GROUPS OF AUTOMATA

CARLO LANZI LUCIANI

MENTOR: GANNA KUDRYAVTSEVA

AUTOMATA ARE A MODEL OF COMPUTATION.

$$\begin{tikzcd} & \text{INPUT} \arrow[d] & \\ \text{AUTOMATON} \arrow[r, squiggly, "\text{defines}"] & \boxed{\text{Initial Automaton}} \arrow[r, squiggly, "\text{defines}"] \arrow[d] & \text{function(INPUT)} = \text{OUTPUT} \\ & \text{OUTPUT} & \text{AIM} \arrow[u] \end{tikzcd}$$

<u>ALPHABETS</u> (INPUT AND OUTPUT):

X = finite set of symbols   <u>Ex</u>: $X = \{0, 1\}$

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

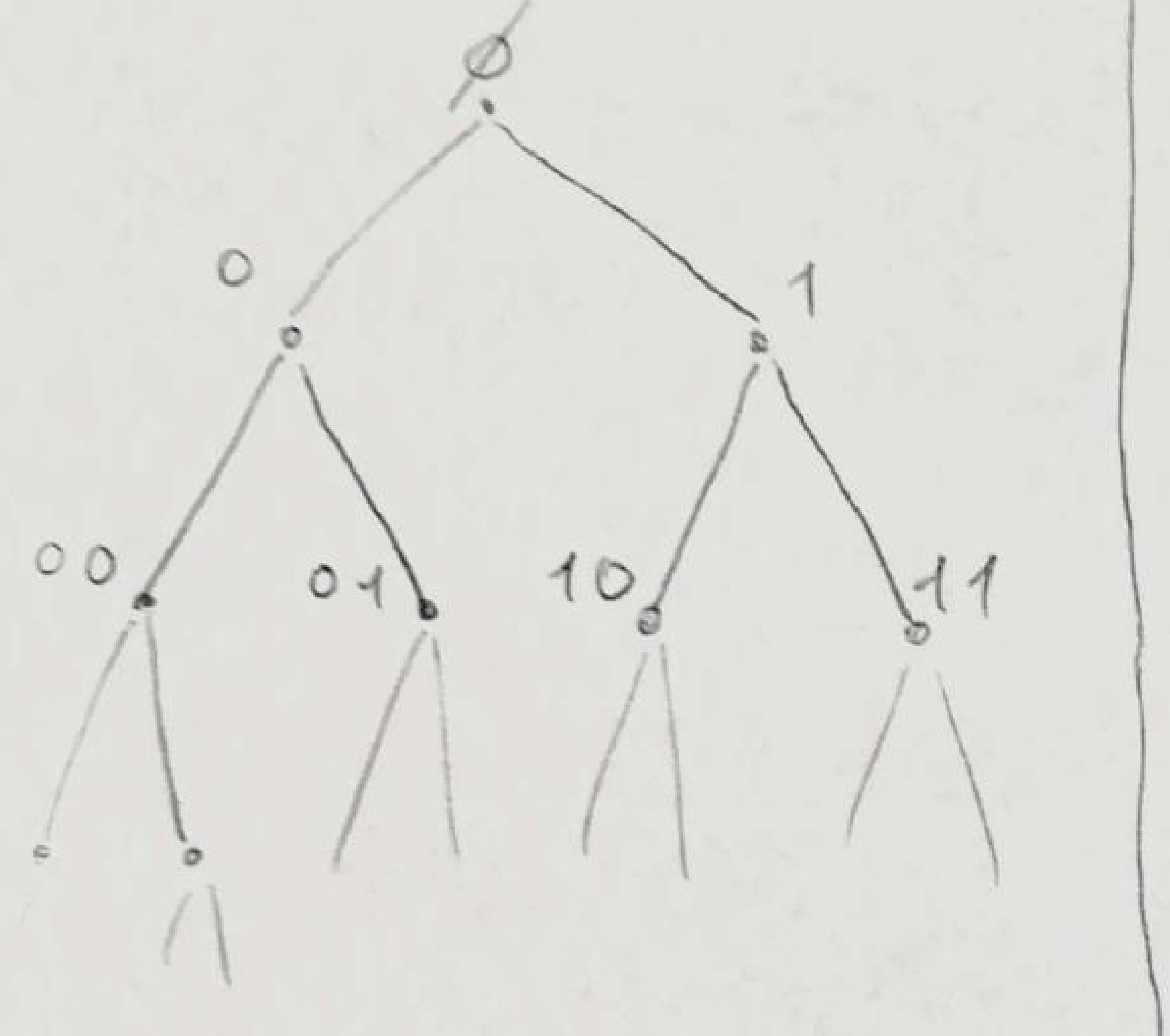
$|w| = |x_1 \cdot \text{—} \cdot x_n|$ = lenght of the word $w = n$

$$\left.\begin{array}{l} (x_1 \cdot \text{—} \cdot x_n) \circ (y_1 \cdot \text{—} \cdot y_m) = x_1 \cdot \text{—} \cdot x_n y_1 \cdot \text{—} \cdot y_m \\ \emptyset := \text{empty word} \end{array}\right\} X^* \text{ MONOID}$$

ALTERNATIVE WAY TO SEE X^*:

X^* as a <u>tree</u> (infinite):
(1) $\emptyset$ is the root
(2) w is son of v whenever $w = vx$ for some x in X

Ex: if $X = \{0,1\}$, X^* is



We observe:

$X^n = \{\text{words of lenght } n\}$
$= n\text{-th floor of } X^*$

DEF] A SYNCHRONOUS INVERTIBLE AUTOMATON $\mathcal{A}$ is a tuple ($\simeq$ list) $\mathcal{A} = \langle X, Q, \pi, \lambda \rangle$ where:

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

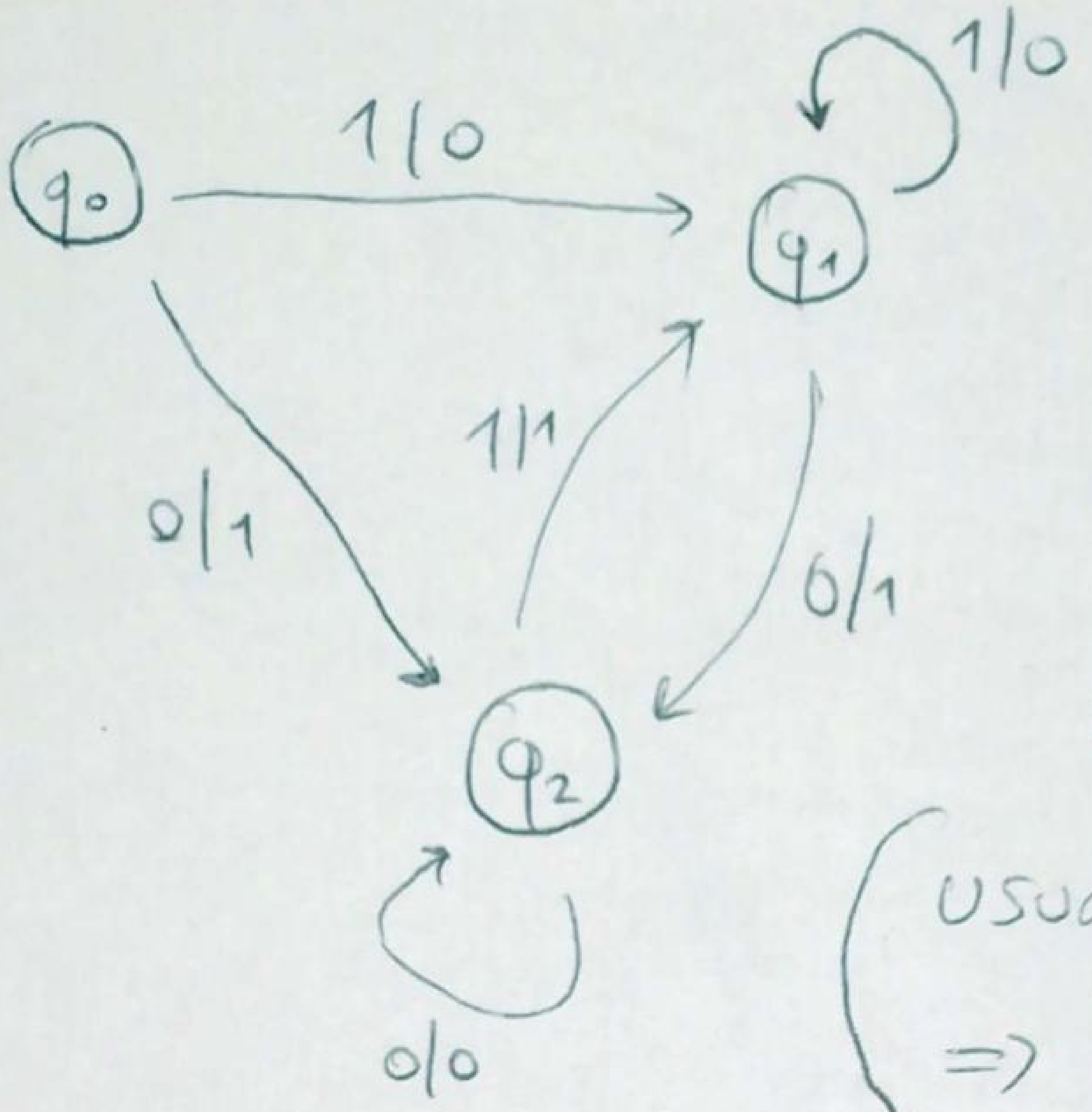
(2) Q is the SET OF STATES

(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, and it's called the OUTPUT FUNCTION

[From now on AUTOMATON = SYNCHRONOUS INV. AUTOMATON]

Ex



$X = \{0, 1\}$

Notation:

input letter | output letter

(usually $|Q| < \infty$
$\Rightarrow$ drawable graph)

---

we can extend π and λ :

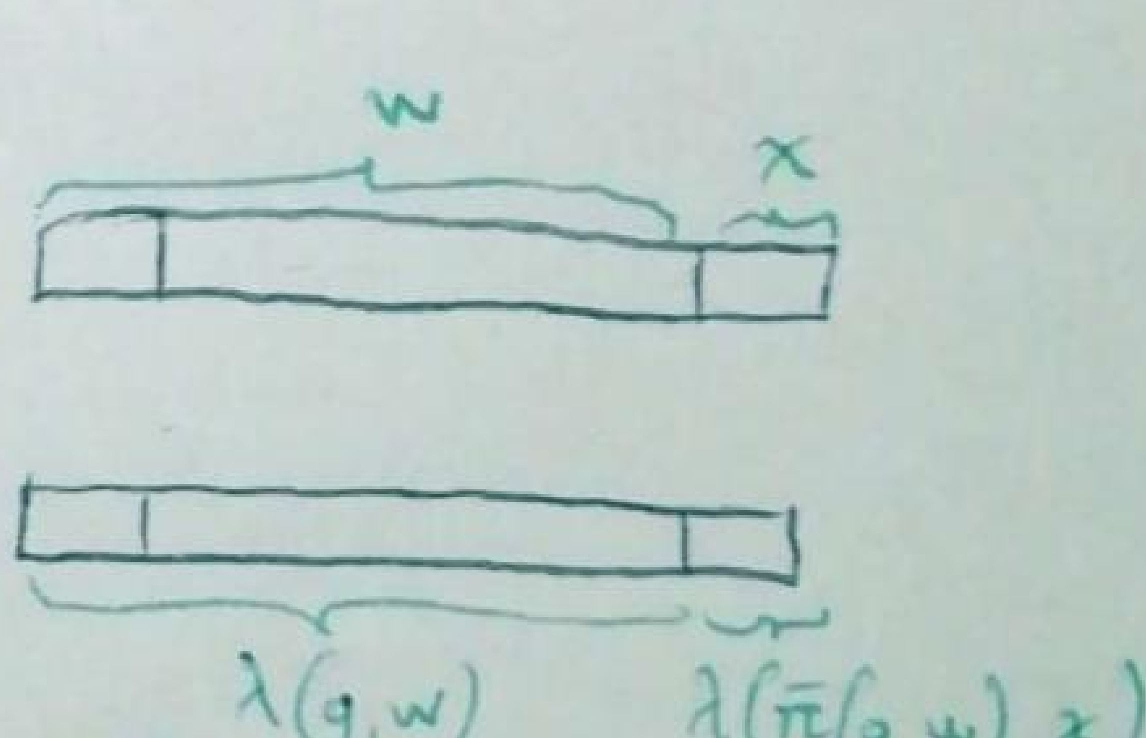
- $\overline{\pi} : Q \times X^* \longrightarrow X^*$

$$\begin{cases} \overline{\pi}(q, \emptyset) = q \\ \overline{\pi}(q, wx) = \overline{\pi}(\overline{\pi}(q, w), x) \end{cases}$$

or equivalently

$$\overline{\pi}(q, xv) = \overline{\pi}(\overline{\pi}(x, q), v)$$

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



$$\begin{cases} \overline{\lambda}(q, \emptyset) = \emptyset \\ \overline{\lambda}(q, wx) = \overline{\lambda}(q, w)\, \overline{\lambda}(\overline{\pi}(q, w), x) \end{cases}$$

or equivalently

$$\overline{\lambda}(q, xv) = \overline{\lambda}(q, x) \cdot \overline{\lambda}(\overline{\pi}(q, x), v)$$

DEF] Given $\mathcal{A}$ automaton, $\mathcal{A}_{q_0}$ with a <u>fixed</u> <u>INITIAL STATE</u> $q_0 \in Q$, is called <u>INITIAL AUTOMATON</u>

NOTE] (1) $\mathcal{A}_{q_0}$ defines $\bar{\lambda}_{q_0} : X^* \longrightarrow X^*$, its <u>ACTION</u>. $\left[\bar{\lambda}_{q_0}(w) = \bar{\lambda}(q_0, w)\right]$

(2) $\bar{\lambda}_{q_0}$ is bijective on X^* $[\Leftarrow \lambda(q, \cdot)$ is bijective on $X]$

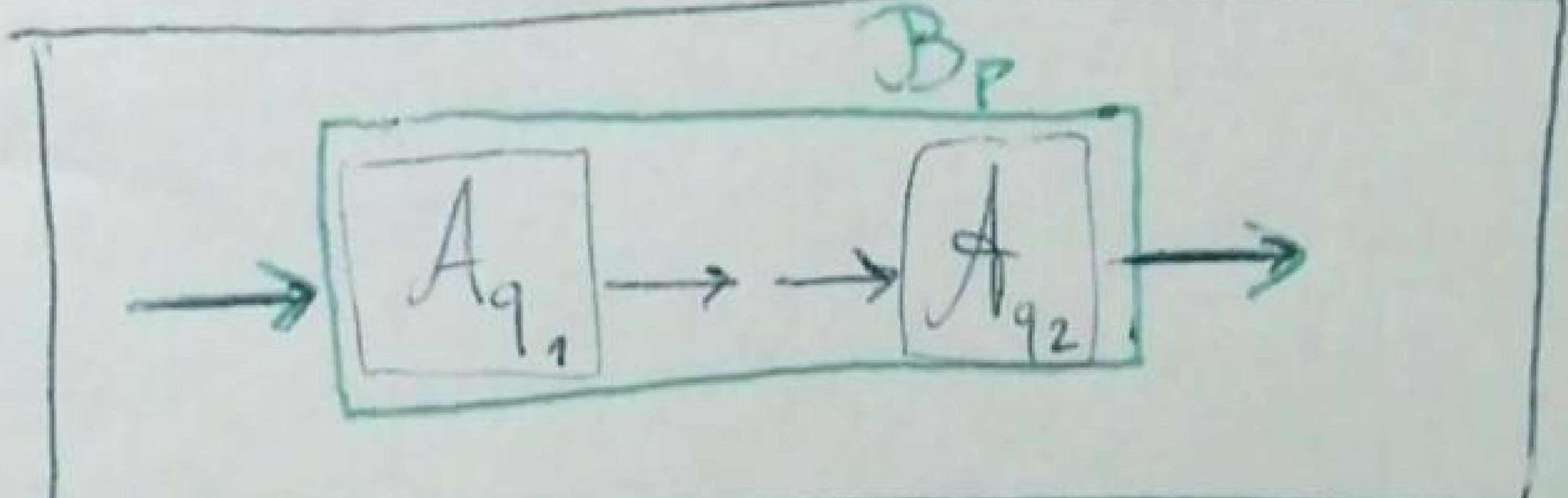
AUTOMATON $\rightsquigarrow$ INITIAL AUTOMATON $\rightsquigarrow$ ACTION OF $\mathcal{A}_{q_0}$

$\mathcal{A}$ $\qquad$ $\mathcal{A}_{q_0}$ $\qquad$ $\bar{\lambda}_{q_0} : X^* \longrightarrow X^*$

<u>Example</u>: pag 3

COMPOSITION LEMMA] Given $\mathcal{A}_{q_1}$, $\mathcal{A}_{q_2}$ initial automata, $\exists\, \mathcal{B}_p$ initial automaton s.t.

$$\bar{\lambda}^{\mathcal{B}}_{p} = \bar{\lambda}^{\mathcal{A}_2}_{q_2} \circ \bar{\lambda}^{\mathcal{A}_1}_{q_1}$$



$\mathcal{B}_p$ is called <u>COMPOSITION</u> of $\mathcal{A}_{q_1}$ and $\mathcal{A}_{q_2}$

DEF] $f : X^* \to X^*$ is <u>SYNCHRONOUS</u> <u>AUTOMATIC</u> if $\exists\, \mathcal{A}_q$ s.t. $f = \bar{\lambda}^{\mathcal{A}_q}_{q}$, so f is defined by an initial automaton (<u>Remark</u>: Automaton always invertible)

Note] $\{f : X^* \longrightarrow X^* \mid f$ is SYNC. AUTOMATIC$\}$ is a group for the COMPOSITION LEMMA.

[if f is synch. autom. $\Rightarrow f^{-1}$ is synch. autom]

CHARACTERIZATION OF SYNCHR. AUTOMATIC FUNCTIONS

Lemma f is synchronous automatic if and only if f is a tree-homomorphism on X^*

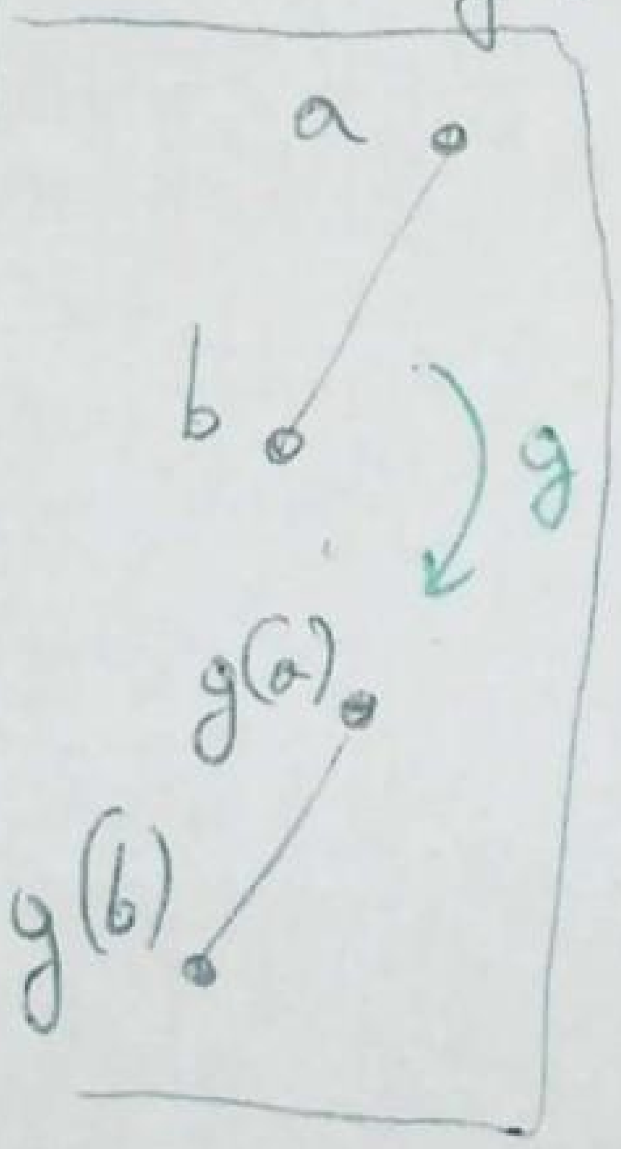
WHAT is a tree-homom?

DEF Given T tree, $g : T \to T$ is a tree-homom. if:

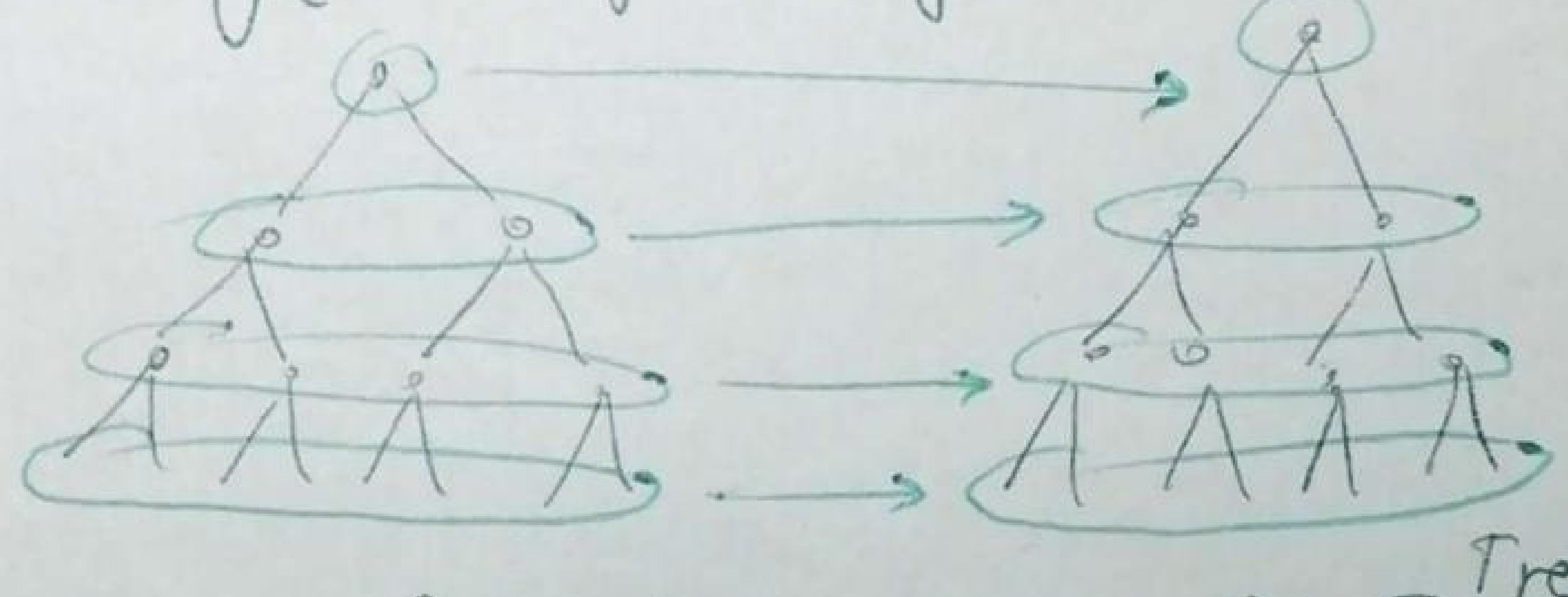
(1) preserves the root r : $g(r) = r$

(2) preserves descendant-relationship:

if b is son of $a \Rightarrow f(b)$ is son of $f(a)$



Note $g(n\text{-th floor of } T) \subseteq n\text{-th floor of } T$



Note • if g is bijective is called Tree-AUTOMORPHISM

• {tree-automorphisms of T} $= Aut(T)$ is a group under composition of functions

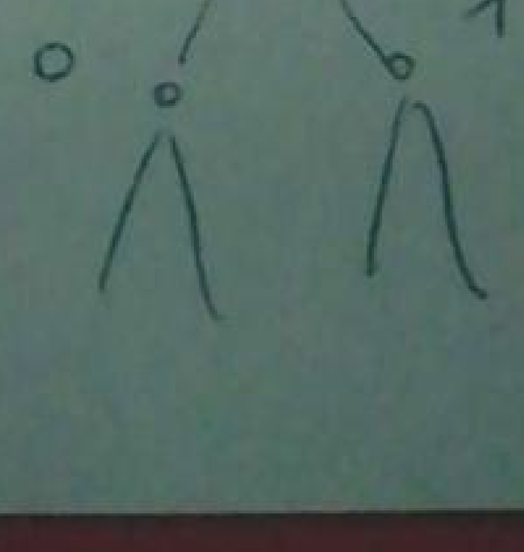
---

Proof of Lemma: (the tree is X^*)

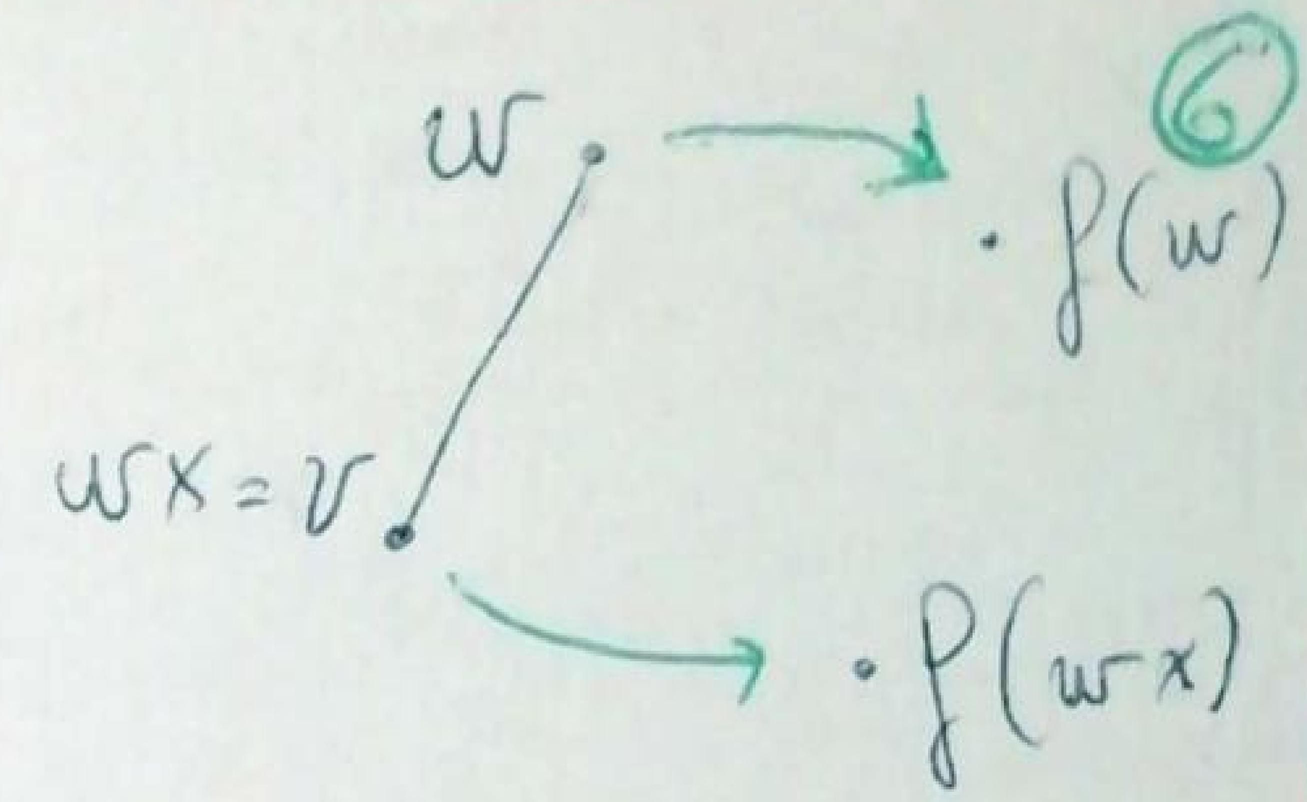
"$\Rightarrow$" f is synch. automatic, so $\exists\, \mathcal{A}_q$ s.t. $f = \bar{\lambda}_q$, action of $\mathcal{A}_q$. Let's verify condition (1):

$f(\emptyset) = \bar{\lambda}_q(\emptyset) = \emptyset$ (root of X^*)

(page 3 formulas) ✓



We want to verify condition (2).



$v, w \in X^*$, v son of $w \Rightarrow$

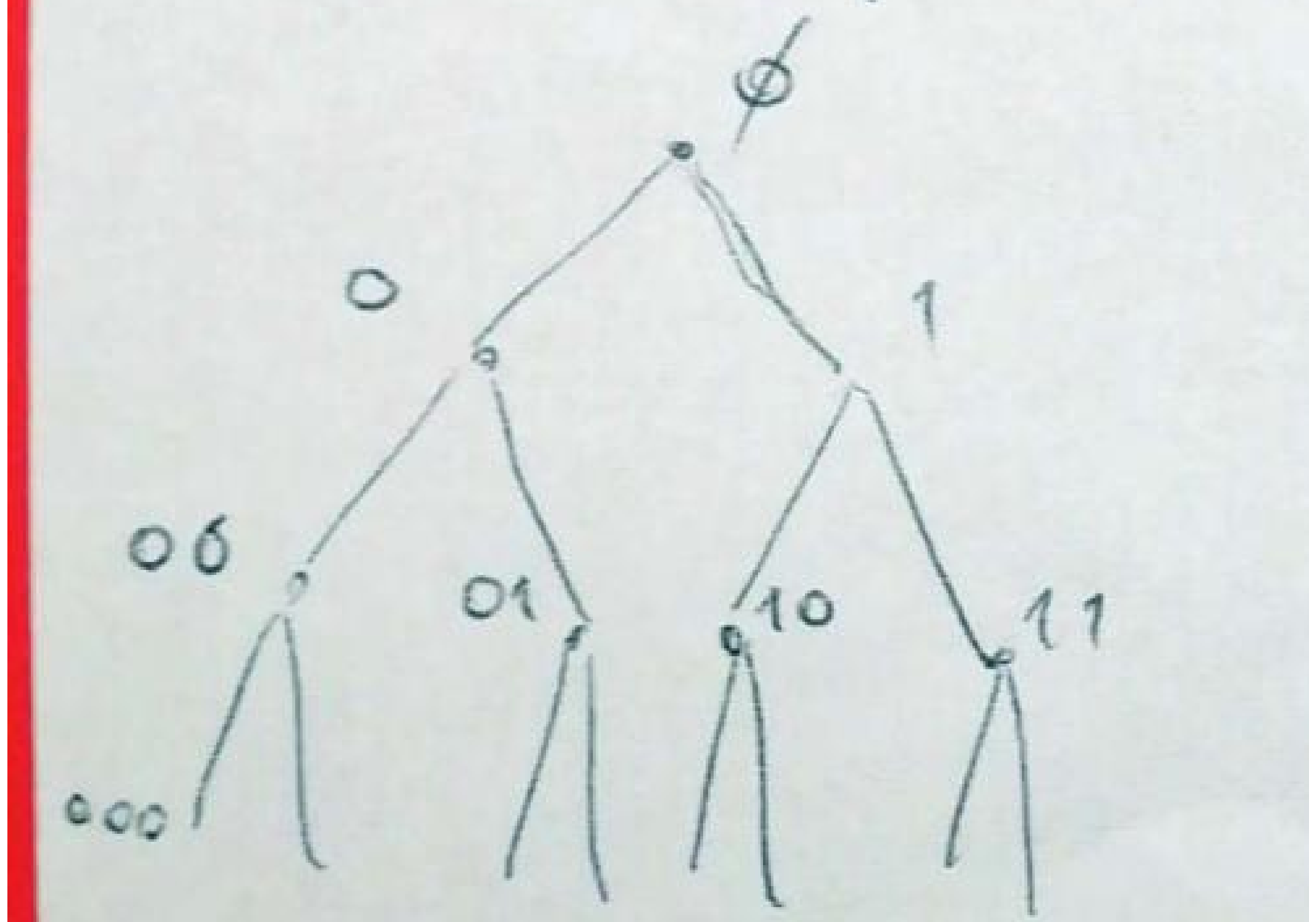
$\Rightarrow v = wx$ for some $x \in X$

$f(v) = f(wx) = \bar{\lambda}_q(wx) \underset{\substack{\uparrow \\ \text{pag 3} \\ \text{Form}}}{=} \bar{\lambda}_q(w) \cdot \bar{\lambda}_{\pi(q,w)}(x) =$

$= \bar{\lambda}_q(w) \cdot \underbrace{\lambda_{\pi(q,v)}(x)}_{\text{Lenght} = 1} = f(w)\, y$ for some $y \in X$

$\Rightarrow f(v)$ is son of $f(w) \Rightarrow f$ is tree-homom.

"$\Leftarrow$" Let f be tree homom.. We want to build

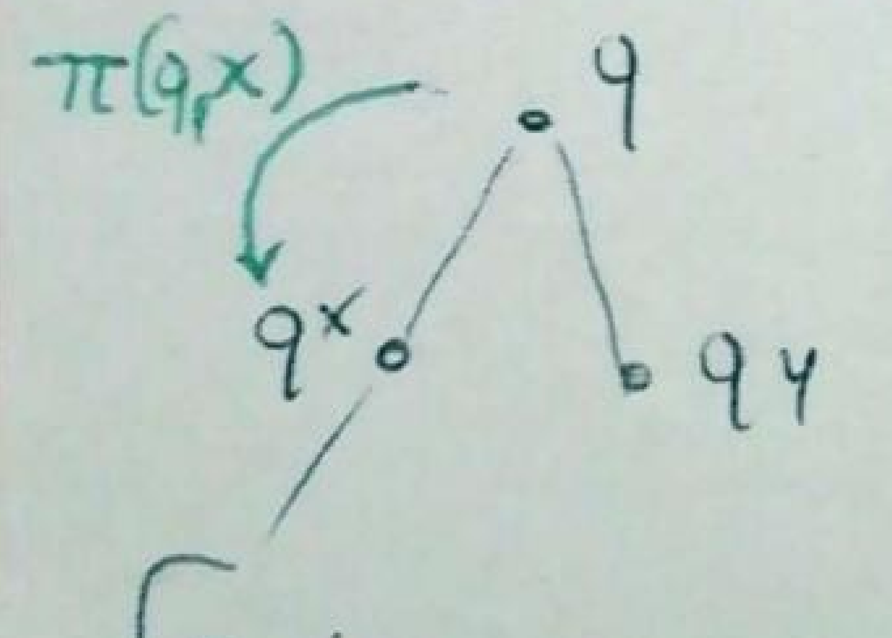


$\mathcal{A}$ s.t. $f = \bar{\lambda}_q$ for some q.

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

$\mathcal{A} = \langle X, Q, \pi, \lambda \rangle := \langle X, X^*, \pi, \lambda \rangle$

with π and λ so defined:



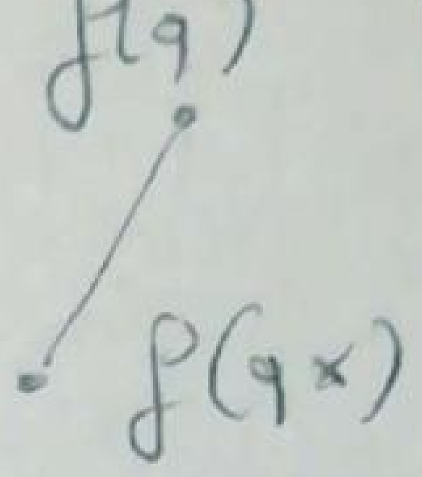
$$\begin{cases} \pi(q,x) = qx \\ \lambda(q,x) = f(qx) - f(q) \end{cases}$$

[Subtraction on X^*: if $w = uv$ (*) $\Rightarrow w - u := v$]

¿ Does (*) condition hold for λ? i.e.

¿ is $f(q)$ beginning of $f(qx)$?

f is tree-homom. $\Rightarrow f(qx)$ is son of $f(q)$



$\Rightarrow \quad f(qx) = f(q)z \quad$ for some $z \in X$

$\Rightarrow \quad f(qx) - f(q) = z. \quad [\Rightarrow \lambda$ is well defined$]$

<u>Claim</u>: $f = \bar{\lambda}_\emptyset \quad . \quad [\bar{\lambda} \neq \lambda]$. For induction on $n =$ lenght of w

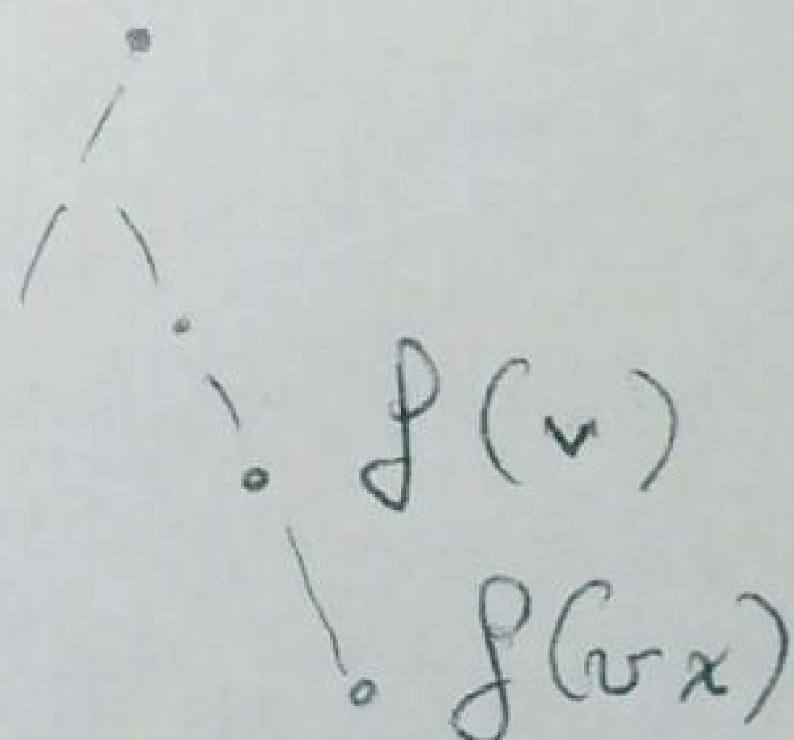
<u>$n=0$</u>: $\bar{\lambda}(\emptyset, \emptyset) = \emptyset = f(\emptyset)$ ✓

<u>$n \rightsquigarrow n+1$</u>: if $w \in X^* \setminus \{\emptyset\}$, w can be written as $\underset{X^*}{v}\underset{X}{x}$.

$$\bar{\lambda}(\emptyset, vx) \underset{\substack{\uparrow \\ \text{pag}(3)}}{=} \bar{\lambda}(\emptyset, v) \cdot \bar{\lambda}(\pi(\emptyset, v), x) = f(v) \cdot \bar{\lambda}(\text{[redacted]} \overset{v}{}, x) =$$

$$= f(v) \cdot [f(vx) - f(v)]$$

$f(vx)$ ✓



<u>Povzetek</u>:

Automata $\mathcal{A}$ $\rightsquigarrow$ init. Automata $\mathcal{A}_q$ $\longmapsto$ Actions $f = \bar{\lambda}_q$ $\longleftrightarrow$ tree Autom. on X^*

<u>DEF</u> Given $\mathcal{A}$ automaton, we define the <u>GROUP GENERATED BY $\mathcal{A}$</u>, as the group whose generators are the actions of all the possible Initial Automata definable on $\mathcal{A}$

i.e. $G\mathcal{A}(\lambda) := \langle \{ \bar{\lambda}_q : X^* \to X^* \mid q \in Q \} \rangle$

<u>Ex:</u> Automaton on page 3 defines a group with 3 generators

Proposition Let $\mathcal{A}$ be a 2-state automaton ($|Q|=2$) over $X=\{0,1\}$. Then $G\mathcal{A}(X)$ is 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) $\mathbb{D}_\infty = \{\text{symmetries of the circle}\}$

(6) $L_2 = \mathbb{Z} \wr \mathbb{Z}_2 =$ Lamplighter group

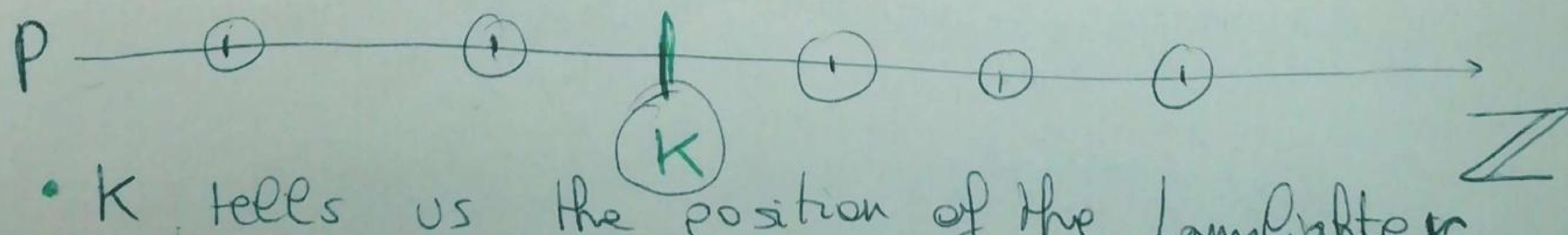
What is L_2?

$$L_2 := \left\{ \begin{pmatrix} y^k & p \\ 0 & 1 \end{pmatrix} \middle| \begin{array}{l} k \in \mathbb{Z} \\ p \in \mathbb{Z}_2[y^{-1}; y] \end{array} \right\}$$ with the usual matrix product

How do we visualise it?

- If $p = a_{-n} y^{-n} + \dots + a_0 + a_1 y + \dots + a_m y^m$, where $a_i \in \mathbb{Z}_2$

  we see it as a straight line, with "lights on" on the indexes j where $a_j = 1$



- K tells us the position of the Lamplighter

How do we visualise this product?

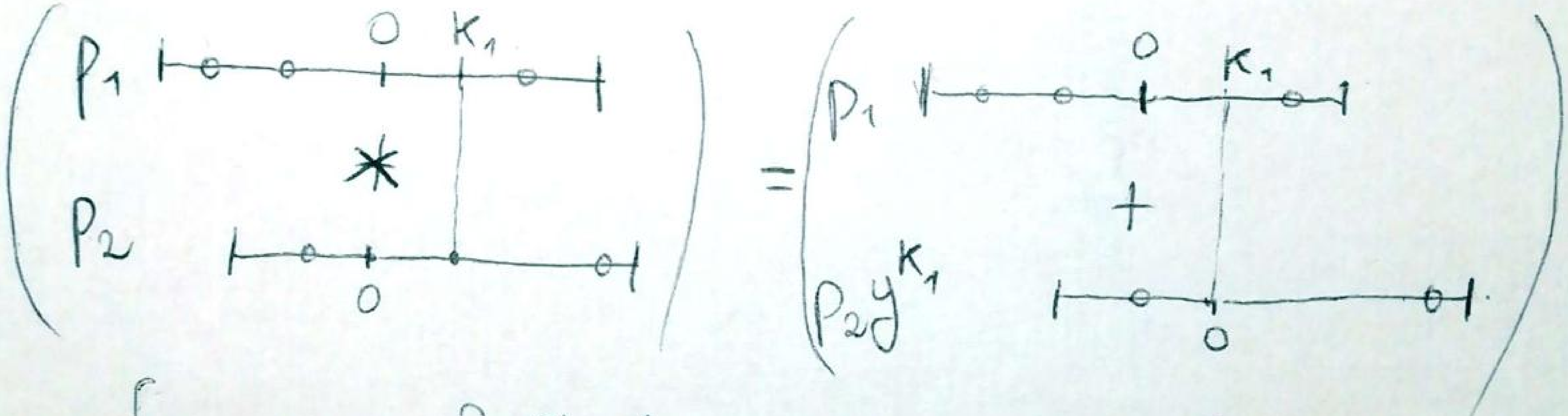
Formally: $\begin{pmatrix} y^{k_1} & p_1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} y^{k_2} & p_2 \\ 0 & 1 \end{pmatrix} = \begin{bmatrix} y^{k_1+k_2} & p_1 + y^{k_1} \cdot p_2 \\ 0 & 1 \end{bmatrix}$

Informally:

- 1st component:

  $k_1 + k_2$ sum in $\mathbb{Z}_2$

- 2nd component:



[p_2 is shifted to the right]

Corollary $\exists\, \mathcal{A}$ s.t. $G\mathcal{A}(X) \simeq \mathcal{L}_2$

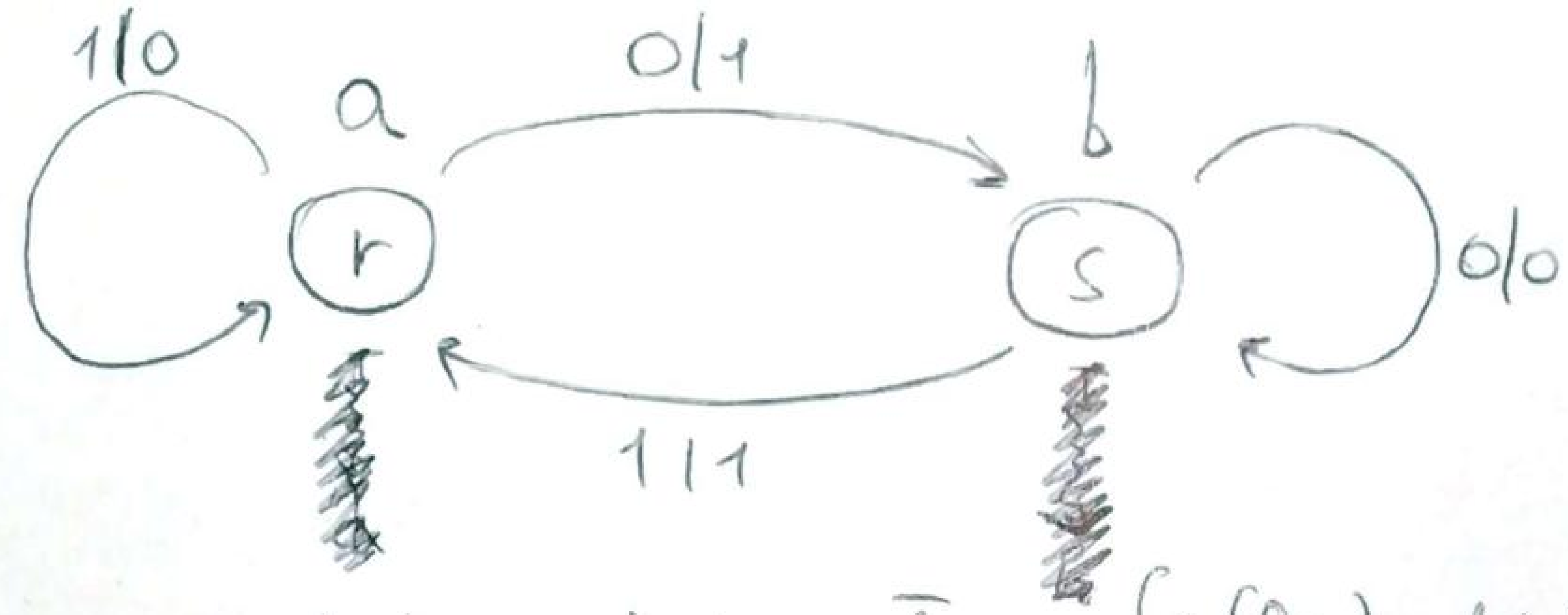
Proof (1) We define $\mathcal{A}$ and we analyse all the actions $\tilde{\lambda}_q$

(2) We project the generators in another environment, and we construct a group T isomorphic to $G\mathcal{A}(X)$

(3) We proove that this group T is $\mathcal{L}_2$

1st Part

$\mathcal{A}$ is defined by this diagram:



$X = \{0,1\} = \mathbb{Z}_2$

$Q = \{r, s\}$

$a :=$ Action of $A_r = \bar{\lambda}_r = \begin{cases} a(0v) = 1\, b(v) \\ a(1v) = 0\, a(v) \end{cases}$ [Observe $\lambda_r = \sigma \in S_2$]

$b :=$ Action of $A_s = \bar{\lambda}_s = \begin{cases} b(0v) = 0\, b(v) \\ b(1v) = 1\, a(v) \end{cases}$ [Observe $\lambda_s = \underset{\shortparallel}{\overset{1_{S_2}}{}} id \in S_2$]

We observe $b^{-1} = \begin{cases} b^{-1}(0v) = 0\, b^{-1}(v) \\ b^{-1}(1v) = 1\, a^{-1}(v) \end{cases}$

$c := b^{-1} \cdot a = a \circ b^{-1}$ $\qquad c(w) = ?$

$$\begin{cases} c(0v) = a \circ b^{-1}(0v) = a(0 . b^{-1}(v)) = 1 . b \circ b^{-1}(v) = 1 . v \\ c(1v) = a \circ b^{-1}(1v) = a(1 . a^{-1}(v)) = 0 . a \circ a^{-1}(v) = 0 . v \end{cases}$$

$\Longrightarrow \boxed{c(x_1 x_2 x_3 \text{—}) = (x_1 + 1) x_2 x_3 \text{—}}$

[In Fact from now on $X = \mathbb{Z}_2$]

¿Why do we analyse c?

$\langle a, b \rangle = \langle b^{-1}, b, a \rangle = \langle b^{-1}a, b \rangle = \langle c, b \rangle$

$b^{-1} \cdot a$

So $G\mathcal{A}(X) = \langle a, b\rangle = \langle b, c\rangle$

We want an explicit formula for b:

$$b(x_1 x_2 x_3 \cdot \text{---}) = y_1 y_2 y_3 \cdot \text{---} \qquad (y_n = ?)$$

We claim
$$\begin{cases} (A) & b(x_1 \cdot \text{---} \cdot x_n \overset{(n+1)}{0} x_{n+2} \text{---}) = y_1 \text{---} y_n y_{n+1} b(x_{n+2} \text{---}) \\ (B) & b(x_1 \cdot \text{---} \cdot x_n \overset{(n+1)}{1} x_{n+2} \text{---}) = y_1 \text{---} y_n y_{n+1} b(x_{n+2} \text{---}) \end{cases}$$

(A): Watching the diagram.
Whenever we encounter a 0, if we are in "r" or in "s", we travel to "s"
$\Rightarrow$ acts b

(B) ~~Analog~~ Similarly:
Whenever we encounter a 1, if we are in "r" or in "s", we travel to "r"
$\Rightarrow$ acts a

✓

We claim

$$b(x_1 x_2 \cdot \text{---} \cdot x_n) = \overbrace{x_1}^{y_1} \overbrace{(x_2 + x_1)}^{y_2} \cdot \text{---} \cdot \overbrace{(x_n + x_{n-1})}^{y_n}$$

We proove it by induction on n.
Adding the condition $x_0 = 0$, our thesis is:

$$y_n = x_n + x_{n-1} \quad \forall n \geq 1$$

$\underline{n=1}$: $b(x_1 x_2 -) = x_1 y_2 - = (x_1 + 0) y_2 - =$

$= (x_1 + x_0) y_2 -$

$\underline{n \Rightarrow n+1}$: $y_1 = x_1 + x_0$, $y_2 = x_2 + x_1$, $-$, $y_n = x_n + x_{n-1}$

$y_{n+1} = ?$

We see four cases $x_n x_{n+1} \in \{00, 01, 10, 11\}$

(1) 00 then $b(x_1 - x_{n-1} 0 0 x_{n+2} -) \overset{(A)}{=} y_1 - y_{n-1} \cdot y_n \, b(0 x_{n+2} -) =$

$= y_1 - y_{n-1} y_n 0 \cdot b(x_{n+2} -)$

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

(2) 01 then $b(x_1 - x_{n-1} 0 1 x_{n+2} -) \overset{(A)}{=} y_1 - y_{n-1} y_n \, b(1 x_{n+2} -) =$

$= y_1 - y_{n-1} y_n 1 \cdot a(x_{n+2} -)$

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

(3) 10 then $b(x_1 - x_{n-1} 1 0 x_{n+2} -) \overset{(B)}{=} y_1 - y_{n-1} y_n \, a(0 x_{n+2} -) =$

$= y_1 - y_{n-1} y_n 1 \cdot a(x_{n+2} -)$

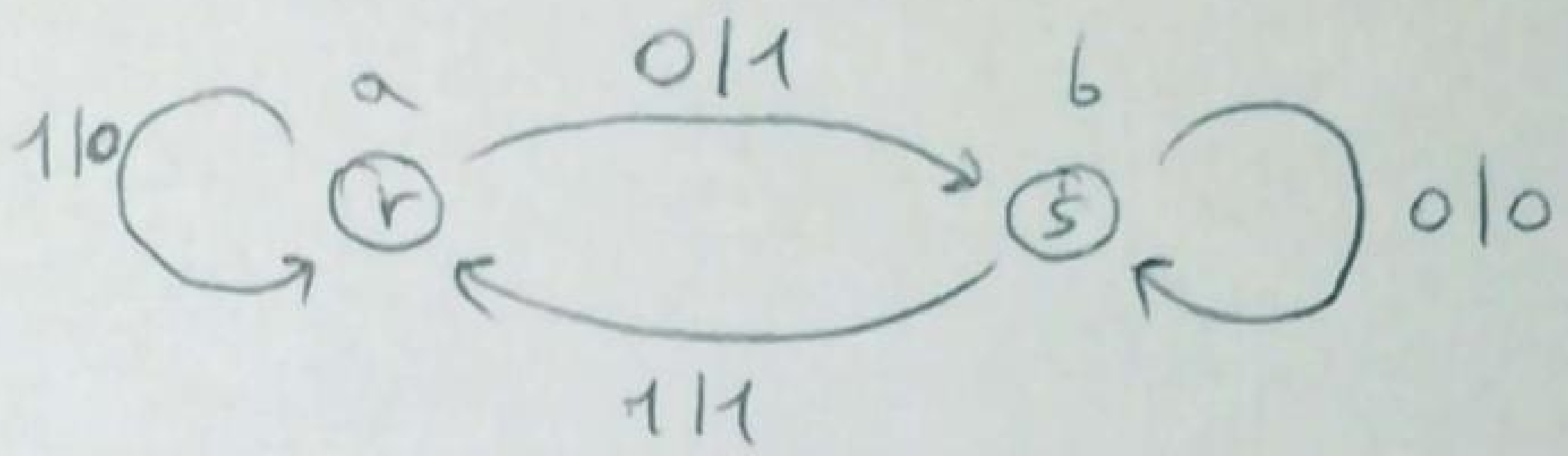
$[y_{n+1} = 1 = 1 + 0 = x_n + x_{n+1}]$

(4) 11 then $b(x_1 - x_{n-1} 1 1 x_{n+2} -) \overset{(B)}{=} y_1 - y_{n-1} y_n \, a(1 x_{n+2} -)$

$= y_1 - y_{n-1} y_n 0 \cdot a(x_{n+2} -)$ $\quad [y_{n+1} = 0 = 1 + 1]$

✓

Povzetek:

$\mathcal{A} :=$ 

$$\begin{cases} a := \bar{\lambda}_r \\ b := \bar{\lambda}_s \end{cases} \Longrightarrow G\mathcal{A}(X) = \langle a, b \rangle =$$

$$= \langle \underbrace{b^{-1}a}_{a \circ b^{-1} : X^* \longrightarrow X^*}, b \rangle = \langle c, b \rangle$$

$$\begin{cases} c(x_1 x_2 x_3 x_4 \text{—}) = (x_1 + 1) x_2 x_3 x_4 \text{—} \\ b(x_1 x_2 x_3 x_4 \text{—}) = x_1 (x_2 + x_1)(x_3 + x_2)(x_4 + x_3) \text{—} \end{cases}$$

2nd Part:

$\forall \; w = x_1 x_2 x_3 - \in X^*$ we can associate

$F(t) = x_1 + x_2 t + x_3 t^2 + - \in \mathbb{Z}_2[[t]]$

$\uparrow$

Formal Power Series on $\mathbb{Z}_2$
(Infinite polinomials)

$$\begin{array}{ccccccc} b & , & c & : & X^* & \longrightarrow & X^* \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \phi_b & , & \phi_c & : & \mathbb{Z}_2[[t]] & \longrightarrow & \mathbb{Z}_2[[t]] \end{array}$$

We study $\langle \phi_b ; \phi_c \rangle \simeq \langle b, c \rangle$

So $\phi_b : \mathbb{Z}_2[[t]] \to \mathbb{Z}_2[[t]]$

$$\phi_b(F(t)) = \phi_b\left(x_1 + x_2 t + x_3 t^2 + x_4 t^3 + \ldots + x_n t^{n-1} + \ldots\right) =$$

$$= x_1 + (x_2 + x_1)t + (x_3 + x_2)t^2 + \ldots + (x_n + x_{n-1})t^{n-1} + \ldots$$

$$= x_1 + x_2 t + \ldots + x_n t^{n-1} + \ldots$$

$$+ \quad x_1 t + \ldots + x_{n-1} t + \ldots$$

$$= (1+t)\left[x_1 + x_2 t + \ldots + x_n t^{n-1} + \ldots\right] = (1+t)F(t)$$

$$\phi_c(F(t)) = \phi_c\left(x_1 + x_2 t + \ldots\right) = (x_1 + 1) + x_2 t + \ldots =$$

$$= F(t) + 1$$

We notice $\phi_c \circ \phi_c(F(t)) = F(t) + \underbrace{1+1}_{0 \in \mathbb{Z}_2} = F(t)$

$$\Rightarrow \phi_c^2 = id \Rightarrow \phi_c^{-1} = \phi_c$$

$\phi_b^{-1} = ?$ $\quad \left[\text{Heuristically: } \phi_b^{-1}(F(t)) = (1+t)^{-1} F(t)\right]$

$(1+t)^{-1} := (1+t+t^2+ \text{——})$ $\quad \left[\Rightarrow \phi_b^{-1}(\mathbb{Z}_2[[t]]) \subseteq \mathbb{Z}_2[[t]]\right]$

$$\phi_b^{-1} \circ \phi_b(F(t)) = \phi_b^{-1}\left(x_1 + (x_2+x_1)t + (x_3+x_2)t^2 + \text{——} + (x_n+x_{n-1})t^{n-1} + \text{-}\right)$$

$$= (1+t+t^2+\text{—}) \cdot \left[x_1 + (x_2+x_1)t + (x_3+x_2)t^2 + \text{—} + (x_n+x_{n-1})t^{n-1} + \text{—}\right] =$$

$$= x_1 + (x_2+x_1)t + (x_3+x_2)t^2 + \text{——} + (x_n+x_{n-1})t^{n-1} + \text{—}$$

$$0 \quad x_1 t + (x_2+x_1)t^2 + \text{——} + (x_{n-1}+x_{n-2})t^{n-1} + \text{—}$$

$$0 \quad 0$$

$$0 \qquad x_1 \cdot t^{n-1} + \text{—}$$

$$= x_1 + (x_2 + \underbrace{x_1 + x_1}) t + (x_3 + \underbrace{x_2 + x_2} + \underbrace{x_1 + x_1}) t^2 + \text{——}$$

$$\text{——} + (x_n + \underbrace{x_{n-1} + x_{n-1}} + \text{——} + \underbrace{x_2 + x_2} + \underbrace{x_1 + x_1}) t^{n-1} \text{——}$$

$\left[\text{Notice } \mathbb{Z}_2 : \; 0 = -0, \; 1 = -1 \Rightarrow x = -x\right]$

$$= x_1 + (x_2 + x_1 - x_1)t + (x_3 + x_2 - x_2 + x_1 - x_1)t^2 + \text{——}$$

$$\overset{!}{=} x_1 + x_2 t + x_3 t^2 + \text{——} = F(t)$$

So $\begin{cases} \phi_b(F(t)) = F(t)(1+t) \\ \phi_b^{-1}(F(t)) = F(t)(1+t)^{-1} \\ \phi_c(F(t)) = F(t)+1 \end{cases}$ $\Rightarrow \phi_b^{z}(F(t)) = F(t)(1+t)^{z}$

<u>Ex]</u>: $\phi_b^3(F(t)) = F(t)(1+t)^3$

We observe the set T:

$$T := \left\{ \begin{array}{l} L : \mathbb{Z}_2[[t]] \longrightarrow \mathbb{Z}_2[[t]] \\ L(F(t)) = \underbrace{(1+t)^n F(t)}_{G(t)} + p \end{array} \middle| \begin{array}{l} n \in \mathbb{Z} \\ p \in \mathbb{Z}_2[(1+t)^{-1}; (1+t)] \end{array} \right\}$$

T is a group, and $\underset{(n=1,\, p=0)}{\phi_b}, \underset{(n=0,\, p=1)}{\phi_c} \in T$

$\Longrightarrow \langle \phi_b ; \phi_c \rangle \leqslant T$.

We want to prove $T = \langle \phi_b, \phi_c \rangle$

We notice $G(t) = \phi_b^n(F(t))$.

$\Rightarrow$ If we find $\mathcal{U}_p \in \langle \phi_b, \phi_c \rangle$ s.t.

$\mathcal{U}_p(G(t)) = G(t) + p$, we have

$(\mathcal{U}_p \circ \phi_b^n)(F(t)) = L(F(t)) \Longrightarrow \langle \phi_b, \phi_c \rangle = T$

¿How to build $\mathcal{U}_p$?

Given $p = x_{-q}(1+t)^{-q} + \text{—} + x_k(1+t)^k$

we have $I \subseteq \{-q, -, k\}$, the set ~~where~~ of indexes i in which $x_i \neq 0$ $(\Rightarrow x_i = 1)$

$$\mathcal{U}_p = \left(\bigcirc_{i\in I} \mathcal{U}_{p_i} \right), \text{ where } p_i = (1+t)^{+i}$$

$\uparrow$ composition $\left[\mathcal{U}_p(G(t)) = G(t) + p = G(t) + \sum_{i\in I} (1+t)^{+i} \right]$

So we need to build $\mathcal{U}_{p_i}$!

$$\left(\phi_b^{-i} \circ \phi_c \circ \phi_b^{i}\right)\left[F(t)\right] = \left(\phi_b^{-i} \circ \phi_c\right)\left[(1+t)^{-i} \cdot F(t)\right] =$$

$$= \phi_b^{-i}\left[(1+t)^{-i} F(t) + 1\right] = F(t) + (1+t)^{i} = \mathcal{U}_{p_i}\left(F(t)\right)$$

$\Rightarrow$ we can generate $\mathcal{U}_{p_i}$ $\forall i$, $\Rightarrow \mathcal{U}_p \in \langle \phi_b, \phi_c \rangle$

$\Rightarrow \left(\mathcal{U}_p \circ \phi_b^{n}\right) = L \in \langle \phi_b ; \phi_c \rangle \Rightarrow T = \langle \phi_b, \phi_c \rangle$

Porzetek :

$$\underbrace{\overbrace{\boxed{\quad | \quad | \; \mathcal{U}_{p_i} \; | \quad | \quad}}^{\mathcal{U}_p}\boxed{\phi_b^{n}}}_{L}$$

$$A \left\langle \begin{matrix} a = \bar{\lambda}_r \\ b = \bar{\lambda}_s \end{matrix} \right\rangle = \langle b, c \rangle \simeq \langle \phi_b ; \phi_c \rangle = T$$

3rd part :

$$T \simeq L_2$$

we identify $(1+t)$ with y

$$\Gamma : T \longrightarrow L_2$$

$$L(F(t)) = (1+t)^n F(t) + p(1+t) \longmapsto \begin{pmatrix} y^n & p(y) \\ 0 & 1 \end{pmatrix}$$

(1) Injective?

if $L_1 \neq L_2 \Rightarrow (n_1 \neq n_2) \vee (p_1 \neq p_2)$

$$\Rightarrow \begin{pmatrix} y^{n_1} & p_1 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} y^{n_2} & p_2 \\ 0 & 1 \end{pmatrix}$$

(2) Surjective?

$\forall n \in \mathbb{Z},\ p \in \mathbb{Z}_2[y^{-1}; y]$

$$L(F(t)) := (1+t)^n F(t) + p(1+t) \longmapsto \begin{pmatrix} y^n & p(y) \\ 0 & 1 \end{pmatrix}$$

(3) Homomorph?

$$\begin{cases} L_1(F(t)) = (1+t)^{n_1} F(t) + p_1 \\ L_2(F(t)) = (1+t)^{n_2} F(t) + p_2 \end{cases} \Rightarrow$$

$$\Rightarrow (L_1 \circ L_2)(F(t)) = L_1\left((1+t)^{n_2} F(t) + p_2\right) = (1+t)^{n_1+n_2} F(t) + (1+t)^{n_1} p_2 + p_1$$

is mapped in $\begin{pmatrix} y^{n_1+n_2} & y^{n_1} p_2 + p_1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} y^{n_1} & p_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y^{n_2} & p_2 \\ 0 & 1 \end{pmatrix}$ ∎

THANK YOU ALL
FOR YOUR
ATTENTION !