇐) We define $(T_l(g))(x) := \tau_l(g, x)$, therefore, for the property of τ_l 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 $x \in X$

(⇒) ~~Analogous to the other direction.~~ 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 $T_l(\sigma)(x) = ~~id_{\mathcal{S}(X)}(x)~~ = \sigma x := \sigma(x) \quad \forall \sigma \in \mathcal{S}(X)$ 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 us that ~~the difference between left and right actions is quite important~~. $T_l(\sigma\eta, x) \neq T_l(x, \sigma\eta)$. ♢

Example 5.5 (translations)**.** Let A be an affine space, and let V be a vector space to it associated. 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 ~~very~~ easy to see that T is a left action. of which group?

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 see this interesting consequence:

$$T_r(\mathbf{v} +_V \mathbf{w})(P) = (\mathbf{v} +_V \mathbf{w}) + P = P + (\mathbf{v} +_V \mathbf{w}) = (P + \mathbf{v}) +_V \mathbf{w} =$$
$$= \mathbf{w} + (\mathbf{v} + P) = (\mathbf{w} +_V \mathbf{v}) + P := P + (\mathbf{w} +_V \mathbf{v}) = T_l(\mathbf{v} +_V \mathbf{w})(P)$$

This happens because V is abelian. ♢

Example 5.6 (synchronous automatic bijective transformations)**.** The group of all the 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 on X by a right-action $T_r : G \longrightarrow (\mathcal{S}(X), \cdot)$. 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**.

An analogous definition can be given to the left permutation group which we denote by (G, X).

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 an 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 an x in X such that $xg \neq xh$.

Proof. We verify the case of left-actions.

($\Leftarrow$) Let us take $T : G \longrightarrow (\mathcal{S}(X), \circ)$ defined by $T(g) = \phi_g$ where $\phi_g(x) := gx$. We can easily verify its injectivity, thus the thesis.

($\Rightarrow$) The group G is embeddable in $(\mathcal{S}(X), \circ)$ by T, thus we identify each g with ϕ_g, where $\phi_g(x) := gx$. Since ϕ is unique, we have that G acts faithfully on X.

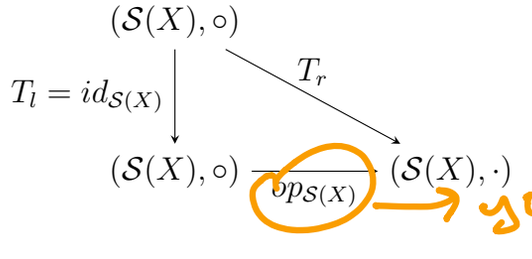
□

Proposition 5.9. *Let $(\mathcal{S}(X), \circ)$ act from the left on X by $T_l = id_{\mathcal{S}(X)}$ as in 5.4. Then the function $T_r : (\mathcal{S}(X), \circ) \longrightarrow (\mathcal{S}(X), \cdot)$ defined by $T_r(\sigma)(x) = \sigma^{-1}(x)$ 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. □

This motivates the introduction of this notation:

Convention 6. *We denote $T_r(\eta^{-1} \circ \sigma^{-1})(x) = (\eta \cdot \sigma)(x) = (\sigma \circ \eta)(x) = \sigma(\eta(x))$ 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 5.9.*



Remark 10. *The symmetric group $\mathcal{S}(Y)$ is the set of all permutations of Y, while a right permutation group (Y, B) is isomorphic to a subgroup of $(\mathcal{S}(Y), \cdot)$. If we have B group, we can take (B, B) as a right permutation group, with B acting on itself by right multiplication.*

Till now we have seen right actions $T : G \longrightarrow (\mathcal{S}(X), \cdot)$. If the set $N := X$ acted upon, is also a group we can search for right-actions such that $T(G) \subseteq \mathcal{AUT}(N)$, where $\mathcal{AUT}(N)$ is the group of group automorphisms of N. In other words, given G group, we find actions on N so that:

$$(n *_N n')\, g = ng \;*_N\; n'g$$

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

Remark 11. *Note that the group $\mathcal{AUT}(N)$ is in general a proper subset of $\mathcal{S}(N)$ (in symbols $\mathcal{AUT}(N) \subsetneq \mathcal{S}(N)$). We can consequently observe that if H acts on N from the right by $\varphi : H \longrightarrow (\mathcal{S}(N), \cdot)$, in general is not true that $\varphi(H) \subseteq \mathcal{AUT}(N)$.*

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 $\varphi : H \longrightarrow (\mathcal{S}(N), \cdot)$ and $\varphi(H) \subseteq \mathcal{AUT}(N)$. This defines the following operation on $H \times N$:

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

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

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

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

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 $H \ltimes_\varphi N$. Then:

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

□

Example 5.12 (dihedral groups)**.** Given a geometrical object A one can consider the set of all bijective geometrical transformations which have A unchanged. For their definition, the composition of two of this transformations also has A unchanged. This set is 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 possible axes of symmetry.

FIGURE 8. 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 this group is isomorphic to the semidirect product $\mathbb{Z}_2 \ltimes_\varphi \mathbb{Z}_n$, where $\varphi(0)(z) := id_{\mathbb{Z}_n}(z) = z$ and $\varphi(1)(z) := inv_{\mathbb{Z}_n}(z) := -z \,(mod\ n)$. So $\mathbb{Z}_2 \times \mathbb{Z}_n \ni (h_2, n_2) * (0, n_1) = (h_2 + 0, n_1 + n_2)$ 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 $h = 1$. Practically, if we have $(h,k) \in \mathbb{Z}_2 \times \mathbb{Z}_n$, h encodes the reflection and k the rotation. ♢

5.3. **Wreath products.** Since there is an alternative definition of the semidirect product, there is also an alternative definition of the wreath product using left permutation groups. We adopt the conventions of [10].

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

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

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

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

In case $|Y|$ 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 $\Phi : B \longrightarrow (\mathcal{S}(A^Y), \cdot)$. 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 $y\beta$ and let A be a group. Then $\Phi : B \longrightarrow (\mathcal{S}(A^Y), \cdot)$ defined as*

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

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 $A^{(Y)}$.

Proof. Let $\beta \in B$ and $\overline{a} \in A^Y$. We have the action Φ of β on $\overline{a} \in A^Y$ defined as follows:

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

(1) We must prove that Φ is a right action on A^Y as a set. This means that $\Phi(\beta)$ is bijective for every $\beta \in B$. For the injectivity we must prove that if $\overline{a} = (a_y)_{y\in Y} \neq (x_y)_{y\in Y} = \overline{x}$ there exists $y' \in Y$ such that $\Phi(\beta)(a_{y'}) \neq \Phi(\beta)(x_{y'})$. Let us look $\Phi_\beta(\overline{a})$ at the index $y'\beta$. We find that at the $y\beta'$-th component $a_{y\beta'}$ is different from $x_{y\beta'}$. So Φ_β 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 have now to prove that $\Phi(B) \subseteq \mathcal{AUT}(A^Y)$, i.e., that Φ_β is an automorphism: $\Phi_\beta(\overline{a}\star\overline{x}) = \Phi_\beta((a_y \star x_y)_{y\in Y}) = (a_{y\beta}\star x_{y\beta})_{y\in Y} = (a_{y\beta})_{y\in Y}\star(x_{y\beta})_{y\in Y} = \Phi_\beta(\overline{a})\star\Phi_\beta(\overline{x})$.

(3) We must prove that Φ is a faithful, i.e., that if $\beta \neq \theta$ then $\Phi_\beta \neq \Phi_\theta$. If $\beta \neq \theta$, there exists y' such that $\beta(y') \neq \theta(y')$. Let us take $(a_y)_{y\in Y}$ and $(x_y)_{y\in Y}$ such that $a_{y'} \neq x_{y'}$. Then $\Phi_\beta((a_y)_{y\in Y}) = (a_{y\beta})_{y\in Y}$ and $\Phi_\theta((x_y)_{y\in Y}) = (x_{y\beta})_{y\in Y}$.

If we take $A^{(Y)}$, the proof is still valid because the permutation of indices always keeps a finite number of them different from the identity. □

All this is still valid if $(B, *) = (\mathcal{S}(X), \circ)$ and the right permutation group is $(Y, B) = (X, \mathcal{S}(X))$ with the notation introduced in convention 6.

Definition 5.15. Let (Y, B) be a right permutation group and let A be a group. We have then a right action $\Phi : B \longrightarrow (\mathcal{AUT}(A^Y), \cdot)$ defined as in 5.14.

- The **unrestricted wreath product**, is the semidirect product $B \ltimes_\Phi A^Y =: B \wr A$.
- The **restricted wreath product**, is the semidirect product on $B \ltimes_\Phi A^{(Y)} =: B \wr A$.

Therefore, having $(\beta, \overline{p}), (\theta, \overline{q})$ in $B \times A^Y$ (or in $B \times A^{(Y)}$), their product in $B \wr A$ is:

$$(\beta, \overline{p}) * (\theta, \overline{q}) = (\beta, (p_y)_{y\in Y}) * (\theta, (q_y)_{y\in Y}) :=$$
$$= (\beta *_B \theta, (\Phi(\theta))(\overline{p}) * \overline{q}) = (\beta *_B \theta, (p_{y\theta} * q_y)_{y\in Y}) = (\beta\theta, (p_{y\theta}q_y)_{y\in Y}).$$

If we take a 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.

Proof. The proof follows from the previous proposition and of the semidirect product construction. □

Remark 13.

- *From the context it will be usually clear of which of the two structure we are talking about. Notice that if Y is finite there is no difference between the restricted and unrestricted wreath product.*
- *Given the right permutation group $(X, \mathcal{S}(X))$ and a group A, because of the notation introduced in 6, given elements $(\eta, (r_x)_{x\in X})$, $(\beta, (p_x)_{x\in X})$, $(\theta, (q_x)_{x\in X})$ of $\mathcal{S}(X) \wr A = \mathcal{S}(X) \ltimes_\Phi A^X$, their product is:*

$$(\eta \circ \beta \circ \theta\ ,\ (r_{x\theta\beta} * p_{x\theta} * q_x)_{x\in X}) = (\eta\beta\theta\ ,\ (r_{x\theta\beta}p_{x\theta}q_x)_{x\in X}).$$

where in the subscript $x\theta\beta$ we are acting by the right following in convention 6.

If $|Y|$ is finite, we use for the wreath product a more precise notation:

Convention 7. *Let (B, Y), A, $B \wr A = B \ltimes_\Phi A^Y$ be as previously defined, with Y **finite** with k elements. Let $Y = \{y_1, \dots, y_k\}$. Then $\overline{a} \in A^Y$ can be uniquely written as $(a_1, \dots, a_k)$. Then we write $(\beta, \overline{a}) \in B \wr A$ as $\beta(a_1, \dots, a_k)$. With this convention, given $\beta(a_1, \dots, a_k)$ and $\theta(g_1, \dots, g_k)$ in $B \wr A$, the multiplication rule becomes:*

$$\beta(a_1, \dots, a_k) * \theta(g_1, \dots, g_k) = \beta\theta((a_{1\theta}, \dots, a_{k\theta}) *_{A^Y} (g_1, \dots, g_k)) = \\ = \beta\theta(a_{1\theta}g_1, \dots, a_{k\theta}g_k)$$

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 14. *Semidirect and wreath products arise often in mathematics. Interesting examples involve groups used to understand and solve sudoku or the Rubik's cube. Otherwise Rhodes in [11] states many examples of the applications of the theory of automata.*

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 8. *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 set of tree-automorphisms on $\mathbf{X}^*$. Then there exists a $\mathcal{AUT}_{tree}(\mathbf{X}^*)$ left 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 3.5, $f(\mathbf{X}) = (\mathbf{X})$, therefore $T(f)$ is a bijection on the alphabet $\mathbf{X}$. □

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 $\circ$ as their operation. We have so an extension to a right-action as a group of $\mathcal{S}(\mathbf{X})$ on $\mathcal{AUT}_{tree}(\mathbf{X}^*)$ as $\Phi(\sigma)(f_{x_1}, \dots, f_{x_k}) = (f_{x_1\sigma}, \dots, f_{x_k\sigma})$, where $x_i\sigma$ is the element $\sigma(x_i) \in \mathbf{X}$, and f_{x_1} is the restriction of f as defined in Equation 3.6.

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 $\Phi(\sigma \in \mathcal{S}(\mathbf{X}))(f_{x_1}, \dots, f_{x_k}) = (f_{x_1\sigma}, \dots, f_{x_k\sigma})$. Let us define $\psi : (\mathcal{AUT}_{tree}(\mathbf{X}^*), \circ) \longrightarrow (\mathcal{S}(X), \circ) \wr (\mathcal{AUT}_{tree}(\mathbf{X}^*), \circ) = \mathcal{S}(\mathbf{X}) \ltimes_\Phi \mathcal{AUT}_{tree}(\mathbf{X}^*)^{\mathbf{X}}$ 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 Equation 3.6. Then ψ is an isomorphism of groups.

Proof.

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

$$\psi(f)\psi(g) = T(f)(f|_{x_1}, \dots, f|_{x_k}) \quad T(g)(g|_{x_1}, \dots, g|_{x_k}) = \\ = T(f)T(g)(f|_{(1T(g))}g|_{x_1}, \dots \; f|_{(kT(g))}g|_{x_k}) = \psi(fg)$$

- We prove that ψ is an injective. If $f \neq g$, we have that there exists $\mathbf{w} = y_1 \dots y_n \in \mathbf{X}^*$ s.t. $u_1 \dots u_n = f(\mathbf{w}) \neq g(\mathbf{w}) = v_1 \dots v_n$. If $T(f) \neq T(g)$, we have that $\psi(f) \neq \psi(g)$. Otherwise, if $T(f) = T(g)$, then $u_1 = v_1$. But $f(y_1 y_2 \dots y_n) = u_1 f|_{y_1}(y_2 \dots y_n) \neq g(y_1 y_2 \dots y_n) = v_1 g|_{y_1}(y_2 \dots y_n)$, therefore the restrictions $g|_{y_1}$ and $f|_{y_1}$ are different and ψ is one-to-one.
- We prove that ψ 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 $f(\varnothing) := \varnothing$. 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 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. *Let $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$ be an automaton such that $|\mathcal{Q}| = n$ and let $\mathbf{X} = \{x_1, \dots, x_k\}$. Then the set of all the possible actions defined by $\mathcal{A}$ can be described with n recurrent formulas*

$$\begin{aligned} f_1 &= \beta_1(h_{1,x_1}, \dots, h_{1,x_k}), \\ f_2 &= \beta_2(h_{2,x_1}, \dots, h_{2,x_k}), \\ &\dots \\ f_n &= \beta_n(h_{n,x_1}, \dots, h_{n,x_k}), \end{aligned}$$

where each h_{j,x_i} is equal to some f_j for some $j \in \{1, \dots, n\}$, and each β_j is a permutation of the alphabet.

Proof. Each initial automaton $\mathcal{A}_q$ where q state of $\mathcal{A}$ gives us a transformation in $\mathcal{GA}(\mathbf{X})$, therefore can be written down by one of the recursive formulas. □

Proposition 6.4. *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 $\mathcal{GA}(\mathbf{X}) = \mathcal{AUT}_{tree}(\mathbf{X}^*)$. The group $\mathcal{AUT}_{tree}(\mathbf{X}^*)$ acts faithfully from the left on $\mathbf{X}^*$ because it is a subgroup of $\mathcal{S}(\mathbf{X}^*)$. Thus it is easy to verify that $\mathcal{S}(\mathbf{X}) \wr \mathcal{AUT}_{tree}(\mathbf{X}^*)$ acts by the left faithfully as stated through $\psi^{-1}(\beta(a_{x_1}, \dots, a_{x_k}))\,(w_1 w_2 \dots w_n)$. □

Part 4. The classification theorem

In this part we present a recent result (2000) discovered by Grigorchuk and Zuk in [7], which describes all groups generated by 2-state-automata on a 2-letter-alphabet. We follow the demonstration as shown in [5]. In [2] can be found the complete classification of 3-state-automata over a 2-letter-alphabet.

7. Introduction

We introduce some of the objects we are going to encounter in the statement and in the proof of the theorem.

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

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

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

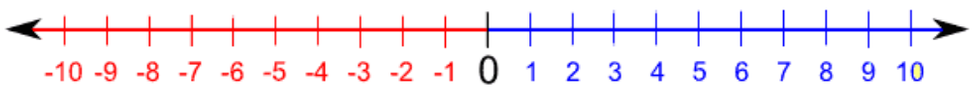


FIGURE 9. The line of integers (image taken from Math Only Math).

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

7.2. **The lamplighter group.** According to [12] the first reference to this algebraic object was anonymously made in [8] 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 amount 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 amount of them turned on (the indexes 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".

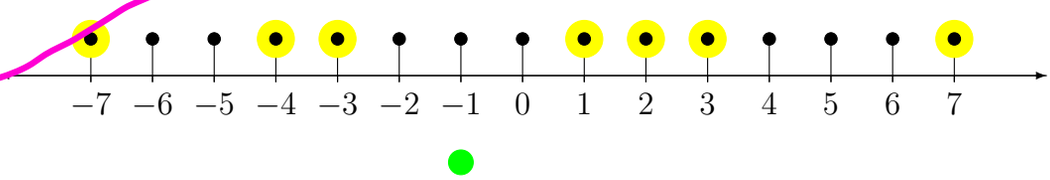


FIGURE 10. A possible representation of an **element** $(-1, (h_i)_{i\in\mathbb{Z}})$ in $\mathcal{L}$. The green circle represent the coordinate -1 of the lamplighter, while the yellow circles represent the lit on lampions at positions $\{-7, -4, -3, 1, 2, 3, 7\}$, i.e., the position i for which $h_i \neq 0_{\mathbb{Z}_2}$.

The product of two elements is:

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

And, given an element $(z, (h_i)_{i\in\mathbb{Z}})$, its inverse 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 $f = \tau(id_{\mathcal{GA}(\mathbf{X})}, f) : \mathbf{X}^* \longrightarrow \mathbf{X}^*$, where τ is a transposition of $\mathcal{S}(\mathbf{X})$.

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

$$f(0y_2 \dots y_n) = \tau(0).id_{\mathcal{GA}(\mathbf{X})}(y_2 \dots y_n) = 1y_2 \dots y_n \tag{4}$$

$$f(1y_2 \dots y_n) = id(1).\tau(y_2 \dots y_n) = 1.ab^{-1}(y_2 \dots y_n) \tag{5}$$

Let us identify each sequence $y_1 \dots y_k \dots y_n$ with the number

$$t = y_1 + y_2 2 + \dots + y_k 2^{k-1} + \dots + y_n 2^{n-1} \in \mathbb{Z}/2^n\mathbb{Z} = \mathbb{Z}_{2^n}$$

This means identifying $\mathbf{X}^n$ with $\mathbb{Z}_{2^n}$. We can so extend the action of f on $\mathbb{Z}_{2^n}$.

The equations above 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 $f(\mathbf{w_1} x_k \mathbf{w_2}) = f(\mathbf{w_1} 0 \mathbf{w_2}) = \mathbf{v_1} 1 \mathbf{w_2}$, where $\mathbf{v_1}$ is a sequence of 0s. Then:

$$\begin{aligned} f\ (t) = \\ = f\ (x_1 + x_2 2 + \dots + x_{k-1} 2^{k-2} + x_k 2^{k-1} + x_{k+1} 2^k \dots + x_n 2^{n-1}) = \\ = f\ (1 + 1 \cdot 2 + \dots + 1 \cdot 2^{k-2} + 0 \cdot 2^{k-1} + x_{k+1} 2^k \dots + x_n 2^{n-1}) = \\ = 0 + 0 \cdot 2 + \dots + 0 \cdot 2^{k-2} + 1 \cdot 2^{k-1} + x_{k+1} 2^k \dots + x_n 2^{n-1} = t + 1 \end{aligned}$$

It follows that f acts on $\mathbb{Z}_{2^n}$ by addign 1 to each number.

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 $\langle s \rangle$, the group generated by s, 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 $|G| \geqslant n$, so G is infinite. □

If we prove that f is spherically transitive we have that $\langle f \rangle$ is infinite and cyclic, so that it is isomorphic to $\mathbb{Z}$.

The transformation f acts on $\mathbf{X}^n$ in the same way as it acts on $\mathbb{Z}_{2^n}$:

$$f(t) = t + 1$$

. Consequently we have:

$$f^m(t) = t + m \quad \text{for every m} \in \mathbb{N}$$

Therefore f is spherically transitive, so $\langle f \rangle$ is infinite, cyclic, and thus it is isomorphic to $\mathbb{Z}$.

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 a 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 ~~the reader~~ 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 [5].

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

(π) ~~Graphically, from~~ each state there exit two possible arrows, and each can arrive to one of the two states. Algebraically, the function 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.

(λ) 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 $\mathbf{X} = \{0, 1\}$ ~~(we can identify $\{0, 1\} = \mathbb{Z}_2$)~~ there are only two possible permutations: the ~~inversion~~ σ, 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 λ.

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

~~Recursive definition:~~ Let $\{q, s\}$ be the states of the automaton $\mathcal{A}$. Consequently the group is generated by $a = \mathcal{A}_q$ and $b = \mathcal{A}_s$. As we have seen in 6.3, we can define $\mathcal{A}$ by the recursive formulas:

$$\begin{aligned} a &= \sigma^{i_1}(x_{11}, x_{12}), \\ b &= \sigma^{i_2}(x_{21}, x_{22}), \end{aligned} \tag{6}$$

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 $\sigma^0 := id_{\mathcal{S}(2)}$ ~~(the identity function)~~, while $\sigma^1 = \tau$ is the other element of $\mathcal{S}_2$, the ~~inversion~~ transposition.

First we define $a = \bar{a}$, and then we analyse which groups arise for each one of the 8 possible definition of b with $a = \bar{a}$. We continue till we treat every possible case of $\bar{a}$ and b.

Remark 15. *Recall that $\mathcal{GA}(\mathbf{X})$ acts **faithfully** on $\mathbf{X}^*$, therefore two elements c, d of $\mathcal{GA}(\mathbf{X})$ acts in the same way on $\mathbf{X}^*$ ($c\mathbf{w} = d\mathbf{w}$ for every $\mathbf{w}$) if and only if $c = d$.*

Convention 9. *From now on id will stand for the identity permutation of some set, usually $\mathcal{GA}(\mathbf{X})$ or $\mathcal{S}(\mathbf{X})$ and it will be clear from the context which specific set is being considered.*

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

$$a = id(x_{11}, x_{12}) = id,$$
$$b = id(x_{21}, x_{22}) = id.$$

From now on we assume that $\sigma^{i_1} := \tau$, the transposition of $\mathcal{S}_2$. The cases with $\sigma^{i_1} := id$ are symmetric.

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

$$\begin{aligned} a^2 &= \tau(\, a|_0 = a \,,\; a|_1 = a \,) * \tau(\, a|_0 = a \,,\; a|_1 = a \,) = \\ &= \tau\tau(a|_{0\tau}a|_0, a|_{1\tau}a_1) = \\ &= id(a^2, a^2) \end{aligned}$$

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 $a \longmapsto 1$ and $b \longmapsto 0$.

(1.2) If $b = \tau(a, a)$, then $b = a$, so $\langle a, b\rangle$ is again isomorphic to $\mathbb{Z}_2$.

(1.3) If $b = \tau(b, b)$, again $b = a$ and so $\langle a, b\rangle$ is 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 15, since they acts in the same way on $\mathbf{X}^*$, $ba = ab$. We can see so that $\langle a, b\rangle = \{a^2, a, b, ab\}$ is isomorphic to $(\mathbb{Z}_2 \oplus \mathbb{Z}_2, +)$ by the maps

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

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

$$ba^{-1} = ba = \tau(b|_0, b|_1)\tau(a|_0, a|_1) = id(b|_1a|_0, b|_0a|_1) = id(ba, aa) = \\ = id(ba, aa).$$

Therefore ba acts by leaving the first letter unchanged, and either acts again on the next letter, either let $a^2 = id_{\mathcal{S}(\mathcal{GA}(\mathbf{X}))} = id$ act. 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)-(1.8) Given $c = \sigma(c|_0, c|_1)$, with $\sigma \in \mathcal{S}_2$, we have that the conjugation $a^{-1}ca = aca = \tau(a, a)\sigma(c|_0, c|_1)\tau(a, a) = \sigma(ac|_1a, ac|_0a)$. Furthermore, $\langle a, b\rangle = \langle a, a^{-1}ba\rangle$ (given a and b we can generate $a^{-1}ba$, and given a and $a^{-1}ba$ we can generate b). Consequently, the case (7) $\langle a, b = \tau(b, a)\rangle$ is analogous

to the case (5) $\langle a, a^{-1}ba\rangle = \langle a, d = \tau(a,d)\rangle$, while the case (7) $\langle a, b = id(b,a)\rangle$ is analogous to the case $\langle a, a^{-1}ba\rangle = \langle a, d = id(a,d)\rangle$.

9.4. **The cases a=t(b,a).** Let $a = \tau(a|_0 = b, a|_1 = a) = \tau(b,a)$. The cases in which $a = \tau(a|_0 = a, a|_1 = b)$ are symmetrical to this one.

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

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

$$c = id(c,d)d = id(d,c)$$

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 by 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. We omit the proof that its cardinality is infinite. Then G, being infinite and cyclic, 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 to $ba = ab$, which tells us that $\langle a, b\rangle$ is abelian. Furthermore,

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

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 demonstration.

(2.8) Given $b = id(a,b)$ 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:

$$(b^{-1})^d = d^{-1}b^{-1}d = \tau(d^{-1},d^{-1})\, id(a^{-1},b^{-1})\, \tau(d,d) = id((b^{-1})^d,(a^{-1})^d)$$
$$(a^{-1})^d = d^{-1}a^{-1}d = \tau(d^{-1},d^{-1})\, \tau(a^{-1},b^{-1})\, \tau(d,d) = \tau((b^{-1})^d,(a^{-1})^d)$$

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 $x_1x_2\dots x_k$ with $x_i \in \{a', b'\}$. We observe that its conjugate by d, $(x_1x_2\dots x_k)^d$, 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:

$$a'' = \tau(b'', a'')$$
$$b'' = id(b'', a'')$$

That is the symmetrical of the case (2.7).

9.5. **The cases a=t(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) This cases lead to the infinite dihedral group. The proof is omitted.

(3.8) If $b = id(a,a)$, then:

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

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 $x_1x_2\dots x_k$ with $x_i \in \{a,b\}$ as a^nb^m where $n+m = k$. In addition we know that $a^n = a^{n \,(mod\, 2)}$ and $b^m = b^{m \,(mod\, 2)}$, so each possible composition of a and b is an element a^ib^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:

$$id \longmapsto (0,0)$$
$$a \longmapsto (1,0)$$
$$b \longmapsto (0,1)$$
$$ba \longmapsto (1,1)$$

□

Concluding remarks

For the curious reader

In this thesis we just scratched the surface of an incredibly enormous field that is the theory of automata. We spoke just about finite deterministic Mealy automata, if instead you want to see a more broad class of objects you should read [4]. If you want to see some more practical application of the theory there is the book [11]. If you feel eager to explore in the details the structures of subsection 5.3 the book [9] is what you are searching for.

In case you have been fascinated as me by the lampighter group I can recommend [1] for an approach which requires just the knowledge of an undergraduate, and [12] for an analysis in the case we take a finite version of this object.

If you would like to see more examples of automata in connection to groups the book [10] is a very good source, and the article [13] 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 [6].

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 to this exchange program. Without them this wouldn't have even started. Finally I need to thank prof. Sašo Strle, which managed to follow me and other tens of students in the completion of the bachelor thesis.

References

[1] Bonanome M.C., Dean M.H., Dean J.P. (2018) The 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

[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] D'Amore B., Sbaragli S., *La matematica e la sua storia. Vol. 1: Dalle origini al miracolo greco.*, Dedalo, La scienza nuova, 2017, 356 p., ill., Brossura, EAN: 9788822002716

[4] 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://www.sciencedirect.com/science/article/pii/S0079816908608727)

[5] 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

[6] 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, ISSN 0304-3975, https://doi.org/10.1016/S0304-3975(98)00161-3. (https://www.sciencedirect.com/science/article/pii/S0304397598001613)

[7] 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

[8] Kaimanovich, V. A.; Vershik, A. M., *Random Walks on Discrete groups: Boundary and Entropy*. Ann. Probab. 11 (1983), no. 3, 457–490. doi:10.1214/aop/1176993497. https://projecteuclid.org/euclid.aop/1176993497

[9] Meldrum J. D. P. (1995), *Wreath products of groups and Semigroups*, Longman [UK] / Wiley [US], p. ix. ISBN 978-0-582-02693-3

[10] Nekrashevych V. V., *Self-similar groups*, volume 117 of Mathematical Surveys and Monographs. Amer. Math. Soc., Providence, RI, 2005.

[11] Rhodes, John and Nehaniv, Chrystopher L and Hirsch, Morris W, *Applications of automata Theory and Algebra*, World Scientific Publishing Co. Pte. Ltd. , 2009, https://www.worldscientific.com/doi/abs/10.1142/7107 (https://www.worldscientific.com/doi/pdf/10.1142/7107)

[12] 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

[13] Zuk A., *Automata groups* - Topics in noncommutative geometry, 165–196, Clay Math. Proc., 16, Amer. Math. Soc., Providence, RI, 2012