Langages formels : automates finis

Stéphane Le Roux stephane.le_roux@ens-paris-saclay.fr

ENS Paris-Saclay

2023-2024

Automates finis déterministes (AFD)

Un AFD est un tuple $\mathcal{A} = (\Sigma, Q, \delta, i, F)$ où

- Σ est un ensemble non vide et fini, appelé l'alphabet.
- Q est un ensemble non vide et fini, dont les éléments sont les états.
- δ est une fonction totale ou partielle, i.e. $\delta : Q \times \Sigma \to Q$ ou $\delta :\subseteq Q \times \Sigma \to Q$, appelée fonction de transition.
- $i \in Q$ est l'unique état initial.
- $F \subseteq Q$ est l'ensemble des états finaux.

Quand la fonction de transition est totale, on dit que l'AFD est complet.

Remarque

- Quand Σ est fixé, on peut écrire (Q, δ, i, F).
- F peut être vide.
- À isomorphisme prêt (à définir plus tard), pour tout $n \in \mathbb{N}$, il y a un nombre fini d'automates à n états, donc il y a un nombre dénombrable d'automates.
- La notion serait aussi bien définie si Σ et Q pouvaient être infinis, mais on verra que ça aurait moins d'intérêt.

Fonction de transition itérée d'un AFD

Fonction de transition itérée

On étend δ en une application de type $\delta^* : Q \times \Sigma^* \to Q$. Soit $q \in Q$. On définit $\delta^*(q, u)$ par récurrence sur le deuxième argument.

- $\delta^*(q, \epsilon) := q$
- Pour tout $(u, a) \in \Sigma^* \times \Sigma$ tel que $\delta^*(q, u)$ et $\delta(\delta^*(q, u), a)$ sont définis, on pose $\delta^*(q, ua) := \delta(\delta^*(q, u), a)$.

Calcul

Si $\delta^*(q, u) = q'$, on écrit $q \xrightarrow{u} q'$, et on dit que $q \xrightarrow{u_1} \dots \xrightarrow{u_{|u|}} q'$ représente le calcul de $\mathcal{A}$ sur l'entrée $u = u_1 \dots u_{|u|}$.

Remarque

À partir de la semaine prochaine, on s'autorisera parfois à écrire $\delta(q, u)$ au lieu de $\delta^*(q, u)$.

Reconnaissance par AFD

Reconnaissance

- On dit que $\mathcal{A}$ accepte $u \in \Sigma^*$ si $\delta^*(i, u) \in F$. Autrement dit, $\mathcal{A}$ accepte u s'il existe $q' \in F$ tel que $q \xrightarrow{u} q'$.
- Le langage des mots acceptés par $\mathcal{A}$ est défini par $\mathcal{L}(\mathcal{A}) := \{u \in \Sigma^* \mid \delta^*(i, u) \in F\}$.
- On dit qu'un langage $L \subseteq \Sigma^*$ est reconnu par AFD s'il existe un AFD $\mathcal{A}$ tel que $L = \mathcal{L}(\mathcal{A})$.
- On appelle $\mathrm{Rec}_{AFD}(\Sigma^*)$ l'ensemble des langages sur Σ reconnus par AFD.

Lemme

Pour tout AFD, il existe un AFD complet reconnaissant le même langage.

Preuve

Ajout d'un puits.

Reconnaissance par AFD et clôtures

lemme

1. Si $L \subseteq \Sigma^*$ est reconnu par AFD, alors $\Sigma^* \setminus L$ aussi.
2. Si $L_1, L_2 \subseteq \Sigma^*$ sont reconnus par AFD, alors $L_1 \cap L_2$ aussi.
3. Si $L_1, L_2 \subseteq \Sigma^*$ sont reconnus par AFD, alors $L_1 \cup L_2$ aussi.
4. Si $L_1, L_2 \subseteq \Sigma^*$ sont reconnus par AFD, alors $L_1 \setminus L_2$ aussi.

Preuve

1. Prendre $F' := Q \setminus F$ sur un AFD complet.
2. Par l'automate produit $(Q_1 \times Q_2, (\delta_1, \delta_2), (i_1, i_2), F_1 \times F_2)$, où $(\delta_1, \delta_2)(q, a) := (\delta_1(q, a), \delta_2(q, a))$.
3. Deux preuves :
   - Car $L_1 \cup L_2 = \Sigma^* \setminus ((\Sigma^* \setminus L_1) \cap (\Sigma^* \setminus L_2)$
   - En prenant $(\ldots, (F1 \times Q_2) \cup (Q_1 \times F_2))$ dans la construction pour l'intersection.
4. $L_1 \setminus L_2 = L_1 \cap (\Sigma^* \setminus L_2)$. (Ou par produit avec $F' := F_1 \times (Q_2 \setminus F_2)$.)

On verra d'autres propriétés de clôture plus tard.

Propriété de la fonction de transition itérée

Fonction de transition itérée (rappel)

Soit $q \in Q$. On définit $\delta^*(q, u)$ par récurrence sur le deuxième argument.

- $\delta^*(q, \epsilon) := q$
- Pour tout $(u, a) \in \Sigma^* \times \Sigma$ tel que $\delta^*(q, u)$ et $\delta(\delta^*(q, u), a)$ sont définis, on pose $\delta^*(q, ua) := \delta(\delta^*(q, u), a)$.

Lemme

Pour tout $(q, a) \in Q \times \Sigma$ on a $\delta^*(q, a) = \delta(q, a)$.

Preuve

$\delta^*(q, a) = \delta(\delta^*(q, \epsilon), a) = \delta(q, a)$

Propriété de la fonction de transition itérée (II)

Fonction de transition itérée (rappel)

Soit $q \in Q$. On définit $\delta^*(q, u)$ par récurrence sur le deuxième argument.

- $\delta^*(q, \epsilon) := q$
- Pour tout $(u, a) \in \Sigma^* \times \Sigma$ tel que $\delta^*(q, u)$ et $\delta(\delta^*(q, u), a)$ sont définis, on pose $\delta^*(q, ua) := \delta(\delta^*(q, u), a)$.

Lemme

Pour tout $(q, u, v) \in Q \times \Sigma^* \times \Sigma^*$ on a $\delta^*(q, uv) = \delta^*(\delta^*(q, u), v)$.

Preuve

Soit $(q, u) \in Q \times \Sigma^*$. Montrons $\forall v \in \Sigma^*, \delta(q, uv) = \delta(\delta(q, u), v)$ par récurrence sur v.

- $\delta(q, u\epsilon) = \delta(q, u) = \delta(\delta(q, u), \epsilon)$
- $\delta(q, u(va)) = \delta(q, (uv)a) \overset{def}{=} \delta(\delta(q, uv), a) \overset{HR}{=} \delta(\delta(\delta(q, u), v), a) \overset{def}{=} \delta(\delta(q, u), va)$

Propriété de la fonction de transition itérée (III)

Fonction de transition itérée (rappel)

Soit $q \in Q$. On définit $\delta^*(q, u)$ par récurrence sur le deuxième argument.

- $\delta^*(q, \epsilon) := q$
- Pour tout $(u, a) \in \Sigma^* \times \Sigma$ tel que $\delta^*(q, u)$ et $\delta(\delta^*(q, u), a)$ sont définis, on pose $\delta^*(q, ua) := \delta(\delta^*(q, u), a)$.

Lemme (rappel)

Pour tout $(q, u, v) \in Q \times \Sigma^* \times \Sigma^*$ on a $\delta^*(q, uv) = \delta^*(\delta^*(q, u), v)$.

Corollaire

Pour tout $(q, a, u) \in Q \times \Sigma \times \Sigma^*$ on a $\delta^*(q, au) = \delta^*(\delta(q, a), u)$.

- On aurait pu le prouver directement par récurrence (à droite) sur u.
- Peut-on définir δ^* par récurrence gauche ? Cf prochaine diapo.

Alternative à la fonction de transition itérée

Fonction de transition itérée (rappel)

Soit $q \in Q$. On définit $\delta^*(q, u)$ par récurrence sur le deuxième argument.

- $\delta^*(q, \epsilon) := q$
- Pour tout $(u, a) \in \Sigma^* \times \Sigma$ tel que $\delta^*(q, u)$ et $\delta(\delta^*(q, u), a)$ sont définis, on pose $\delta^*(q, ua) := \delta(\delta^*(q, u), a)$.

Alternative similaire, par récurrence gauche

On définit $\delta'(q, u)$ par récurrence sur le deuxième argument.

- $\forall q \in Q, \delta'(q, \epsilon) := q$
- Pour tout $(q, a, u) \in Q \times \Sigma \times \Sigma^*$ tel que $\delta(q, a)$ et $\delta'(\delta(q, a), u)$ sont définis,on pose $\delta'(q, au) := \delta'(\delta(q, a), u)$.

Alternative à la fonction de transition itérée (II)

Alternative similaire, par récurrence gauche

On définit $\delta'(q, u)$ par récurrence sur le deuxième argument.

- $\forall q \in Q, \delta'(q, \epsilon) := q$
- Pour tout $(q, a, u) \in Q \times \Sigma \times \Sigma^*$ tel que $\delta(q, a)$ et $\delta'(\delta(q, a), u)$ sont définis, on pose $\delta'(q, au) := \delta'(\delta(q, a), u)$.

Lemme

$\forall u \in \Sigma^*, \forall q \in Q, \delta^*(q, u) = \delta'(q, u)$.

Preuve

Par récurrence à gauche sur u.

- Pour tout $q \in Q$, on a $\delta^*(q, \epsilon) = q = \delta'(q, \epsilon)$ par définition.
- Soit $(a, u) \in \Sigma \times \Sigma^*$. Pour tout $q \in Q$, on a
  $\delta^*(q, au) \overset{cor}{=} \delta^*(\delta(q, a), u) \overset{HR}{=} \delta'(\delta(q, a), u) \overset{def}{=} \delta'(q, au)$

Alternative à la fonction de transition itérée (III)

Alternative similaire, par récurrence gauche (rappel)

On définit $\delta'(q, u)$ par récurrence sur le deuxième argument.

- $\forall q \in Q, \delta'(q, \epsilon) := q$
- Pour tout $(q, a, u) \in Q \times \Sigma \times \Sigma^*$ tel que $\delta(q, a)$ et $\delta'(\delta(q, a), u)$ sont définis, on pose $\delta'(q, au) := \delta'(\delta(q, a), u)$.

Lemme (pour raisons pédagogiques)

Pour tout $(q, u, v) \in Q \times \Sigma^* \times \Sigma^*$ on a $\delta'(q, uv) = \delta'(\delta'(q, u), v)$.

Preuve (pour raisons pédagogiques)

Soit $v \in \Sigma^*$. Montrons $\forall u \in \Sigma^* \forall q \in Q, \delta'(q, uv) = \delta'(\delta'(q, u), v)$ par récurrence sur u.

- Pour tout $q \in Q$ on a $\delta'(q, \epsilon v) = \delta'(q, v) = \delta'(\delta'(q, \epsilon), v)$
- Pour tout $q \in Q$ on a $\delta'(q, (au)v) = \delta'(q, a(uv)) \overset{def}{=} \delta'(\delta(q, a), uv) \overset{HR}{=} \delta'(\delta'(\delta(q, a), u), v) \overset{def}{=} \delta'(\delta'(q, au), v)$

Reconnaissance d'un mot par un AFD (alternative)

Définition

La fonction Accept attend un automate et un mot en arguments. Elle renvoie vrai si l'automate accepte le mot, et faux sinon. Elle est définie par récurrence à droite sur le mot.

- Si $i \in F$ on pose $\mathrm{Accept}(\mathcal{A}, \epsilon) := \top$, sinon $\mathrm{Accept}(\mathcal{A}, \epsilon) := \bot$.
- Pour tout $(a, u) \in \Sigma \times \Sigma^*$ tel que $\delta(i, a)$ est défini, on pose $\mathrm{Accept}(\mathcal{A}, au) := \mathrm{Accept}(\mathcal{A}[i \leftarrow \delta(i, a)], u)$.

Lemme

Pour tout $u \in \Sigma^*$, pour tout $\mathcal{A}$, on a $\mathrm{Accept}(\mathcal{A}, u)$ ssi $\delta^*(i, u) \in F$.

Preuve

Par récurrence sur u.

- $\mathrm{Accept}(\mathcal{A}, \epsilon) = \top$ ssi $i \in F$ ssi $\delta^*(i, \epsilon) \in F$
- $\mathrm{Accept}(\mathcal{A}, au) = \top$ ssi $\mathrm{Accept}(\mathcal{A}[i \leftarrow \delta(i, a)], u)) = \top$ ssi (HR) $\delta^*(\delta(i, a), u) \in F$ ssi (cor) $\delta^*(i, au) \in F$.

Automates finis non-déterministes (AFN)

Un AFN est un tuple $\mathcal{A} = (\Sigma, Q, \Delta, I, F)$ où

- Σ est un ensemble non vide et fini, appelé l'alphabet.
- Q est un ensemble non vide et fini, dont les éléments sont les états.
- $\Delta \subseteq Q \times \Sigma \times Q$ est une relation, appelée relation de transition.
- $I \subseteq Q$ est l'ensemble des états initiaux.
- $F \subseteq Q$ est l'ensemble des états finaux.

- I peut être vide.
- La notion de complétude est moins intéressante pour les AFN.

Transitions non-déterministes itérées et calcul

Transitions non-déterministes itérées

- On pose $q \xrightarrow{a} q'$ si $(q, a, q') \in \Delta$.
- On pose $q \xrightarrow{\epsilon} q$.
- Si $q \xrightarrow{u} q'$ et $q' \xrightarrow{a} q''$, alors on pose $q \xrightarrow{ua} q''$.

Lemme

Pour tout $u, v \in \Sigma^*$ on a $\xrightarrow{uv} = \xrightarrow{u}\xrightarrow{v}$. (Par récurrence à droite sur v.)

- On aurait pu définir "Si $q \xrightarrow{a} q'$ et $q' \xrightarrow{u} q''$, alors $q \xrightarrow{au} q'''$", et la preuve ci-dessous aurait été par récurrence à gauche sur u.
- Les AFN présentent une symétrie forte, contrairement aux AFD.

Calcul

Si $q \xrightarrow{u} q'$, on dit que $q \xrightarrow{u_1} \dots \xrightarrow{u_{|u|}} q'$ représente un calcul possible de $\mathcal{A}$ sur l'entrée $u = u_1 \dots u_{|u|}$.

Transitions étendues aux parties

Transitions étendues aux parties

Pour tout $S, S' \subseteq Q$, on pose $S \xrightarrow{u} S'$ s'il existe $(q, q') \in S \times S'$ tel que $q \xrightarrow{u} q'$.

Lemme

Pour tout $u, v \in \Sigma^*$ on a $\xrightarrow{uv} = \xrightarrow{u}\xrightarrow{v}$, aussi pour l'extension aux parties.

Reconnaissance par AFN

Reconnaissance

- On dit que $\mathcal{A}$ accepte $u \in \Sigma^*$ si $I \xrightarrow{u} F$. (Comparer avec $\delta^*(i, u) \in F$.) Autrement dit, $\mathcal{A}$ accepte u s'il existe $(i, f) \in I \times F$ tel que $i \xrightarrow{u} f$.
- Le langage des mots acceptés par $\mathcal{A}$ est défini par $\mathcal{L}(\mathcal{A}) := \{u \in \Sigma^* \mid I \xrightarrow{u} F\}$.
- On dit qu'un langage $L \subseteq \Sigma^*$ est reconnu par AFN s'il existe un AFN $\mathcal{A}$ tel que $L = \mathcal{L}(\mathcal{A})$.
- On appelle $\mathrm{Rec}_{AFN}(\Sigma^*)$ l'ensemble des langages sur Σ reconnus par AFN.

Transitions non-déterministes itérées "fonctionnelles"

Transitions non-déterministes itérées "fonctionnelles"

- Pour $S \subseteq Q$ et $u \in \Sigma^*$ on pose $(S \xrightarrow{u}) := \{q \in Q \mid \exists q' \in S, q' \xrightarrow{u} q\}$.
  De même $(\xrightarrow{u} S) := \{q \in Q \mid \exists q' \in S, q \xrightarrow{u} q'\}$.

Lemme

- $(S \xrightarrow{\epsilon}) = S$ et $(\xrightarrow{\epsilon} S) = S$.
- $(S \xrightarrow{uv}) = ((S \xrightarrow{u}) \xrightarrow{v})$, noté $S \xrightarrow{u}\xrightarrow{v}$,
  et $(\xrightarrow{uv} S) = (\xrightarrow{u}\xrightarrow{v} S)$.
- $S \xrightarrow{u} S'$ ssi $(S \xrightarrow{u}) \cap S' \neq \emptyset$ ssi $S \cap (\xrightarrow{u} S') \neq \emptyset$.

Reconnaissance par AFN (alternative)

- $\mathrm{Accept}(\mathcal{A}, \epsilon) = \top$ si $I \cap F \neq \emptyset$, et sinon $\mathrm{Accept}(\mathcal{A}, \epsilon) = \bot$
- $\mathrm{Accept}(\mathcal{A}, au) := \mathrm{Accept}(\mathcal{A}[I := (I \xrightarrow{a})], u)$
- ou bien $\mathrm{Accept}(\mathcal{A}, ua) := \mathrm{Accept}(\mathcal{A}[F := (\xrightarrow{a} F)], u)$

Lemme

$\mathrm{Accept}(\mathcal{A}, u)$ ssi $I \xrightarrow{u} F$ ssi $(I \xrightarrow{u}) \cap F \neq \emptyset$ ssi $I \cap \xrightarrow{u} F \neq \emptyset$

Liens entre AFD et AFN

Lemme

$\mathrm{Rec}_{AFD}(\Sigma^*) \subseteq \mathrm{Rec}_{AFN}(\Sigma^*)$

Preuve

Soit $\mathcal{A} = (Q, \delta, i, F)$ un AFD. Soit $\mathcal{B} := (Q, \Delta, \{i\}, F)$ un AFN tel que $(q, a, q') \in \Delta$ ssi $q' = \delta(q, a)$. Mq $\mathcal{L}(\mathcal{A}) = \mathcal{L}(\mathcal{B})$. Pour cela montrons que pour tout $u \in \Sigma^*$, on a $(\{i\} \xrightarrow{u}_{\mathcal{B}}) = \{\delta^*(i, u)\}$.

- $(\{i\} \xrightarrow{\epsilon}_{\mathcal{B}}) = \{i\} = \{\delta^*(i, \epsilon)\}$
- $(\{i\} \xrightarrow{ua}_{\mathcal{B}}) = ((\{i\} \xrightarrow{u}_{\mathcal{B}}) \xrightarrow{a}_{\mathcal{B}}) = (\{\delta^*(i, u)\} \xrightarrow{a}_{\mathcal{B}}) = \{\delta(\delta^*(i, u), a)\} = \{\delta^*(i, ua)\}$

Ainsi $(\{i\} \xrightarrow{u}_{\mathcal{B}}) \cap F \neq \emptyset$ ssi $\delta^*(i, u) \in F$.

Liens entre AFD et AFN : automate des parties

Lemme

$\mathrm{Rec}_{AFN}(\Sigma^*) \subseteq \mathrm{Rec}_{AFD}(\Sigma^*)$

Preuve

Soit $\mathcal{A} = (Q, \Delta, I, F)$ un AFN. Soit $\mathcal{B} := (\mathcal{P}(Q), \delta, I, F')$ un AFD où $F' := \{S \subseteq Q \mid S \cap F \neq \emptyset\}$ et $\delta(S, a) := (S \xrightarrow{a})$.
Montrons par récurrence sur $u \in \Sigma^*$ que $\delta^*(S, u) = (S \xrightarrow{u})$.

- $\delta^*(S, \epsilon) = S = (S \xrightarrow{\epsilon})$.
- $\delta^*(S, ua) = \delta(\delta^*(S, u), a) = \delta(S \xrightarrow{u}, a) = ((S \xrightarrow{u}) \xrightarrow{a}) = (S \xrightarrow{ua})$.

Ainsi, pour tout $u \in \Sigma^*$ on a $\delta(I, u) \in F'$ ssi $(I \xrightarrow{u}) \in F'$ ssi $(I \xrightarrow{u}) \cap F \neq \emptyset$ ssi $I \xrightarrow{u} F$.

Théorème

$\mathrm{Rec}_{AFN}(\Sigma^*) = \mathrm{Rec}_{AFD}(\Sigma^*)$

On note $\mathrm{Rec}(\Sigma^*) := \mathrm{Rec}_{AFD}(\Sigma^*)$.

Clôture par miroir

Automate miroir

Soit un AFN $\mathcal{A} = (Q, \Delta, I, F)$. Son automate miroir est $\overline{\mathcal{A}} := (Q, \overline{\Delta}, F, I)$, où $(q, a, q') \in \overline{\Delta}$ ssi $(q', a, q) \in \Delta$.

Lemme

$\mathcal{L}(\overline{A}) = \overline{\mathcal{L}(\mathcal{A})}$.

Preuve

On note que $q \xrightarrow{a}_{\overline{\mathcal{A}}} q'$ ssi $q' \xrightarrow{a}_{\mathcal{A}} q$, donc $q \xrightarrow{u}_{\overline{\mathcal{A}}} q'$ ssi $q' \xrightarrow{\overline{u}}_{\mathcal{A}} q$, donc $F \xrightarrow{u}_{\overline{\mathcal{A}}} I$ ssi $I \xrightarrow{\overline{u}}_{\mathcal{A}} F$, donc $\mathcal{B}$ accepte u ssi $\mathcal{A}$ accepte $\overline{u}$.

Clôture par union, preuve par non-déterminisme

Lemme (rappel)

Si $L_1, L_2 \subseteq \Sigma^*$ sont reconnus par AFD, alors $L_1 \cup L_2$ aussi.

Preuve alternative

Soient deux ANF $\mathcal{A}_1$ et $\mathcal{A}_2$ tels que $\mathcal{L}(\mathcal{A}_1) = L_1$ et $\mathcal{L}(\mathcal{A}_2) = L_2$. Soit $\mathcal{A} := \mathcal{A}_1 \sqcup \mathcal{A}_2 = (Q_1 \sqcup A_2, \Delta_1 \sqcup \Delta_2, I_1 \sqcup I_2, F_1 \sqcup F_2)$ (union disjointe).

- Le non-déterminisme n'aide pas à faire l'intersection : il faut aussi faire le produit.
- Pour le complémentaire, il faut déterminiser.

Complexité algorithmique

Problème du mot avec AFD

- Entrée : un AFD $\mathcal{A} = (Q, \delta, i, F)$ et $u \in \Sigma^*$
- Sortie : Oui si $u \in \mathcal{L}(\mathcal{A})$

Lemme

Ce problème est dans $\mathrm{LOGSPACE}$.

Preuve

On lit les lettres une par une et on passe dans les états correspondants, puis on regarde si le dernier état est acceptant.

Complexité algorithmique (II)

Problème du mot avec AFN

- Entrée : un AFN $\mathcal{A} = (Q, \Delta, I, F)$ et $u \in \Sigma^*$
- Sortie : Oui si $u \in \mathcal{L}(\mathcal{A})$

Lemme

Il existe un algorithme résolvant ce problème en temps $O(|u| \cdot |Q^2|)$ et en espace $O(|Q|)$.

Preuve : on simule le déterminé de $\mathcal{A}$ à la volée, i.e. à chaque lecture d'une nouvelle lettre on met a jour un ensemble d'états.

Lemme

Ce problème est dans $\mathrm{NLOGSPACE}$.

Preuve : on devine un chemin de longueur $|u|$ à la volée en ne stockant qu'un état.

Complexité algorithmique (III)

Graphe sous-jacent d'un automate

Soit un AFN $\mathcal{A} = (Q, \Delta, I, F)$. Son graphe sous-jacent est $(Q, \rightarrow)$ où $q \rightarrow q'$ si $\exists a \in \Sigma, q \xrightarrow{a} q'$. (On pourrait écrire $q \xrightarrow{\Sigma}$ q') Concept et notation similaires pour les AFD.

Problème de l'AFN vide

- Entrée : un AFN $\mathcal{A} = (Q, \Delta, I, F)$
- Sortie : Oui si $\mathcal{L}(\mathcal{A})$ vide

Lemme

Ce problème est dans $\mathrm{NLOGSPACE}$.

Preuve

C'est de l'atteignabilité dans le graphe sous-jacent : s'il existe un chemin de I à F, il en existe un de longueur au plus $|Q|$. On devine un tel chemin la volée. La version ADF ne donne a priori rien de mieux.

Complexité algorithmique (IV)

Problème de l'inclusion de langages d'AFD

- Entrée : Deux AFD $\mathcal{A}_1$ et $\mathcal{A}_2$
- Sortie : Oui si $\mathcal{L}(\mathcal{A}_1) \subseteq \mathcal{L}(\mathcal{A}_2)$

Lemme

Ce problème est dans $\mathrm{NLOGSPACE}$.

Preuve

On devine à la volée un mot de longueurs au plus $|Q_1 \times Q_2|$. On regarde s'il est dans $\mathcal{L}(\mathcal{A}_1)$ mais pas dans $\mathcal{L}(\mathcal{A}_2)$. Enfin on invoque que $\mathrm{NLOGSPACE} = \mathrm{coNLOGSPACE}$.

Complexité algorithmique (V)

Problème de l'universalité d'un AFN

- Entrée : un AFN $\mathcal{A} = (\Sigma, Q, \Delta, I, F)$
- Sortie : Oui si $\mathcal{L}(\mathcal{A}) = \Sigma^*$

Lemme

Ce problème est PSPACE-complet.

Problème de l'inclusion de langages d'AFN

- Entrée : Deux AFN $\mathcal{A}_1$ et $\mathcal{A}_2$
- Sortie : Oui si $\mathcal{L}(\mathcal{A}_1) \subseteq \mathcal{L}(\mathcal{A}_2)$

Lemme

Ce problème est PSPACE-complet.

Automate avec ϵ-transitions

Un AFN avec ϵ-transitions est un tuple $\mathcal{A} = (\Sigma, Q, \Delta, I, F)$ généralisant la notion de AFN : on a maintenant $\Delta \subseteq Q \times (\Sigma \cup \{\epsilon\}) \times Q$.

On pose $q \xrightarrow{a} q'$ si $(q, a, q') \in \Delta$ et $q \xrightarrow{\epsilon} q'$ si $(q, \epsilon, q') \in \Delta$.

$$\frac{}{q \overset{\epsilon}{\twoheadrightarrow} q} \qquad \frac{q \xrightarrow{\epsilon} q'}{q \overset{\epsilon}{\twoheadrightarrow} q'} \qquad \frac{q \xrightarrow{a} q'}{q \overset{a}{\twoheadrightarrow} q'} \qquad \frac{q \xrightarrow{\epsilon} q' \quad q' \overset{a}{\twoheadrightarrow} q''}{q \overset{a}{\twoheadrightarrow} q''}$$

$$\frac{q \overset{u}{\twoheadrightarrow} q' \quad q' \xrightarrow{\epsilon} q''}{q \overset{u}{\twoheadrightarrow} q''} \qquad \frac{q \overset{u}{\twoheadrightarrow} q' \quad q' \xrightarrow{a} q''}{q \overset{ua}{\twoheadrightarrow} q''}$$

Lemme

1. $\overset{\epsilon}{\twoheadrightarrow} = (\xrightarrow{\epsilon})^*$
2. $\overset{a}{\twoheadrightarrow} = (\xrightarrow{\epsilon})^* \xrightarrow{a} (\xrightarrow{\epsilon})^*$
3. $\overset{uv}{\twoheadrightarrow} = \overset{u}{\twoheadrightarrow} \overset{v}{\twoheadrightarrow}$.

Transitions étendues aux parties

Transitions étendues aux parties (comme pour les AFN)

Pour tout $S, S' \subseteq Q$, on pose $S \overset{u}{\twoheadrightarrow} S'$ s'il existe $(q, q') \in S \times S'$ tel que $q \overset{u}{\twoheadrightarrow} q'$.

Lemme (étendu aux parties)

1. $\overset{\epsilon}{\twoheadrightarrow} = (\overset{\epsilon}{\rightarrow})^*$
2. $\overset{a}{\twoheadrightarrow} = (\overset{\epsilon}{\rightarrow})^* \overset{a}{\rightarrow} (\overset{\epsilon}{\rightarrow})^*$
3. $\overset{uv}{\twoheadrightarrow} = \overset{u}{\twoheadrightarrow} \overset{v}{\twoheadrightarrow}$.

Reconnaissance par ϵ-AFN et calcul

Reconnaissance (comme pour les AFN)

- On dit que $\mathcal{A}$ accepte $u \in \Sigma^*$ si $I \overset{u}{\twoheadrightarrow} F$. Autrement dit, $\mathcal{A}$ accepte u s'il existe $(i, f) \in I \times F$ tel que $i \overset{u}{\twoheadrightarrow} f$.
- ...
- ...
- On appelle $\mathrm{Rec}_\epsilon(\Sigma^*)$ l'ensemble des langages sur Σ reconnus par ϵ-AFN.

- Les AFN avec ϵ-transitions présentent la même symétrie forte que les AFN.
- Tout chemin $q \overset{u_1}{\to} \dots q_i \overset{\epsilon}{\to} q_{i+1} \dots \overset{u_{|u|}}{\to} q'$ représente un calcul possible de $\mathcal{A}$ sur l'entrée $u = u_1 \dots u_{|u|}$.

Transitions non-déterministes itérées "fonctionnelles"

Transitions non-déterministes itérées "fonctionnelles"

- Pour $S \subseteq Q$ et $u \in \Sigma^*$ on pose $(S \overset{u}{\twoheadrightarrow}) := \{q \in Q \mid \exists q' \in S, q' \overset{u}{\twoheadrightarrow} q\}$.
  De même $(\overset{u}{\twoheadrightarrow} S) := \ldots$.

Lemme

- Seulement inclusions : $S \subseteq (S \overset{\epsilon}{\twoheadrightarrow})$ et $S \subseteq (\overset{\epsilon}{\twoheadrightarrow} S)$.
- $(S \overset{uv}{\twoheadrightarrow}) = ((S \overset{u}{\twoheadrightarrow}) \overset{v}{\twoheadrightarrow})$, noté $S \overset{u}{\twoheadrightarrow}\overset{v}{\twoheadrightarrow}$,
  et $(\overset{uv}{\twoheadrightarrow} S) = (\overset{u}{\twoheadrightarrow}\overset{v}{\twoheadrightarrow} S)$.
- $S \overset{u}{\twoheadrightarrow} S'$ ssi $(S \overset{u}{\twoheadrightarrow}) \cap S' \neq \emptyset$ ssi $S \cap (\overset{u}{\twoheadrightarrow} S') \neq \emptyset$.

Liens entre AFD et ϵ-AFN : automate des parties

Lemme

$\mathrm{Rec}(\Sigma^*) \subseteq \mathrm{Rec}_\epsilon(\Sigma^*)$

Preuve : dans un AFN, $\overset{a}{\to} = \overset{a}{\twoheadrightarrow}$ et $\overset{\epsilon}{\to} = \overset{\epsilon}{\twoheadrightarrow}$.

Lemme

$\mathrm{Rec}_\epsilon(\Sigma^*) \subseteq \mathrm{Rec}(\Sigma^*)$

Preuve : comme $\mathrm{Rec}_{AFN}(\Sigma^*) \subseteq \mathrm{Rec}_{AFD}(\Sigma^*)$, en remplaçant $\to$ par $\twoheadrightarrow$.

Théorème

$\mathrm{Rec}_\epsilon(\Sigma^*) = \mathrm{Rec}(\Sigma^*)$

Clôture par concaténation

Lemme

Si $L_1, L_2 \in \mathrm{Rec}(\Sigma^*)$, alors $L_1 \cdot L_2 \in \mathrm{Rec}(\Sigma^*)$

Preuve

Juxtaposer $\mathcal{A}_1$ et $\mathcal{A}_2$. Ajouter des ϵ-transitions des $q \in F_1$ aux $q' \in I_2$, et prendre F_2 comme états finaux.

Preuve pour les AFN

1. Si $\epsilon \notin L_1$, pour chaque $q \xrightarrow{a} F_1$ ajouter $q \xrightarrow{a} i_2$ pour tout $i_2 \in I_2$, et prendre I_1 comme états initiaux et F_2 comme états finaux.
2. Si $\epsilon \notin L_2$, pour chaque $i_2 \xrightarrow{a} q$ ajouter $f_1 \xrightarrow{a} q$ pour tout $f_1 \in F_1$, et prendre I_1 comme états initiaux et prendre F_2 comme états finaux. C'est la construction ci-dessus pour l'automate miroir.
3. Si $\epsilon \in L_1 \cap L_2$, ajouter F_1' des copies vraiment finales de F_1 et ajouter I_2' des copies vraiment initiales de I_2.

Clôture par itération

Lemme

Si $L \in \mathrm{Rec}(\Sigma^*)$, alors $L^* \in \mathrm{Rec}(\Sigma^*)$

Preuve

Ajouter un nouveau et unique état initial et final q_ϵ. Ajouter des ϵ-transitions de q_ϵ vers tous les $i \in I$ et depuis tous les $f \in F$.

Preuve pour les AFN

Ajouter des ϵ-transitions de chaque $f \in F$ vers chaque $i \in I$. Si $\epsilon \notin L$, ajouter un état q_ϵ initial et final, sans transition entrante ni sortante.

Automate accessible, co-accessible, émondés

Soit un AFN $\mathcal{A} = (Q, \Delta, I, F)$. (Ça vaut aussi pour les ϵ-AFN.)

- Soit $Q' := I \overset{\Sigma^*}{\to}$. I.e. $q \in Q'$ ssi $\exists i \in I, i \to^* q$. On appelle $\mathrm{Access}(\mathcal{A}) := (Q', \Delta_{Q'}, I, F \cap Q')$ la restriction accessible de $\mathcal{A}$. On dit que $\mathcal{A}$ est accessible si $Q' = Q$.
- Soit $Q' := \overset{\Sigma^*}{\to} F$. I.e. $q \in Q'$ ssi $\exists f \in F, f \to^* q$. On appelle $\mathrm{CoAcc}(\mathcal{A}) := (Q', \Delta_{Q'}, I \cap Q', F)$ la restriction co-accessible de $\mathcal{A}$. On dit que $\mathcal{A}$ est co-accessible si $Q' = Q$.
- On appelle $\mathrm{CoAcc}(\mathrm{Access}(\mathcal{A}))$ la restriction émondée de $\mathcal{A}$. On dit que $\mathcal{A}$ est emondé s'il est accessible et co-accessible.

Lemme

- $\mathcal{L}(\mathrm{Access}(\mathcal{A})) = \mathcal{L}(\mathcal{A})$
- $\mathcal{L}(\mathrm{CoAcc}(\mathcal{A})) = \mathcal{L}(\mathcal{A})$
- $\mathrm{CoAcc}(\mathcal{A}) = \overline{\mathrm{Access}(\overline{\mathcal{A}})}$
- $\mathrm{CoAcc}(\mathrm{Access}(\mathcal{A})) = \mathrm{Access}(\mathrm{CoAcc}(\mathcal{A}))$

Clôture par préfixe, suffixe, facteur, sous-mot

Soit $L \subseteq \Sigma^*$.

- $\mathrm{Pref}(L) := \{u \in \Sigma^* \mid \exists v \in \Sigma^*, uv \in L\}$
- $\mathrm{Suff}(L) := \{u \in \Sigma^* \mid \exists v \in \Sigma^*, vu \in L\}$
- $\mathrm{Fact}(L) := \{u \in \Sigma^* \mid \exists v \in \Sigma^*, uv \in L\}$
- $\mathrm{SousMot}(L) := \{u \in \Sigma^* \mid \exists v \in L, \mathrm{sousmot}(u, v)\}$

Lemme

Si $L \in \mathrm{Rec}(\Sigma^*)$ alors $\mathrm{Pref}(L), \mathrm{Suff}(L), \mathrm{Fact}(L), \mathrm{SousMot}(L) \in \mathrm{Rec}(\Sigma^*)$

Preuve

- Soit un AFN $\mathcal{A}$ co-accessible tel que $L = \mathcal{L}(\mathcal{A})$. On pose $F' := Q$
- Soit un AFN $\mathcal{A}$ accessible tel que $L = \mathcal{L}(\mathcal{A})$. On pose $I' := Q$. (S'obtient aussi par dualité/miroir.)
- Soit un AFN $\mathcal{A}$ émondé tel que $L = \mathcal{L}(\mathcal{A})$. On pose $I' := F' := Q$
- À toute transition $q \xrightarrow{a} q'$ on ajoute $q \xrightarrow{\epsilon} q'$

Clôture par "quotient"

Lemme

Si $L \in \mathrm{Rec}(\Sigma^*)$ alors $K^{-1}L, LK^{-1} \in \mathrm{Rec}(\Sigma^*)$

Preuve : pour $K^{-1}L = \{u \in \Sigma^* \mid \exists v \in K, vu \in L\} \subseteq \mathrm{Suff}(L)$, soit $I' := (I \xrightarrow{K})$. Pour LK^{-1} on utilise la dualité.

Lemme

La fonction suivante est calculable

- Entrée : deux AFN $\mathcal{A}, \mathcal{B}$
- Sortie : un AFN $\mathcal{A}'$ tel que $\mathcal{L}(\mathcal{A}') = \mathcal{L}(\mathcal{B})^{-1}\mathcal{L}(\mathcal{A})$.

Preuve : La difficulté restante est de calculer $I(\mathcal{A}') := (I(\mathcal{A}) \xrightarrow{\mathcal{L}(B)})$. Pour chaque $(i_\mathcal{A}, i_\mathcal{B}, q, f_\mathcal{B}) \in I_\mathcal{A} \times I_\mathcal{B} \times Q_\mathcal{A} \times F_\mathcal{B}$ et $f \in F_\mathcal{B}$ et , s'il existe $u \in \Sigma^*$ tel que $i_\mathcal{A} \xrightarrow{u}_\mathcal{A} q$ et $i_\mathcal{B} \xrightarrow{u}_\mathcal{B} f_\mathcal{B}$, alors il en existe un de longueur au plus $|Q_\mathcal{A} \times Q_\mathcal{B}|$.

Clôture par pré-image de morphisme

Lemme

Soit $L \in \mathrm{Rec}(B^*)$ et $f : A^* \to B^*$ un morphisme de monoïdes. Alors $f^{-1}[L] \in \mathrm{Rec}(A^*)$

Preuve

Soit $\mathcal{B} = (Q, I, \Delta_{\mathcal{B}}, F)$ un AFN tel que $\mathcal{L}(\mathcal{B}) = L$. On construit $\mathcal{A} = (Q, I, \Delta_{\mathcal{A}}, F)$. Pour chaque transition $q \xrightarrow{f(a)}_{\mathcal{B}} q'$, on pose $q \xrightarrow{a}_{\mathcal{A}} q'$.

Mq $\forall u \in \Sigma^* \forall q, q' \in Q, q \xrightarrow{f(u)}_{\mathcal{B}} q' \Leftrightarrow q \xrightarrow{u}_{\mathcal{A}} q'$. Par récurrence sur u.

- $q \xrightarrow{f(\epsilon)}_{\mathcal{B}} q'$ ssi $q \xrightarrow{\epsilon}_{\mathcal{B}} q'$ ssi $q = q'$ ssi $q \xrightarrow{\epsilon}_{\mathcal{A}} q'$.
- $q \xrightarrow{f(ua)}_{\mathcal{B}} q'$ ssi $\exists q'' \in Q, q \xrightarrow{f(u)}_{\mathcal{B}} q'' \xrightarrow{f(a)}_{\mathcal{B}} q'$ ssi $\exists q'' \in Q, q \xrightarrow{u}_{\mathcal{A}} q'' \xrightarrow{a}_{\mathcal{A}} q'$ ssi $q \xrightarrow{ua}_{\mathcal{A}} q'$.

Ainsi, $I \xrightarrow{f(u)}_{\mathcal{B}} F$ ssi $I \xrightarrow{u}_{\mathcal{A}} F$, donc $f(u) \in \mathcal{L}(\mathcal{B}) = L$ ssi $u \in \mathcal{L}(\mathcal{A})$, i.e. $\mathcal{L}(\mathcal{A}) = f^{-1}[L]$.

Clôture par morphisme

Lemme

Soit $L \in \mathrm{Rec}(A^*)$ et $f : A^* \to B^*$ un morphisme de monoïdes. Alors $f[L] \in \mathrm{Rec}(B^*)$

Preuve

Soit $\mathcal{A} = (Q, I, \Delta, F)$ un AFN tel que $\mathcal{L}(\mathcal{A}) = L$. Chaque transition $q \xrightarrow{a}_{\mathcal{A}} q'$ est remplacée par une chaîne de transitions $q \xrightarrow{f(a)} q'$ (avec de nouveaux états si $|f(a)| > 1$ et une ϵ-transition si $f(a) = \epsilon$.) Soit $\mathcal{B}$ ce nouvel ϵ-AFN.

- Pour tout $u \in \mathcal{L}(A)$, on a $f(u) \in \mathcal{L}(\mathcal{B})$ en suivant le chemin transformé.
- Pour tout $v \in \mathcal{L}(\mathcal{B})$, on peut récupérer les états et transitions d'origine dans $\mathcal{A}$, ce qui nous donne un $u \in \mathcal{A}$ tel que $f(u) = v$.

Subsitutions

Substitutions

Soient A, B deux alphabets. Dans ce cours, une subsitution est une application $\sigma : A \to \mathcal{P}(B^*)$, qu'on étend ainsi par récurrence :

- $\sigma(\epsilon) := \{\epsilon\}$
- Pour tout $u \in A^*$ et $a \in A$, on pose $\sigma(ua) := \sigma(u) \cdot \sigma(a)$

σ est dite rationnelle ou reconnaissable si $\sigma(a) \in \mathrm{Rec}(B^*)$ pour tout $a \in A$.

Lemme

Soient $u \in A^*$ et $v \in B^*$. Alors $v \in \sigma(u)$ ssi $\exists w_1, \ldots, w_{|u|} \in B^*$ tel que $v = w_1 \ldots w_{|u|}$ et $\forall i \in \{1, \ldots, |u|\}, w_i \in \sigma(u_i)$.

Preuve par récurrence sur u.

- Cas $u = \epsilon$: on a bien $v \in \sigma(u)$ ssi $v = \epsilon$ ssi il existe une suite vide...
- Cas inductif : $v \in \sigma(ua)$ ssi v s'écrit xy avec $x \in \sigma(u)$ et $y \in \sigma(a)$, ssi $\exists w_1, \ldots, w_{|u|}, y \in B^*$ tel que $v = w_1 \ldots w_{|u|} y$ et $\forall i \in \{1, \ldots, |u|\}, w_i \in \sigma(u_i)$ et $y \in \sigma(a)$.

Subsitutions (II)

Substitutions (rappel)

Soient A, B deux alphabets. Dans ce cours, une subsitution est une application $\sigma : A \to \mathcal{P}(B^*)$, qu'on étend ainsi par récurrence :

- $\sigma(\epsilon) := \{\epsilon\}$
- Pour tout $u \in A^*$ et $a \in A$, on pose $\sigma(ua) := \sigma(u) \cdot \sigma(a)$

σ est dite rationnelle ou reconnaissable si $\sigma(a) \in \mathrm{Rec}(B^*)$ pour tout $a \in A$.

Lemme

Soient $w_1, \ldots, w_n \in A^*$ et pour tout $j \in [n]$ soit $L_j \subseteq B^*$ tels que $L_j \cap \sigma(w_j) \neq \emptyset$. Alors $L_1 \ldots L_n \cap \sigma(w_1 \ldots w_n) \neq \emptyset$.

Preuve

Pour tout $j \in [n]$ soit $v_j \in L_j \cap \sigma(w_j)$. Alors $v_1 \ldots v_n \in L_1 \ldots L_n$ et $v_1 \ldots v_n \in \sigma(w_1) \ldots \sigma(w_n) = \sigma(w_1 \ldots w_n)$.

Subsitutions et clôture

Modifications d'un langage par substitution

- Pour tout $L \subseteq A^*$, on note $\sigma(L) := \cup_{u \in L} \sigma(u)$.
- Pour tout $L \subseteq B^*$, on note $\sigma^{-1}(L) := \{u \in A^* \mid \sigma(u) \cap L \neq \emptyset\}$.

Théorème

1. Si $L \in \mathrm{Rec}(A^*)$ et $\sigma : A \to \mathrm{Rec}(B^*)$ est une substitution, alors $\sigma(L) \in \mathrm{Rec}(B^*)$.
2. Si $L \in \mathrm{Rec}(B^*)$ et $\sigma : A \to \mathrm{Rec}(B^*)$ est une substitution, alors $\sigma^{-1}(L) \in \mathrm{Rec}(A^*)$.

Un lemme général

Lemme

Tout langage reconnaissable $L \subseteq A^*$ est reconnu par un automate avec ϵ-transition et

- un seul état initial, avec seulement des transitions sortantes
- un seul état final, sans transition sortante.

Preuve

Soit $\mathcal{A} = (Q, \Delta, I, F)$ un automate reconnaissant L. Soit $\mathcal{B} = (Q \uplus \{i, f\}, \Delta', i, f)$ avec Δ' contient Δ et

- pour tout $q \in I$ on pose $(i, \epsilon, q) \in \Delta'$,
- pour tout $q \in F$ on pose $(q, \epsilon, f) \in \Delta'$.

On peut vérifier facilement que $\mathcal{L}(\mathcal{B}) = \mathcal{L}(\mathcal{A})$, par double inclusion.

Clôture par subsitution

Théorème

Si $L \in \mathrm{Rec}(A^*)$ et $\sigma : A \to \mathrm{Rec}(B^*)$, alors $\sigma(L) \in \mathrm{Rec}(B^*)$.

Soit $\mathcal{A} = (A, Q, \Delta, i, F)$ un automate sans ϵ-transitions reconnaissant L.
Pour tout $(q_1, a, q_2) \in \Delta$, soient
$B_{q_1,a,q_2} = (B, Q_{q_1,a,q_2} \cup \{q_1, q_2\}, \Delta_{q_1,a,q_2}, q_1, q_2)$ un automate reconnaissant $\sigma(a)$ sans transition entrante vers q_1, et sans transition sortante de q_2. Soit $\mathcal{B} = (B, Q', \Delta', i, F)$ l'automate où:

- $Q' := Q \uplus \biguplus_{(q_1,a,q_2)\in\Delta} Q_{q_1,a,q_2}$.
- $\Delta' := \biguplus_{(q_1,a,q_2)\in\Delta} \Delta_{q_1,a,q_2}$.

Notons que pour tout $q \in Q$ et $a \in A$, on a $\Delta(q, a) = \Delta'(q, \sigma(a)) \cap Q$.
Mq $\mathcal{L}(\mathcal{B}) = \sigma(L)$ par double inclusion.
Soit $v \in \sigma(L)$, soit donc $u \in L$ tel que $v \in \sigma(u)$. Comme $u \in L$, soient $q_0, \ldots, q_{|u|} \in Q$ tel que $q_0 = i$, $q_{|u|} \in F$ et $(q_{j-1}, u_j, q_j) \in \Delta$. Or $v \in \sigma(u)$, donc v s'écrit $w_1 \ldots w_{|u|}$ avec $w_j \in \sigma(u_j)$. Or $(q_{j-1}, u_j, q_j) \in \Delta$, donc $q_j \in \Delta'(q_{j-1}, w_j)$, i.e. $q_{|u|} \in \Delta'(i, v) \cap F$, i.e $v \in \mathcal{L}(\mathcal{B})$.

Clôture par substitution

Théorème (rappel)

Si $L \in \mathrm{Rec}(A^*)$ et $\sigma : A \to \mathrm{Rec}(B^*)$, alors $\sigma(L) \in \mathrm{Rec}(B^*)$.

Soit $\mathcal{A} = (A, Q, \Delta, i, F)$ un automate sans ϵ-transitions reconnaissant L.
Pour tout $(q_1, a, q_2) \in \Delta$, soient
$B_{q_1,a,q_2} = (B, Q_{q_1,a,q_2} \cup \{q_1, q_2\}, \Delta_{q_1,a,q_2}, q_1, q_2)$ un automate reconnaissant $\sigma(a)$ sans transition entrante vers q_1, et sans transition sortante de q_2. Soit $\mathcal{B} = (B, Q', \Delta', i, F)$ l'automate où:

- $Q' := Q \cup \cup_{(q_1,a,q_2)\in\Delta} Q_{q_1,a,q_2}$.
- $\Delta' := \cup_{(q_1,a,q_2)\in\Delta} \Delta_{q_1,a,q_2}$.

Mq $\mathcal{L}(\mathcal{B}) = \sigma(L)$ par double inclusion.
Soit $v \in \mathcal{L}(\mathcal{B})$, i.e. il existe un calcul $i \xrightarrow{v} F$. Soient $q_0, \ldots, q_n$ les états de Q (pas Q') au cours de ce calcul, avec $q_0 = i$ et $q_n \in F$. Soit $w_1, \ldots, w_n \in B^*$ tel que $v = w_1 \ldots w_n$ et $q_{j-1} \xrightarrow{w_j} q_j$ pour tout $j \in [n]$.
Ainsi pour tout j, il existe $a_j \in A$ tel que $w_j \in \mathcal{L}(B_{q_{j-1},a_j,q_j}) = \sigma(a_j)$. Soit $u = a_1 \ldots a_n$, donc $v \in \sigma(u)$. Or $(q_{j-1}, a, q_j) \in \Delta$, donc $u \in L$.

Clôture par substitution inverse

Théorème

Si $L \in \mathrm{Rec}(B^*)$ et $\sigma : A \to \mathrm{Rec}(B^*)$ est une substitution, alors $\sigma^{-1}(L) \in \mathrm{Rec}(A^*)$.

- Soit $\mathcal{B} = (B, Q, \delta, i, F)$ reconnaissant L. Pour tout $q_1, q_2 \in Q$, soient $\mathcal{B}_{q_1,q_2} := (B, Q, \delta, q_1, q_2)$ et $L_{q_1,q_2} := \mathcal{L}(\mathcal{B}_{q_1,q_2})$. Notons que $L_{q_1,q_2} L_{q_2,q_3} \subseteq L_{q_1,q_3}$. Soit $\mathcal{A} := (A, Q, \Delta, i, F)$ avec $(q_1, a, q_2) \in \Delta$ ssi $L_{q_1,q_2} \cap \sigma(a) \neq \emptyset$. Montrons que $\mathcal{L}(\mathcal{A}) = \sigma^{-1}(L)$ par double inclusion.
- Soit $u \in \mathcal{L}(\mathcal{A})$. Soit donc $q_0, \ldots, q_{|u|} \in Q$ tels que $q_0 = i$, $q_{|u|} \in F$ et $(q_{j-1}, u_j, q_j) \in \Delta$. Donc $L_{q_{j-1},q_j} \cap \sigma(u_j) \neq \emptyset$, donc $L_{q_0,q_1} \ldots L_{q_{|u|-1},q_{|u|}} \cap \sigma(u) \neq \emptyset$. Donc $L_{q_0,q_{|u|}} \cap \sigma(u) \neq \emptyset$. Or $L_{q_0,q_{|u|}} \subseteq L$, donc $u \in \sigma^{-1}(L)$.
- Soit $u \in \sigma^{-1}(L)$. Soit donc $v \in L \cap \sigma(u)$. Or $\sigma(u) = \sigma(u_1) \ldots \sigma(u_{|u|})$, soient donc $w_1, \ldots w_{|u|}$ tels que $v = w_1 \ldots w_{|u|}$ et $w_j \in \sigma(u_j)$. Soit $q_j := \delta(i, w_1 \ldots w_j)$. Ainsi $w_j \in L_{q_{j-1},q_j} \cap \sigma(u_j)$, donc $(q_{j-1}, u_j, q_j) \in \Delta$. Or $q_0 = i$ et $q_{|u|} \in F$ car $v \in L$, donc $u \in \mathcal{L}(\mathcal{A})$.

Lemme de l'étoile (Pumping Lemma)

$\forall L \in \mathrm{Rec}(\Sigma^*), \exists N \in \mathbb{N} \setminus \{0\}, \forall u \in L \cap (\Sigma^N \Sigma^*), \exists x, y, z \in \Sigma^*$ tels que :

- $u = xyz$
- $y \neq \epsilon$
- $xy^*z \subseteq L$, i.e. $\forall n \in N, xy^n z \in L$

Preuve : Soit $\mathcal{A} = (Q, \delta, i, F)$ un AFD et $L := \mathcal{L}(\mathcal{A})$. Mq $N := |Q|$ convient. Soit $u \in L \cap (\Sigma^{|Q|}\Sigma^*)$. Soit $(i, f) \in I \times F$ tq $i \xrightarrow{u} f$. Ce calcul visite $\delta^*(i, u[1, j])$ pour $j \in \{0, \ldots, |u|\}$. Or $|Q| \leq |u|$ donc $\exists j < k \in \{0, \ldots, |u|\}$ tel que $\delta^*(i, u[1, j]) = \delta^*(i, u[1, k])$. Soit $x := \delta^*(i, u[1, j])$ et y tel que $xy = \delta^*(i, u[1, k])$. On a $y \neq \epsilon$. Soit $q := \delta^*(i, x) = \delta^*(i, xy)$. Alors $\delta(q, y) = \delta(\delta(i, x), y) = \delta(i, xy) = q$. Montrons que $\forall n \in \mathbb{N}, \delta^*(i, xy^n) = q$ par récurrence sur n.

- $\delta^*(i, xy^0) = \delta^*(i, x) = q$
- $\delta^*(i, xy^{n+1}) = \delta^*(i, xy^n y) = \delta^*(i, xy^n y) = \delta(\delta^*(i, xy^n), y) \overset{HR}{=} \delta(q, y) = q$.

Soit z tel que $u = xyz$. Alors $\delta^*(i, xy^n z) = \delta^*(q, z) = \delta^*(i, xyz) \in F$.

Généralisation du lemme de l'étoile

Lemme de l'étoile (rappel)

$\forall L \in \mathrm{Rec}(\Sigma^*), \exists N \in \mathbb{N} \setminus \{0\}, \forall u \in L \cap (\Sigma^N \Sigma^*), \exists x, y, z \in \Sigma^*$ tels que :

- $u = xyz$
- $y \neq \epsilon$
- $xy^*z \subseteq L$, i.e. $\forall n \in N, xy^n z \in L$

1ère généralisation du lemme de l'étoile

$\forall L \in \mathrm{Rec}(\Sigma^*), \exists N \in \mathbb{N} \setminus \{0\}, \forall vuw \in L$, si $N \leq |u|$ alors $\exists x, y, z \in \Sigma^*$ tels que :

- $u = xyz$
- $y \neq \epsilon$
- $vxy^*zw \subseteq L$

Preuve similaire

Généralisation du lemme de l'étoile (II)

1ère généralisation du lemme de l'étoile (rappel)

$\forall L \in \mathrm{Rec}(\Sigma^*), \exists N \in \mathbb{N} \setminus \{0\}, \forall vuw \in L$, si $N \leq |u|$ alors $\exists x, y, z \in \Sigma^*$ tels que :

- $u = xyz$
- $y \neq \epsilon$
- $vxy^*zw \subseteq L$

2ème généralisation du lemme de l'étoile

$\forall L \in \mathrm{Rec}(\Sigma^*), \exists N \in \mathbb{N} \setminus \{0\}, \forall (v, u_1, \ldots, u_N, w) \in \Sigma^* \times (\Sigma^+)^N \times \Sigma^*$, si $vu_1 \ldots u_N w \in L$ alors il existe $0 < j < k \leq N$ tels que $vu_1 \ldots u_j (u_{j+1} \ldots u_k)^* u_{k+1} \ldots u_N w \subseteq L$

Preuve similaire

Généralisation du lemme de l'étoile (III)

3ème généralisation du lemme de l'étoile

Soit $L \in \Sigma^*$. Les trois assertions suivantes sont équivalentes.

1. L est rationnel.
2. $\exists N \in \mathbb{N}\setminus\{0\}, \forall (v, u_1, \ldots, u_N, w) \in \Sigma^* \times (\Sigma^+)^N \times \Sigma^*, \exists 0 < j < k \leq N$ tels que pour tout $n \in \mathbb{N}$
   $vu_1 \ldots u_N w \in L$ ssi $vu_1 \ldots u_j (u_{j+1} \ldots u_k)^n u_{k+1} \ldots u_N w \in L$
3. $\exists N \in \mathbb{N}\setminus\{0\}, \forall (v, u_1, \ldots, u_N, w) \in \Sigma^* \times (\Sigma^+)^N \times \Sigma^*, \exists 0 < j < k \leq N$ tels que $vu_1 \ldots u_N w \in L$ ssi $vu_1 \ldots u_j (u_{j+1} \ldots u_k)^* u_{k+1} \ldots u_N w \subseteq L$
4. $\exists N \in \mathbb{N}\setminus\{0\}, \forall (v, u_1, \ldots, u_N, w) \in \Sigma^* \times (\Sigma^+)^N \times \Sigma^*, \exists 0 < j < k \leq N$ tels que $vu_1 \ldots u_N w \in L$ ssi $vu_1 \ldots u_j u_{k+1} \ldots u_N w \in L$

Preuve en TD (en invoquant le théorème fini de Ramsey)

Application du lemme de l'étoile et cie

Lemme de l'étoile (rappel)

$\forall L \in \mathrm{Rec}(\Sigma^*), \exists N \in \mathbb{N} \setminus \{0\}, \forall u \in L \cap (\Sigma^N \Sigma^*), \exists x, y, z \in \Sigma^*$ tels que :

- $u = xyz$
- $y \neq \epsilon$
- $xy^*z \subseteq L$, i.e. $\forall n \in N, xy^n z \in L$

Proposition

$L_1 := \{a^n b^n \mid n \in \mathbb{N}\}$ n'est pas rationnel.

Preuve (invoquant le lemme de l'étoile)

Supposons que L_1 est rationnel. Soit donc un N correspondant du lemme de l'étoile. Soit $u = a^N b^N$. On a $N \leq |u|$, soit donc x, y, z tq $u = xyz$ et $y \neq \epsilon$ et $xy^2z \in L_1$. Si $y \in a^*$, alors $a^{N+|y|} b^N \in L_1$, contradiction. Si $y \in b^*$, alors $a^N b^{N+|y|} \in L_1$, contradiction. Si $y \in a^+ b^+$, alors $xy^2z \notin a^+ b^+$, contradiction car $xy^2z \in L_1 \cap \{a, b\}^+ \subseteq a^+ b^+$.

Application du lemme de l'étoile et cie (II)

Première généralisation du lemme de l'étoile (rappel)

$\forall L \in \mathrm{Rec}(\Sigma^*), \exists N \in \mathbb{N} \setminus \{0\}, \forall vuw \in L$, si $N \leq |u|$ alors $\exists x, y, z \in \Sigma^*$ tels que :

- $u = xyz$
- $y \neq \epsilon$
- $vxy^*zw \subseteq L$

Proposition

$L_1 := \{a^n b^n \mid n \in \mathbb{N}\}$ n'est pas rationnel.

Preuve (invoquant la première généralisation du lemme de l'étoile)

Supposons que L_1 est rationnel. Soit donc un N correspondant de la première généralisation du lemme de l'étoile. Soit $u = a^N b^N$. Notons que u se décompose en $\epsilon \cdot a^N \cdot b^N$ avec $N \leq |a^N|$. Soient donc x, y, z tel que $a^N = xyz$ et $y \neq \epsilon$ et $\epsilon \cdot xy^2z \cdot b^N \in L_1$. Or $xy^2z \in a^{N+1}a^*$, contradiction.

Application du lemme de l'étoile et cie (III)

Proposition

$L_2 := \{u \in \{a,b\}^* \mid |u|_a = |u|_b\}$ n'est pas rationnel.

La seconde preuve pour L_1 mot pour mot.

Proposition

$L_3 := L_2 \setminus \{a,b\}^*(a^3 + b^3)\{a,b\}^*$ n'est pas rationnel.

Supposons que L_3 est rationnel. Soit le N de la 2ème généralisation. Soit $u = (aab)^N(abb)^N \in L_3$. Soit $u_1 = \cdots = u_N = aab$. Ainsi $u = \epsilon \cdot u_1 \ldots u_N \cdot (abb)^N$. Donc $(aab)^{N+k}(abb)^N \in L_3$ avec $0 < k$.

Proposition

$L_4 := \{u \in \{a,b\}^* \mid \overline{u} = u\}$ n'est pas rationnel.

$u = a^N b^N a^N \in L_4$ se décompose en $\epsilon \cdot a^N \cdot b^N a^N$, donc $\exists k > 0, \epsilon \cdot a^{N+k} \cdot b^N a^N$!!!

Puissances du lemme de l'étoile et de ses généralisations

- Rappel : $L_2 := \{u \in \{a,b\}^* \mid |u|_a = |u|_b\}$ n'est pas rationnel, en utilisant la 1ère généralisation du lemme de l'étoile. Soit $u \in L_2 \setminus \{\epsilon\}$. Si $u_1 = a$, u se décompose en $u = a^n(ab)v$, et $a^n(ab)^*v \subseteq L_2$. Donc le lemme de l'étoile n'est pas adapté pour L_2.
- Soit $K_2 := \{(ab)^n(cd)^n \mid \in \mathbb{N}\} \cup \Sigma^*\{aa, bb, cc, dd, ac\}\Sigma^*$. K_2 n'est pas rationnel, en utilisant la 2ème généralisation du lemme de l'étoile. Mais K_2 vérifie le critère de la 1ère généralisation.
- Soit K_3 l'ensemble des udv avec $u, v \in \{a,b,c\}^*$ tels que $u \neq v$ ou u ou v contient un carré non vide. K_3 satisfait vérifie le critère de la 2ème généralisation mais n'est pas rationnel.

Autres techniques de preuve de non-rationalité

Par "réduction".

1. Rappel : $L_1 := \{a^n b^n \mid n \in \mathbb{N}\}$ n'est pas rationnel et $L_2 = \{u \in \{a,b\}^* \mid |u|_a = |u|_b\}$.

   Nouvauté : Soit $L_1' := \{a^n b^p \mid n, p \in \mathbb{N}\}$. On a $L_1 = L_2 \cap L_1'$. Or L_1' est rationnel, donc L_2 ne l'est pas.

2. Rappel : $L_3 := L_2 \setminus \{a,b\}^*(a^3 + b^3)\{a,b\}^*$.

   Nouvauté : Soit $f : \{a,b\}^* \to \{a,b\}^*$ morphisme défini par $f(a) := aab$ et $f(b) := abb$. On peut montrer que $f^{-1}[L_3] = L_2$, on peut alors conclure que L_3 n'est pas rationnel, par contraposée de la préservation de la rationalité par image inverse de morphisme.

3. Soit $L_5 = \{u \in \{a,b\}^* \mid |u|_a \neq |u|_b\}$. $L_5 = \{a,b\}^* \setminus L_2$. Or L_2 n'est pas rationnel, donc L_5 non plus.