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, 2021

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

2021

Contents

Groups of automata

Abstract

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

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

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

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

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

Math. Subj. Class. (2020): 68Q45, 68Q70, 20E07, 20E22, 20E08, 18B20, 20M05

Keywords: automaton, finite automaton, word space, Moore diagram, wreath product, semidirect 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 razdelku raziščemo osnove teorije avtomatov. Hevristično uvedemo avtomat kot računski model, tj. stroj, ki vsakemu vhodnemu podatku (input) priredi izhodnega (output). Input in output predstavimo z elementi množice $\mathbf{X}$, ki ji pravimo abeceda. Množico končnih zaporedij $\mathbf{X}^*$, imenovano končni slovar, si ogledamo kot monoid glede na opercijo stikanja besed $\circ$, pri čemer za identiteto vzamemo prazno besedo $\varnothing$. Za dano besedo $x_1 \dots x_n \in \mathbf{X}^*$ definiramo njeno dolžino $|x_1 \dots x_n| = n$. Definiramo $\mathbf{X}^\omega$, množico neskončnih zaporedij elementov $\mathbf{X}$, imenovano neskončni slovar. Beseda $\mathbf{w} = x_1 \dots x_n$ je prefiks besede $\mathbf{u} \in \mathbf{X}^*$ (ali $\mathbf{u} \in \mathbf{X}^\omega$), če velja $\mathbf{u} = \mathbf{wv} = x_1 \dots x_n\mathbf{v}$ za nek $\mathbf{u} \in \mathbf{X}^*$ (ali $\in \mathbf{X}^\omega$). V tem primeru definiramo $\mathbf{v} = \mathbf{u} - \mathbf{w}$. Podamo definicijo skupnega prefiksa maksimalne dolžine neke množice besed v $\mathbf{X}^* \cup \mathbf{X}^\omega$ in ga uporabimo za vpeljavo metrike na $\mathbf{X}^\omega$. Ogledamo si nato karakterizacijo $\mathbf{X}^*$ z drevesnim grafom: vozlišče $\mathbf{w}$ je potomec vozlišča $\mathbf{v} \in \mathbf{X}^*$ natanko tedaj, ko velja $\mathbf{w} = \mathbf{v}x$ za nek $x \in \mathbf{X}$. Le tej konstrukciji rečemo drevo besed na $\mathbf{X}$. Vpeljemo koncept homomorfizma drevesa besed, tj. funkcijo $f : A \longrightarrow B$, za taki drevesi besed A, B, da sta zadoščena pogoja (1) $f(\varnothing) = \varnothing$, in (2) če je $\mathbf{w} \in A$ potomec $\mathbf{v} \in A$, potem je $f(\mathbf{w})$ potomec $f(\mathbf{v})$. Nadaljujemo z definicijo Mealyjevega končnega deterministočnega avtomata:

Definicija 0.1. Avtomat je četvorka $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$, kjer so:

- $\mathbf{X}$ je abeceda, na katero se običajno naslavljamo kot abeceda inputov in/ali outputov,
- $\mathcal{Q}$ je množica imenovana množica notranjih stanj avtomata,
- $\pi : \mathbf{X} \times \mathcal{Q} \longrightarrow \mathcal{Q}$ je funkcija imenovana funkcija tranzicije,
- $\lambda : \mathbf{X} \times \mathcal{Q} \longrightarrow \mathbf{X}$ je funkcija imenovana funkcija outputa.

Rečemo, da je $\mathcal{A}$ avtomat $|\mathcal{Q}|$ stanj na $\mathbf{X}$.

Predstavimo ponazoritev avtomatov z Mooreovimi diagrami in ugotovimo, da vsak Mooreov diagram enolično definira avtomat. Posplošimo definiciji funkcije tranzicije in funkcije outputa s pomočjo rekurzivnih zvez:

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

Nadaljujemo z definicijo začetnega avtomata $\mathcal{A}_{q_0}$ (oziroma avtomata $\mathcal{A}$ s fiksiranim stanjem q_0) in delovanjem slednjega $\bar{\lambda}_{q_0} : \mathbf{X}^* \longrightarrow \mathbf{X}^*$.

V drugem razdelku si ogledamo algebraične strukture, ki jih definirajo avtomati. Z danima avtomatoma $\mathcal{A}_1$ in $\mathcal{A}_2$ definiramo kompozicijo $\mathcal{A}_1 * \mathcal{A}_2$, ki nam omogoča, da za delovanji $\bar{\lambda}_{\mathcal{A}_1}, \bar{\lambda}_{\mathcal{A}_2}$ avtomatov $\mathcal{A}_1$ in $\mathcal{A}_2$, izpeljemo $\bar{\lambda}_{q_2}^{\mathcal{A}_2} \circ \bar{\lambda}_{q_1}^{\mathcal{A}_1} = \bar{\lambda}_p^{\mathcal{A}_1 * \mathcal{A}_2}$ za nek p iz množice stanj $\mathcal{A}_1 * \mathcal{A}_2$. Opazimo torej lahko, da je množica funkcij $f : \mathbf{X}^* \longrightarrow \mathbf{X}^*$, definiranih s kakim začetnim avtomatom, ki jim pravimo sinhrone avtomatske transformacije, polgrupa glede na operacijo komponiranja funkcij. Pišemo $\mathcal{FSA}(\mathbf{X})$. Ugotovimo, da je funkcija $f : \mathbf{X}^* \longrightarrow \mathbf{X}^*$ avtomatska sinhrona transformacija,

natanko tedaj, ko je endomorfizem drevesa na $\mathbf{X}^*$. Opazimo: če je f endomorfizem drevesa na $\mathbf{X}^*$, velja $f(\mathbf{X}^n) \subseteq \mathbf{X}^n$ (f ohranja dolžino besed iz $\mathbf{X}^*$) in je $f(\mathbf{v})$ prefiks $f(\mathbf{vw})$ za vse elemente $\mathbf{vw} \in \mathbf{X}^*$. Nato definiramo zožitev endomorfizma drevesa f na $\mathbf{v} \in \mathbf{X}^*$ kot funkcijo $f|_{\mathbf{v}} : \mathbf{X}^* \longrightarrow \mathbf{X}^*$, definirano s $f|_{\mathbf{v}}(\mathbf{w}) = f(\mathbf{vw}) - f(\mathbf{v})$. Opazimo, da za dano delovanje $\bar{\lambda}_{q_0}$ začetnega avtomata velja $(\bar{\lambda}_{q_0})|_{\mathbf{v}} = \bar{\lambda}_{\bar{\pi}(\mathbf{v},q_0)}$.

V naslednjem podrazdelku, za dana $q_0, q \in \mathcal{Q}$ in avtomat $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$ rečemo, da je stanje q dostopno glede na stanje q_0, če obstaja beseda $\mathbf{w} \in \mathbf{X}^*$, da velja $\bar{\lambda}_{q_0}(\mathbf{w}) = q$. Dokažemo sledečo trditev:

Trditev 0.1. *Za dani avtomat $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$ in stanje $q_0 \in \mathcal{Q}$, je $\bar{\lambda}_{q_0}$ obrnljiva funkcija če in samo če za vsako dostopno stanje $q \in \mathcal{Q}$ (glede na q_0), je funkcija $\lambda_q : \mathbf{X} \longrightarrow \mathbf{X}$ obrnljiva.*

Rečemo, da je začetni avtomat $\mathcal{A}_{q_0}$ obrnljiv, če je njegovo delovanje $\bar{\lambda}_{q_0}$ obrnljivo. Podobno rečemo, da je $\mathcal{A}$ obrnljiv, če je delovanje $\mathcal{A}_{q_0}$obrnljivo za vsak q_0 iz množice stanj $\mathcal{A}$, in vpeljemo alternativno notacijo Mooreovih diagramov. Za dani avtomat $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$, označimo polgrupo generirano z $\mathcal{A}$ kot množico:

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

kjer je $\langle S \rangle$, za neko množico S, najmanjša podpolgrupa, ki vsebuje S. Od tod naprej privzemamo, da so avtomati obrnljivi: torej bo $H(\mathcal{A})$ podgrupa $\mathcal{GA}(\mathbf{X})$, množice bijektivnih sinhronih avtomatskih transformacij.

V tretjem razdelku se posvetimo specifičnim algebraičnim konstrukcijam, ki so potrebne za analizo z avtomati generiranih grup. Definiramo simetrično grupo $\mathcal{S}(X)$ množice X, in operacijo produkta funkcij $f \cdot g := g \circ f$. Nato definiramo levo delovanje grupe G na množico X kot homomorfizem $T_l : G \longrightarrow (\mathcal{S}(X), \circ)$, in desno delovanje kot homomorfizem $T_r : G \longrightarrow (\mathcal{S}(X), \cdot)$. Dokažemo, da obstaja levo delovanje G na X natanko tedaj, ko obstaja funkcija $\tau_l : G \times X \longrightarrow X$, ki zadošča pogojema:

(1) $1x := \tau_l(1, x) = x$ za vsak $x \in X$,
(2) $g(hx) := \tau_l(g, \tau_l(h, x)) = \tau_l(g * h, x) =: (g * h)x$ za vsak $x \in X$ in $g, h \in G$.

Analogna karakterizacija velja za desna delovanja. Rečemo, da je delovanje $T_l : G \longrightarrow (\mathcal{S}(X), \circ)$ grupe G na množico X zvesto, če je T_l injektivna. V takem primeru (G, X) imenujemo grupa levih permutacij. Analogno opišemo grupo desnih permutacij (X, G) in si ogledamo nekaj primerov. Definiramo desno delovanje grupe H na grupo N kot homomorfizem $\varphi : H \longrightarrow (\mathcal{AUT}(N), \cdot)$. Za dani grupi H, N in desno delovanje $\varphi : H \longrightarrow (\mathcal{AUT}(N), \cdot)$, na $H \times N$ definiramo delovanje:

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

Poimenujemo $(H \times N, \star_\varphi)$ semidirektni produkt $H \ltimes_\varphi N$ grup H in N glede na φ, in uvedemo notacijo $H \ltimes_\varphi N$. Dokažemo, da je $H \ltimes_\varphi N$ grupa, ter si ogledamo primer izomorfnosti $\mathbb{Z}_2 \ltimes_\varphi \mathbb{Z}_n$ in $\mathcal{D}_n$, diederske grupe reda n. V naslednjem podrazdelku, za poljubno grupo A in množico Y, definiramo direktni produkt

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

ter direktno vsoto:

$$A^{(Y)} := \{ \widetilde{a} = (a_\omega)_{\omega \in Y} : a_\omega \in A \text{ in } a_\omega \neq 1_A \text{ le za končno mnogo } \omega \}.$$

Nato dokažemo, da je za poljubno grupo desnih permutacij (Y, B) in poljubno grupo A, delovanje $\Phi : B \longrightarrow \mathcal{AUT}(A^Y)$ definirano kot

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

desno delovanje B na grupo A^Y, kjer A^Y jemljemo z operacijo grupe A po komponentah. Analogno velja, če A^Y nadomestimo z $A^{(Y)}$. Z enakimi predpostavkami definiramo še zoženi venčni produkt $B \wr A$ med B in A kot $B \ltimes_\Phi A^{(Y)}$, z notacijo $B \wr A$, medtem ko ne-zoženi venčni produkt $B \wr A$ med B in A definiramo kot $B \ltimes_\Phi A^Y$, z notacijo $B \wr A$. Opazimo, da se enako notacijo uporablja za $B \ltimes_\Phi A^{(Y)}$ in $B \ltimes_\Phi A^Y$, kar pa ne privede do dvoumij, saj iz konteksta vedno razumemo v kateri situaciji smo. Če je $Y = \{y_1, \ldots, y_k\}$, pišemo $(\beta, (a_i)_{i \in Y}) \in B \wr A$ kot $\beta(a_1, \ldots, a_k)$.

Nazadnje, preučene strukture apliciramo na analizo avtomatov. Definiramo $T : (\mathcal{AUT}_{tree}(\mathbf{X}^*), \circ) \longrightarrow (\mathcal{S}(\mathbf{X}), \circ)$ kot $T(f)(x) := f(x)$, kjer je $\mathcal{AUT}_{tree}(\mathbf{X}^*)$ množica avtomorfizmov dreves na $\mathbf{X}^*$, tj. bijektivnih sinhronih avtomatskih transformacij, in dokažemo, da je homomorfizem. S tako definiranim T podamo trditev:

Trditev 0.2. *Naj bo $\mathbf{X} = \{x_1, \ldots, x_k\}$ in T kot zgoraj. Vzemimo grupo desnih permutacij $(\mathbf{X}, \mathcal{S}(\mathbf{X}))$, kjer $\mathcal{S}(\mathbf{X})$ deluje z desne na $\mathcal{AUT}_{tree}(\mathbf{X}^*)^{\mathbf{X}}$ kot $\Phi(\sigma)(f_{x_1}, \ldots, f_{x_k}) = (f_{x_1\sigma}, \ldots, f_{x_k\sigma})$. Definiramo $\psi : (\mathcal{AUT}_{tree}(\mathbf{X}^*), \circ) \longrightarrow (\mathcal{S}(\mathbf{X}), \circ) \wr (\mathcal{AUT}_{tree}(\mathbf{X}^*), \circ) = \mathcal{S}(\mathbf{X}) \ltimes_\Phi \mathcal{AUT}_{tree}(\mathbf{X}^*)^{\mathbf{X}}$ kot*

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

kjer je $f|_{x_k}$ zožitev f na x_k. Sledi: ψ je izomorfizem grup.

S pomočjo ψ prepišemo levo delovanje $\mathcal{AUT}_{tree}(\mathbf{X}^*)$ na $\mathbf{X}^*$ v obliko:

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

kjer je $w_1 w_2 \ldots w_n$ beseda iz $\mathbf{X}^*$. Nadaljujemo s pomembnim rezultatom:

Trditev 0.3. *Naj bo $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$ tak avtomat, za katerega sta $\mathcal{Q} = \{q_1, \ldots, q_n\}$ in $\mathbf{X} = \{x_1, \ldots, x_k\}$. Množico delovanj $\bar{\lambda}_{q_l}$, definiranih z $\mathcal{A}$, lahko torej opišemo z n rekurzivnimi zvezami*

$$\begin{aligned} f_{q_1} &= \beta_{q_1}(h_{x_1,q_1}, \ldots, h_{x_k,q_1}), \\ f_{q_2} &= \beta_{q_2}(h_{x_1,q_2}, \ldots, h_{x_k,q_2}), \\ &\ldots \\ f_{q_n} &= \beta_{q_n}(h_{x_1,q_n}, \ldots, h_{x_k,q_n}), \end{aligned} \tag{1}$$

pri čemer je vsak h_{x_i,q_j} enak nekemu f_{q_l}, in je β_{q_j} neka permutacija abecede $\mathbf{X}$. Velja še več. Naj bo S sistem (1), pri čemer je vsak h_{x_i,q_j} enak nekemu f_{q_l}, in je β_j neka permutacija abecede. Potem S enolično definira tak avtomat $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$, da je $\bar{\lambda}_{q_l} = f_{q_l}$ za vsak $q_l \in \mathcal{Q}$.

V četrtem razdelku predstavljamo rezultat, ki opisuje vse grupe generirane z avtomati dveh stanj na abecedi dveh črk $\mathbf{X} = \{0, 1\}$. Najprej vpeljemo nekatere matematične objekte, ki se pojavijo v formulaciji in dokazu klasifikacijskega izreka. Ogledamo si neskončno diedersko grupo $\mathbb{Z}_2 \ltimes_\varphi \mathbb{Z}$, oziroma grupo simetrij $\mathbb{Z}$, in grupo svetilničarja $\mathbb{Z} \wr \mathbb{Z}_2 = \mathbb{Z} \ltimes \mathbb{Z}_2^{(\mathbb{Z})}$. Nato definiramo partikularno bijektivno sinhrono avtomatsko transformacijo na $\mathbf{X} = \{0, 1\}$, seštevalni stroj $f = \tau(f, \mathrm{id}_{\mathcal{GA}(\mathbf{X})})$. S preučevanjem lastnosti f pridelamo dokaz izomorfnosti $\langle f \rangle$ in $\mathbb{Z}$. Formuliramo izrek:

Izrek 0.4. *Naj bo $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$ avtomat. Naj velja $\mathbf{X} = \{0, 1\}$ in $|\mathcal{Q}| = 2$. Grupa generirana z $\mathcal{A}$ je potem izomorfna eni izmed naslednjih grup:*

(1) *trivialni grupi* $\{1\}$,
(2) *grupi* $(\mathbb{Z}_2, +)$,
(3) *direktni vsoti* $\mathbb{Z}_2 \oplus \mathbb{Z}_2$,

(4) *neskončni ciklični grupi* $\mathbb{Z}$,
(5) *neskončni diederski grupi* $\mathcal{D}_\infty$,
(6) *grupi svetilničarja* $\mathcal{L}$.

Za konec predstavimo še del dokaza zgornjega izreka. Opazimo: če velja $\mathcal{Q} = \{r, s\}$, in $a := \bar{\lambda}_r$ ter $b := \bar{\lambda}_s$, so možne definicije a, b oblike:

$$\begin{aligned} a &= \sigma^{i_1}(x_{11}, x_{12}), \\ b &= \sigma^{i_2}(x_{21}, x_{22}), \end{aligned} \tag{2}$$

kjer $x_{ij} \in \{a, b\}$ in $\sigma^{i_1}, \sigma^{i_2} \in \mathcal{S}(\mathbf{X})$, $i_1, i_2 \in \{0, 1\}$, pri čemer $\sigma^0 := \mathrm{id}_{\mathcal{S}(\mathbf{X})}$ ter $\sigma^1 := \tau$, transpozicija $\mathcal{S}(\mathbf{X})$. Ugotovimo, da je za opazovanje vseh grup definiranih z $\mathcal{A}$, do izomorfizma natančno, dovolj analizirati zgolj 24 primerov, za katere je $a \in \{\tau(a, a), \tau(a, b), \tau(b, b)\}$. Zaključimo z analizo nekaterih primerov izmed slednjih.

Ključne besede: avtomat, končni avtomat, besedni prostor, Moorov diagram, semidirektni produkt, venčni produkt, rekurzivnost, grupa svetilničarja, neskončna diedrska grupa, stroj dodajanja, delovanje grup na drevesih

Gruppi di automi

Sintesi Estesa

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

Nella prima sezione esploriamo le basi della teoria degli automi. Introduciamo euristicamente l'automa come modello di computazione, ovvero una macchina che per ogni dato in ingresso (input), ritorna un altro dato (output). Presentiamo input ed output con elementi dell'insieme $\mathbf{X}$, che chiamiamo alfabeto. Vediamo l'insieme delle sequenze finite $\mathbf{X}^*$, detto dizionario finito, come un monoide rispetto all'operazione di composizione di parole $\circ$, dove l'identità è data da $\varnothing$, la parola senza lettere. Data una parola $x_1 \dots x_n \in \mathbf{X}^*$ definiamo la sua lunghezza come $|x_1 \dots x_n| = n$. Definiamo $\mathbf{X}^\omega$, l'insieme delle sequenze infinite di elementi di $\mathbf{X}$, detto dizionario infinito. Una parola $\mathbf{w} = x_1 \dots x_n$ è il prefisso di una parola $\mathbf{u} \in \mathbf{X}^*$ (o $\mathbf{u} \in \mathbf{X}^\omega$) se $\mathbf{u} = \mathbf{wv} = x_1 \dots x_n\mathbf{v}$ per qualche $\mathbf{u} \in \mathbf{X}^*$ (o $\in \mathbf{X}^\omega$). In questo caso definiamo $\mathbf{v} = \mathbf{u} - \mathbf{w}$. Diamo la definizione di prefisso comune di lunghezza massima di un insieme di parole in $\mathbf{X}^* \cup \mathbf{X}^\omega$ e lo usiamo per definire una metrica su $\mathbf{X}^\omega$. Vediamo poi la caratterizzazione di $\mathbf{X}^*$ come grafo ad albero: un nodo $\mathbf{w}$ è discendente di un altro $\mathbf{v} \in \mathbf{X}^*$ se e solo se $\mathbf{w} = \mathbf{v}x$, per qualche $x \in \mathbf{X}$. Chiamiamo questa costruzione albero delle parole su $\mathbf{X}$. Introduciamo la nozione di omomorfismo d'albero di parole, ovvero una funzione $f : A \longrightarrow B$, con A, B alberi di parole, tali che (1) $f(\varnothing) = \varnothing$ e (2) se $\mathbf{w} \in A$ è discendente di $\mathbf{v} \in A$, allora $f(\mathbf{w})$ è discendente di $f(\mathbf{v})$. Passiamo alla definizione di automa deterministico finito di Mealy:

Definizione 0.1. Un automa è una 4-tupla $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$ dove:

- $\mathbf{X}$ è un alfabeto, a cui di solito ci riferiamo con alfabeto degli input e/o output,
- $\mathcal{Q}$ è un insieme detto insieme degli stati interni dell'automa,
- $\pi : \mathbf{X} \times \mathcal{Q} \longrightarrow \mathcal{Q}$ è una funzione detta funzione di transizione,
- $\lambda : \mathbf{X} \times \mathcal{Q} \longrightarrow \mathbf{X}$ è una funzione detta funzione d'output.

Diciamo che $\mathcal{A}$ è un automa a $|\mathcal{Q}|$ stati su $\mathbf{X}$.

Diamo una rappresentazione degli automi con i diagrammi di Moore e scopriamo che ogni diagramma di Moore definisce unicamente un automa. Estendiamo le definizioni della funzione di transizione e della funzione d'output tramite le formule ricorsive:

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

Passiamo alla definizione di automa iniziale $\mathcal{A}_{q_0}$ (ovvero l'automa $\mathcal{A}$ con lo stato q_0 fissato) e della sua azione $\bar{\lambda}_{q_0} : \mathbf{X}^* \longrightarrow \mathbf{X}^*$.

Nella sezione due vediamo le strutture algebriche definite dagli automi. Dati due automi $\mathcal{A}_1$ ed $\mathcal{A}_2$ definiamo la loro composizione $\mathcal{A}_1 * \mathcal{A}_2$, che ci permette di dire che se $\bar{\lambda}_{\mathcal{A}_1}, \bar{\lambda}_{\mathcal{A}_2}$ sono le azioni di $\mathcal{A}_1$ ed $\mathcal{A}_2$ rispettivamente, allora $\bar{\lambda}_{q_2}^{\mathcal{A}_2} \circ \bar{\lambda}_{q_1}^{\mathcal{A}_1} = \bar{\lambda}_p^{\mathcal{A}_1 * \mathcal{A}_2}$ per qualche p nell'insieme degli stati di $\mathcal{A}_1 * \mathcal{A}_2$. Ciò ci permette di osservare

che l'insieme delle funzioni $f : \mathbf{X}^* \longrightarrow \mathbf{X}^*$ definite da qualche automa iniziale, dette trasformazioni automatiche sincrone, è un semigruppo rispetto all'operazione di composizione di funzioni. Lo denotiamo con $\mathcal{FSA}(\mathbf{X})$. Scopriamo che una funzione $f : \mathbf{X}^* \longrightarrow \mathbf{X}^*$ è una trasformazione automatica sincrona se e solo se è un endomorfismo d'albero su $\mathbf{X}^*$. Osserviamo che se f è un endomorfismo d'albero su $\mathbf{X}^*$ allora $f(\mathbf{X}^n) \subseteq \mathbf{X}^n$ (f preserva la lunghezza delle parole in $\mathbf{X}^*$) e $f(\mathbf{v})$ è un prefisso di $f(\mathbf{vw})$ per tutti gli elementi $\mathbf{vw} \in \mathbf{X}^*$. Definiamo poi la restrizione di un endomorfismo d'albero f in $\mathbf{v} \in \mathbf{X}^*$ come la funzione $f|_{\mathbf{v}} : \mathbf{X}^* \longrightarrow \mathbf{X}^*$ definita come $f|_{\mathbf{v}}(\mathbf{w}) = f(\mathbf{vw}) - f(\mathbf{v})$. Osserviamo che data un'azione $\bar{\lambda}_{q_0}$ di un automa iniziale, $(\bar{\lambda}_{q_0})|_{\mathbf{v}} = \bar{\lambda}_{\bar{\pi}(\mathbf{v},q_0)}$.

Nella sottosezione successiva, dati $q_0, q \in \mathcal{Q}$ per un automa $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$, diciamo che uno stato q è accessibile rispetto ad uno stato q_0 se esiste una parola $\mathbf{w} \in \mathbf{X}^*$ tale che $\bar{\lambda}_{q_0}(\mathbf{w}) = q$. Dimostriamo la seguente proposizione:

Proposizione 0.5. *Dato un automa $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$ ed uno stato $q_0 \in \mathcal{Q}$, $\bar{\lambda}_{q_0}$ è una funzione invertibile se e solo se per ogni stato accessibile $q \in \mathcal{Q}$ (rispetto a q_0) la funzione $\lambda_q : \mathbf{X} \longrightarrow \mathbf{X}$ è invertibile.*

Diciamo che un automa iniziale $\mathcal{A}_{q_0}$ è invertibile se la sua azione $\bar{\lambda}_{q_0}$ è invertibile. Diciamo che un automa $\mathcal{A}$ è invertibile se l'azione di $\mathcal{A}_{q_0}$ è invertibile per ogni q_0 nell'insieme degli stati di $\mathcal{A}$, ed introduciamo una notazione alternativa per i diagrammi di Moore. Dato un automa $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$ chiamiamo il semigruppo generato da $\mathcal{A}$ l'insieme:

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

dove $\langle S \rangle$, per un isieme S, è il più piccolo sottosemigruppo che contiene S. Da qui in poi per automa intendiamo automa invertibile, quindi $H(\mathcal{A})$ sarà un sottogruppo di $\mathcal{GA}(\mathbf{X})$, l'insieme delle trasformazioni sincrone automatiche biettive.

Nella terza sezione affrontiamo alcune costruzioni algebriche necessarie per l'analisi dei gruppi generati da automi. Definiamo il gruppo simmetrico $\mathcal{S}(X)$ di un insieme X, e l'operazione di prodotto di funzioni $f \cdot g := g \circ f$. Poi definiamo un'azione sinistra di un gruppo G su un insieme X come un omomorfismo $T_l : G \longrightarrow (\mathcal{S}(X), \circ)$ ed un'azione destra come un omomorfismo $T_r : G \longrightarrow (\mathcal{S}(X), \cdot)$. Mostriamo che esiste un'azione sinistra di G su X se e solo se esiste una funzione $\tau_l : G \times X \longrightarrow X$ tale che sono valide le condizioni:

(1) $1x := \tau_l(1, x) = x$ per ogni $x \in X$,
(2) $g(hx) := \tau_l(g, \tau_l(h, x)) = \tau_l(g * h, x) =: (g * h)x$ per ogni $x \in X$ e $g, h \in G$.

Una caratterizzazione analoga vale per le azioni destre. Diciamo che un'azione $T_l : G \longrightarrow (\mathcal{S}(X), \circ)$ di un gruppo G su un insieme X è fedele se T_l è iniettiva. In questo caso chiamiamo (G, X) un gruppo di permutazioni sinistro. Descriviamo analogamente un gruppo di permutazioni destre (X, G), e vediamo qualche esempio. Definiamo l'azione destra di un gruppo H su un gruppo N come con un omomorfismo $\varphi : H \longrightarrow (\mathcal{AUT}(N), \cdot)$. Dati gruppi H, N, e data un'azione destra $\varphi : H \longrightarrow (\mathcal{AUT}(N), \cdot)$, su $H \times N$ costruiamo la seguente operazione:

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

Chiamiamo $(H \times N, \star_\varphi)$ il prodotto semidiretto $H \ltimes_\varphi N$ di H e N relativo a φ e lo segnamo come $H \ltimes_\varphi N$. Dimostriamo che $H \ltimes_\varphi N$ è un gruppo e vediamo l'esempio di $\mathbb{Z}_2 \ltimes_\varphi \mathbb{Z}_n$ isomorfo a $\mathcal{D}_n$, il gruppo diedrale di ordine n. Nella sottosezione successiva

definiamo, presi un gruppo A ed un insieme Y, il prodotto diretto

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

e la somma diretta:

$$A^{(Y)} := \{\widetilde{a} = (a_\omega)_{\omega \in Y} : a_\omega \in A \text{ e } a_\omega \neq 1_A \text{ solo per un numero finito di } \omega\}.$$

Dimostriamo poi che avendo un gruppo di permutazioni destre (Y, B) ed un gruppo A, L'applicazione $\Phi : B \longrightarrow \mathcal{AUT}(A^Y)$ definita come

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

è un'azione destra di B sul gruppo A^Y, dove A^Y è preso con l'operazione di A componente per componente. Analogo risultato vale sostituendo A^Y con $A^{(Y)}$. Con le stesse premesse definiamo quindi il prodotto intrecciato ristretto $B \wr A$ di B e A come $B \ltimes_\Phi A^{(Y)}$, e lo segnamo come $B \wr A$, mentre definiamo il prodotto intrecciato non ristretto $B \wr A$ di B e A come $B \ltimes_\Phi A^Y$ e lo segnamo come $B \wr A$. Notiamo che si usa lo stesso simbolo per indicare sia $B \ltimes_\Phi A^{(Y)}$, sia $B \ltimes_\Phi A^Y$, ma questo fatto non dovrebbe creare particolare confusione, visto che il contesto permette sempre di capire in quale situazione ci si trovi. Se $Y = \{y_1, \ldots, y_k\}$ segnamo $(\beta, (a_i)_{i \in Y}) \in B \wr A$ come $\beta(a_1, \ldots, a_k)$.

Infine applichiamo le strutture studiate alla teoria degli automi. Definiamo $T : (\mathcal{AUT}_{tree}(\mathbf{X}^*), \circ) \longrightarrow (\mathcal{S}(\mathbf{X}), \circ)$ come $T(f)(x) := f(x)$, dove $\mathcal{AUT}_{tree}(\mathbf{X}^*)$ è l'insieme degli automorfismi d'albero su $\mathbf{X}^*$, i.e., delle trasformazioni sincrone automatiche biettive, e dimostriamo che è un omomorfismo. Con T così definito vediamo la seguente proposizione:

Proposizione 0.6. *Sia $\mathbf{X} = \{x_1, \ldots, x_k\}$ e T come prima. Prendiamo il gruppo di permutazioni destre $(\mathbf{X}, \mathcal{S}(\mathbf{X}))$, dove $\mathcal{S}(\mathbf{X})$ agisce da destra su $\mathcal{AUT}_{tree}(\mathbf{X}^*)^{\mathbf{X}}$ con $\Phi(\sigma)(f_{x_1}, \ldots, f_{x_k}) = (f_{x_1\sigma}, \ldots, f_{x_k\sigma})$. Definiamo $\psi : (\mathcal{AUT}_{tree}(\mathbf{X}^*), \circ) \longrightarrow (\mathcal{S}(\mathbf{X}), \circ) \wr (\mathcal{AUT}_{tree}(\mathbf{X}^*), \circ) = \mathcal{S}(\mathbf{X}) \ltimes_\Phi \mathcal{AUT}_{tree}(\mathbf{X}^*)^{\mathbf{X}}$ come*

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

dove $f|_{x_k}$ è la restrizione di f in x_k. Allora ψ è un isomorfismo di gruppi.

Attraverso ψ riscriviamo l'azione sinistra di $\mathcal{AUT}_{tree}(\mathbf{X}^*)$ su $\mathbf{X}^*$ come:

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

dove $w_1 w_2 \ldots w_n$ è una parola in $\mathbf{X}^*$. Proseguiamo poi con un altro importante risultato:

Proposizione 0.7. *Sia $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$ un automa tale che $\mathcal{Q} = \{q_1, \ldots, q_n\}$ e $\mathbf{X} = \{x_1, \ldots, x_k\}$. Allora l'insieme delle azioni $\bar{\lambda}_{q_l}$ definite da $\mathcal{A}$ può essere descritto con n formule ricorsive*

$$\begin{aligned} f_{q_1} &= \beta_{q_1}(h_{x_1,q_1}, \ldots, h_{x_k,q_1}), \\ f_{q_2} &= \beta_{q_2}(h_{x_1,q_2}, \ldots, h_{x_k,q_2}), \\ &\ldots \\ f_{q_n} &= \beta_{q_n}(h_{x_1,q_n}, \ldots, h_{x_k,q_n}), \end{aligned} \tag{3}$$

dove ogni h_{x_i,q_j} è uguale a qualche f_{q_l} ed ogni β_{q_j} è un permutazione dell'alfabeto $\mathbf{X}$. Inoltre, sia S un sistema (3), dove ogni h_{x_i,q_j} è uguale a qualche f_{q_l} ed ogni β_j è una permutazione dell'alfabeto. Allora S definisce unicamente un automa $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$ tale che $\bar{\lambda}_{q_l} = f_{q_l}$ per ogni $q_l \in \mathcal{Q}$.

Nella quarta sezione portiamo un risultato che descrive tutti i gruppi generati da un automa a due stati su un alfabeto con due lettere $\mathbf{X} = \{0, 1\}$. Per prima cosa introduciamo alcuni oggetti matematici che compaiono nella formulazione e nella dimostrazione del teorema di classificazione. Vediamo il gruppo diedrale infinito $\mathbb{Z}_2 \ltimes_\varphi \mathbb{Z}$, ovvero il gruppo delle simmetrie di $\mathbb{Z}$ ed il gruppo del lampionaio $\mathbb{Z} \wr \mathbb{Z}_2 = \mathbb{Z} \ltimes \mathbb{Z}_2^{(\mathbb{Z})}$. Poi definiamo una trasformazione sincrona automatica biettiva particolare su $\mathbf{X} = \{0, 1\}$, la macchina delle addizioni $f = \tau(f, \mathrm{id}_{\mathcal{G}\mathcal{A}(\mathbf{X})})$. Studiando alcune prioprietà di f siamo poi in grado di mostrare che $\langle f \rangle$ è isomorfo a $\mathbb{Z}$. Formuliamo il teorema:

Teorema 0.8. *Sia $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$ un automa. Sia $\mathbf{X} = \{0, 1\}$ e $|\mathcal{Q}| = 2$. Allora il gruppo generato da $\mathcal{A}$ è isomorfo ad uno dei seguenti gruppi:*

(1) *Il gruppo triviale $\{1\}$,*
(2) *Il gruppo $(\mathbb{Z}_2, +)$,*
(3) *La somma diretta $\mathbb{Z}_2 \oplus \mathbb{Z}_2$,*
(4) *Il gruppo ciclico infinito $\mathbb{Z}$,*
(5) *Il gruppo diedrale infinito $\mathcal{D}_\infty$,*
(6) *Il gruppo del lampionaio $\mathcal{L}$.*

Infine presentiamo una parte della dimostrazione. Vediamo che, se $\mathcal{Q} = \{r, s\}$, ed $a := \bar{\lambda}_r$ and $b := \bar{\lambda}_s$, allora le possibili definizioni di a, b sono:

$$\begin{aligned} a &= \sigma^{i_1}(x_{11}, x_{12}), \\ b &= \sigma^{i_2}(x_{21}, x_{22}), \end{aligned} \tag{4}$$

dove $x_{ij} \in \{a, b\}$ e $\sigma^{i_1}, \sigma^{i_2} \in \mathcal{S}(\mathbf{X})$, $i_1, i_2 \in \{0, 1\}$ con $\sigma^0 := \mathrm{id}_{\mathcal{S}(\mathbf{X})}$ mentre $\sigma^1 := \tau$, la trasposizione in $\mathcal{S}(\mathbf{X})$. Ci accorgiamo che per vedere tutti i gruppi definiti da $\mathcal{A}$, a meno di isomorfismi, possiamo analizzare esclusivamente i 24 casi dove $a \in \{\tau(a, a), \tau(a, b), \tau(b, b)\}$. Proseguiamo analizzando alcuni di questi casi.

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

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 see later that such functions form groups.

1.1. Words spaces and alphabet trees.

We begin with the formalization of input and output.

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

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

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 1.1. 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 by $\mathcal{P}(A)$ the *longest common prefix of all the words from* A. Note that $\mathcal{P}(A)$ that is uniquely defined.

We can endow the set $\mathbf{X}^\omega$ with a metric, and consequently a topology.

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

$$d_{\widetilde{\lambda}}(\mathbf{w_1}, \mathbf{w_2}) = \lambda_n \tag{5}$$

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. The function $d_{\widetilde{\lambda}}$ is always positive, is symmetrical and it can be easily proved that $d_{\widetilde{\lambda}}(\mathbf{w_1}, \mathbf{w_2}) = 0$ if and only if $\mathbf{w_1} = \mathbf{w_2}$. We prove the triangle 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. Suppose that $p > n$. We denote the word $\mathcal{P}(\{\mathbf{w_1}, \mathbf{w_2}\})$ by $x_1 \dots x_n$, the word $\mathcal{P}(\{\mathbf{w_1}, \mathbf{w_3}\})$ by $x_1 \dots x_n y_{n+1} \dots y_p$ and the word $\mathcal{P}(\{\mathbf{w_3}, \mathbf{w_2}\})$ by $x_1 \dots x_n z_{n+1} \dots z_p \dots z_q$. But then $x_1 \dots x_n y_{n+1} \dots y_p = x_1 \dots x_n z_{n+1} \dots z_p$ because they are of the same lenght and they are both prefixes of $\mathbf{w_3}$. Consequently the last word, of lenght p, is prefix both of $\mathbf{w_1}$ and $\mathbf{w_2}$. Therefore it is a prefix of $x_1 \dots x_n$, so $p \leq n$, contradicting the assumption that $p > n$. □

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

Remark 1.2. It is often useful to set $\widetilde{\lambda} = (\frac{1}{n})_{n \in \mathbb{N} \cup \{0\}}$.

It is useful to represent $\mathbf{X}^*$ in the form of a tree graph: $\varnothing$ is the root and $\mathbf{v} \in \mathbf{X}^*$ is a child of $\mathbf{u} \in \mathbf{X}^*$ if and only if $\mathbf{u} = \mathbf{v}x$ for some $x \in \mathbf{X}$. We call the resulting tree graph a *word tree* on $\mathbf{X}$. An example is given in Figure 2.

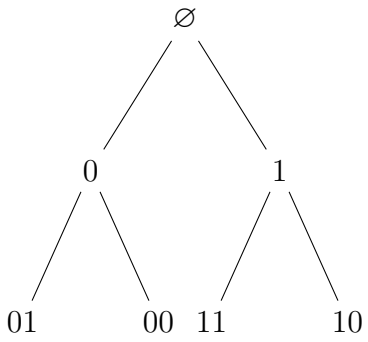

FIGURE 2. An example of the first three floors of the word tree on $\mathbf{X} = \{0, 1\}$.

Remark 1.3. We will mostly use the alphabet $\mathbf{X} = \{0, 1\}$.

The set $\mathbf{X}^n$ is called the the n-th floor of $\mathbf{X}^*$. Finally we define the notion of an endomorphism of a tree and describe some of its properties.

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

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

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

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

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

Definition 1.10. 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 definition explains us how an automaton performs the action of transforming an input into an output. We can imagine that for every input letter x we plug in the machine, and for every state q, from which we decide to start, the machine moves to a state $p = \pi(x, q) \in \mathcal{Q}$ and returns an output letter $y = \lambda(x, q) \in \mathbf{X}$.

Definition 1.11. Given an automaton $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$ we define its *Moore diagram* as the oriented graph $M = (\mathcal{Q}, \mathcal{E})$ where there is a directed edge from q_1 to q_2 whenever there exists $x \in \mathbf{X}$ such that $\pi(x, q_1) = q_2$ and the label assigned to this edge is $x|\lambda(x, q_1)$.

An example of Moore diagram is given in Figure 3.

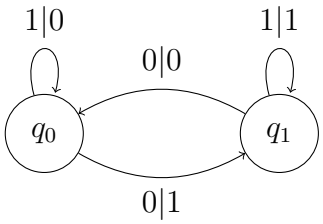

FIGURE 3. Example of the Moore diagram of a 2-state automaton over the alphabet $\mathbf{X} = \{0, 1\}$

Remark 1.4. Let $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$ be an automaton and $M = (\mathcal{Q}, \mathcal{E})$ its Moore diagram. Then M has the following property:

$$\forall (x, q) \in \mathbf{X} \times \mathcal{Q} \quad \exists! e = (q, p_{(x,q)}) \in \mathcal{E} \text{ for some } p \in \mathcal{Q} \; s.t. \\ \text{the left-hand side of the label of } e \text{ reads } \text{“}x\text{”}. \tag{6}$$

It follows that if an automaton $\mathcal{B} = \langle \mathbf{X}, \mathcal{Q}_{\mathcal{B}}, \pi_{\mathcal{B}}, \lambda_{\mathcal{B}} \rangle$ defines the same Moore diagram M, then $\mathcal{Q}_{\mathcal{B}} = \mathcal{Q}$, and for each $(x, q) \in \mathbf{X} \times \mathcal{Q}$ we have $\pi_{\mathcal{B}}(x, q) = p_{(x,q)} = \pi(x, q)$. Furthermore $\lambda_{\mathcal{B}}(x, q)$ is the left-hand side of the label of the edge $(q, p_{(x,q)})$, i.e., it is $\lambda(x, q)$. So automata are uniquely determined by their Moore diagram.

Example 1.12. 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 1.13. 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 1.5. The Definition 1.13 is equivalent to:
$$\bar{\pi}(\mathbf{w}x, q) = \bar{\pi}(x, \bar{\pi}(\mathbf{w}, q))$$
and
$$\bar{\lambda}(\mathbf{w}x, q) = \bar{\lambda}(\mathbf{w}, q)\bar{\lambda}(x, \bar{\pi}(\mathbf{w}, q)),$$
respectively.

Example 1.14. 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. For example, in Figure 3 to get an output we need to feed the machine both with an input x and a state q. So let us fix $q \in \mathcal{Q}$.

Definition 1.15. If an automaton $\mathcal{A}$ has a fixed state q_0, we call it an *initial automaton with the initial state* q_0 and we write it as $\mathcal{A}_{q_0}$. Each $\mathcal{A}_{q_0}$ naturally defines the map $\bar{\lambda}_{q_0} : \mathbf{X}^* \longrightarrow \mathbf{X}^*$ with $\bar{\lambda}_{q_0}(\mathbf{w}) := \bar{\lambda}(\mathbf{w}, q_0)$, called the *action of the automaton* $\mathcal{A}_{q_0}$. Two initial automata are said to be *equivalent* if they define the same actions.

Proposition 1.16. *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. We verify the statement by induction on $n = |\mathbf{w}|$.

Case $n = 0$: We defined $\bar{\lambda}_{q_0}(\varnothing) = \bar{\lambda}(\varnothing, q_0) = \varnothing$, and $|\varnothing| = |\bar{\lambda}_{q_0}(\varnothing)| = 0$.

Case $n \Rightarrow n + 1$: Let $|\bar{\lambda}_{q_0}(\mathbf{w})| = |\mathbf{w}| = n$ for every $\mathbf{w} \in \mathbf{X}^n$. Following Definition 1.13 we have $|\bar{\lambda}_{q_0}(\mathbf{w}x)| = |\bar{\lambda}_{q_0}(\mathbf{w})\bar{\lambda}_{\bar{\pi}(\mathbf{w},q_0)}(x)| = |\bar{\lambda}_{q_0}(\mathbf{w})| + |\bar{\lambda}_{\bar{\pi}(\mathbf{w},q_0)}(x)| = n + 1$. □

Remark 1.6. Given an initial automaton $\mathcal{A}_{q_0}$, we can define the infinite action $\bar{\lambda}_{q_0} : \mathbf{X}^\omega \longrightarrow \mathbf{X}^\omega$ by similar recursive formulas, and we can consequently declare that two initial automata are ω-equivalent if they determine the same infinite action. Two automata are equivalent if and only if they are ω-equivalent (Proposition 2.3 and Subsection 3.1 in [5]).

Example 1.17. In Figure 4 we present the Moore diagrams of two equivalent initial automata. ♢

Remark 1.7. An initial automaton is usually drawn depicting the initial state with a double circle around the respective vertex (Figure 4).

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

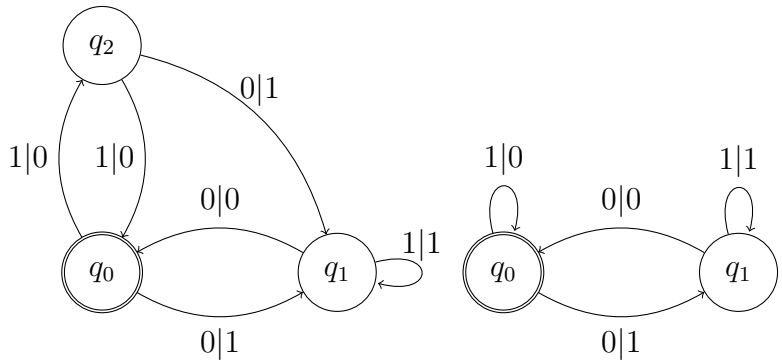

FIGURE 4. Two different initial automata which describe the same action. The double circle around q_0 tells us q_0 is the initial state.

2. The algebraic structures defined by automata

Here we will show how automata can define algebraic structures and how certain synchronous automatic transformations can be characterised.

Definition 2.1. Given automata $\mathcal{A}_1 = \langle \mathbf{X}, \mathcal{Q}_1, \pi_1, \lambda_1 \rangle$ and $\mathcal{A}_2 = \langle \mathbf{X}, \mathcal{Q}_2, \pi_2, \lambda_2 \rangle$, we define their composition $\mathcal{B} := \mathcal{A}_1 * \mathcal{A}_2 = \langle \mathbf{X}, \mathcal{Q}_1 \times \mathcal{Q}_2, \pi, \lambda \rangle$ 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 $x \in \mathbf{X}$ and $(s_1, s_2) \in \mathcal{Q}_1 \times \mathcal{Q}_2$.

Remark 2.1. 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. It can be verified 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 that the operation $*$ on the set of automata gives rise to an operation $*'$ on the set of initial automata defined as $(\mathcal{A}_1)_{q_1} *' (\mathcal{A}_2)_{q_2} := (\mathcal{A}_1 * \mathcal{A}_2)_{(q_1,q_2)}$. With the operation $*'$ the set of all initial automata on an alphabet $\mathbf{X}$ becomes a semigroup.

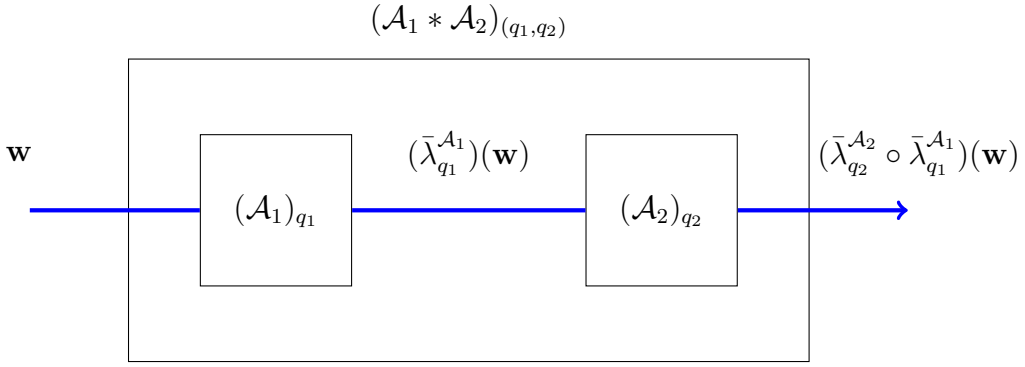

FIGURE 5. Concept of composition of initial automata.

2.1. **Synchronous automatic transformations.** In this section, given an action of an initial automaton, we describe and study its properties.

Definition 2.2. 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 2.3. 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 2.4. *The finite synchronous automatic transformations form a semigroup denoted by* $\mathcal{FSA}(\mathbf{X})$.

Proof. This arises from Remark 2.1. Let $f_1 = \bar{\lambda}_{q_1}^{\mathcal{A}_1}$ and $f_2 = \bar{\lambda}_{q_2}^{\mathcal{A}_2}$ be the actions of two initial automata $(\mathcal{A}_1)_{q_1}$ and $(\mathcal{A}_2)_{q_2}$ respectively. We have seen that

$$f_2 \circ f_1 = \bar{\lambda}_{q_2}^{\mathcal{A}_2} \circ \bar{\lambda}_{q_1}^{\mathcal{A}_1} = \bar{\lambda}_{(q_1,q_2)}^{\mathcal{A}_1 * \mathcal{A}_2},$$

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

Now we provide an important characterization of synchronous automatic transformations:

Proposition 2.5. *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) preserves the adjacency of vertices. 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:

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

But $|\bar{\lambda}(x, \bar{\pi}(q_0, \mathbf{w}))| = 1$ because every action is lenght-preserving, thus $y = \bar{\lambda}(x, \bar{\pi}(q_0, \mathbf{w})) \in \mathbf{X}$, so $f(\mathbf{v}) = f(\mathbf{w}x) = f(\mathbf{w})y$, hence (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 equal to f. We define $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle := \langle \mathbf{X}, \mathbf{X}^*, \pi, \lambda \rangle$ ($\mathcal{Q} = \mathbf{X}^*$ is infinite) with $\pi(\mathbf{q}, x) := \mathbf{q}x$ and $\lambda(\mathbf{q}, x) := f(\mathbf{q}x) - f(\mathbf{q})$.

First we show that the output function λ is well defined, i.e., the subtraction $f(\mathbf{q}x) - f(\mathbf{q})$ is well defined. Because f is a tree-endomorphism, $f(\mathbf{q}x)$ is a child of $f(\mathbf{q})$. Now we 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 2.6. *If f is a tree-endomorphism on $\mathbf{X}^*$, then $f(\mathbf{X}^n) \subseteq \mathbf{X}^n$. In particular, if f is a tree-automorphism, then $f(\mathbf{X}^n) = \mathbf{X}^n$, i.e., it is a permutation on $\mathbf{X}^n$.*

Proof. It follows from Proposition 1.16 and Proposition 2.5. The second point arises from the bijectivity of the f tree-automorphism. □

Proposition 2.6 provides a graph persepective on the lenght-preserving condition of actions of automata.

Proposition 2.7. *Let $\mathbf{vw} \in \mathbf{X}^*$ and g a tree-endomorphism. Then $g(\mathbf{v})$ is a prefix of $g(\mathbf{vw})$.*

Proof. We prove it by induction on $|\mathbf{w}| = n$.

Case $n = 0$: We have that $g(\mathbf{vw}) = g(\mathbf{v})$, which is a prefix of itself.

Case $n \Rightarrow n + 1$: Let us suppose $g(\mathbf{v})$ is a prefix of $g(\mathbf{vw})$ for every $\mathbf{w} \in \mathbf{X}^n$. We have that $g(\mathbf{vw}x) = g(\mathbf{vw})y$ for some $y \in \mathbf{X}$. Since $g(\mathbf{v})$ is a prefix of $g(\mathbf{vw})$ which is a prefix of $g(\mathbf{vw})y = g(\mathbf{vw}x)$, we have that $g(\mathbf{v})$ is a prefix of $g(\mathbf{vw}x)$, and thus the thesis. □

Definition 2.8. 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:

$$g(\mathbf{vw}) = g(\mathbf{v})g|_\mathbf{v}(\mathbf{w}). \tag{7}$$

Remark 2.2. The Equation (7) is well defined because, as proved in Proposition 2.7, $g(\mathbf{v})$ is a prefix of $g(\mathbf{vw})$.

Proposition 2.9. *Let g,$\mathbf{v}$ and $g|_\mathbf{v}$ be as in Definition 2.8, then $g|_\mathbf{v}(\mathbf{w}) = g(\mathbf{vw}) - g(\mathbf{v})$. Furthermore $g|_\mathbf{v}$ is a tree-endomorphism.*

Proof. The first point is a direct consequence of Proposition 2.7. 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 $x \in \mathbf{X}$, then $g|_\mathbf{v}(\mathbf{w}x) = g(\mathbf{vw}x) - g(\mathbf{v}) = g(\mathbf{vw})y - g(\mathbf{v})$ for some $y \in \mathbf{X}$ (because g is a tree-endomorphism), and finally $g(\mathbf{vw})y - g(\mathbf{v}) = (g(\mathbf{vw}) - g(\mathbf{v}))y = g|_\mathbf{v}(\mathbf{w})y$, and therefore $g|_\mathbf{v}$ is a tree-endomorphism. □

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

Proposition 2.10. *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 $g(\mathbf{vw}) := \bar{\lambda}_{q_0}(\mathbf{vw}) = \bar{\lambda}_{q_0}(\mathbf{v})\bar{\lambda}_{\bar{\pi}(\mathbf{v}, q_0)}(\mathbf{w}) = g(\mathbf{v})\bar{\lambda}_{\bar{\pi}(\mathbf{v}, q_0)}(\mathbf{w})$, consequently $g|_\mathbf{v} = \bar{\lambda}_{\bar{\pi}(\mathbf{v}, q_0)}$. □

2.2. **Groups generated by automata.**

Definition 2.11. Given an initial automaton $\mathcal{A}_{q_0}$, a state q is called *accessible* if there exists a word $\mathbf{w} \in \mathbf{X}$ such that $\bar{\pi}(\mathbf{w}, q_0) = q$. We can also say that q *is accessible with respect to* q_0 or *from* q_0.

This means that in the Moore diagram there is a path from q_0 to q.

Definition 2.12. 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 2.13. *Given an automaton $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$ and a state $q_0 \in \mathcal{Q}$, $\bar{\lambda}_{q_0}$ is an invertible function if and only if for every accessible state $q \in \mathcal{Q}$ (respect to q_0) the function $\lambda_q : \mathbf{X} \longrightarrow \mathbf{X}$ 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 $\bar{\pi}_{q_0}(\mathbf{w}) = q$. 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 $\bigcup_{n \in \mathbb{N} \cup \{0\}} \mathbf{X}^n = \mathbf{X}^*$.

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

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

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

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

Proposition 2.14. *The set $\mathcal{GA}(\mathbf{X})$ of all bijective synchronous automatic transformations on an alphabet $\mathbf{X}$ is a group with respect to the composition operation. Furthermore, it is isomorphic to $\mathcal{AUT}_{tree}(\mathbf{X}^*)$, the group of all tree-automorphism of $\mathbf{X}^*$.*

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

Definition 2.15. 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 $q_0 \in \mathcal{Q}$.

Remark 2.3. We introduce a different notation for Moore diagrams. Let q, p be vertices of a Moore diagram and $q \longrightarrow p$ an edge between them. Recalling Definition 1.2, this means there exists $x, y \in \mathbf{X}$ such that $\pi(x, q) = p$ and $\lambda(x, q) = y$. Then we label the arrow from q to p by the letter x and the vertex p by the function $\lambda(\cdot, q) : \mathbf{X} \longrightarrow \mathbf{X}$. See Figure 6 for an example.

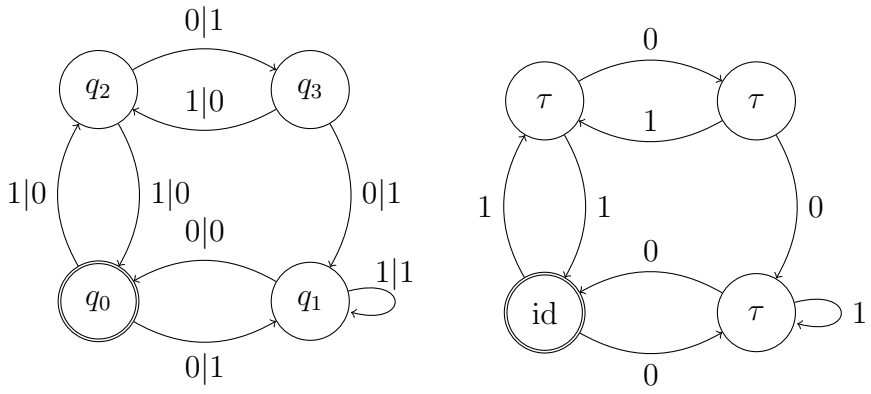

FIGURE 6. An example of the same initial automaton represented in two different ways. In the right figure $\tau, \mathrm{id} \in \mathcal{S}_2 := \mathcal{S}(\{0, 1\})$, where, τ inverts the elements in $\{0, 1\}$ and id leaves them unchanged.

Definition 2.16. Given an automaton $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$ we can define $|\mathcal{Q}|$ initial automata, which define $|\mathcal{Q}|$ actions $\bar{\lambda}_q$ on $\mathbf{X}^*$ inside $\mathcal{FSA}(\mathbf{X})$. By the *semigroup generated by* $\mathcal{A}$ we mean the subsemigroup $H(\mathcal{A})$ of $\mathcal{FSA}(\mathbf{X})$ generated by all the actions $\bar{\lambda}_q$ with $q \in \mathcal{Q}$:

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

where, for a set S, $\langle S \rangle$ means the semigroup generated by the elements of S, i.e., the smallest subsemigroup of $\mathcal{FSA}(\mathbf{X})$ which contains all the elements of S.

Remark 2.4. If $\mathcal{A}$ is invertible then $H(\mathcal{A})$ is the *group generated by* $\mathcal{A}$, and we have that $H(\mathcal{A}) \subseteq \mathcal{GA}(\mathbf{X})$.

Remark 2.5. From now on by an automaton and by an initial automaton we mean an *invertible automaton* and an *invertible initial automaton*, respectively.

3. Semidirect and wreath products

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

Definition 3.1. Let $\circ$ be the composition of functions. We define $f \cdot g := g \circ f$.

3.1. Actions.

Definition 3.2. Given a group G and a set X, we call a *left G-action on X* or an *left action of G on X* an homomorphism of groups $T_l : G \longrightarrow (\mathcal{S}(X), \circ)$. We can also say that G *acts on X from the left by T_l*. We say that G acts on X from the right by T_r if there exists an homomorphism $T_r : G \longrightarrow (\mathcal{S}(X), \cdot)$.

Proposition 3.3. *Let us take a group $(G, *)$ and a set X. Then G is acting on X from the left if and only if exist a function $\tau_l : G \times X \longrightarrow X$ such that:*

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

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

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

Proof. We prove just the case of left action.

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

($\Rightarrow$) This is similar.

□

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

Example 3.4. The symmetric group $(\mathcal{S}(X), \circ)$ on a set X acts on X from the left, in fact we can define $T_l(\sigma)(x) = \sigma x := \sigma(x) \quad \forall \sigma \in \mathcal{S}(X)$ and $\forall x \in X$. Analogously we can define $T_r(\sigma)(x) = x\sigma := \sigma(x)$. Let X be such that $|X| > 3$, then $\mathcal{S}(X)$ is not abelian. Let us take $\sigma, \eta \in \mathcal{S}(X)$ such that $\sigma \circ \eta \neq \eta \circ \sigma$. Then there exists x such that $x\sigma\eta \neq \sigma\eta x$. This shows that $\tau_l(\sigma\eta, x) \neq \tau_r(x, \sigma\eta)$. ♢

Example 3.5 (translations)**.** Let A be an affine space, and let V be a vector space associated to it. Let $T_l : V \longrightarrow \mathcal{S}(A)$ be a function such that $T_l(\mathbf{v})(P) := P + \mathbf{v}$, where $P + \mathbf{v}$ is the translation of $P \in A$ by the vector $\mathbf{v} \in V$. Then it is easy to see that T_l is a left action of V on A.

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

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

This happens because V is abelian. ♢

Example 3.6 (synchronous automatic bijective transformations)**.** The group of all synchronous automatic bijective transformations $(\mathcal{GA}(\mathbf{X}), \circ)$ acts from the left on $\mathbf{X}^*$:

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

♢

Definition 3.7. Let G be a group acting from the right on X by $T_r : G \longrightarrow (\mathcal{S}(X), \cdot)$. 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*.

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

Proposition 3.8. *(1) A group* G *acts faithfully on a set* X *from the left if and only if for every* h *and* g *in* G *there exists* x *in* X *such that* $gx \neq hx$.

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

Proof. It follows directly from Definition 3.7 and Proposition 3.3. □

Remark 3.1. If B is a group, we can consider (B, B) as a right permutation group, with B acting on itself by right multiplication.

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

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

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

Remark 3.2. Note that $\mathcal{AUT}(N) \subset \mathcal{S}(N)$.

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

Definition 3.9. Let H, N be groups, with operations $*_H$ and $*_N$, where H acts on N *from the right* by $\varphi : H \longrightarrow (\mathcal{AUT}(N), \cdot)$. On $H \times N$ we define the following operation:

$$\star_\varphi : ((h_2, n_2), (h_1, n_1)) \longmapsto (\; h_2 *_H h_1 \;,\; \varphi(h_1)(n_2) *_N n_1) = (\; h_2h_1 \;,\; (n_2h_1) *_N n_1)$$

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

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

Proposition 3.10. *The semidirect product* $H \ltimes_\varphi N$ *is a group, where the identity element is* $(1_H, 1_N)$ *and* $(h^{-1}, \varphi(h^{-1}))(n^{-1}))$ *is the inverse for* (h, n).

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

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

Example 3.11 (dihedral groups)**.** Given a geometrical object A one can consider the set $\mathbf{Sym}(A)$ of all bijective geometrical transformations which leave A unchanged. By the definition, the composition of two such transformations also leaves A unchanged. The set $\mathbf{Sym}(A)$ forms a group called the group of symmetries of A.

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

It turns out that the group $\mathcal{D}_n$ is isomorphic to the semidirect product $\mathbb{Z}_2 \ltimes_\varphi \mathbb{Z}_n$, where the action of $\mathbb{Z}_2$ on $\mathbb{Z}_n$ is given by $\varphi(0)(z) := \mathrm{id}_{\mathbb{Z}_n}(z) = z$ and

$\varphi(1)(z) := -z \pmod n$. For example, $\mathbb{Z}_2 \ltimes_\varphi \mathbb{Z}_n \ni (h_2, n_2) * (0, n_1) = (h_2 + 0, n_1 + n_2)$ and $(h_2, n_2) * (1, n_1) = (h_2, n_1 - n_2)$. We can notice that $(h, k) = (h, 0) * (0, k)$. The transformation $(0, k)$ is necessarily always a rotation, while $(h, 0)$ is the identity or the reflection through the central axis, depending if $h = 0$ or $h = 1$. In other words, if we have $(h, k) \in \mathbb{Z}_2 \ltimes_\varphi \mathbb{Z}_n$, h encodes the reflection part of (h, k) and k the rotation part of (h, k). ♢

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

Definition 3.12. Given a group A and a 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:

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

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

Remark 3.3. 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 $B \ltimes_\Phi A^Y$. Let us formalise this:

Proposition 3.13. *Let (Y, B) be a right permutation group with action given by $(y, \beta) \mapsto y\beta$ and let A be a group. Then $\Phi : B \longrightarrow (\mathcal{S}(A^Y), \cdot)$ 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.

A similar statement holds also if A^Y is replaced with $A^{(Y)}$.

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

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

(1) We must prove that $\Phi(\beta)$ is bijective for every $\beta \in B$. Let us first prove the injectivity. Let $\overline{a}, \overline{x} \in A^Y$ and let us consider $\Phi(\beta)(\overline{a}) = (a_{y\beta})_{y \in Y} = (x_{y\beta})_{y \in Y} = \Phi(\beta)(\overline{x})$. Then $a_y = a_{y\beta\beta^{-1}} = x_{y\beta\beta^{-1}} = x_y$ for every $y \in Y$, and so $\overline{a} = \overline{x}$, hence $\Phi(\beta)$ is injective. The surjectivity is very simple: if we have $(a_y)_{y \in Y}$, the element $(a_{y\beta^{-1}})_{y \in Y}$ is its inverse image.

(2) We now prove that $\Phi(B) \subseteq \mathcal{AUT}(A^Y)$, i.e., that 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 faithful, i.e., that if $\Phi_\beta = \Phi_\theta$ then $\beta = \theta$. Let us suppose that $\Phi_\beta = \Phi_\theta$. We have, for every $(a_y)_{y \in Y} \in A^Y$, that $(a_{y\beta})_{y \in Y} = \Phi_\beta((a_y)_{y \in Y}) = \Phi_\theta((a_y)_{y \in Y}) = (a_{y\theta})_{y \in Y}$. It follows that $y\beta = y\theta$ for every $y \in Y$. Since the action of B on Y, given by $(y, \beta) \mapsto y\beta$, is faithful, we have that $\beta = \theta$. The proof is finished.

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

Definition 3.14. Let (Y, B) be a right permutation group and let A be a group. Suppose that we have a right action $\Phi : B \longrightarrow (\mathcal{AUT}(A^Y), \cdot)$ defined as in Proposition 3.13.

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

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

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

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

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

Remark 3.4. Let (B, Y), A, $B \wr A = B \ltimes_\Phi A^Y$ be as previously defined, and let $Y = \{y_1, \ldots, y_k\}$. Then $\overline{a} \in A^Y$ is uniquely written as $(a_1, \ldots, a_k)$. We denote $(\beta, \overline{a}) \in B \wr A$ by $\beta(a_1, \ldots, a_k)$. With this convention, given $\beta(a_1, \ldots, a_k)$ and $\theta(g_1, \ldots, g_k)$ in $B \wr A$, the multiplication rule $*_\Phi$ becomes:

$$\begin{aligned}\beta(a_1, \ldots, a_k) *_\Phi \theta(g_1, \ldots, g_k) &= \beta\theta((a_{1\theta}, \ldots, a_{k\theta}) *_{A^Y} (g_1, \ldots, g_k)) \\ &= \beta\theta(a_{1\theta} g_1, \ldots, a_{k\theta} g_k)\end{aligned}$$

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

$$\beta^{-1}((g_{1\beta^{-1}})^{-1}, \ldots, (g_{k\beta^{-1}})^{-1}).$$

3.4. **Applications to automata.** We will see that the wreath product construction arises in the context of automata.

Remark 3.5. From now on the operation of composition of words will be denoted by the dot ".".

Proposition 3.15. *Let* $\mathbf{X}$ *be an alphabet. Denote by* $\mathcal{AUT}_{tree}(\mathbf{X}^*)$ *the group of tree-automorphisms on* $\mathbf{X}^*$. *Then there exists a left* $\mathcal{AUT}_{tree}(\mathbf{X}^*)$*-action* T *on* $\mathbf{X}$ *as a set (*$T : (\mathcal{AUT}_{tree}(\mathbf{X}^*), \circ) \longrightarrow (\mathcal{S}(\mathbf{X}), \circ)$*) defined by* $T(f)(x) := f(x)$.

Proof. The function f is a tree-automorphism, so by Proposition 2.6, $f(\mathbf{X}) = (\mathbf{X})$, therefore $T(f)$ is a bijection on the alphabet $\mathbf{X}$. Furthermore we have that $T(f \circ g)(x) = (f \circ g)(x) = f(g(x)) = T(f)(g(x)) = (T(f) \circ T(g))(x)$, consequently $T(f \circ g) = T(f) \circ T(g)$, and so T is an homomorphism. □

We now take the right permutation group $(\mathbf{X}, \mathcal{S}(\mathbf{X}))$ and the group $\mathcal{AUT}_{tree}(\mathbf{X}^*)$, where both $\mathcal{S}(\mathbf{X})$ and $\mathcal{AUT}(\mathbf{X}^*)$ are provided with the composition of functions denoted by $\circ$ as their operation. We have so a right action of $\mathcal{S}(\mathbf{X})$ on $\mathcal{AUT}_{tree}(\mathbf{X}^*)^{\mathbf{X}}$

defined by $\Phi(\sigma)(f_{x_1},\dots,f_{x_k})=(f_{x_1\sigma},\dots,f_{x_k\sigma})$, where $x_i\sigma$ is the element $\sigma(x_i)\in\mathbf{X}$, and f_{x_i} is the restriction of f in x_i as defined in (7).

Proposition 3.16. *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 from the right on $\mathcal{AUT}_{tree}(\mathbf{X}^*)^{\mathbf{X}}$ by $\Phi(\sigma)(f_{x_1},\dots,f_{x_k})=(f_{x_1\sigma},\dots,f_{x_k\sigma})$. Let us define $\psi:(\mathcal{AUT}_{tree}(\mathbf{X}^*),\circ)\longrightarrow(\mathcal{S}(\mathbf{X}),\circ)\wr(\mathcal{AUT}_{tree}(\mathbf{X}^*),\circ)=\mathcal{S}(\mathbf{X})\ltimes_\Phi\mathcal{AUT}_{tree}(\mathbf{X}^*)^{\mathbf{X}}$ as*

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

where $f|_{x_k}$ is the restriction of f in x_k as defined in 2.8. 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:

$$\begin{aligned}\psi(f)\psi(g)&=T(f)(f|_{x_1},\dots,f|_{x_k})*_\Phi T(g)(g|_{x_1},\dots,g|_{x_k})\\&=T(f)T(g)(f|_{x_1T(g)}g|_{x_1},\dots\ f|_{x_kT(g)}g|_{x_k})\\&=T(fg)((fg)|_{x_1},\dots\ (fg)|_{x_k})\\&=\psi(fg)\end{aligned}$$

- We prove that ψ is injective. If $T(f)(f|_{x_1},\dots,f|_{x_k})=\psi(f)=\psi(g)=T(g)(g|_{x_1},\dots,g|_{x_k})$ we have that $f(x)=T(f)(x)=T(g)(x)=g(x)$ for every $x\in\mathbf{X}$. And since $f|_{x_i}=g|_{x_i}$ for every $x_i\in\mathbf{X}$, it follows that $f(x\mathbf{v})=f(x)f|_x(\mathbf{v})=g(x)g|_x(\mathbf{v})=g(x\mathbf{v})$. Consequently $f=g$, and ψ is one-to-one.
- We prove that ψ is 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 Proposition 2.14 $\mathcal{GA}(\mathbf{X})$, 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 vice versa. This leads to the following result:

Proposition 3.17. *The group $\mathcal{S}(\mathbf{X})\wr\mathcal{AUT}_{tree}(\mathbf{X}^*)$ acts* faithfully *on $\mathbf{X}^*$ as a set from the left by:*

$$\beta(a_{x_1},\dots,a_{x_k})(w_1w_2\dots w_n)=\beta(w_1).a_{w_1}(w_2\dots w_n)$$

Proof. Let ψ be the isomorphism from Proposition 3.16. The action of f coincides with the action of $\psi(f)$ for any $f\in\mathcal{AUT}_{tree}(\mathbf{X}^*)$. Thus the action of $\psi(f)$ is faithful for any $f\in\mathcal{AUT}_{tree}(\mathbf{X}^*)$. The statement follows. □

Proposition 3.18. *Let $\mathcal{A}=\langle\mathbf{X},\mathcal{Q},\pi,\lambda\rangle$ be an automaton such that $\mathcal{Q}=\{q_1,\dots,q_n\}$ and $\mathbf{X}=\{x_1,\dots,x_k\}$. Then the set of all the actions $\bar{\lambda}_{q_l}\in\mathcal{AUT}_{tree}(\mathbf{X}^*)$*

defined by $\mathcal{A}$ can be described with n recurrent formulas

$$
\begin{aligned}
f_{q_1} &= \beta_{q_1}(h_{x_1,q_1}, \ldots, h_{x_k,q_1}),\\
f_{q_2} &= \beta_{q_2}(h_{x_1,q_2}, \ldots, h_{x_k,q_2}),\\
&\ldots\\
f_{q_n} &= \beta_{q_n}(h_{x_1,q_n}, \ldots, h_{x_k,q_n}),
\end{aligned}
\tag{8}
$$

where each h_{x_i,q_j} is equal to some f_{q_l} and each β_{q_j} is a permutation of the alphabet. Conversely, Let S be a system of type (8), where each h_{x_i,q_j} is equal to some f_{q_l} and each β_j is a permutation of the alphabet. Then S defines uniquely an automaton $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda\rangle$ such that $\bar{\lambda}_{q_l} = f_{q_l}$ for every $q_l \in \mathcal{Q}$.

Proof. Let $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda\rangle$ be an automaton. Each initial automaton $\mathcal{A}_{q_l}$ defines a transformation $\bar{\lambda}_{q_l}$ in $\mathcal{AUT}_{tree}(\mathbf{X}^*)$. By Proposition 2.10 we have that the restriction $\bar{\lambda}_{q_l}|_x$ is equal to $\bar{\lambda}_{\pi(x,q_l)} = \bar{\lambda}_p$ for some $p \in \mathcal{Q}$. Therefore $\psi(\bar{\lambda}_{q_l}) = T(\bar{\lambda}_{q_l})(\bar{\lambda}_{\pi(x_1,q_l)}, \ldots, \bar{\lambda}_{\pi(x_k,q_l)}) = \lambda_{q_l}(\bar{\lambda}_{\pi(x_1,q_l)}, \ldots, \bar{\lambda}_{\pi(x_k,q_l)})$, where ψ is defined as in Proposition 3.16 and λ_{q_l} is a permutation of $\mathbf{X}$ because $\mathcal{A}$ is invertible. Hence we obtain:

$$
\begin{aligned}
\bar{\lambda}_{q_1} &= \lambda_{q_1}(\bar{\lambda}_{\pi(x_1,q_1)}, \ldots, \bar{\lambda}_{\pi(x_n,q_1)}),\\
\bar{\lambda}_{q_2} &= \lambda_{q_2}(\bar{\lambda}_{\pi(x_1,q_2)}, \ldots, \bar{\lambda}_{\pi(x_n,q_2)}),\\
&\ldots\\
\bar{\lambda}_{q_n} &= \lambda_{q_n}(\bar{\lambda}_{\pi(x_1,q_n)}, \ldots, \bar{\lambda}_{\pi(x_n,q_n)}),
\end{aligned}
\tag{9}
$$

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

From the converse let us take a system S of the type (8). We have that each h_{x_i,q_j} is equal to some f_{q_l}. Let us define:

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

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

4. The classification theorem

In this section we present a result discovered by Grigorchuk and Zuk in [6], which describes all groups generated by 2-state automata on a 2-letter-alphabet. Our demonstration here follows [5]. First we introduce some of the objects that arise in the formulation and in the proof of the classification theorem.

4.1. **The infinite dihedral group.**

We have seen that in the finite case the dihedral group $\mathbb{Z}_2 \ltimes_\varphi \mathbb{Z}_n$ (3.11) is given as the simmetry group of the regular polygon with n sides. We now generalise this.

Definition 4.1. The group $\mathbb{Z}_2 \ltimes_\varphi \mathbb{Z}$ is called the *infinite dihedral group* and is denoted by $\mathcal{D}_\infty$.

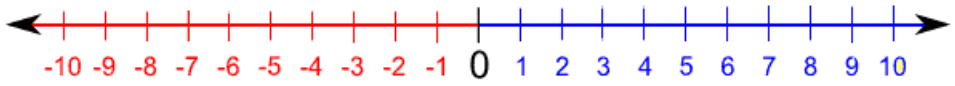

FIGURE 7. The line of integers (image taken from [13]).

We think of $\mathbb{Z}$ as of the infinite line of integers.

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

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

Definition 4.2. The *lamplighter group* $\mathcal{L}$ is the restricted wreath product $\mathbb{Z} \wr \mathbb{Z}_2 = \mathbb{Z} \ltimes \mathbb{Z}_2^{(\mathbb{Z})}$.

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

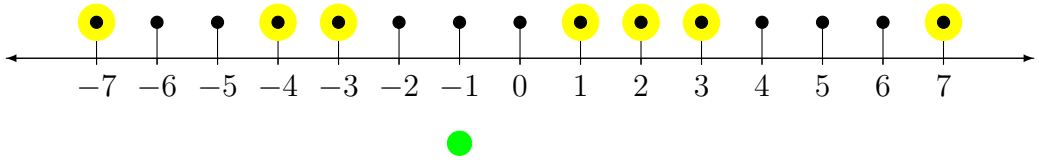

FIGURE 8. A representation of an *element* $(-1, (h_i)_{i\in\mathbb{Z}})$ in $\mathcal{L}$. The green circle represent the coordinate -1 of the lamplighter, while the yellow circles represent the lit on lampions at positions $\{-7, -4, -3, 1, 2, 3, 7\}$, i.e., the position i for which $h_i \neq 0_{\mathbb{Z}_2}$.

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

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

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

4.3. **The adding machine.**

Definition 4.3. Let $\mathbf{X} = \{0, 1\}$. The *adding machine* is the synchronous automatic transformation $f = \tau(\mathrm{id}_{\mathcal{GA}(\mathbf{X})}, f) : \mathbf{X}^* \longrightarrow \mathbf{X}^*$, where τ is the transposition of $\mathcal{S}(\mathbf{X})$.

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

$$\begin{aligned} f(0y_2 \dots y_n) &= \tau(0).\,\mathrm{id}_{\mathcal{GA}(\mathbf{X})}(y_2 \dots y_n) = 1y_2 \dots y_n \\ f(1y_2 \dots y_n) &= \tau(1).f(y_2 \dots y_n) = 0.f(y_2 \dots y_n) \end{aligned} \tag{10}$$

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

$$t_n(y_1 \dots y_k \dots y_n) = y_1 + y_2 2 + \dots + y_k 2^{k-1} + \dots + y_n 2^{n-1}. \tag{11}$$

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

The equations (10) tell us that if $x_1 \dots x_k \dots x_n = \mathbf{w_1} x_k \mathbf{w_2} = \mathbf{w_1} 0 \mathbf{w_2}$ is a sequence, where $\mathbf{w_1}$ is a sequence of 1s, while at position k there is the first element $x_k = 0$, then $f(\mathbf{w_1} x_k \mathbf{w_2}) = f(\mathbf{w_1} 0 \mathbf{w_2}) = \mathbf{v_1}.f(0\mathbf{w_2}) = \mathbf{v_1}.\tau(0).\,\mathrm{id}(\mathbf{w_2}) = \mathbf{v_1} 1 \mathbf{w_2}$, where $\mathbf{v_1}$ is a sequence of 0s. Then (11) yields:

$$
\begin{aligned}
&(f \circ t_n^{-1})\,(t_n(x_1 \dots x_k \dots x_n)) = \\
&= (f \circ t_n^{-1})\,(x_1 + x_2 2 + \dots + x_{k-1} 2^{k-2} + x_k 2^{k-1} + x_{k+1} 2^k \dots + x_n 2^{n-1}) \\
&= (f \circ t_n^{-1})\,(1 + 1 \cdot 2 + \dots + 1 \cdot 2^{k-2} + 0 \cdot 2^{k-1} + x_{k+1} 2^k \dots + x_n 2^{n-1}) \\
&= f(1 \dots 10 x_{k+1} \dots x_n) = 0 \dots 0.f(0 x_{k+1} \dots x_n) = 0 \dots 0.\tau(0).\,\mathrm{id}(x_{k+1} \dots x_n) \\
&= t_n^{-1}(0 + 0 \cdot 2 + \dots + 0 \cdot 2^{k-2} + 1 \cdot 2^{k-1} + \mathrm{id}(x_{k+1} 2^k \dots + x_n 2^{n-1})) \\
&= t_n^{-1}(0 + 0 \cdot 2 + \dots + 0 \cdot 2^{k-2} + 1 \cdot 2^{k-1} + x_{k+1} 2^k \dots + x_n 2^{n-1}) \\
&= t_n^{-1}(t_n(x_1 \dots x_k \dots x_n) + 1).
\end{aligned}
$$

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

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

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

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

Definition 4.4. 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 4.5. A synchronous transformation $s : \mathbf{X}^* \longrightarrow \mathbf{X}^*$ is called *spherically transitive* if $\langle s \rangle$ acts transitively on $\mathbf{X}^n$ for each n.

Proposition 4.6. *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. □

Proposition 4.7. *Let f be the adding machine. Then $\langle f \rangle$ is spherically transitive and isomorphic to $\mathbb{Z}$.*

Proof. Let $\mathbf{y} = y_1 y_2 \dots y_n$, $\mathbf{x} = x_1 x_2 \dots x_n$ be two sequences in $\mathbf{X}^n$. As in (11) let us consider $t_n(\mathbf{y})$ and $t_n(\mathbf{x})$ in $\mathbb{Z}_{2^n}$. We define $m \in \mathbb{N} \cup \{0\}$ such that $m = t_n(\mathbf{y}) - t(\mathbf{x}) \pmod{2^n}$. Let us consider $f^m \in \langle f \rangle$. Then we have that:

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

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

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

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

We now proceed with the formulation of the theorem.

4.4. **The theorem.**

Theorem 4.8. *Let $\mathcal{A} = \langle \mathbf{X}, \mathcal{Q}, \pi, \lambda \rangle$ be an automaton. Let $\mathbf{X} = \{0, 1\}$ and $|\mathcal{Q}| = 2$. Then the group generated by $\mathcal{A}$ is isomorphic to one of the following groups:*

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

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

4.5. **Define the cases.** To prove Theorem 4.8 we need to examine case by case groups defined by each possible automaton $\mathcal{A}$. Let us verify in how many ways we can define the functions 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 π 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 $\mathbf{X} = \{0, 1\}$, there are only two possible permutations: the transposition τ, 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 $\mathcal{A}$. Let $\{q, s\}$ be the states of the automaton $\mathcal{A}$. Consequently the group is generated by the actions $a = \bar{\lambda}_q$ and $b = \bar{\lambda}_s$. As we have seen in Proposition 3.18, we can define $\mathcal{A}$ by the recursive formulas:

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

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 $\sigma^0 := \mathrm{id}_{\mathcal{S}(2)}$, while $\sigma^1 := \tau$ is the other element of $\mathcal{S}_2$, the transposition.

Remark 4.1. Recall that $\mathcal{GA}(\mathbf{X})$ acts *faithfully* on $\mathbf{X}^*$, therefore two elements c, d of $\mathcal{GA}(\mathbf{X})$ act in the same way on $\mathbf{X}^*$ ($c\mathbf{w} = d\mathbf{w}$ for every $\mathbf{w}$) if and only if $c = d$.

Remark 4.2. From now on id will stand for the identity permutation of some group, usually $\mathcal{GA}(\mathbf{X})$ or $\mathcal{S}(\mathbf{X})$ and it will be clear from the context which specific group is being considered.

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

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

We need to consider just the cases where at least one between σ^{i_1} and σ^{i_2} acts non trivially on $\mathbf{X}$. We notice that each case:

$$\begin{aligned} a &= \tau(x_{11}, x_{12}), \\ b &= \sigma^{i_2}(x_{21}, x_{22}), \end{aligned} \tag{13}$$

generates the same group as the case:

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

This means that we can analyse just the $2^5 = 32$ cases (each non-fixed variable has two possible definitions) of the system (13) to see every possible group generated.

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

$$\sigma(c|_0, c|_1) \mapsto \sigma(c|_1, c|_0). \tag{14}$$

We have that:

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

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

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

generates a group isomorphic to the one generated by the case

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

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

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

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

Therefore $a^2 = \mathrm{id}(a^2, a^2) = \mathrm{id}_{\mathcal{GA}(\mathbf{X})}$. 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 $b = \mathrm{id}(b,b)$, $b = a^2$ 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 $b = a$ and $\langle a, b\rangle = \langle a\rangle = \{\mathrm{id}, a\}$. Since a has order 2, $\langle a\rangle$ is isomorphic to $\mathbb{Z}_2$.

(1.3) If $b = \tau(b,b)$, b acts on $\mathbf{X}^*$ changing each letter in a word to its opposite, so $b = a$ (recall Remark 4.1) and so $\langle a, b\rangle = \langle a\rangle$ is again isomorphic to $\mathbb{Z}_2$.

(1.4) If $b = \mathrm{id}(a,a)$, then b acts on $\mathbf{X}^*$ by changing each letter but the first one, so $b^2 = \mathrm{id}_{\mathcal{GA}(\mathbf{X})}$. Furthermore, ab acts by changing just the first letter, and the same does ba, so recalling Remark 4.1, since they acts in the same way on $\mathbf{X}^*$, $ba = ab$. It follows that $\langle a, b\rangle = \{\mathrm{id} = a^2, a, b, ab\}$ is isomorphic to $(\mathbb{Z}_2 \oplus \mathbb{Z}_2, +)$ by the maps

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

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

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

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

(1.6) If $b = \mathrm{id}(a,b)$ we obtain the infinite dihedral group. The proof is omitted.

(1.7) If $b = \tau(b,a)$, with the homomorphism f defined in (14), we have that $\langle a, b\rangle = \langle \tau(a,a), \tau(b,a)\rangle$ is isomorphic to the group of case (1.5) $\langle f(a), f(b)\rangle = \langle \tau(a,a), \tau(a,b)\rangle$.

(1.8) If $b = \mathrm{id}(b,a)$ the group $\langle a, b\rangle = \langle \tau(a,a), \mathrm{id}(b,a)\rangle$ is isomorphic to $\langle f(a), f(b)\rangle = \langle \tau(a,a), \mathrm{id}(a,b)\rangle$, i.e., case (1.6).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Let us call $b' := b^{-1}$ and $a' = a^{-1}$. We showed that we can study the group generated by a', b'. Let us take the generic element $x_1x_2 \dots x_k$ 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:

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

That is the case (2.7).

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

(3.1)-(3.2) The case $b = \tau(a, b)$ is analogous to (2.4), while the case $b = \tau(b, a)$ is symmetrical to (2.4), both leading to $\mathbb{Z}_2$.

(3.3)-(3.4) If $b = \tau(b, b)$ then $b = a = \tau(a, a)$, and we have the case (1.2) with $\mathbb{Z}_2$. If $b = \tau(a, a)$ we arrive to the same conclusion.

(3.5) If $b = (b, b)$ then $b = \mathrm{id}$ and $a = \tau(\mathrm{id}, \mathrm{id})$, so $\langle a \rangle = \{\mathrm{id}, a\}$ is isomorphic to $\mathbb{Z}_2$.

(3.6)-(3.7) These cases lead to the infinite dihedral group. The proof is omitted.

(3.8) If $b = \mathrm{id}(a, a)$, then:

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

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

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

□

Concluding remarks

In this thesis we have gone through just a part of the theory of automata. We considered just finite deterministic Mealy automata, but if instead the reader may want to explore a broader class of objects, [3] is a very good source where to start from. Otherwise for some more practical application of the theory there is the book [10]. The book [8] explores in the details the structures of Subsection 3.3.

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

For more examples of automata in connection to groups I recommend [2], where the complete classification of 3-state automata over a 2-letter-alphabet can be found. The book [9] is another very good source, and the article [12] shows some important 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 [4].

Acknowledgements

I would like to thank both my Supervisors prof. Alessandro Logar and izr. prof. Ganna Kudryavtseva, and in particular the latter one, for all the time she spent helping me and for her infinite patience with my clumsiness. Then I would like to thank prof. Valentina Beorchia and prof. Marko Petkovšek thanks to whom I could participate in this exchange program. Without them this would not have even started. I need to thank also prof. Sašo Strle, who managed to follow me and other tens of students in the completion of the bachelor thesis, and the administrative offices of Ljubljana and Trieste, which helped me with the bureaucracy. Remarkably important was the assistance of my dear friend and collegue Matej Jazbec, who corrected my slovenian translations. Finally I would like to thank my beloved ones, who managed to bear me during the last period.

References

[1] M.C. Bonanome, M.H. Dean, J.P Dean, *A sampling of remarkable groups*, in: Compact Textbooks in Mathematics (Birkhäuser), Springer Nature Switzerland AG, Cham, 2018.

[2] I. Bondarenko, R. Grigorchuk, R. Kravchenko, Y. Muntyan, V. Nekrashevych, D. Savchuk, Z. Sunic, *Classification of groups generated by 3-state automata over a 2-letter alphabet*, Algebra Discrete Math. **1** (2008).

[3] S. Eilenberg, *Automata, Language, and Machines*, Academic Press, New York, 1974.

[4] R.I. Grigorchuk, A. Machí, *An example of an indexed language of intermediate growth*, Theoretical Computer Science **215** (1999) 325–327.

[5] R.I. Grigorchuk, V.V. Nekrashevych, V.V. Sushchanskiix, *Automata, dynamical systems, and groups*, Proc. Steklov Inst. Math. **231** (2000) 128–203.

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

[7] V.A. Kaimanovich, A.M. Vershik, *Random walks on discrete groups: Boundary and entropy*, Ann. Probab. **11** (1983) 457–490.

[8] J.D.P. Meldrum, *Wreath products of groups and semigroups*, Chapman and Hall, Longman/Wiley, 1995.

[9] V.V. Nekrashevych, *Self-similar groups*, in: Mathematical Surveys and Monographs(Amer. Math. Soc.), Amer. Math. Soc., Providence, 2005.

[10] J. Rhodes, C.L. Nehaniv, M.W. Hirsch, *Applications of automata theory and algebra*, World Scientific Publishing Co. Pte. Ltd., Singapore, 2009.

[11] J.A. Siehler, *The finite lamplighter groups: A guided tour*, The College Mathematics Journal **43** (2012) 203–211.

[12] A. Zuk, *Automata groups*, Clay Math. Proc. **16** (2012) 165–196.

[13] https://www.math-only-math.com/images/integers-numbers-on-number-line.png