Automates et calculabilité

Leçon 9 : **Relations de Myhill-Nerode**

Simon Kramer

15 décembre 2003

Plan de la leçon

1. Motivation
2. Définition du concept
3. $\{\ A \mid \mathsf{AFD}(A)\ \} \ \cong\ \{\ \equiv\ \mid \mathsf{MN}(\equiv)\ \}$
4. Le théorème de Myhill-Nerode
5. Une application
6. Exercises

Motivation

L'algorithme de minimisation $\min$ pour les AFD

Admettons

- deux AFD A et B acceptant le langage E
- A et B n'ont pas d'états inaccessibles
- $A' \stackrel{\text{def}}{=} \min(A)$ et $B' \stackrel{\text{def}}{=} \min(B)$

Question $A' = B'$?

Réponse non, mais $A' \cong B'$

Justification $A' \cong \equiv_{A'} = \equiv_E = \equiv_{B'} \cong B'$

Définition du concept

Admettons

– Σ un alphabet

– $E \subseteq \Sigma^*$ un ensemble régulier

Définissons une relation $\equiv \subseteq \Sigma^* \times \Sigma^*$, dite *de Myhill-Nerode pour* E[a], par les propriétés suivantes :

Équivalence $\equiv$ est une relation d'équivalence

Congruence à droite pour tout $m, n \in \Sigma^*$ et $l \in \Sigma$,
si $m \equiv n$ alors $m{\cdot}l \equiv n{\cdot}l$

Raffinement pour tout $m, n \in \Sigma^*$,
si $m \equiv n$ alors $m \in E$ ssi $n \in E$

Finitude de l'index $\equiv$ a un nombre fini de classes d'équivalence

[a] nous introduisant le prédicat unaire 'MN' prononcé "est une relation de Myhill-Nerode"

$$\{\ A \mid \mathsf{AFD}(A)\ \} \ \cong\ \{\ \equiv\ \mid \mathsf{MN}(\equiv)\ \}$$

$$(A \mapsto \equiv_A) : \{\ A \mid \mathsf{AFD}(A)\ \} \to \{\ \equiv\ \mid \mathsf{MN}(\equiv)\ \}$$

Admettons

- Σ un alphabet et $E \subseteq \Sigma^*$ un ensemble régulier
- $A \stackrel{\text{def}}{=} \langle Q, \Sigma, \delta, s, F\rangle$ un AFD (sans états inaccess.) acceptant E

Définissons une relation $\equiv_A \subseteq \Sigma^* \times \Sigma^*$ t.q. pour tout $m, n \in \Sigma^*$,

$$\boxed{m \ \equiv_A\ n \quad \textsf{ssi} \quad \hat{\delta}(s, m) = \hat{\delta}(s, n)}$$

Intuition deux mots m et n sont dans la relation $\equiv_A$ si et seulement si l'automate A *s'arrête dans le même état* pour les deux mots

Remarques

1. $\equiv_A$ est une relation de Myhill-Nerode pour E
2. on dit que A *induit* la relation $\equiv_A$ dans l'ensemble Σ^*

$$\{\ A \mid \mathsf{AFD}(A)\ \} \ \cong \ \{\ \equiv \ \mid \mathsf{MN}(\equiv)\ \}$$

$$(\equiv \mapsto A_{\equiv}) : \{\ \equiv \ \mid \mathsf{MN}(\equiv)\ \} \to \{\ A \mid \mathsf{AFD}(A)\ \}$$

Admettons

- Σ un alphabet et $E \subseteq \Sigma^*$ un ensemble
- $\equiv$ une relation de Myhill-Nerode pour E

Définissons $A_{\equiv} \stackrel{\text{def}}{=} \langle Q, \Sigma, \delta, s, F \rangle$ un AFD tel que

$$\boxed{\begin{array}{llll} Q \stackrel{\text{def}}{=} \{\ [m]_{\equiv} \mid m \in \Sigma^*\ \} & & \delta([m]_{\equiv}, l) \stackrel{\text{def}}{=} [m{\cdot}l]_{\equiv} \\ F \stackrel{\text{def}}{=} \{\ [m]_{\equiv} \mid m \in E\ \} & & s \stackrel{\text{def}}{=} [\epsilon]_{\equiv} \end{array}}$$

Remarques

1. δ *est bien définie* : pour tout $n \in [m]_{\equiv}$, $[m{\cdot}l]_{\equiv} = [n{\cdot}l]_{\equiv}$.
2. $\mathcal{L}(A_{\equiv}) = E$

$$\{\ A \mid \mathsf{AFD}(A)\ \} \cong \{\ \equiv\ \mid \mathsf{MN}(\equiv)\ \}$$

$$(a \circ (\equiv \mapsto A_\equiv)) \circ (A \mapsto \equiv_A) = 1_{\{\ A\ \mid\ \mathsf{AFD}(A)\ \}}$$

Admettons

- $A \stackrel{\text{def}}{=} \langle Q, \Sigma, \delta, s, F \rangle$
- $A_{\equiv_A} \stackrel{\text{def}}{=} ((\equiv \mapsto A_\equiv) \circ (A \mapsto \equiv_A))(A) \stackrel{\text{def}}{=} \langle Q', \Sigma, \delta', s', F' \rangle$
- une application $a : Q' \to Q$ telle que $a([m]_{\equiv_A}) \stackrel{\text{def}}{=} \hat{\delta}(s, m)$

Montrons a est un isomorphisme d'automates :

1. a est bien défini : $[m]_{\equiv_A} = [n]_{\equiv_A}$ ssi $\hat{\delta}(s, m) = \hat{\delta}(s, n)$ par définition de $\equiv_A$
2. a est injective : si $[m]_{\equiv_A} \neq [n]_{\equiv_A}$ alors $\hat{\delta}(s, m) \neq \hat{\delta}(s, n)$
3. a est surjective : A n'a pas d'états inaccessibles
4. a est un *homomorphisme* (d'automates) : . . .

$\{\ A \mid \mathsf{AFD}(A)\ \} \ \cong\ \{\ \equiv\ \mid \mathsf{MN}(\equiv)\ \}$

$(a \circ (\equiv\ \mapsto A_{\equiv})) \circ (A \mapsto\ \equiv_A) = 1_{\{\ A \mid \mathsf{AFD}(A)\ \}}$ **(suite)**

a est un homomorphisme (d'automates), à savoir a conserve :

1. l'état initial s' : $a(s') = s$
   par définition de s', a, et $\hat{\delta}$
2. la fonction de transition δ' : $a(\delta'([m]_{\equiv_A}, l)) = \delta(a([m]_{\equiv_A}), l)$
   par définition de δ', a, $\hat{\delta}$, et a
3. les états finaux : $[m]_{\equiv_A} \in F'$ ssi $a([m]_{\equiv_A}) \in F$
   par définition de F', par $\mathcal{L}(A) = E$, et par définition de a

Conséquence $a \circ (\equiv\ \mapsto A_{\equiv}) \circ (A \mapsto\ \equiv_A) = 1_{\{\ A \mid \mathsf{AFD}(A)\ \}}$

$$\{\ A \mid \mathsf{AFD}(A)\ \} \ \cong\ \{\ \equiv\ \mid \mathsf{MN}(\equiv)\ \}$$

$$(A \mapsto \equiv_A) \circ (a \circ (\equiv \mapsto A_\equiv)) = 1_{\{\ \equiv\ \mid\ \mathsf{MN}(\equiv)\ \}}$$

Admettons $\equiv_{A_\equiv} \stackrel{\text{def}}{=} ((A \mapsto \equiv_A) \circ (\equiv \mapsto A_\equiv))(\equiv)$

Montrons $(m,n) \in \equiv_{A_\equiv}$ **ssi** $(m,n) \in \equiv$

$$\begin{array}{lll} m \equiv_{A_\equiv} n & \textbf{ssi} & \hat{\delta}(s,m) = \hat{\delta}(s,n) \\ & \textbf{ssi} & \hat{\delta}([\epsilon]_\equiv, m) = \hat{\delta}([\epsilon]_\equiv, n) \\ & \textbf{ssi} & [m]_\equiv = [n]_\equiv \\ & \textbf{ssi} & m \equiv n \end{array}$$

Conclusion $(A \mapsto \equiv_A) \circ (\equiv \mapsto A_\equiv) = 1_{\{\ \equiv\ \mid\ \mathsf{MN}(\equiv)\ \}}$

$\{\ A \mid \mathsf{AFD}(A)\ \} \cong \{\ \equiv\ \mid \mathsf{MN}(\equiv)\ \}$

$(A \mapsto \equiv_A) \circ (a \circ (\equiv \mapsto A_\equiv)) = 1_{\{\ \equiv\ \mid\ \mathsf{MN}(\equiv)\ \}}$ **(suite)**

$$
\begin{aligned}
1_{\{\ \equiv\ \mid\ \mathsf{MN}(\equiv)\ \}} &= (A \mapsto \equiv_A) \circ (\equiv \mapsto A_\equiv) \\
&= (A \mapsto \equiv_A) \circ 1_{\{\ A\ \mid\ \mathsf{AFD}(A)\ \}} \circ (\equiv \mapsto A_\equiv) \\
&= (A \mapsto \equiv_A) \circ a \circ (\equiv \mapsto A_\equiv) \circ (A \mapsto \equiv_A) \circ (\equiv \mapsto A_\equiv) \\
&= (A \mapsto \equiv_A) \circ a \circ (\equiv \mapsto A_\equiv) \circ 1_{\{\ \equiv\ \mid\ \mathsf{MN}(\equiv)\ \}} \\
&= (A \mapsto \equiv_A) \circ a \circ (\equiv \mapsto A_\equiv)
\end{aligned}
$$

Conclusion $(A \mapsto \equiv_A)^{-1} \stackrel{\text{def}}{=} a \circ (\equiv \mapsto A_\equiv)$ — et par conséquence $(A \mapsto \equiv_A)$ — est un isomorphisme (un homomorphisme bijectif) :

$$
\boxed{
\begin{aligned}
(A \mapsto \equiv_A)^{-1} \circ (A \mapsto \equiv_A) &= 1_{\{\ A\ \mid\ \mathsf{AFD}(A)\ \}} \\
(A \mapsto \equiv_A) \circ (A \mapsto \equiv_A)^{-1} &= 1_{\{\ \equiv\ \mid\ \mathsf{MN}(\equiv)\ \}}
\end{aligned}
}
$$

Le théorème de Myhill-Nerode

Admettons Σ un alphabet et $E \subseteq \Sigma^*$ un ensemble

Définissons une relation $\equiv_E \subseteq \Sigma^* \times \Sigma^*$ t.q. pour tout $m, n \in \Sigma^*$,

$$\boxed{m \equiv_E n \quad \text{ssi} \quad \text{pour tout } m' \in \Sigma^*, \;\; m \bullet m' \in E \;\text{ ssi }\; n \bullet m' \in E}$$

Propriétés $\equiv_E$ est (1) une relation d'équivalence, (2) une congruence à droite, (3) *le raffinement le plus grand pour* E, et (4) si E est régulier alors $\equiv_E$ correspond à un AFD minimal pour E et a donc un index fini.

Théorème les propositions suivantes sont équivalentes :

1. E est régulier
2. il existe une relation de Myhill-Nerode pour E
3. $\equiv_E$ a un index fini

Le théorème de Myhill-Nerode

$\equiv_E$ est une congruence à droite

1	$m \equiv_E n$	hyp
2	$\forall(v \in \Sigma^*)(m \bullet v \in E \;\Leftrightarrow\; n \bullet v \in E)$	1
3	$\quad l \in \Sigma$	hyp
4	$\quad m \bullet (\text{"}l\text{"} \bullet m') \in E \;\Leftrightarrow\; n \bullet (\text{"}l\text{"} \bullet m') \in E$	2
5	$\quad (m \bullet \text{"}l\text{"}) \bullet m' \in E \;\Leftrightarrow\; (n \bullet \text{"}l\text{"}) \bullet m' \in E$	4
6	$\quad m{\cdot}l \bullet m' \in E \;\Leftrightarrow\; n{\cdot}l \bullet m' \in E$	5
7	$\quad \forall(v \in \Sigma^*)(m{\cdot}l \bullet v \in E \;\Leftrightarrow\; n{\cdot}l \bullet v \in E)$	6
8	$\quad m{\cdot}l \equiv_E n{\cdot}l$	7
9	$l \in \Sigma \Rightarrow m{\cdot}l \equiv_E n{\cdot}l$	3, 8
10	$\forall(l \in \Sigma)(m{\cdot}l \equiv_E n{\cdot}l)$	9

Le théorème de Myhill-Nerode

$\equiv_E$ est un raffinement pour E

1	$m \equiv_E n$	hyp
2	$\forall (v \in \Sigma^*)(m \bullet v \in E \;\Leftrightarrow\; n \bullet v \in E)$	1
3	$m \bullet \epsilon \in E \;\Leftrightarrow\; n \bullet \epsilon \in E$	2
4	$m \in E \Leftrightarrow n \in E$	3
5	$m \equiv_E n \Rightarrow (m \in E \Leftrightarrow n \in E)$	1,4

Le théorème de Myhill-Nerode

$\equiv_E$ est le raffinement le plus grand pour E

Soit $\equiv\ \Sigma^* \times \Sigma^*$ une congruence à droite et un raffinement de E :

1	$\quad m \equiv n$	hyp
2	$\quad \forall (v \in \Sigma^*)(m \bullet v \equiv n \bullet v)$	1, congr., lemme
3	$\quad m \bullet v \equiv n \bullet v$	2
4	$\quad m \bullet v \in E \;\Leftrightarrow\; n \bullet v \in E$	3, raffinement
5	$\quad \forall (v \in \Sigma^*)(m \bullet v \in E \;\Leftrightarrow\; n \bullet v \in E)$	4
6	$\quad m \equiv_E n$	5
7	$m \equiv n \Rightarrow m \equiv_E n$	1,6

Le théorème de Myhill-Nerode

$\equiv_E$ correspond à un AFD minimal

Rappel Soit $A' \stackrel{\text{def}}{=} \langle Q', \Sigma, \delta', s', F' \rangle \stackrel{\text{def}}{=} \min(A)$ acceptant E. Alors $p, q \in Q$ sont regroupés dans le même état dans A' ssi $p \approx q$:

$p \approx q$:ssi pour tout $m \in \Sigma^*$, $\hat{\delta}(p, m) \in F$ ssi $\hat{\delta}(q, m) \in F$

$m \equiv_E n$ ssi $\forall (v \in \Sigma^*)(m \bullet v \in E \Leftrightarrow n \bullet v \in E)$

ssi $\forall (v \in \Sigma^*)(\hat{\delta}'(s', m \bullet v) \in F' \Leftrightarrow \hat{\delta}'(s', n \bullet v) \in F')$

ssi $\forall (v \in \Sigma^*)(\hat{\delta}'(\hat{\delta}'(s', m), v) \in F' \Leftrightarrow \hat{\delta}'(\hat{\delta}'(s', n), v) \in F')$

ssi $\hat{\delta}'(s', m) \approx \hat{\delta}'(s', n)$

ssi $\hat{\delta}'(s', m) = \hat{\delta}'(s', n)$

ssi $m \equiv_{A'} n$

Une application

Montrons $E \stackrel{\mathrm{def}}{=} \{ a^i \bullet b^i \mid i \geq 0 \}$ n'est pas régulier, c'est-à-dire, $\equiv_E$ n'a pas un index fini.

Preuve Soient $k, l \in \mathbb{N}$ t.q. $k \neq l$. Alors $a^k \bullet b^k \in E$ mais $a^l \bullet b^k \notin E$. Donc il n'est pas vrai que $a^k \bullet b^k \in E$ ssi $a^l \bullet b^k \in E$, et ainsi $a^k \not\equiv_E a^l$. C'est-à-dire, a^k et a^l sont dans 2 classes d'équivalence différentes, et ceci *pour k (ou l) aussi grand qu'il soit*. Donc $\equiv_E$ a un nombre infini de classes d'équivalence.

Exercices

Relations montrer que

1. $\equiv_A$ est une relation de Myhill-Nerode, et que $\mathcal{L}(A_\equiv) = E$
2. si une relation $\equiv \subseteq \Sigma^* \times \Sigma^*$ est une congruence à droite, alors pour tout $m' \in \Sigma^*$, si $m \equiv n$ alors $m \bullet m' \equiv n \bullet m'$

Théorème le démontrer

Application montrer que $E \stackrel{\text{def}}{=} \{ a^n \bullet b^m \mid n > m \}$ n'est pas un ensemble régulier en utilisant ce théorème