GROUPS OF AUTOMATA

CARLO LANZI LUCIANI

MENTOR: GANNA KUDRYAVTSEVA

Automata are a <u>MODEL OF COMPUTATION</u>:

INPUT
↓
Automaton $\xrightarrow{\text{defines}}$ $\boxed{\text{Initial Automaton}}$ $\xrightarrow{\text{defines}}$ Function(INPUT) = = OUTPUT
↓
OUTPUT

Aim

<u>1st part</u>:

(1) INPUT and OUTPUT

(2) Automata and their visualization

(3) Initial Automaton and "actions"

Then we will analise the functions in detail.

Finally: interesting examples

INPUT and OUTPUT

- X = finite set of symbols

  Ex] $X = \{0, 1\}$

- X^* = set of words of $X = \{x_1 \cdot \ldots \cdot x_n \mid x_i \in X, n \in \mathbb{N}\} =$

  $= \{$ finite strings of $X \}$

- $|w| = |x_1 \cdot \ldots \cdot x_n| := n =$ lenght of w

- ## Monoid Structure

  $\emptyset :=$ empty word $=$ identity respect to $\circ$

  $(x_1 \cdot \ldots x_n) \circ (y_1 \cdot \ldots \cdot y_m) = x_1 \cdot \ldots x_n y_1 \cdot \ldots y_m$

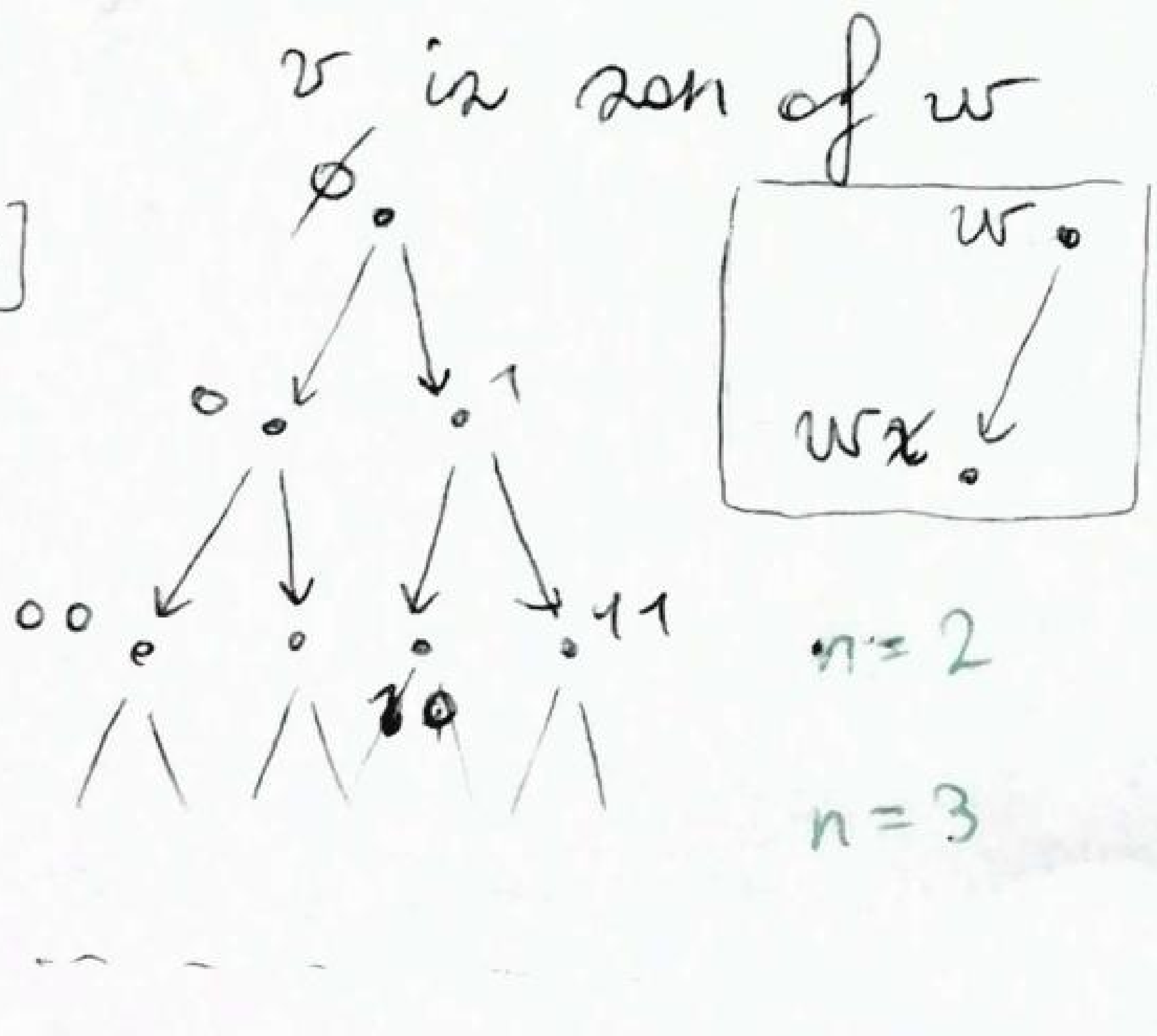
  Ex]: $\underbrace{001}\circ\underbrace{101} = \underbrace{001}\underbrace{101}$

- ## Tree Structure

  $\emptyset$ = root

  v is son of w whenever $v = wx$

Ex]



Observation:

$X^n = \{$words of lenght $n\}$

$=$ n-th level of X

AUTOMATA

DEF A SYNCHRONUS INVERTIBLE AUTOMATON $\mathcal{A}$ is a tuple $\mathcal{A} = (X, Q, \lambda, \pi)$ where

(1) X is a finite set, the INPUT and OUTPUT ALPHABET

(2) Q is a set, the SET OF STATES

(3) $\pi : Q \times X \longrightarrow Q$ is the TRANSITION FUNCTION

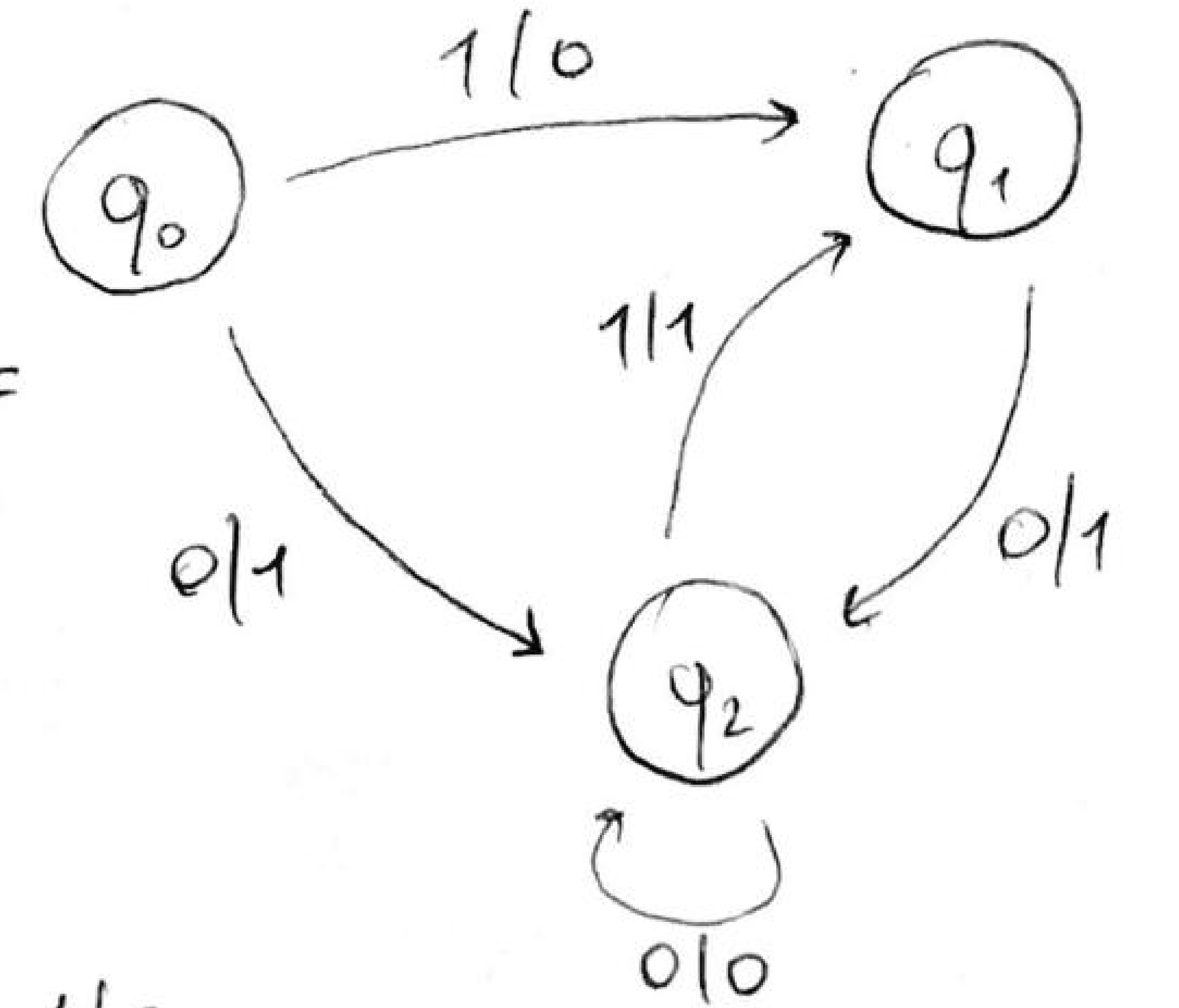
(4) $\lambda : Q \times X \longrightarrow X$ is a function such that

$\lambda(q; \cdot) : X \longrightarrow X$ is bijective ($\Rightarrow$ permutation), and it's called OUTPUT FUNCTION

[From now on AUTOMATON = SYNC. INV. AUTOMATON]

Example 1:

$\Gamma_1 :=$

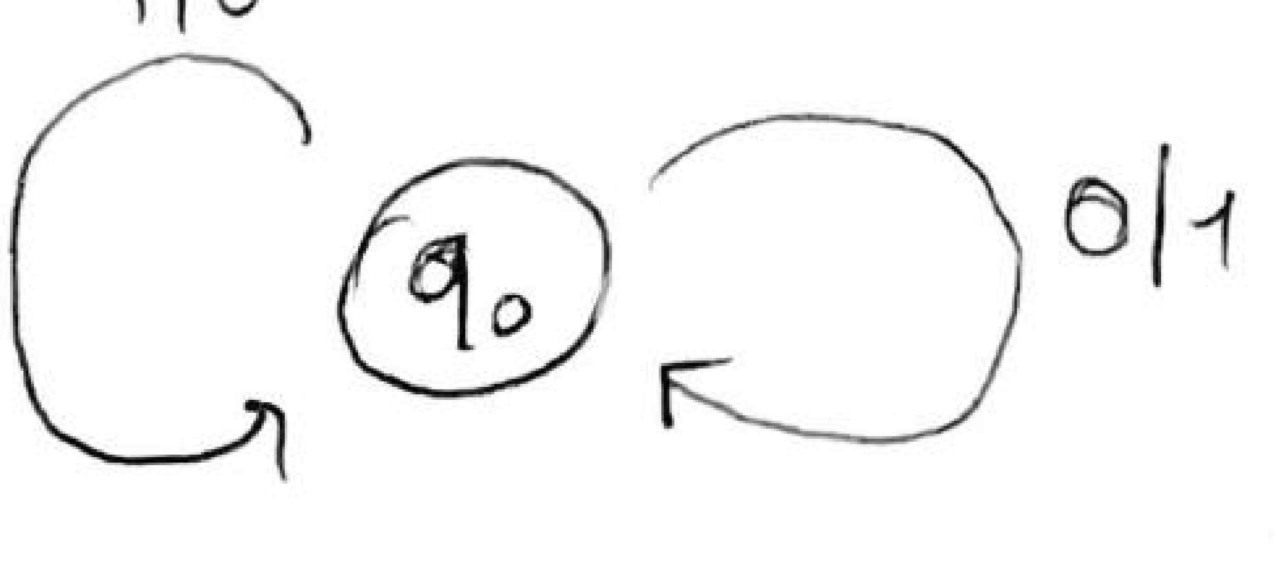


Notation: INPUT LETTER | OUTPUT LETTER

$X = \{0, 1\}$

Ex. 2

$\Gamma_2 :=$



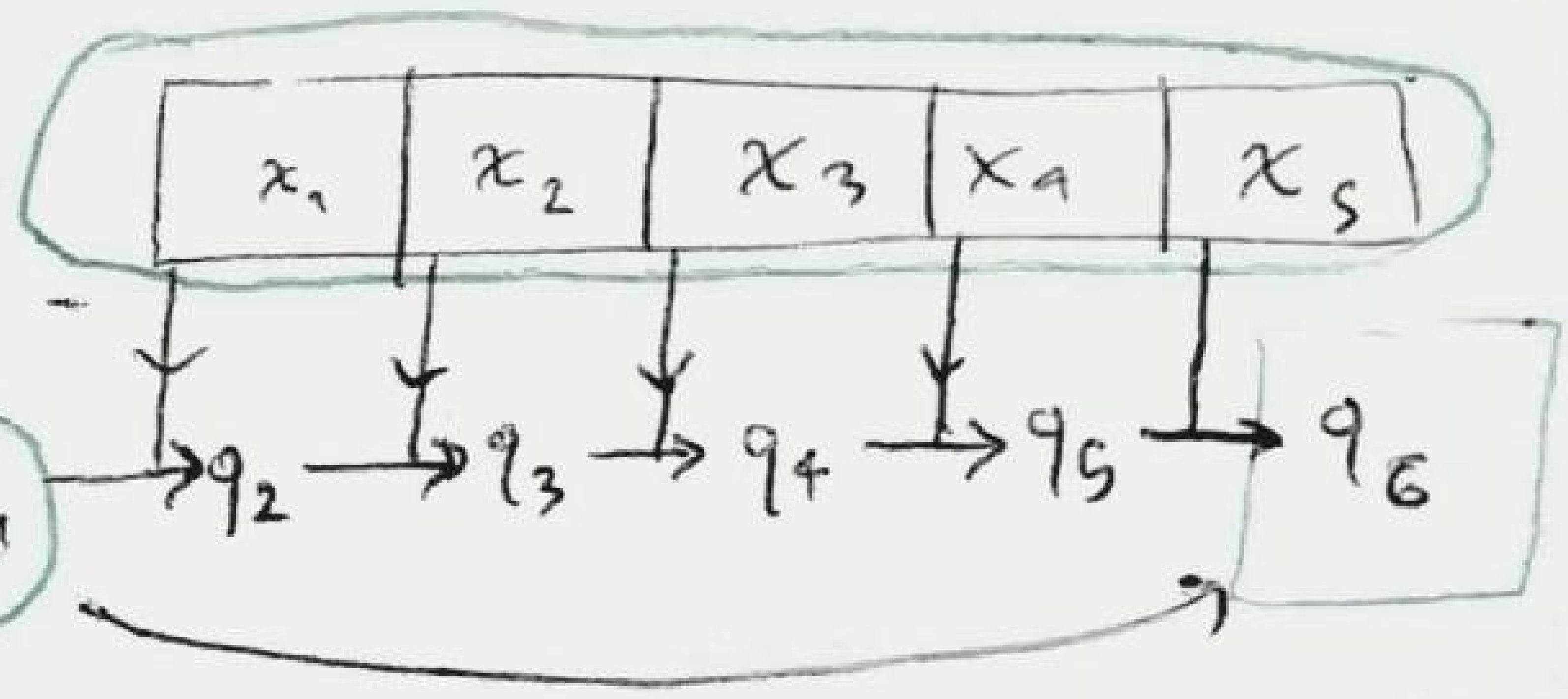
Extension of π and λ

$\pi(q, x) = q \qquad \pi : Q \times X \longrightarrow Q$

$\lambda(q, x) = y \qquad \lambda : Q \times X \longrightarrow X$

Recursive Extension:

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

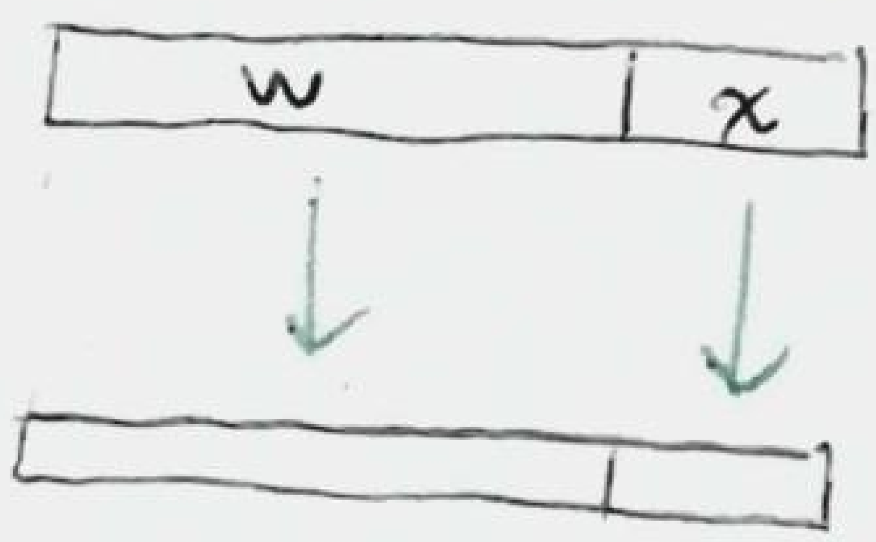


$$\begin{cases} \bar{\pi}(q, \emptyset) := q \\ \bar{\pi}(q, \underset{\substack{\cap \\ X^*}}{w} \cdot \underset{\substack{\cap \\ X}}{x}) := \bar{\pi}\left(\bar{\pi}(q, w), x\right) \end{cases}$$

$\boxed{Ex}$: page 2A

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

$$\begin{cases} \bar{\lambda}(q, \emptyset) := \emptyset \\ \bar{\lambda}(q, \underset{\substack{\cap \\ X^*}}{w} \cdot \underset{\substack{\cap \\ X}}{x}) := \underbrace{\bar{\lambda}(q, w)}_{\in X^*} \cdot \underbrace{\bar{\lambda}\left(\bar{\pi}(q, w), x\right)}_{\in X} \end{cases}$$



Notation: $\bar{\lambda}_q(w) := \bar{\lambda}(q, w)$

$\boxed{Ex}$: page 2A

DEF Given $\mathcal{A}$ automaton, $\mathcal{A}_{q_0}$, with fixed INITIAL ~~STATE~~ STATE q_0, is called INITIAL AUTOMATON

NOTE (1) $\mathcal{A}_{q_0}$ defines $\bar{\lambda}_{q_0} : X^* \longrightarrow X^*$, called the ACTION of $\mathcal{A}_{q_0}$

(2) λ_q is bijective (on X) $\Rightarrow \bar{\lambda}_q$ is bijective (on X^*)

Povzetek:

Ex: page 2A

Automaton $\mathcal{A}$ $\rightsquigarrow$ Initial Automaton $\mathcal{A}_{q_0}$ $\rightsquigarrow$ action $\bar{\lambda}_{q_0}$ $(X^* \longrightarrow X^*)$

Note $\forall \mathcal{A}$ we can define $|Q|$ different $\mathcal{A}_q$

Ex (1) Page 2A: (Γ_1) $\mathcal{A}$ $\rightsquigarrow$

$$\begin{cases} (\Gamma_1)_{q_0} \rightsquigarrow \bar{\lambda}_{q_0} \\ (\Gamma_1)_{q_1} \rightsquigarrow \bar{\lambda}_{q_1} \\ (\Gamma_2)_{q_2} \rightsquigarrow \bar{\lambda}_{q_2} \end{cases}$$

(2) $(\Gamma_2) \rightsquigarrow (\Gamma_2)_q \rightsquigarrow \bar{\lambda}_q$

DEF $f : X^* \longrightarrow X^*$ is <u>synchronous</u> <u>automatic</u> if is definable as the action of some initial automaton $\mathcal{A}_{q_0}$, i.d. (=to je) $f = \bar{\lambda}_{q_0}$.

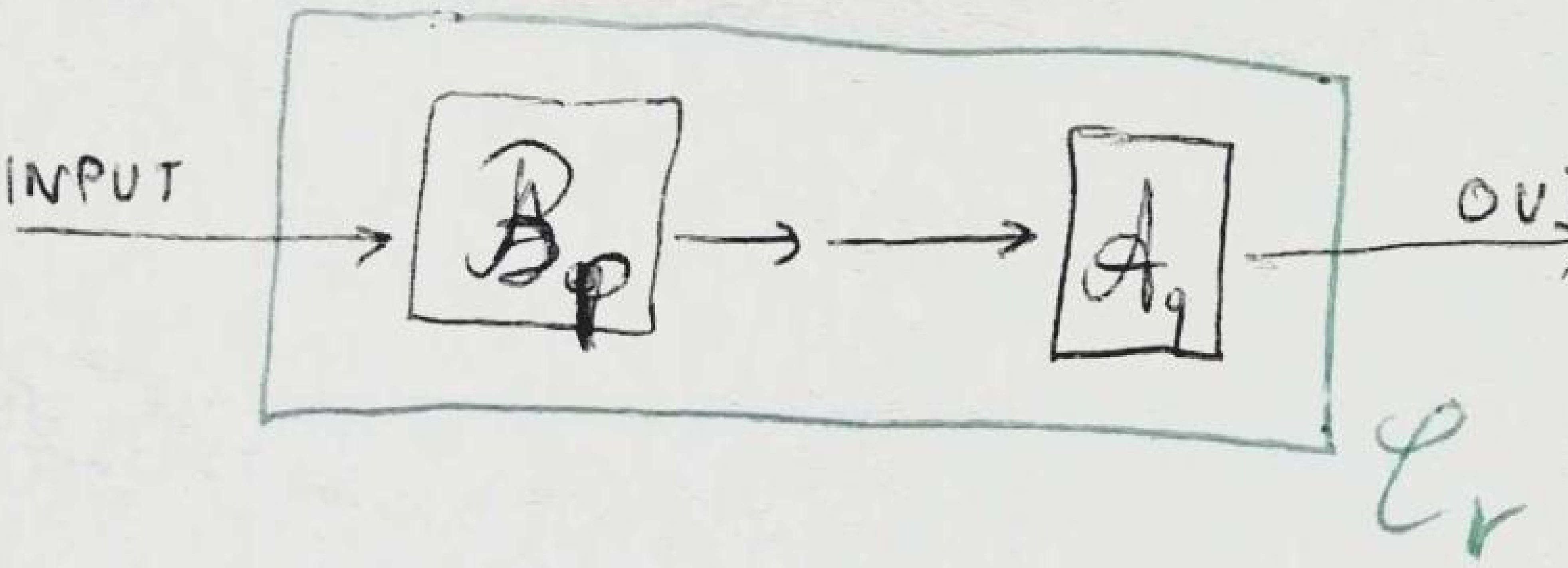
DEF $S := \{ f : X^* \to X^* \mid f \text{ is synchronous automatic} \}$

Note $f \in S \Rightarrow f = \bar{\lambda}_{q_0} \Rightarrow f$ is <u>bijective</u>

<u>We want to study S</u>

<u>Composition Lemma</u> Given $\mathcal{A}_q$ and $\mathcal{B}_p$, initial automata on X, $\exists\ \mathcal{C}_r$, initial automaton, such that:

$$\begin{pmatrix} \text{Action of} \\ \mathcal{C}_r \end{pmatrix} = \begin{pmatrix} \text{Action} \\ \text{of} \\ \mathcal{A}_q \end{pmatrix} \circ \begin{pmatrix} \text{Action} \\ \text{of} \\ \mathcal{B}_p \end{pmatrix}$$



$\Rightarrow S$ is closed under composition!

Similarly we have:

$[f \in S \Rightarrow f^{-1} \in S]$

$\Rightarrow (id : X^* \longrightarrow X^*) \in S$

$\Rightarrow (S, \circ)$ is a group

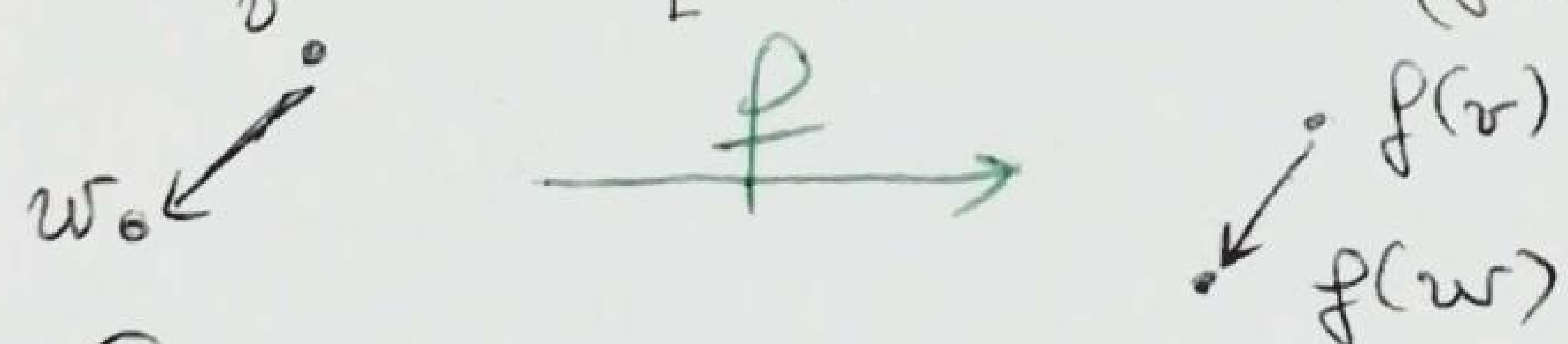
Characterization of the Actions of Automata

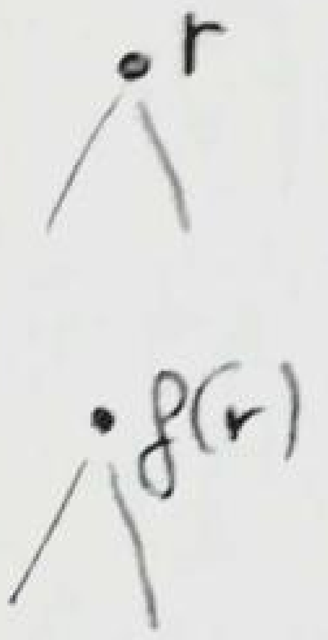
Povzetek:

Automaton $\mathcal{A}$ ⇝ Initial automaton $\mathcal{A}_{q_0}$ ⇝ $\bar{l}_{q_0} : X^* \to X^*$

$$S := \{ f : X^* \to X^* \mid f \text{ is the action of some } \mathcal{A}_{q_0} \}$$

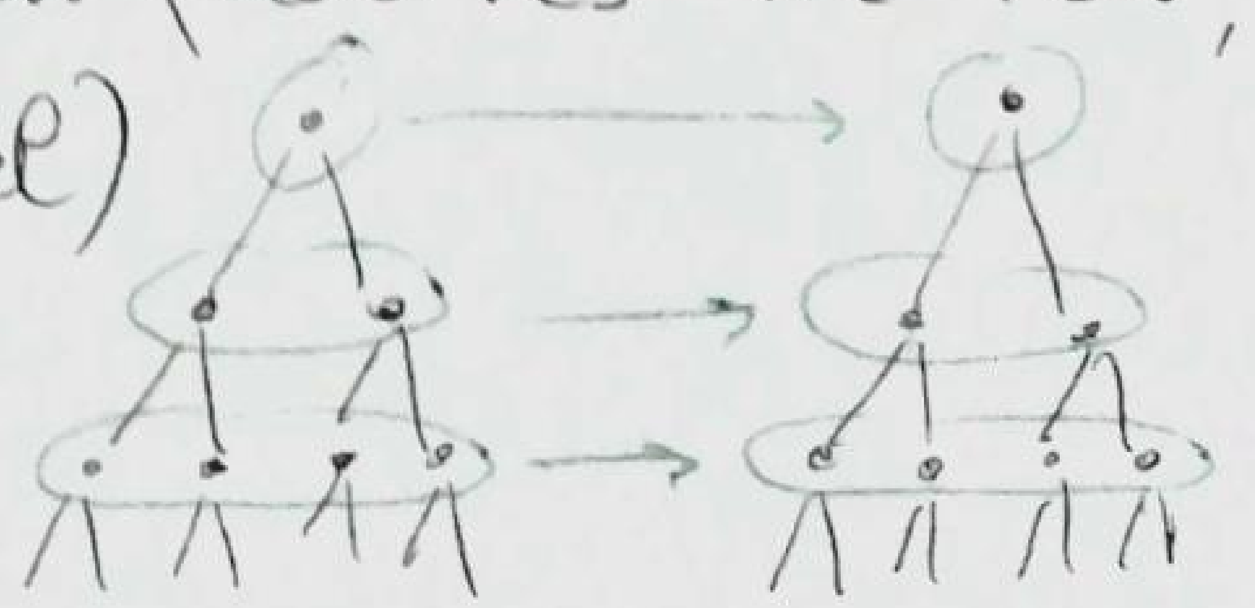
Remark • Given $G=(V,E)$ graph, $f: V \to V$ is said to be a graph-homomorphism if preserve the adjacencies $[\,(v,w)\in E \Longrightarrow (f(v),f(w)) \in E$





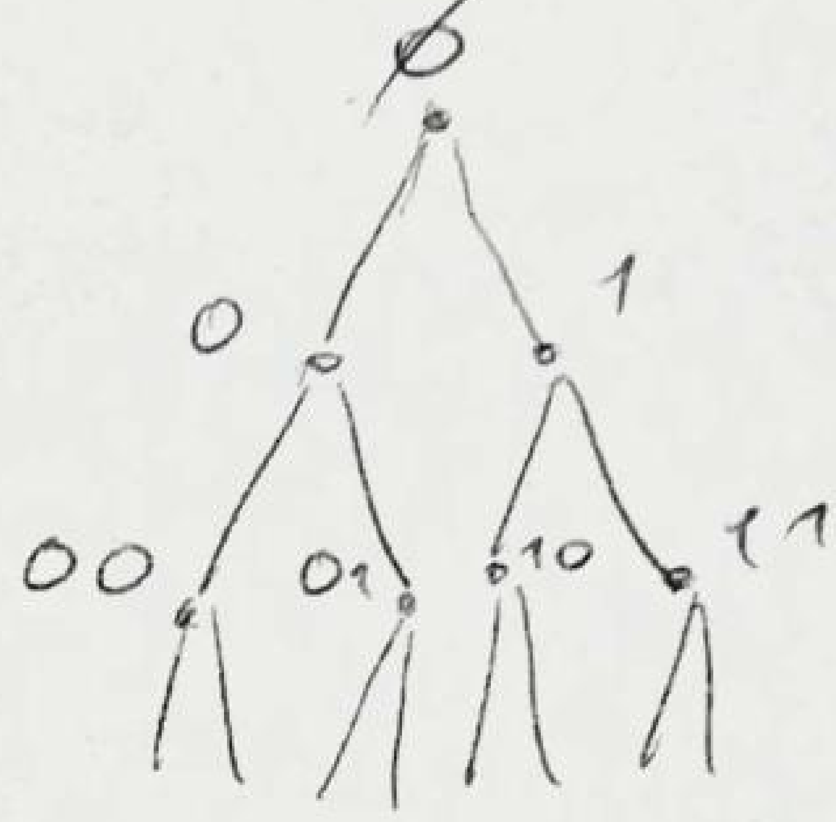
• If G is a tree, f is said to be a graph-homorphism that preserves the root if (1) is a graph-homomorphism and if (2) $f(r) = r$, where r is the root of G

Note If f is a graph-hom. that preserves the root, $f(\text{n-th level of } G) \subseteq (\text{n-th level})$



Proposition: $f : X^* \longrightarrow X^*$ is synchr. automatic if and only if f is a graph homomorphism that preserves the root on X^*.

Remark: X^* is a tree



Proof ($\Rightarrow$) f is sync. automatic, i.d. $f \in S$, so $f = \bar{\lambda}_q$, for some $\mathcal{A}_q$.

- condition 1: $¿\, v \sim w \Rightarrow f(v) \sim f(w)\,?$

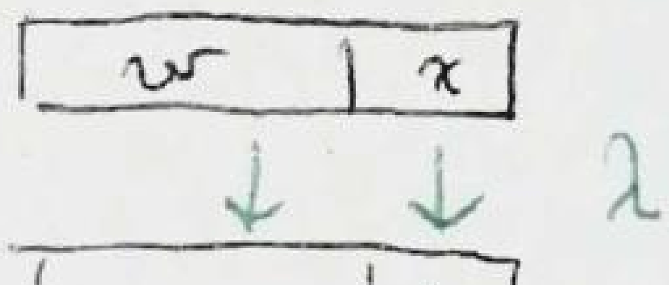
0010

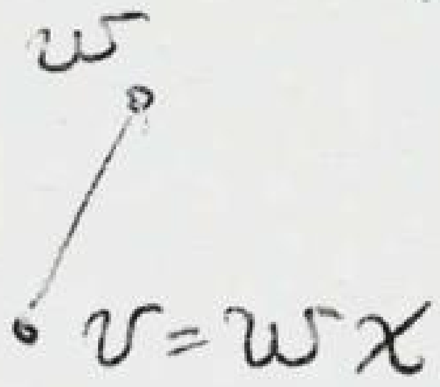
00101

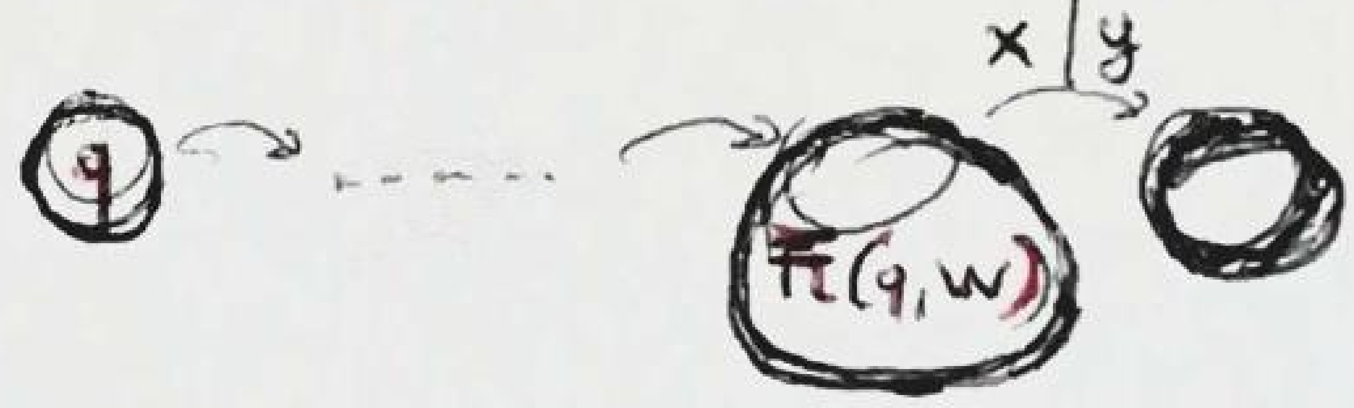
$v \in X^*$ is son of $w \in X^* \Leftrightarrow v = wx$

$$f(v) = \bar{\lambda}_q(v) = \bar{\lambda}_q(wx) = \bar{\lambda}_q(w) \cdot \bar{\lambda}_{\pi(q,w)}(x) =$$

recursive formulas







$$= f(w) \cdot y \quad \text{for some } y \in X$$ ✓

- condition 2: $¿\, f(r) = r\,?$

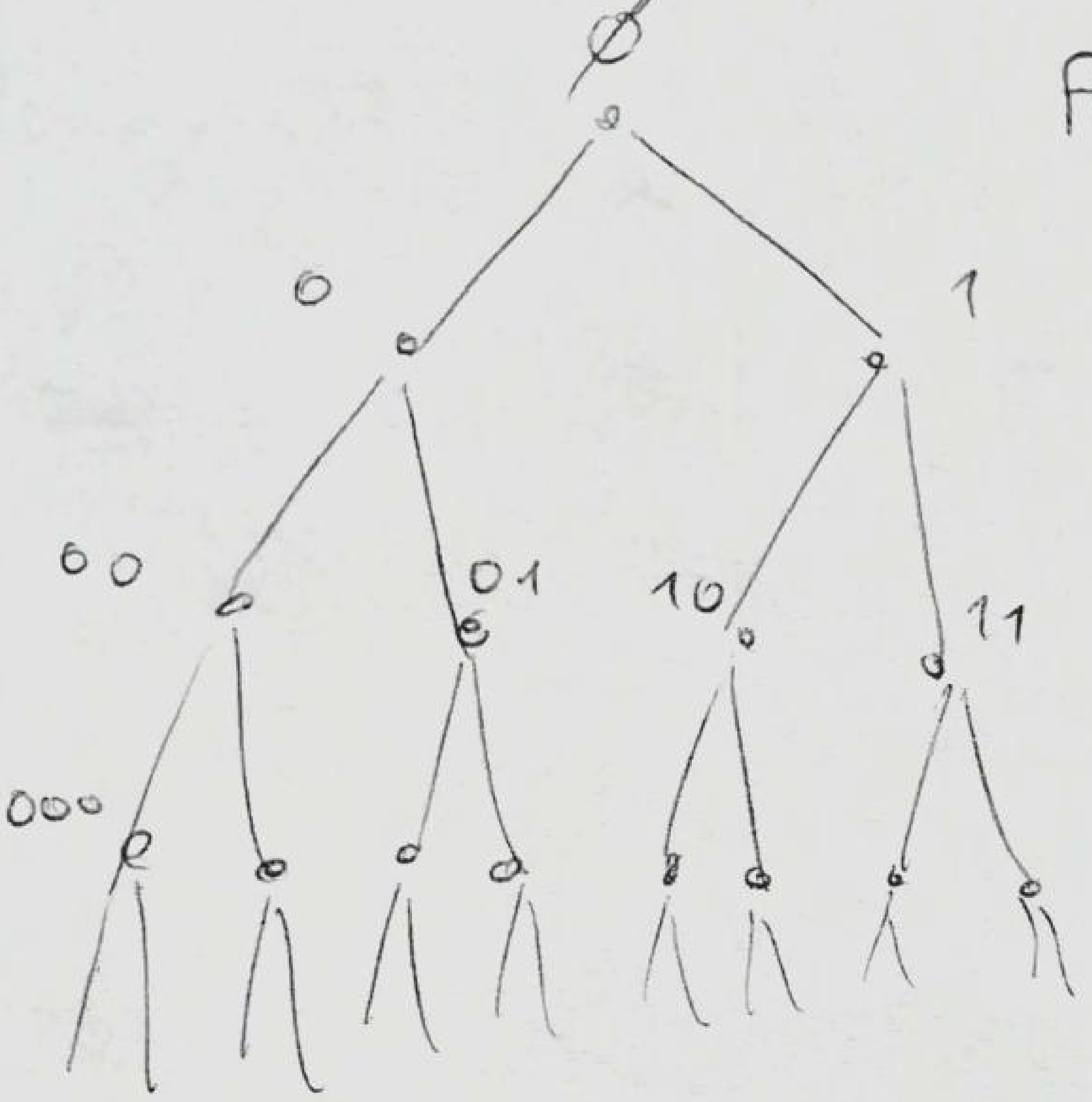
root of X^* is $\emptyset$

$$f(\emptyset) = \bar{\lambda}_q(\emptyset) = \emptyset$$ ✓

$\Rightarrow f$ is graph-hom. that preserves the root

(⇐)

Let f be a graph-hom. that preserves the root on X^*. We need to build $\mathcal{A}$, then find q s.t. $\mathcal{A}_q$ defines f as its action.



$$\mathcal{A} \rightsquigarrow \mathcal{A}_q \longrightarrow \bar{\lambda}_q = f$$

[Trick $Q := X^*$ (infinite)]

First we build $\mathcal{A}$

$$\mathcal{A} = (X, Q, \pi, \lambda) := (X, X^*, \pi, \lambda)$$

with
$$\begin{cases} \pi(q, x) = qx & (*) \\ \lambda(q, x) = f(qx) - f(q) & (**) \end{cases}$$

where $q \in X^* = Q$, $x \in X$

Note] condition $(*)$ tells the diagram of $\mathcal{A}$ is X^*!

Exspression $(**)$?

[Subtraction in X^*: if $\underset{\in X^*}{w} = \underset{\in X^*}{v}\,\underset{\in X^*}{u}$, i.d. v is the "beginning" of w $\Longrightarrow$ $w - v := u$

$$\underbrace{\boxed{\;v\;}\boxed{\;u\;}}_{w}$$
]

$\mathcal{A}$ can be ~~...~~ defined just if $(**)$ is defined.

(**) is defined only if $f(q)$ is the beginning of $f(qx)$. In a drawing, we want $\underbrace{\boxed{\quad f(q) \quad \mid \ }}_{f(qx)}$.

qx is son of $q \Rightarrow f(qx)$ is son of $f(q)$

$$\begin{tikzcd} q \arrow[d] & & f(q) \arrow[d] \\ qx & \xrightarrow{f} & f(qx) \end{tikzcd}$$

In X^* this means $f(qx) = f(q) \circ y$, for some $y \in X \Rightarrow$ (**) is defined (and has lenght 1) $\Rightarrow \lambda(q, x)$ is defined $\Rightarrow A$ is defined.

Now we claim: $f = \bar{\lambda}(\emptyset; \cdot) = \bar{\lambda}_\emptyset$

Let's see:

- $\bar{\lambda}(\emptyset; \emptyset) = \bar{\lambda}_\emptyset(\emptyset) = \emptyset = f(\emptyset)$
- if $w \in X^* \setminus \{0\}$, $w = vx$, for some $v \in X^*, x \in X$

$$\boxed{\quad v \quad \mid x}$$

$$\bar{\lambda}_\emptyset(w) = \bar{\lambda}(\emptyset, w) = f(\emptyset w) - f(\emptyset) =$$
$$= f(w) - \emptyset = f(w) \quad \checkmark$$

∎

Note] $S = \{$bijective hom. that preserve the root on $X^*\}$

DEF Given $\mathcal{A}$ automaton we can define $|Q|$ initial automata $\mathcal{A}_q$, so $|Q|$ actions $\bar{\lambda}_q \in S$.
The <u>group generated by $\mathcal{A}$</u> is defined as:

$$G(\mathcal{A}) := \langle \{ \bar{\lambda}_q \mid q \in Q \text{ of } \mathcal{A} \} \rangle \leq S$$

$$\text{Automaton} \rightsquigarrow \begin{cases} \mathcal{A}_{q_1} \\ \vdots \\ \mathcal{A}_{q_n} \end{cases} \begin{matrix} \rightsquigarrow \\ \\ \rightsquigarrow \end{matrix} \begin{cases} \bar{\lambda}_{q_1} \\ \vdots \\ \bar{\lambda}_{q_n} \end{cases} \longrightarrow \langle \bar{\lambda}_{q_1}, \dots, \bar{\lambda}_{q_n} \rangle \leq S$$

Ex: page 2A, (1) Γ_1 defines $G(\Gamma_1) := \langle \bar{\lambda}_{q_0}, \bar{\lambda}_{q_1}, \bar{\lambda}_{q_2} \rangle$

Interesting Results and Examples

PROPOSITION Given $X = \{0, 1\}$, and $\mathcal{A}$, 2-state automaton on X, $G(\mathcal{A})$ must be isomorphic to one of these groups:

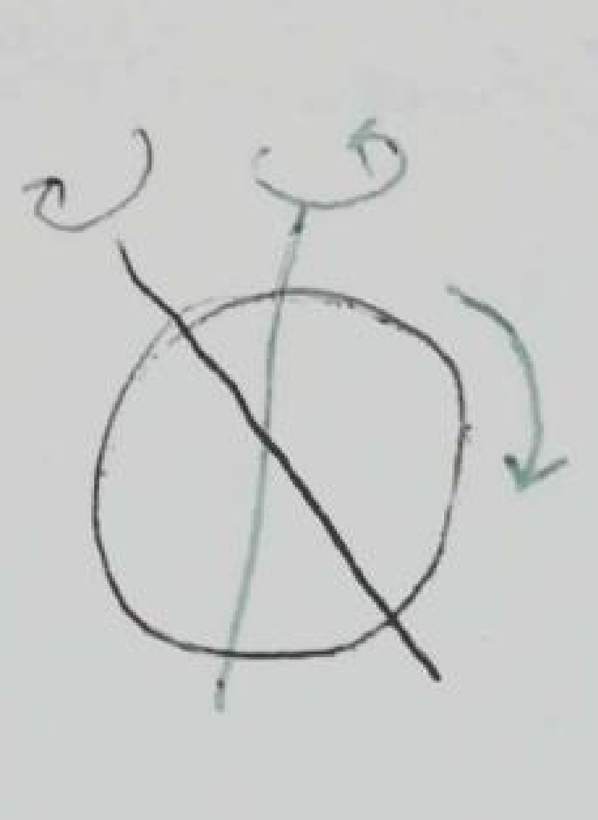
(1) $\{1_G\}$

(2) $\mathbb{Z}_2$

(3) $\mathbb{Z}_2 \oplus \mathbb{Z}_2$

(4) $\mathbb{Z}$

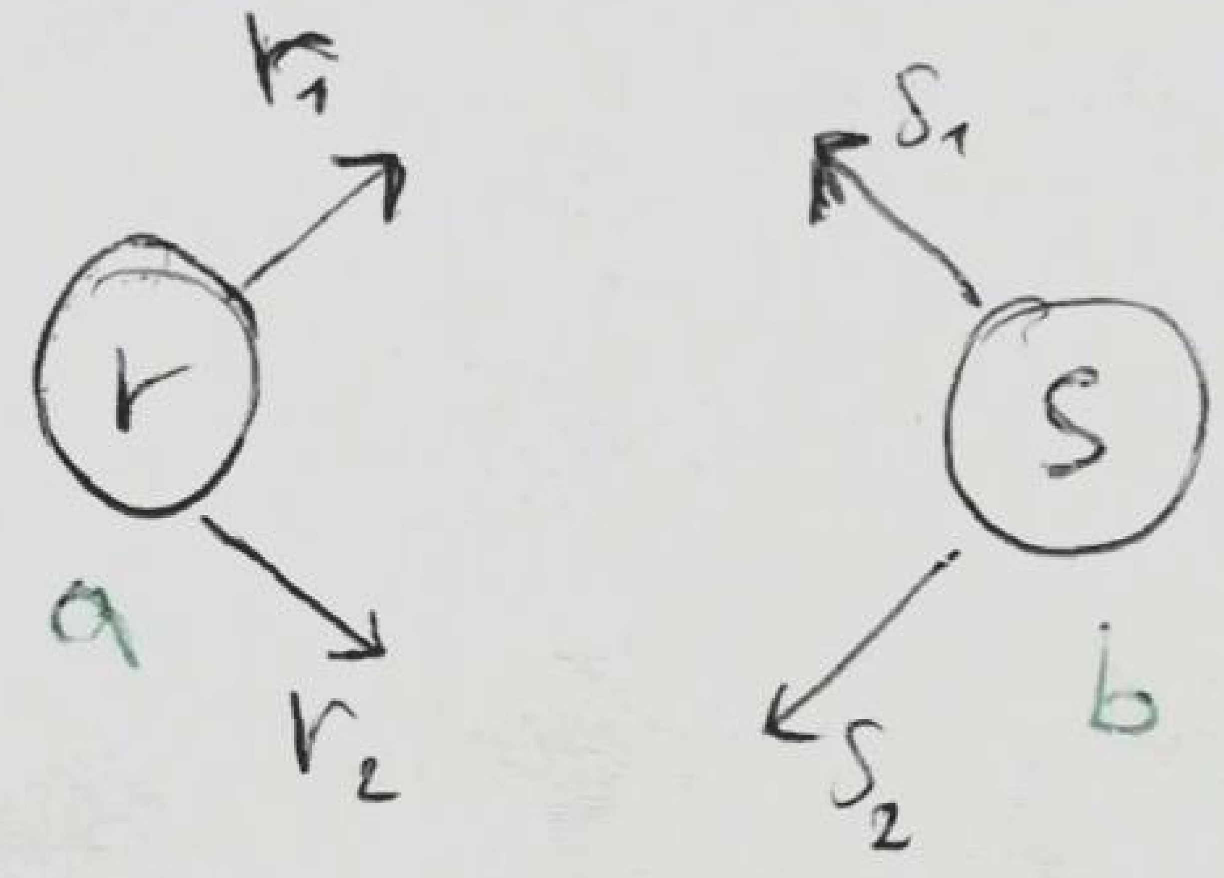
(5) D_∞ = Infinite dihedral group = {symm. of the circle}



(6) $\mathbb{Z} \wr \mathbb{Z}_2$ = Lamplighter group

Sketch of proof : Q, the set of states

$$Q = \{r, s\} \quad , \quad X = \{0, 1\}. \ \mathcal{A} = (X, Q, \pi, \lambda)$$



- $\lambda_s, \lambda_r : X \to X$ are permutation of a 2-element set $X \Rightarrow \lambda_s, \lambda_r \in S_2$, $S_2 = \{id = 1, \sigma\}$

$$\begin{cases} \sigma(0) = 1 \\ \sigma(1) = 0 \end{cases}$$

- each arrow in $\{r_1, r_2, s_1, s_2\}$ can point on an element of $Q = \{r, s\}$

So all the possible $\mathcal{A}$, with $Q = \{r, s\}$, $X = \{0, 1\}$ are the ones in witch $\lambda_s, \lambda_r \in S_2$ (uniquely determines λ), and $r_1, r_2, s_1, s_2 \in \{r, s\}$ (uniquely determines π) $\Longrightarrow$

$$\Longrightarrow \text{they are } \underset{\lambda_s}{2} \cdot \underset{\lambda_r}{2} \cdot \underset{r_1}{2} \cdot \underset{r_2}{2} \cdot \underset{s_1}{2} \cdot \underset{s_2}{2} = 2^6.$$

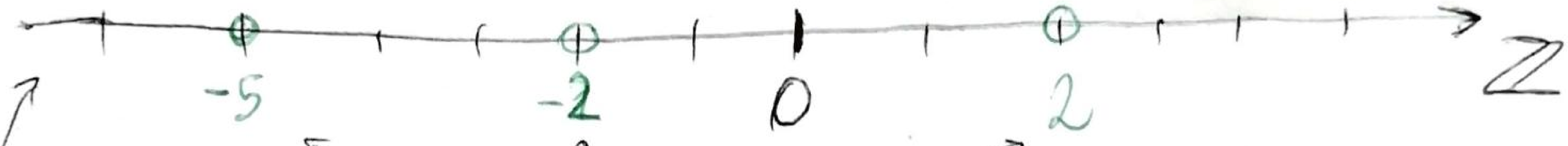
Analysing each case we get [$G(\mathcal{A})$ is isomorphic to ~~one~~ ~~case~~ of the latter cases].

Interesting group:

$$\mathbb{Z} \wr \mathbb{Z}_2 := \left(\mathbb{Z} \times \mathbb{Z}_2^{(\mathbb{Z})} \, ; \, \star \right)$$

- $\mathbb{Z}_2^{(\mathbb{Z})} := \{ (b_i)_{i \in \mathbb{Z}} \mid b_i \in \mathbb{Z}_2 = \{0,1\}, \ b_i = 1$ just for a finite set of indexes $I \}$

Practically:



Infinite dark road $\mathbb{Z}$

indexes of the ~~open~~ lamps turned on (indexes in I)

Ex] The previous represented element is $(\tilde{b}_i)_{i \in \mathbb{Z}}$, where $b_{-5}, b_{-2}, b_2 = 1$.
[We can sign $(\tilde{b}_i)_{i \in \mathbb{Z}}$ with $\{-5, -2, 2\} = I$]

- $\star$ is not a direct product!

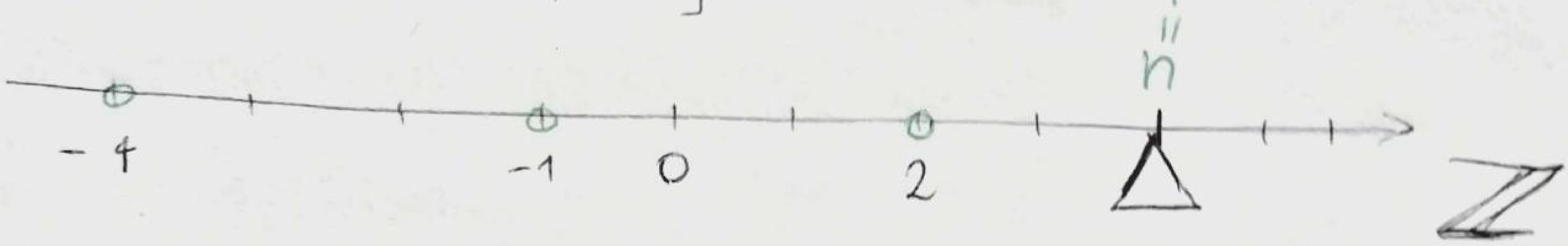
$$\left(n_1 , (b_i)_{i \in \mathbb{Z}} \right) \star \left(n_2 , (q_i)_{i \in \mathbb{Z}} \right) :=$$

$$= \left(n_1 + n_2 \, , \, \left(b_i + q_{i + n_1} \right)_{i \in \mathbb{Z}} \right)$$

Visualization:

• Of an element $(n, (b_i)_{i\in\mathbb{Z}}) \in \mathbb{Z} \times \mathbb{Z}_2^{(\mathbb{Z})}$

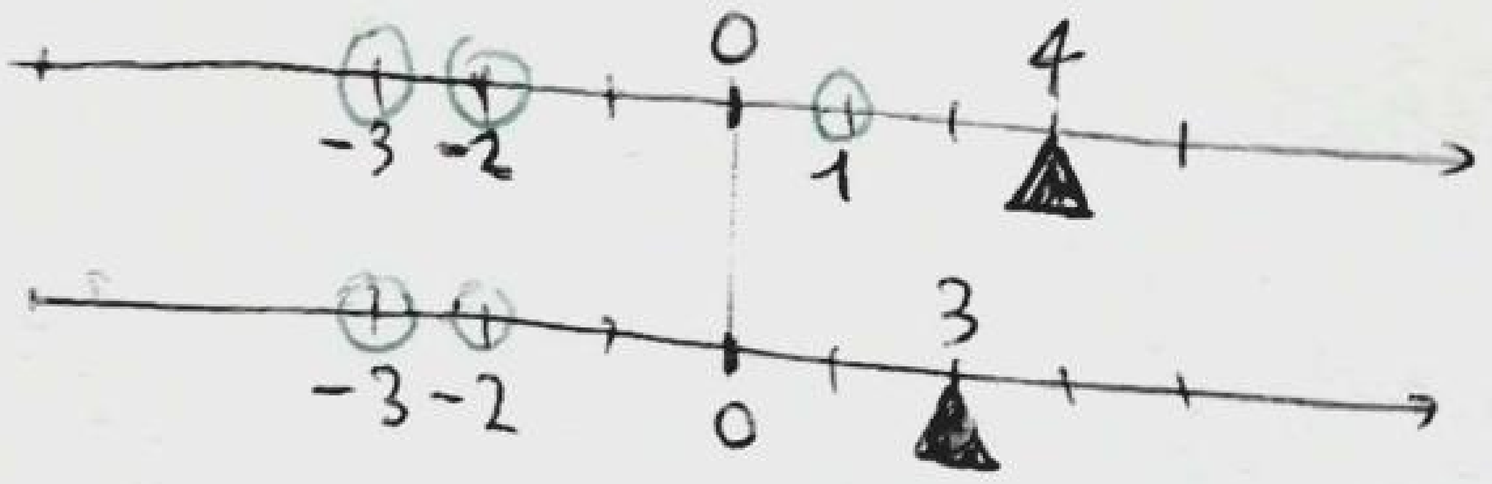
$[(4, (b_i)_{i\in\mathbb{Z}})$, where $b_{-4}, b_{-1}, b_2 = 1] =$



n = position of the "lamplighter on the infinite road

• Of the product $\star$:

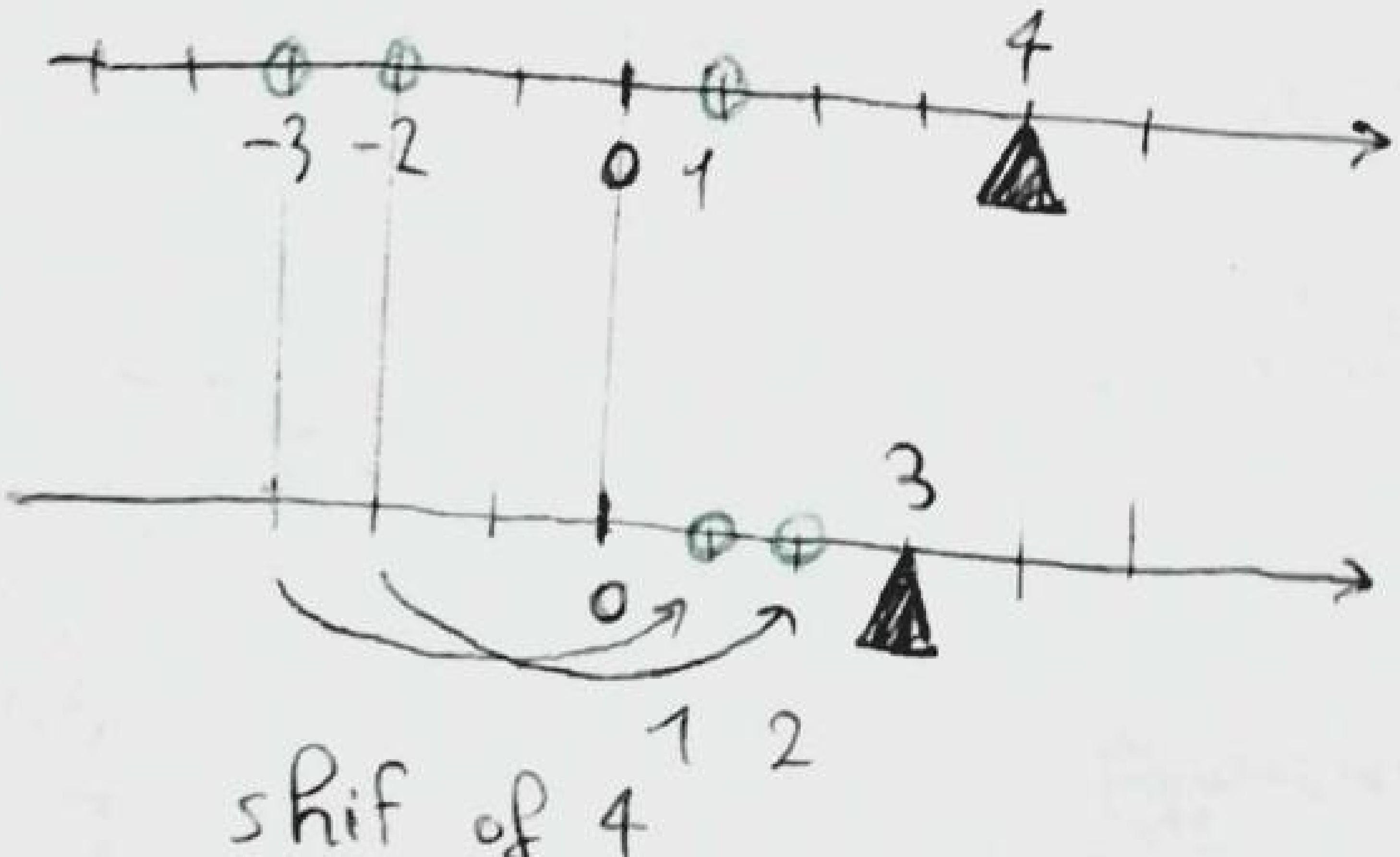
$$\Big(\overset{n_1}{4} ; \overset{(b_i)_{i\in\mathbb{Z}}}{\{-3;-2;1\}}\Big) \star \Big(\overset{n_2}{3} ; \overset{(q_i)_{i\in\mathbb{Z}}}{\{-3;-2\}}\Big) =$$



$(n_1 , (b_i)_{i\in\mathbb{Z}})$

$(n_2 , (q_i)_{i\in\mathbb{Z}})$

$$= \Big(\underset{n_1}{4} , \underset{(b_i)_{i\in\mathbb{Z}}}{\{-3,-2,-1\}}\Big) + \Big(\underset{n_2}{3} , \underset{(q_i+n_1)_{i\in\mathbb{Z}}}{\{\overset{-3+4}{1}, \overset{-2+4}{2}\}}\Big) =$$

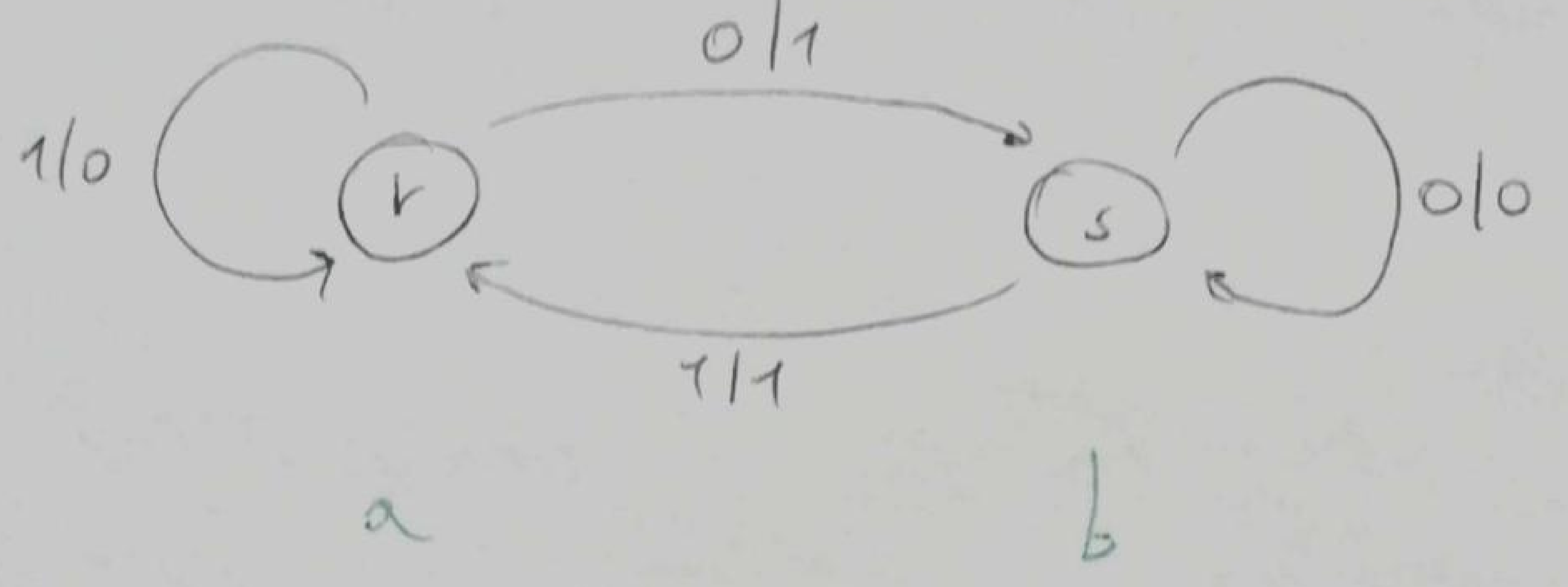


$(n_1 , (b_i)_{i\in\mathbb{Z}})$

$(n_2 ; (q_i + n_1)_{i\in\mathbb{Z}})$

$$= (4+3 ; \{-3 ; -2 ; 2\})$$

The automaton which defines $\mathbb{Z} \wr \mathbb{Z}_2$:



$=: \mathcal{A}$

$$a := \bar{\lambda}_r \quad , \quad b := \bar{\lambda}_s$$

$$\mathbb{Z} \wr \mathbb{Z}_2 = \langle a , b \rangle = G(\mathcal{A})$$

Let's watch closer:

$$\begin{cases} a(0v) = 1b(v) \\ a(1v) = 0a(v) \end{cases} \qquad \begin{cases} b(0v) = 0b(v) \\ b(1v) = 1a(v) \end{cases}$$

$$\lambda_r : X \to X \qquad \lambda_s : X \to X$$

$$\lambda_r = \sigma \in S_2 \qquad \lambda_s = id \in S_2$$

$$\Rightarrow \begin{array}{c} b^{-1} : \\ X^* \\ \downarrow \\ X^* \end{array} = \begin{cases} b^{-1}(0v) = 0b^{-1}(v) \\ b^{-1}(1v) = 1a^{-1}(v) \end{cases}$$

1

$$c := b^{-1} \cdot a = a \circ b^{-1}$$

$$\begin{cases} c(0v) = a \circ b^{-1}(0v) = a(0\, b^{-1}(v)) = 1\, \overbrace{b \circ b^{-1}}^{id}(v) = 1v \\ c(1v) = a \circ b^{-1}(1v) = a(1\, b^{-1}(v)) = 0\, \underbrace{b \circ b^{-1}}_{id}(v) = 0v \end{cases}$$

- we see $\langle a, b \rangle = \langle b^{-1} a, b \rangle = \langle c, b \rangle = G(\mathcal{A})$

$b^{-1}a = c$ $\quad\in$ $\quad a \in$

- $\mathbb{Z}_2 = (X ; +_{\mathbb{Z}_2})$

$0+0=0$
$1+1=0$
$1+0=1$

$$c(x_1 x_2 x_3 \,—) = (x_1+1)\, x_2 x_3 \,—$$

we search an explicit formula for b:

$$b(x_1 x_2 x_3 \,—) = y_1 y_2 y_3 \,— \qquad y_n = ?$$

we claim (A) $b(x_1 x_2 - x_n \overset{(n+1)}{0} x_{n+2} -) =$
$= y_1 y_2 \; y_n y_{n+1} b(x_{n+2} -)$

(B) $b(x_1 x_2 - x_n \overset{(n+1)}{1} x_{n+2} -) =$
$= y_1 y_2 - y_n y_{n+1} a(x_{n+2} -)$

Proof | (A) Watch diagram of $\mathcal{A}$. Whenever we encounter a "0", b acts on the next letter

(B) Analogous

We claim $b(x_1 x_2 - x_n -) = \underbrace{x_1}_{y_1}\underbrace{(x_2+x_1)}_{y_2} - \underbrace{(x_n+x_{n-1})}_{y_n} -$

Proof: For induction on n.

$n=1$ We set $x_0 = 0 \Rightarrow y_1 = x_1 = x_1 + 0 = x_1 + x_0$

$n \rightsquigarrow n+1$ 4 cases: $x_n x_{n+1} \in \{00, 01, 10, 11\}$

Case 00: $y_n = \cancel{x_n} + \cancel{x_{n+1}}$; $y_{n+1} = ?$

$$b(x_1 - x_{n-1} \overset{n}{0} \overset{(n+1)}{0} x_{n+2} -) \overset{(4)}{=} y_1 - y_n b(0 x_{n+2} -) =$$

$$= y_1 - y_n 0 y_{n+2} -$$

$$y_{n+1} = 0 = 0 + 0 = x_n + x_{n+1}$$

The other cases are analogous ✓

$$\Rightarrow c(x_1 x_2 x_3 -) = \underbrace{(x_1+1)}_{\sigma(x_1)} x_2 x_3 -$$

$$b(x_1 x_2 x_3 -) = x_1 (x_2+x_1)(x_3+x_2) - =$$

$$= x_1 \quad x_2 \quad x_3 \quad x_4 \quad - \quad +$$

[shift to right] $\quad x_1 \quad x_2 \quad x_3 \quad -$

It can be prooved, with these formulas, that

$$< b, c > = \mathbb{Z} \wr \mathbb{Z}_2$$