Des automates au service de la théorie combinatoire des groupes

Ines Klimann

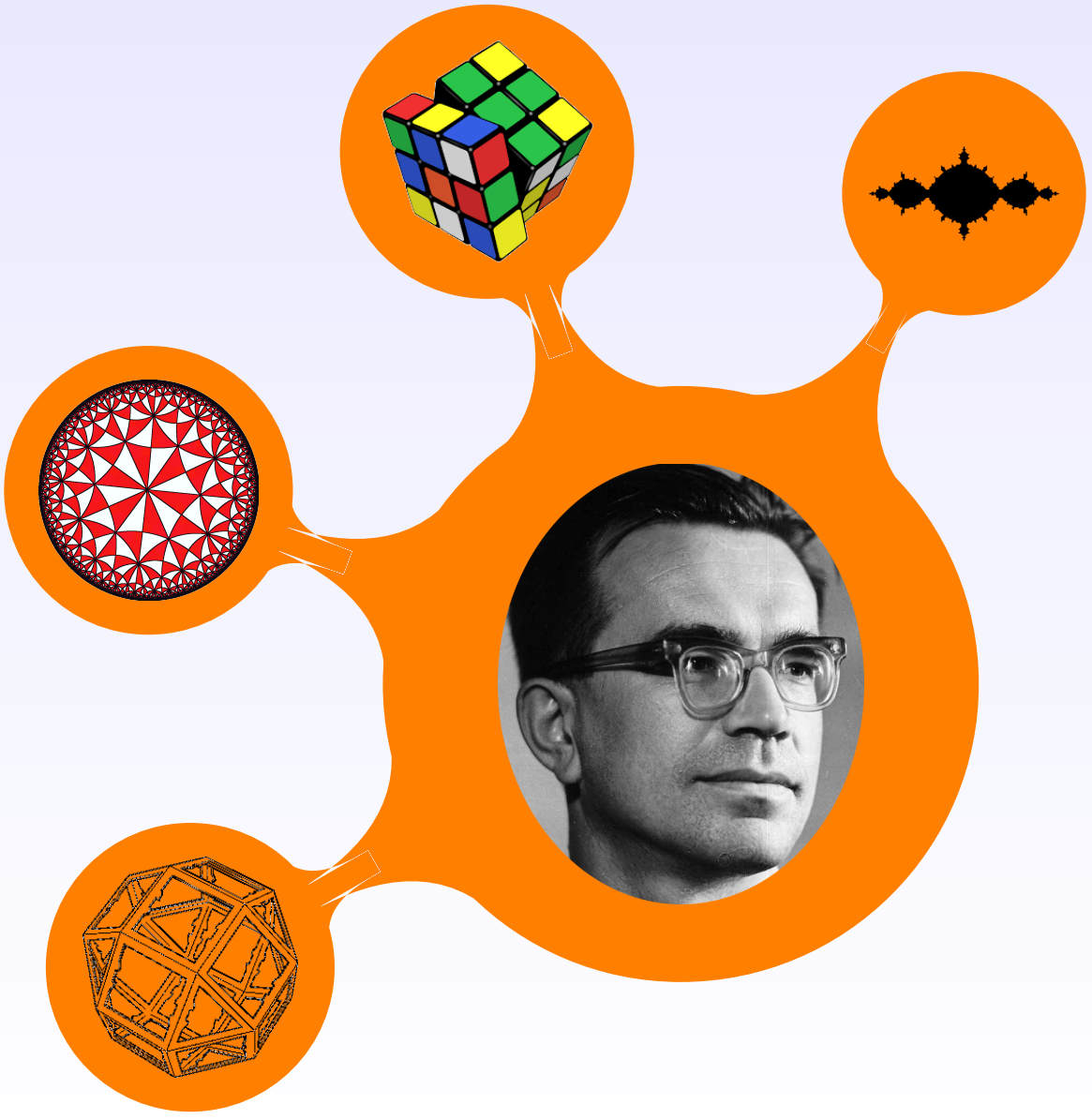
IRIF – UMR 8243 CNRS & Université Paris Diderot

MealyM
JCJC-12-JS02-012-01

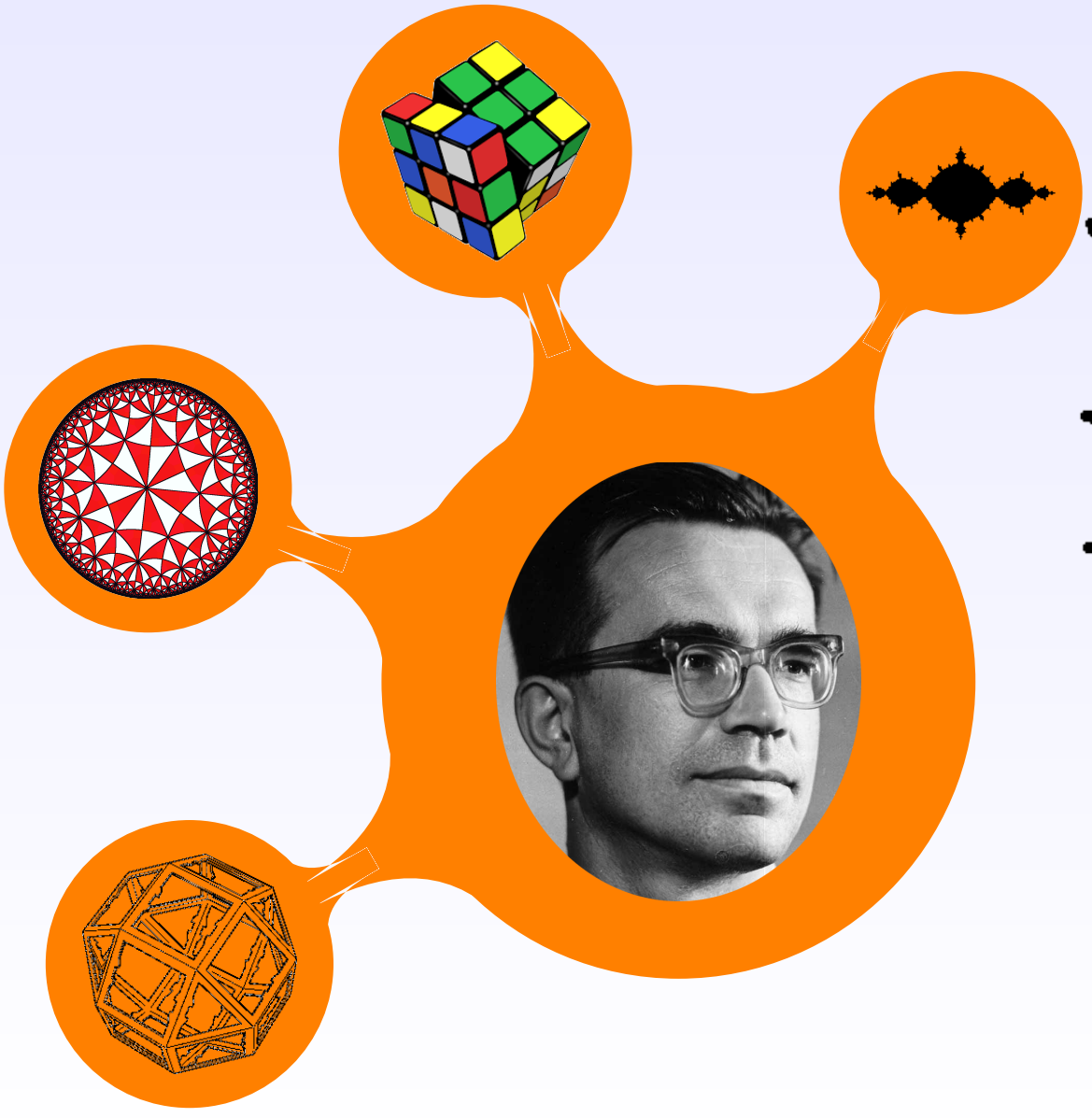
Burnside

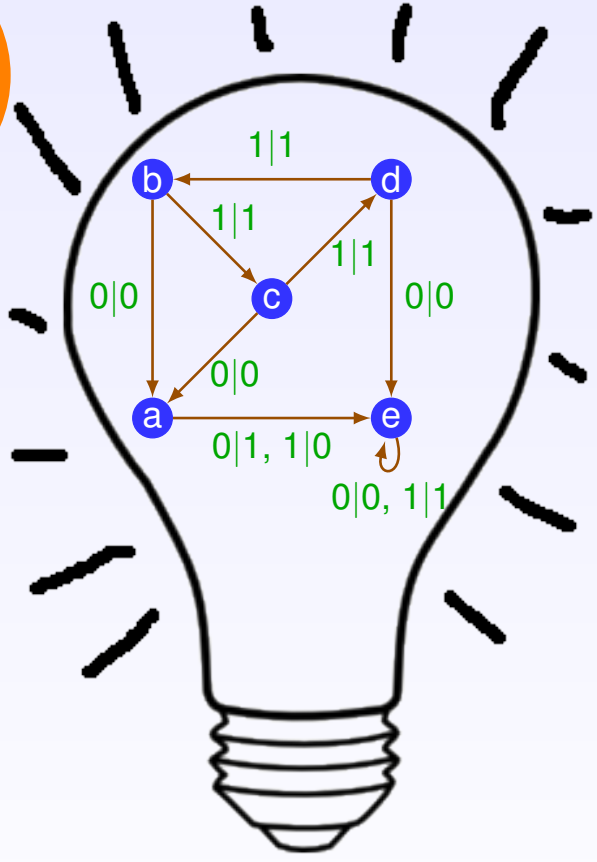
Milnor

1961

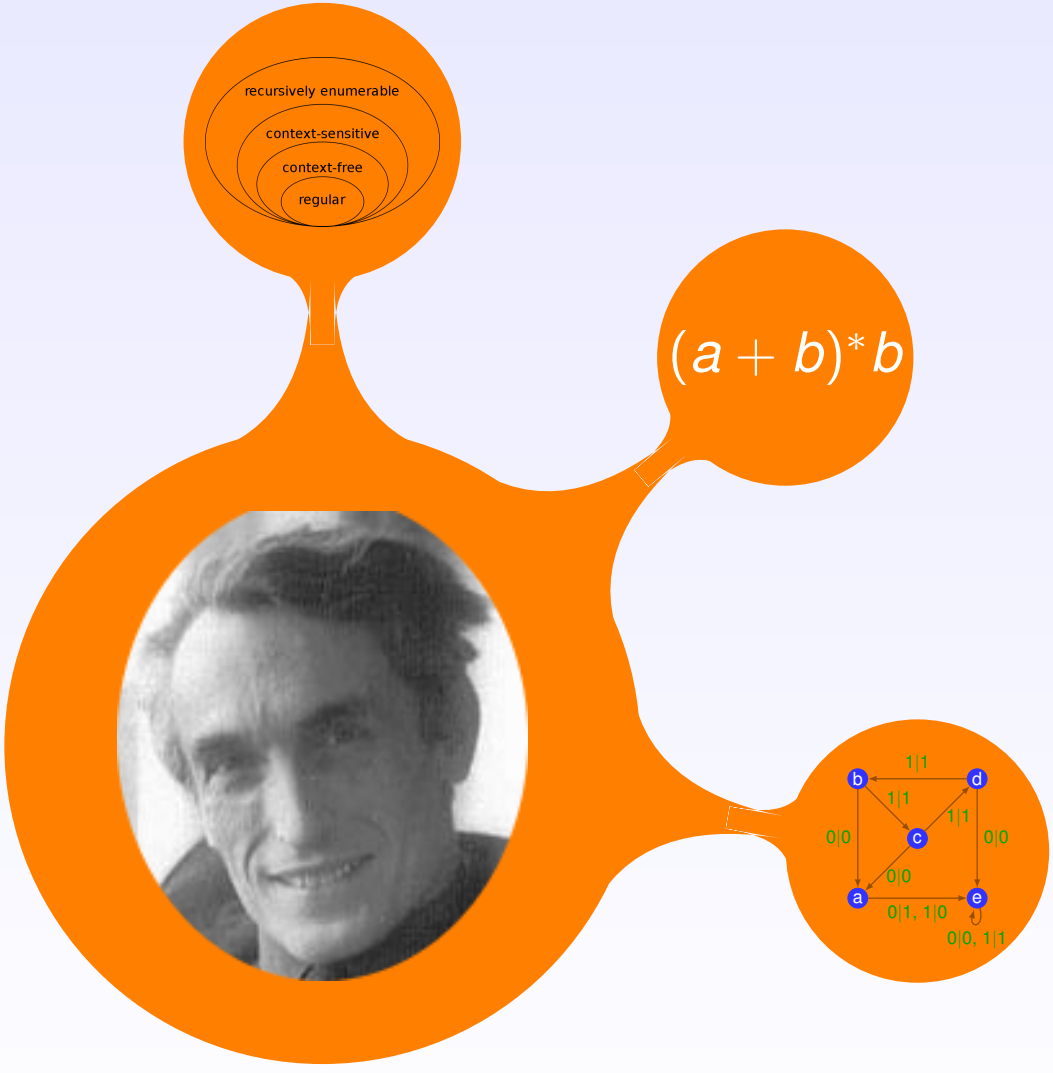


1961

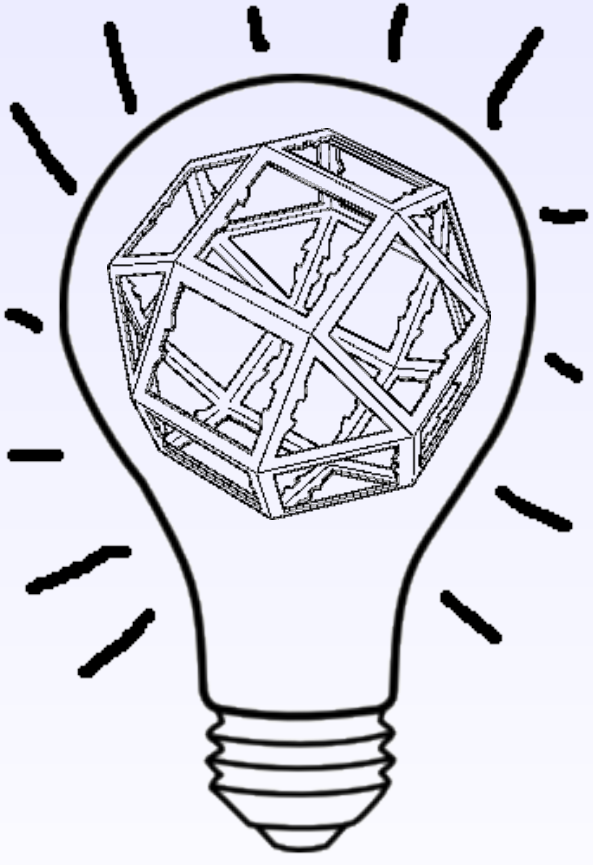


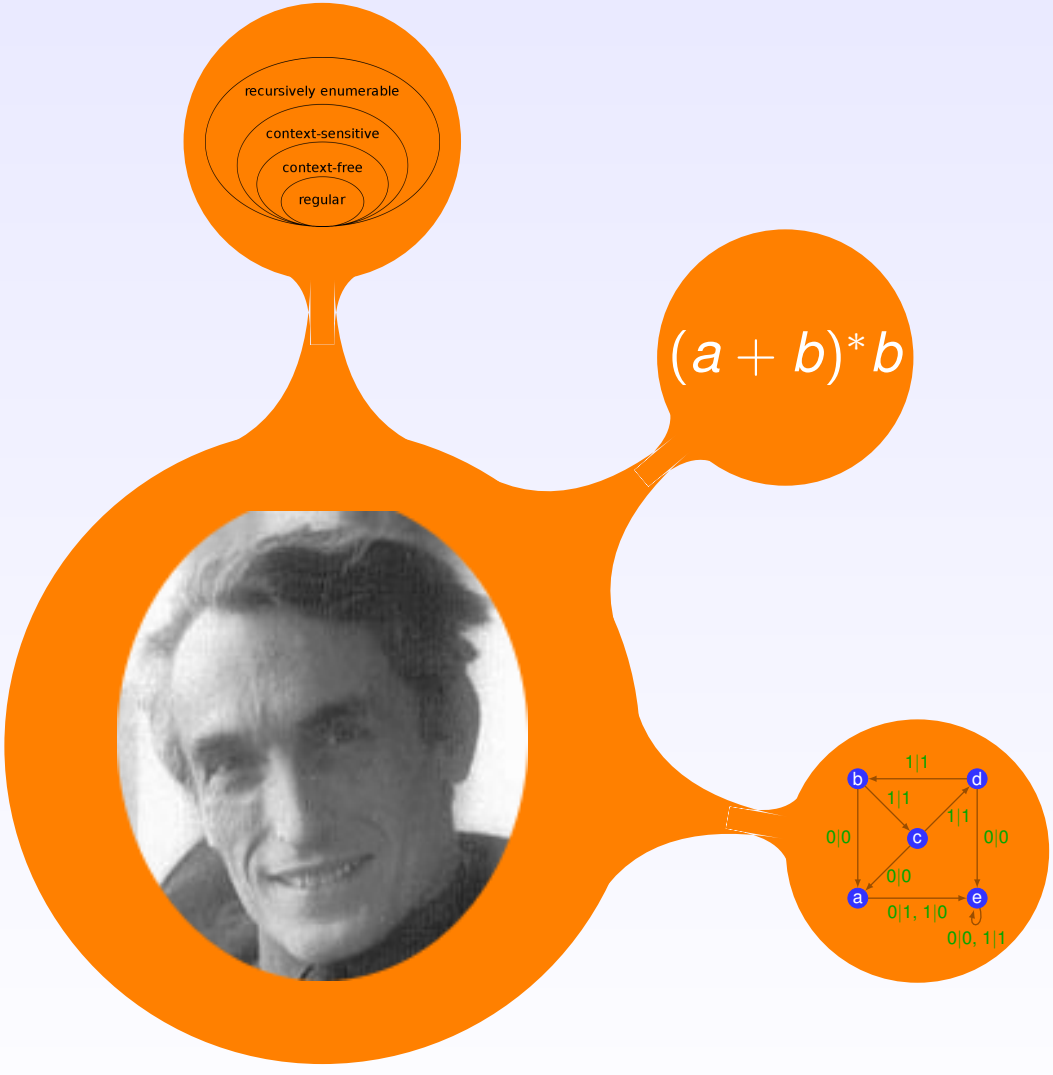


1956

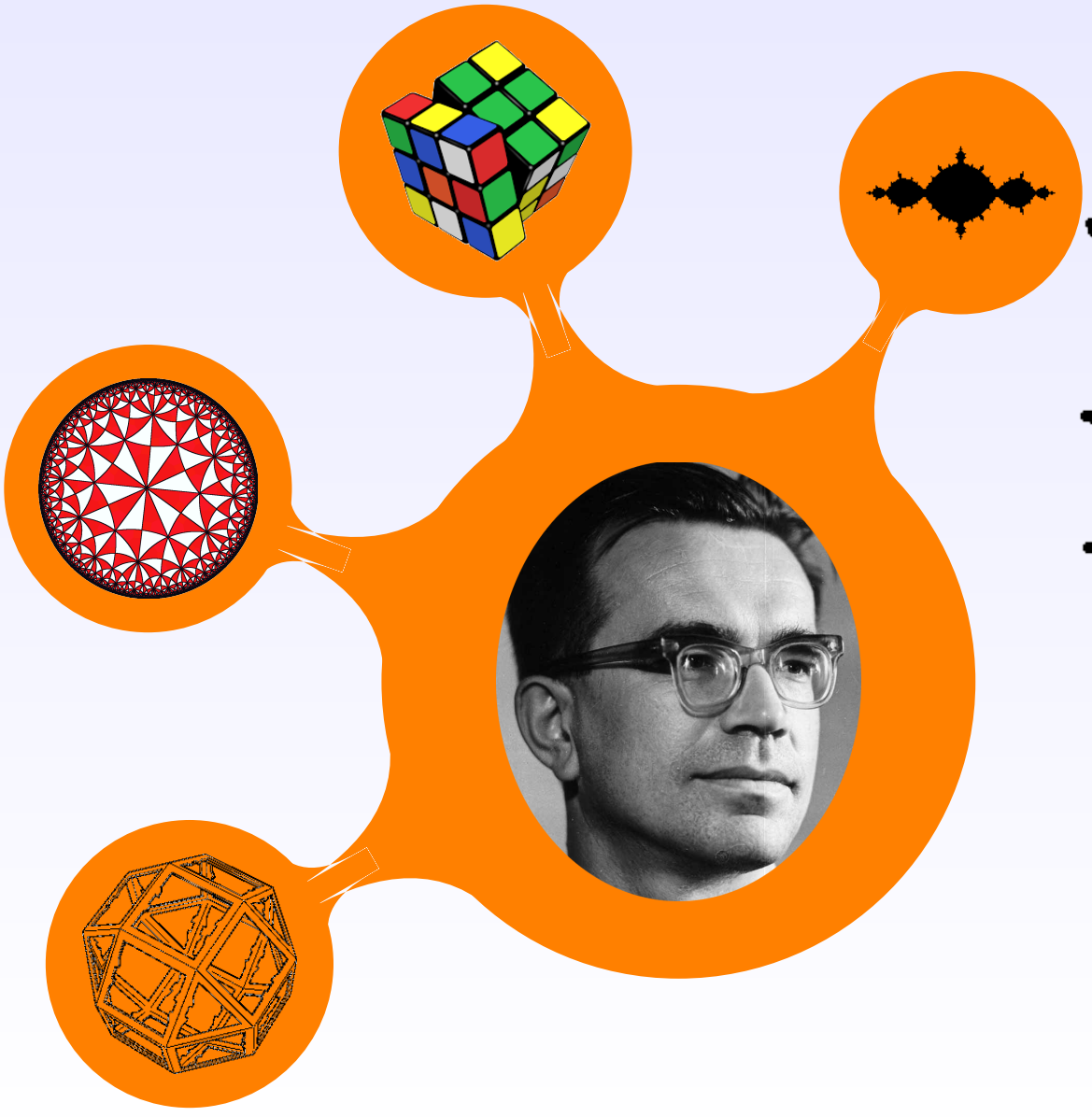

recursively enumerable
context-sensitive
context-free
regular
$(a+b)^*b$
b
d
c
a
e
1|1
1|1
1|1
0|0
0|0
0|0
0|1, 1|0
0|0, 1|1

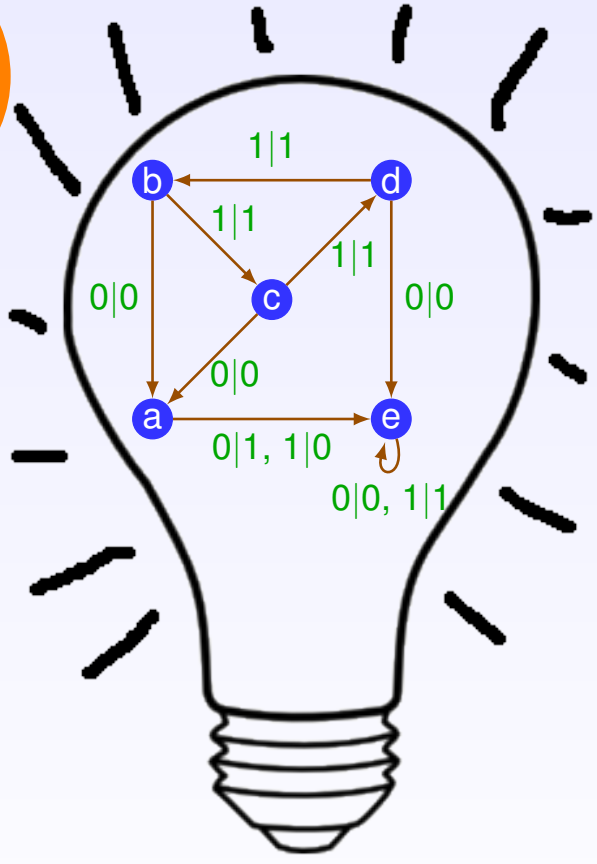
1956




recursively enumerable
context-sensitive
context-free
regular
$(a+b)^*b$
b
d
c
a
e
1|1
1|1
1|1
0|0
0|0
0|1, 1|0
0|0, 1|1

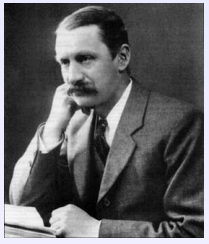
1961





1902

Un groupe finiment engendré dont tous les éléments sont d'ordre fini est-il fini ?



Burnside

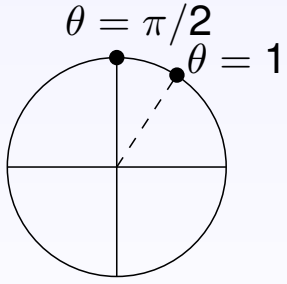
Ordre d'un élément

$$x \in G \text{ d'ordre fini } \iff \exists n \geq 1, x^n = \mathbb{1}$$

Ordre d'un élément

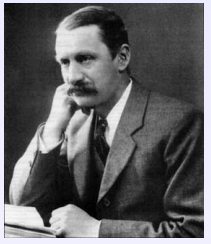
$$x \in G \text{ d'ordre fini } \iff \exists n \geq 1, x^n = \mathbb{1}$$

- $\mathbb{Z}/n\mathbb{Z}$: tout élément d'ordre fini
- $\mathbb{Z}$: seul 0 d'ordre fini
- $\mathbb{R}/2\pi\mathbb{Z}$: $\pi/2$ d'ordre fini — 1 d'ordre infini



1902

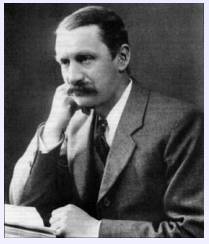
Un groupe finiment engendré dont tous les éléments sont d'ordre fini est-il fini ?



Burnside

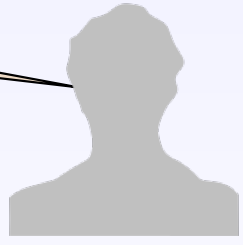
1902 1964

Un groupe finiment engendré dont tous les éléments sont d'ordre fini est-il fini ?

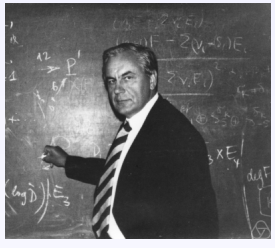


Burnside

Non!



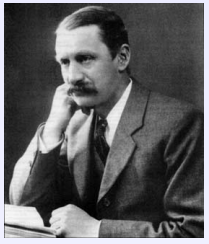
Golod



Shafarevich

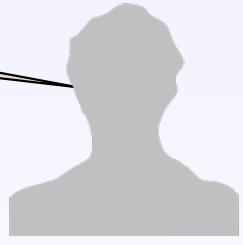
1902 — 1964 — 1968

Un groupe finiment engendré dont tous les éléments sont d'ordre fini est-il fini ?

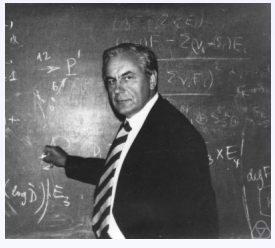


Burnside

Non!

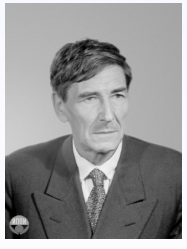


Golod

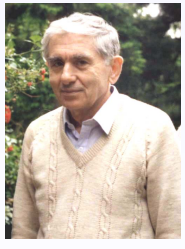


Shafarevich

Même si les ordres sont bornés



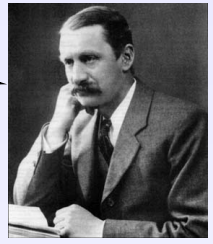
Novikov



Adian

1902 — 1964 — 1968

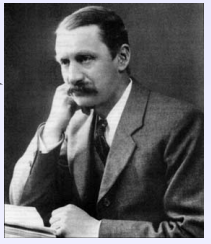
Un groupe finiment engendré dont tous les éléments sont d'ordre fini est-il fini ?



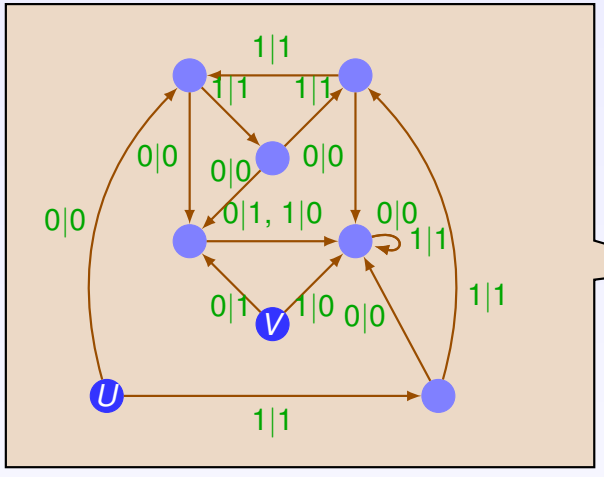
Burnside

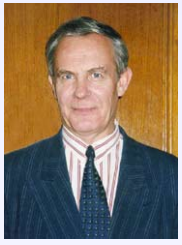
1902 1964 1972 1968

Un groupe finiment engendré dont tous les éléments sont d'ordre fini est-il fini ?



Burnside

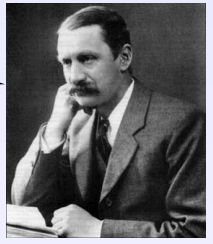




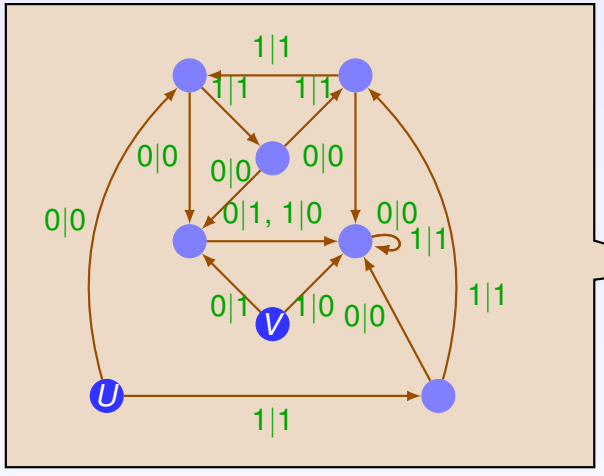
Aleshin

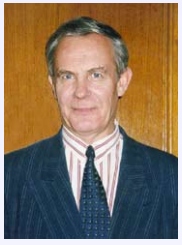
1902 — 1964 1972 1980 — 1968

Un groupe finiment engendré dont tous les éléments sont d'ordre fini est-il fini ?

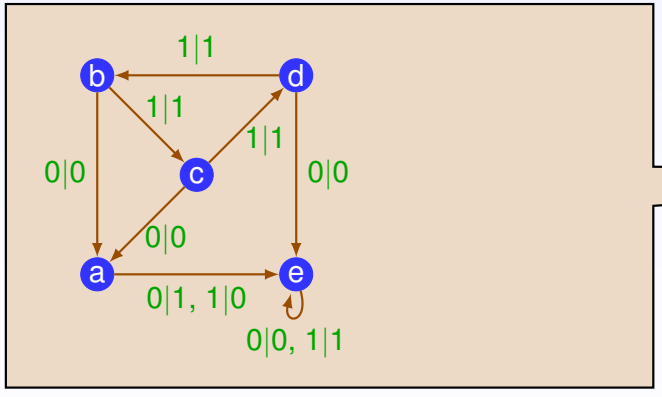


Burnside





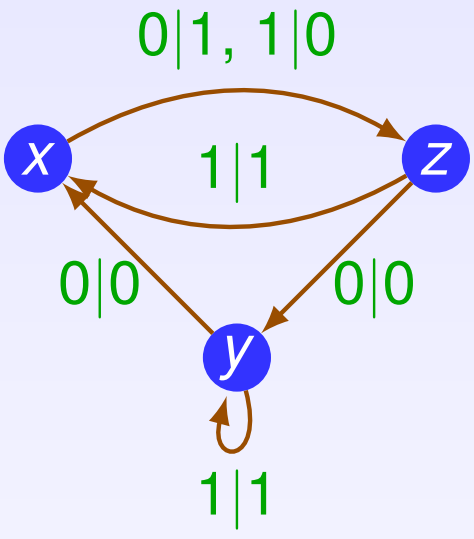
Aleshin



Grigorchuk

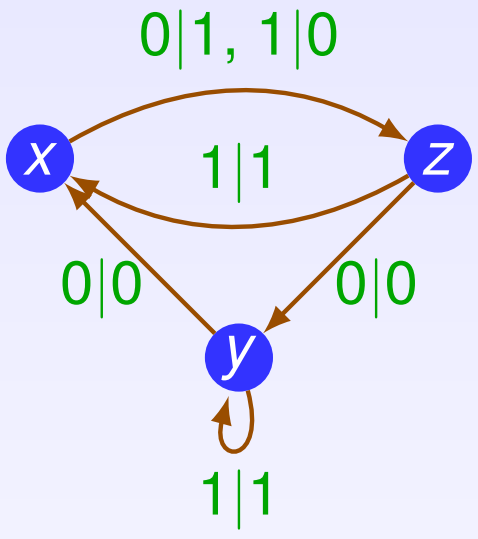
(Semi-)groupes d'automate

$\mathcal{A}$



(Semi-)groupes d'automate

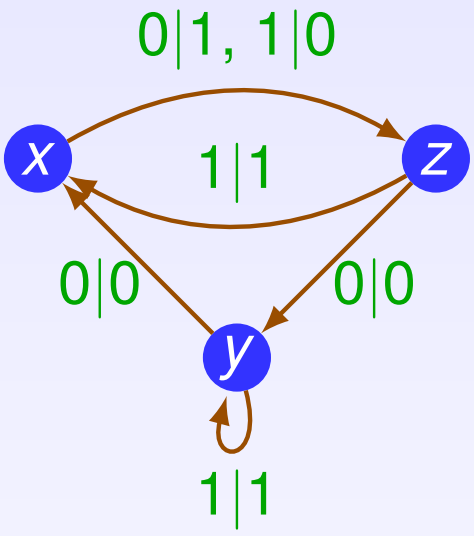
$\mathcal{A}$



ρ_x : 01000 $\mapsto$ 11100

(Semi-)groupes d'automate

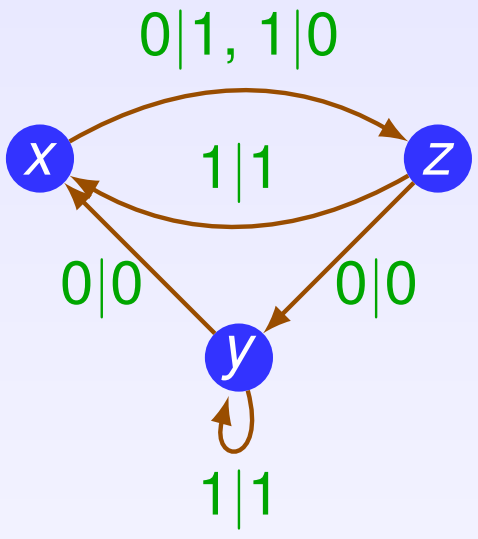
$\mathcal{A}$



ρ_x : $01000 \mapsto 11100$

$\Sigma^* \to \Sigma^*$

(Semi-)groupes d'automate



$\mathcal{A}$

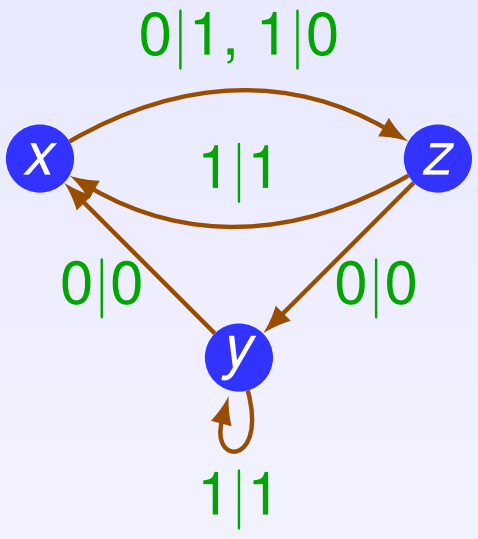
- déterministe [fonction]
- complet [défini sur tout Σ^*]

$\langle \mathcal{A} \rangle_+$ semi-groupe

ρ_x : $01000 \mapsto 11100$

$\Sigma^* \to \Sigma^*$

(Semi-)groupes d'automate



$\mathcal{A}$

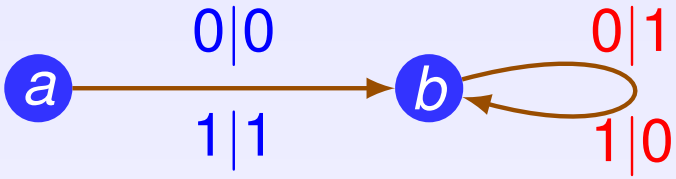
- déterministe [fonction]
- complet [défini sur tout Σ^*]
- les états permutent l'alphabet [pour les groupes]

$\langle \mathcal{A} \rangle_+$ semi-groupe
$\langle \mathcal{A} \rangle$ groupe

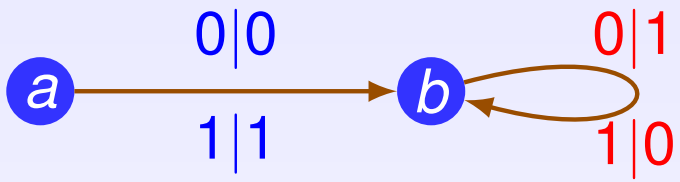
ρ_x : $01000 \mapsto 11100$

$\Sigma^* \to \Sigma^*$

Des exemples



Des exemples



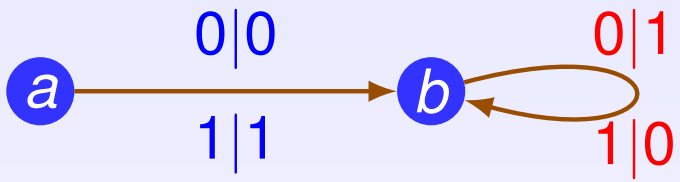
ρ_b :

001110010101 . . . 101110010101 . . .

↧ ↧

110001101010 . . . 010001101010 . . .

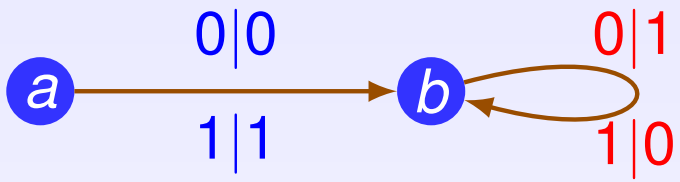
Des exemples



$$\rho_b : \begin{array}{c} 001110010101\ldots \quad 101110010101\ldots \\ \downarrow \qquad\qquad \downarrow \\ 110001101010\ldots \quad 010001101010\ldots \end{array}$$

$$\rho_b^2 = \mathrm{id}_{\Sigma^*}$$

Des exemples



ρ_a :

001110010101 . . . 101110010101 . . .

↧ ↧

010001101010 . . . 110001101010 . . .

ρ_b :

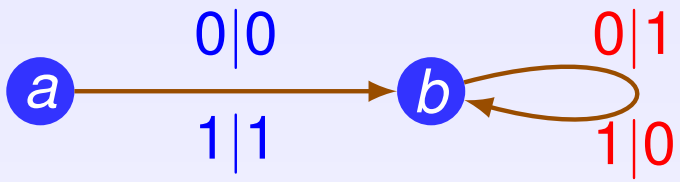
001110010101 . . . 101110010101 . . .

↧ ↧

110001101010 . . . 010001101010 . . .

$\rho_b^2 = \mathrm{id}_{\Sigma^*}$

Des exemples



ρ_a :

001110010101 . . . 101110010101 . . .

↧ ↧

010001101010 . . . 110001101010 . . .

$\rho_a^2 = \mathrm{id}_{\Sigma^*}$

ρ_b :

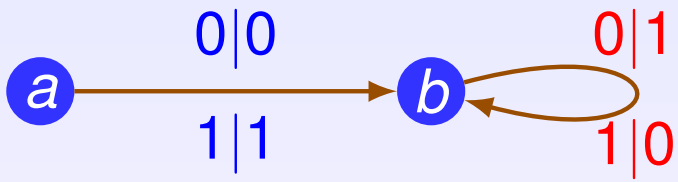
001110010101 . . . 101110010101 . . .

↧ ↧

110001101010 . . . 010001101010 . . .

$\rho_b^2 = \mathrm{id}_{\Sigma^*}$

Des exemples



ρ_a :

001110010101 . . . 101110010101 . . .

↧ ↧

010001101010 . . . 110001101010 . . .

$\rho_a^2 = \mathrm{id}_{\Sigma^*}$

ρ_b :

001110010101 . . . 101110010101 . . .

↧ ↧

110001101010 . . . 010001101010 . . .

$\rho_b^2 = \mathrm{id}_{\Sigma^*}$

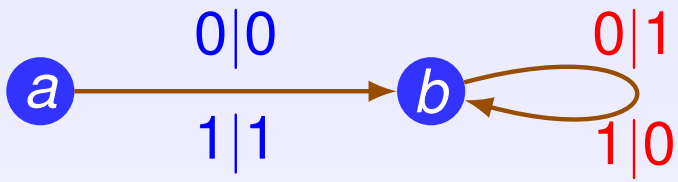
$\rho_b\rho_a = \rho_a\rho_b$:

001110010101 . . . 101110010101 . . .

↧ ↧

101110010101 . . . 001110010101 . . .

Des exemples



ρ_a :

001110010101 . . . 101110010101 . . .

↧ ↧

010001101010 . . . 110001101010 . . .

$\rho_a^2 = \mathrm{id}_{\Sigma^*}$

ρ_b :

001110010101 . . . 101110010101 . . .

↧ ↧

110001101010 . . . 010001101010 . . .

$\rho_b^2 = \mathrm{id}_{\Sigma^*}$

$\rho_b\rho_a = \rho_a\rho_b$:

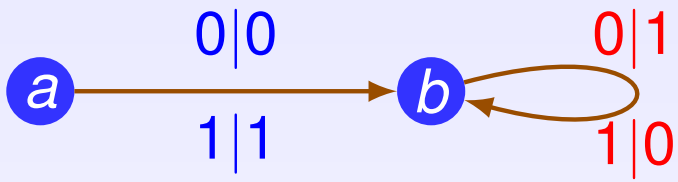
001110010101 . . . 101110010101 . . .

↧ ↧

101110010101 . . . 001110010101 . . .

$(\rho_a\rho_b)^2 = \mathrm{id}_{\Sigma^*}$

Des exemples



$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

ρ_a :

001110010101 . . . 101110010101 . . .

↧ ↧

010001101010 . . . 110001101010 . . .

$\rho_a^2 = \mathrm{id}_{\Sigma^*}$

ρ_b :

001110010101 . . . 101110010101 . . .

↧ ↧

110001101010 . . . 010001101010 . . .

$\rho_b^2 = \mathrm{id}_{\Sigma^*}$

$\rho_b\rho_a = \rho_a\rho_b$:

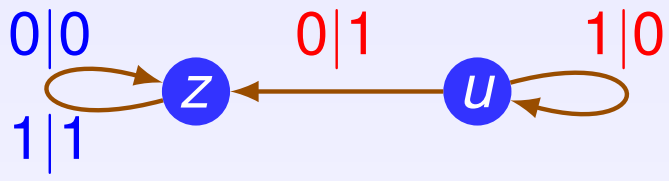
001110010101 . . . 101110010101 . . .

↧ ↧

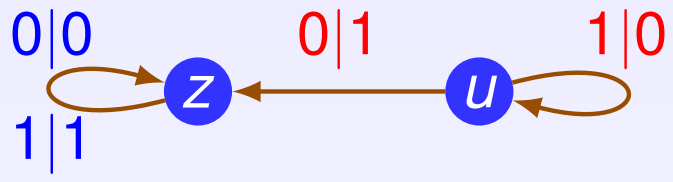
101110010101 . . . 001110010101 . . .

$(\rho_a\rho_b)^2 = \mathrm{id}_{\Sigma^*}$

Des exemples



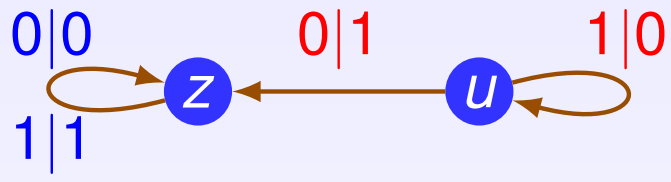
Des exemples



$z : 111001010100 \mapsto 111001010100$

$u : 111001010100 \mapsto 000101010100$

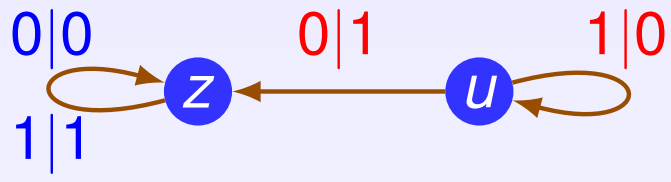
Des exemples



$z : 111001010100 \mapsto 111001010100$

$u : 111001010100 \mapsto 000101010100 \qquad +1$

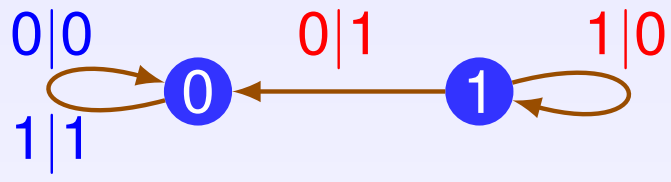
Des exemples



$z : 111001010100 \mapsto 111001010100 \qquad +0$

$u : 111001010100 \mapsto 000101010100 \qquad +1$

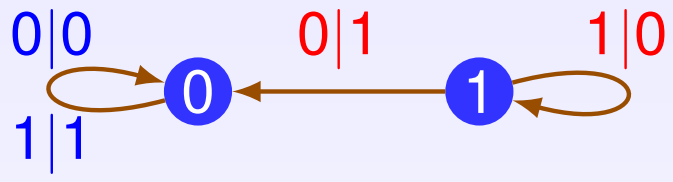
Des exemples



$z : 111001010100 \mapsto 111001010100 \qquad +0$

$u : 111001010100 \mapsto 000101010100 \qquad +1$

Des exemples

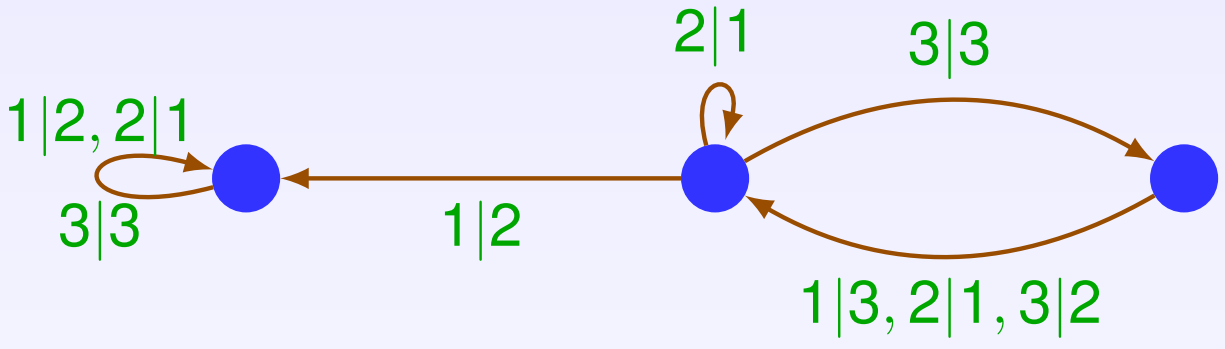


$\mathbb{N}, \quad \mathbb{Z}$

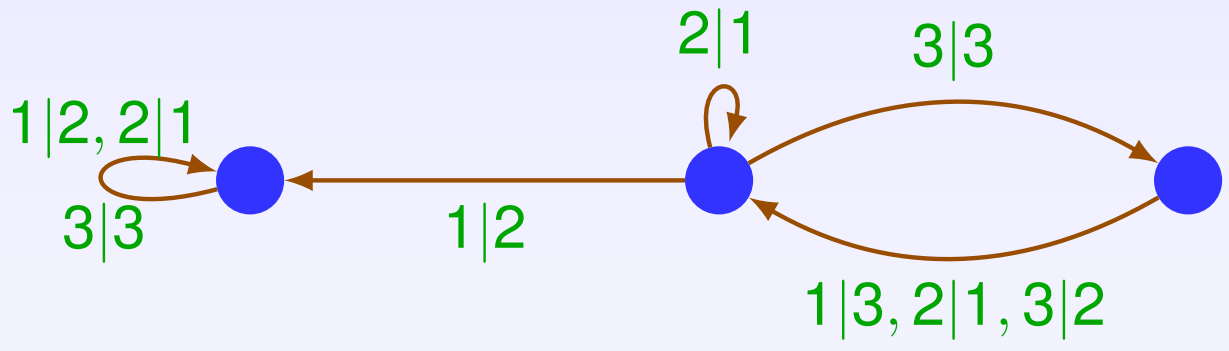
$z : 111001010100 \mapsto 111001010100 \qquad +0$

$u : 111001010100 \mapsto 000101010100 \qquad +1$

Des exemples



Des exemples

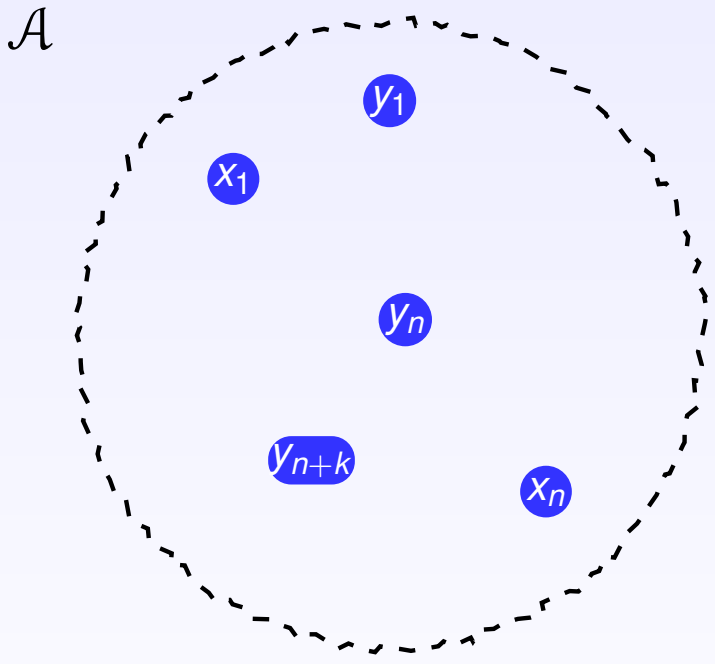


$$1\,494\,186\,269\,970\,473\,680\,896 = 2^{64} \cdot 3^4 \approx 1.5 \times 10^{21}$$

Un levier combinatoire

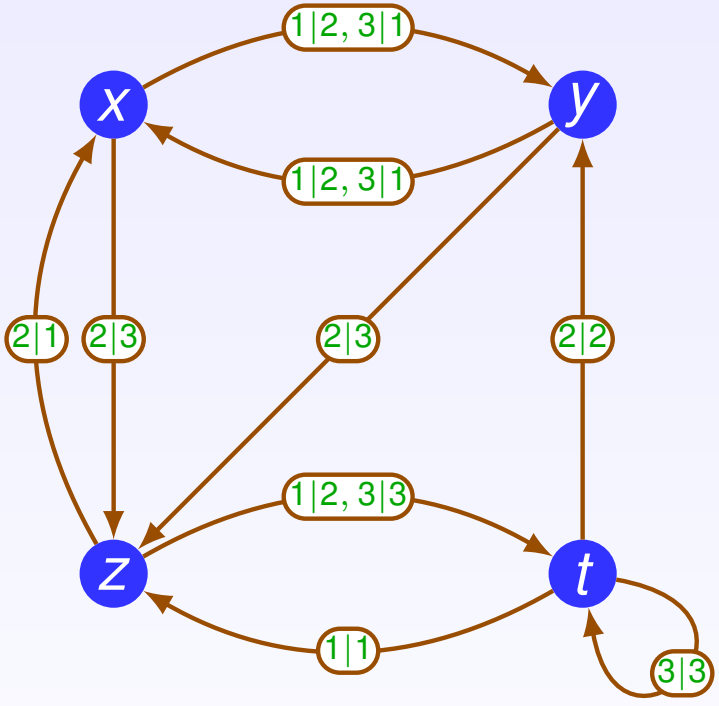
Exemple du problème du mot

$$\rho x_1 \cdots x_n \stackrel{?}{=} \rho y_1 \cdots y_{n+k}$$



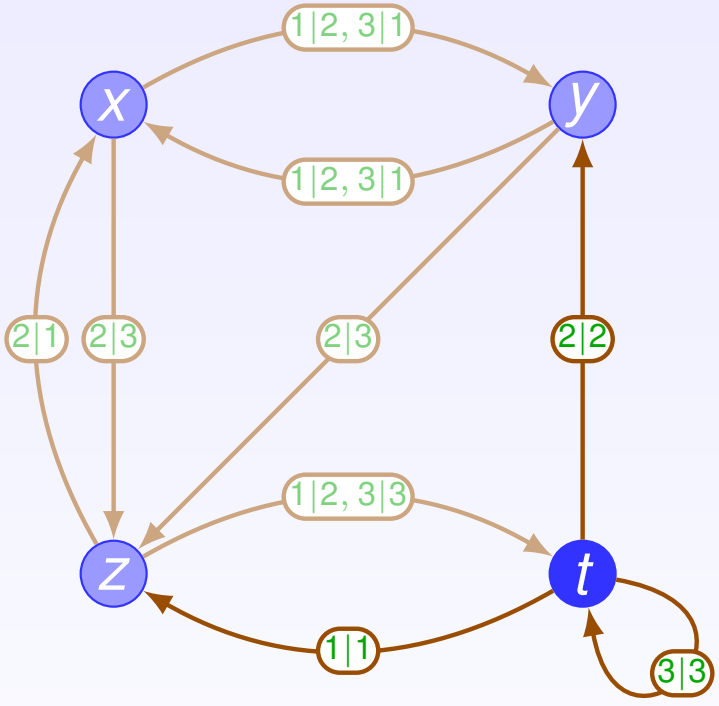
Un levier combinatoire

Exemple du problème du mot



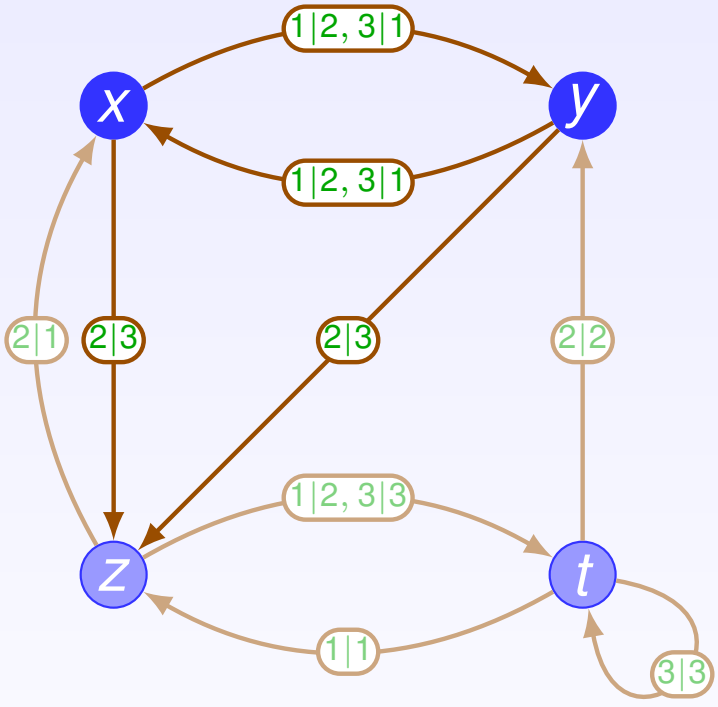
Un levier combinatoire

Exemple du problème du mot



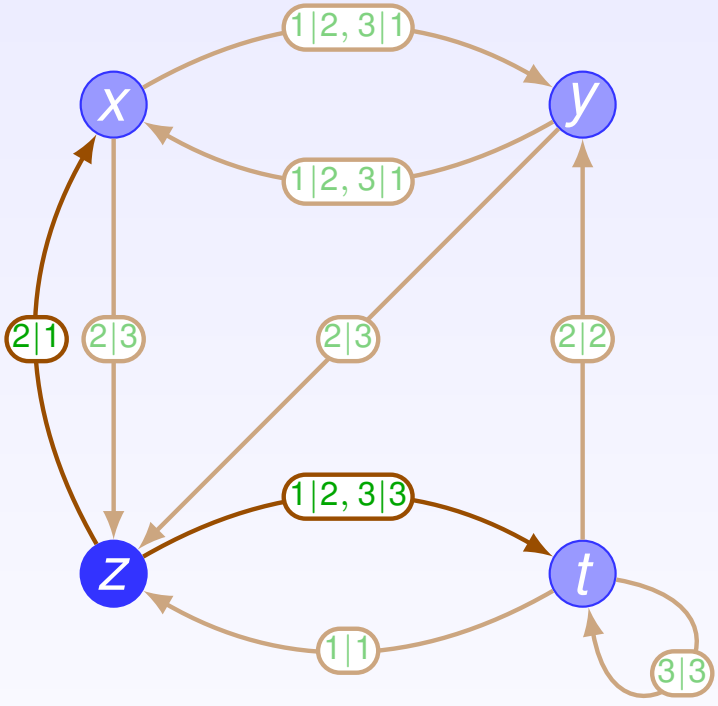
Un levier combinatoire

Exemple du problème du mot



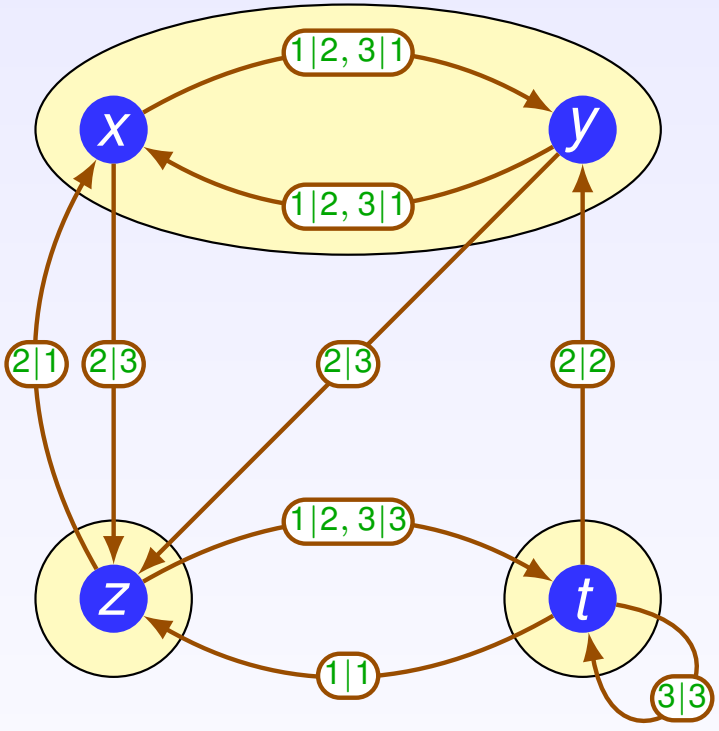
Un levier combinatoire

Exemple du problème du mot



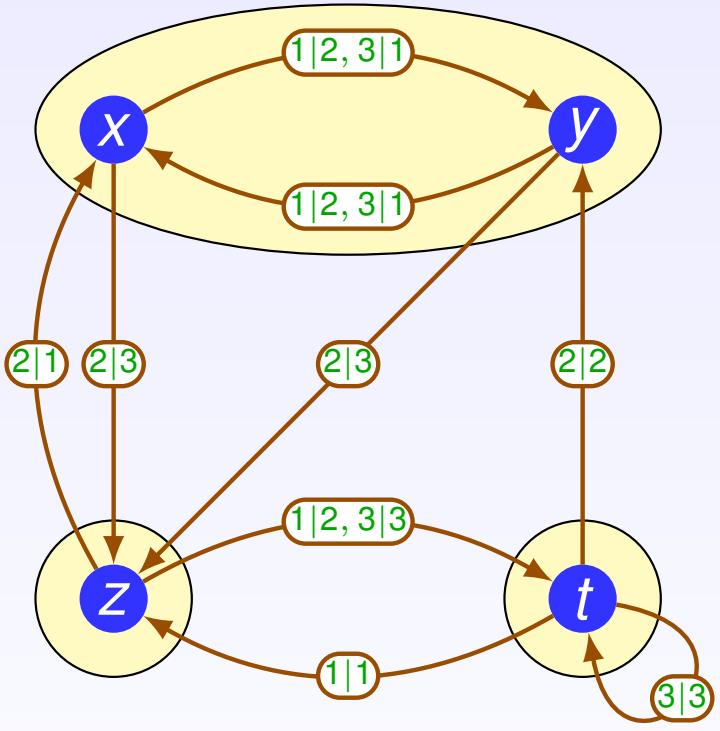
Un levier combinatoire

Exemple du problème du mot



Un levier combinatoire

Exemple du problème du mot



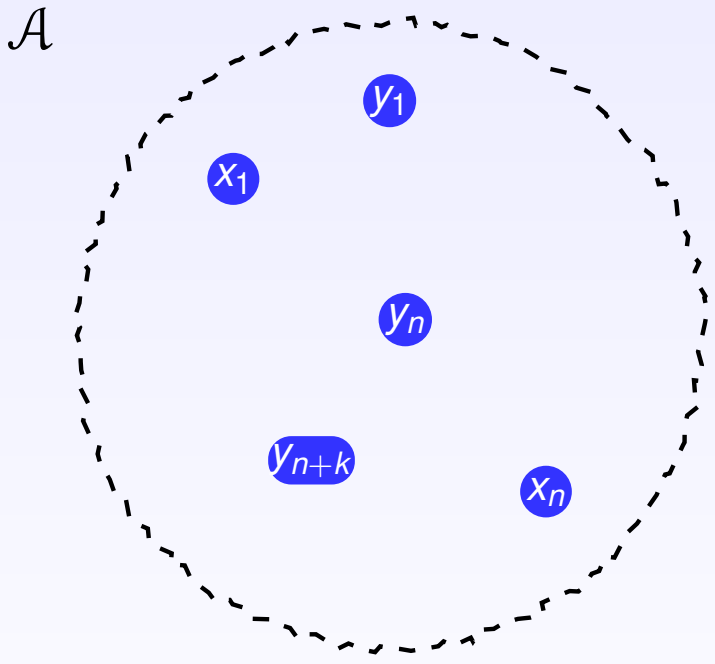
+ minimisation classique :

$$[x] = [y] \iff \rho_{x_{|\Sigma^*}} = \rho_{y_{|\Sigma^*}}$$

Un levier combinatoire

Exemple du problème du mot

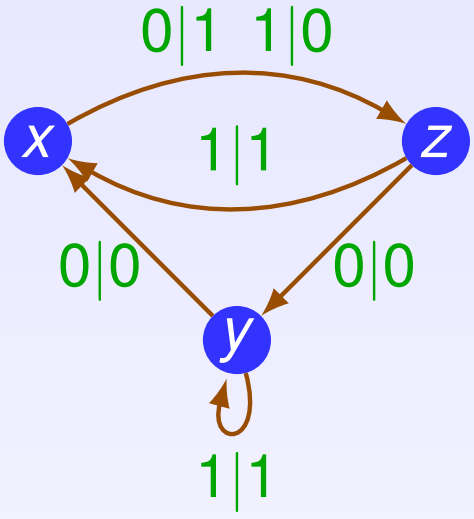
$$\rho x_1 \cdots x_n \stackrel{?}{=} \rho y_1 \cdots y_{n+k}$$



$$\rho_{x_i} : \Sigma^* \to \Sigma^*$$

$$\rho_{x_1 x_2 \ldots x_n} = \rho_{x_n} \circ \cdots \circ \rho_{x_1}$$

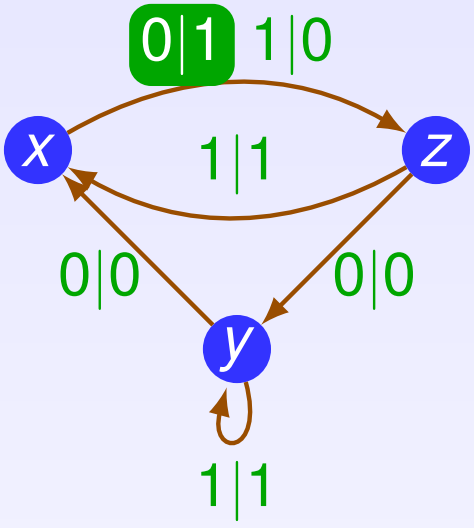
$\mathcal{A}$

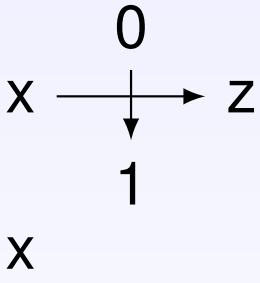


$$\rho_{x_i} : \Sigma^* \to \Sigma^*$$

$$\rho_{x_1 x_2 \ldots x_n} = \rho_{x_n} \circ \cdots \circ \rho_{x_1}$$

$\mathcal{A}$

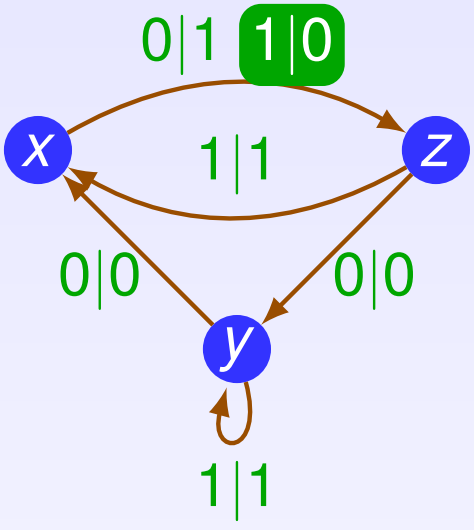


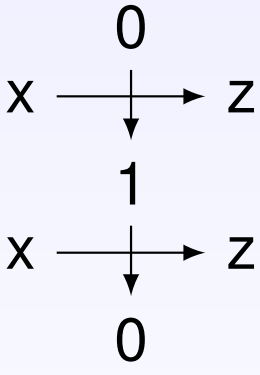


$$\rho_{x_i} : \Sigma^* \to \Sigma^*$$

$$\rho_{x_1 x_2 \ldots x_n} = \rho_{x_n} \circ \cdots \circ \rho_{x_1}$$

$\mathcal{A}$

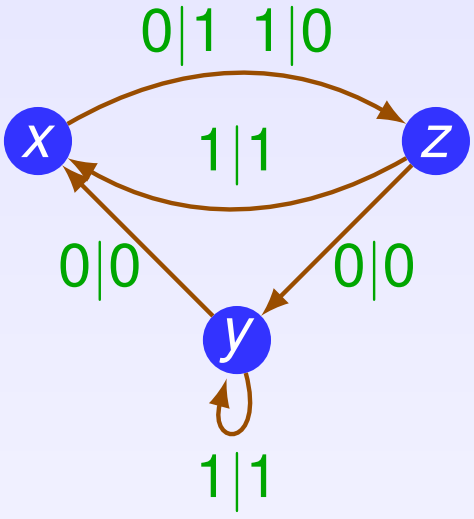


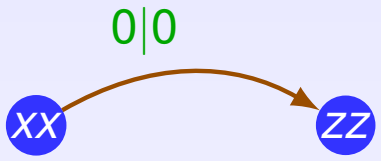


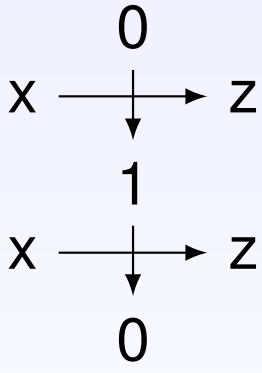
$$\rho_{x_i} : \Sigma^* \to \Sigma^*$$

$$\rho_{x_1 x_2 \ldots x_n} = \rho_{x_n} \circ \cdots \circ \rho_{x_1}$$

$\mathcal{A}$



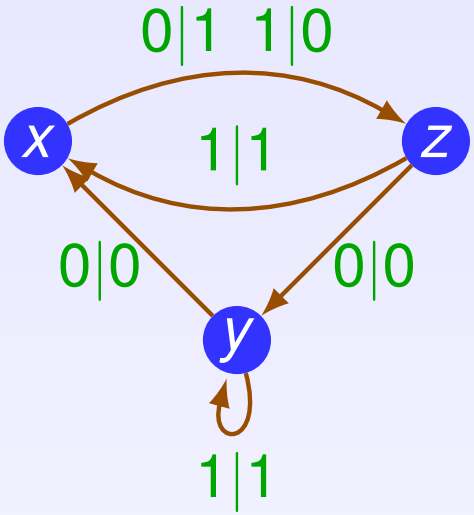


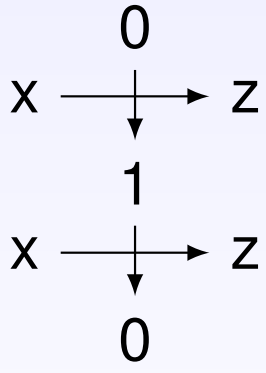


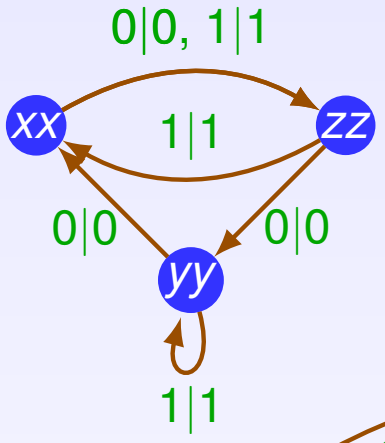
$$\rho_{x_i} : \Sigma^* \to \Sigma^*$$

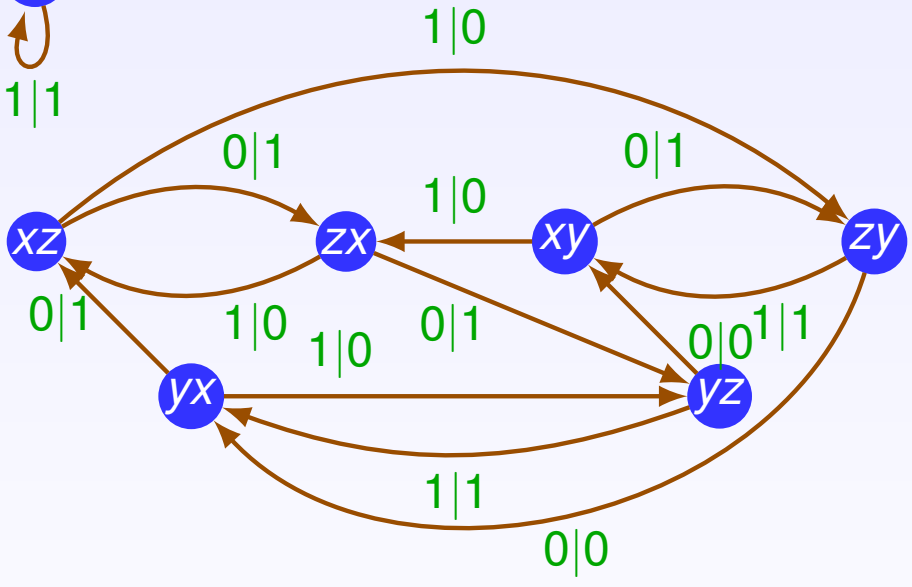
$$\rho_{x_1 x_2 \ldots x_n} = \rho_{x_n} \circ \cdots \circ \rho_{x_1}$$

$\mathcal{A}$





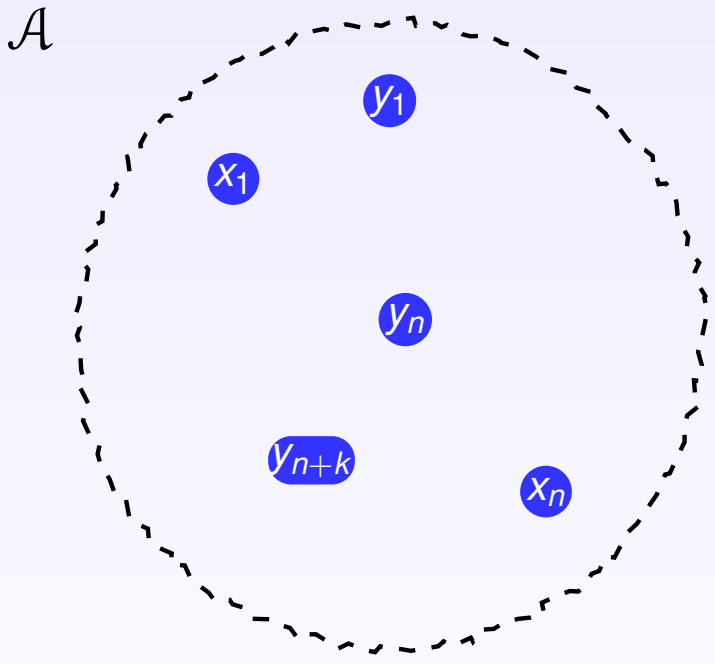




Un levier combinatoire

Exemple du problème du mot

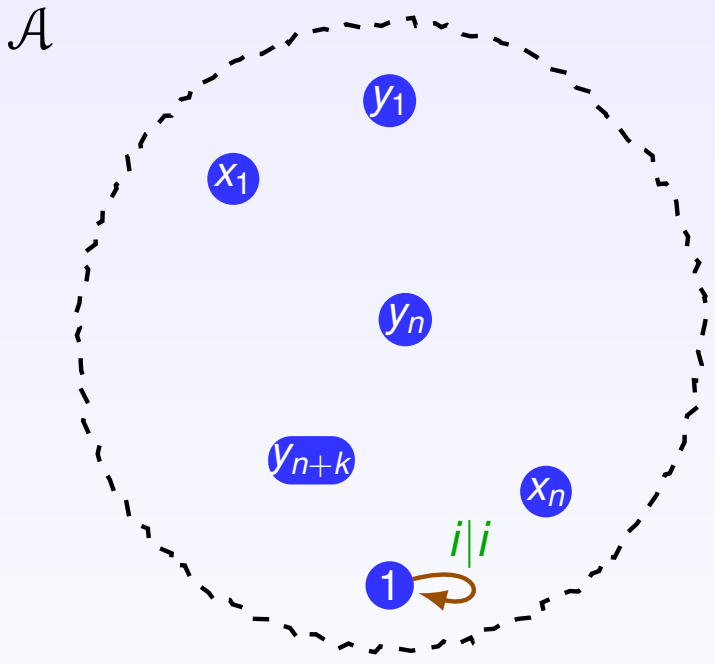
$$\rho x_1 \cdots x_n \stackrel{?}{=} \rho y_1 \cdots y_{n+k}$$



Un levier combinatoire

Exemple du problème du mot

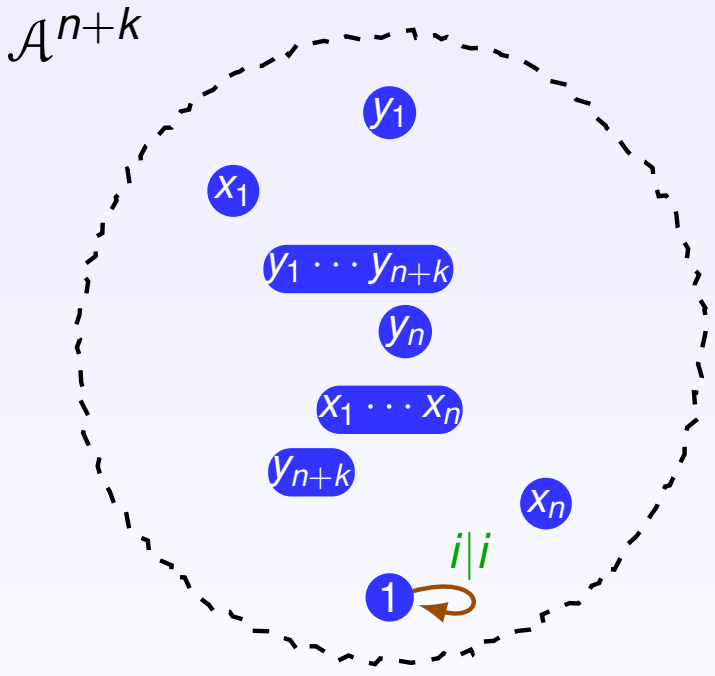
$$\rho x_1 \cdots x_n \stackrel{?}{=} \rho y_1 \cdots y_{n+k}$$



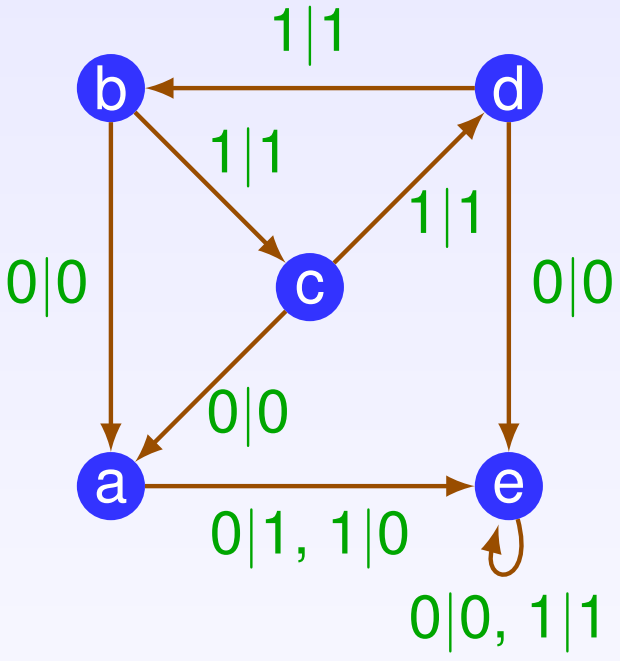
Un levier combinatoire

Exemple du problème du mot

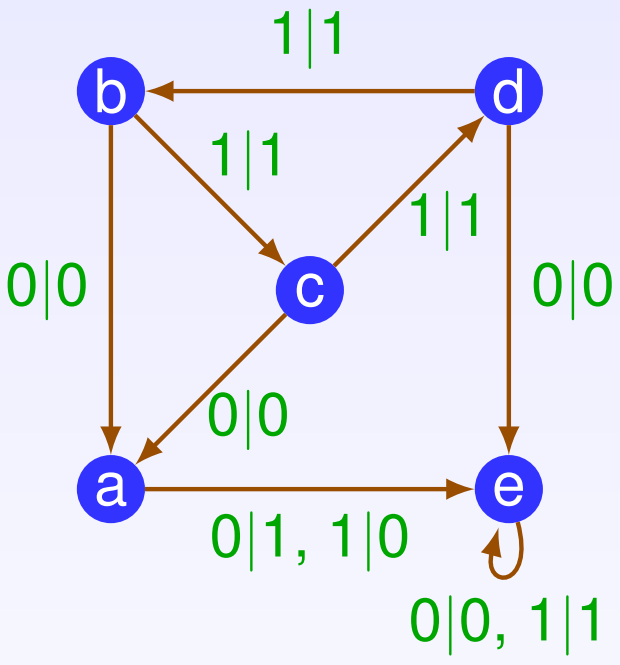
$$\rho_{x_1 \cdots x_n} \stackrel{?}{=} \rho_{y_1 \cdots y_{n+k}}$$



Le groupe de Grigorchuk est Burnside infini



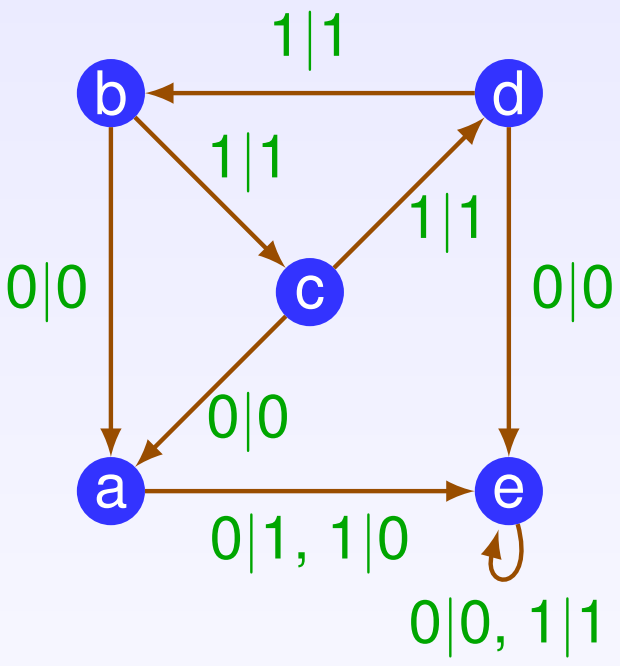
Le groupe de Grigorchuk est Burnside infini



Fait 1

Γ est infini

Le groupe de Grigorchuk est Burnside infini

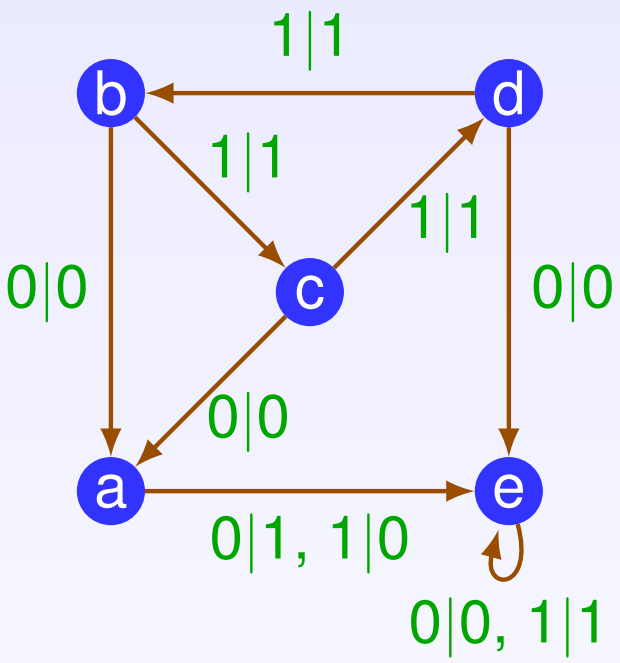


Fait 1

Γ est infini

$$(\mathbf{u}_k \qquad)_{k\geq 0}$$

Le groupe de Grigorchuk est Burnside infini



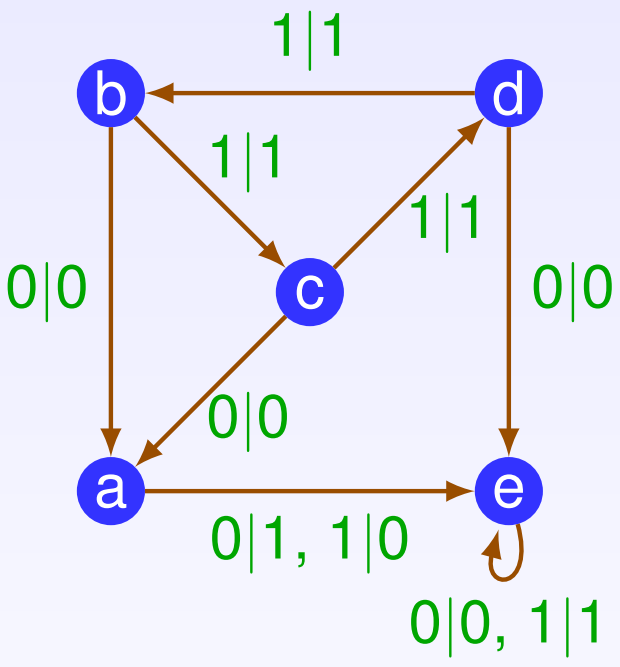
Fait 1

Γ est infini

$$(\eta^k(a) : 1^\omega \mapsto 1^k 0 1^\omega)_{k \geq 0}$$

$$\eta : a \mapsto aba, \qquad b \mapsto d$$
$$c \mapsto b, \qquad d \mapsto c$$

Le groupe de Grigorchuk est Burnside infini



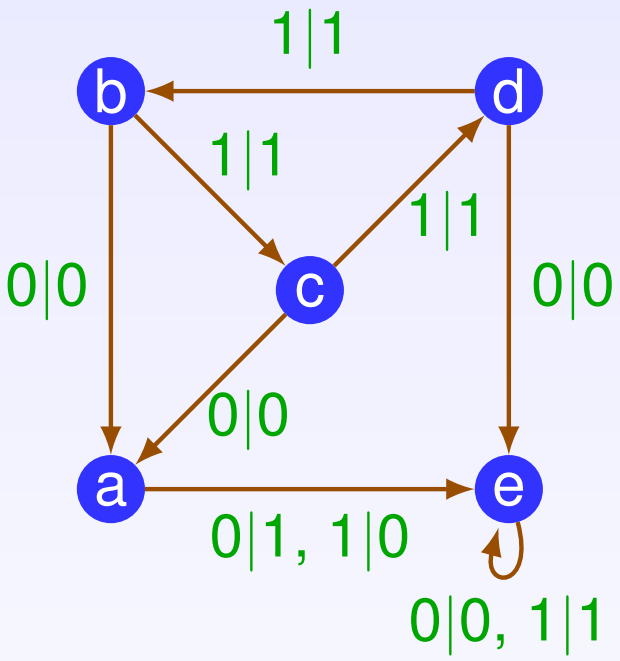
Fait 1

Γ est infini

Fait 2

Γ est un 2-groupe

Le groupe de Grigorchuk est Burnside infini



Fait 1

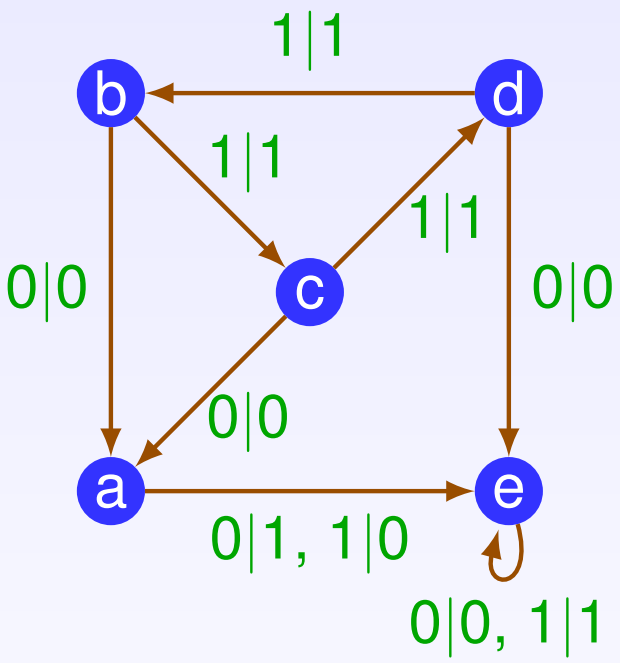
Γ est infini

Fait 2

Γ est un 2-groupe

$\circ$	b	c	d	e
b	e	d	c	b
c	d	e	b	c
d	c	b	e	d
e	b	c	d	e

Le groupe de Grigorchuk est Burnside infini



Fait 1

Γ est infini

Fait 2

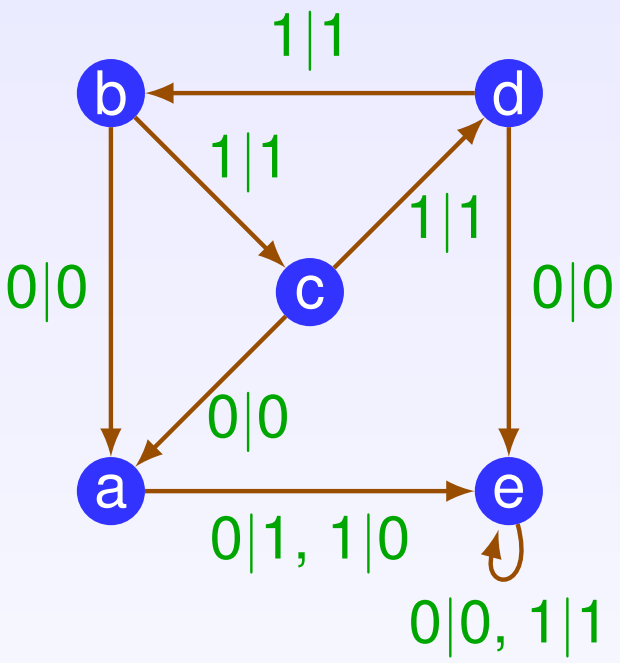
Γ est un 2-groupe

∘	b	c	d	e
b	e	d	c	b
c	d	e	b	c
d	c	b	e	d
e	b	c	d	e

$aSaS \dots Sa$
$SaSa \dots aS$

longueur impaire : conjugué à un élément plus court

Le groupe de Grigorchuk est Burnside infini



Fait 1

Γ est infini

Fait 2

Γ est un 2-groupe

$\circ$	b	c	d	e
b	e	d	c	b
c	d	e	b	c
d	c	b	e	d
e	b	c	d	e

longueur impaire : conjugué à un élément plus court
longueur paire : plus technique

Burnside

Milnor

Croissance

$$\mathbb{Z}^2 = \langle a = (0,1), b = (1,0) \mid ab = ba \rangle$$

Croissance

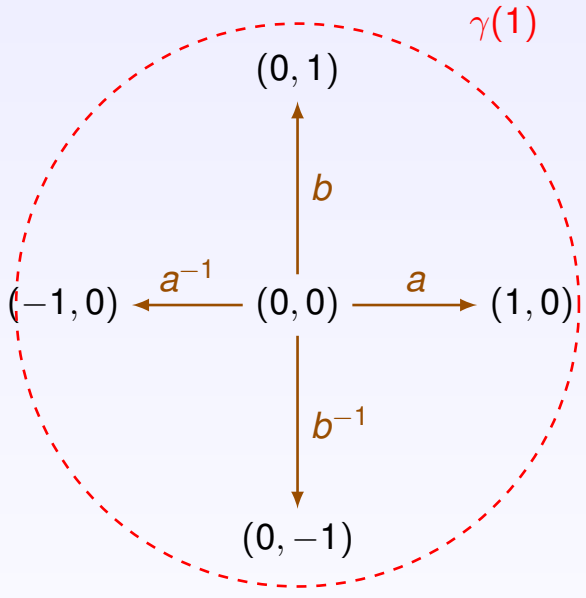
$$\mathbb{Z}^2 = \langle a = (0,1), b = (1,0) \mid ab = ba \rangle$$

$$\gamma(0) = 1$$

$(0,0)$

Croissance

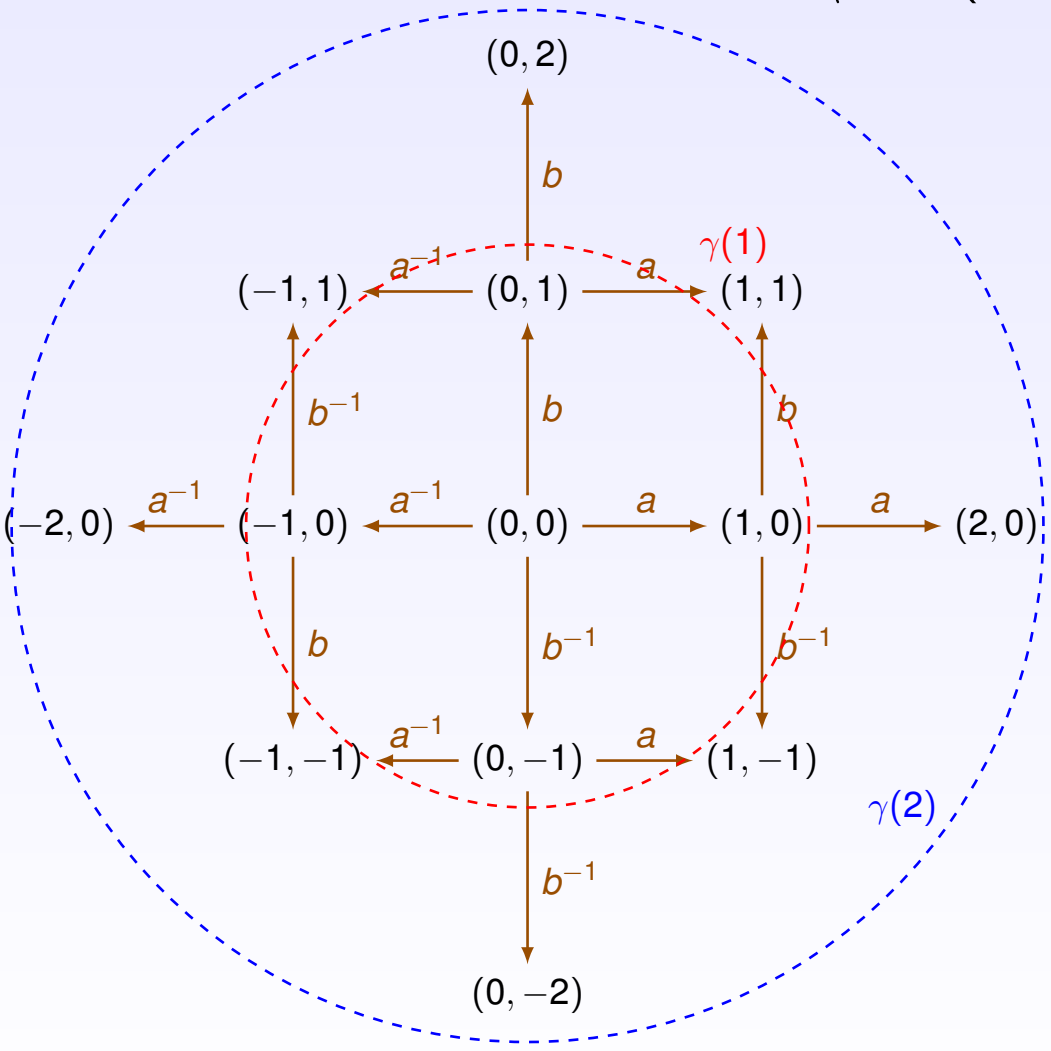
$$\mathbb{Z}^2 = \langle a = (0,1), b = (1,0) \mid ab = ba \rangle$$



$$\gamma(0) = 1$$
$$\gamma(1) = 5$$

Croissance

$$\mathbb{Z}^2 = \langle a = (0,1), b = (1,0) \mid ab = ba \rangle$$



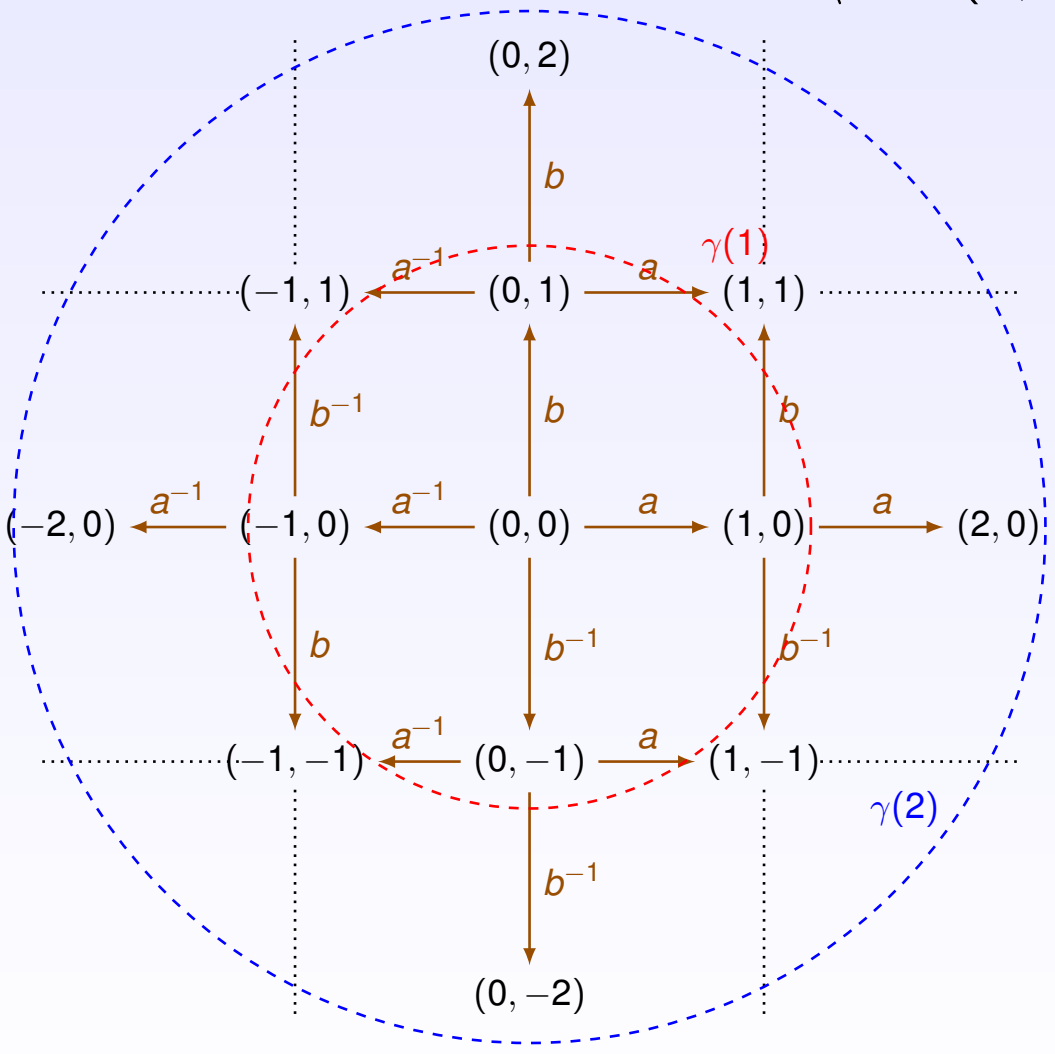
$\gamma(0) = 1$

$\gamma(1) = 5$

$\gamma(2) = 13$

Croissance

$$\mathbb{Z}^2 = \langle a = (0,1), b = (1,0) \mid ab = ba \rangle$$



$$\gamma(0) = 1$$
$$\gamma(1) = 5$$
$$\gamma(2) = 13$$
$$\vdots$$
$$\gamma(n) = 2n^2 + 2n + 1$$

Croissance

$\mathbb{F}_2 = \langle a, b \rangle$

Croissance

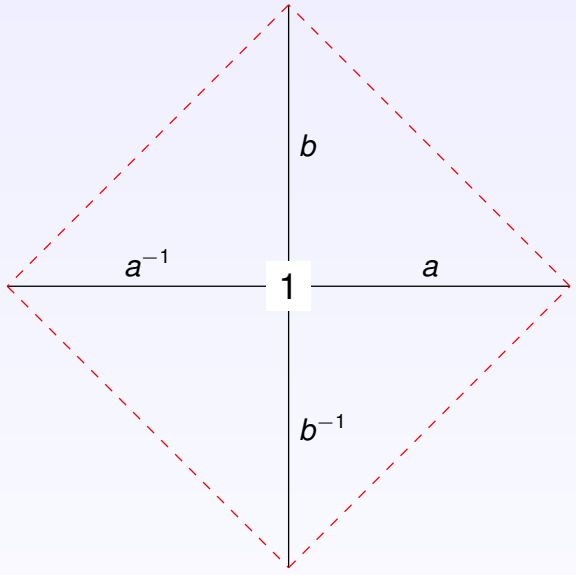
$\mathbb{F}_2 = \langle a, b \rangle$

$\gamma(0) = 1$

1

Croissance

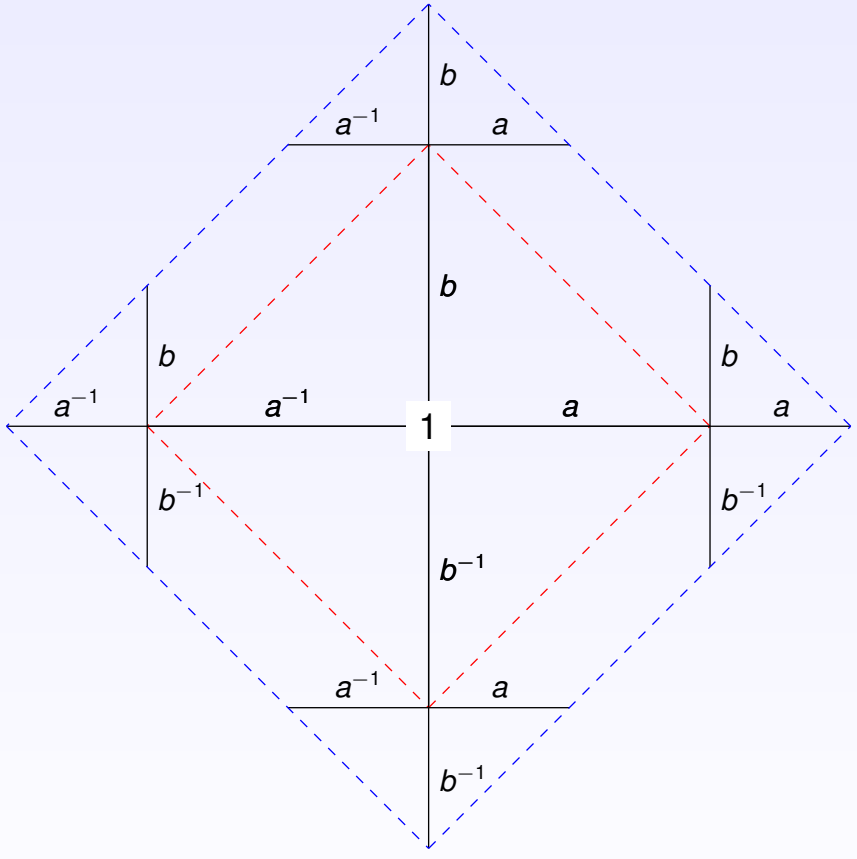
$\mathbb{F}_2 = \langle a, b \rangle$



$\gamma(0) = 1$
$\gamma(1) = 5$

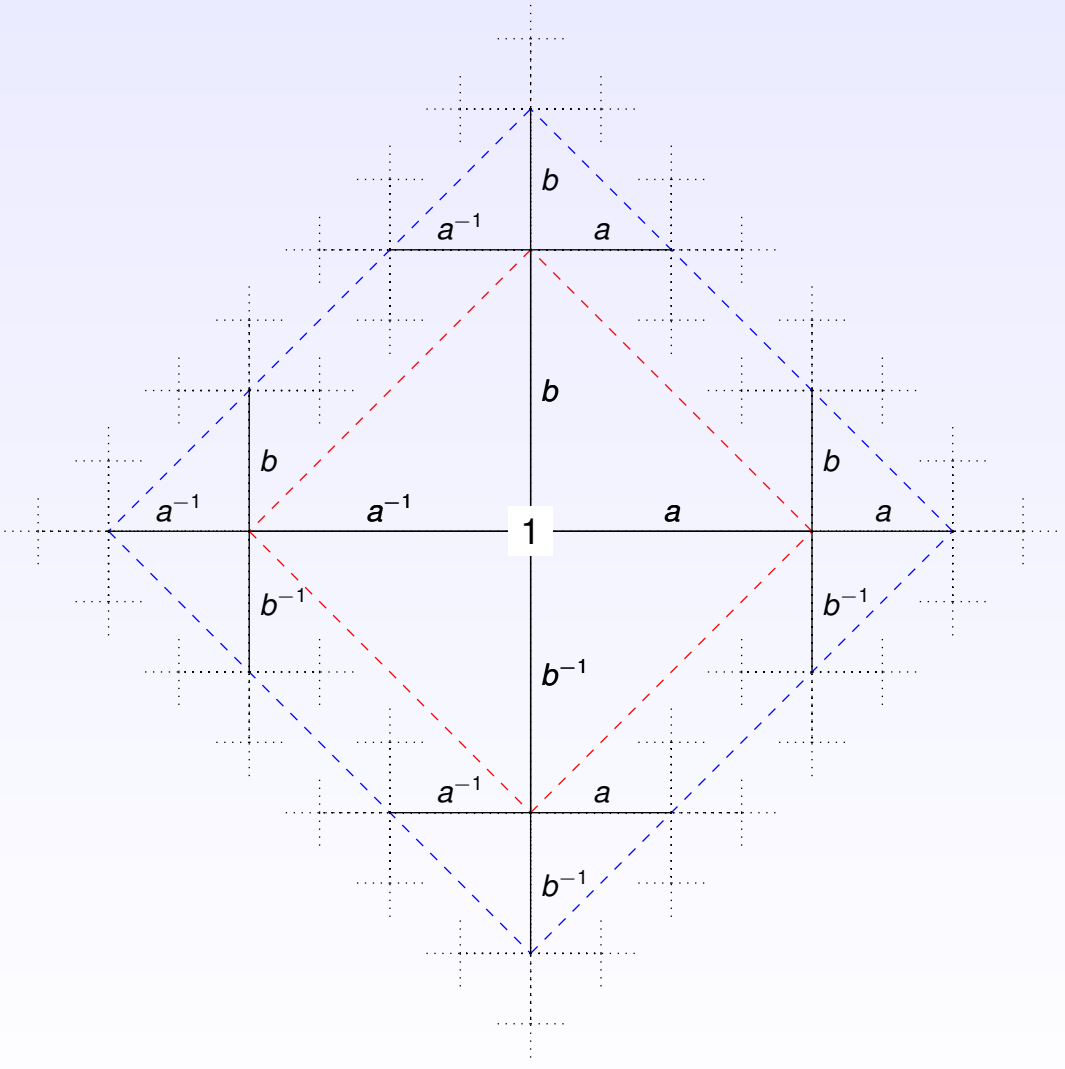
Croissance

$\mathbb{F}_2 = \langle a, b \rangle$



$\gamma(0) = 1$
$\gamma(1) = 5$
$\gamma(2) = 17$

Croissance

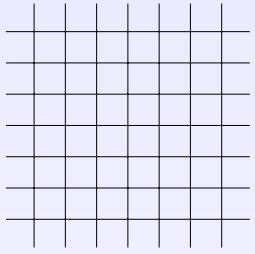


$$\mathbb{F}_2 = \langle a, b \rangle$$

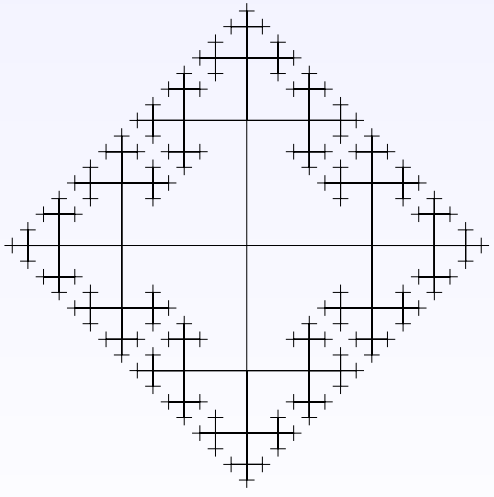
$$\gamma(0) = 1$$
$$\gamma(1) = 5$$
$$\gamma(2) = 17$$
$$\vdots$$
$$\gamma(n) = 2 \times 3^n - 1$$

croissance bornée : groupes finis

croissance polynomiale : $\mathbb{Z}^d$, groupes abéliens

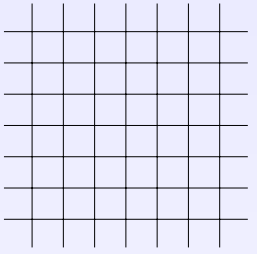


croissance exponentielle : $\mathbb{F}_d$



croissance bornée : groupes finis

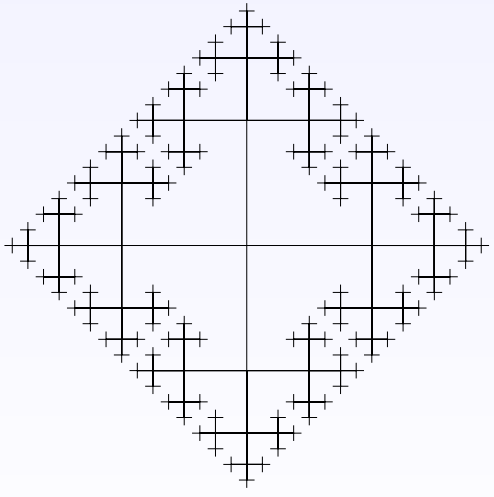
croissance polynomiale : $\mathbb{Z}^d$, groupes abéliens



Milnor

Et entre les deux ?

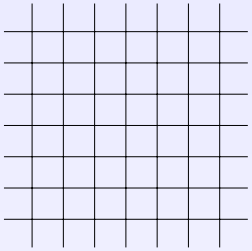
croissance exponentielle : $\mathbb{F}_d$



1968 1983

croissance bornée : groupes finis

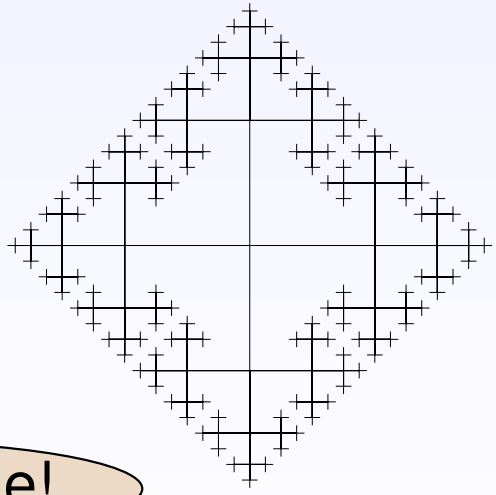
croissance polynomiale : $\mathbb{Z}^d$, groupes abéliens



Milnor

Et entre les deux ?

croissance exponentielle : $\mathbb{F}_d$



Grigorchuk

C'est possible!

Le groupe de Grigorchuk est à croissance intermédiaire

Fait 1

Γ n'est pas à croissance polynomiale

Le groupe de Grigorchuk est à croissance intermédiaire

Fait 1

Γ n'est pas à croissance polynomiale

Γ et $\Gamma \times \Gamma$

Le groupe de Grigorchuk est à croissance intermédiaire

Fait 1

Γ n'est pas à croissance polynomiale

Γ et $\Gamma \times \Gamma$ sont commensurables

Le groupe de Grigorchuk est à croissance intermédiaire

Fait 1

Γ n'est pas à croissance polynomiale

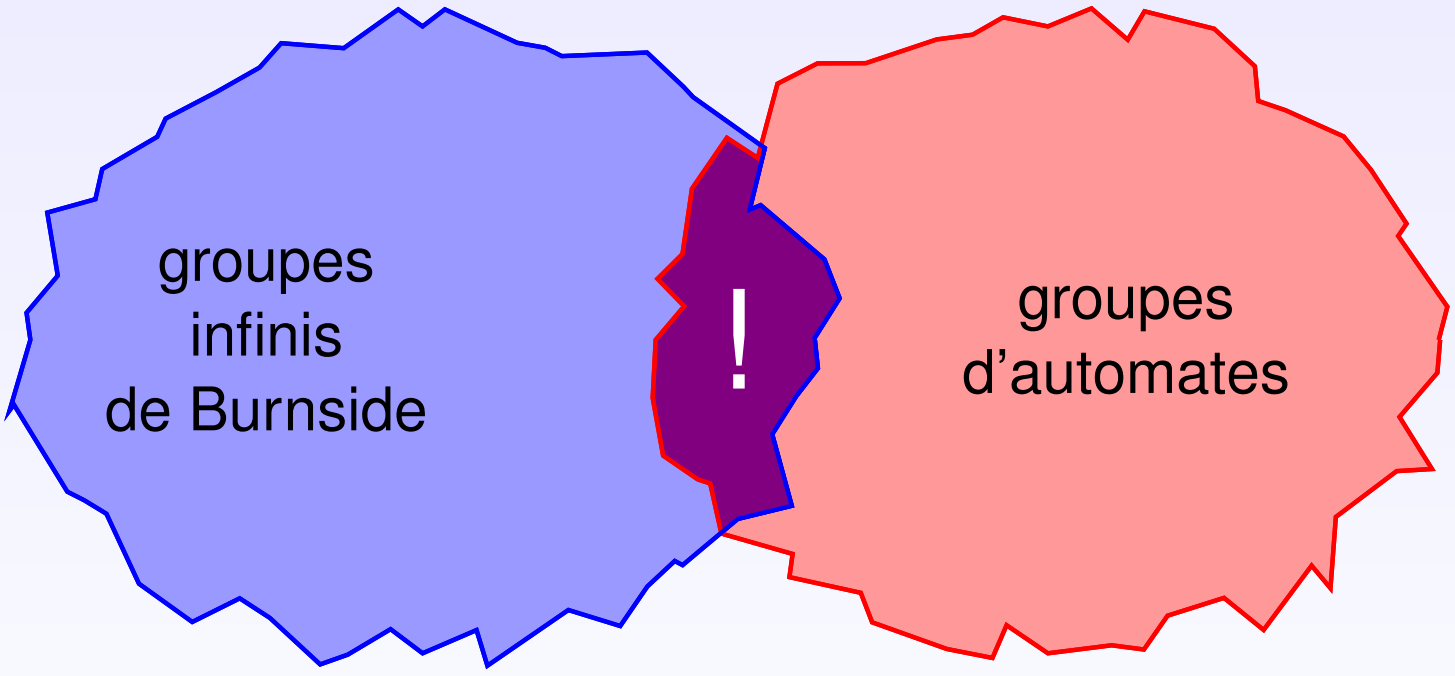
Γ et $\Gamma \times \Gamma$ sont commensurables

Fait 2

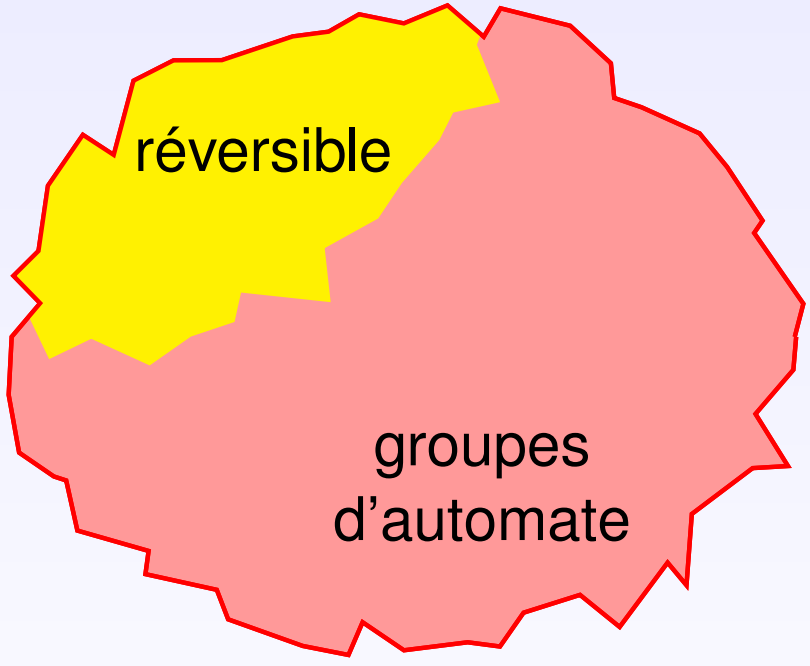
Γ n'est pas à croissance exponentielle

(considérations très "théorie des groupes")

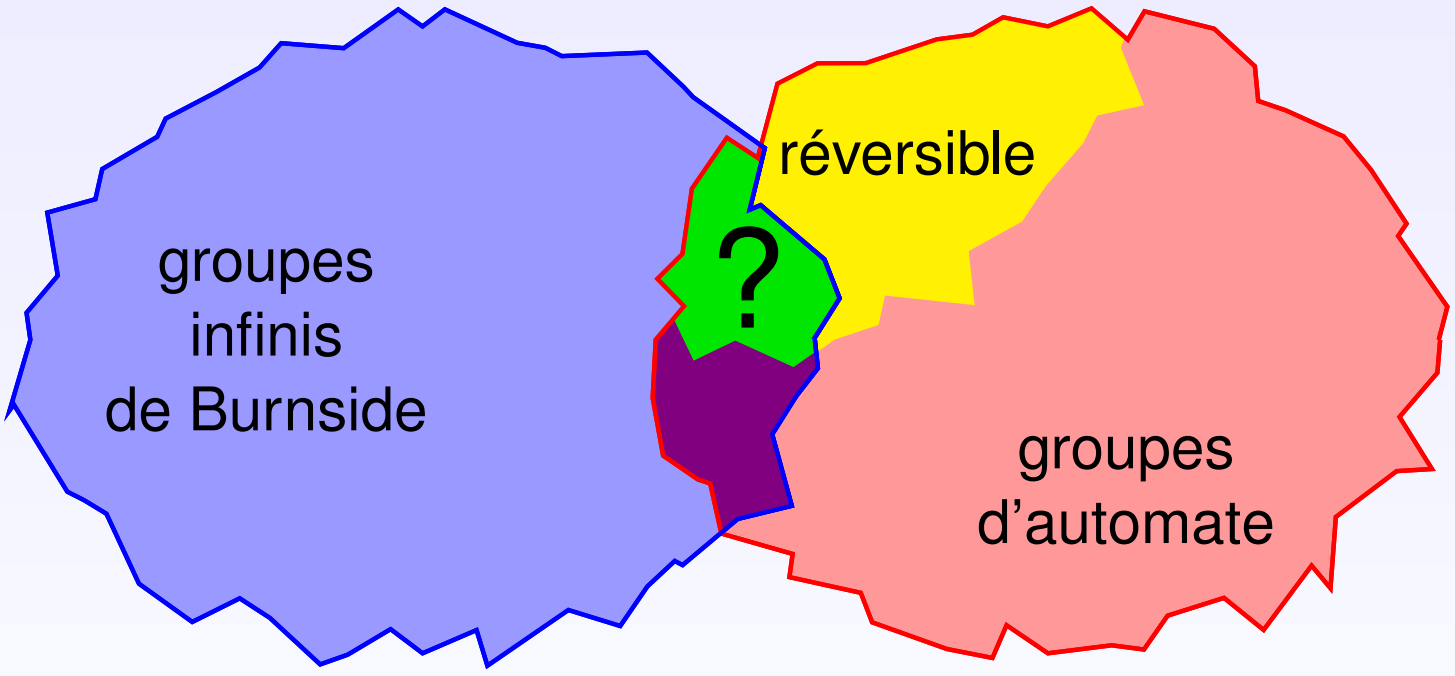
Aleshin + Grigorchuk



Projet JCJC MealyM



Projet JCJC MealyM



Ordres et puissances

$\mathcal{A}$ réversible (les lettres induisent des permutations des états)

Problème de finitude

$\langle \mathcal{A} \rangle$ est fini $\Longleftrightarrow$ les cc des $\mathcal{A}^n$ sont bornées

Problème d'ordre

$\rho_{\mathbf{u}}$ d'ordre fini $\Longleftrightarrow$ les cc des $\mathbf{u}^n$ sont bornées

Ordres et puissances

$\mathcal{A}$ réversible (les lettres induisent des permutations des états)

Problème de finitude

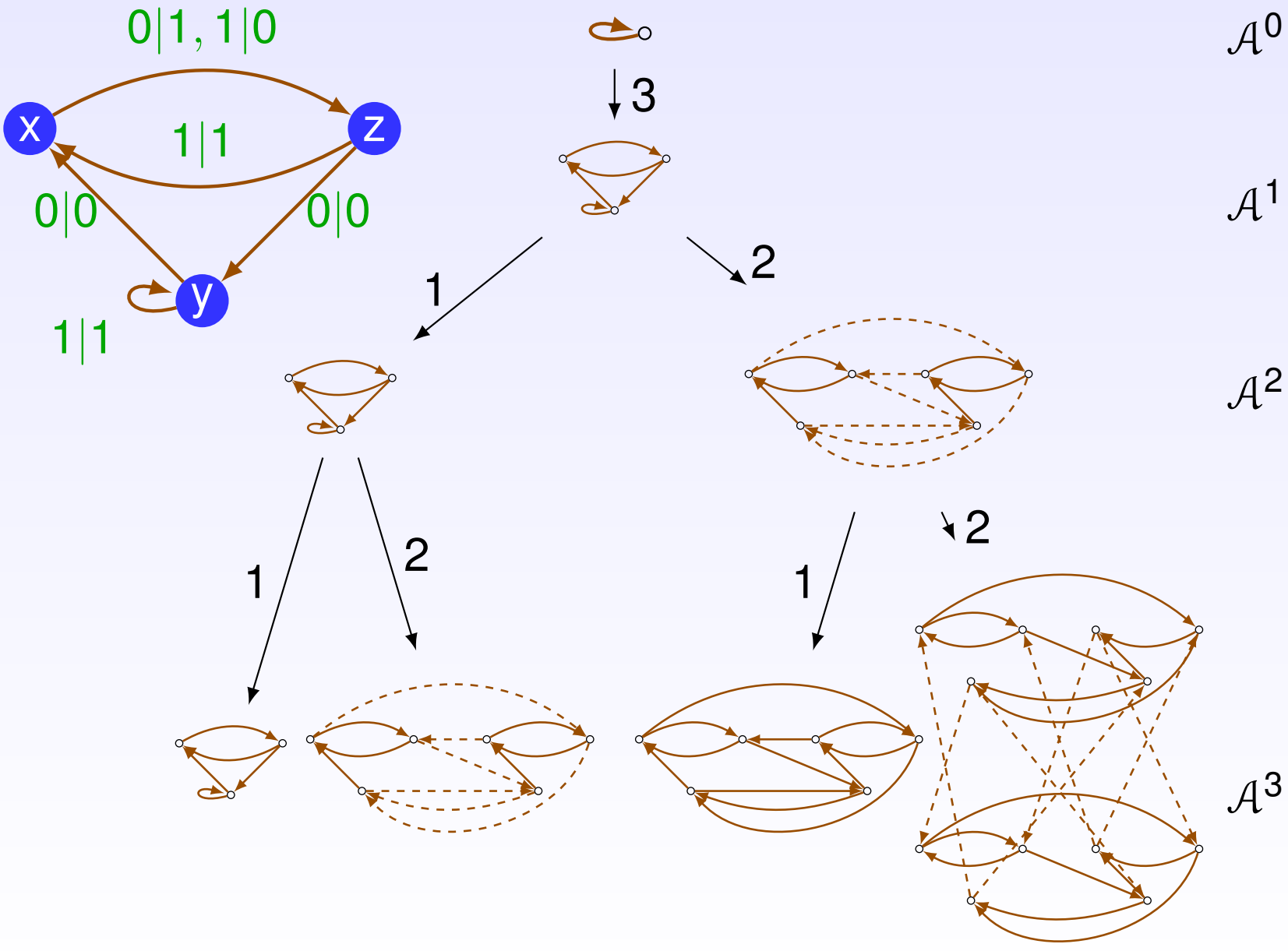
$\langle \mathcal{A} \rangle$ est fini $\Longleftrightarrow$ les cc des $\mathcal{A}^n$ sont bornées

propriétés de certains chemins dans l'arbre lex de Schreier

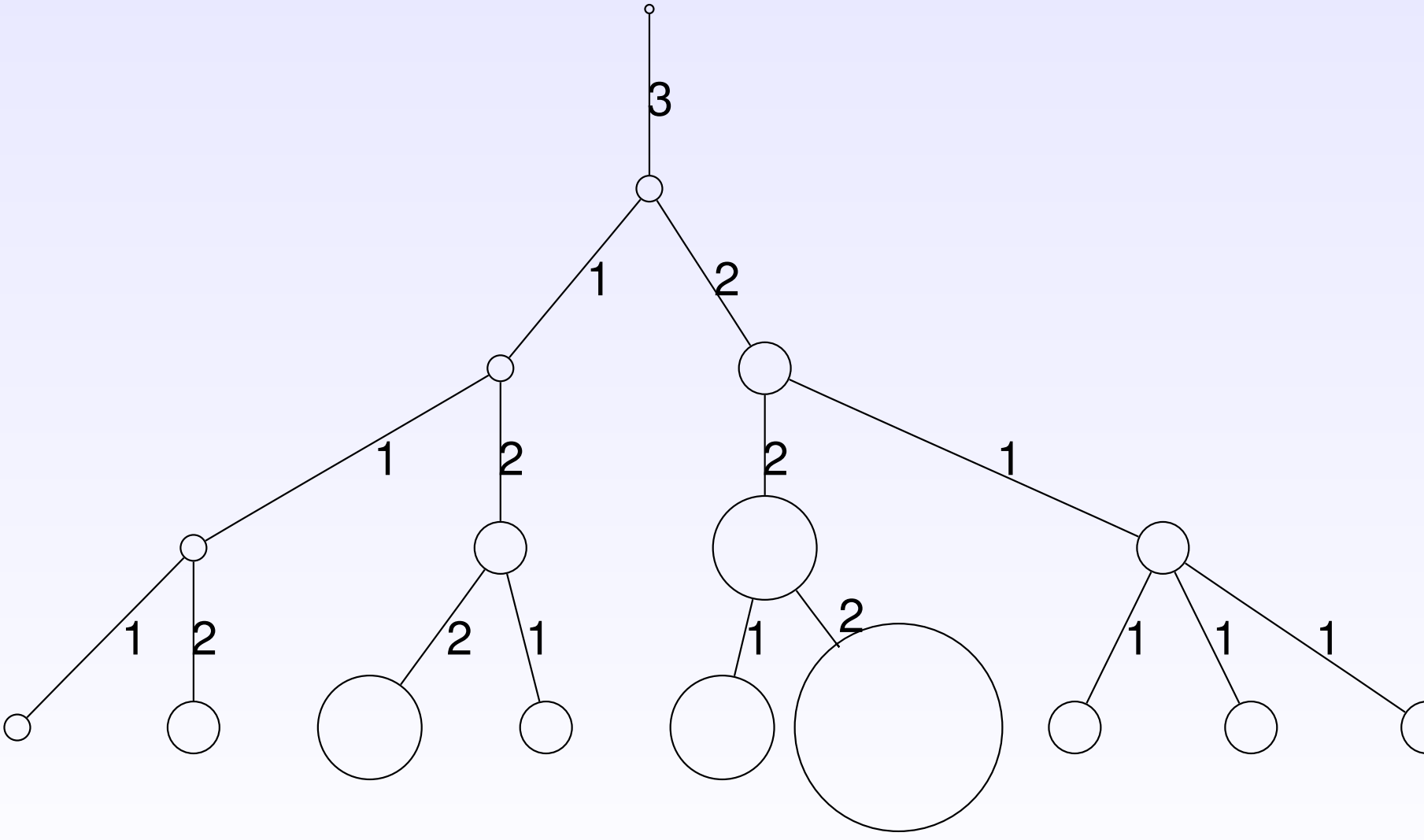
Problème d'ordre

$\rho_{\mathbf{u}}$ d'ordre fini $\Longleftrightarrow$ les cc des $\mathbf{u}^n$ sont bornées

L'arbre lexicographique de Schreier



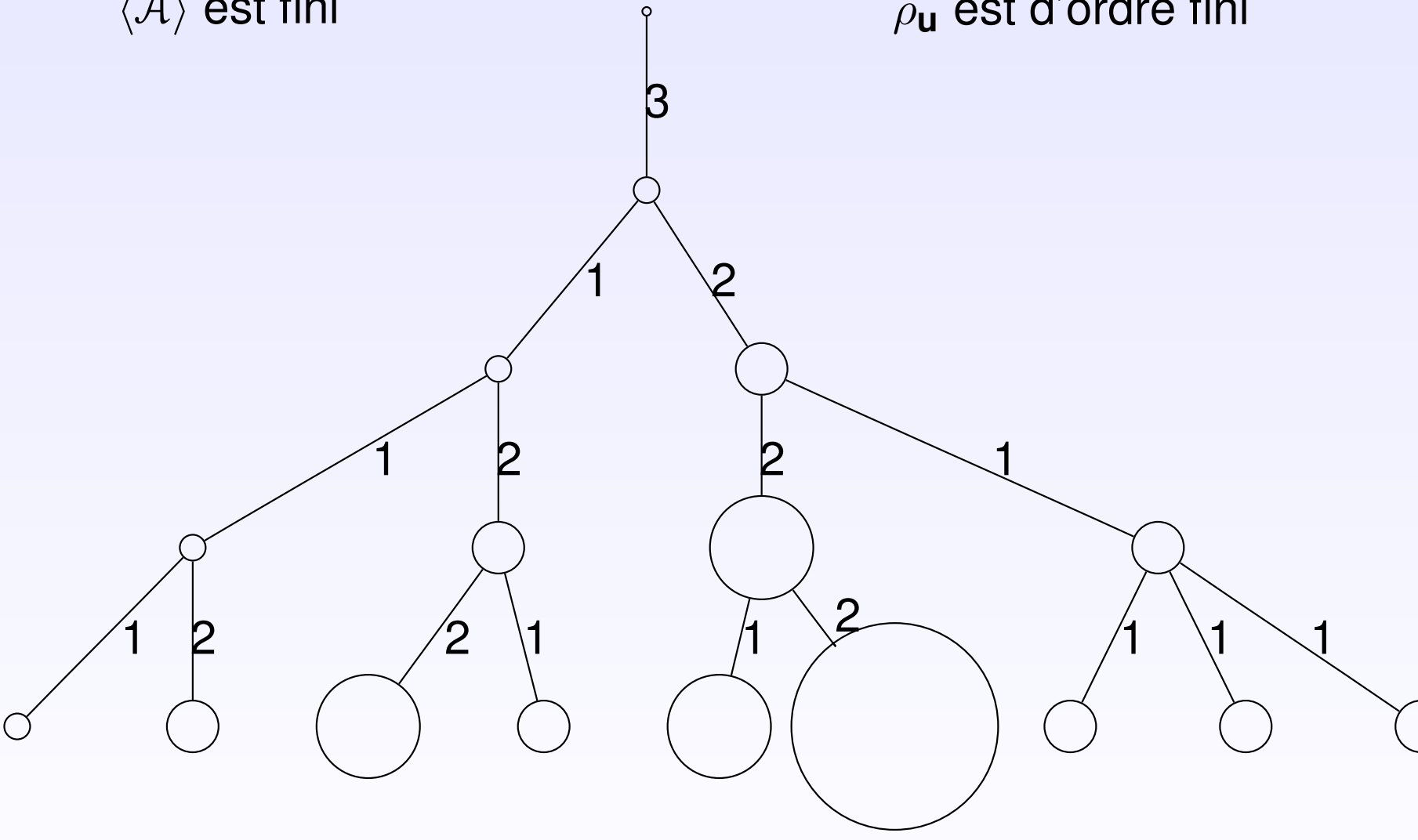
L'arbre lexicographique de Schreier



L'arbre lexicographique de Schreier

$\langle \mathcal{A} \rangle$ est fini

$\rho_{\mathbf{u}}$ est d'ordre fini



L'arbre lexicographique de Schreier

$\langle \mathcal{A} \rangle$ est fini

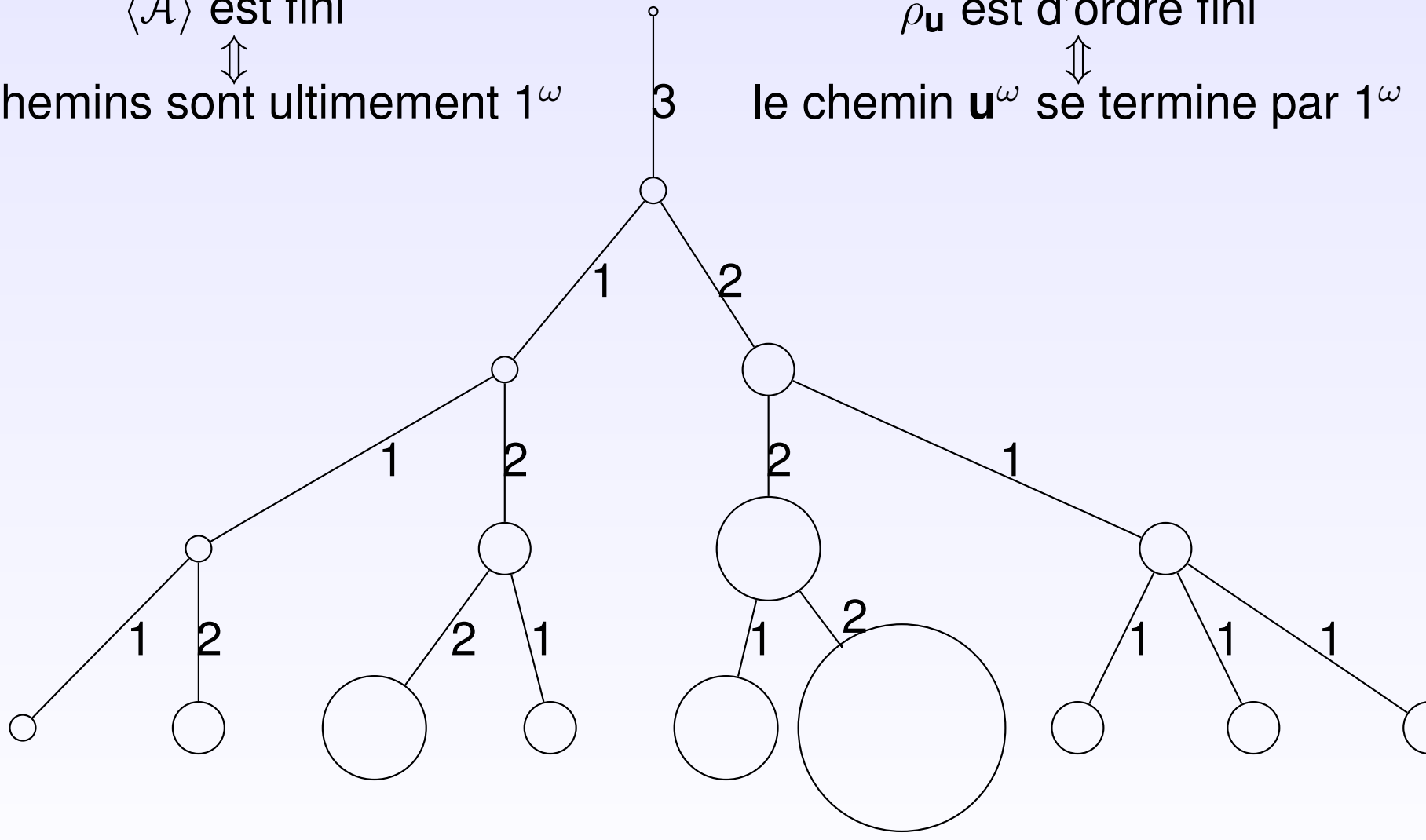
$\Updownarrow$

les chemins sont ultimement 1^ω

$\rho_{\mathbf{u}}$ est d'ordre fini

$\Updownarrow$

le chemin $\mathbf{u}^\omega$ se termine par 1^ω



Problème de Burnside et réversibilité

Question

Un automate réversible peut-il engendrer un groupe de Burnside infini ?

Problème de Burnside et réversibilité

Question

Un automate réversible peut-il engendrer un groupe de Burnside infini ?

impossible :

- 2 états [K., STACS'13]
- 3 états connexe [K. Picantin Savchuk, DLT'15]
- non biréversible [Godin K. Picantin, LATA'15]
- p états connexe, p premier [Godin K., MFCS'16]

Journées de clôture

11 et 12 juillet 2017