Automates et circuits : Automates

Arnaud Labourel
Courriel : arnaud.labourel@lif.univ-mrs.fr

Aix-Marseille Université

Représenter un système par un automate

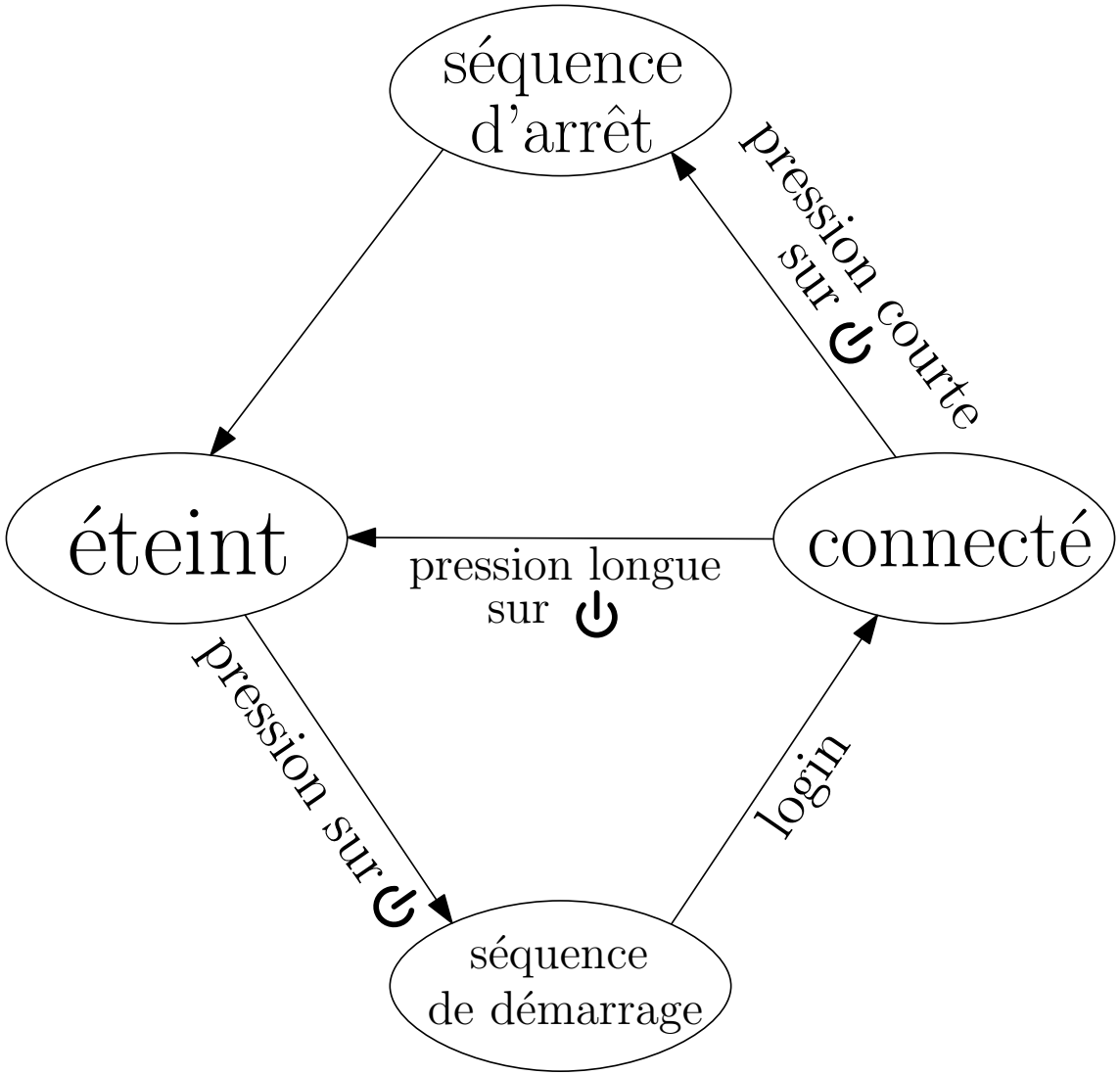
But de ce cours

Etre capable de représenter un système ou une machine avec un automate.

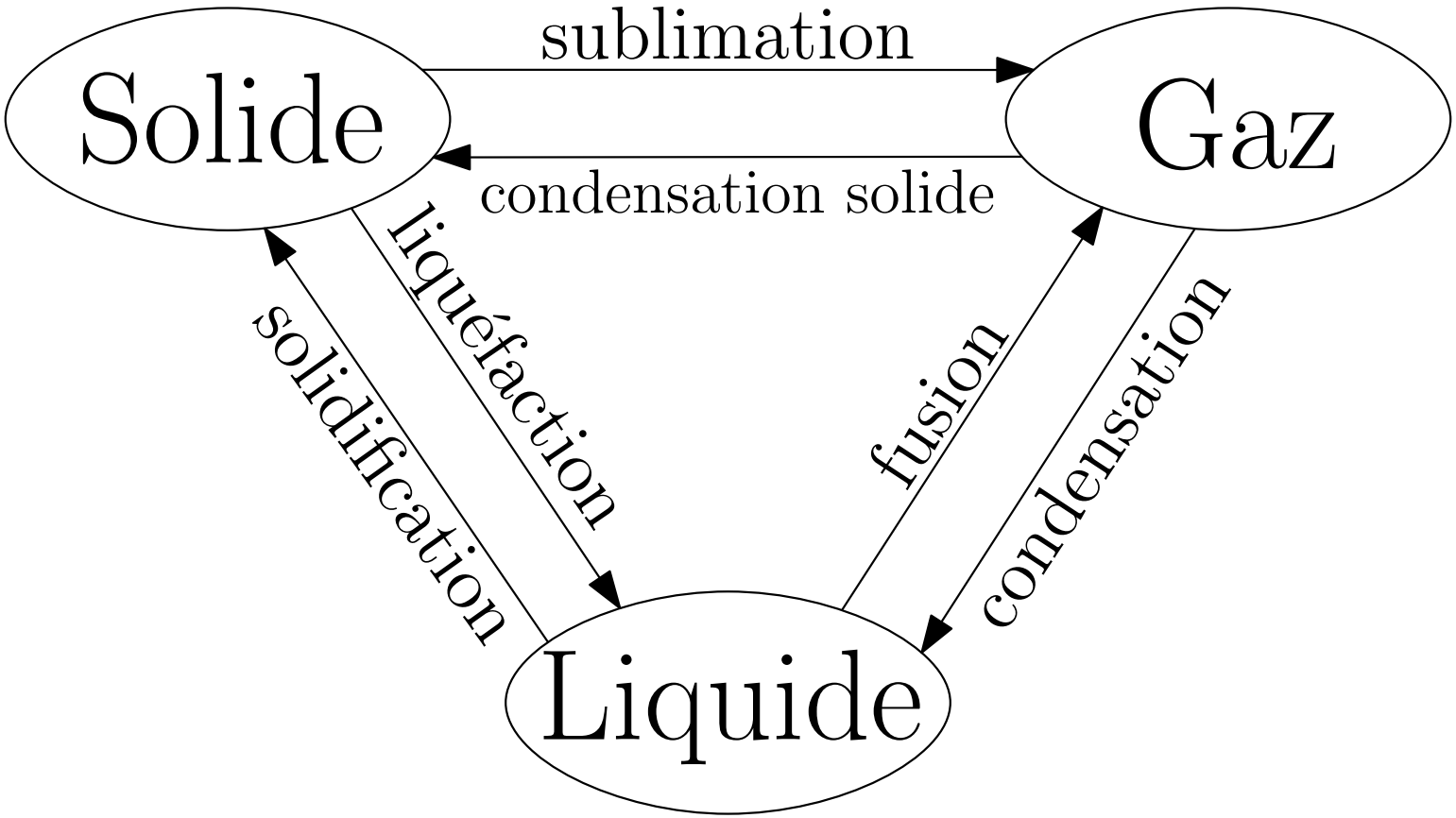
Concepts importants

- états = position du système
- transition = changement d'états du système

Exemple : états d'un ordinateur



Exemple : états de l'eau



Automates

Comment définir un automate ?

Avec

- un ensemble d'états
- un ensemble de transitions : condition de passage d'un état à l'autre

Exemples : états de l'eau

États : états physiques de l'eau
Transitions : conditions de températures et pression
Exemple :
Température>100°$\Rightarrow$ passage de l'état liquide à gazeux.

Définition formelle d'un automate

Définition

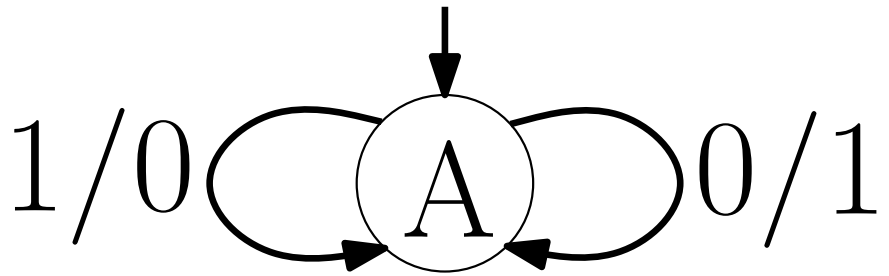
Un automate est définie par un quintuplet (Q, i, E, S, δ) où :

- Q est un ensemble fini d'états
- i est l'état initial ($i \in Q$)
- E est l'alphabet des valeurs d'entrées
- S est l'alphabet des valeurs de sorties
- δ est la fonction de transition $\delta : Q \times E \rightarrow Q \times S$

Automate et fonction

Un automate va coder une fonction f de l'ensemble des mots de E vers l'ensemble des mots de S.

Représentation d'un automate



Notation :

$A \xrightarrow{x/y} B$ signifie que si on lit x dans l'état A alors on écrit y et on passe à l'état B.

On a dans ce cas $\delta(A, x) = (B, y)$.

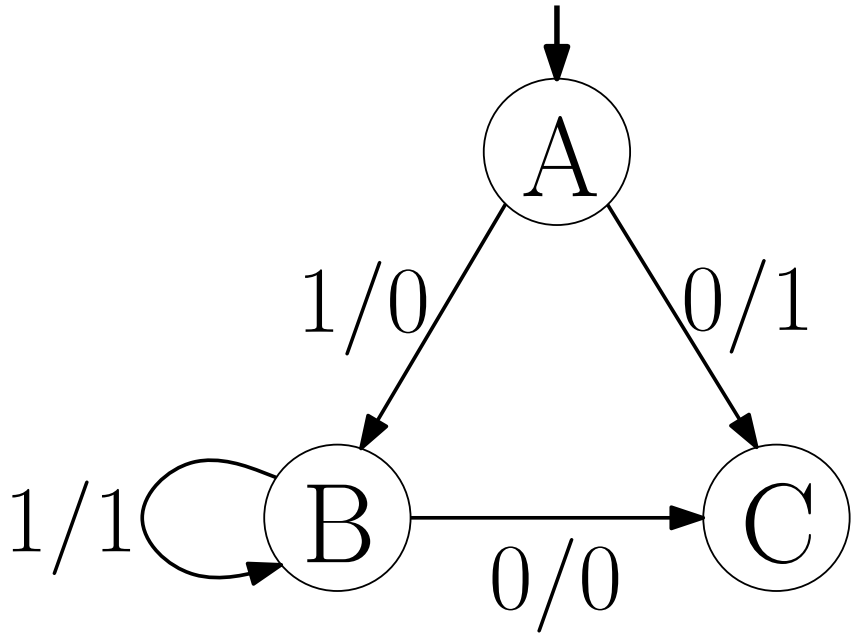
Dans l'exemple il y a deux transitions :

$A \xrightarrow{1/0} A$

$A \xrightarrow{0/1} A$

On met un flèche pour indiquer l'état initial (ici A)

Définition d'un automate



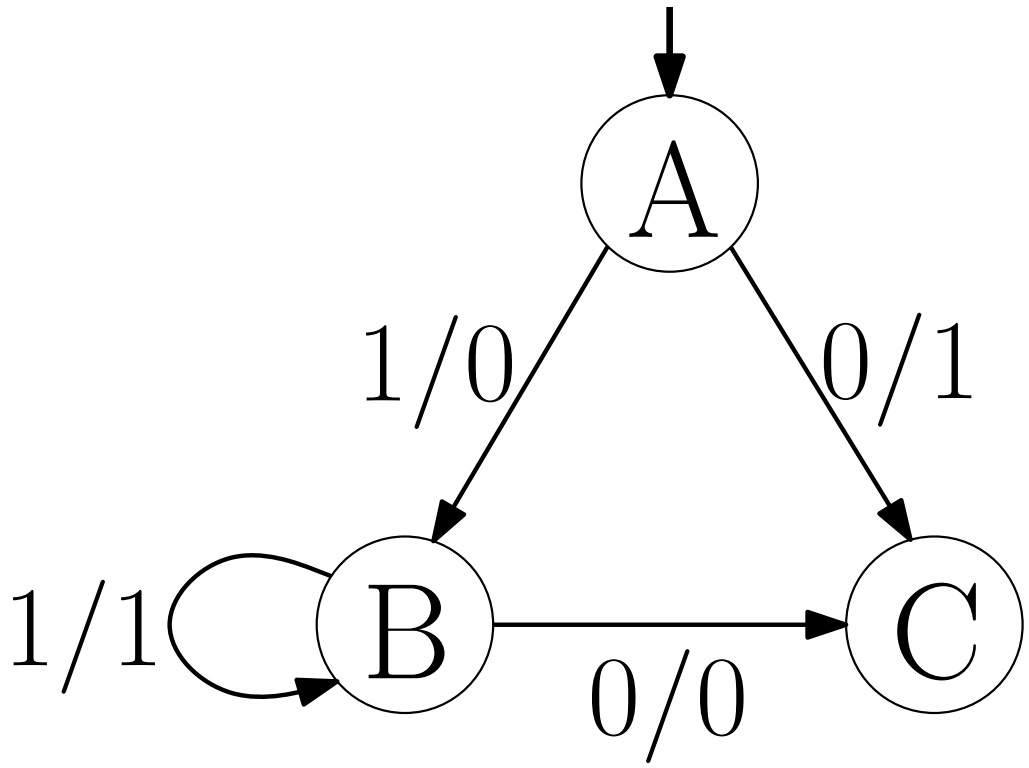
Ensemble d'états : $Q = \{A, B, C\}$
état initial : $i = A$
Alphabet d'entrée : $E = \{0, 1\}$
Alphabet de sortie : $S = \{0, 1\}$

Fonction de transition δ :

$$\delta(A, 0) = (C, 1)$$
$$\delta(A, 1) = (B, 0)$$
$$\delta(B, 0) = (C, 0)$$
$$\delta(B, 1) = (B, 1)$$

Table de transition

Un automate est défini par son état initial et sa table de transition (table de vérité de la fonction de transition)



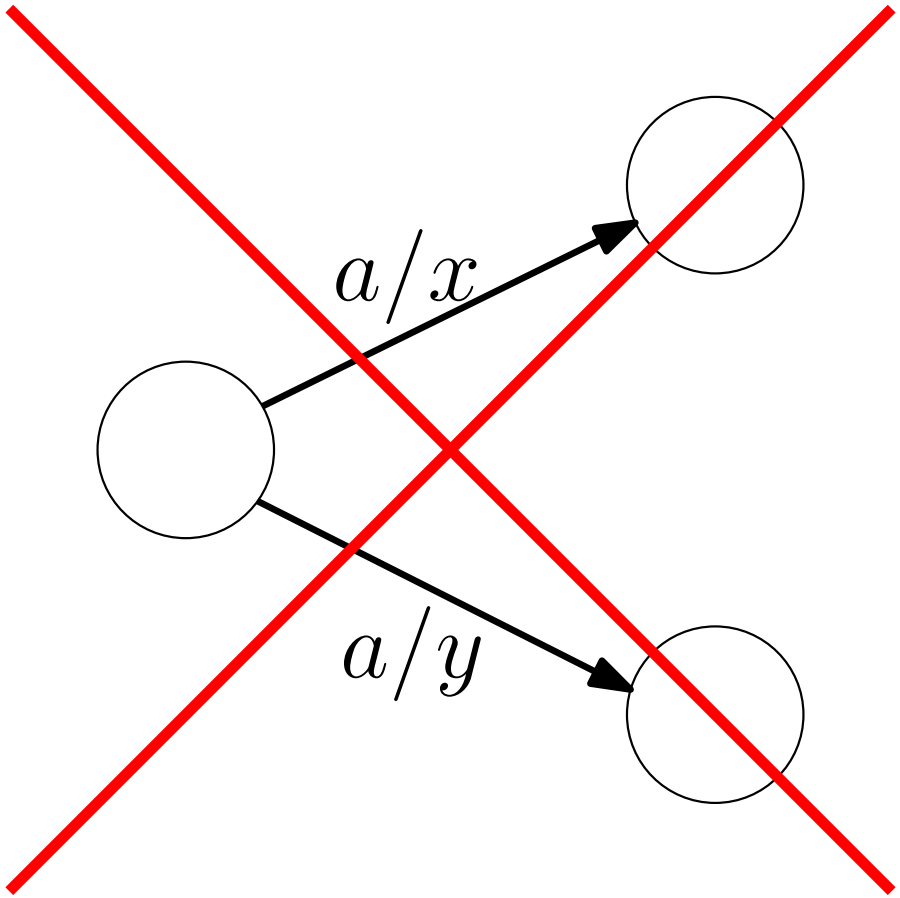
état initial : A

table de vérité de δ

$Q \times E$	$Q \times S$
$(A, 0)$	$(C, 1)$
$(A, 1)$	$(B, 0)$
$(B, 0)$	$(C, 0)$
$(B, 1)$	$(B, 1)$
$(C, 0)$	non défini
$(C, 1)$	non défini

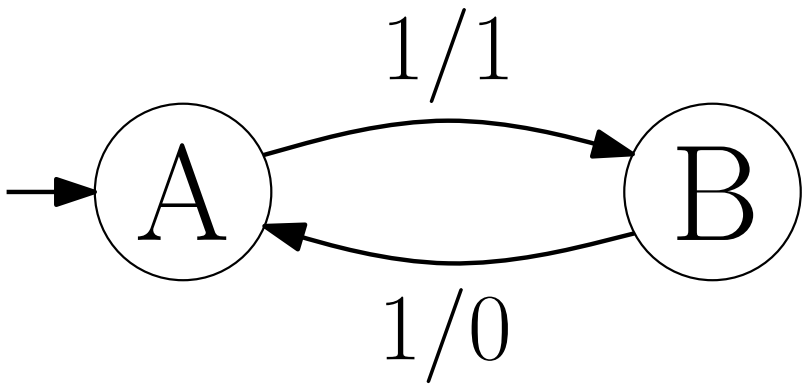
Propriétés d'un automate

On ne peut pas avoir deux transitions sortant d'un même état qui correspondent à la même lettre.



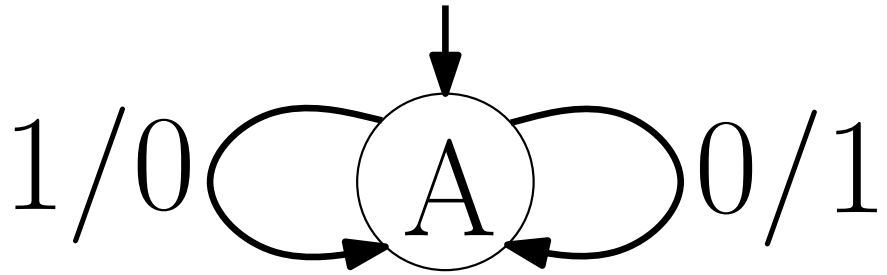
Propriétés d'un automate

Il n'y a pas forcément à chaque état une transition qui correspond à chaque lettre de l'alphabet d'entrée.



Exemple d'automate : inversion de bits

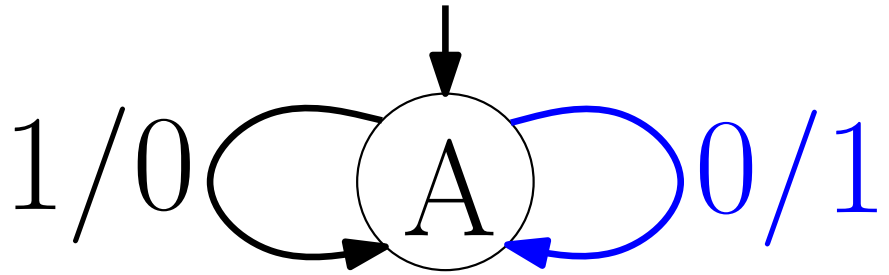
Lecture du mot 01011



Exemple d'automate : inversion de bits

Lecture du mot 01011

On lit 0

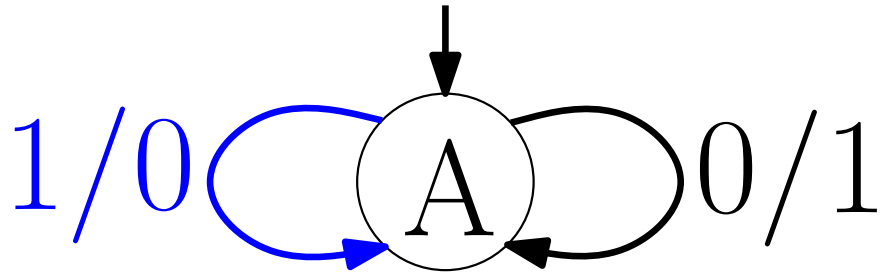


On écrit 1 et on va à l'état A
Sortie : 1

Exemple d'automate : inversion de bits

Lecture du mot 01011

On lit 1

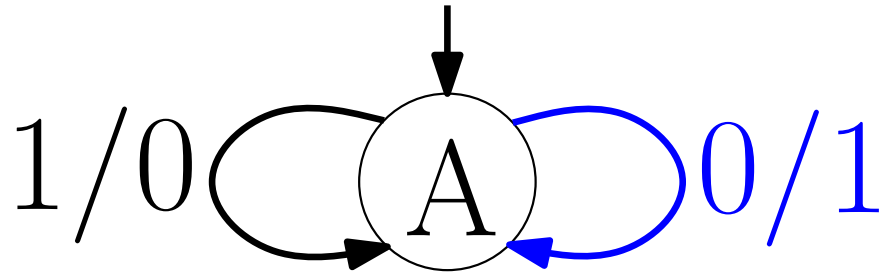


On écrit 0 et on va à l'état A
Sortie : 10

Exemple d'automate : inversion de bits

Lecture du mot 01011

On lit 0

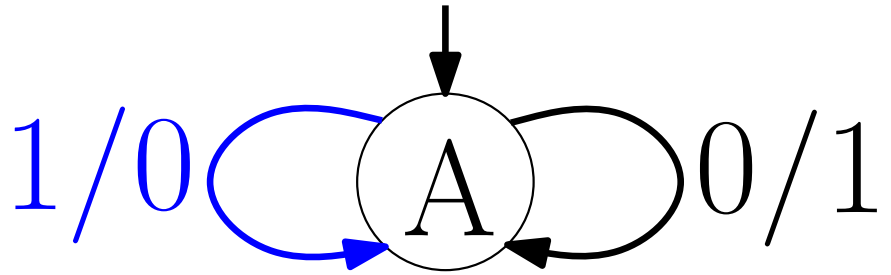


On écrit 1 et on va à l'état A
Sortie : 101

Exemple d'automate : inversion de bits

Lecture du mot 01011

On lit 1



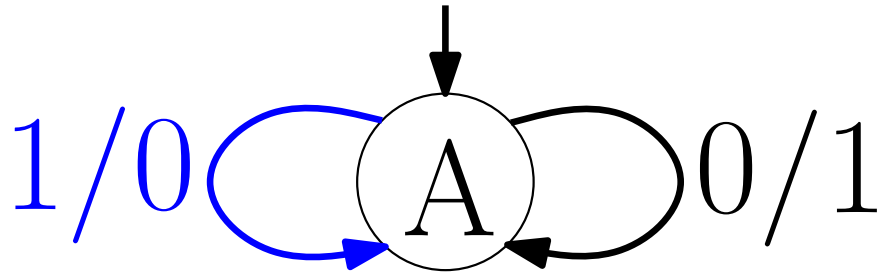
On écrit 0 et on va à l'état A

Sortie : 1010

Exemple d'automate : inversion de bits

Lecture du mot 01011

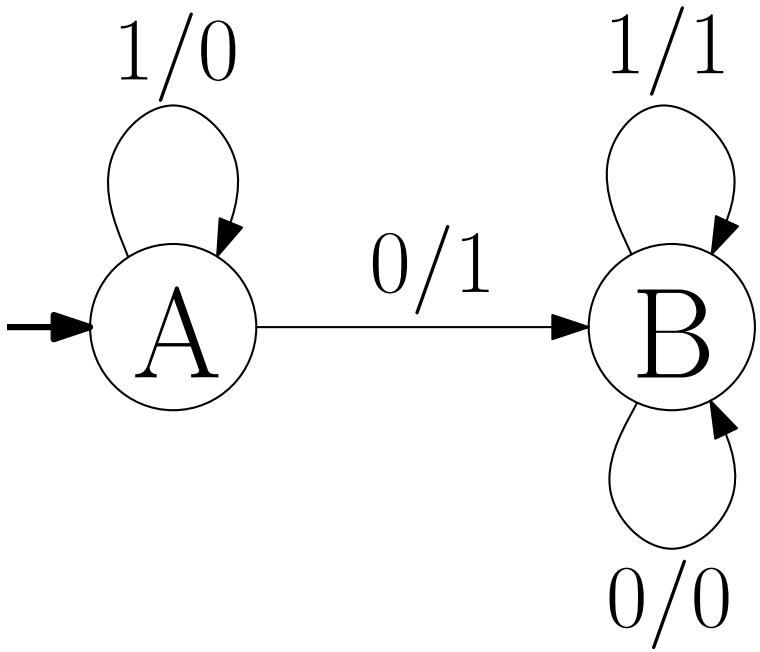
On lit 1



On écrit 0 et on va à l'état A

Sortie : 10100

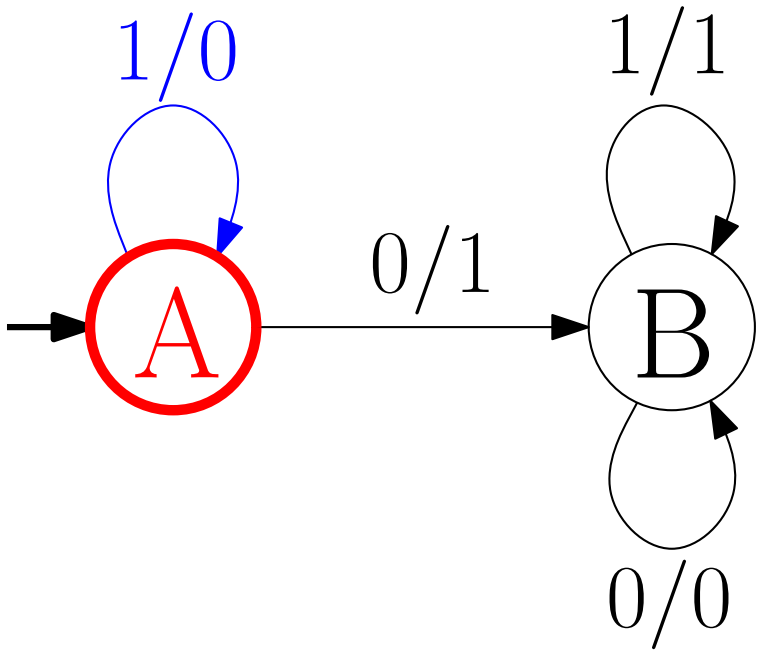
Exemple d'automate : incrémenteur



Exemple d'automate : incrémenteur

Lecture du mot 11001

On est à l'état A et on lit 1

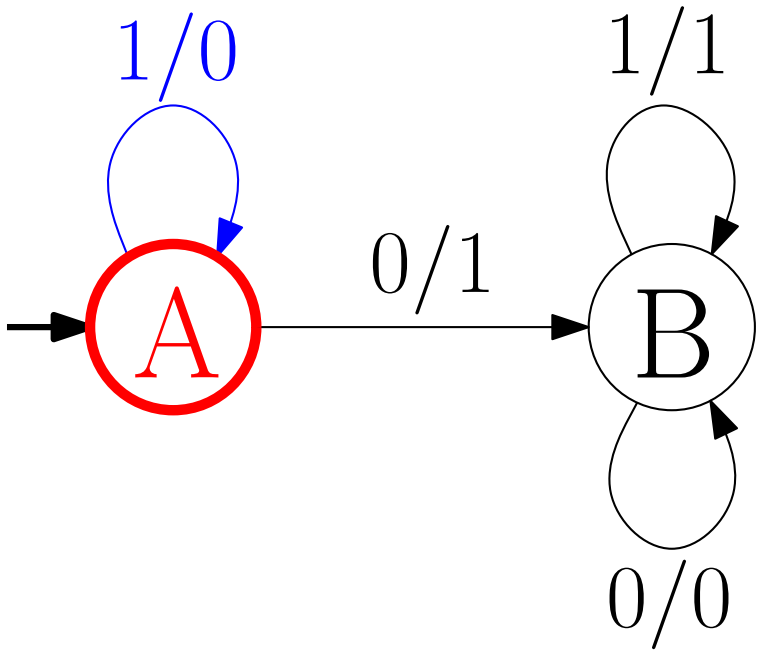


On écrit 0 et on va à l'état A
Sortie : 0

Exemple d'automate : incrémenteur

Lecture du mot 11001

On est à l'état A et on lit 1

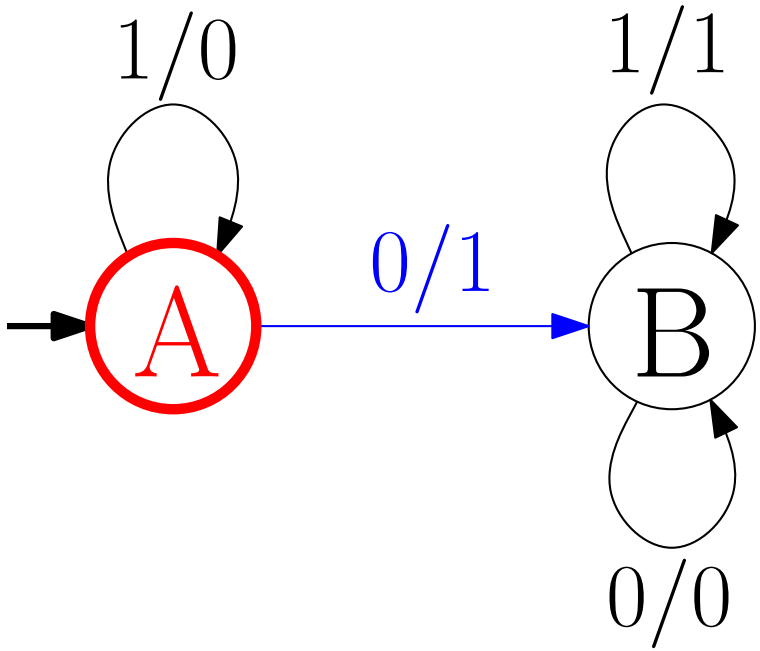


On écrit 0 et on va à l'état A
Sortie : 00

Exemple d'automate : incrémenteur

Lecture du mot 11001

On est à l'état A et on lit 0

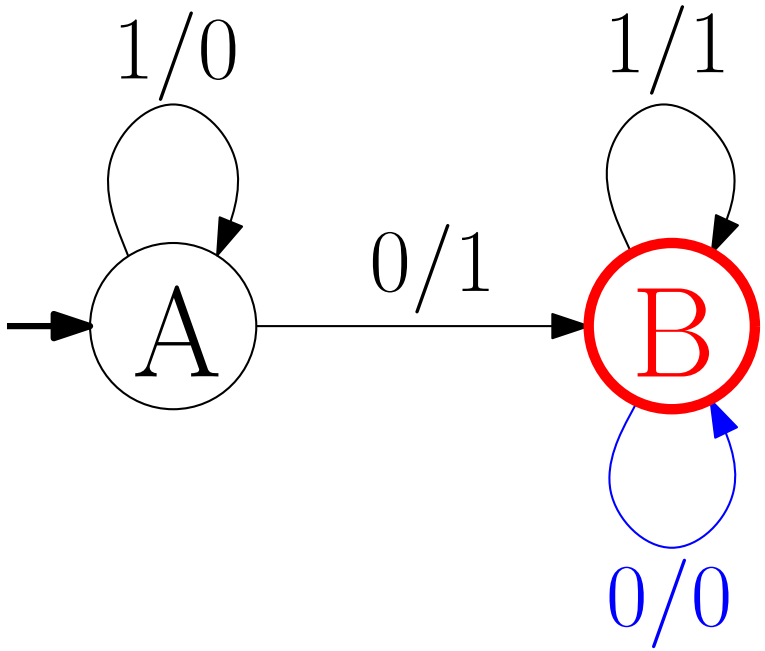


On écrit 1 et on va à l'état B
Sortie : 001

Exemple d'automate : incrémenteur

Lecture du mot 11001

On est à l'état B et on lit 0

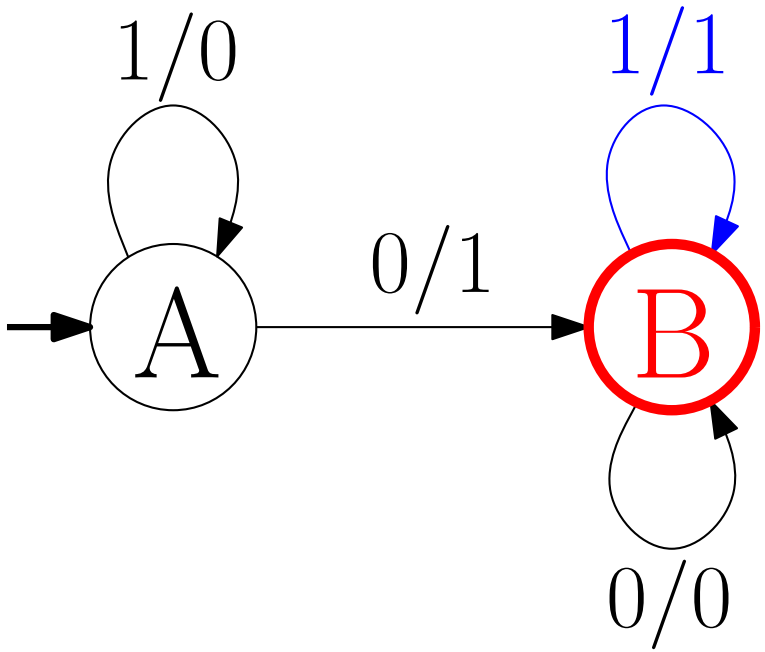


On écrit 0 et on va à l'état B
Sortie : 0010

Exemple d'automate : incrémenteur

Lecture du mot 11001

On est à l'état B et on lit 1



On écrit 1 et on va à l'état B
Sortie : 00101

Exemple d'automate : incrémenteur

Mot en entrée : 11001

Mot en sortie : 00101

Mot en entrée inversé : 10011
Mot en sortie inversé : 10100

Additionneur pour la représentation binaire :

$(10011)_2 + (1)_2 = (10100)_2$

Automates pour le codage

Un automate peut implémenter un code.

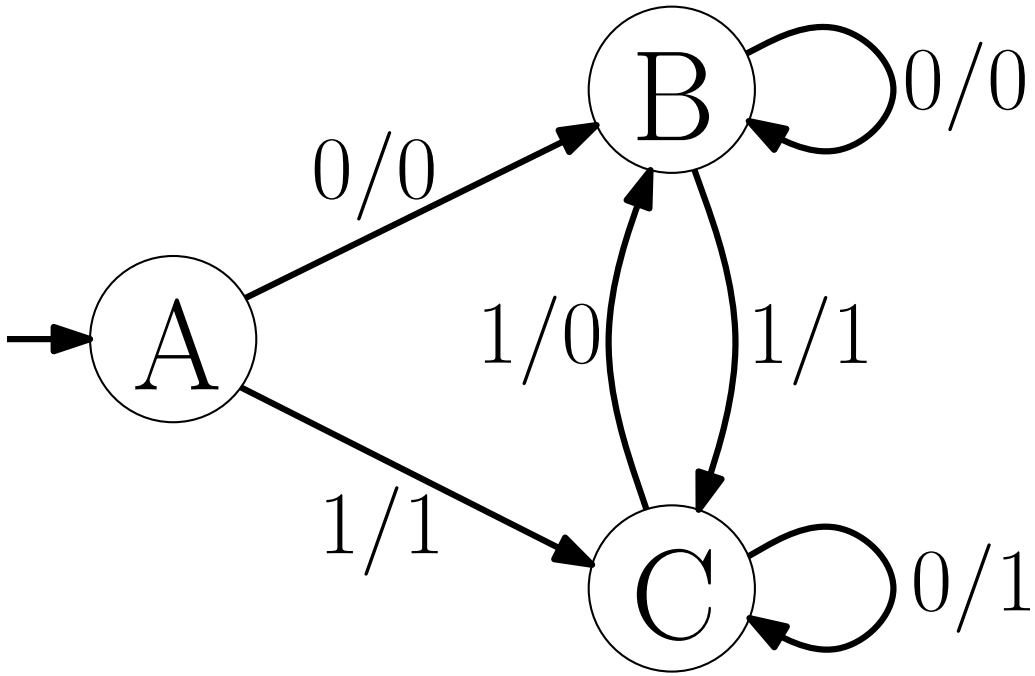
Cela permet de crypter de l'information.

Cette information sera incompréhensible pour toute personne n'ayant pas l'automate.

Définition d'un code

Un code est une application injective d'un ensemble de mots vers un ensemble de mot.

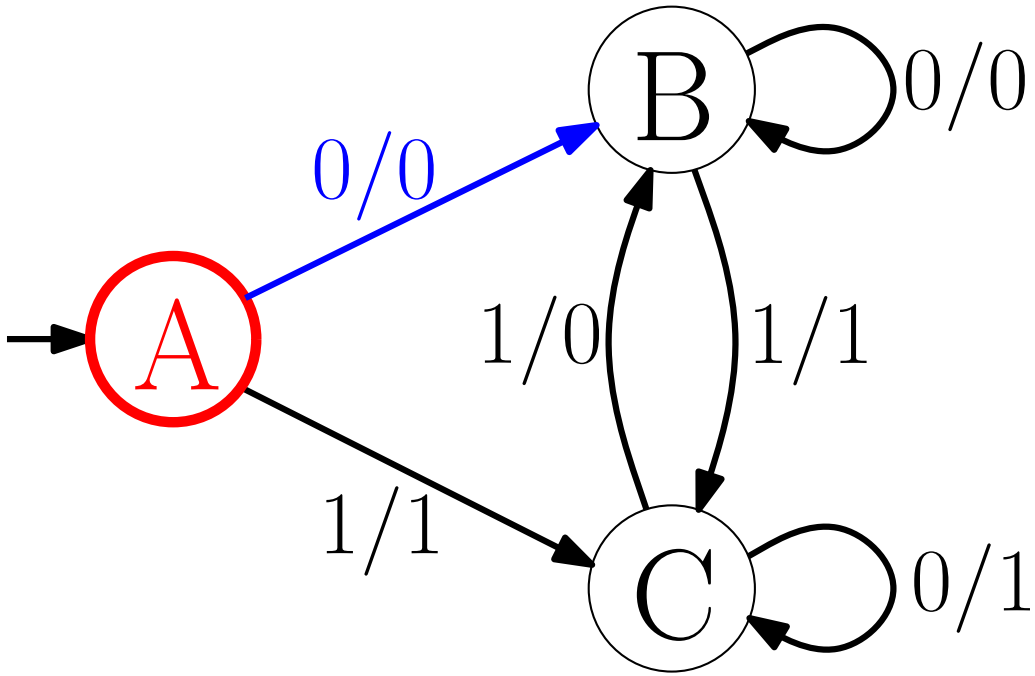
Exemple d'automate : crypteur



Exemple d'automate : crypteur

Lecture du mot 01110

On est à l'état A et on lit 0

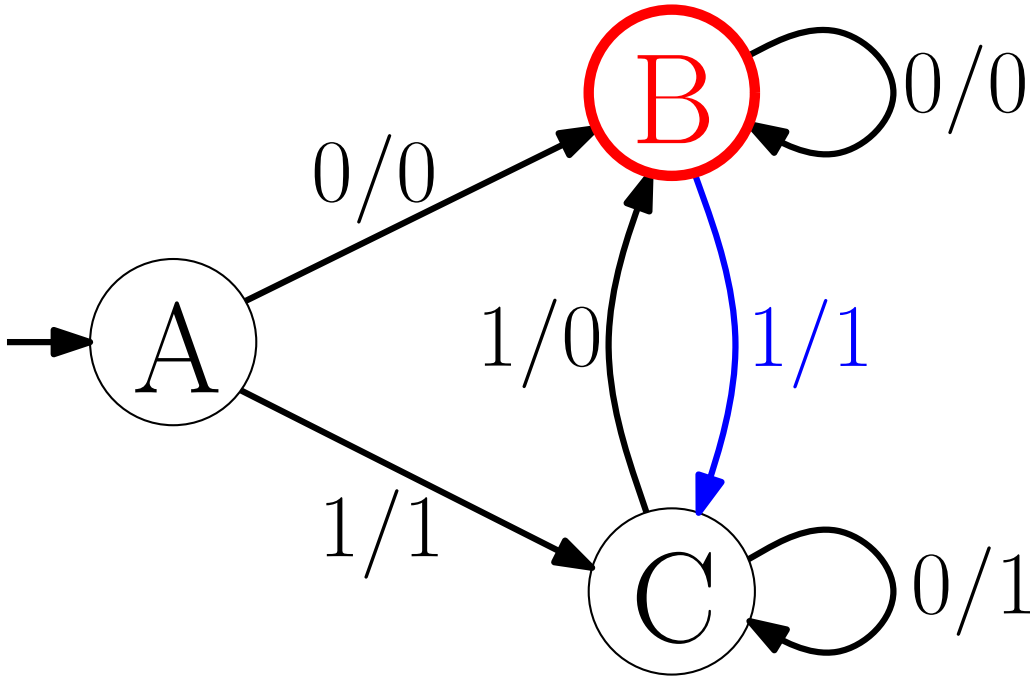


On écrit 0 et on va à l'état B
Sortie : 0

Exemple d'automate : crypteur

Lecture du mot 01110

On est à l'état B et on lit 1

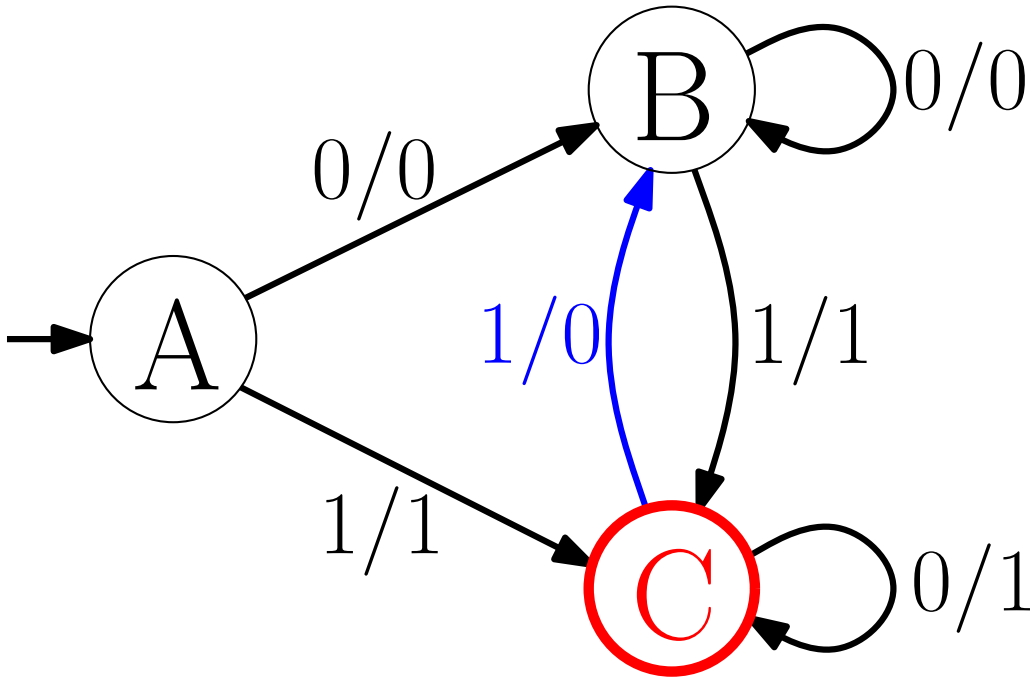


On écrit 1 et on va à l'état C
Sortie : 01

Exemple d'automate : crypteur

Lecture du mot 01110

On est à l'état C et on lit 1

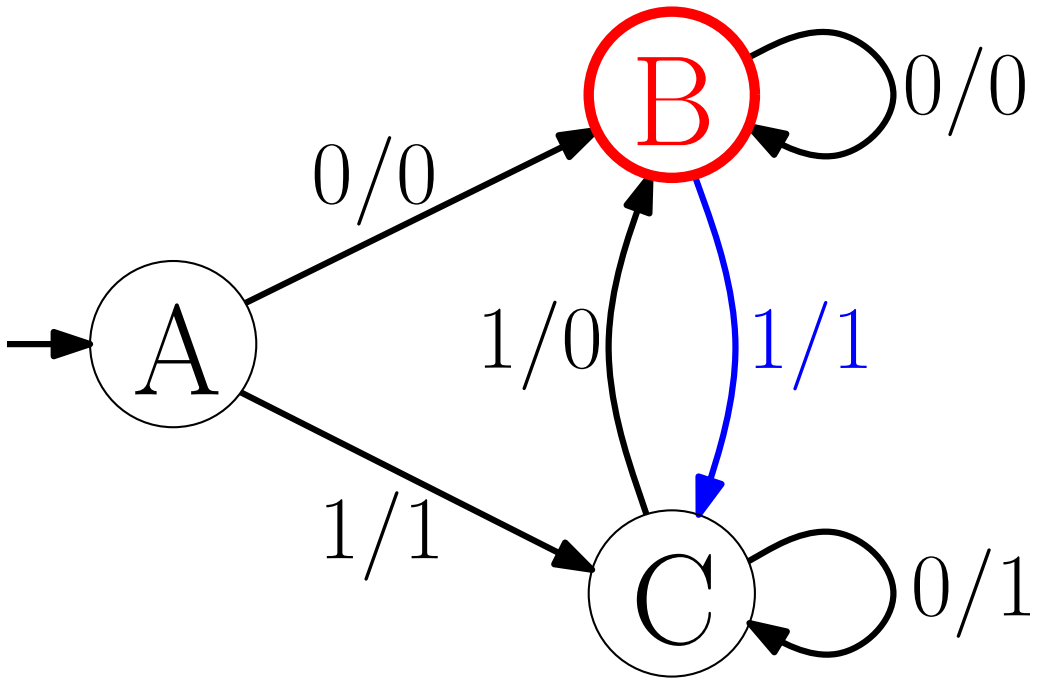


On écrit 0 et on va à l'état B
Sortie : 010

Exemple d'automate : crypteur

Lecture du mot 01110

On est à l'état B et on lit 1

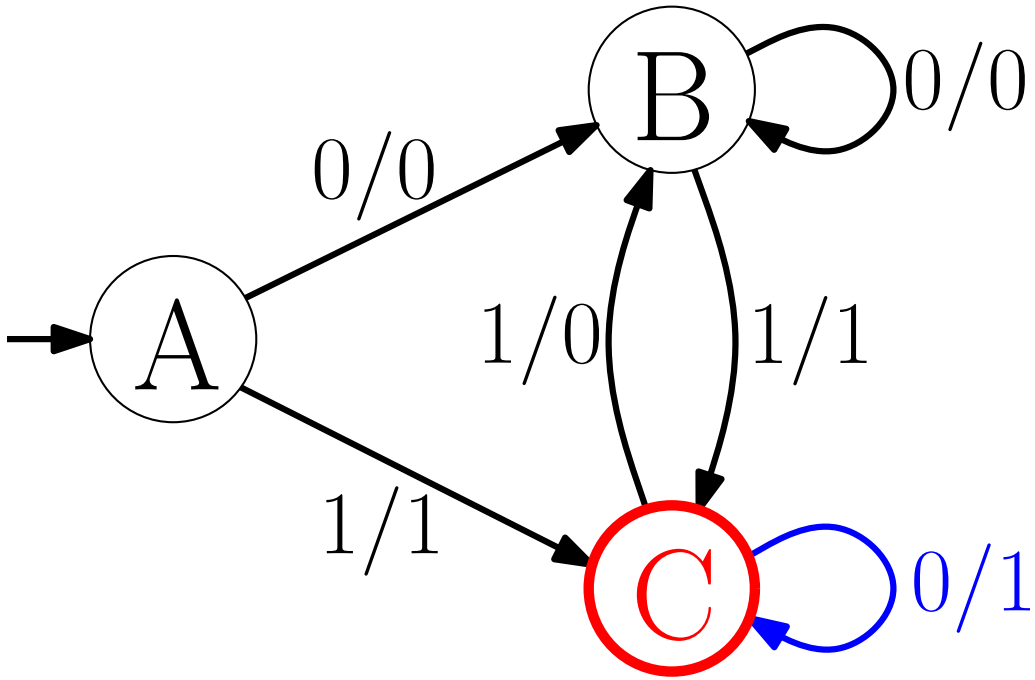


On écrit 1 et on va à l'état C
Sortie : 0101

Exemple d'automate : crypteur

Lecture du mot 01110

On est à l'état C et on lit 0



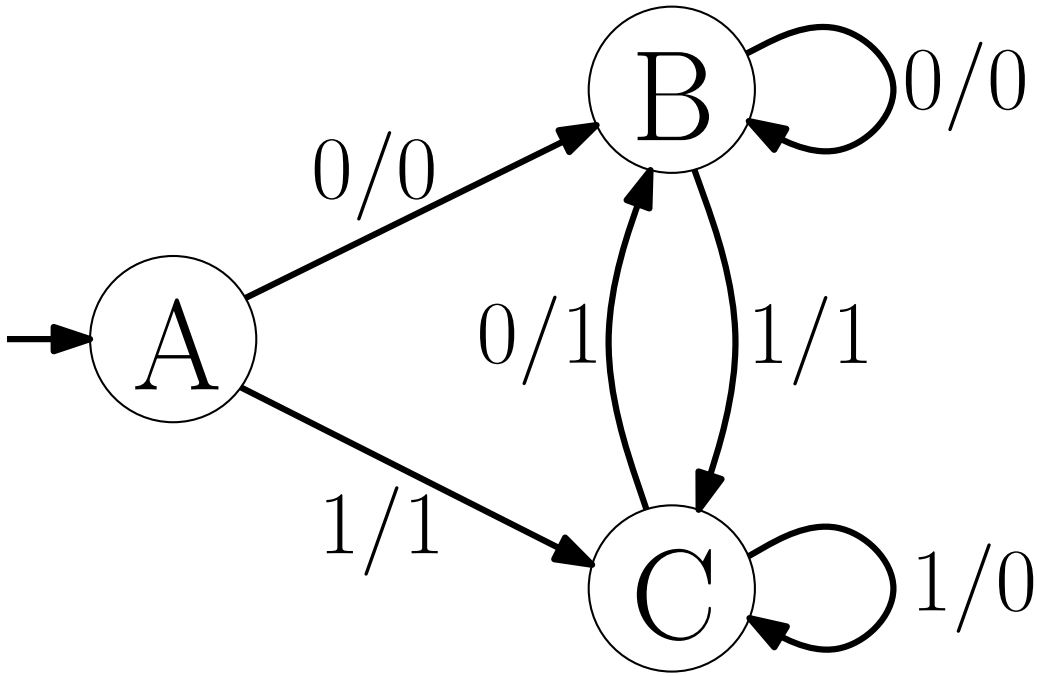
On écrit 1 et on va à l'état C
Sortie : 01011

Résultat du codage

L'automate a lu le mot 01110 et a produit le mot 01011.

La fonction implémentée par cet automate est bijective et il est possible de coder sa réciproque sous forme d'automate.

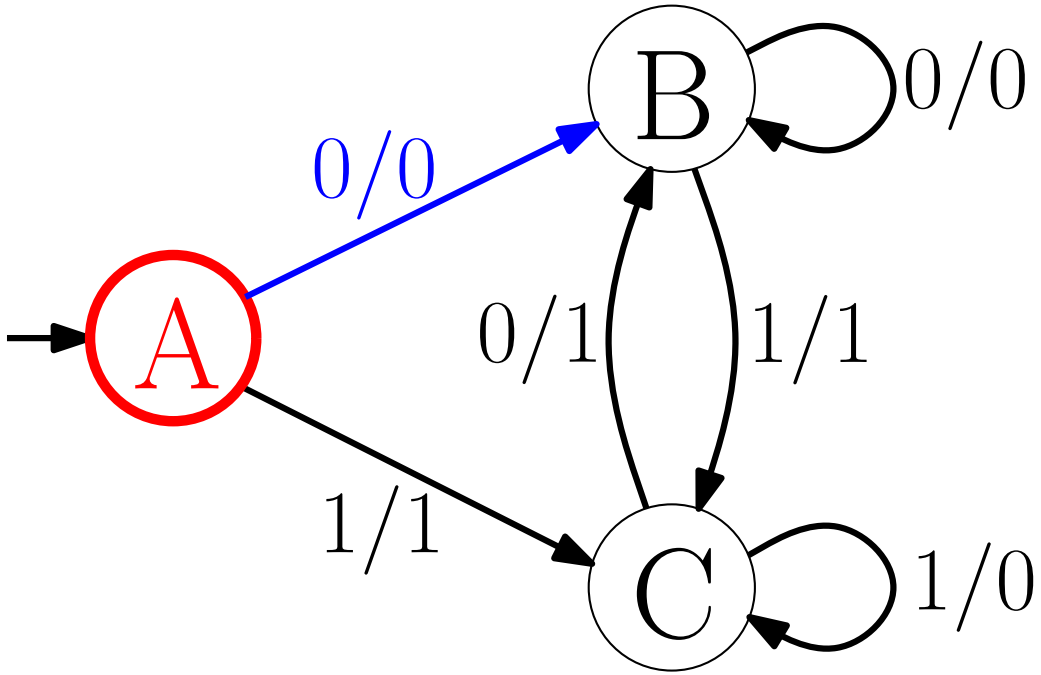
Exemple d'automate : décrypteur



Exemple d'automate : décrypteur

Lecture du mot 01011

On est à l'état A et on lit 0

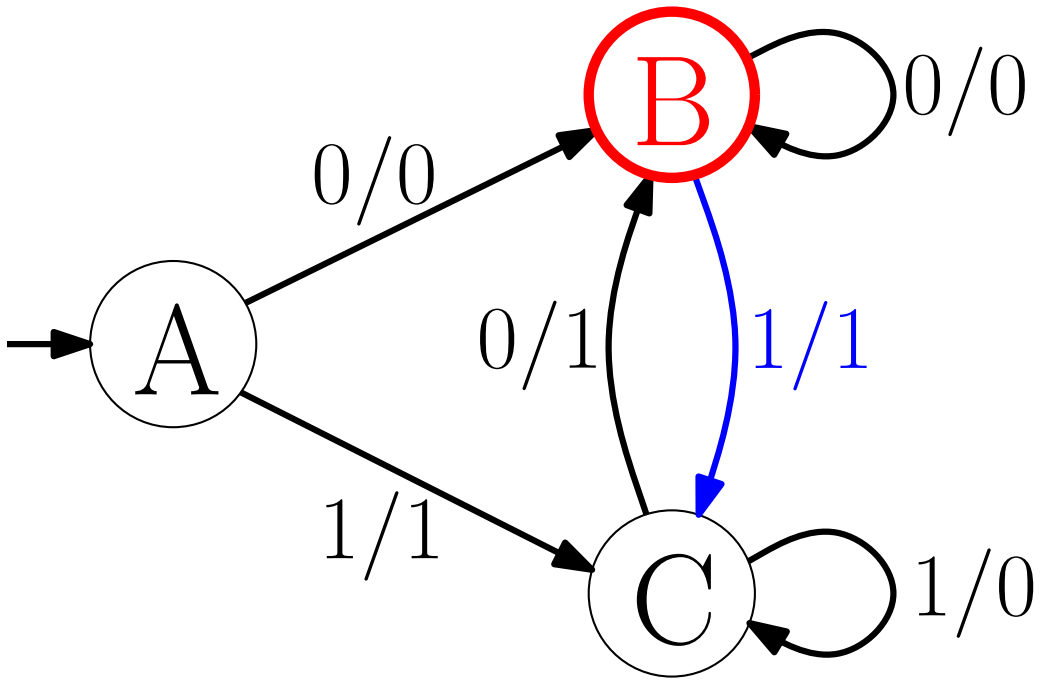


On écrit 0 et on va à l'état B
Sortie : 0

Exemple d'automate : décrypteur

Lecture du mot 01011

On est à l'état B et on lit 1

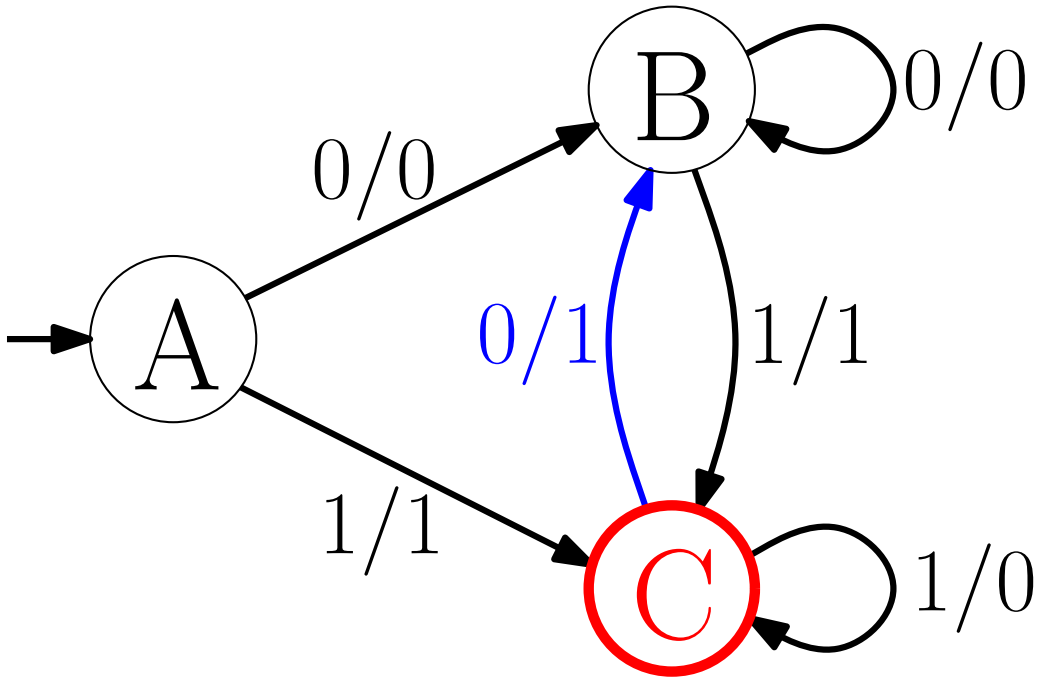


On écrit 1 et on va à l'état C
Sortie : 01

Exemple d'automate : décrypteur

Lecture du mot 01011

On est à l'état C et on lit 0

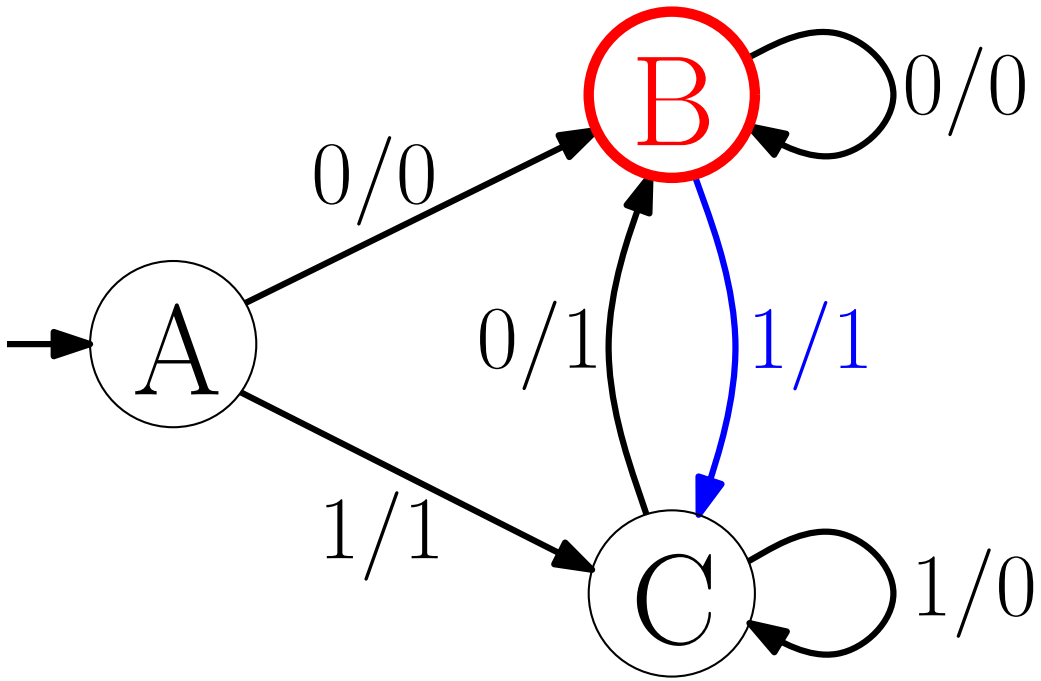


On écrit 1 et on va à l'état B
Sortie : 011

Exemple d'automate : décrypteur

Lecture du mot 01011

On est à l'état B et on lit 1

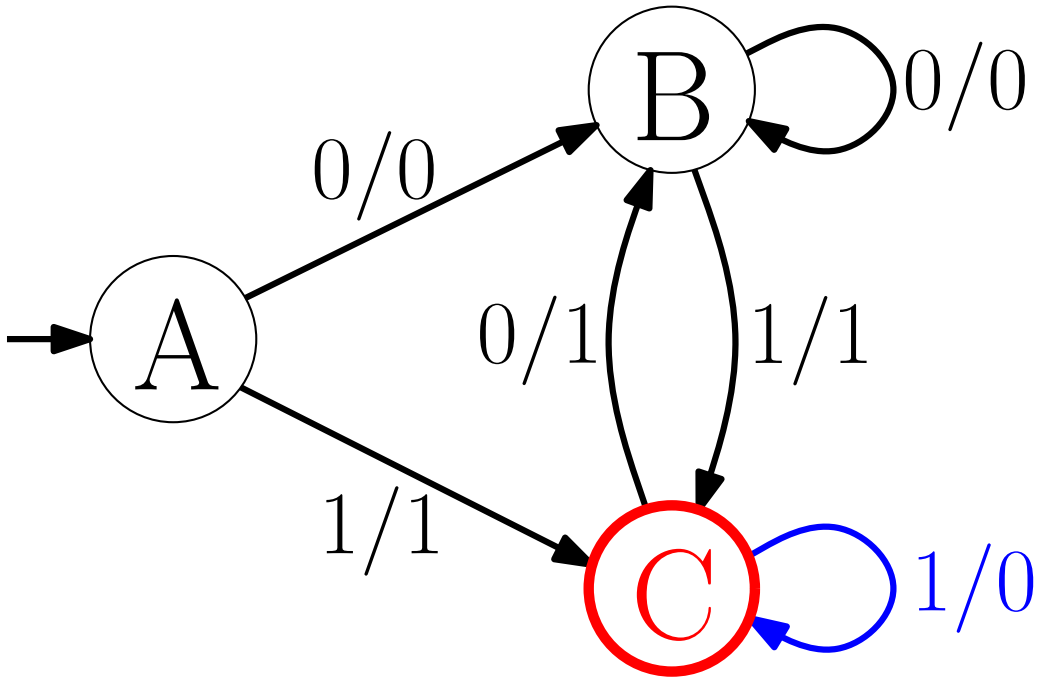


On écrit 1 et on va à l'état C
Sortie : 0111

Exemple d'automate : décrypteur

Lecture du mot 01011

On est à l'état C et on lit 1



On écrit 0 et on va à l'état C
Sortie : 01110

Résultat du décryptage

L'automate a lu le mot 01011 et a produit le mot 01110.

L'automate crypteur décrit une fonction $f : \mathbb{B}^* \to \mathbb{B}^*$

L'automate décrypteur décrit la fonction inverse $f^{-1} : \mathbb{B}^* \to \mathbb{B}^*$

Il est donc possible de retrouver l'information originelle à partir du code si on nous donne l'automate décrypteur.

$$01011 \xrightarrow{\text{codage}} 01110 \xrightarrow{\text{décodage}} 01011$$

Exemple d'utilisation

On peut utiliser notre automate pour coder du texte en utilisant le code ASCII.

Exemple : ANANAS

$A \rightarrow 0100\ 0001 \xrightarrow{codage} 0111\ 1110 \rightarrow \sim$

$N \rightarrow 0100\ 1110 \xrightarrow{codage} 0111\ 0011 \rightarrow t$

$S \rightarrow 0101\ 0011 \xrightarrow{codage} 0110\ 0010 \rightarrow b$

$ANANAS \xrightarrow{codage} \sim\ t \sim t \sim b$

Méthode générale pour inverser un automate

On part d'un automate $A = (Q, i, E, S, \delta)$ qui implémente la fonction $f : \mathbb{B}^* \to \mathbb{B}^*$.

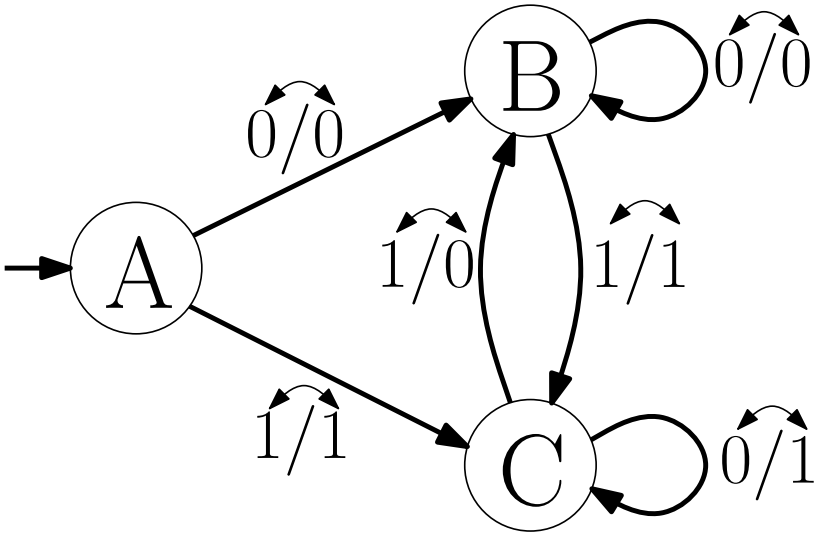
Si f est injective alors, on peut construire l'automate $A' = (Q', i', E', S', \delta)$ implémente la fonction f^{-1} (la fonction inverse de f).

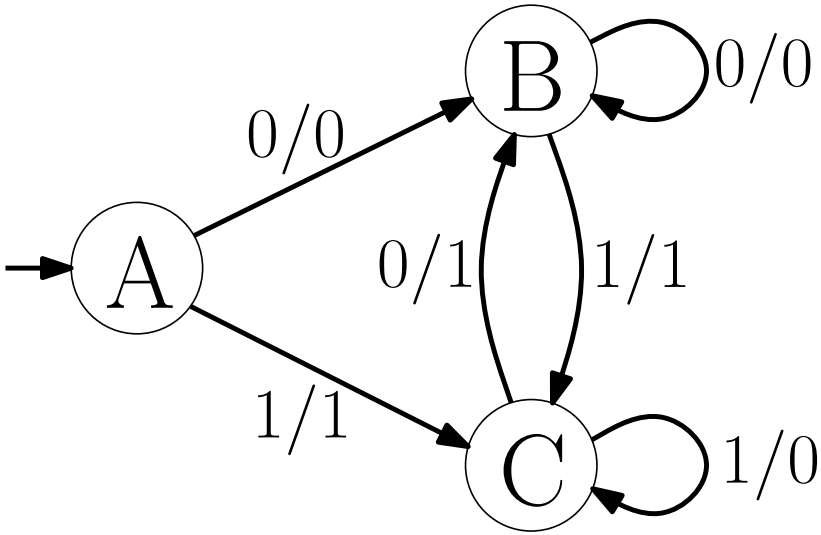
A' a le même ensemble d'états et le même état initial que A : $Q' = Q$ et $i' = i$

L'alphabet de sortie de A' est l'alphabet d'entrée de A et inversement : $S' = E$ et $E' = S$

Chaque transition $B \xrightarrow{x/y} C$ dans A devient une transition $B \xrightarrow{y/x} C$ dans A' :
$\forall B, C \in Q, \forall x \in E, \forall y \in S, \delta(B, x) = (C, y) \Leftrightarrow \delta'(B, y) = (C, x)$.

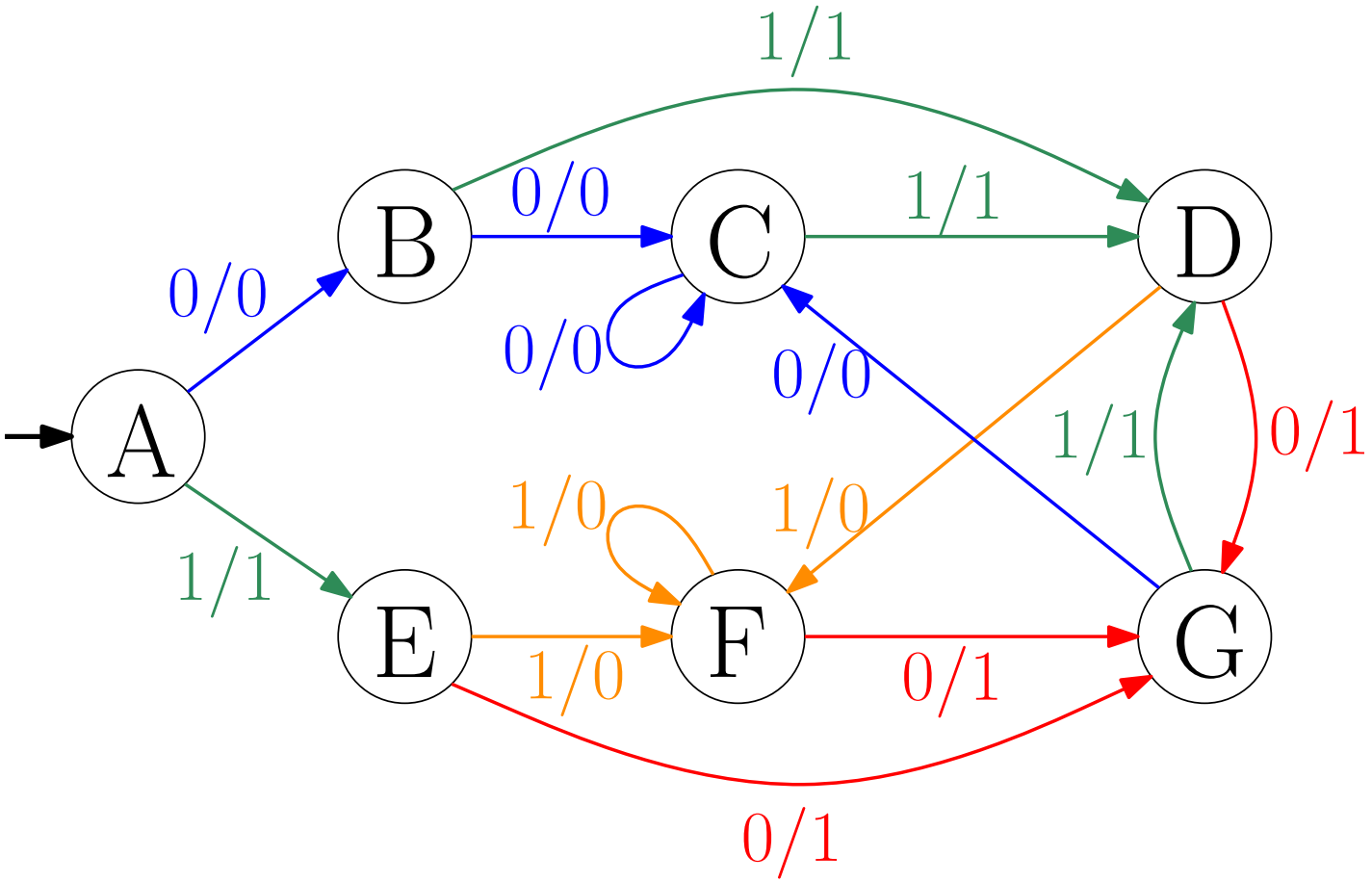
Inversion sur l'exemple





Fonction et automates

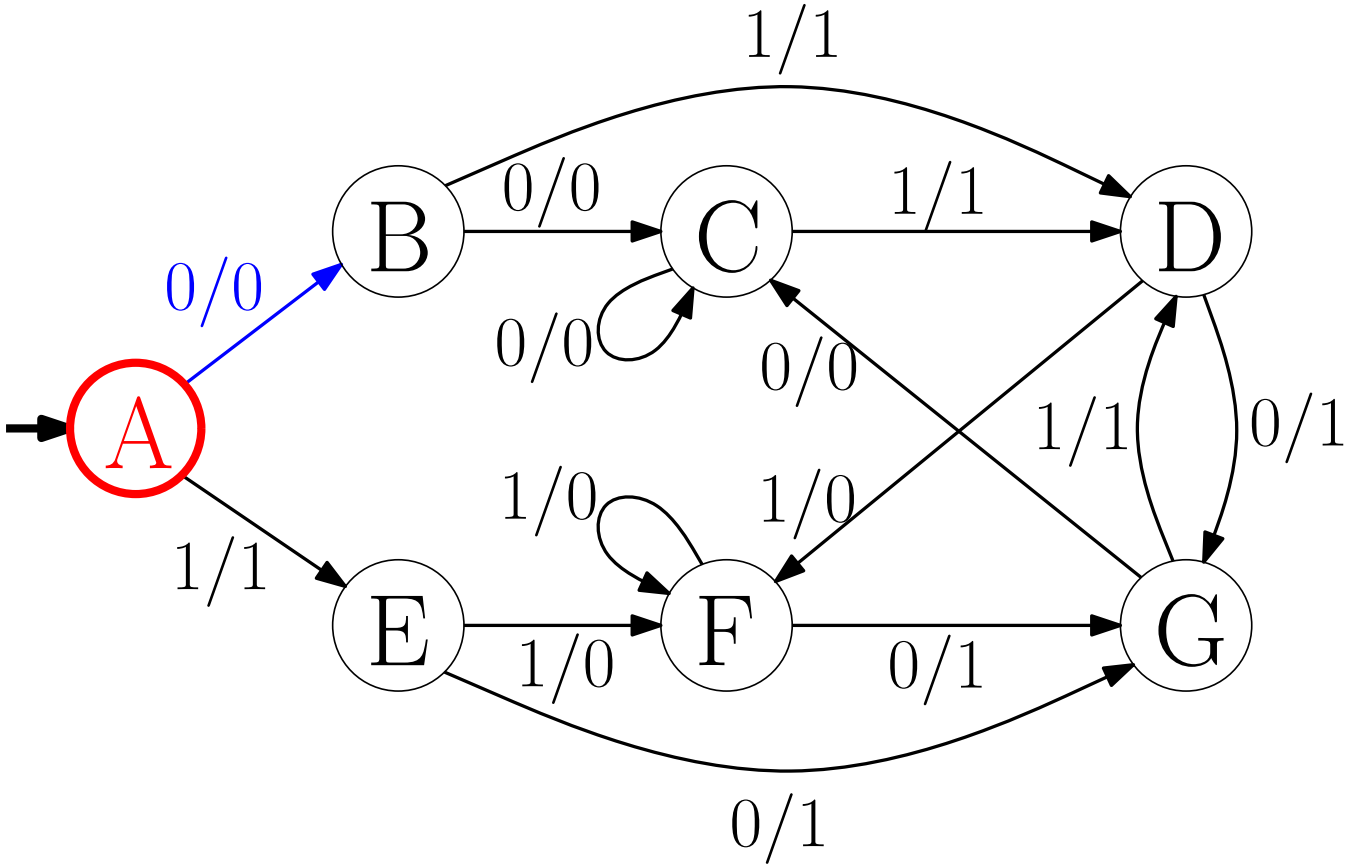
Une fonction peut être implémenté par plusieurs automates Par exemple, l'automate suivant implémente la même fonction que l'automate décrypteur.



Lecture d'un mot par décrypteur 2

Lecture du mot 01011

On est à l'état A et on lit 0



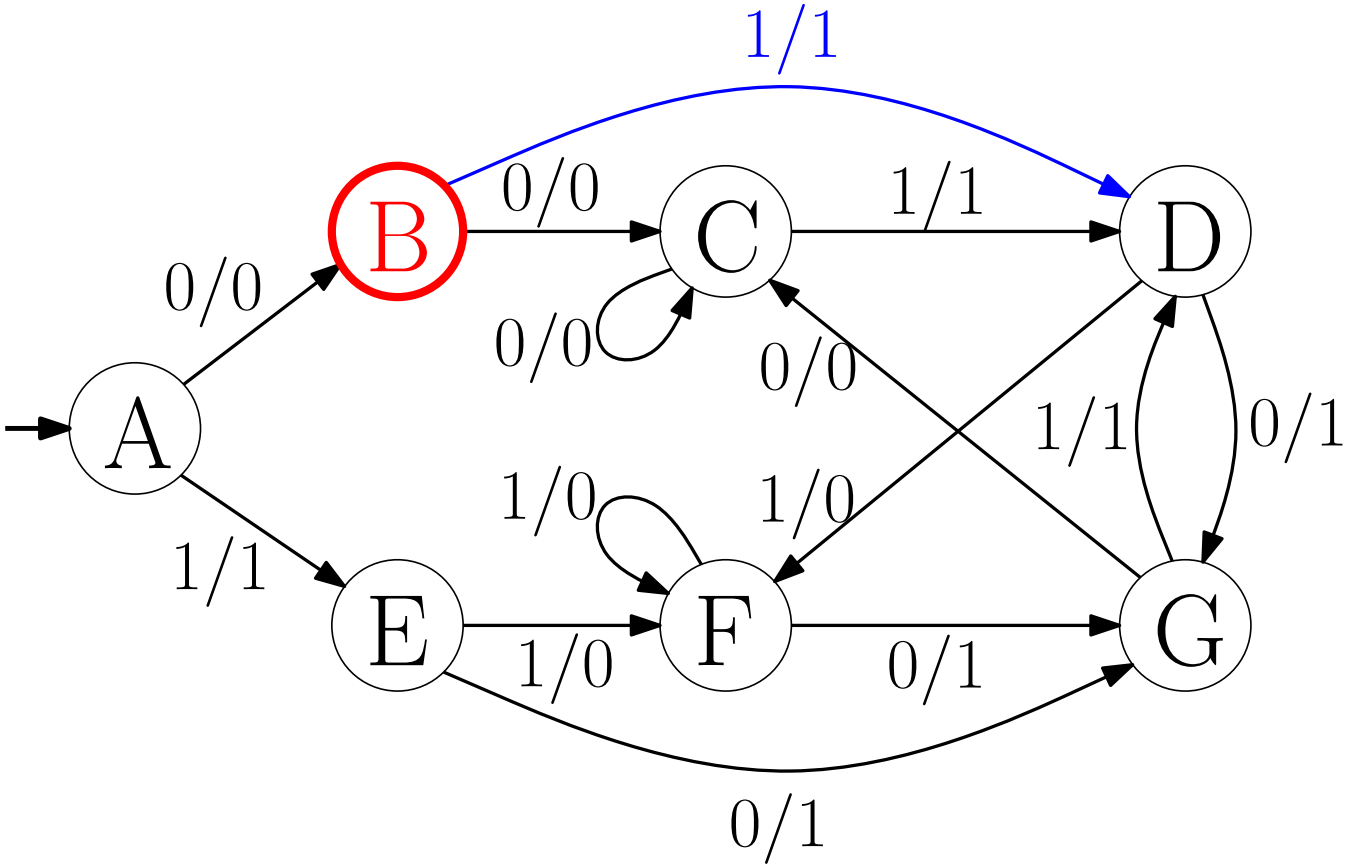
On écrit 0 et on va à l'état B

Sortie : 0

Lecture d'un mot par décrypteur 2

Lecture du mot 01011

On est à l'état B et on lit 1



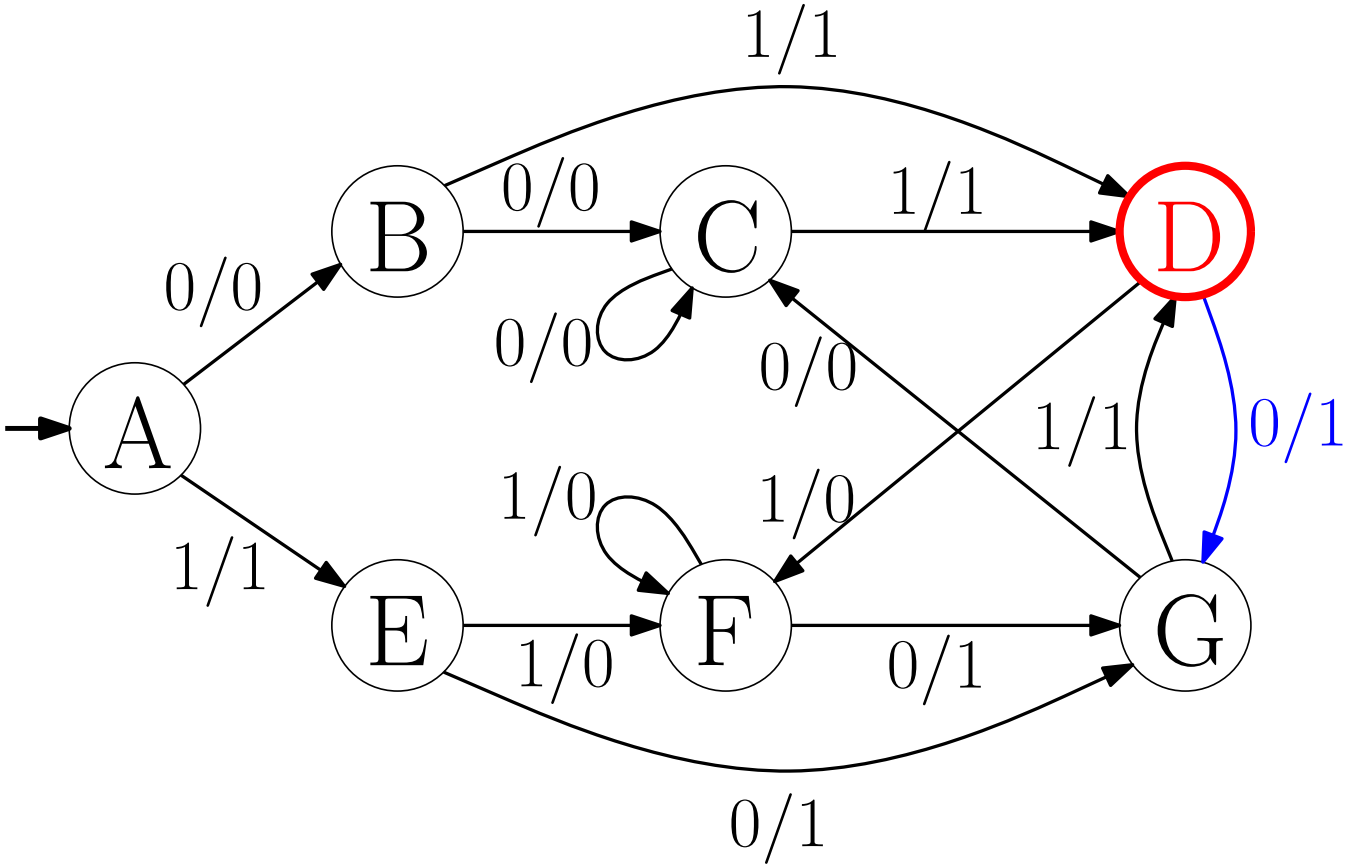
On écrit 1 et on va à l'état D

Sortie : 01

Lecture d'un mot par décrypteur 2

Lecture du mot 01011

On est à l'état D et on lit 0



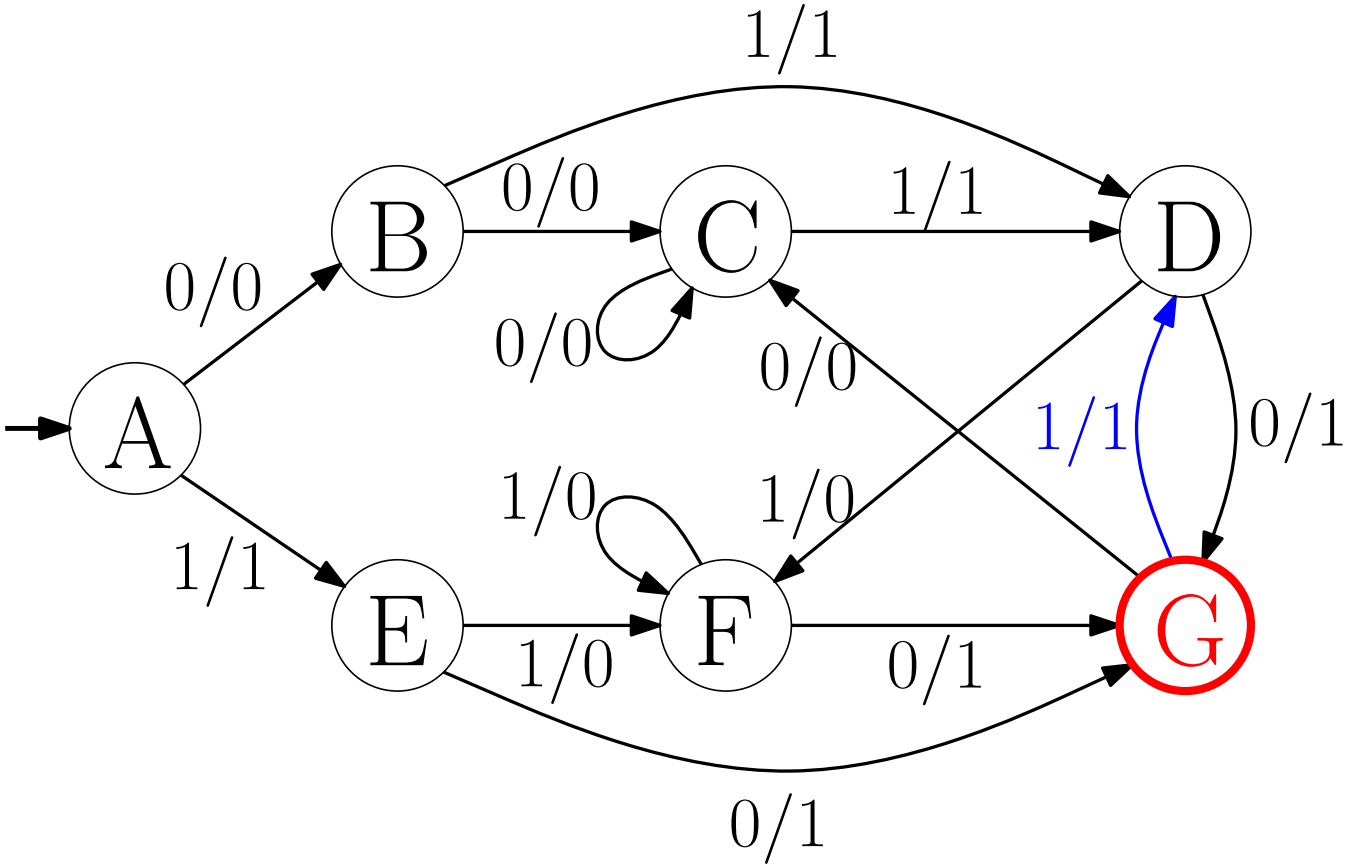
On écrit 1 et on va à l'état G

Sortie : 011

Lecture d'un mot par décrypteur 2

Lecture du mot 01011

On est à l'état G et on lit 1



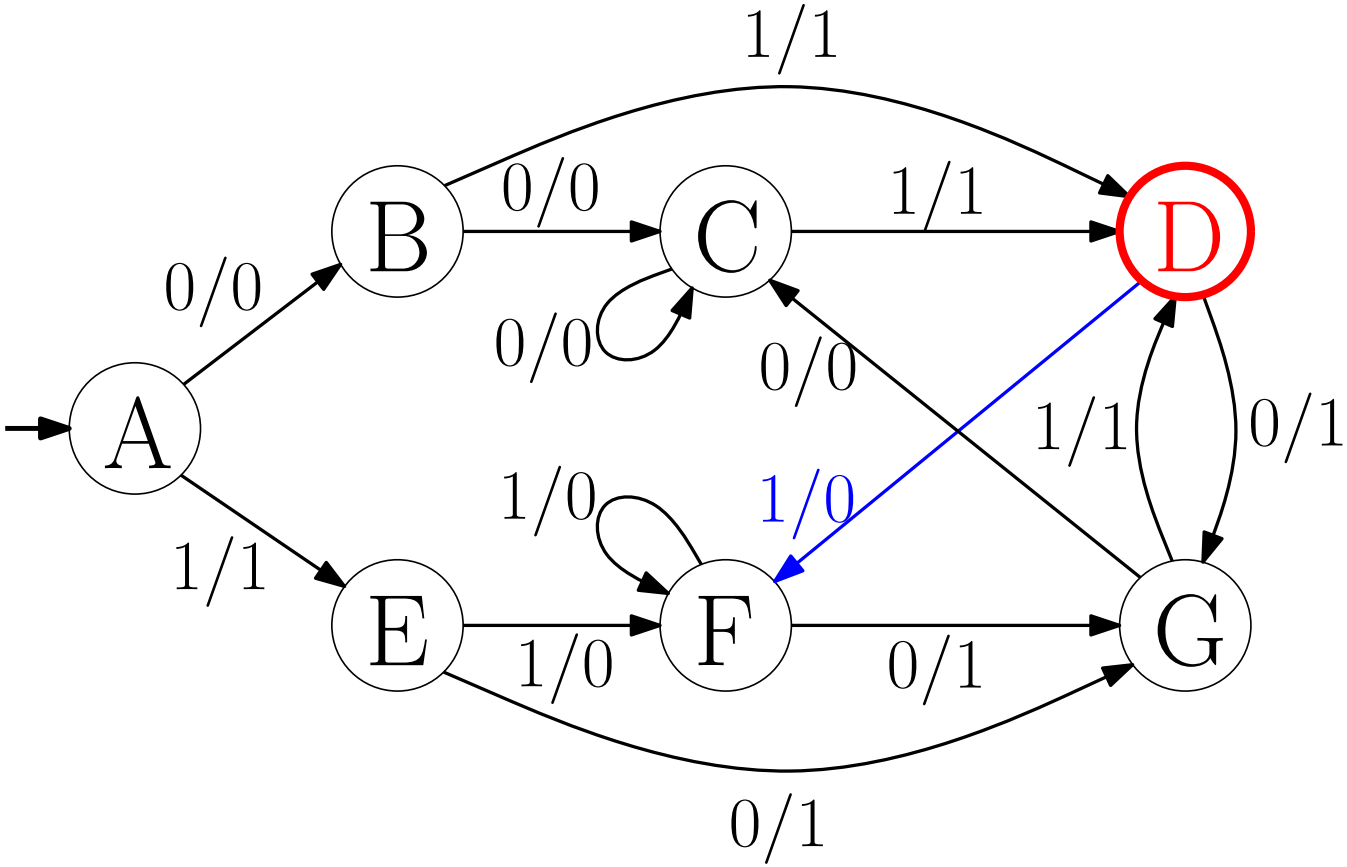
On écrit 1 et on va à l'état D

Sortie : 0111

Lecture d'un mot par décrypteur 2

Lecture du mot 01011

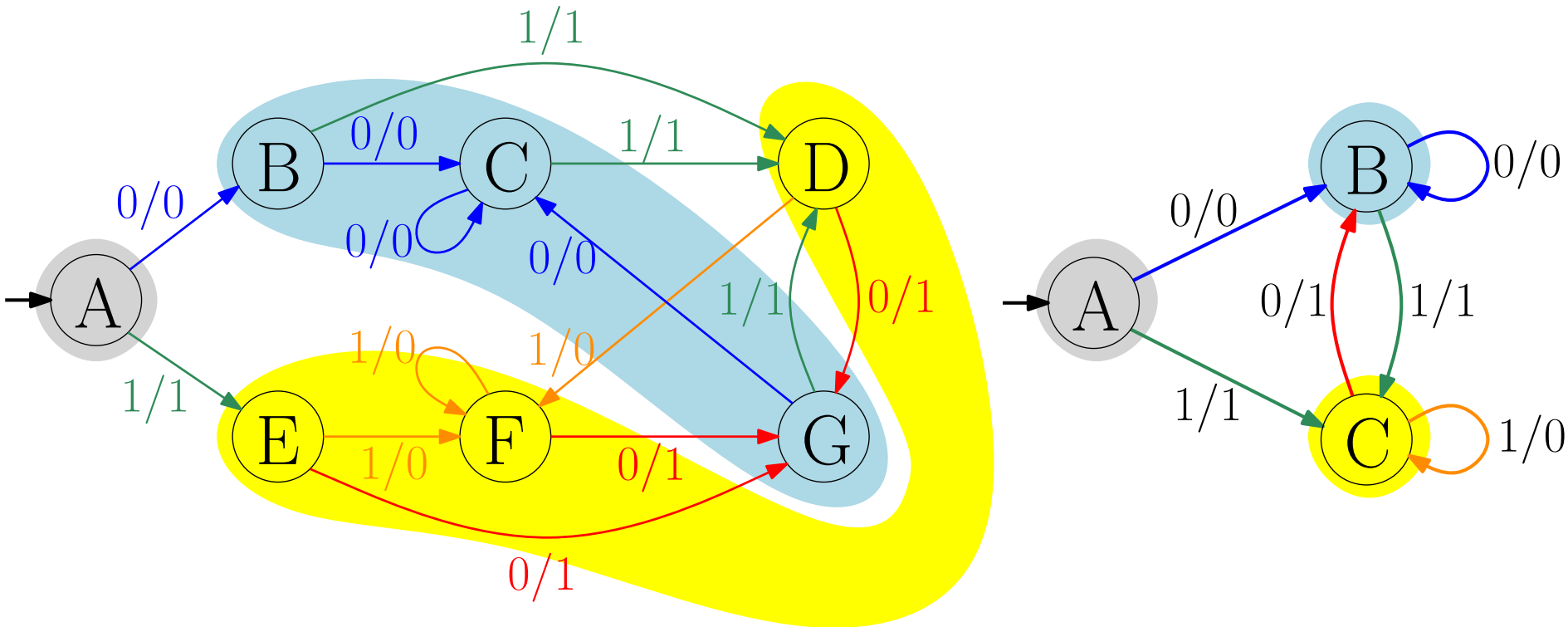
On est à l'état D et on lit 1



On écrit 0 et on va à l'état F

Sortie : 01110

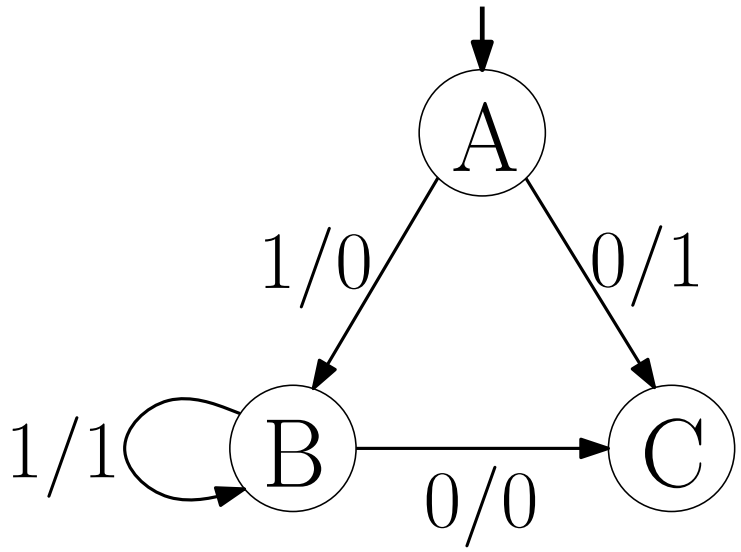
Equivalence d'automates



Lorsque deux automates implémentent la même fonction, il est possible de trouver une correspondance entre leurs états.

Implémenter un automate avec un circuit

Un automate est défini par son état initial et sa fonction de transition δ.



état initial : A

table de vérité de δ

$Q \times E$	$Q \times S$
$(A, 0)$	$(C, 1)$
$(A, 1)$	$(B, 0)$
$(B, 0)$	$(C, 0)$
$(B, 1)$	$(B, 1)$
$(C, 0)$	non défini
$(C, 1)$	non défini

Il suffit donc de coder la fonction de transition dans un circuit pour coder l'automate.

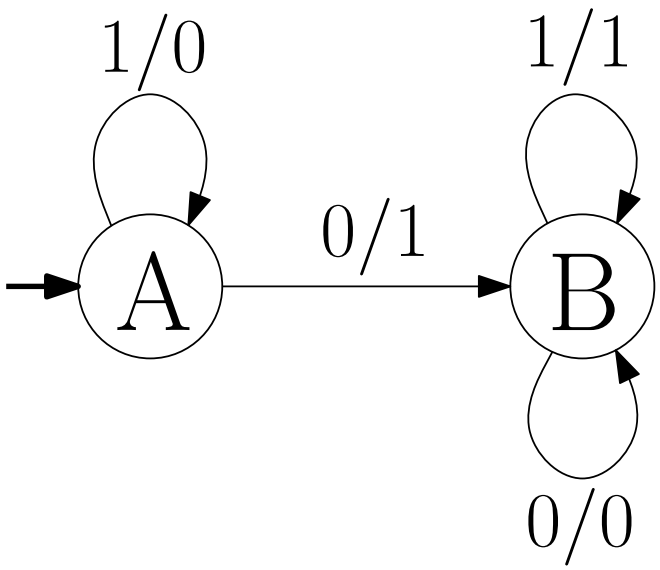
Rappel sur les circuits

Implémentation dune fonction avec un circuit

Pour pouvoir implémenter une fonction $f : A \rightarrow B$ il faut d'abord coder les éléments de A et B sous forme de mot binaires.

Avant de pouvoir coder la fonction de transition δ dans un circuit, il nous faut coder les élément de Q, E et S sous forme de mot binaires.

Exemple d'implémentation par un circuit

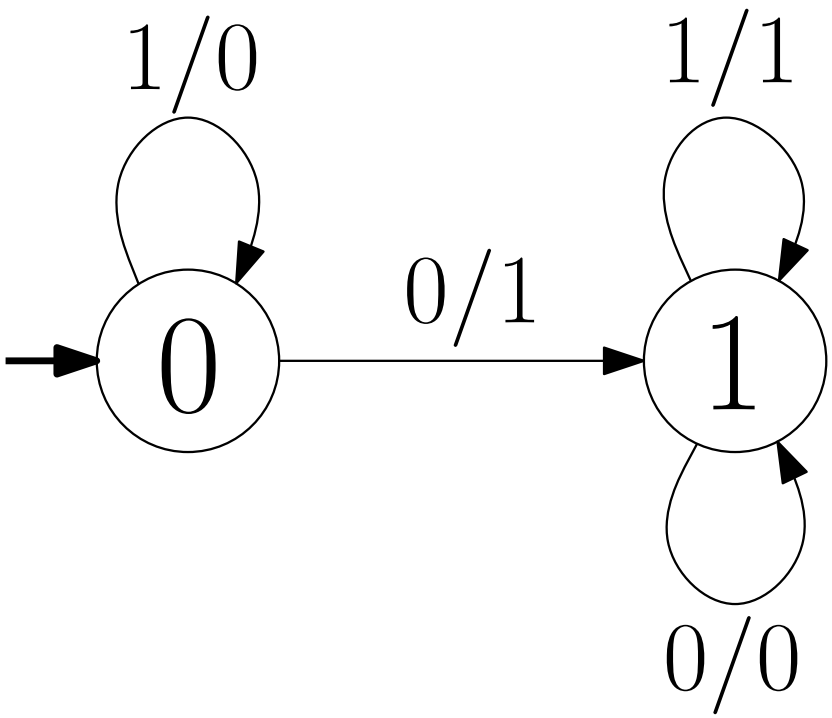


Ensemble d'états : $Q = \{A, B\}$
Alphabet d'entrée : $E = \{0, 1\}$
Alphabet de sortie : $S = \{0, 1\}$

Les éléments E et S sont déjà codés sous forme de mots binaires

On peut coder les éléments de Q avec des mots d'un bit :
$A \to 0$ et $B \to 1$

Exemple d'implémentation par un circuit



état initial : 0

table de transition donnant le nouvel état Q' et la sortie S

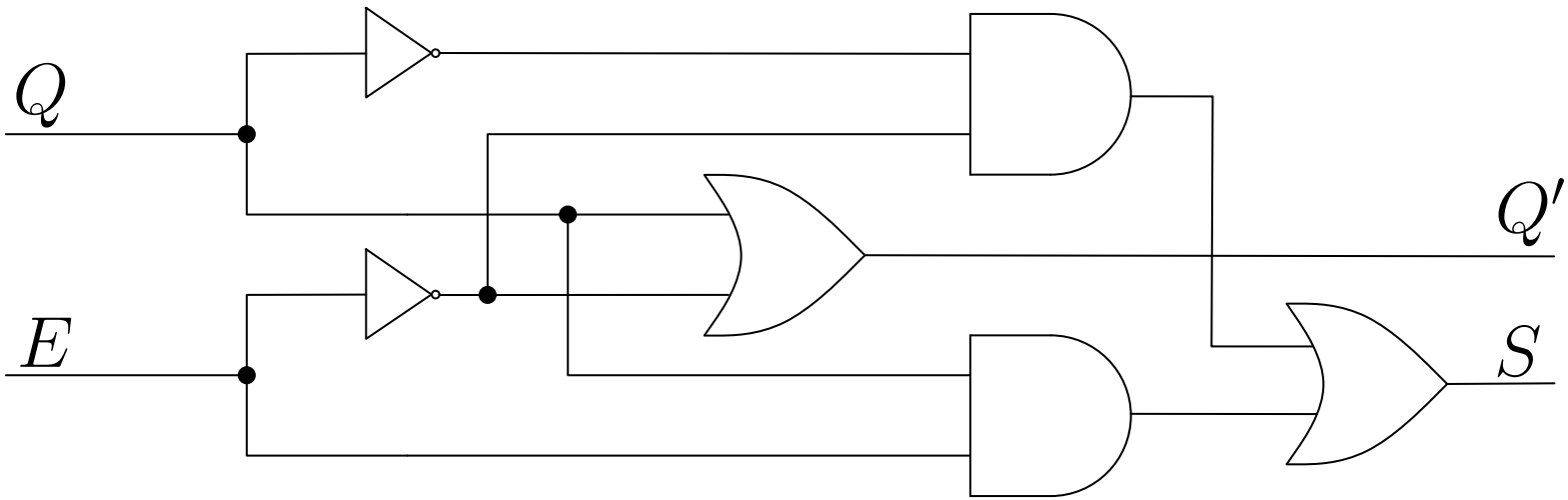
Q	E	Q'	S
0	0	1	1
0	1	0	0
1	0	1	0
1	1	1	1

Exemple d'implémentation par un circuit

table de transition donnant le nouvel état Q' et la sortie S

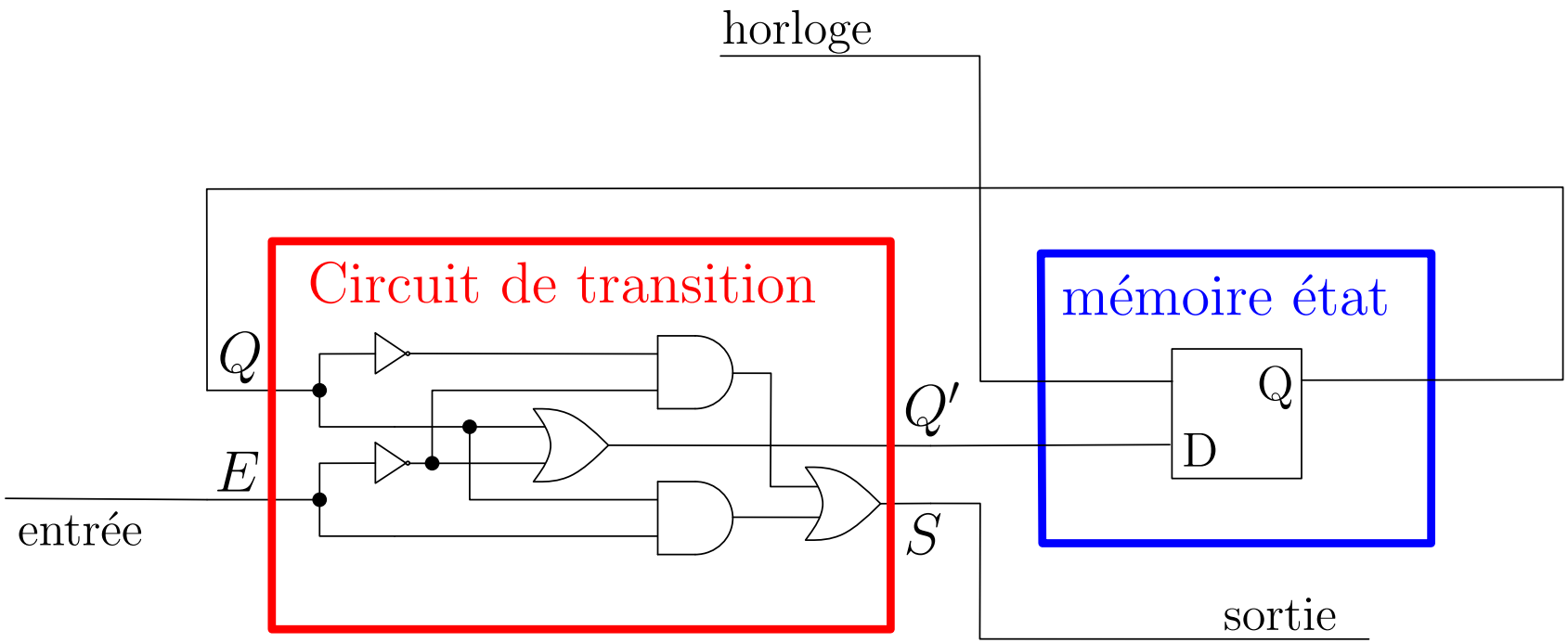
Q	E	Q'	S
0	0	1	1
0	1	0	0
1	0	1	0
1	1	1	1

circuit correspondant



Exemple d'implémentation par un circuit

Il faut rajouter de la mémoire pour conserver l'état



Exemple d'implémentation par un circuit