Méthodes Formelles Approche Probabiliste

Arnaud Sangnier

IRIF - Université de Paris

Cours 3

Les propriétés régulières

Problème :

- Comment décrire de façon concise et manipulable des propriétés temporelles linéaires qui sont en pratique des sous-ensembles de $(2^{PA})^{\omega}$?

Solution :

- On va utiliser la théorie des automates
- Un automate permet en effet de décrire de façon fini un ensemble (possiblement infini) de mots
- Dans un deuxième temps, on verra aussi des formalismes logiques

Les automates finis

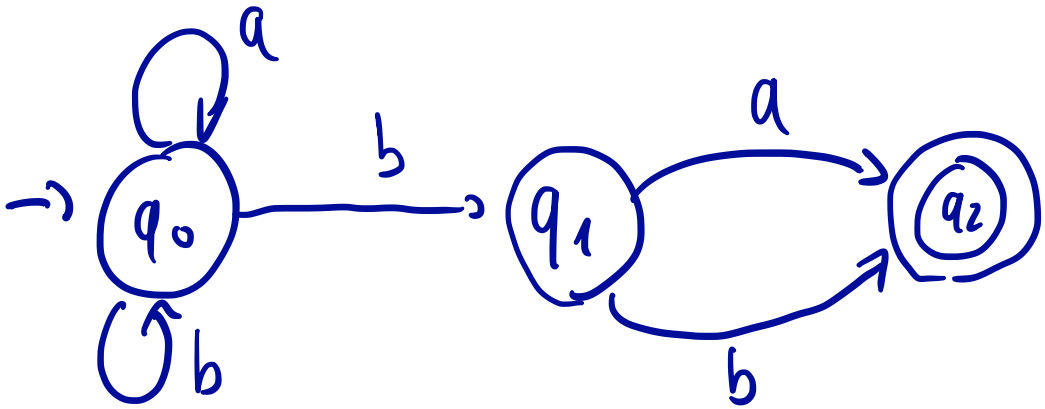
Définition

Un automate fini non-déterministe (AFN) est un n-uplet $A = (Q, \Sigma, \delta, Q_0, F)$ où :

- Q est un ensemble fini d'états
- Σ est l'alphabet
- $\delta : Q \times \Sigma \mapsto 2^Q$ est la fonction de transitions
- $Q_0 \subseteq Q$ est l'ensemble des états initiaux
- $F \subseteq Q$ est l'ensemble des états finaux

- **Notation :** On notera $q \xrightarrow{a} q'$ si, et seulement si, $q' \in \delta(q, a)$

Exemple



$\Sigma = \{a, b\}$

$Q = \{q_0, q_1, q_2\}$

$Q_0 = \{q_0\}$

$F = \{q_2\}$

$\delta(q_0, a) = \{q_0\}$

$\delta(q_0, b) = \{q_0, q_1\}$

$\delta(q_1, a) = \{q_2\}$

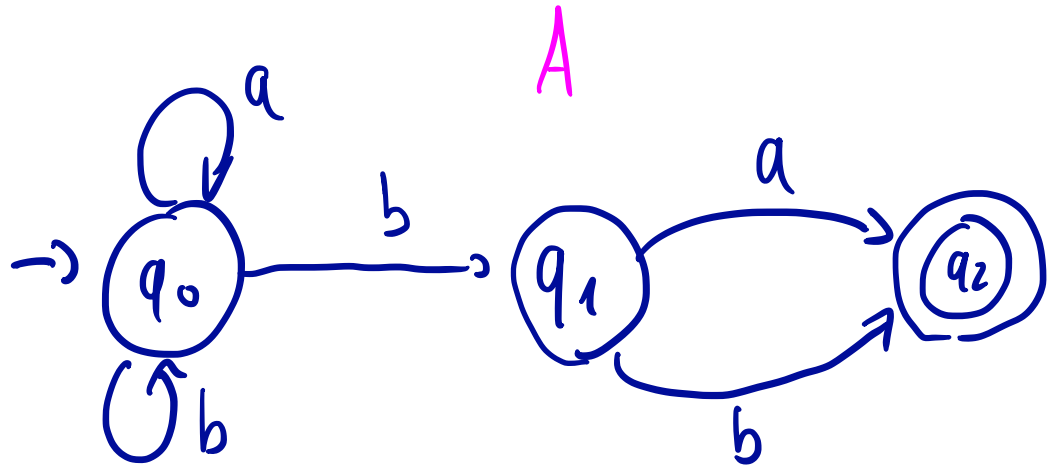
$\delta(q_1, b) = \{q_2\}$

$\delta(q_2, a) = \delta(q_2, b) = \emptyset$

Langage

- Soit $A = (Q, \Sigma, \delta, Q_0, F)$ un AFN.
- Soit $w \in \Sigma^*$ tel que $w = a_0 \dots a_n$
- Une exécution acceptante pour w dans A est une séquence finie d'états $q_0 q_1 \dots q_n q_{n+1}$ telle que $q_0 \in Q_0$ et $q_{n+1} \in F$ et $q_i \xrightarrow{a_i} q_{i+1}$ pour tout $i \in \{0, \dots, n\}$
- On note alors $\mathcal{L}(A) = \{w \in \Sigma^* \mid$ il existe une exécution acceptante pour w dans $A\}$
- $\mathcal{L}(A)$ est le langage de A - A reconnait $\mathcal{L}(A)$
- Remarquons que $\mathcal{L}(A) \subseteq \Sigma^*$

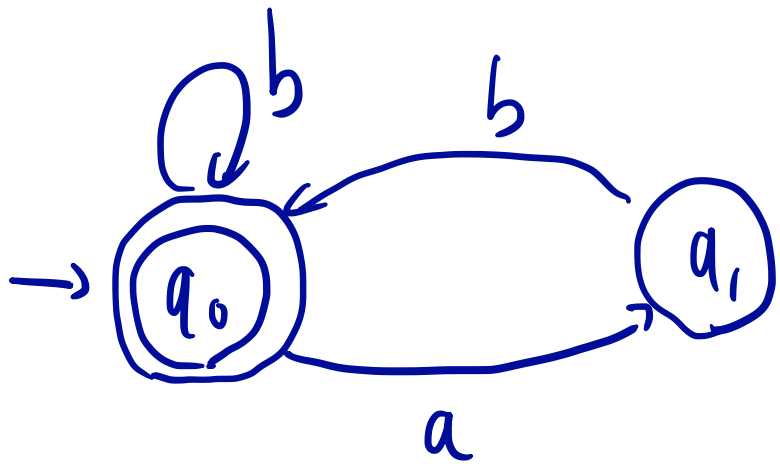
Exemple I



$$\mathcal{L}(A) = \{ w_1 w_2 \dots w_n \in \{a,b\}^+ \mid n \geq 2 \text{ et } w_{n-1} = b \}$$

Exemple II

Notre finie sur $\Sigma = \{a, b\}$ tels que à chaque fois qu'on voit un a la lettre suivante est un b



Quelques points sur les AFN

Tester le vide du langage

- Un enjeu est de savoir si un AFN A a un langage non vide (c'est-à-dire $\mathcal{L}(A) \neq \emptyset$)
- Pour cela, il suffit de chercher un chemin partant d'un état dans Q_0 vers un état dans F.
- On peut faire cela facilement avec un algorithme en profondeur d'abord d'exploration de graphe

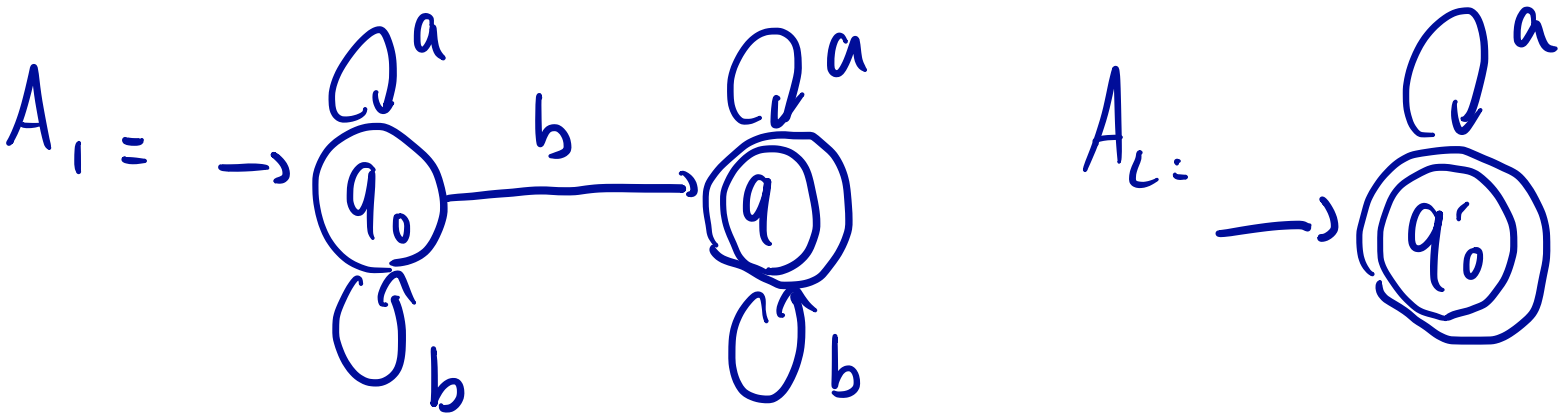
Remarque

- Les langages reconnus par des AFN sont dits réguliers, ils sont clos par union, intersection et complément

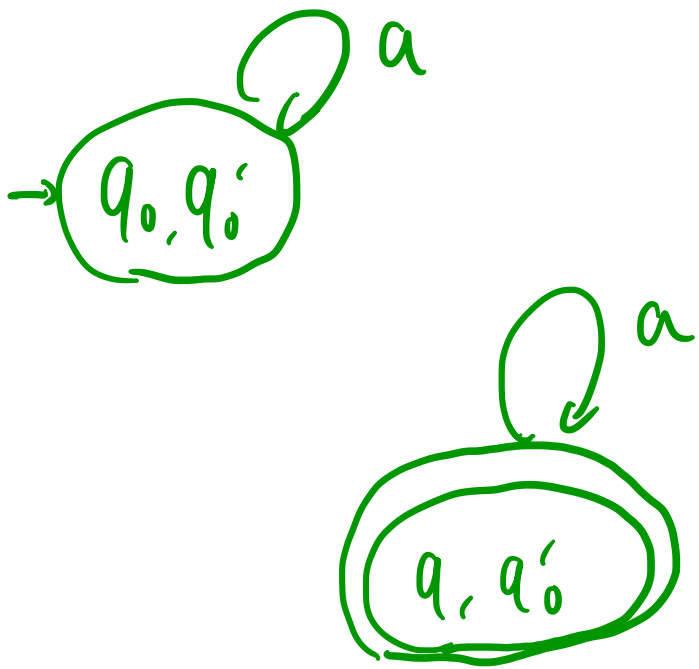
Intersection de langages réguliers

- Soient $A_1 = (Q_1, \Sigma, \delta_1, Q_{0,1}, F_1)$ et $A_2 = (Q_2, \Sigma, \delta_2, Q_{0,2}, F_2)$ deux AFNs
- On peut construite un AFN A tel que $\mathcal{L}(A) = \mathcal{L}(A_1) \cap \mathcal{L}(A_2)$
- **Produit synchronisé d'automates :**
  On considère l'automate $A_1 \otimes A_2 = (Q, \Sigma, \delta, Q_0, F)$ avec :
  - $Q = Q_1 \times Q_2$
  - $Q_0 = Q_{0,1} \times Q_{0,2}$
  - $F = F_1 \times F_2$
  - $(q_1, q_2) \xrightarrow{a} (q_1', q_2')$ si, et seulement si, $q_1 \xrightarrow{a} q_1'$ **et** $q_2 \xrightarrow{a} q_2'$
- On a $\mathcal{L}(A_1 \otimes A_2) = \mathcal{L}(A_1) \cap \mathcal{L}(A_2)$

Exemple



$A_1 \otimes A_2$



$\mathcal{L}(A_1 \otimes A_2) = \emptyset$

Propriétés de sûreté régulières

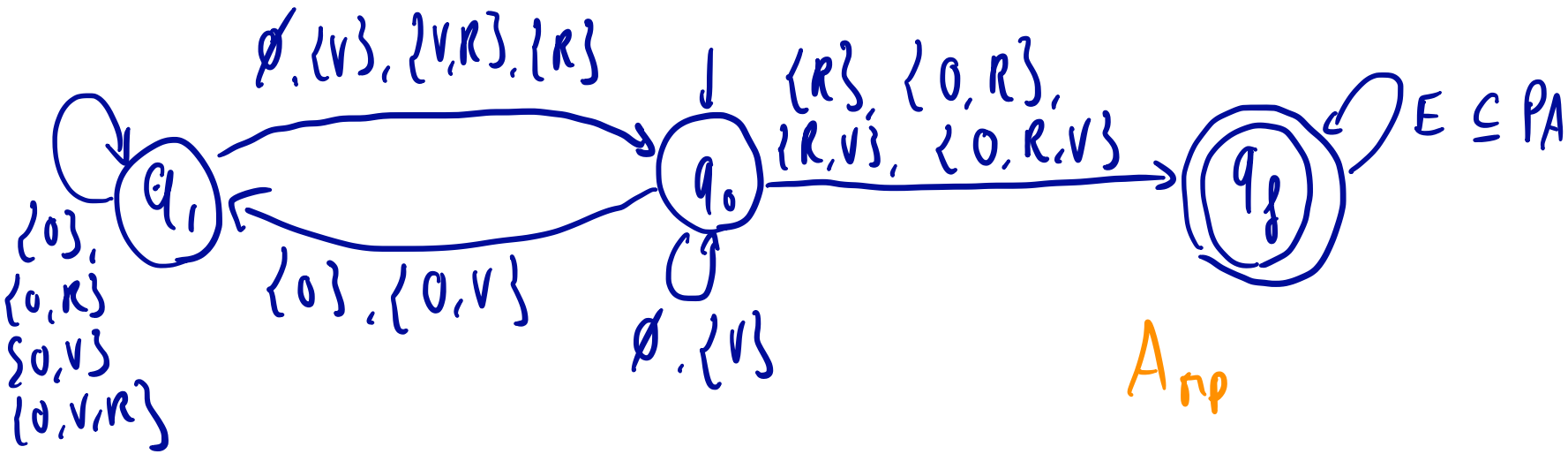
Rappel : une propriété temporelle linéaire P_{safe} sur PA est une propriété de sûreté si pour toute séquence $\sigma \in (2^{PA})^\omega \setminus P$, il existe un préfixe fini $\hat{\sigma}$ de σ tel que :

$$P_{safe} \cap \{\sigma' \in (2^{PA})^\omega \mid \hat{\sigma} \text{ est préfixe de } \sigma'\} = \emptyset$$

- Un tel préfixe $\hat{\sigma}$ est appelé mauvais préfixe.
- Une propriété de sûreté est dite régulière si l'ensemble de ses mauvais préfixes est langage régulier (c'est-à-dire reconnu par un AFN)
- Formellement $\mathit{MauvaisPref}(P_{safe}) = \{\hat{\sigma} \in (2^{PA})^* \mid P_{safe} \cap \{\sigma \in (2^{PA})^\omega \mid \hat{\sigma} \text{ préfixe de } \sigma\} = \emptyset\}$
- Une propriété régulière de sûreté P_{safe} et donc donnée par un AFN A_{MP} tel que $\mathcal{L}(A_{MP}) = \mathit{MauvaisPref}(P_{safe})$
- L'alphabet de A_{MP} est 2^{PA}
- On a alors
  $P_{safe} = \{\sigma \in (2^{PA})^\omega \mid \nexists \hat{\sigma} \text{ préfixe de } \sigma \text{ tel que } \hat{\sigma} \in \mathcal{L}(A_{MP})\}$

Exemple I

- Un feu avec trois couleurs; $PA = \{V, O, R\}$
- $P_{or} = \{A_0 A_1 A_2 \ldots \in (2^{PA})^\omega \mid R \in A_i$ implique $(i > 0$ et $O \in A_{i-1})\}$ est une propriété de sûreté
- $\mathcal{L}(A_{MP})$ correspond aux mots finis sur 2^{PA} où à un moment on a R non précédé par O.



Exemple II

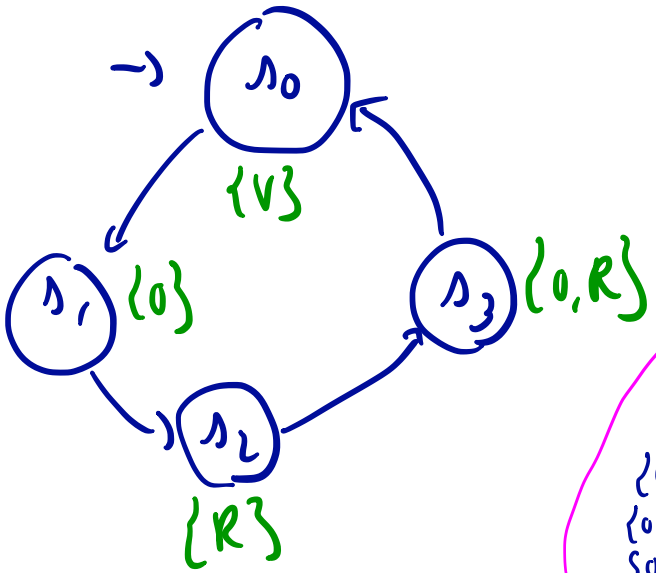
- Un distributeur de boisson qui reçoit des pièces et distribue des boissons; $PA = \{P, B\}$
- Propriété P_{PB} : Le nombre de fois où l'on a vu une boisson (B) et toujours au moins égal au nombre de fois où l'on a vu une pièce (P)
- C'est une propriété de sûreté
- On a $\mathit{MauvaisPref}(P_{PB}) = \{\sigma_0 ... \sigma_n \in (2^{PA})^* \mid \exists k \in \{0, \ldots, n\}. |\{i \mid 0 \leq i \leq k \text{ et } P \in \sigma_i\}| < |\{i \mid 0 \leq i \leq k \text{ et } B \in \sigma_i\}|\}$
- Il n'existe pas d'AFN A tel que $\mathcal{L}(A) = \mathit{MauvaisPref}(P_{PB})$
- P_{PB} n'est pas une propriété de sûreté régulière.

Comment vérifier que $ST \models P_{safe}$?

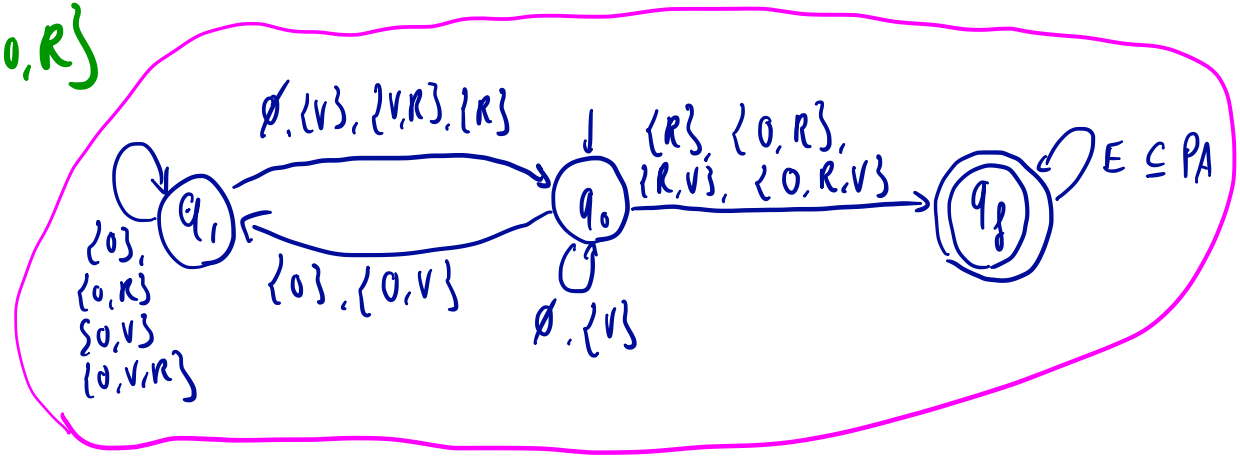
- Soit P_{safe} une propriété de sûreté régulière et A_{MP} l'automate reconnaissant ses mauvais préfixes.
- $ST \models P_{safe}$ si, et seulement si, il n'existe pas $\hat{\sigma} \in \mathcal{L}(A_{MP})$ et $\sigma \in (2^{PA})^{\omega}$ tel que $\hat{\sigma}\sigma \in \mathit{Trace}(ST)$.
- On va chercher l'existence d'un tel préfixe $\hat{\sigma}$.
- Si $ST = (S, \rightarrow, s_{in}, PA, L)$ et $A_{MP} = (Q, \Sigma, \delta, Q_0, F)$, on définit la structure $ST \otimes A_{MP} = (S', \rightarrow', I)$ telle que :
  - $S' = S \times Q$
  - $\rightarrow' \subseteq S' \times S'$ vérifie $(s, q) \rightarrow' (t, p)$ ssi $s \rightarrow t$ et $q \xrightarrow{L(t)} p$
  - $I = \{(s_{in}, q) \mid \exists q_0 \in Q_0 . q_0 \xrightarrow{L(s_{in})} q\}$
- On regarde si il y a un chemin dans $ST \otimes A_{MP}$ depuis un sommet de I vers un sommet (s, q_f) avec $q_f \in F$.
- Si il n'y a pas de tel chemin on a $ST \models P_{safe}$ sinon on a $ST \not\models P_{safe}$

Exemple

ST



P_{safe} : chaque état avec R est précédé d'un état avec O.



$A_{\neg P}$

$ST \otimes A_{\neg P}$