

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

Programma di doppio titolo
in Matematica

Double Degree Program in Mathematics

UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Program dvojne diplome
iz matematike

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

Part 1. Introduction	7
1. Words Spaces and Alphabet Trees	7
1.1. Topology on the Infinite Dictionaries	8
1.2. Tree Structure of the Dictionaries	8
2. Automata and Initial Automata	9
Part 2. Automata, Trees and Algebra	11
3. Synchronous Automatic functions	11
4. Groups generated by an Automaton	13
Part 3. Some advanced Group Theory	14
5. Actions, Semidirect Product and Wreath Product	14
5.1. Step 0: Actions and Embeddings in Permutation Groups	15
5.2. Step 1: Faithful Actions and Permutation Groups	15
5.3. Step 2: Semidirect Product	16
5.4. Step 3: Restricted and Unrestricted Wreath Product	16
6. Free Groups	17
Part 4. Classification of every 2-state Automaton over a 2-letter alphabet	18
7. Overtoure	18
7.1. Case of Z 2	18
7.2. Klein Group	18
7.3. case 3	18
7.4. case 4	18
7.5. Infinite Dihedral Group	18
7.6. Lamplighter Group	18
References	18

Groups of Automata

present ABSTRACT

In this Bachelor Thesis we ~~review~~ some interesting examples and results of groups generated by Automata. First we treat the mathematical idea of input and output and we give the definition of Finite Synchronous Deterministic Mealy Automaton. We exploit it to generate groups and we link all these concepts with some abstract structures, as the tree homomorphism~~x~~ or the wreath product. Finally we treat some interesting examples, that is the Infinite Dihedral Group and the Lamplighter Group. Finally, we present the classification of all groups generated by 2-state automata over a 2-letter alphabet.

such as ~~on~~ ~~we~~ ~~include~~

Math. Subj. Class. (2010): 20E07, 20E22, 20E08, 68Q70, 68Q45, 20E07, 20M35

Keywords: Automata, Finite Automata, Word Spaces, Moore Diagram, Wreath Product~~x~~

Automatne Grupe
RAZŠIRJENI POVZETEK

Kasual

Ključne besede: Kasual **ADD¹**,

Gruppi di Automi

SINTESI ESTESA

Kasual

Parole chiave: Kasual

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, taking an input, spews out an output(1).

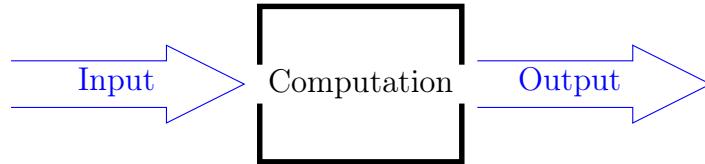


FIGURE 1. Model of Computation

So to first understand the topic 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:

Definition 1. An Alphabet X is a finite set of elements called **letters**.

Definition 2. $X^* := \{x_1 \dots x_n \mid n \in \mathbb{N}, x_i \in X\}$ is called the **Set of Finite Words** or **Finite Dictionary**, and its elements are called **words**. The element with no letter, written as \emptyset , is called the *empty word*.

Definition 3. Given words $w = x_1 \dots x_n$ and $u = y_1 \dots y_m$. The lenght of w , written as $|w|$, is n . The lenght of the empty word is 0. The **concatenation** of w and u , written as $w \circ u = wu$, is the word $x_1 \dots x_n y_1 \dots y_m$.

Example 1. Let $X = \{0, 1\}$. $0100 \circ 111 = 0100111$. Let X be $\{0, 1, 2\}$. $02 \circ 20 = 0220$. $|2| = 2$.

Proposition 1. (X^*, \circ) is a monoid, called the **Free Monoid on X** .

Proof. \circ is associative with \emptyset as identity element. □

A question might now come to the mind of the reader: can a word with an infinite lenght exist?

Definition 4. The Set of Infinite Words or Infinite Dictionary is $X^\omega := \{x_1 \dots x_i \dots \mid x_i \in X\} = X^{\mathbb{N}}$.

Remark The concatenation can be extend. In fact taken $u = x_1 \dots x_n \in X^*$ and $v = y_1 \dots y_i \dots \in X^\omega$, $u \circ v := x_1 \dots x_n y_1 \dots y_i \dots \in X^\omega$.

Definition 5. $w = x_1 \dots x_n$ is the **beginning** or **prefix** of a word $u \in X^*$ (or $u \in X^\omega$) if $u = wv = x_1 \dots x_n v$ for some $v \in X^*$ (or $v \in X^\omega$). In this case we set $v = u - w$.

Given $A \in X^* \cup X^\omega$, we denote $P(A)$ the **longest common prefix** of A , that is uniquely defined.

A word $v \in X^\omega$ is called **almost periodic** if $v = uwuw\dots$ for some $u \in X^*$.
General comment: avoid starting a sentence from formula,
 Start it from a word!

if you write "notice", provide a proof.

a metric?

1.1. Topology on the Infinite Dictionaries. We can provide this space X^ω with a distance, and consequently a topology, in order then to exploit the properties of some continuous functions for our egoist means.

For every decreasing sequence of positive numbers $\lambda = (\lambda_n)_{n \in \mathbb{N}}$ such that $\lim_{n \rightarrow \infty} \lambda_n = 0$ we can find a metric d_λ on X^ω such that

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

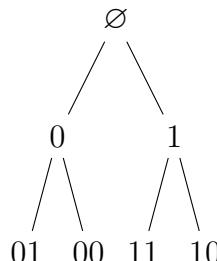
defined on X^ω , where $n = |\mathcal{P}(\{\mathbf{w}_1, \mathbf{w}_2\})|$ is the longest common prefix of the words \mathbf{w}_1 and \mathbf{w}_2 . This tells us that every set $\mathbf{w}X^\omega := \{\mathbf{w}\mathbf{u} \mid \mathbf{u} \in X^\omega\}$ can be seen as a ball of radius $\lambda_{|\mathbf{w}|}$ with the center on an arbitrary point $\mathbf{u} \in \mathbf{w}X^\omega$. In particular notice that $\mathbf{w}X^\omega$ is clopen (open and closed).

Observation 2. It will be often useful to set $\tilde{\lambda} = (\frac{1}{n})_{n \in \mathbb{N}}$.

1.2. Tree Structure of the Dictionaries. It's sometimes very useful to imagine X^* in the form of a tree graph: the vertexes will be the elements of X^* with \emptyset as the root. We then say that v is son of u if and only if $u = vx$ for some $x \in X$. An example is 3.

a child

?



↙ is the length
of the longest
common prefix

of a tree graph

FIGURE 2. An example in the case $X = \{0, 1\}$

Norm 1. From now on we will always use the alphabet $X = \{0, 1\}$; this will also help the reader to better visualise the concept. The case where $|X| = n \geq 2$ is similar.

The set X^n , the set of the words of length n , is called the the n -th floor of X^* (see Fig. 1).

Notice that X^ω is the very bottom of the graph of 3, therefore that's also called the Boundary tree of the tree.

Finally we define the notion of endomorphisms on a tree, and some of their properties.

Definition 6. Given A, B trees, $f : A \rightarrow B$ is a tree-homomorphism if preserves the root and the adjacency of the tree, i. e.:

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

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

It is
easy
to verify

It's easy verifiable that all the tree-homomorphisms of a tree are a semigroup under the composition of functions, and the tree-automorphisms are a subsemigroup that is also a group.

all write

form a
group

form its

Norm 2. Very often we will simply say "-morphism" instead of "tree -morphism". The meaning will be clear by the context.

from

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.

Definition 7. An **Automaton** is a set $\mathcal{A} = \langle X, Q, \pi, \lambda \rangle$ where:

- X is an alphabet, usually referred as the **Input and/or Output Alphabet**,
- Q is a set called the **Set of Internal States of the Automaton**,
- $\pi : X \times Q \rightarrow Q$ is a function called the **Transition Function**,
- $\lambda : X \times Q \rightarrow X$ is a function called the **Output Function**.

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

This technical description explains us how an automaton performs the action of transforming an input in 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 $p = \pi(x, q) \in Q$ and *spits out* an *output letter* $y = \lambda(x, q) \in X$. Don't worry, there is also a way to visualise it. *returns this. its*

Definition 8. Given an Automaton $\mathcal{A} = \langle X, Q, \pi, \lambda \rangle$ we define his **Moore Diagram** as the oriented graph $G = (Q, E)$ where 2 states (q_1, q_2) are connected whenever $\exists x \in X \ s.t. \ \pi(x, q_1) = q_2$ and the label referred to each edge is $x|\lambda(x, q_1)$ (=input|output). *q₁ and q₂*

I thank Edward F. Moore, for he gave us an easy-manageable representation of these objects. We can see here an example: *BETTER: Here is an example:*

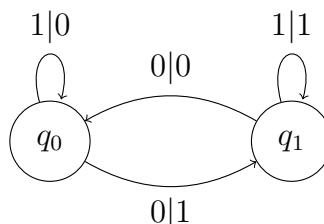


FIGURE 3. Example of a Moore Diagram of a 2-state-Automaton over the alphabet $X = \{0, 1\}$

We observe that for every automaton his Moore Diagram has *this characteristic*:

- (2) $\forall q \in Q$ and $\forall x \in X_I \ \exists! e \in E$ such that the left side of its label reads "x"

That is, for every vertex in the graph and for every letter of the input alphabet, exists an arrow (from that vertex) through which we travel with that input. We can see many examples in 3)?

Observation 3. These Diagram are so important not just for the visual insight, but also because whenever a graph respects the condition (2), it *uniquely* defines an automaton. So given $\mathcal{M} := \{G \mid G \text{ is a Moore Diagram}\}$, there is a unique correspondence between \mathcal{M} and the set of all Automaton. This means that instead of defining this types of machine through some tedious list of outputs for each possible input $x \in X$ and $q \in Q$, we can simply draw them. Then to compute the outcome of (x, q) , we just follow the arrow to $\pi(x, q)$ and *watch* the left side $\lambda(x, q)$ of the label.

look at

in figures?

Example 2. In 2, given input $w = 0$ and state $q = q_0$, then $\pi(w, q) = q_1$ and $\lambda(w, q) = 1$. Or if $w = 1$ and $q = q_1$, $\pi(w, q) = q_1$ and $\lambda(w, q) = 1$.

Proposition 2. We can naturally extend the Domain of π and λ from single letters in X to words in X^* : recursively

- $\bar{\pi} : X^* \times Q \rightarrow Q$

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

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

- $\bar{\lambda} : X^* \times Q \rightarrow X^*$

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

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

Remark

Observation 4. The two definitions are equivalent to:

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

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

give exact reference

Example 3. We can compute $\bar{\pi}$ and $\bar{\lambda}$ following the arrows as before, and then making the composition of the single right side of the labels. In 2, given input $w = 0000$ and state $q = q_0$, then $\bar{\pi}(q, w) = q_0$ and $\bar{\lambda}(q, w) = 1010$. Or if $w = 110$ and $q = q_1$, $\bar{\pi}(q, w) = q_0$ and $\bar{\lambda}(q, w) = 110$.

Figures

To make an automaton a word transducer we need to specify an initial state.

Now we start to point out a problem. For each Automaton we don't have really an output till we don't decide where we start from. In other words in ??, together with the input, we need to give a state (and different states, with the same input might get us different output). So what happens if we fix $q \in Q$, and we imagine to start always there? Rework this, e.g.

Definition 9. 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 $\bar{\lambda}_{q_0} : X^* \rightarrow X^*$, with $\bar{\lambda}_{q_0}(w) := \bar{\lambda}(w, q_0)$, called **Action of the Automaton** \mathcal{A}_{q_0} . Two Initial Automata are said to be *equivalent* if they define the same actions.

Proposition 3. The Action $\bar{\lambda}_{q_0}$ of an Initial Automaton preserves the length of words, i.e. $|\bar{\lambda}_{q_0}(w)| = |w|$.

Proof. For induction on $n = |w|$. The statement easily proved by induction by \square on $n = |w|$

Observation 5. Given \mathcal{A}_{q_0} , we can define an **Infinite Action** $\bar{\lambda}_{q_0} : X^\omega \rightarrow X^\omega$ from the same 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 iff are ω -equivalent. This comes naturally from the fact that the defining formula is the same.

similar

Example 4. In 2 there are two equivalent Initial Automata.

Norm 3. An Initial Automaton is usually drawn *evidentiating* the Initial State with a double circle around its vertex(2).

depicting

If an Automaton is a skeleton, an Initial Automaton is an alive working machine, is our model of computation, that for each input gets an output travelling through the states. I underline this concept: an Automaton doesn't define any function, till we don't fix a state q_0 . Take care of distinguish the two in every definition, porposition and example that we will give.

it is important to bear this in mind in all definitions, ...

Part 2. Automata, Trees and Algebra

Here we will show how Automata can build algebraic structures and how synchronous functions can be characterised.

Definition 2.1. Given $\mathcal{A}_1 = \langle X, Q_1, \pi_1, \lambda_1 \rangle$ and $\mathcal{A}_2 = \langle X, Q_2, \pi_2, \lambda_2 \rangle$ we define their composition $\mathcal{B} := \mathcal{A}_1 * \mathcal{A}_2 = \langle X, Q_1 \times Q_2, \pi, \lambda \rangle$ with π and λ as follows:

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

with $x \in X$ and $(s_1, s_2) \in Q_1 \times Q_2$.

one next to the other. this means that

This is something similar to put two machine in serie. Informally means we feed the second machine with the output of the first one(2), so we use the both of them as a single bigger and more complicated transducer. Notice that the two Automata are not Initial Automata.

into

Observation 6. With this operation the set of all Automata on an alphabet X becomes a semigroup.

the operation of composition

? Reformulate this!

Remark

Observation 7. $(\text{Action of } (\mathcal{A}_2)_{q_2}) \circ (\text{Action of } (\mathcal{A}_1)_{q_1}) = \text{Action of } (\mathcal{A}_1 * \mathcal{A}_2)_{(q_1, q_2)} = \text{Action of } (\mathcal{B})_{(q_1, q_2)}$ for all $q_1 \in Q_1$ and for all $q_2 \in Q_2$. This means the operation on the set of Automata extends to an operation on the set of Initial Automata! However there are certain characteristic for which this operation is not yet very maneuverable, for example the fact that there can be many different Automata which, for every pair of states (q_1, q_2) describe the same Action.

? Reformulate this!

? Reformulate this!

In this section

3. SYNCHRONOUS AUTOMATIC FUNCTIONS

Here, given an Action of an Initial Automaton, we describe and study its properties.

Definition 10. A transformation on X^* (i.e. a function $f : X^* \rightarrow X^*$) is called **Finite Synchronous Automatic** if it is the (finite) action of some Initial Automaton \mathcal{A}_{q_0} , i.e. if $f = \bar{\lambda}_{q_0}$.

of

Definition 11. A transformation on X^ω (i.e. a function $f : X^\omega \rightarrow X^\omega$) is called **Infinite Synchronous Automatic** if it is the infinite action of some Initial Automaton.

Proposition 3.1. The Finite Synchronous Automatic transformations form a semigroup $\mathcal{SF}(X)$ (S stands for "Synchronous" and F for "Finite"). The Infinite Synchronous Automatic transformations form a semigroup isomorphic to $\mathcal{SF}(X)$.

Proof. The first point comes from the fact that the Composition of Initial Automata is an Initial Automaton, therefore $\mathcal{SF}(X)$ is closed under composition of functions.

The second point arise from 5. ?

□

Observation 8. If we are interested to describe the set of all possible actions, it is the same to study $\mathcal{SF}(X)$ or its isomorphic copy. Thus we will just generally speak about **Synchronous Automatic** Transformations and we will usually refer to the finite case. Different usage will be clear from the context.

we provide
Now let's see an important characterization of synchronous automatic transformations.
Proposition 4. f is Synchronous Automatic iff f is a tree-homomorphism on $X^*(\mathbb{N})$.

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

Since
 (\Leftarrow) f is synchronous automatic, therefore 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. For the definition $f(\emptyset) = \bar{\lambda}_{q_0}(\emptyset) = \emptyset$, thus (1) holds. Now (2): if v is son of w (i.e. $v = wx$ for some $x \in X$) is it true that $f(v)$ is son of $f(w)$ (i.e. $f(v) = f(w)y$ for some $y \in X$)?

we prove

$$(3) \quad f(v) = f(wx) = \bar{\lambda}_{q_0}(wx) = \bar{\lambda}(wx, q_0) = \\ = \bar{\lambda}(w, q_0)\bar{\lambda}(x, \bar{\pi}(q_0, w)) = f(w)\bar{\lambda}(x, \bar{\pi}(q_0, w))$$

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

(\Rightarrow) Let $f : X^* \rightarrow X^*$ be a tree-endomorphism. We must find an Initial Automaton such that its action is exactly f . We define $\mathcal{A} = \langle X, \mathcal{Q}, \pi, \lambda \rangle := \langle X, X^*, \pi, \lambda \rangle (\mathcal{Q} = X^* \text{ is infinite})$ with $\pi(q \in X^*, x \in X^*) := qx$ and $\lambda(q \in X^*, x \in X^*) := f(qx) - f(q)$.

First: is the output function λ well defined, i.e. is the subtraction $f(qx) - f(q)$ well defined? Yes, because f is a tree-endomorphism, so $f(qx)$ is son of $f(q)$. Second: is $\bar{\lambda}_\emptyset$, the action of \mathcal{A}_\emptyset , our function? For induction on $n = |w|$, with $w \in X^*$.

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

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

tree-endomorphism?

□

Proposition 5. If f is an endomorphism on X^* , then $f(X^n) \subset X^n$.

Proof. By induction on n .

This can be easily proved by induction on n.

Remark

Observation 9. The last proposition is a graph perspective on the length-preserving condition.

and vex

Definition 12. Given a tree-endomorphism $g : X^* \rightarrow X^*$, we can define its restriction in v as the function $g|_v : X^* \rightarrow X^*$ defined by the equality:

$$g(vw) = g(v)g|_v(w)$$

I think $f(x^n) = x^n$?

what does this mean?

Observation 10. Since g is a tree-endomorphism, and since $vX^* \cong g(v)X^* \cong X^*$, we have that $g : vX^* \rightarrow g(v)X^*$ is identifiable as $g|_v : X^* \rightarrow X^*$, and the latter one is consequently a tree-endomorphism.

In the language of Automata what does this becomes? \leftarrow reformulate this!

E.g. We now give a description of the restriction $g|_v$ in terms of automata.

Proposition 6. If $\bar{\lambda}_{q_0} : X^* \rightarrow X^*$ is the action of \mathcal{A}_{q_0} , then, for every $v \in X^*$, the action of $\mathcal{A}_{\bar{\pi}(v, q_0)}$ is given by $(\bar{\lambda}_{q_0})|_v = \bar{\lambda}_{\bar{\pi}(v, q_0)}$, so the restriction of $\bar{\lambda}_{q_0}$ in v . \leftarrow verb

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

4. GROUPS GENERATED BY AN AUTOMATON

BETTER: automata

Our groups will live inside $\mathcal{SF}(X)$, so we will need to have invertible elements, i.e. invertible transformations f in $\mathcal{SF}(X)$. This means requiring a special condition on all the possible Initial Automata \mathcal{A}_{q_0} describing f , i.e. $\bar{\lambda}_{q_0}$ is invertible. To formalise and approach this concept there will be a bit of technical work. \leftarrow there

Definition 13. Given an Initial Automaton \mathcal{A}_{q_0} , a state q is *accessible* if exists a word $w \in X$ such that $\bar{\pi}(w, q_0) = q$. We can also say that q is accessible respect to q_0 . \leftarrow (OR: from q_0) \leftarrow with

Practically this means that in the Moore Diagram there's a path from q_0 to q for each vertex $q \in Q$.

Definition 14. An Initial Automaton \mathcal{A}_{q_0} is called *accessible* if each $q \in Q$ is accessible respect to q_0 . An Automaton is called *accessible* if each Initial Automaton by it definable is accessible.

Proposition 7. Given an Automaton $\mathcal{A} = \langle X, Q, \pi, \lambda \rangle$ and a state $q_0 \in Q$, $\bar{\lambda}_{q_0}$ is an invertible function if and only if for every accessible state $q \in Q$ (respect to q_0) $\lambda_q : X \rightarrow X$ is invertible.

Proof. \Rightarrow $\bar{\lambda}_{q_0}$ is an invertible function. Let's take an accessible $q \in Q$ and the word w such that $\bar{\pi}_{q_0}(w) = q$. Let's observe $\lambda_q : X \rightarrow X$. Is it injective? Given $x \neq y$, is it true that $\lambda_q(x) \neq \lambda_q(y)$? Supposing absurdly that $\lambda_q(x) = \lambda_q(y)$, we would have that

$$\bar{\lambda}_{q_0}(wx) = \bar{\lambda}_{q_0}(w) \underbrace{\bar{\lambda}_{\bar{\pi}(w, q_0)}(x)}_{\text{with state}} = \bar{\lambda}_{q_0}(w) \underbrace{\lambda_q(x)}_{\text{with state}} = \bar{\lambda}_{q_0}(w) \lambda_q(y) = \bar{\lambda}_{q_0}(wy)$$

Consequently we would loose the injectivity of $\bar{\lambda}_{q_0}$, against the hypothesis of its invertibility. Analogously we can see that λ_q is surjective: let's take the word $w \in X^*$ such that $\bar{\pi}(w, q_0) = q$ and $y \in X$. We search a $x \in X$ such that $\lambda_q(x) = y$. Since $\bar{\lambda}_{q_0}$ is invertible and synchronous automatic exists a unique preimage of the word $\bar{\lambda}_{q_0}(w)y$, and it's of the form wx for some x .

Therefore: $\lambda_{q_0}(w)y = \lambda_{q_0}(wx) = \bar{\lambda}_{q_0}(w)\lambda_q(x)$. \rightarrow it is

\Leftarrow $\bar{\pi}_{q_0}(w) = \bar{\pi}_{q_0}(x_1 \dots x_n)$ lands necessarily on an accessible state q for each $w \in X^*$. We know that $\lambda_p : X \rightarrow X$ is invertible (i.e. is a permutation of X) for each p accessible, included all the states on the path to q .

Now for induction on n we will prove that $\bar{\lambda}_{q_0}$ is invertible on X^n , thus it will be invertible on $\bigcup_{n \in \mathbb{N}} X^n = X^*$.

the word $\bar{\lambda}_{q_0}(w)$ has a unique preimage by induction on n
Consequently

please try to write more formally!

The groups we will consider are subgroups of $S(X)$.

we check that it is injective.

Start a sentence from a word.

we have

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

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

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

So the surjectivity is proven. □

Definition 15. An *Initial Automaton* \mathcal{A}_{q_0} is **invertible** if its action is invertible. An Automaton \mathcal{A} is **Invertible** if \mathcal{A}_{q_0} is invertible for each $q \in Q$.

Norm 4. Henceforth with Automaton and Initial Automaton we mean Accessible Invertible Automaton and Accessible Invertible Initial Automaton, respectively

Norm 5. We observe that now λ is a permutation of X . Exploiting this we will sometime use a different label-notation for the Moore Diagram. Given an edge $q \rightarrow p$, on its label there will be written not $x|\lambda(x, q)$ but x , and on the vertex q not q but $\lambda(\cdot, q)$.

This is not clear!

Example 5. ADD!

Suppose that $\lambda : X \rightarrow X$ is invertible. Then it is a permutation on X .

Observation 11. Since now our Automata are always invertible their actions, in term of functions on trees are **automorphisms**, so bijective endomorphisms. This means that they permute the children of each node, and the respective lower trees.

Now we can finally introduce the wannabe-protagonist of the topic.

Definition 16. Given an Automaton $\mathcal{A} = \langle \mathbf{X}, Q, \pi, \lambda \rangle$ we can define $|Q|$ Initial Automata, which define $|Q|$ actions $\bar{\lambda}_q$ on \mathbf{X}^* inside $\mathcal{SF}(X)$. We call the **Group Generated by \mathcal{A}** the subgroup $\mathcal{GA}(\mathbf{X})$ of $\mathcal{SF}(X)$ generated by all the actions $\bar{\lambda}_q$ with $q \in Q$, or in symbols:

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

Part 3. Some advanced Group Theory

We need some advanced notions of Group Theory to understand and represent (in mathematics to understand and to represent are very often the same concept, and we could open a very interesting philosophical and historical debate on this declaration) some examples we are going to see. to consider.

5. ACTIONS, SEMIDIRECT PRODUCTS AND WREATH PRODUCTS

These quite complicated structures, regardless of the skepticism of the reader, arise very often naturally in Algebra. Particularly in environments involving some kind of recursion or selfsimilarity, as Automata do. The order of construction will be:

This is particularly the case

What is norm?
(never encountered this!) BETTER: definition, or
NOTATION.
?

FIGURE 4. A pattern

Norm 6. Given a set X , $\mathcal{S}(X)$ denotes the **Symmetrical Group of X** , so the group of all permutations $\sigma : X \rightarrow X$.

5.1. Step 0: Actions and Embeddings in Permutation Groups.

Definition 17. Let us take a group G and a set X . Then a function $\tau : G \times X \rightarrow X$ is called an **Action of G on X** if:

- $\tau(1, x) = x$ for every $x \in X$
 - $\tau(g, \tau(h, x)) = \tau(g *_G h, x)$ for every $x \in X$ and $g, h \in G$

In this case we write $qx := \tau(q, x)$.

$$\begin{aligned} \widetilde{\iota}(gh, x) &= \\ &= \widetilde{\iota}(g, \widetilde{\iota}(h, x)) \end{aligned}$$

Example 6. $\mathcal{S}(X)$ acts on X , in fact $\sigma x := \sigma(x)$ $\forall \sigma \in \mathcal{S}(X)$ and $\forall x \in X$

To practically work with actions is much more comfortable to use a more abstract characterization:

Proposition 8. Given a group G and a set X , $\tau : G \times X \rightarrow X$ is an action iff $T(g)G \rightarrow S(X)$ defined by $(T(g))(x) := \tau(g, x) =: \phi_g(x)$ is a homomorphism of groups. **START THIS FROM A WORD!**

Proof. (\Rightarrow): $T(g)(x) := \tau(g, x)$, therefore, for the property of τ we have $T(g * h)(x) = \tau(g * h, x) = \tau(g, \tau(h, x)) = T(g)(\tau(h, x)) = T(g) \circ T(h)(x)$ for every $x \in X$

(\Leftarrow): Analogous to the other sense.

5.2. Step 1: Faithful Actions and Permutation Groups.

Definition 18. A **Permutation Group** is a pair (B, Y) such that B is a group that can be embedded in $S(Y)$, the Symmetric Group of Y .

Observation 12. Take care: The Symmetric Group is the set of **ALL** permutations, while a Permutation Group is, mangling the definition, a subgroup of the Symmetric Group.

Definition 19. A **Faithful Action** of G on X is an action $f : G \times X \rightarrow X$ such that, given $g \neq h$ in G , exists $x \in X$ for which $gx \neq hx$. We then say that G acts faithfully on X .

Proposition 9 G acts faithfully on X iff (G, X) is a permutation group.

Proof. (\Rightarrow): Let's take $\Phi : G \longrightarrow S(X)$ defined by $\Phi(g) = \phi_g$ where $\phi_g(x) := gx$. We can easily verify its injectivity, thus the thesis. (\Leftarrow): G is embeddable in $S(X)$, thus we identify each g with its unique copy ϕ , where $\phi_g(x) := gx$. Since the copy is unique, we have that G acts faithfully on X . \square

Example 7 (Translations). Given (V, A) with A , affine space built on V , K -vector space, then $\text{Tr} := \{t_v : A \rightarrow A | t_v(p) = p + v\}$, the group of translations, is acting faithfully on A .

Observation 13. Note that if X is a group $\text{AUT}(X) \subsetneq \mathcal{S}(X)$. Therefore in general if (G, X) is a permutation group and X is a group, the injective endomorphism $\Phi : G \rightarrow \mathcal{S}(X)$ doesn't necessarily induce an endomorphism $G \rightarrow \text{AUT}(X)$.

15

This definition
should be before Remark 13

5.3. Step 2: Semidirect Products

Definition 20. Given two groups H, N , with operations $*_H$ and $*_N$ and an homomorphism $\varphi : H \rightarrow \text{AUT}(N)$, where $\text{AUT}(N)$ is the group $\{f : N \rightarrow N \mid f \text{ is bijective}\}$, we can define on the set $H \times N$ the subsequent operation:

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

We call $(H \times N, \star_\varphi)$ the **Semidirect Product** of N and H relative to φ and we write it down as $H \ltimes_\varphi N$.

Proposition 10. $H \ltimes_\varphi N$ is a group, where the identity is $(1_H, 1_N)$ and, for each (h, n) the inverse is $(h^{-1}, (\varphi(h))(n^{-1}))$. **for each** $(h, n) \in H \ltimes_\varphi N$.

Example 8 (Dihedral Groups). Among the first groups studied there were the groups of symmetries, i.e. given a geometric shape A , the set of all geometrical transformation which leave A unchanged. Let A be a regular polygon of n sides, and you will obtain the group of symmetries D_n , the so called n -Dihedral Group. In it we can have two types of transformations, the rotation of $\frac{k\pi}{n}$ degrees around the centre of the polygon, or the reflection around one of the n possible axes of symmetry. It turns out that a possible way to represent this group is through the Semidirect Product $\mathbb{Z}_2 \ltimes_\varphi \mathbb{Z}_n$, where $\varphi(0)(z) := \text{id}_{\mathbb{Z}_n}(z) = z$ and $\varphi(1)(z) := \text{inv}_{\mathbb{Z}_n}(z) := -z$. So $\mathbb{Z}_2 \times \mathbb{Z}_n \ni (0, n_1) * (h_2, n_2) = (h_2, n_1 + n_2)$ and $(1, n_1) * (h_2, n_2) = (h_2, n_1 - n_2)$. Practically, if we have $(h, k) \in \mathbb{Z}_2 \times \mathbb{Z}_n$, h tells us if we are reflecting the figure or not, and k tells us we are rotating of $\frac{k\pi}{n}$ radians.

5.4. Step 3: Restricted and Unrestricted Wreath Products

Definition 21. Given a group A and an arbitrary set of indexes Y we define:

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

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

In case $|Y|$ is finite there's no difference between the two structures.

Remark

Observation 14. If A is a group we can extend its operation on the two structures component-wise, to obtain so another 'bigger' group.

Norm 7. If the reader is already familiar with the concepts we will treat, note that we will use a notation inverted respect to western researchers, that means: Western Notation: $A \wr B$ $A \rtimes_\varphi B$ Grigorchuk Notation: $B \wr A$ $B \ltimes_\varphi A$. This choice is made because in the case of an infinite wreath or semidirect product is useful to have a finite number of symbols on our left.

Example 9.

Now let's take (B, Y) , A groups, where (B, Y) is a permutation group. If we construct A^Y we have a group on which B can act faithfully, so we have an injective homomorphism $\Phi : B \rightarrow \mathcal{S}(A^Y)$, through the action of B on the indexes of A^Y . If we prove that $\Phi(B) \subset \text{AUT}(A^Y)$ we have everything we need to construct $B \ltimes_\Phi A^Y = H \ltimes_\varphi N$. The same can be done substituting A^Y with $A^{(Y)}$.

Let's formalise this:

TO AVOID THESE BLACK BOXES, YOU CAN PUT SLOPPY TO THE EXAMPLE ↗ overfull lines

Let (B, Y) be a transformation group and A a group.

Proposition 11. Given (B, Y) and A groups, with (B, Y) permutation group, we can extend the action of B on A^Y , so (B, A^Y) is a permutation group. Plus, B is a subgroup of $\text{AUT}(A^Y)$ with $\text{AUT}(A^Y)$ group respect to the component-wise operation on A . The same can be done substituting A^Y with $A^{(Y)}$. ? in addition

Proof. If bY is the action of B on Y , we can define the action q of B on A^Y as follow:

$$q(b \in B, \bar{a} \in A^Y) = q_b(\bar{a}) = b\bar{a} = b(a_y)_{y \in Y} := (a_{by})_{y \in Y} = (a_y)_{b^{-1}y \in Y}$$

- (1) We have to prove that q is a faithful, i.e. that $q_b \in \mathcal{S}(A^Y)$: if $\bar{a} = (a_y)_{y \in Y} \neq (x_y)_{y \in Y} = \bar{x} \Rightarrow \exists y' \in Y$ such that $a_{y'} \neq x_{y'}$. Let's now look $q_b(\bar{a})$ at the index by' . We find that at the by' -th component $a_{by'}$ is different from $x_{by'}$. So q_b is injective. The surjectivity is very simple: if we have $(a_y)_{y \in Y}$ the element $(a_{b^{-1}y})_{y \in Y}$ is its counter-image.
- (2) We have now to prove that q_b is an automorphism: $q_b(\bar{a} * \bar{x}) = q_b((a_y * x_y)_{y \in Y}) = (a_{by} * x_{by})_{y \in Y} = (a_{by})_{y \in Y} * (x_{by})_{y \in Y} = q_b(\bar{a}) * q_b(\bar{x})$

□

Definition 22. Given a permutation group (B, Y) and a group A we call **Wreath Product**, and we sign it $B \wr A$ one of these two structures:

- The **Unrestricted Wreath Product**, so the semidirect product on $B \times A^Y$ where the required homomorphism is the application $\varphi : B \rightarrow \mathcal{S}(A^Y)$ defined by $(\varphi(b))(\bar{a} = (a_y)_{y \in Y}) = (a_{by})_{y \in Y}$.
- The **Restricted Wreath Product**, so the semidirect product on $(B, A^{(Y)})$ where the required homomorphism is the application $\varphi : B \rightarrow \mathcal{S}(A^{(Y)})$ defined by $(\varphi(b))(\bar{a} = (a_y)_{y \in Y}) = (a_{by})_{y \in Y}$.

reward
+ mis

Therefore, having $(b_1, \bar{p}), (b_2, \bar{q})$ in $B \times A^Y$ or in $B \times A^{(Y)}$, their product is:

$$\begin{aligned} (b_1, \bar{p}) *_{\phi} (b_2, \bar{q}) &= (b_1, (p_y)_{y \in Y}) *_{\phi} (b_2, (q_y)_{y \in Y}) := \\ &= (b_1 *_B b_2, \bar{p} * (\phi(b_1))(\bar{q})) = (b_1 *_B b_2, (p_y * q_{b_1 y})_{y \in Y}) \end{aligned}$$

If we take a two group B, A , we can anyway consider their wreath product considering (B, B) a permutation group, where B acts faithfully on himself by left multiplication.

Observation 15. From the context it will be understandable, or it will be stated, of which of the two structure are we talking about. Notice that if Y is finite there's no difference between the restricted and unrestricted wreath product.

After all this technical work we need to breathe with some example.

Example 10 (Generalised Symmetric Groups).

"in nature"
↓ I am not
sure :)

Observation 16. Wreath products arise quite often in mathematics and nature. Interesting examples involve groups used to understand and solve Sudoku or the Rubik's Cube. Otherwise John Rodes in [?] states many examples of the applications of the theory of Automata, which as we will see, are deeply bounded with the structure of the Wreath Product.

6. FREE GROUPS

Often in Group Theory, we ask ourselves: is it possible to build a group G with a set S of characteristics? And then we have to search for a specimen of G "in the wild", exactly how Grigorchuk did for his group. But if the set S is simple enough, so our requirements are all of a certain type, Free Groups give us a way to plasm the searched object directly from S ! The difference is thin.

Part 4. Classification of every 2-state Automaton over a 2-letter
alphabet

7. OVERTOURE

- 7.1. Case of \mathbb{Z}_2 .
- 7.2. Klein Group.
- 7.3. case 3.
- 7.4. case 4.
- 7.5. Infinite Dihedral Group.
- 7.6. Lamplighter Group.

REFERENCES

General comments:

1. First do the following:

formulate the Classification Theorem
and before the formulation define
all the groups that are mentioned there:
pay special attention to the lamplighter group.

2. Then: go on to the proof of
the classification Theorem.

I suggest that you include only
a part of the proof (in particular,
that you skip the part with the
lamplighter group, and maybe
even more).

3. Then: Enter changes, as I

specified, to the first part.

If some definition is not used
in the sequel, think that you may be
exclude it

4. Remember: your thesis
should not be too long !!!

[if you want a longer thesis,
this can be your Master's thesis
later on]

For now, only a shorter version
is needed!

Overall, the beginning is OK,
go on!
