Leçons de Mathématiques d'aujourd'hui

Automates réversibles: combinatoire, algèbre et topologie

Jean-Éric Pin

LIAFA, CNRS et Université Paris 7

6 Octobre 2005, Bordeaux

Plan de l'exposé

(1) Rappels sur les automates
(2) L'approche algébrique
(3) Automates réversibles
(4) Groupes libres
(5) Topologie pro-groupe
(6) Lemme d'itération
(7) Caractérisation algébrique
(8) Algorithmes : le retour des automates !
(9) Problèmes connexes et questions ouvertes

Première partie I

Rappels sur les automates

Mots

Un alphabet est un ensemble dont les éléments sont appelés des lettres. Exemple : $\{a, b, c\}$.

Un mot est une suite finie de lettres : a, bab, $aabab$.
Le mot vide, noté 1, ne contient aucune lettre.

Le produit (de concaténation) de deux mots est obtenu en les écrivant bout à bout.

$$abra, cadabra \longrightarrow abracadabra$$

L'ensemble de tous les mots sur un alphabet A est noté A^*. C'est un monoïde de neutre 1.

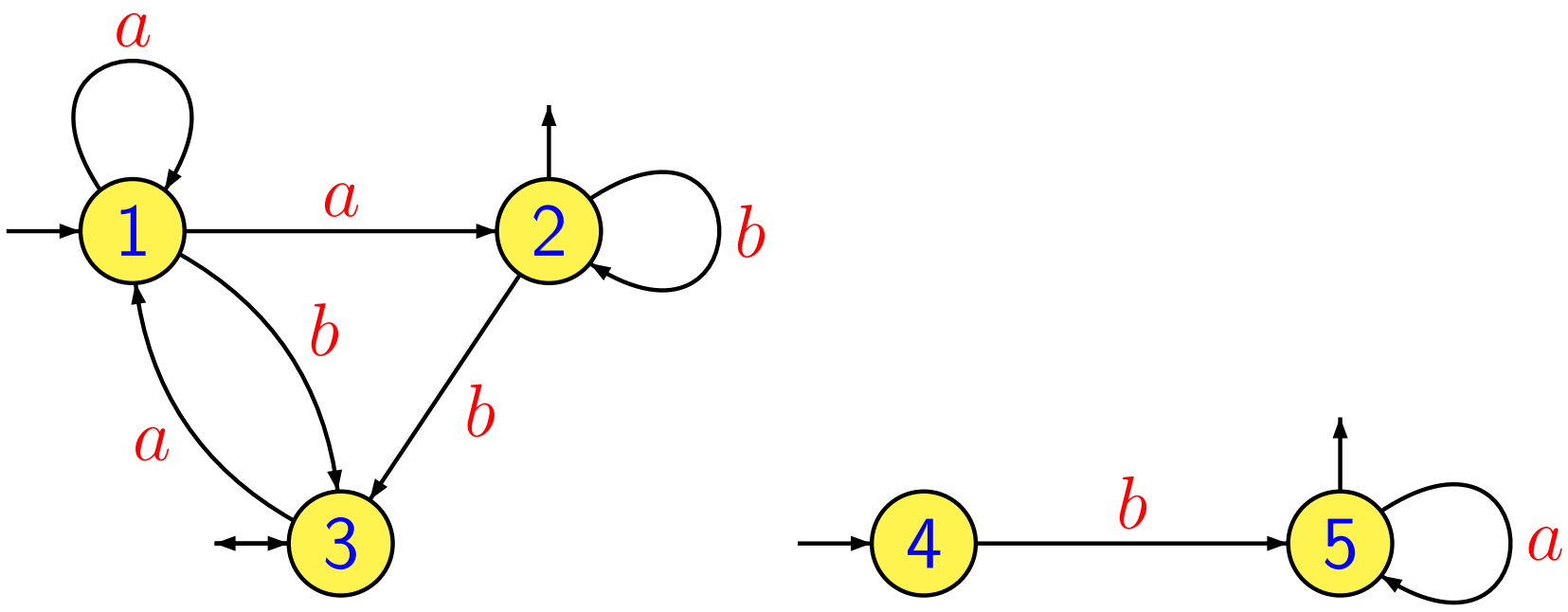
Automates

Un automate est un quintuplet

$$\mathcal{A} = (Q, A, E, I, F)$$

où Q est un ensemble fini appelé l'ensemble des états, A est un alphabet, E est un sous-ensemble de $Q \times A \times Q$, appelé l'ensemble des transitions, I et F sont des parties de Q, appelées resp. l'ensemble des états initiaux et l'ensemble des états finaux.

Un exemple d'automate



Les états initiaux sont 1, 3 et 4, les états finaux sont 2, 3 et 5.

Langages

Un langage (sur l'alphabet A) est une partie de A^*.

Le langage reconnu par un automate est l'ensemble des mots ayant au moins une lecture réussie dans l'automate, i.e. issue d'un état initial, et arrivant dans un état final.

Un langage est reconnaissable s'il existe un automate qui le reconnait.

Deux automates sont équivalents s'ils reconnaissent le même langage.

Automates déterministes

Un automate déterministe est un quintuplet

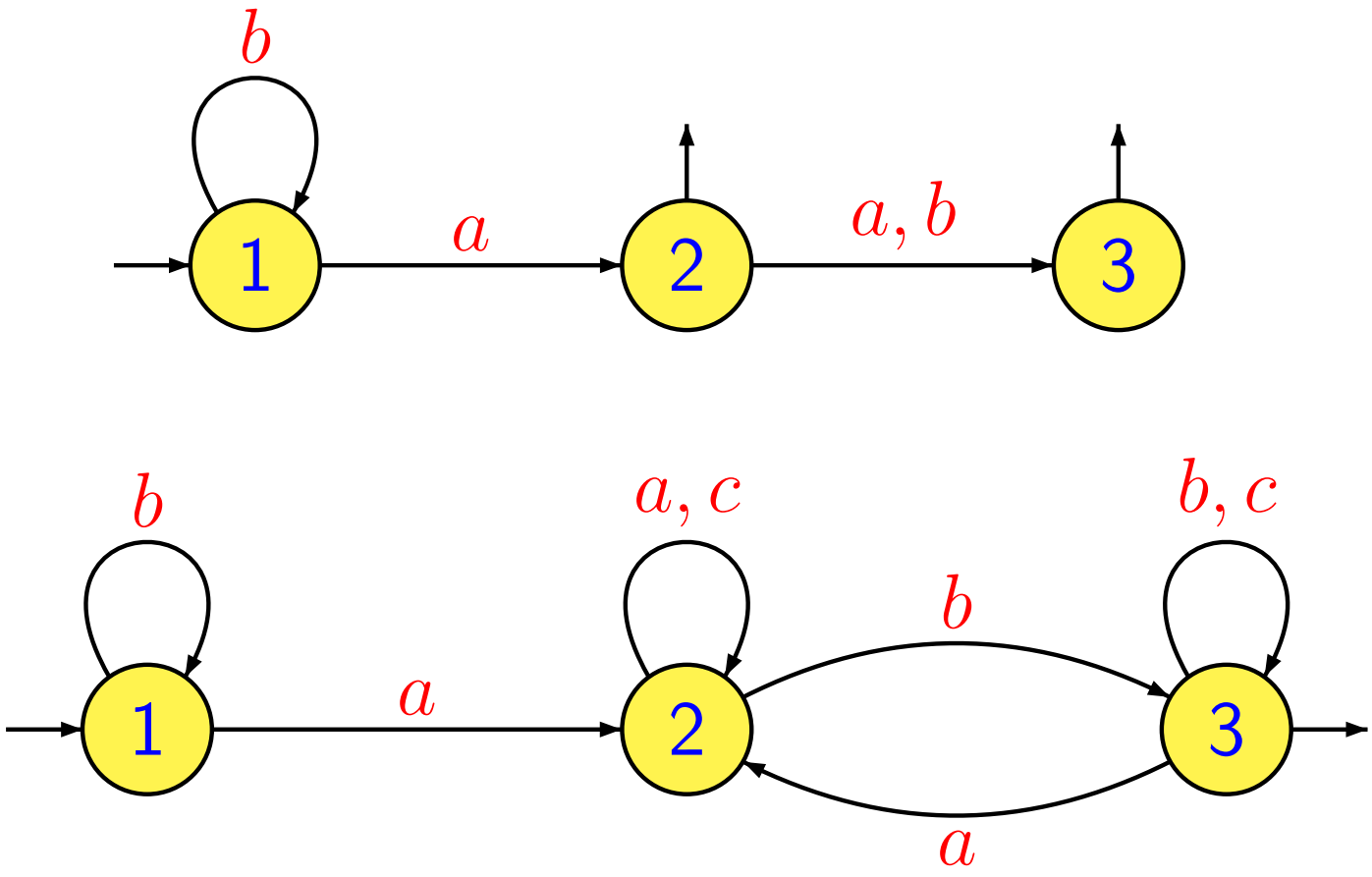
$$\mathcal{A} = (Q, A, q_0, \cdot, F)$$

où Q est un ensemble fini appelé l'ensemble des états, A est un alphabet, $q_0 \in Q$ est l'état initial, $F \subseteq Q$ est l'ensemble des états finaux. Enfin, la fonction

$$(q, a) \to q \cdot a$$

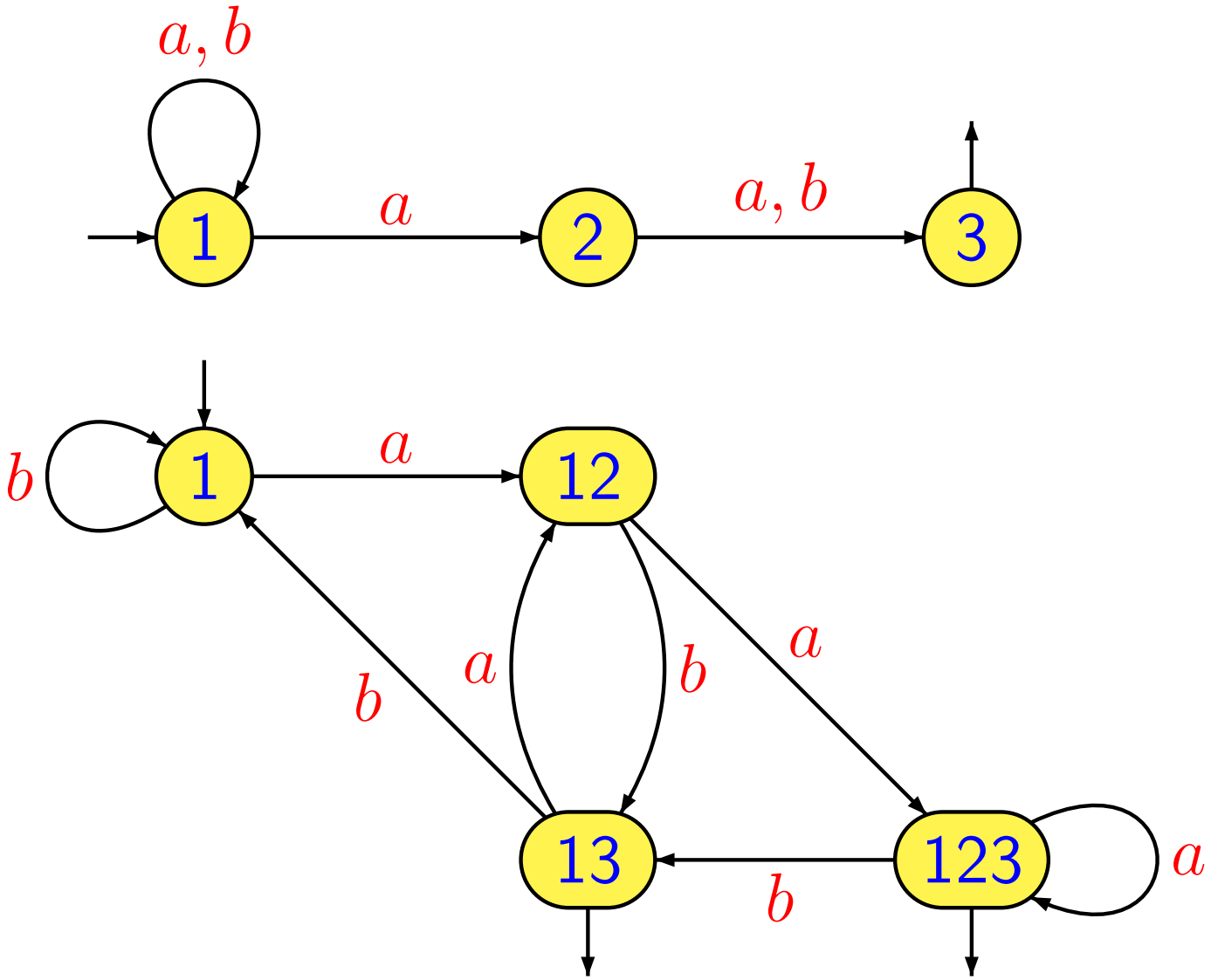
de $Q \times A$ dans Q, est la fonction de transition de $\mathcal{A}$.

Deux automates déterministes



$1 \cdot a = 2, \quad 1 \cdot b = 1, \quad 1 \cdot c$ non défini, $\quad 1 \cdot acbbca = 2$

Tout automate est équivalent à un déterministe



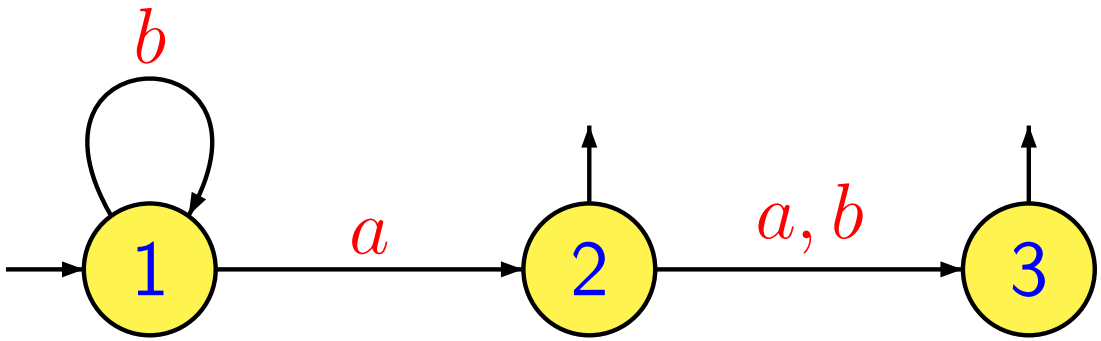
Automate minimal

Dans un automate déterministe, on peut éliminer tous les états qui ne sont pas accessibles à partir de l'état initial ou à partir desquels on ne peut pas atteindre un état final.

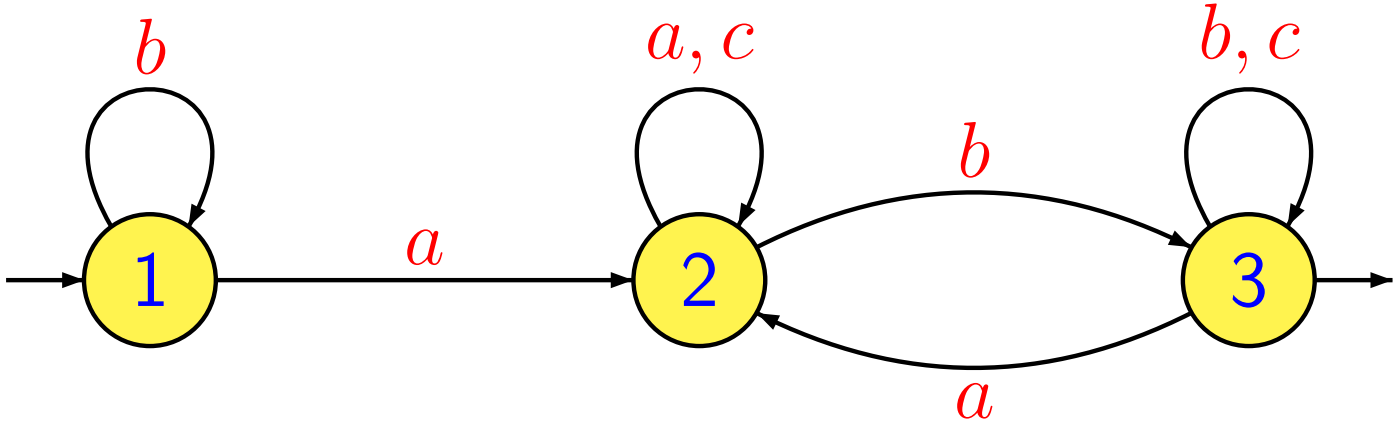
Equivalence sur l'ensemble des états : deux états p et q sont équivalents si, pour tout mot u, l'état $p \cdot u$ est final ssi l'état $q \cdot u$ l'est aussi. On peut identifier des états équivalents sans changer le langage reconnu. L'automate obtenu après cette identification est l'automate minimal.

Les langages reconnus.

$b^*a + b^*aa + b^*ab$



$b^*aA^*b\{b, c\}^*$



Opérations sur les langages

Soient L, L_1 et L_2 des langages de A^*.

Union : $L_1 + L_2$

Produit (de concaténation) :
$L_1 L_2 = \{u_1 u_2 \mid u_1 \in L_1, u_2 \in L_2\}$

Etoile : $L^* = \{u \in A^* \mid$ il existe $n \geqslant 0$ et des mots $u_1, \ldots, u_n$ de L tels que $u = u_1 u_2 \cdots u_n\}$

Remarque : L^* est aussi le sous-monoïde de A^* engendré par L.

Langages rationnels

La classe des langages rationnels est la plus petite classe de langages contenant les langages finis, et fermée par union, produit et étoile.

Théorème (Kleene 1954)

Un langage est rationnel ssi si il est reconnaissable.

Corollaire

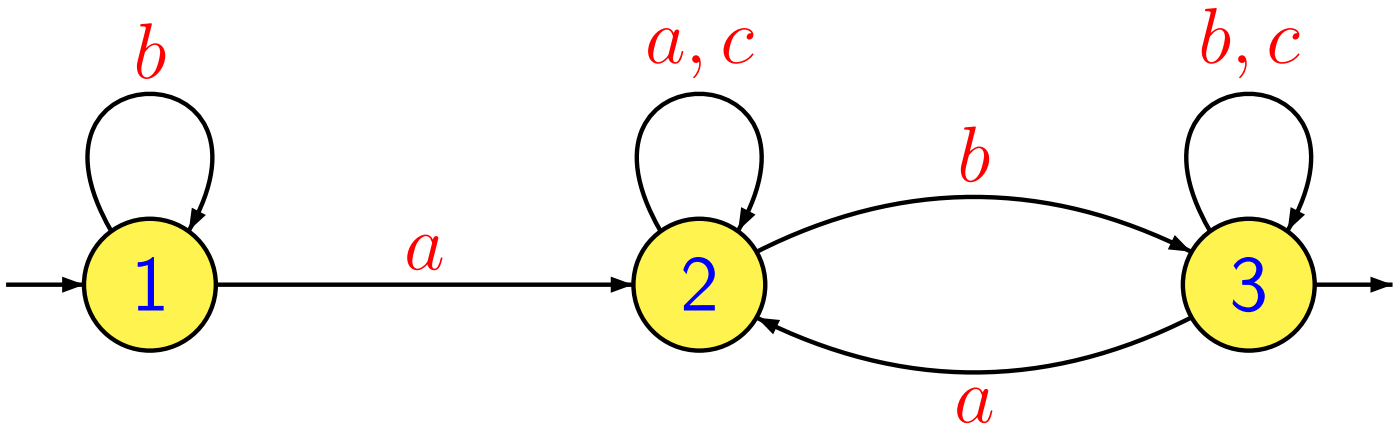
Les langages rationnels sont fermés par intersection et par complémentation (dans A^*).

Deuxième partie II

L'approche algébrique

Idée : remplacer les automates par des monoïdes.

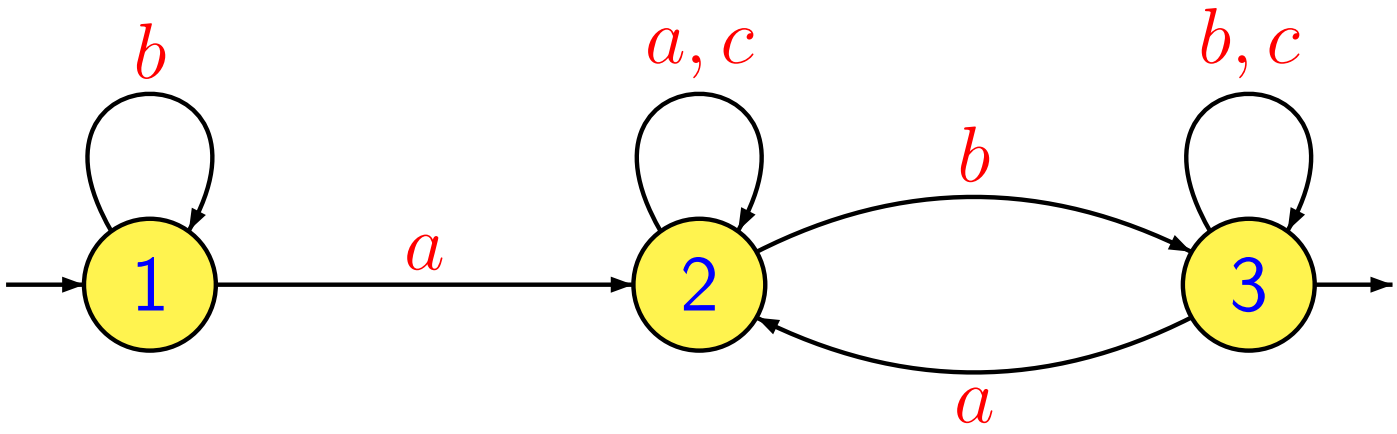
Monoïde de transition d'un automate



1	1	2	3
a	2	2	2
b	1	3	3
c	-	2	3

Relations :

Monoïde de transition d'un automate

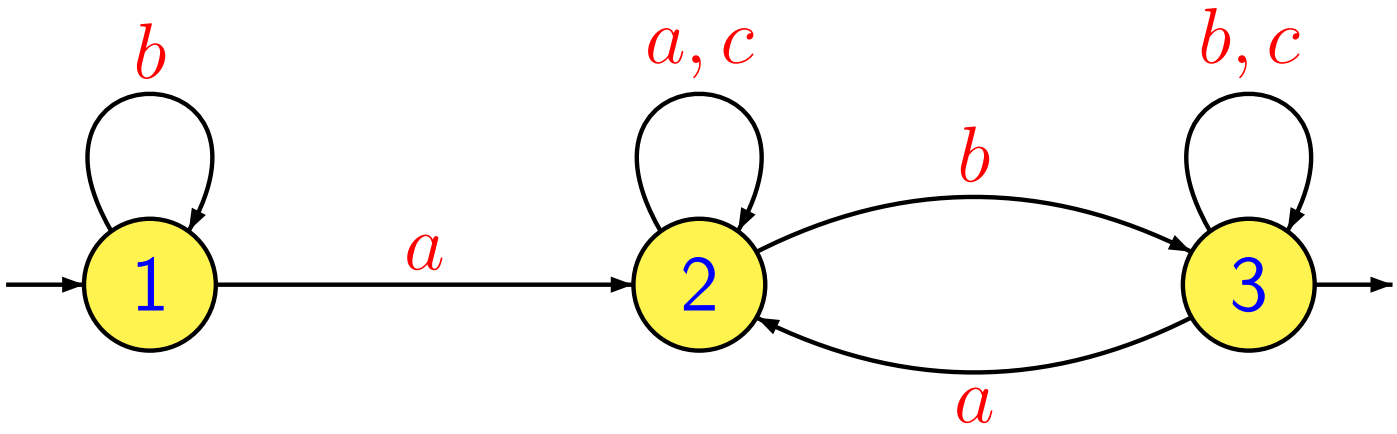


1	1	2	3
a	2	2	2
b	1	3	3
c	-	2	3

Relations :

$aa = a$

Monoïde de transition d'un automate

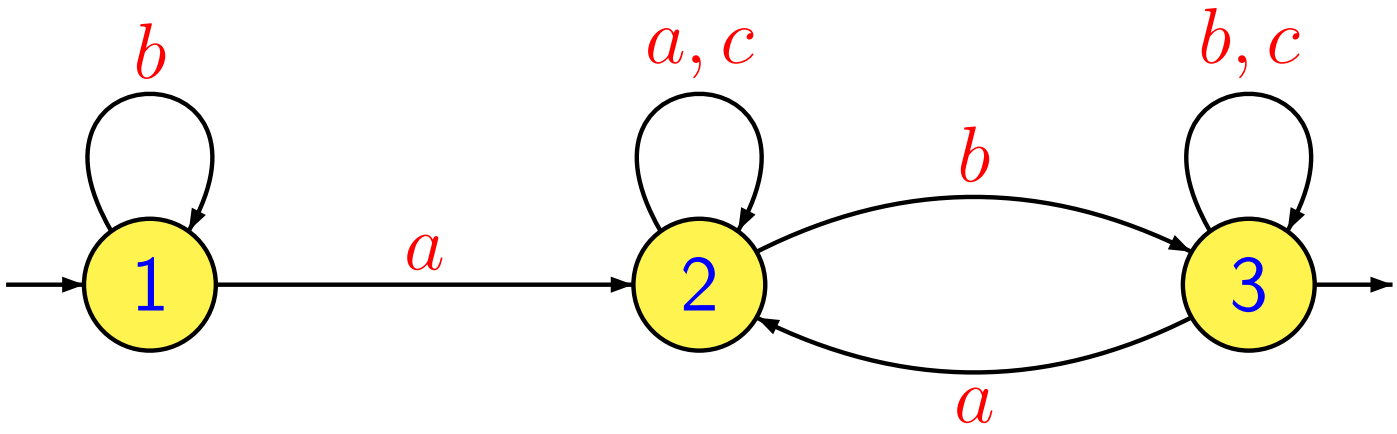


1	1	2	3
a	2	2	2
b	1	3	3
c	-	2	3
ab	3	3	3

Relations :

$$aa = a$$

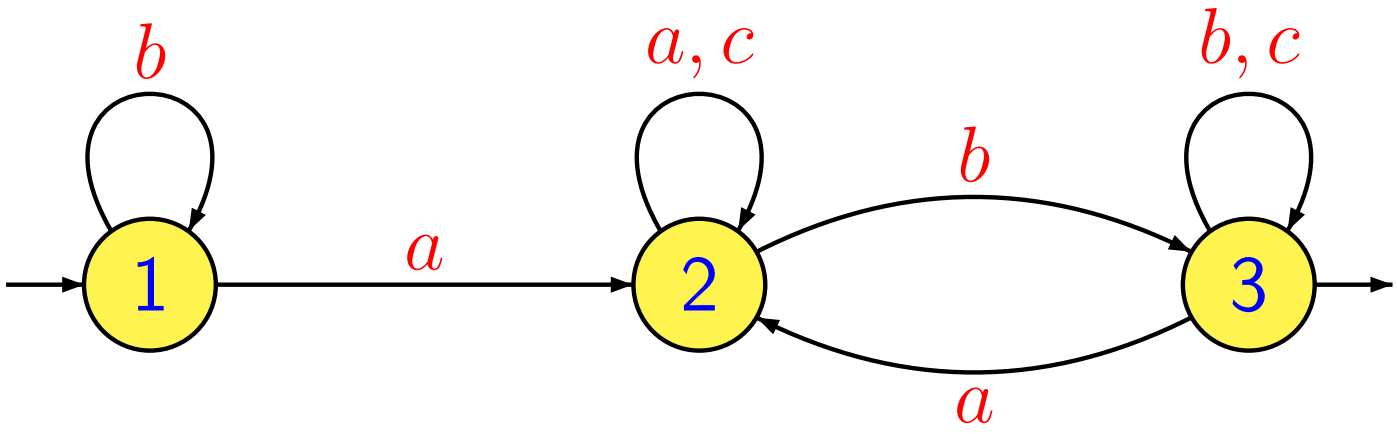
Monoïde de transition d'un automate



1	1	2	3
a	2	2	2
b	1	3	3
c	-	2	3
ab	3	3	3

Relations :
$aa = a$
$ac = a$

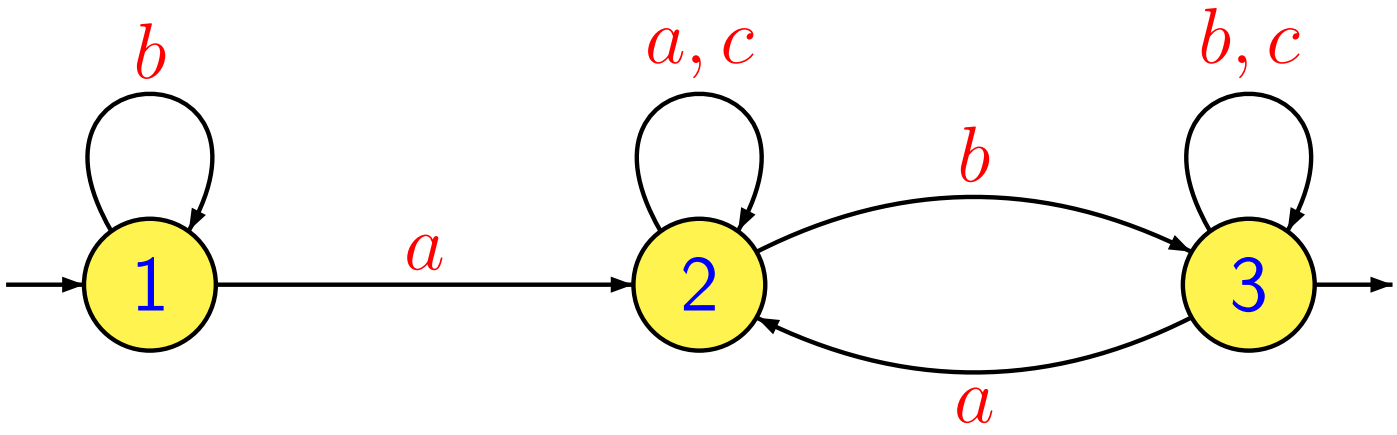
Monoïde de transition d'un automate



1	1	2	3
a	2	2	2
b	1	3	3
c	-	2	3
ab	3	3	3

Relations :
$aa = a$
$ac = a$
$ba = a$

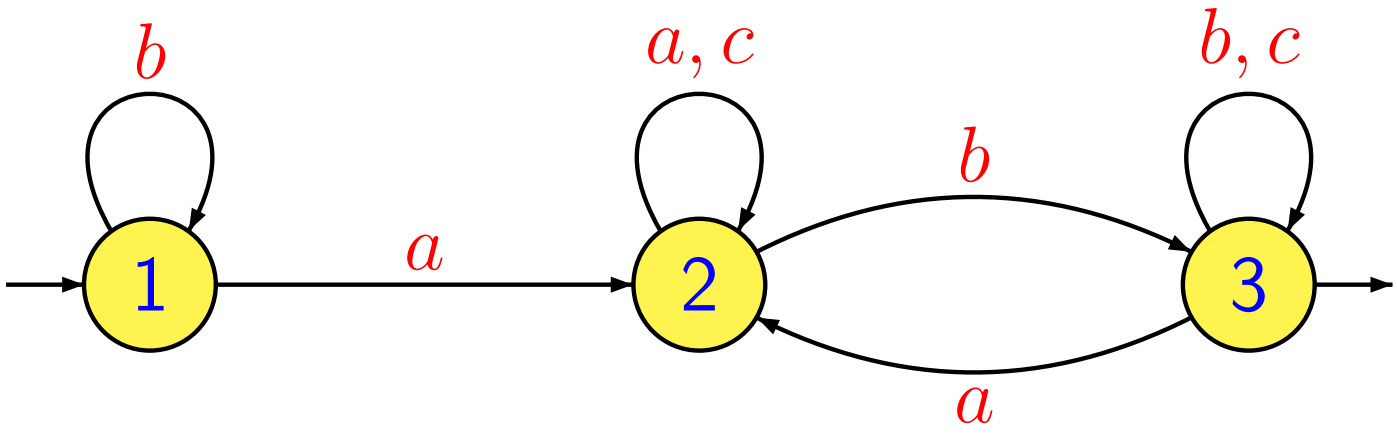
Monoïde de transition d'un automate



1	1	2	3
a	2	2	2
b	1	3	3
c	-	2	3
ab	3	3	3

Relations :
$aa = a$
$ac = a$
$ba = a$
$bb = b$

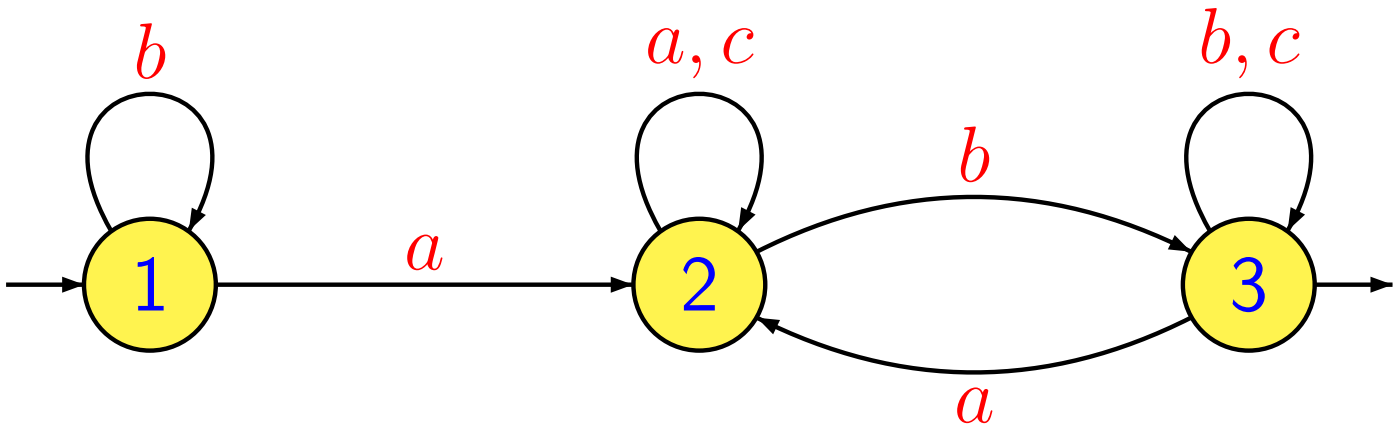
Monoïde de transition d'un automate



1	1	2	3
a	2	2	2
b	1	3	3
c	-	2	3
ab	3	3	3
bc	-	3	3

Relations :
$aa = a$
$ac = a$
$ba = a$
$bb = b$

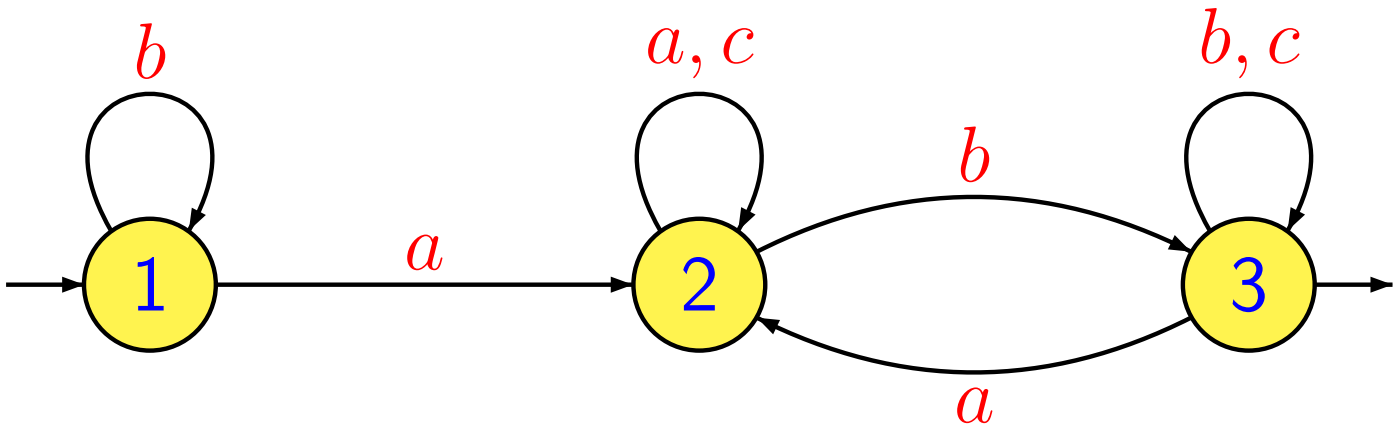
Monoïde de transition d'un automate



1	1	2	3
a	2	2	2
b	1	3	3
c	-	2	3
ab	3	3	3
bc	-	3	3
ca	-	2	2

Relations :
$aa = a$
$ac = a$
$ba = a$
$bb = b$

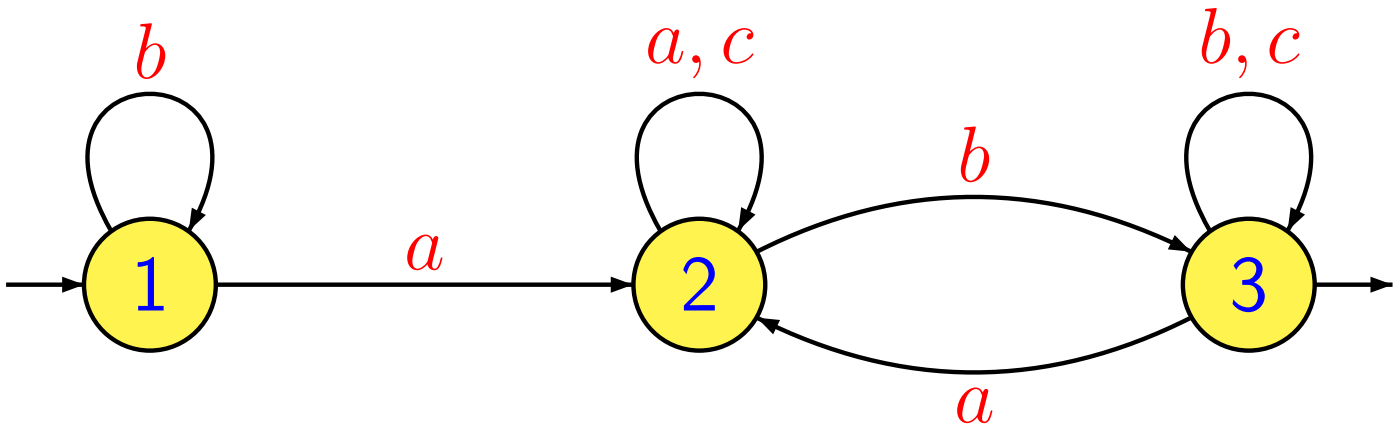
Monoïde de transition d'un automate



1	1	2	3
a	2	2	2
b	1	3	3
c	-	2	3
ab	3	3	3
bc	-	3	3
ca	-	2	2

Relations :
$aa = a$
$ac = a$
$ba = a$
$bb = b$
$cb = bc$

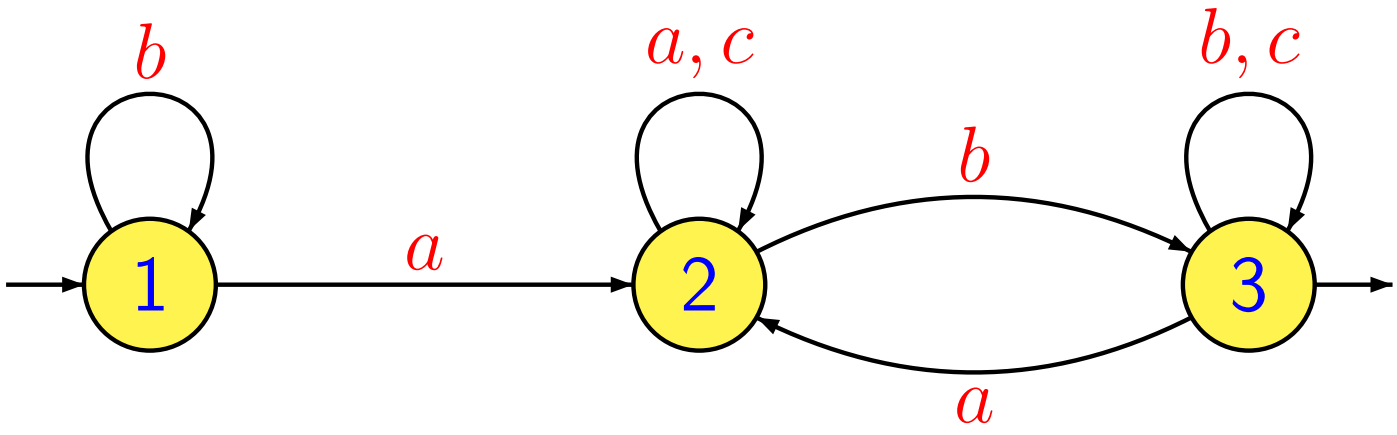
Monoïde de transition d'un automate



1	1	2	3
a	2	2	2
b	1	3	3
c	-	2	3
ab	3	3	3
bc	-	3	3
ca	-	2	2

Relations :
$aa = a$
$ac = a$
$ba = a$
$bb = b$
$cb = bc$
$cc = c$

Monoïde de transition d'un automate

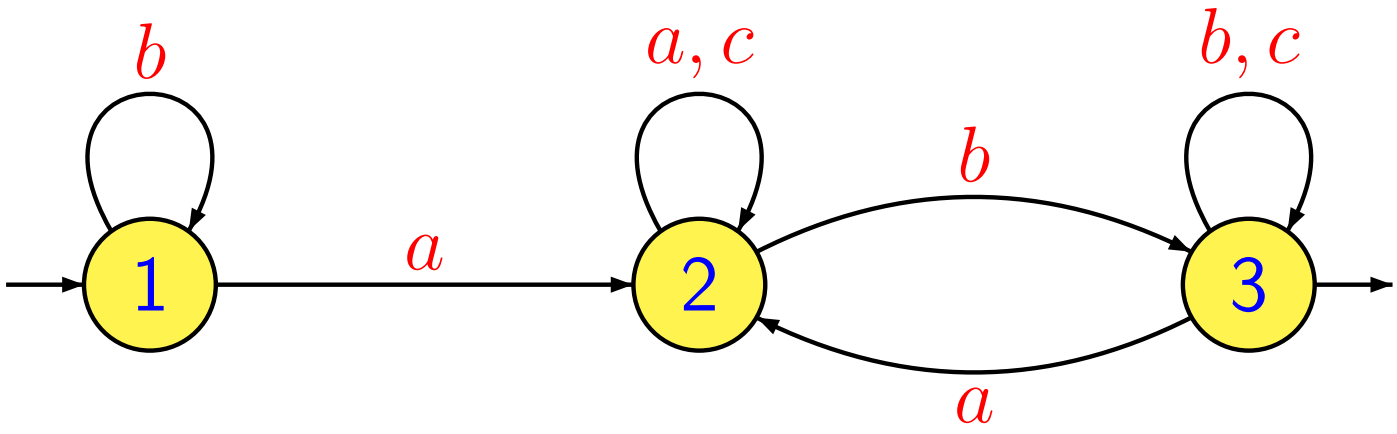


1	1	2	3
a	2	2	2
b	1	3	3
c	-	2	3
ab	3	3	3
bc	-	3	3
ca	-	2	2

Relations :
$aa = a$
$ac = a$
$ba = a$
$bb = b$
$cb = bc$
$cc = c$

$$abc = ab$$

Monoïde de transition d'un automate

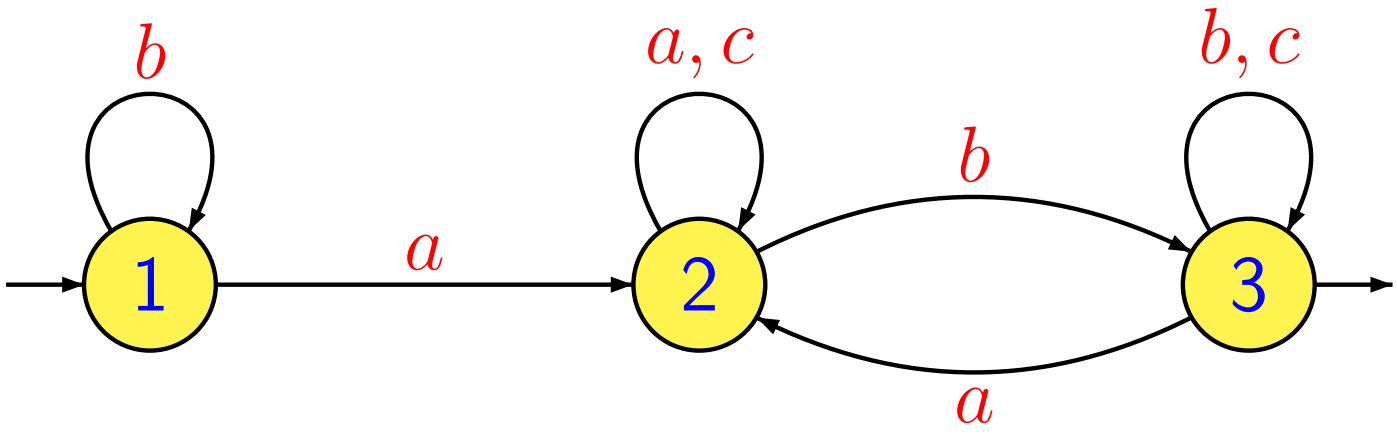


1	1	2	3
a	2	2	2
b	1	3	3
c	-	2	3
ab	3	3	3
bc	-	3	3
ca	-	2	2

Relations :
$aa = a$
$ac = a$
$ba = a$
$bb = b$
$cb = bc$
$cc = c$

$$abc = ab$$
$$bca = ca$$

Monoïde de transition d'un automate



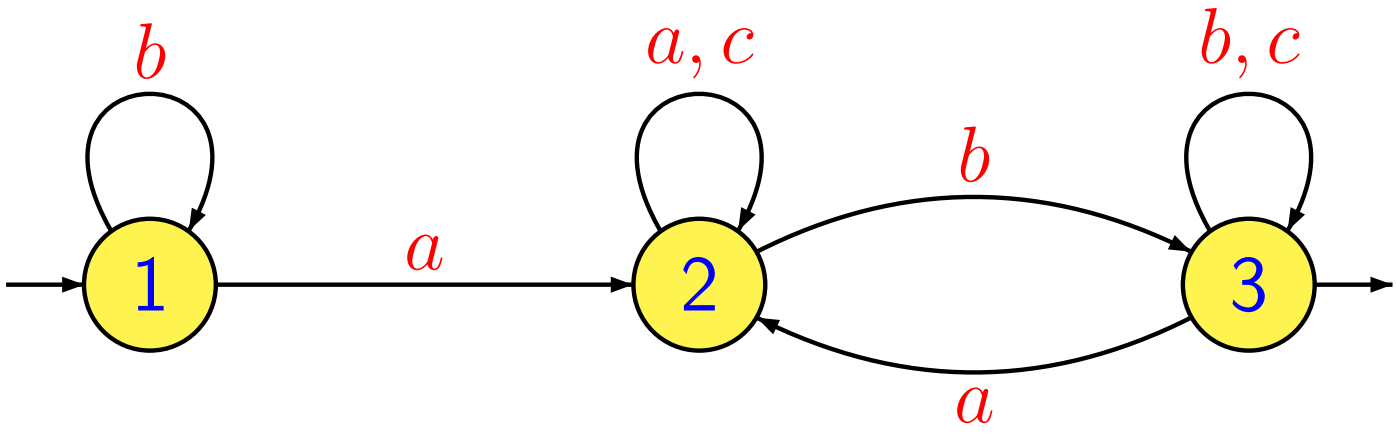
1	1	2	3
a	2	2	2
b	1	3	3
c	-	2	3
ab	3	3	3
bc	-	3	3
ca	-	2	2

Relations :

$$aa = a$$
$$ac = a$$
$$ba = a$$
$$bb = b$$
$$cb = bc$$
$$cc = c$$

$$abc = ab$$
$$bca = ca$$
$$cab = bc$$

Monoïde de transition d'un automate



1	1	2	3
a	2	2	2
b	1	3	3
c	-	2	3
ab	3	3	3
bc	-	3	3
ca	-	2	2

Relations :

$$aa = a$$
$$ac = a$$
$$ba = a$$
$$bb = b$$
$$cb = bc$$
$$cc = c$$

$$abc = ab$$
$$bca = ca$$
$$cab = bc$$

Fin !

Morphisme naturel

Soit M le monoïde de transitions de $\mathcal{A}$ et soit $\varphi : A^* \to M$ le morphisme de monoïde défini par $\varphi(a) = a$ pour tout $a \in A$. Autrement dit $\varphi(u)$ est la transformation sur Q définie par u.

Deux mots u et v tels que $\varphi(u) = \varphi(v)$ ont la même action sur l'automate. Ils sont donc simultanément acceptés ou rejetés.

Remarque. La définition du monoïde de transition ne fait pas intervenir les états finaux.

Reconnaissance par morphisme

Définition

Soit M un monoïde et L un langage de A^*. On dit que M reconnait L s'il existe un morphisme de monoïde $\varphi : A^* \to M$ et une partie P de M telle que $L = \varphi^{-1}(P)$.

Proposition

Un langage est reconnu par un monoïde fini ssi il est reconnu par un automate déterministe fini.

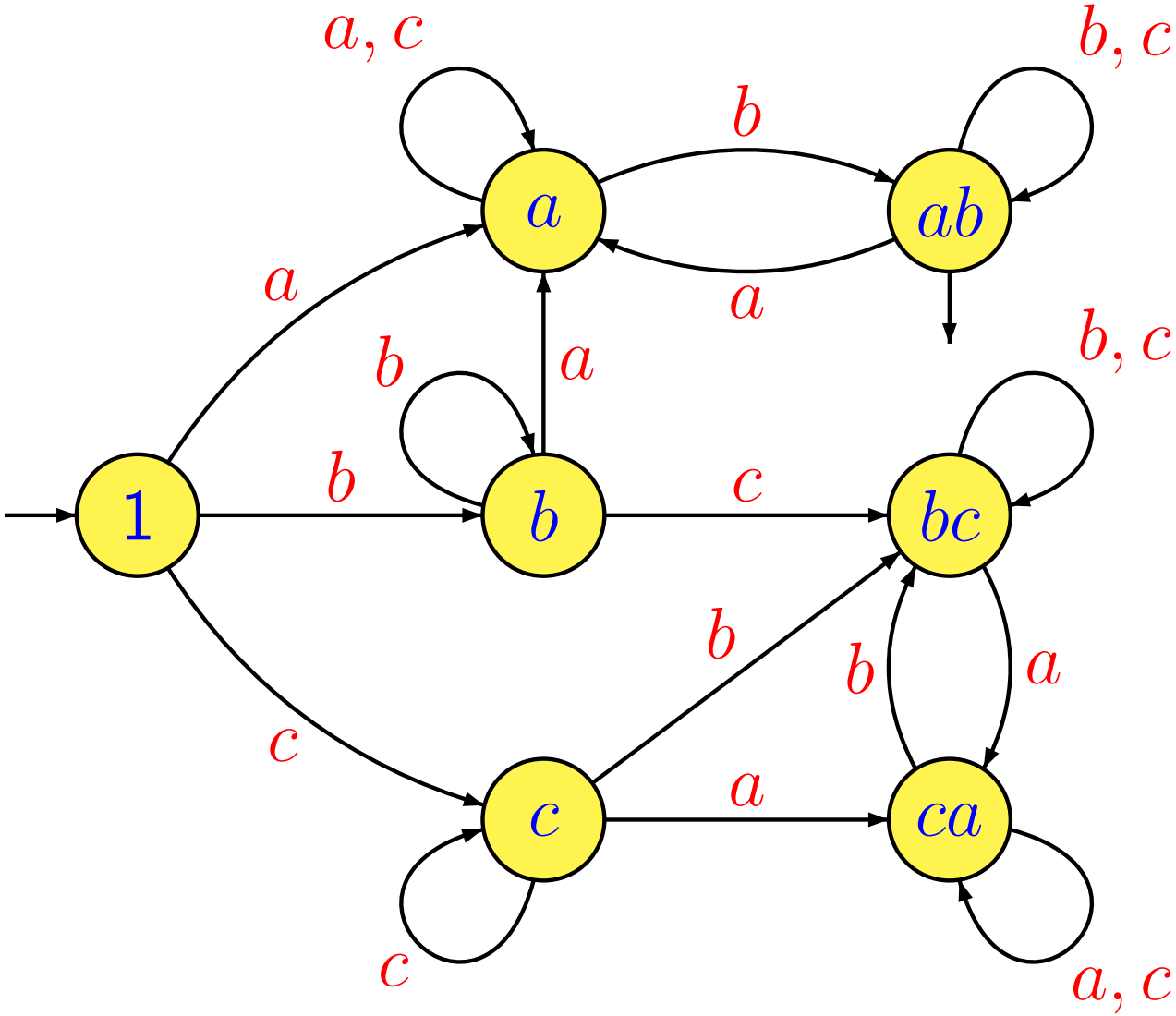
Des morphismes aux automates

Soit $\varphi : A^* \to M$ un morphisme de monoïdes, qui définit une action de A sur M :

$$m \cdot a = m\varphi(a)$$

Le graphe de Cayley de (M, A) a pour ensemble de sommets M. Ses arcs sont de la forme $m \xrightarrow{a} m \cdot a$ pour $m \in M$ et $a \in A$.
On prend 1 comme état initial et on prend comme états finaux les éléments de $\varphi(L)$.

Le graphe de Cayley vu comme un automate



Monoïde syntactique

Définition (algorithmique)

Le monoïde syntactique d'un langage est le monoïde de transition de son automate minimal.

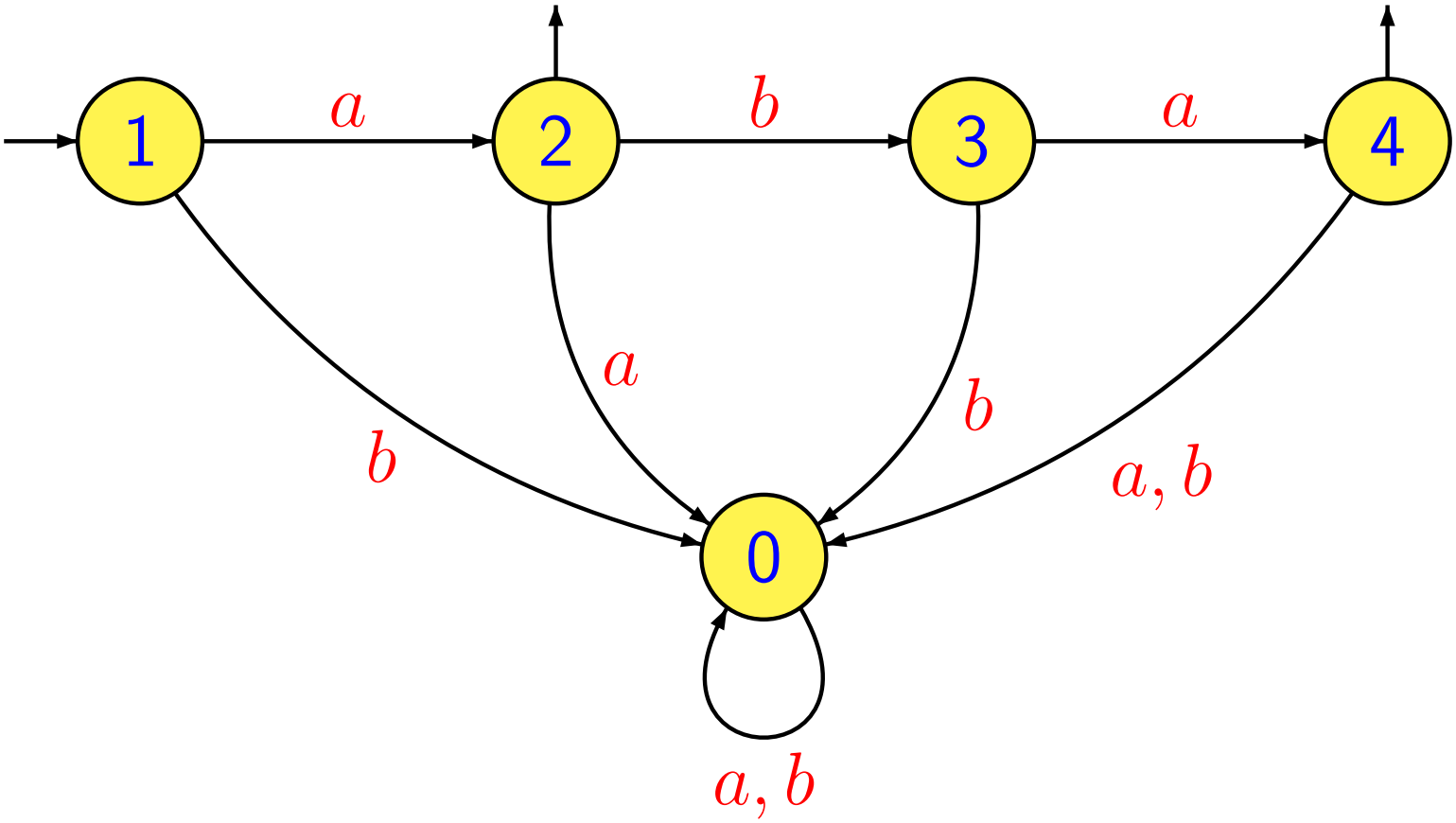
Définition (algébrique)

Le monoïde syntactique d'un langage $L \subset A^*$ *est le monoïde quotient de* A^* *par la congruence syntactique de* L *:* $u \sim_L v$ *ssi, pour tout* $x, y \in A^*$, $xvy \in L \Leftrightarrow xuy \in L$

Un peu d'ordre !

Soit $\mathcal{A} = (Q, A, \cdot, q_0, F)$ un automate minimal. On définit une relation $\leqslant$ sur Q en posant $p \leqslant q$ ssi pour tout $u \in A^*$, $q \cdot u \in F \Rightarrow p \cdot u \in F$.

Exemple



L'ordre est ici $1 \leqslant 3$, $2 \leqslant 4$ et $1, 2, 3, 4 \leqslant 0$.

Monoïde syntactique ordonné

Définition (algorithmique)

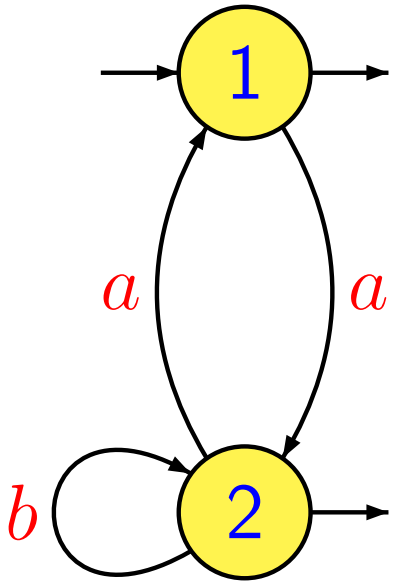
C'est le monoïde de transition de l'automate minimal, ordonné par $u \leqslant v$ *ssi pour tout* $q \in Q$, $q \cdot u \leqslant q \cdot v$.

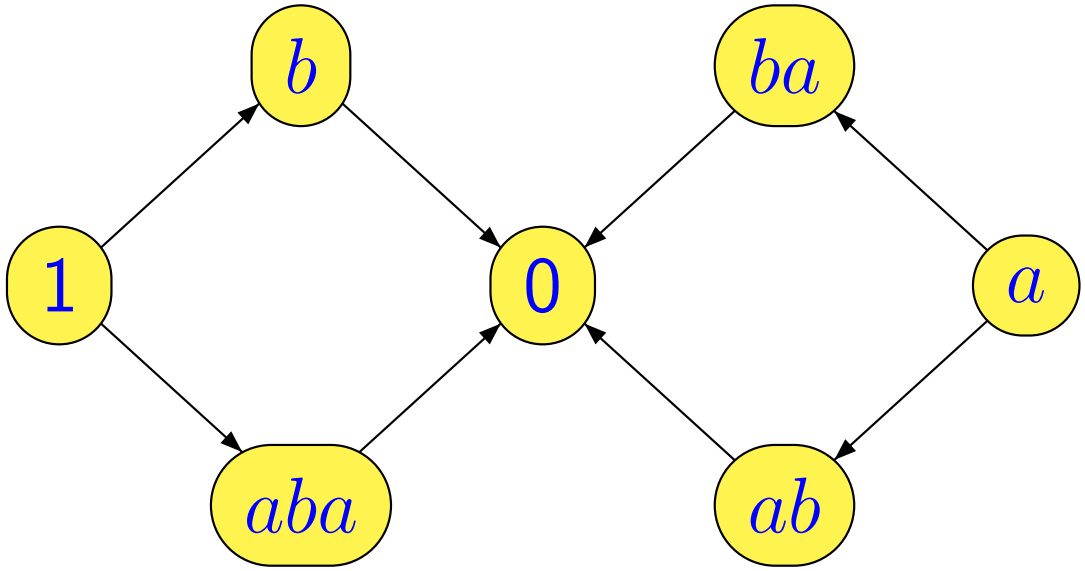
Définition (algébrique)

C'est le monoïde syntactique, muni de l'ordre induit par l'ordre syntactique : $u \leqslant_L v$ *ssi, pour tout* $x, y \in A^*$, $xvy \in L \Rightarrow xuy \in L$.

L'ordre syntactique de $L = (ab^*a)^*(1 + a)$.

$u \leqslant v$ ssi $xvy \in L \Rightarrow xuy \in L$.





$1 \leqslant b$ puisque $ubv \in L \Rightarrow uv \in L$.

$1 \not\leqslant ab$ puisque $1(ab)ba \in L$ mais $1(1)ba \notin L$.

Troisième partie III

Automates réversibles

Automates réversibles

Un automate réversible est un automate dans lequel chaque lettre induit une fonction injective de l'ensemble des états dans lui-même. Les transitions d'un automate réversible sont déterministes et co-déterministes.

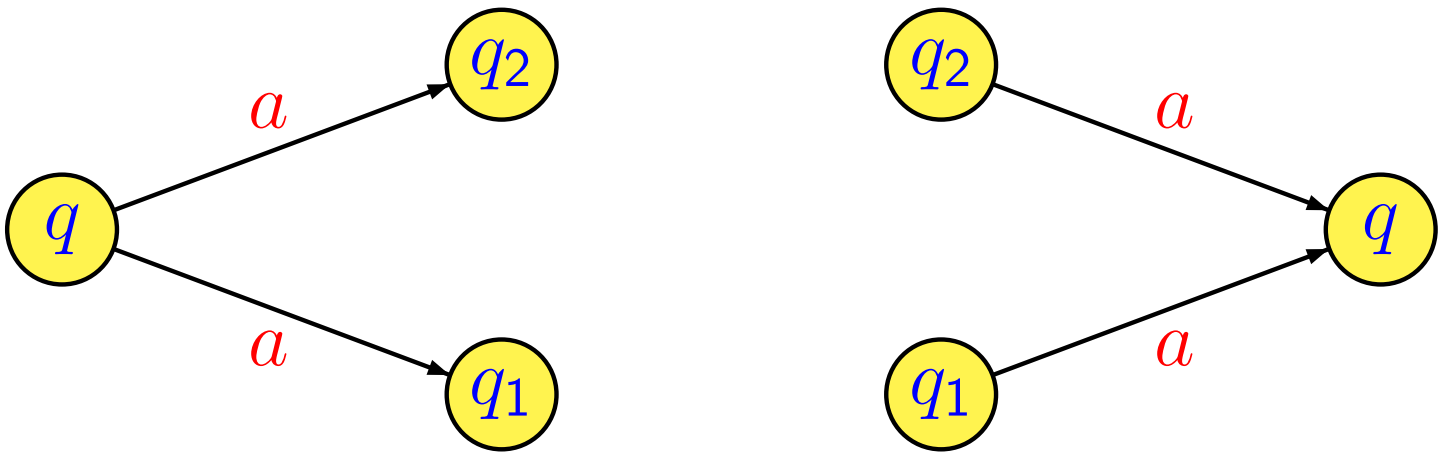
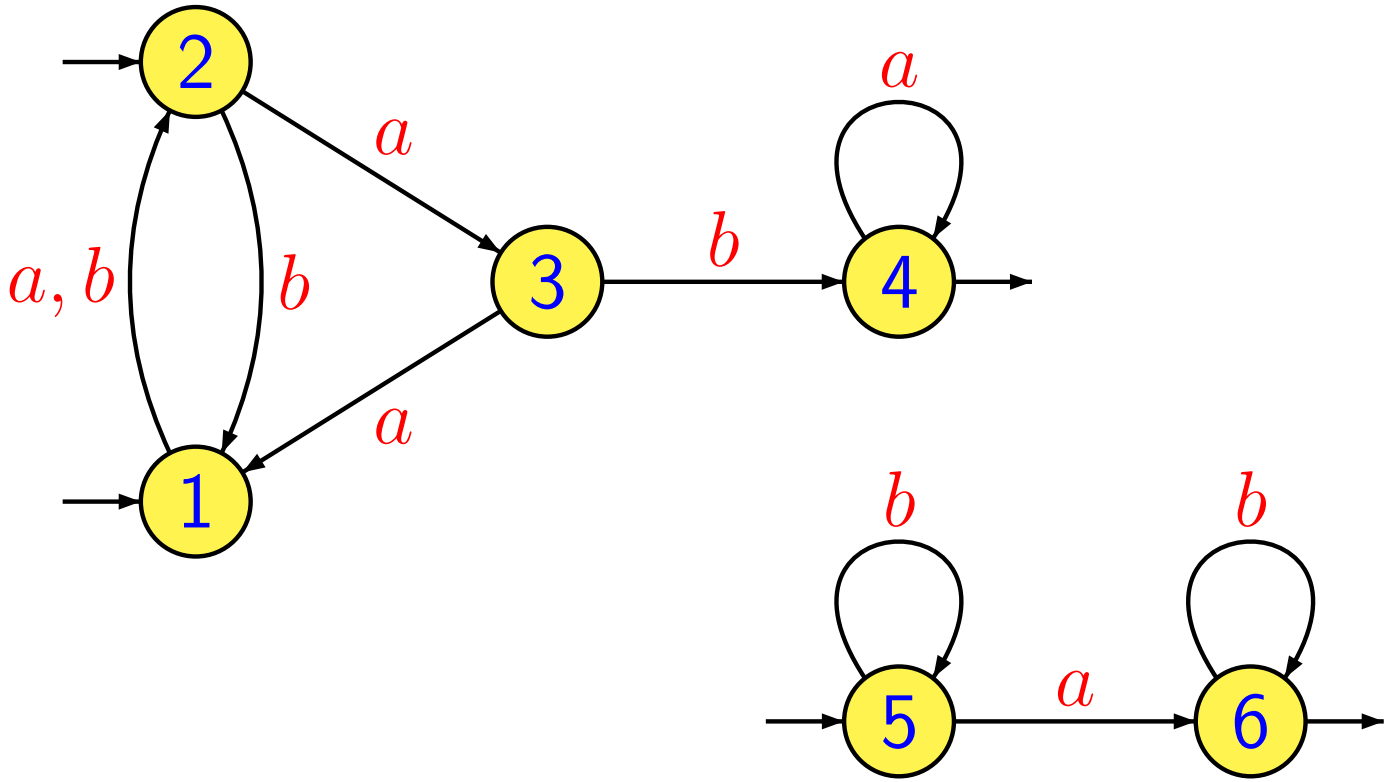


FIG.: Configurations interdites dans un automate réversible.

Un exemple d'automate réversible



Langages réversibles

Définition

Un langage est réversible s'il est accepté par un automate réversible (muni de plusieurs états initiaux et de plusieurs états finaux).

Problème

Peut-on décider si un langage rationnel donné est réversible ?

Mise en garde

L'automate minimal d'un langage réversible n'est pas nécessairement réversible !

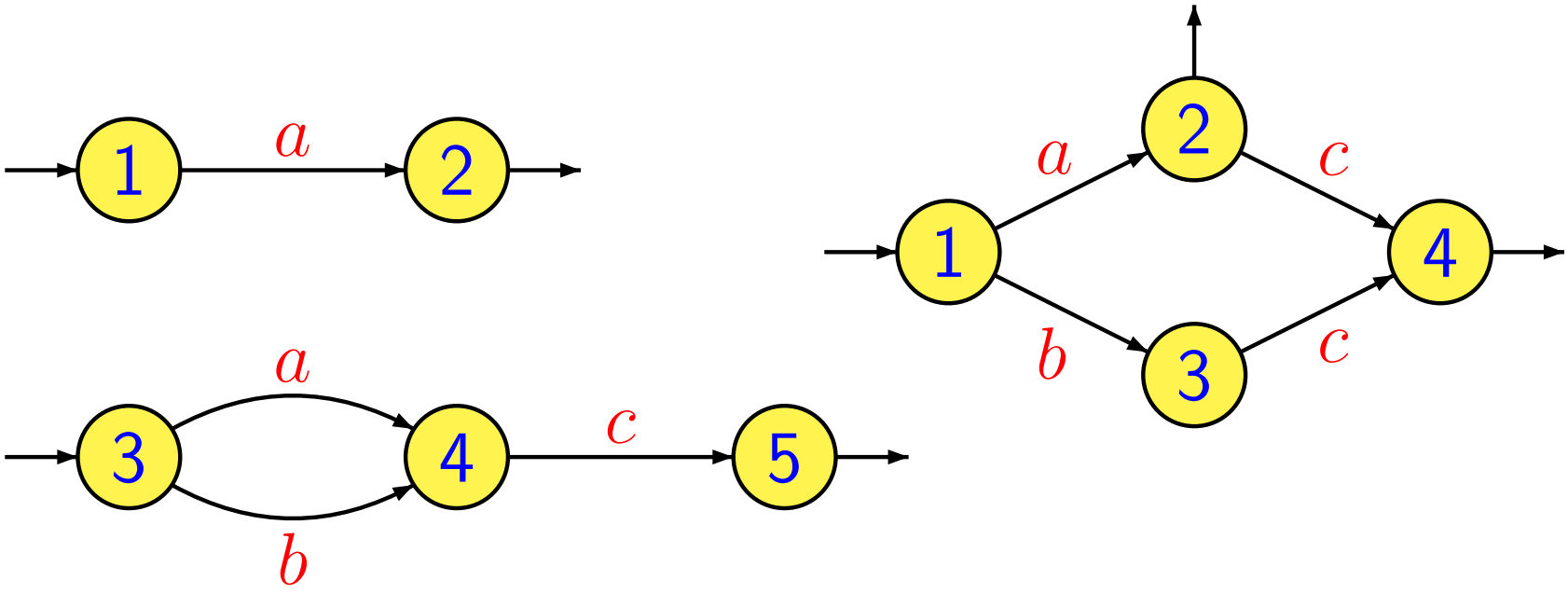


FIG.: Automates réversible et minimal de $\{a, ac, bc\}$.

Exemples de langages réversibles

- Les langages finis sont réversibles.
- Les langages à groupe (c'est-à-dire reconnus par des groupes finis ou, si l'on préfère, par des automates de permutations) sont réversibles.
- Toute combinaison booléenne positive (i.e. union finie d'intersections finies) de langages réversibles est réversible.

Description des langages réversibles

Proposition

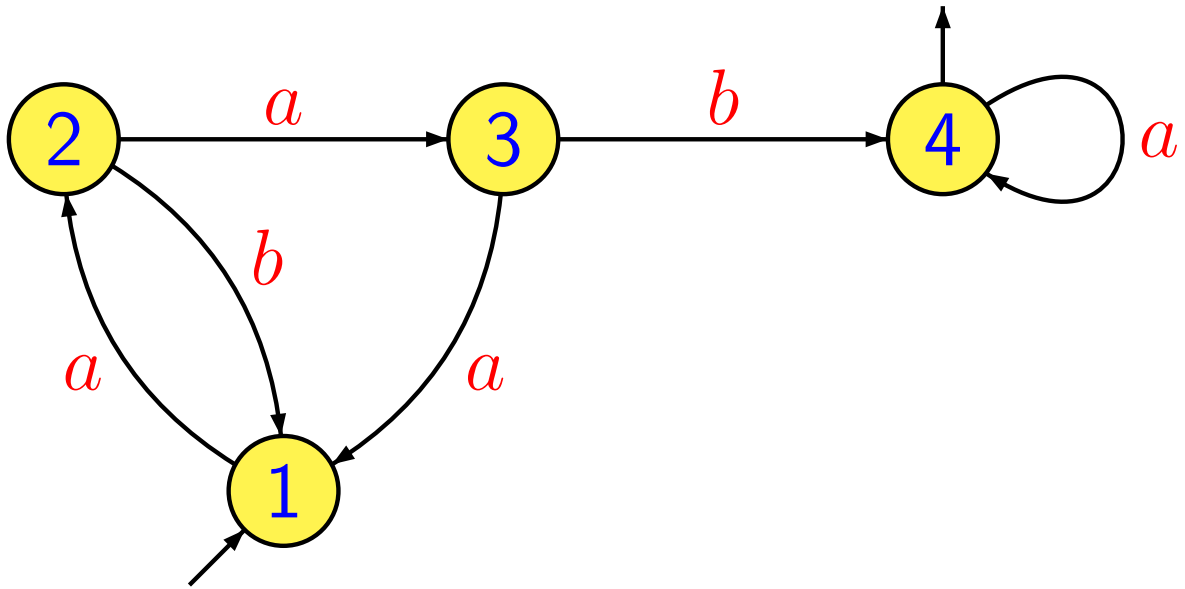
Soit L un langage réversible de A^*. Alors

(1) *L^c est une combinaison booléenne positive de langages de la forme R ou A^*aR où R est un langage à groupe,*

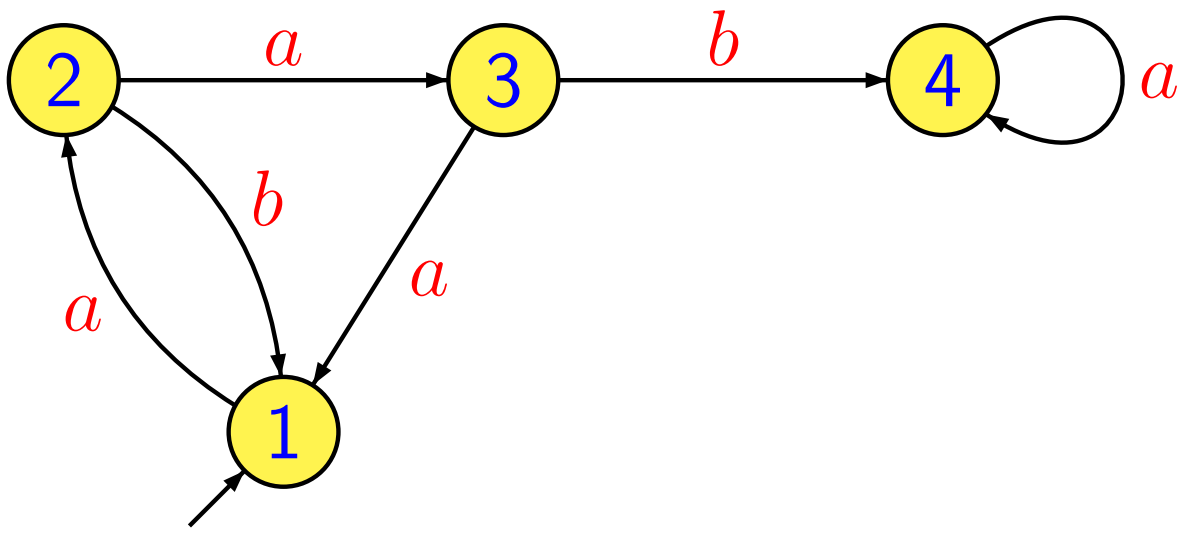
(2) *L^c est une combinaison booléenne positive de langages de la forme R ou RaA^* où R est un langage à groupe.*

Preuve sur exemple

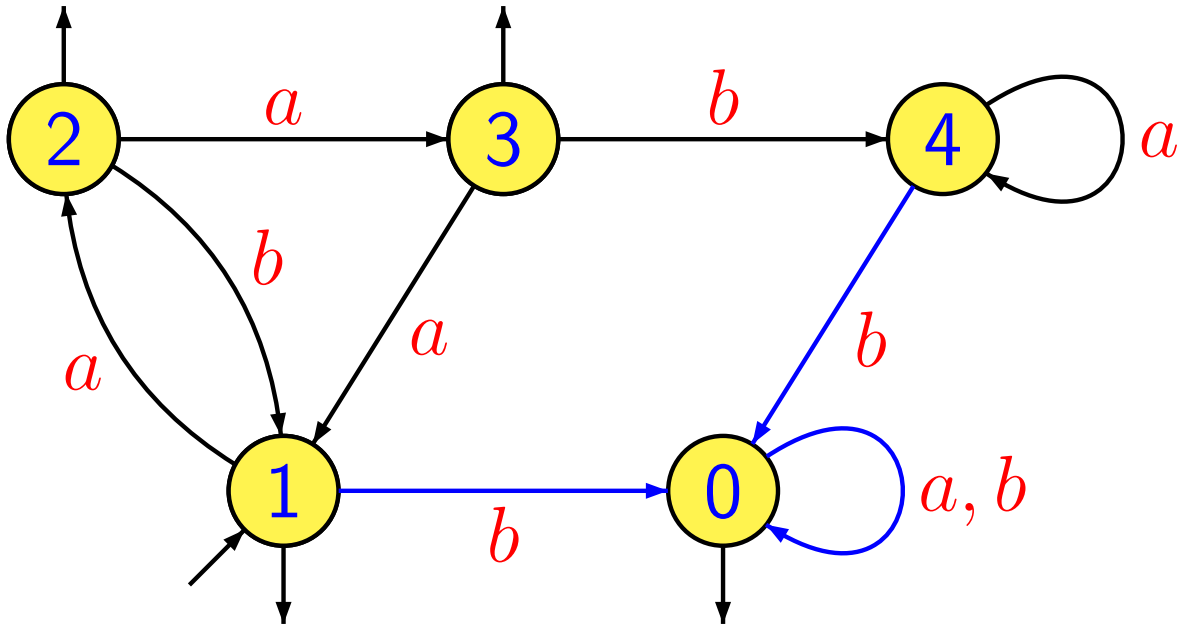
(1) On se ramène au cas d'un automate réversible ayant un seul état initial et un seul état final.



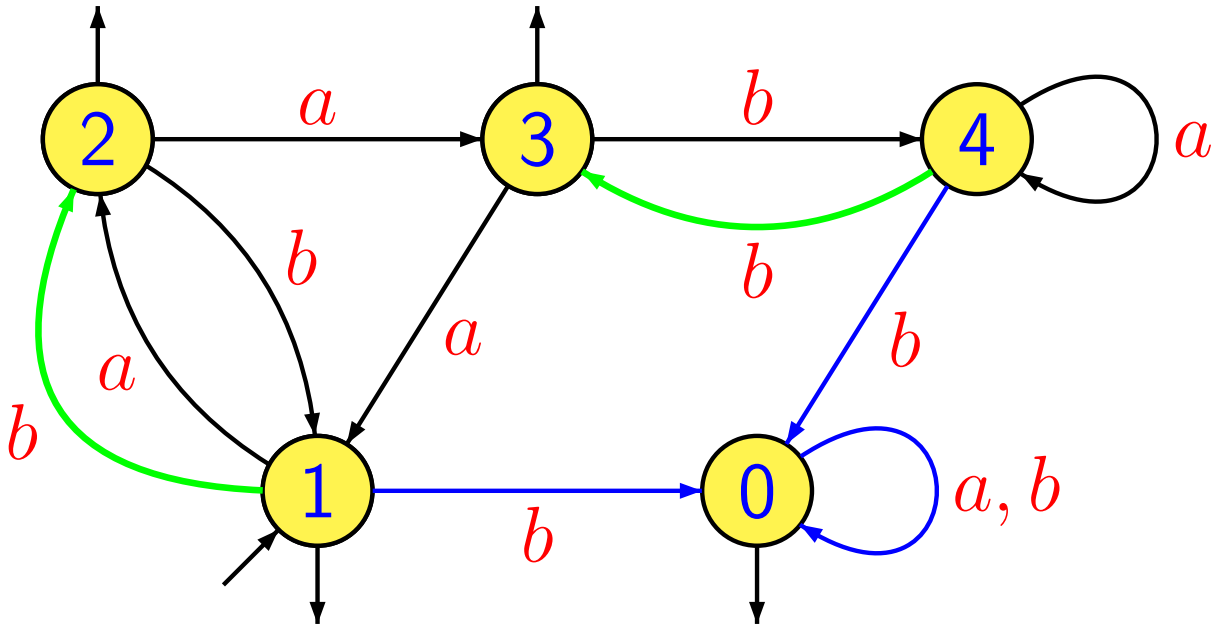
Automate du complémentaire



Automate du complémentaire

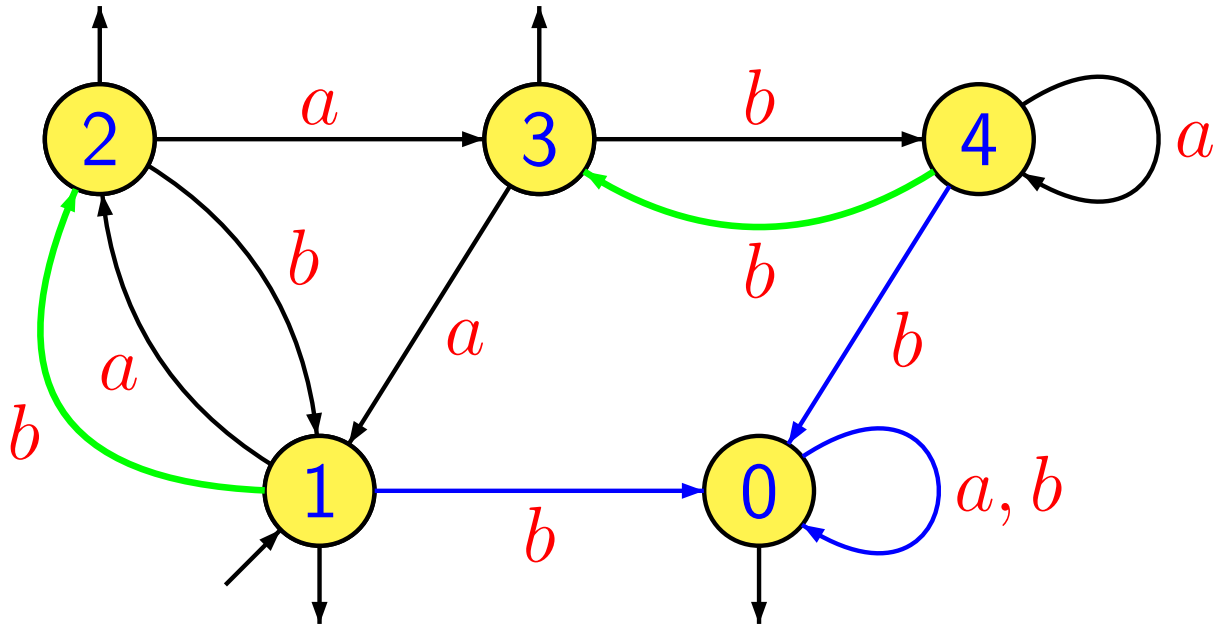


Automate du complémentaire



On ajoute les flèches vertes.

Automate du complémentaire



On ajoute les flèches vertes. Notons $R(q)$ le langage reconnu par l'automate à groupe obtenu en prenant $\{1, 2, 3, 4\}$ pour états et q comme état final. Alors $L^c = R(1) \cup R(2) \cup R(3) \cup R(1)bA^* \cup R(4)bA^*$.

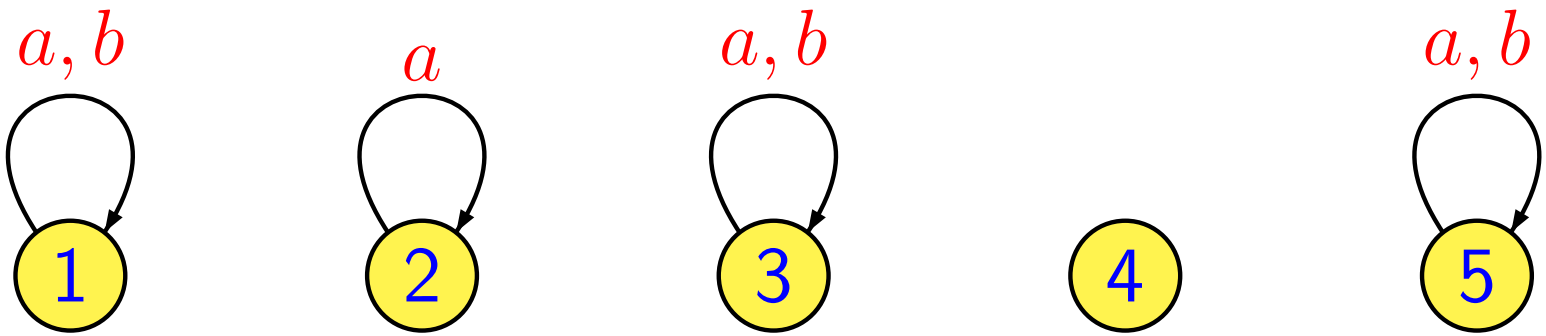
Première condition nécessaire

Un élément e est idempotent si $e^2 = e$.

Proposition

Les idempotents du monoïde syntactique d'un langage réversible commutent.

Idée : les fonctions définies par a et b commutent...



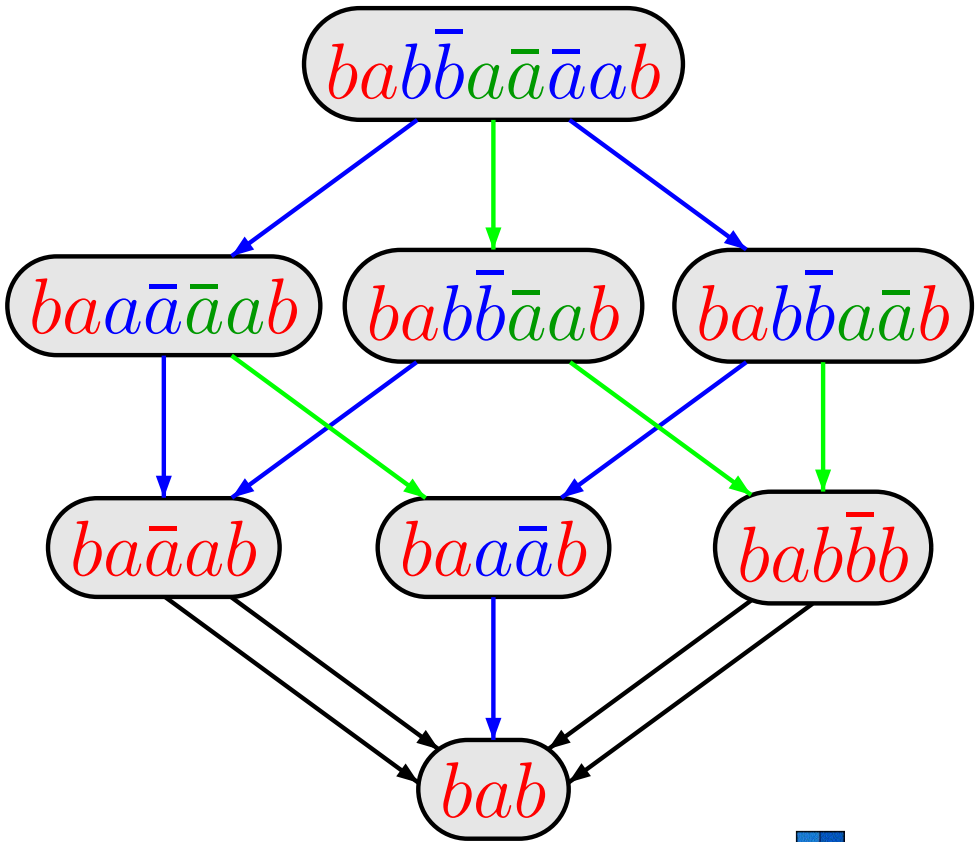
Quatrième partie IV

Groupe libre

Groupe libre sur l'ensemble A

Soit $\tilde{A} = A \cup \bar{A}$, où $\bar{A}$ est une copie de A. Le groupe libre sur A, noté $FG(A)$, est le quotient de $\tilde{A}^*$ par les relations $a\bar{a} = 1 = \bar{a}a$ (pour tout $a \in A$).

La réduction est confluente :



Parties rationnelles du groupe libre

C'est la plus petite classe $\mathcal{R}$ de parties du groupe libre telle que :

(1) chaque sous-ensemble fini du groupe libre appartient à $\mathcal{R}$,

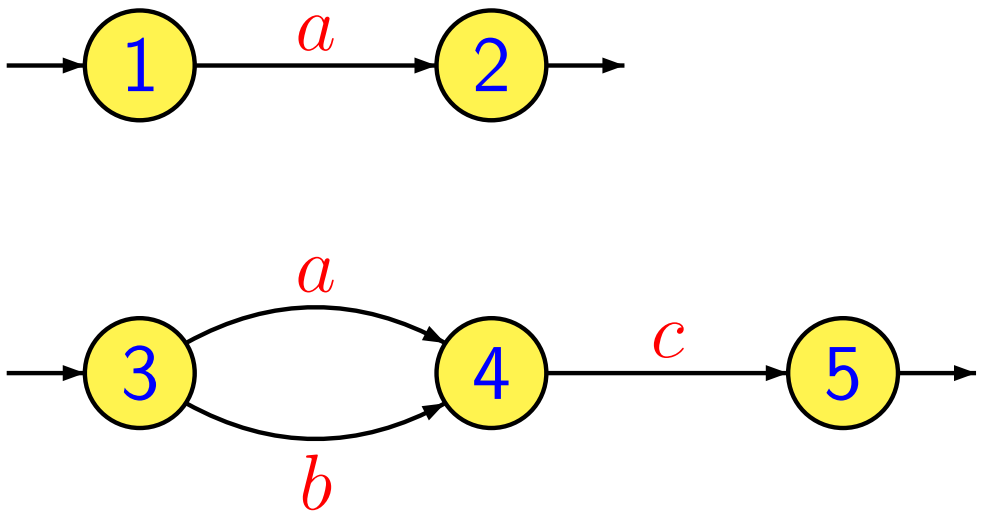
(2) si S et T sont dans $\mathcal{R}$, alors ST et $S \cup T$ y sont aussi,

(3) si S est dans $\mathcal{R}$, alors S^*, le sous-monoïde engendré par S, y est aussi.

Remarque. Si S est rationnel, le sous-groupe $\langle S \rangle$ engendré par S est rationnel ($\langle S \rangle = (S \cup \bar{S})^*$, où $\bar{S}$ est l'ensemble des inverses des éléments de S).

Automates réversibles dans le groupe libre

On associe à chaque transition $p \xrightarrow{a} q$ une transition inverse $q \xrightarrow{\bar{a}} p$. Par exemple, l'automate



reconnait $\{a\} \cup a\langle \bar{b}a \rangle c$.

Sous-groupes rationnels du groupe libre

Un groupe est finiment engendré s'il admet un ensemble fini de générateurs.

Théorème

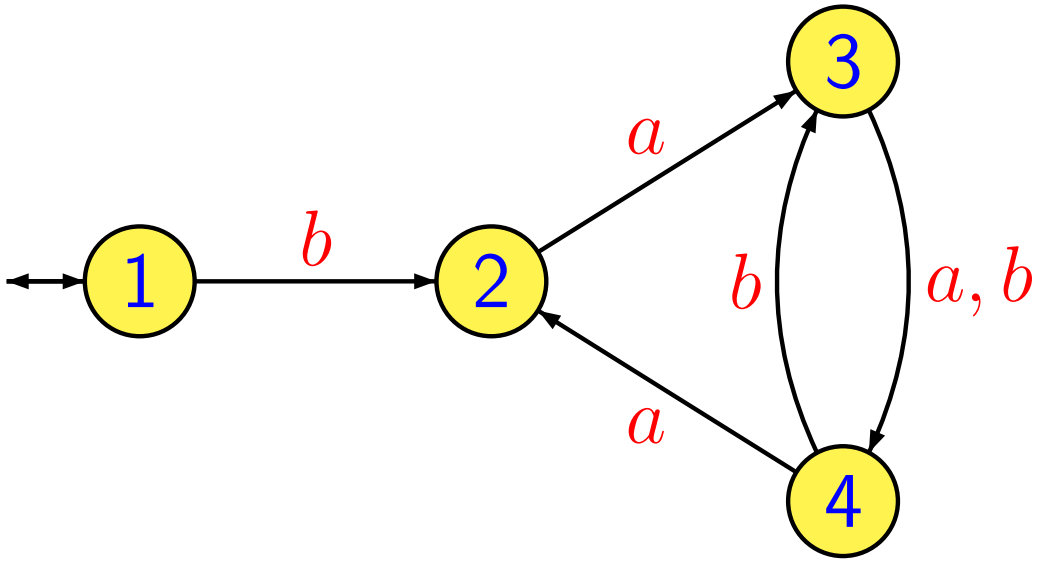
Soit H une partie du groupe libre. Sont équivalents

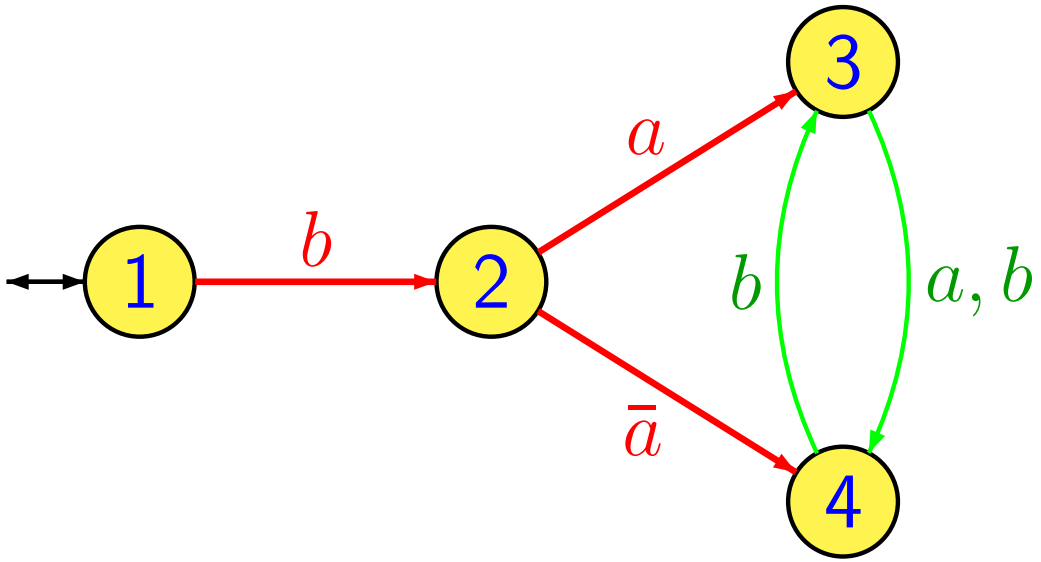
(1) *H est un sous-groupe rationnel,*

(2) *H est un sous-groupe finiment engendré,*

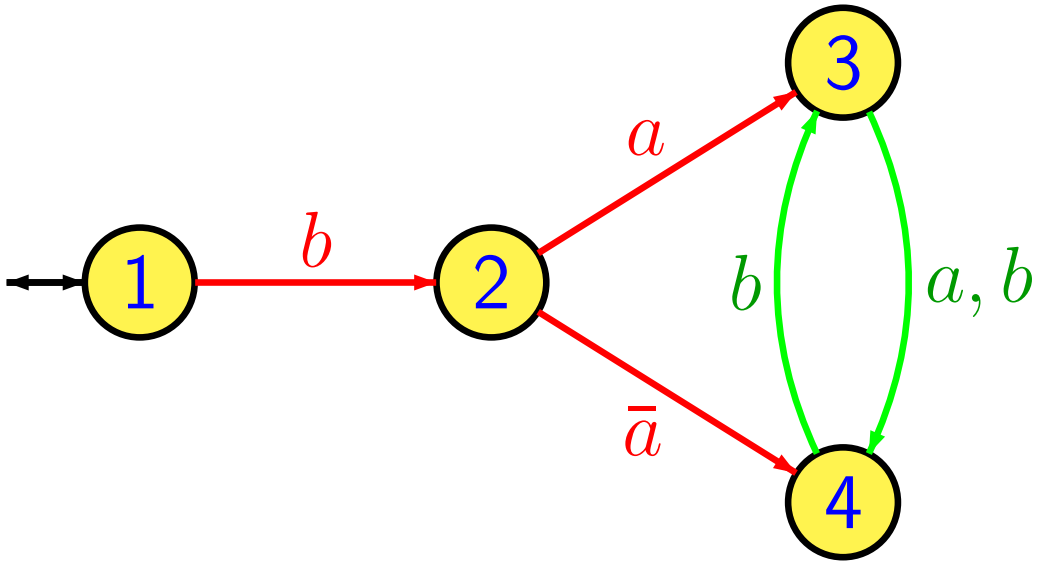
(3) *H est reconnu par un automate réversible dont l'unique état initial est aussi l'unique état final.*

(3) $\Rightarrow$ (2). Recherche d'arbre couvrant





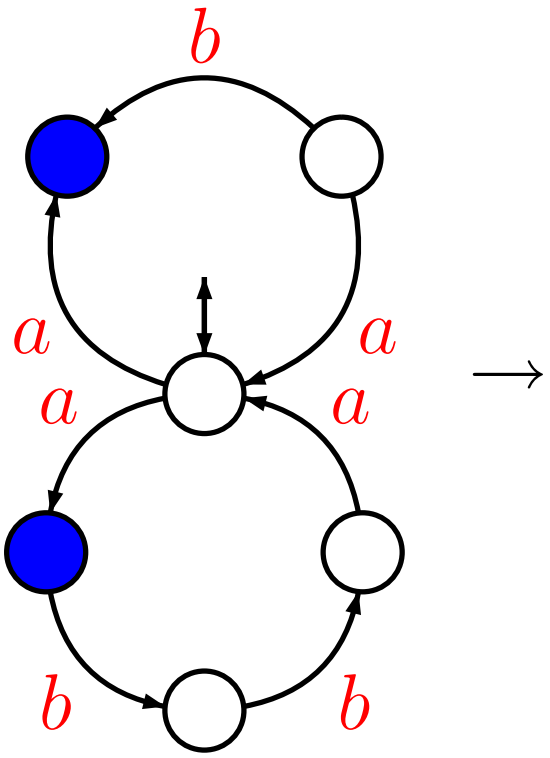
Trouver des générateurs : $\{ba^3\bar{b}, baba\bar{b}, b\bar{a}b\bar{a}\bar{b}\}$



Pour chaque $p \xrightarrow{c} q$ construire $1 \xrightarrow{u} p \xrightarrow{c} q \xrightarrow{v} 1$

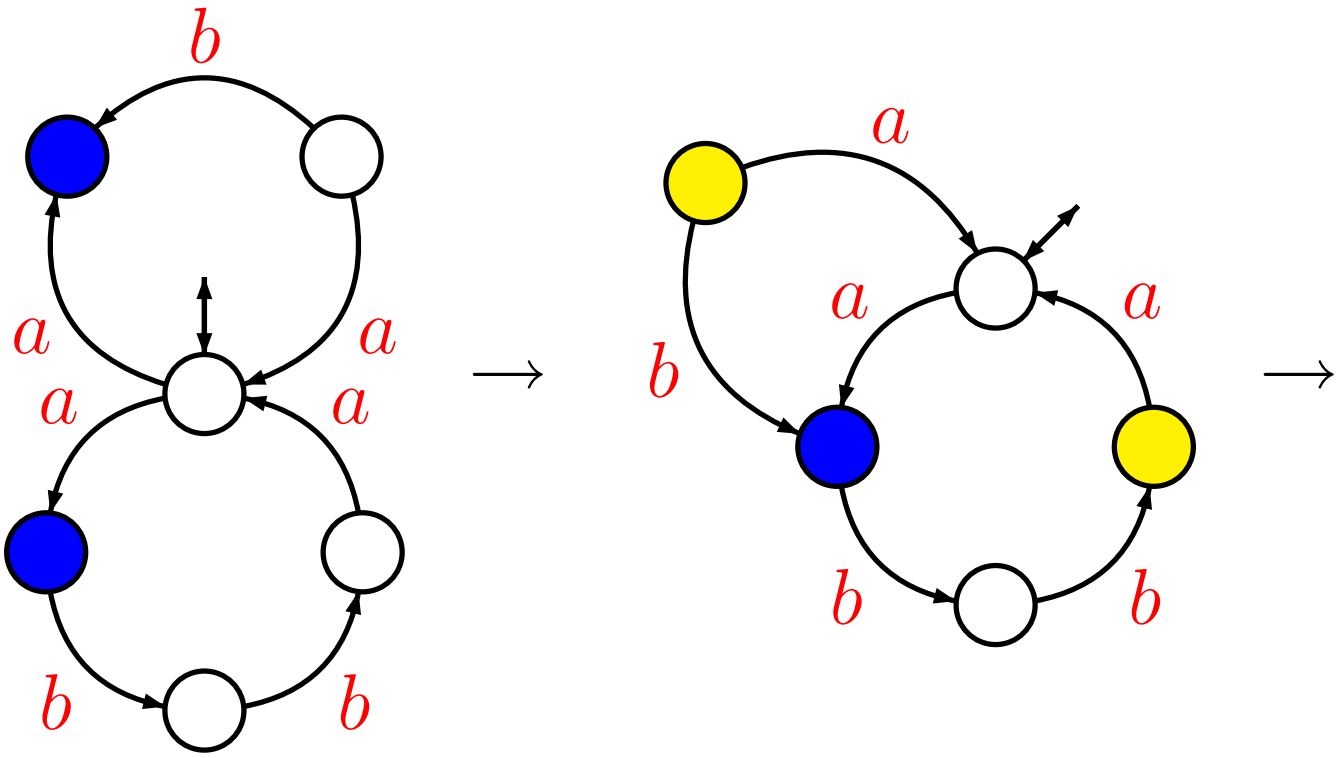
$3 \xrightarrow{a} 4$	$1 \xrightarrow{ba} 3 \xrightarrow{a} 4 \xrightarrow{a\bar{b}} 1$	$ba^3\bar{b}$
$3 \xrightarrow{b} 4$	$1 \xrightarrow{ba} 3 \xrightarrow{b} 4 \xrightarrow{a\bar{b}} 1$	$baba\bar{b}$
$4 \xrightarrow{b} 3$	$1 \xrightarrow{b\bar{a}} 4 \xrightarrow{b} 3 \xrightarrow{\bar{a}\bar{b}} 1$	$b\bar{a}b\bar{a}\bar{b}$

(2) $\Rightarrow$ (3). Bouquets de cercles et réductions



$\longrightarrow$

(2) ⇒ (3). Bouquets de cercles et réductions



(2) ⇒ (3). Bouquets de cercles et réductions

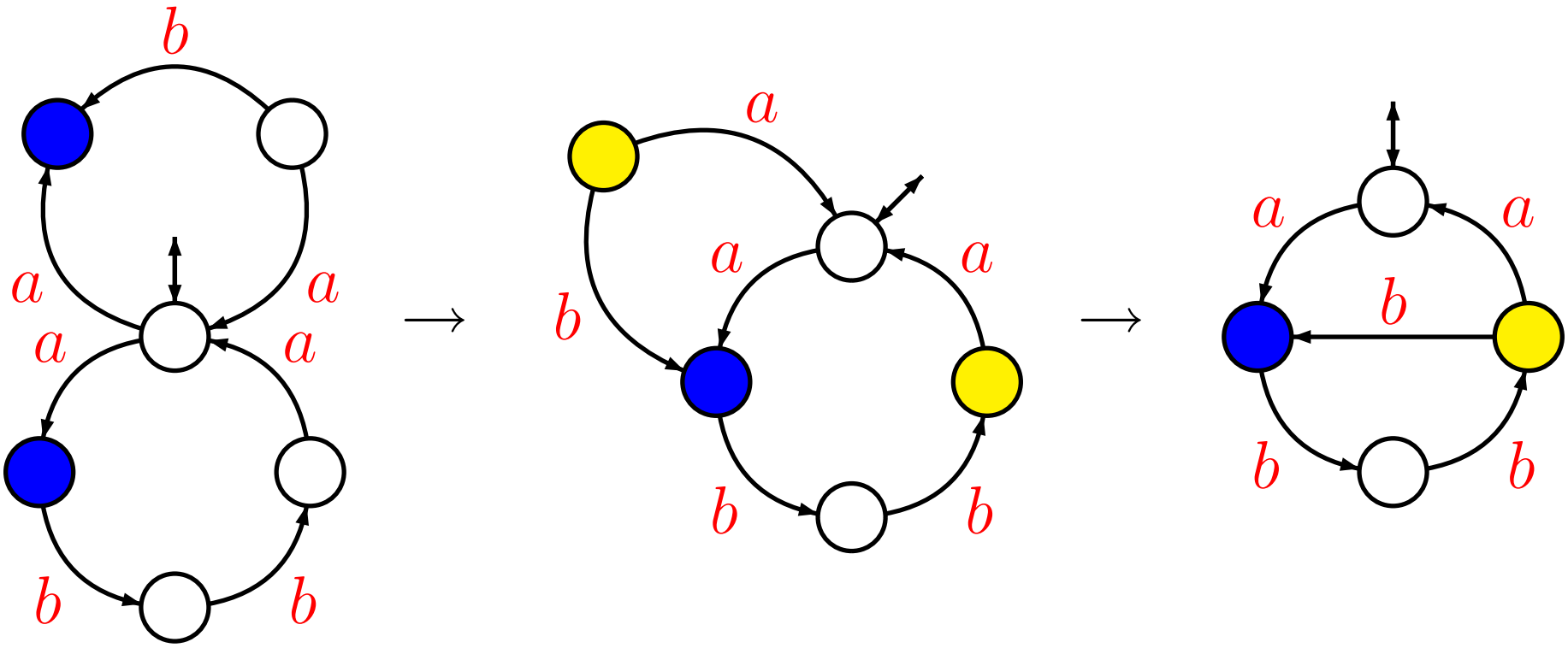


FIG.: Automate réversible acceptant $\langle a\bar{b}a, abba\rangle$.

Parties réversibles du groupe libre

Définition

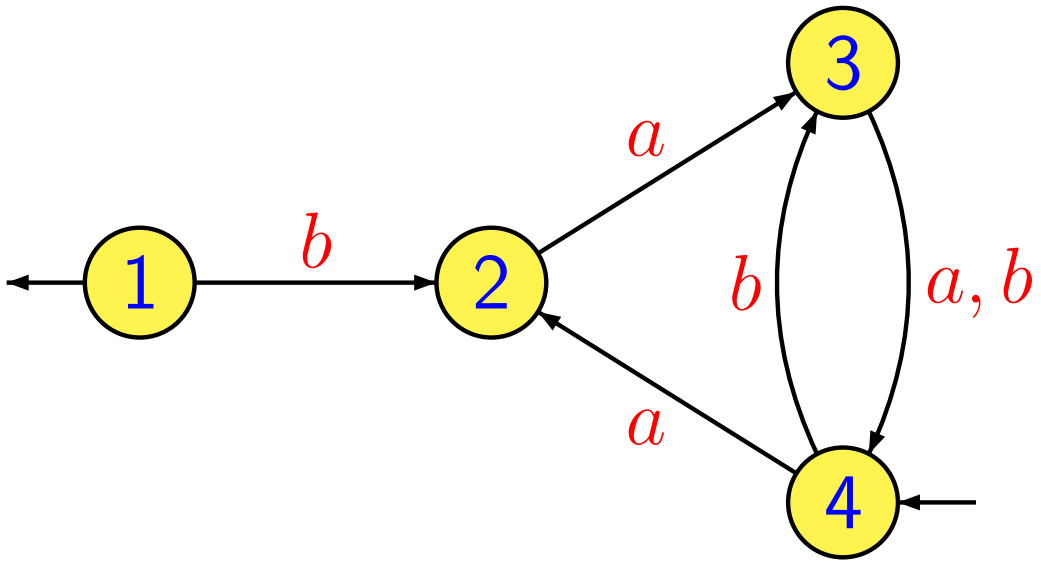
Une partie du groupe libre est réversible si elle est acceptée par un automate réversible.

Théorème

Une partie du groupe libre est réversible ssi elle est union finie de classes latérales gauches de sous-groupes finiment engendrés du groupe libre.

Preuve

On se ramène au cas où l'automate a un seul état initial i et un seul état final f.
Soit H le sous-groupe finiment engendré reconnu en prenant f comme état initial et final. Si u est un mot tel que $i \cdot u = f$, la partie reconnue est uH.
Sur l'exemple, on obtient $a\bar{b}\langle ba^3\bar{b}, baba\bar{b}, b\bar{a}ba\bar{a}\bar{b}\rangle$.



Les réversibles du groupe libre

Théorème (Kleene pour les réversibles !)

Les parties réversibles du groupe libre forment la plus petite classe $\mathcal{F}$ de parties telles que

(1) $\emptyset \in \mathcal{F}$ *et, pour tout* $g \in FG(A)$, $\{g\} \in \mathcal{F}$,

(2) *si* $S_1, S_2 \in \mathcal{F}$, *alors* $S_1 \cup S_2 \in \mathcal{F}$,

(3) *si* $S \in \mathcal{F}$ *et* $g \in FG(A)$, *alors* $gS \in \mathcal{F}$,

(4) *si* $S \in \mathcal{F}$, *alors* $\langle S \rangle \in \mathcal{F}$.

Retour au monoïde libre

Le monoïde libre A^* peut être considéré comme un sous-monoïde du groupe libre $FG(A)$.

Théorème

Un langage L de A^* est réversible ssi $L = K \cap A^*$, où K est une union finie de classes latérales de sous-groupes finiment engendrés du groupe libre $FG(A)$.

Cinquième partie V

Topologie pro-groupe

Séparation de deux mots dans un groupe fini

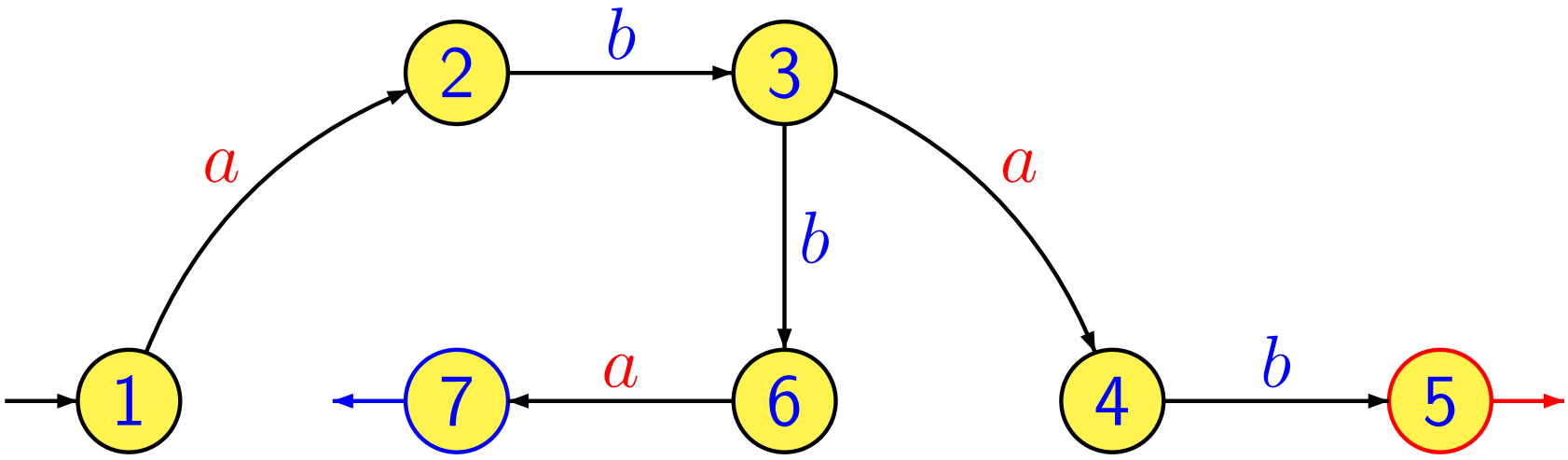
Théorème

Deux mots distinct u et v de A^* peuvent toujours être séparés : il existe un groupe fini G et un morphisme de monoïde $\varphi : A^* \to G$ tel que $\varphi(u) \neq \varphi(v)$.

Exemple. Le groupe $\mathbb{Z}/2\mathbb{Z}$ sépare les mots de longueur paire des mots de longueur impaire : prendre $\varphi(u) = |u| \bmod 2$.

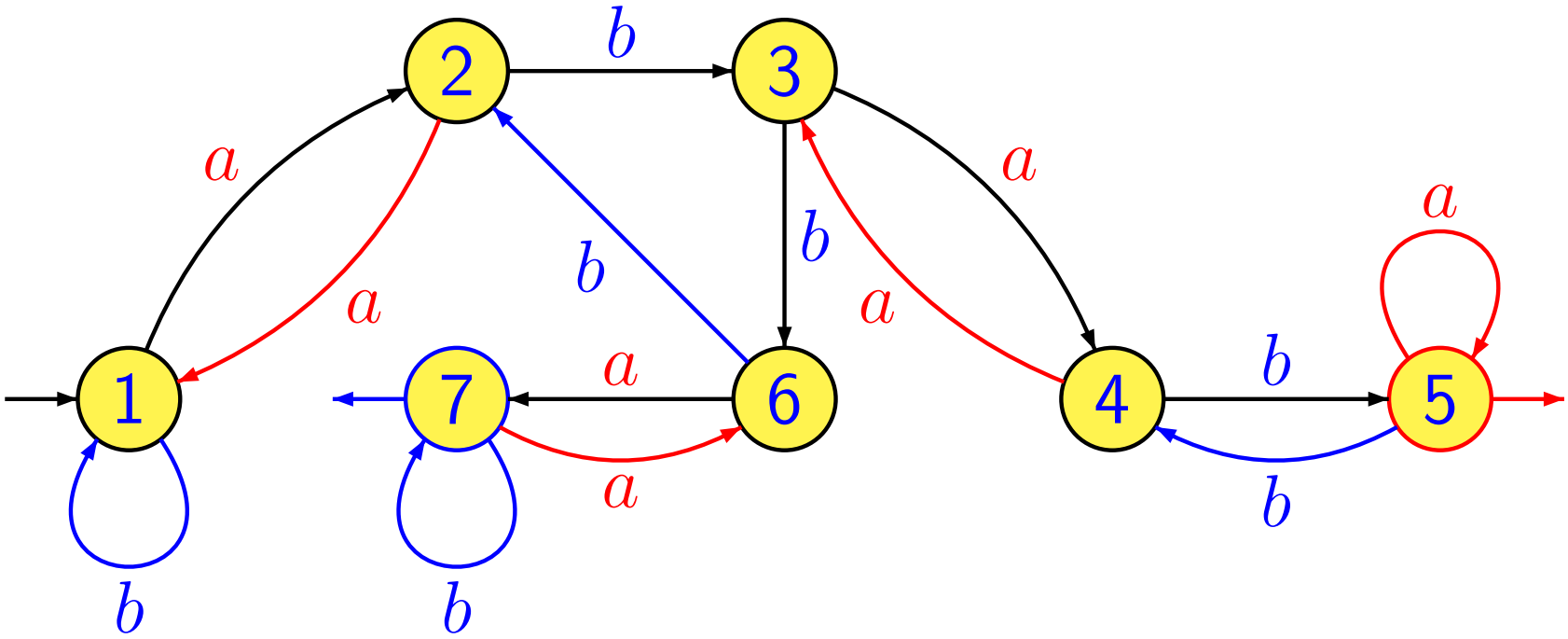
Exemple : séparer $abab$ et $abba$

(1) Construire un automate avec les deux mots



Exemple : séparer $abab$ et $abba$

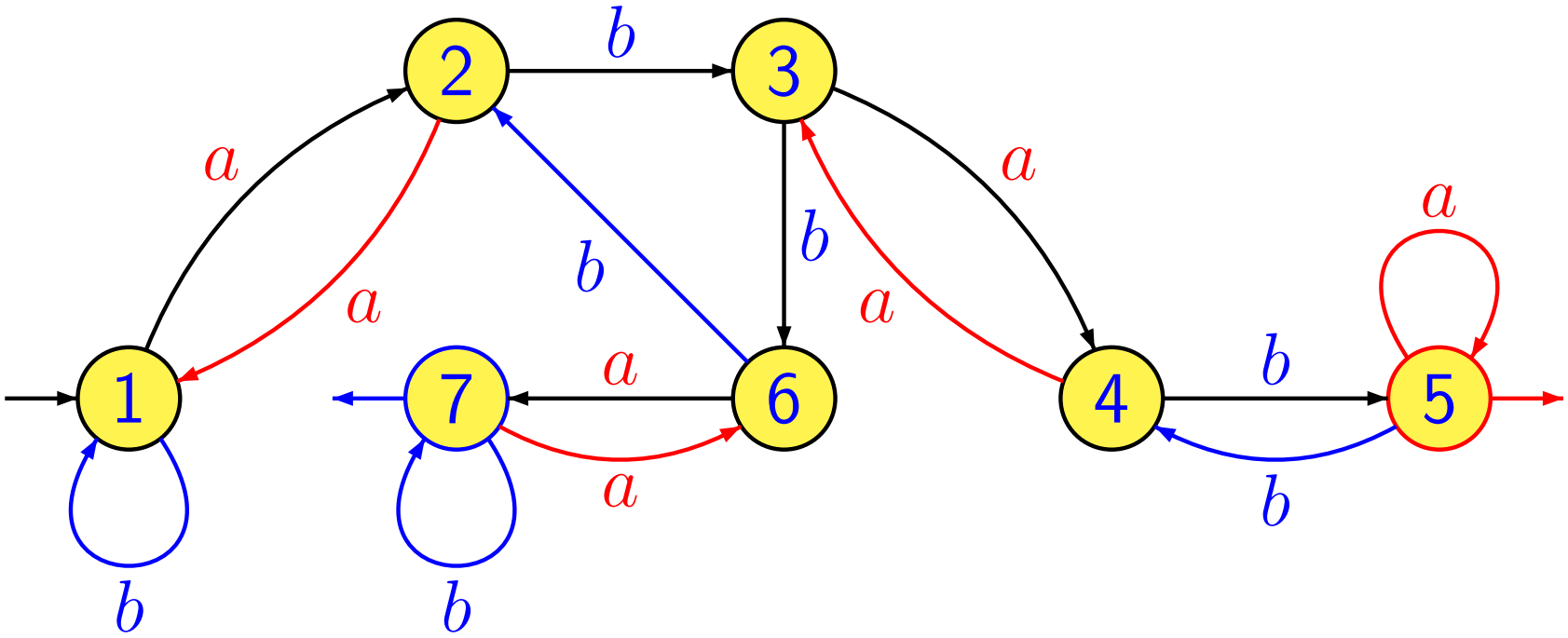
(1) Construire un automate avec les deux mots



(2) Compléter en permutations.

Exemple : séparer $abab$ et $abba$

(1) Construire un automate avec les deux mots



(2) Compléter en permutations. Le groupe de permutation obtenu sépare $abab$ et $abba$ puisque $1 \cdot abab = 5$ et $1 \cdot baba = 7$.

Une distance sur les mots

Posons, pour tout $u, v \in A^*$,

$$r(u,v) = \min \{|G| \mid G \text{ est un groupe fini qui sépare } u \text{ et } v\}$$

et $d(u,v) = 2^{-r(u,v)}$ (avec $\min \emptyset = \infty$ et $2^{-\infty} = 0$).

Alors d est une distance ultramétrique :

$$d(u,w) \leqslant \max(d(u,v), d(v,w))$$

Intuition : deux mots sont proches s'il faut un grand groupe pour les séparer.

Propriétés de la distance

(1) Le produit $(u, v) \to uv$ est uniformément continu.

(2) Les morphismes de monoïde de A^* dans B^* sont uniformément continus.

(3) Les morphismes de monoïde de A^* dans un groupe fini discret sont uniformément continus.

Autres propriétés topologiques

La topologie de d est la topologie initiale définie par les morphismes sur un groupe fini.

Conséquences :

• Une suite u_n converge vers u ssi, pour tout morphisme $\varphi : A^* \to G$ (groupe fini), $\varphi(u_n)$ est ultimement égal à $\varphi(u)$.

• Une partie de A^* reconnue par un groupe fini est ouverte et fermée (clopen).

Une suite convergente...

Théorème (Hall, Reutenauer)

Pour tout mot $u \in A^*$, $\lim_{n \to \infty} u^{n!} = 1$.

Une suite convergente...

Théorème (Hall, Reutenauer)

Pour tout mot $u \in A^*$, $\lim_{n\to\infty} u^{n!} = 1$.

Preuve. Soit G un groupe fini et $\varphi : A^* \to G$ un morphisme de monoïde. Posons $g = \varphi(u)$. Si k est l'ordre de G, on a donc $g^k = 1$.

Par conséquent, pour $n \geqslant k$, $\varphi(u^{n!}) = g^{n!} = 1$ et la suite $g^{n!}$ est donc ultimement égale à $\varphi(1)$. □

Une seconde condition nécessaire

Proposition (Reutenauer 1979)

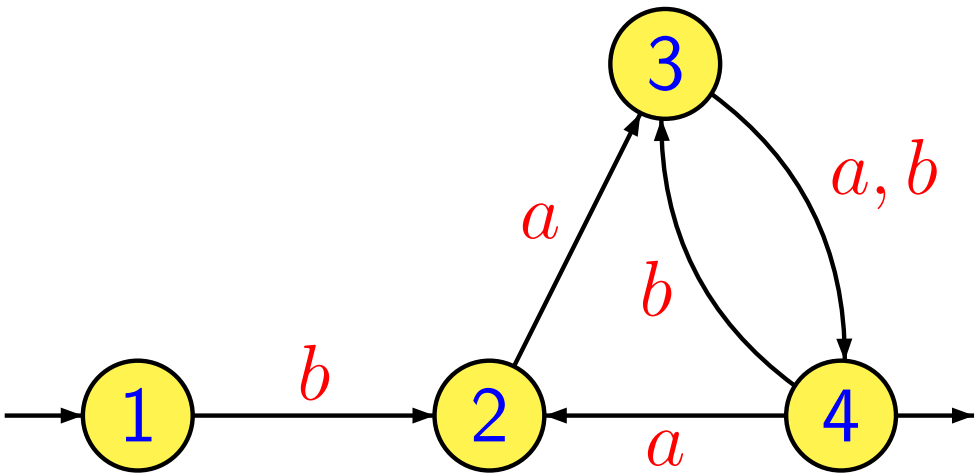
Les langages réversibles sont fermés.

Preuve à suivre...

Note. La réciproque n'est pas vraie : a^*b^* est fermé, mais n'est pas réversible.

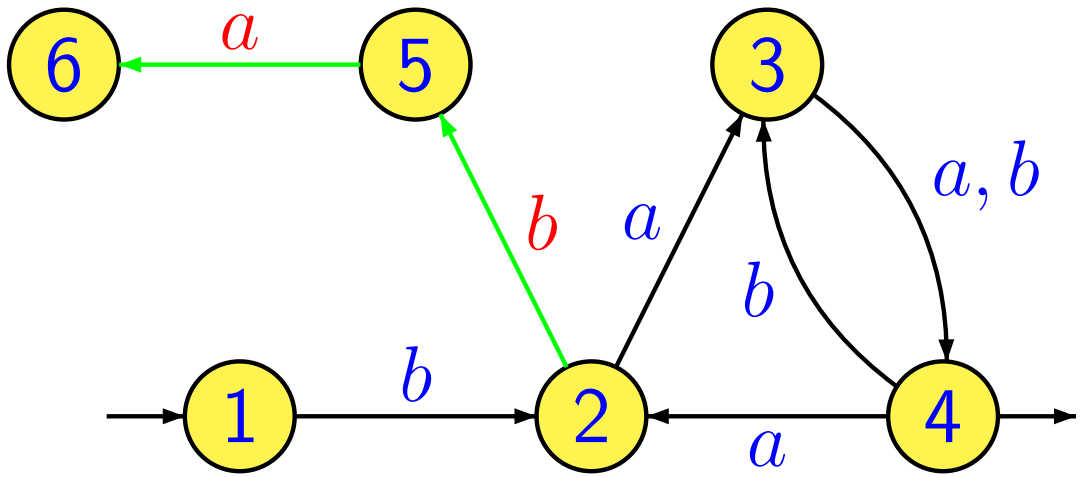
Preuve sur un exemple...

Soit L le langage reconnu par l'automate réversible. On prouve que L^c est ouvert en montrant que pour chaque mot $u \notin L$, il existe un ouvert contenant u et disjoint de L.

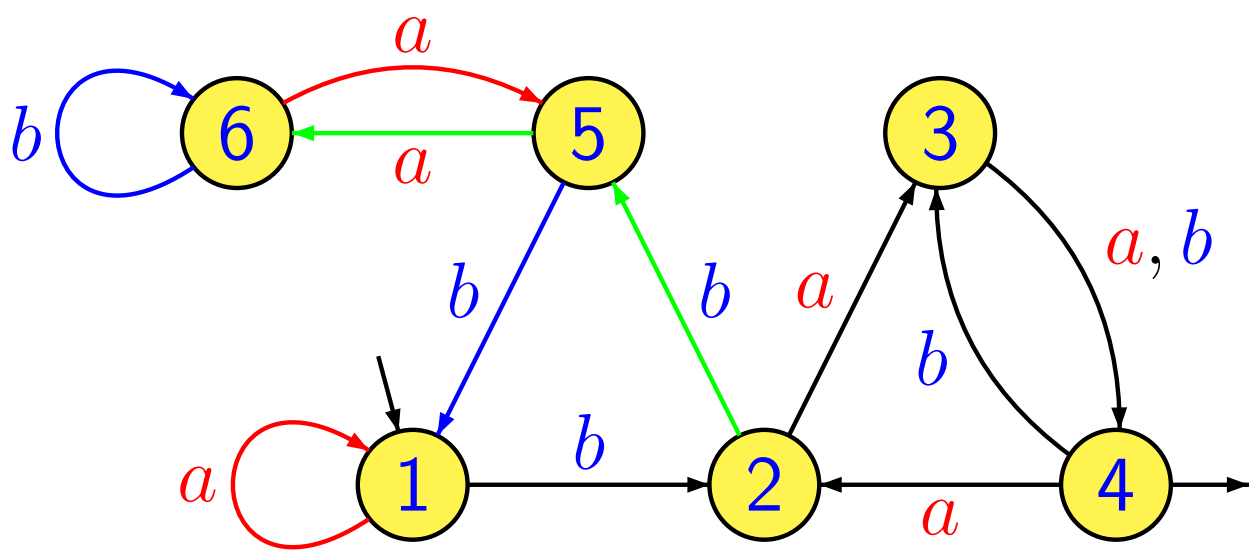


Etape 1 : ajout de transitions pour lire u.

On étend l'automate réversible pour pouvoir lire le mot u. Ici $u = bababa$.



Etape 2 : complétion en automate de permutations



Soit G le groupe engendré par les permutations a et b et soit $\varphi : A^* \to G$ le morphisme naturel. Soit $g = \varphi(u)$. Comme G est discret, $\{g\}$ est ouvert. Comme φ est continue, $U = \varphi^{-1}(g)$ est aussi ouvert. Or U contient u et est disjoint de L, car $1 \cdot x$ vaut 4 si $x \in L$ et 6 si $x \in U$. □

Sixième partie VI

Un lemme d'itération

Un lemme d'itération

Corollaire

Soit L un langage réversible et soient $x, u, y \in A^*$. Si, pour tout $n > 0$, $xu^n y \in L$, alors $xy \in L$.

Preuve. Puisque le produit est continu, $\lim_{n\to\infty} xu^{n!}y = xy$. Comme L est fermé, $xy \in L$. □

Version algébrique du lemme d'itération

Proposition

Soit L un langage reconnaissable et M son monoïde syntactique ordonné. Sont équivalents :

(1) *L vérifie le lemme d'itération,*

(2) *pour tout idempotent $e \in M$, $1 \leqslant e$.*

Septième partie VII

Caractérisation algébrique

Théorème principal

Théorème

Soit L un langage reconnaissable et M son monoïde syntactique ordonné. Alors L est réversible ssi

(1) *les idempotents de M commutent,*

(2) *pour tout idempotent $e \in M$, $1 \leqslant e$.*

On a déjà vu que ces conditions sont nécessaires. Pour la réciproque, on étudie de près le graphe de Cayley de (M, A).

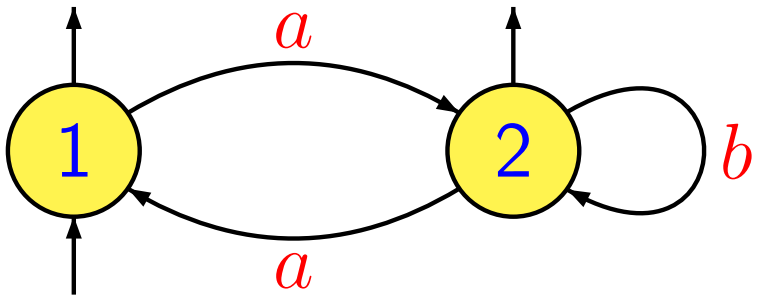
Composantes régulières du graphe de Cayley

Une composante fortement connexe du graphe de Cayley est régulière si l'un de ses sommets est un idempotent.

Proposition

Si les idempotents de M commutent, l'automate défini par une composante régulière est réversible.

Exemple : $L = (ab^*a)^*(1 + a)$



1	1	2
a	2	1
b	0	2
ab	2	0
ba	0	1
aba	1	0
bab	0	0

Relations :

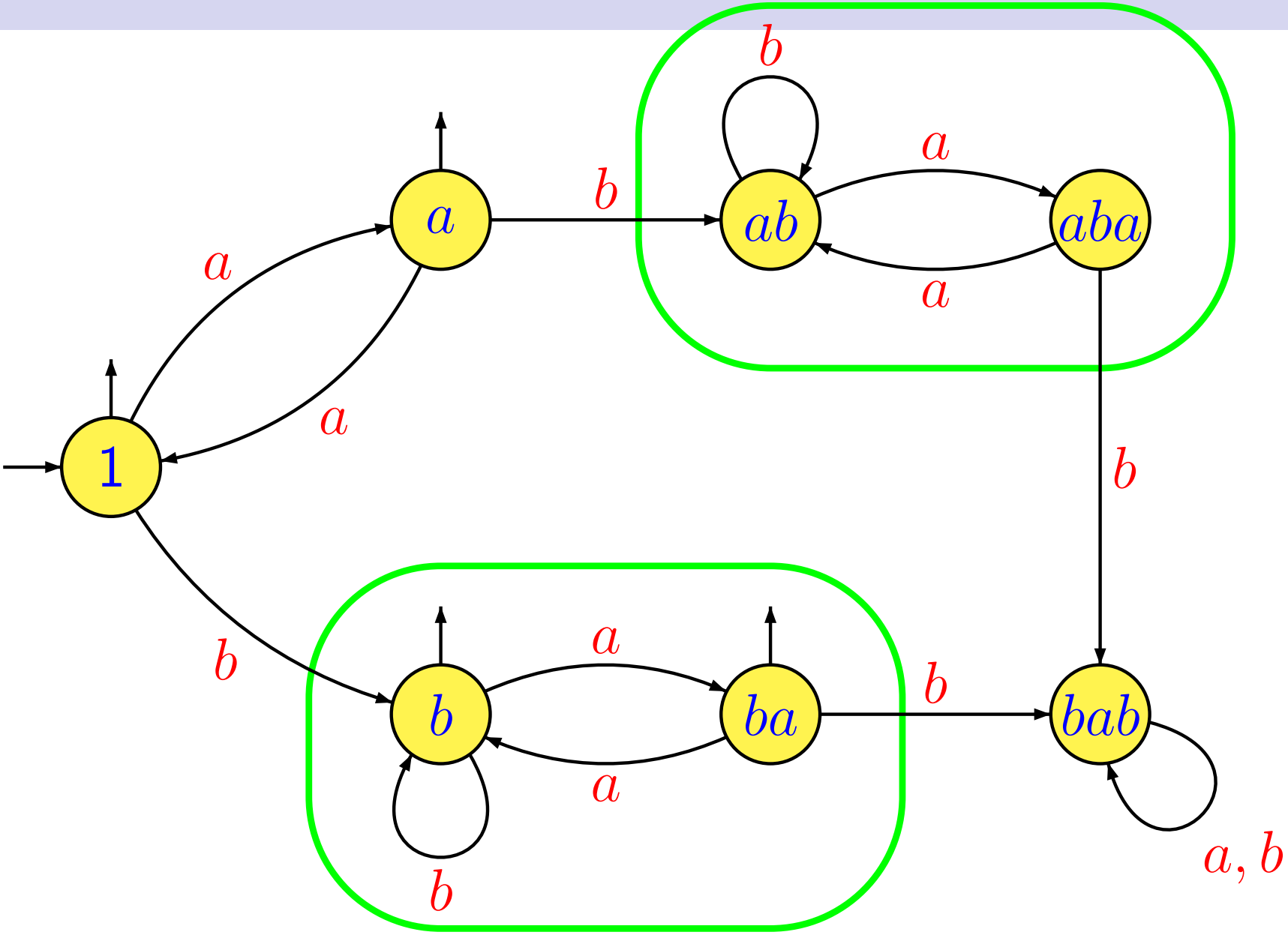
$a^2 = 1$

$b^2 = b$

$bab = 0$

Les idempotents commutent.

Exemple



Un résultat combinatoire

Proposition

Soit φ un morphisme de A^* dans un monoïde M dont les idempotents commutent. Alors il existe un entier $N > 0$ tel que tout mot w de A^* se factorise en $w = u_0 v_1 u_1 \cdots v_k u_k$, avec $u_1, \ldots, u_{k-1}$ non vides et

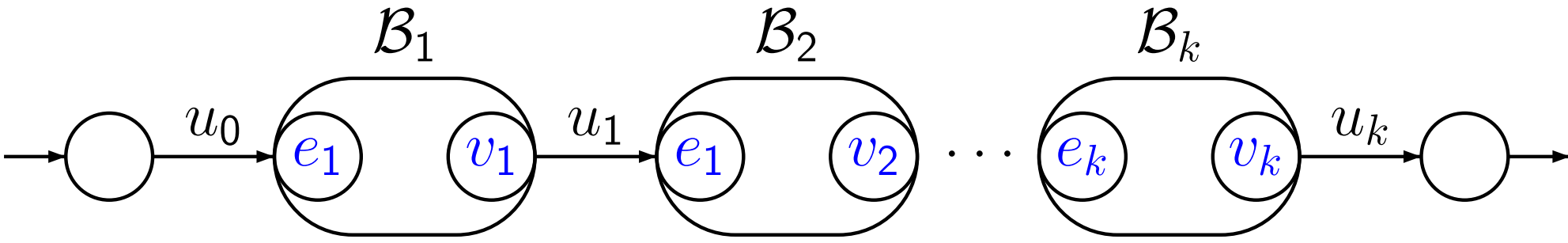
(1) *les $\varphi(v_i)$ sont des éléments réguliers de M,*

(2) *ces facteurs réguliers v_i sont maximaux,*

(3) *la longueur totale des autres facteurs est $\leqslant N$.*

Schéma de la preuve

Sous les hypothèses sur M, on montre que pour chaque factorisation $w = u_0 v_1 u_1 \cdots v_k u_k$, l'automate suivant est réversible.



De plus, si $w \in L$, le langage reconnu par cet automate est inclus dans L.
Or il n'y a qu'un nombre fini d'automates de ce type et L est donc union finie de langages réversibles.

Huitième partie VIII

Synthèse des résultats

Synthèse des résultats (1)

Théorème

Soit L un langage de A^*. Sont équivalents :

(1) *L est réversible,*

(2) *L^c est une combinaison booléenne positive de langages de la forme R ou A^*aR où R est un langage à groupe,*

(3) *L^c est une combinaison booléenne positive de langages de la forme R, R_1aR_2 où R_1 et R_2 sont des langages à groupe.*

Synthèse des résultats (2)

Théorème

Soit L un langage rationnel et M son monoïde syntactique ordonné. Sont équivalentes :

(1) *L est réversible,*

(2) *$L = K \cap A^*$, où K est une union finie de classes latérales de sous-groupes finiment engendrés du groupe libre $FG(A)$,*

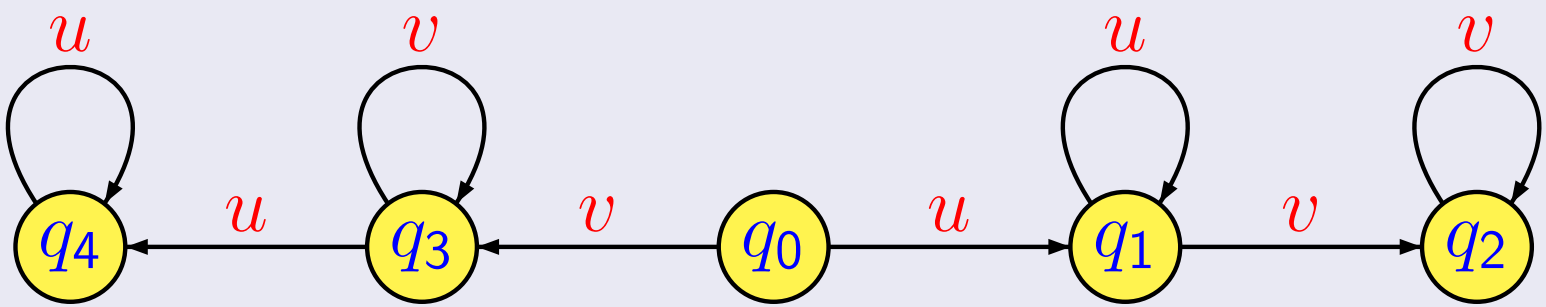
(3) *les idempotents de M commutent et, pour chaque idempotent e de M, $1 \leqslant e$,*

(4) *les idempotents de M commutent et L est fermé.*

Algorithme 1

Théorème

Soit $\mathcal{A}$ l'automate minimal du langage L. Les idempotents de $M(L)$ commutent ssi $\mathcal{A}$ ne contient aucune configuration de la forme

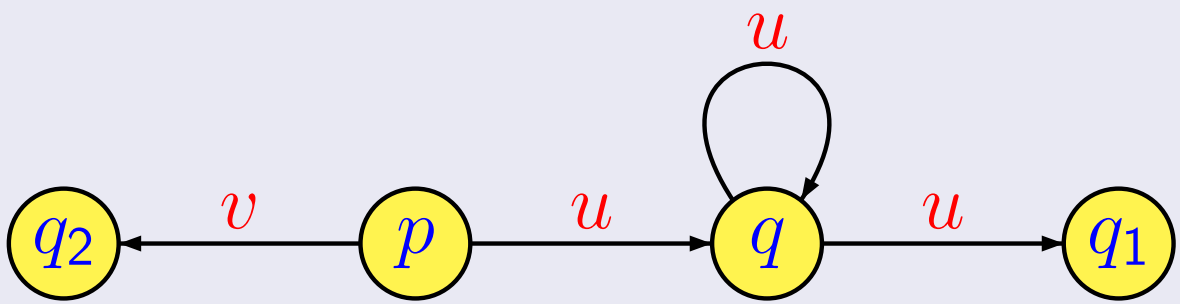


avec $u, v \in A^*$ et $q_2 \neq q_4$.

Algorithme 2

Théorème

Soit $\mathcal{A}$ l'automate minimal d'un langage L. On a $1 \leqslant e$ pour tout idempotent $e \in M(L)$ ssi $\mathcal{A}$ ne contient aucune configuration de la forme



avec $u, v \in A^*$ et $q_1 \in F$ et $q_2 \notin F$.

Algorithme 3

Théorème

Soit $\mathcal{A}$ l'automate minimal d'un langage L. Alors L est réversible ssi $\mathcal{A}$ ne contient aucune des deux configurations précédentes.

Corollaire

On peut tester en temps polynomial si un langage accepté par un automate déterministe à n états est réversible.

Neuvième partie IX

Pour aller plus loin...

Retour sur la topologie du groupe libre

Théorème (M. Hall Jr.,)

Tout sous-groupe finiment engendré du groupe libre est fermé.

Théorème (Ribes–Zalesskii, 1993)

Tout produit de sous-groupes finiment engendrés du groupe libre est fermé.

Plusieurs démonstrations, dont une via la théorie des modèles !

Cloture d'un langage rationnel

Théorème

La fermeture (topologique) d'un langage rationnel est un langage rationnel. On dispose d'un algorithme pour la calculer.

- De nombreuses conséquences en théorie des semigroupes finis.

Problèmes ouverts

On peut définir des topologies pro-p-groupe, pro-groupe pro- groupe nilpotent, etc.

On a vu que la fermeture d'un langage rationnel est toujours rationnelle. On dispose d'un algorithme pour la topologie pro-groupe, p-groupe, groupe nilpotent, mais pas groupe résoluble !

Le problème se ramène à décider si un automate réversible peut être complété, quitte à rajouter des états et des flèches, en un automate à groupe résoluble.

Pourquoi s'arrêter aux groupes ?

On peut construire des topologies profinies pour d'autres variétés de monoïdes finis. Le monoïde libre A^* est alors muni d'une structure d'espace métrique, dont la complétion est un monoïde compact.

Ces objets sont encore très mal connus et sont la clé de la solution de nombreux problèmes de théorie des automates et l'objet de recherches très actives.

References I

- C.J. Ash, Finite semigroups with commuting idempotents, *J. Austral. Math. Soc. (Series A)* **43**, (1987) 81–90.
- C. J. Ash, Inevitable Graphs : A proof of the type II conjecture and some related decision procedures, *Int. Jour. Alg. and Comp.* **1**, (1991), 127–146.
- M. Hall Jr., A topology for free groups and related groups, *Ann. of Maths* **52**, (1950) 127–139.

References II

- J.E. Pin, *On the languages recognized by finite reversible automata*, 14th ICALP, LNCS 267, (1987) 237–249.
- J.E. Pin, Topologies for the free monoid, *Journal of Algebra* **137** (1991) 297–337.
- J.-E. Pin, On reversible automata, in *Proceedings of the first LATIN conference*, Saõ-Paulo, LNCS 583, (1992), 401–416.
- J.-E. Pin, Topologie p-adique sur les mots, *Journal de théorie des nombres de Bordeaux* **5** (1993), 263–281.

References III

- J.-E. Pin and C. Reutenauer, A conjecture on the Hall topology for the free group, *Notices of the London Math. Society* **23**, (1991), 356–362.
- Ch. Reutenauer, Une topologie du monoïde libre, *Semigroup Forum* **18**, (1979) 33–49. Correction *Semigroup Forum* **22**, (1981) 93–95.
- L. Ribes and P.A. Zalesskii, On the profinite topology on a free group, *Bull. London Math. Soc.* **25**, (1993), 37–43.
- J. Stallings, Topology of finite graphs, *Invent. Math.* **71**, (1983), 551–565.

References IV