Langages formels : congruence syntaxique

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

ENS Paris-Saclay

2023-2024

Relation d'équivalence, rappel du cours de maths discrètes

Soient E, F deux ensembles et $f : E \to F$.

- On note $x \sim_f y$ si $f(x) = f(y)$.
- $\sim_f$ est une relation d'équivalence.
- Soit $\sim \subseteq E \times E$ une relation d'équivalence. On dit que $\sim$ et f sont compatibles si $x \sim y \Rightarrow f(x) = f(y)$.
- Lemme : $\sim$ et f sont compatibles ssi $\sim \subseteq \sim_f$.
  Preuve par double implication :
  - Si $x \sim y \Rightarrow f(x) = f(y)$ et $x \sim y$, alors $f(x) = f(y)$, donc $x \sim_f y$.
  - Si $\sim \subseteq \sim_f$ et $x \sim y$, alors $x \sim_f y$, donc $f(x) = f(y)$.

Congruence de monoïde, rappel du cours de maths discrètes

Definition

Soit M un monoïde. Une relation d'équivalence $\sim \subseteq M \times M$ est une congruence si $\forall u, v \in M, u \sim v \Rightarrow \forall x, y \in M, xuy \sim xvy$

Lemma

Une relation d'équivalence $\sim$ sur un monoïde M est une congruence ssi $\forall x, x', y, y' \in M, x \sim x' \wedge y \sim y' \Rightarrow xy \sim x'y'$.
Cela structure $M/\sim$ en monoïde via $[x][y] = [xy]$.

Lemma

Soit $\phi : M \to N$ un morphisme de monoïdes.

- $\sim_\phi$ *est une congruence*
- *Une congruence $\sim$ est compatible avec ϕ ssi $\sim \subseteq \sim_\phi$*
- *De plus $|M/\sim_\phi| = |\phi[M]| \leq |N|$ et quand N est fini on a égalité ssi ϕ est surjective.*

Congruence et quotient de quotient

Proposition

Soit M un monoïde et $\sim_1 \subseteq \sim_2$ deux congruences sur M. Soit $\sim_3 \subseteq (E/\sim_1) \times (E/\sim_1)$ définie par $[u]_1 \sim_3 [v]_1$ s'il existe $u', v' \in M$ tels que $u \sim_1 u' \sim_2 v' \sim_1 v$. Alors

1. $[u]_1 \sim_3 [v]_1$ ssi $u \sim_2 v$.
2. $\sim_3$ est une congruence.
3. La relation $\{([[u]_1]_3, [u]_2) \mid u \in M\}$ est un isomorphisme de monoïde.

Relation d'équivalence et langage compatibles

Définition

On dit qu'une relation d'équivalence $\sim$ sur Σ^* est compatible avec $L \subseteq \Sigma^*$ si elle l'est avec la fonction caractéristique de L.

Lemme

Soient une relation d'équivalence $\sim \subseteq \Sigma^* \times \Sigma^*$ et un langage $L \subseteq \Sigma^*$. Les quatre assertions suivantes sont équivalentes.

1. $\sim$ est compatible avec L.
2. L est une union de classes d'équivalence de $\sim$.
3. $\forall x, y \in \Sigma^*, (x \sim y \wedge x \in L) \Rightarrow y \in L$
4. $\forall x, y \in \Sigma^*, x \sim y \Rightarrow (x \in L \Leftrightarrow y \in L)$

Remarques :

- L'égalité est compatible avec tout langage.
- La relation universelle est compatible avec Σ^* et $\emptyset$ uniquement.

Congruence syntaxique

Rappel : l'équivalence résiduelle est définie par $u \sim_L v$ ssi $u^{-1}L = v^{-1}L$ ssi $\forall y \in \Sigma^*, uy \in L \Leftrightarrow vy \in L$.

- $\sim_L$ est compatible avec L, car $u \sim_L v \Rightarrow (u \in L \Leftrightarrow v \in L)$ en prenant $y := \epsilon$ ci-dessus.
- La plus grande rel. d'éq. compatible avec L est $\sim_{\chi(L)}$ et a une ou deux classes d'équivalence: les ensembles non-vides parmi L et $\Sigma^* \setminus L$.

Définition (congruence syntaxique)

On pose $u \approx_L v$ si $\forall x, y \in \Sigma^*, xuy \in L \Leftrightarrow xvy \in L$

Lemme

$\approx_L$ est une congruence

Preuve : $\approx_L$ est une relation d'équivalence, pour des raisons purement syntaxiques. Soient u, v tels que $u \approx_L v$ et soient $x, y \in \Sigma^*$. Mq $xuv \approx_L xvy$. Pour tout $x', y' \in \Sigma^*$, on a $x'(xuy)y' \in L$ ssi $(x'x)u(yy') \in L$ ssi $(x'x)v(yy') \in L$ ssi $x'(xvy)y' \in L$.

Congruence syntaxique (II)

- Rappel : l'éq. résiduelle est définie par $u \sim_L v$ ssi $u^{-1}L = v^{-1}L$ ssi $\forall y \in \Sigma^*, uy \in L \Leftrightarrow vy \in L$. De plus, $\sim_L$ est compatible avec L.
- Rappel : On pose $u \approx_L v$ si $\forall x, y \in \Sigma^*, xuy \in L \Leftrightarrow xvy \in L$. Alors $\approx_L$ est une congruence.

Lemme

1. $\approx_L \subseteq \sim_L$
2. $\approx_L$ est compatible avec L
3. $\approx_L$ est la plus grande congruence compatible avec L

1. Dans la déf de $\approx_L$, on remplace x par ϵ et on obtient la déf de $\sim_L$
2. Deux preuves ci-dessous.
   - $\approx_L \subseteq \sim_L \subseteq \sim_{\chi(L)}$, donc $\approx_L \subseteq \sim_{\chi(L)}$, donc $\approx_L$ est compatible avec L.
   - Supposons $u \approx_L v$ et $u \in L$. Donc $v \in L$ en prenant $x = y = \epsilon$.
3. Soit $\approx$ une congruence compatible avec L. Soient $u \approx v$. Mq $u \approx_L v$. $\forall x, y \in \Sigma^*, xuy \approx xvy$, car $\approx$ est une congruence. Par compatibilité de $\approx$ avec L, on a donc $\forall x, y \in \Sigma^*, xuy \in L \Leftrightarrow xvy \in L$. I.e. $u \approx_L v$.

Congruence syntaxique et reconnaissance par morphisme

Rappel :

- On pose $u \approx_L v$ si $\forall x, y \in \Sigma^*, xuy \in L \Leftrightarrow xvy \in L$
- $\approx_L$ est une congruence
- $\approx_L$ est compatible avec L
- $\approx_L$ est la plus grande congruence compatible avec L

Lemme

Soit $\phi : \Sigma^* \to M$ reconnaissant L. Alors $|\Sigma^* / \approx_L| \leq |M|$.

Preuve : on a $|\Sigma^* / \sim_\phi| \leq |M|$ pour des raisons ensemblistes et car $u \sim_\phi v$ ssi $\phi(u) = \phi(v)$. Or $\approx_L$ est la congruence la plus grande compatible avec L, donc $\sim_\phi \subseteq \approx_L$, donc $|\Sigma^* / \approx_L| \leq |\Sigma^* / \sim_\phi|$. Ainsi $|\Sigma^* / \approx_L| \leq |M|$.

Corollaire

Si L est reconnu par monoïde fini, alors $\approx_L$ a un nombre fini de classes.

Congruence syntaxique et reconnaissance par morphisme (II)

Rappel : $u \approx_L v$ si $\forall x, y \in \Sigma^*, xuy \in L \Leftrightarrow xvy \in L$

Lemme

Considérons la surjection canonique $[\cdot]_L : \Sigma^* \to \Sigma^*/\approx_L$

1. $\sim_{[\cdot]_L} = \approx_L$
2. $[\cdot]_L$ est un morphisme de monoïde.
3. $[\cdot]_L$ reconnait L.

1. $u \sim_{[\cdot]_L} v$ ssi $[u]_L = [v]_L$ ssi $u \approx_L v$
2. Parce que $\approx_L$ est une congruence. ($[\epsilon]_L$ est bien le neutre de $\Sigma^*/\approx_L$ et $[uv]_L = [u]_L[v]_L$)
3. Par un lemme précédent L est compatible avec $\approx_L$, donc avec $\sim_{[\cdot]_L}$, donc par une caractérisation précédente $[\cdot]_L$ reconnait L.

Corollaire

Si $\approx_L$ a un nombre fini de classes, L est reconnu par monoïde fini.

Langages rationnels et congruences syntaxiques

Théorème

Soit $L \subseteq \Sigma^*$. Il existe un monoïde de cardinal $|\Sigma^*/\approx_L|$ reconnaissant L, mais il n'en existe pas de cardinal plus petit.

Théorème

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

1. L est rationnel.
2. La congruence syntaxique de L a un nombre fini de classes.
3. L est compatible avec une congruence qui a un nombre fini de classes.

Preuve

- $1 \Leftrightarrow 2$ par les deux corollaires précédents.
- $2 \Leftrightarrow 3$ car $\approx_L$ est la plus grande congruence compatible avec L.

Monoïde syntaxique et reconnaissance par morphisme

Lemme

Soit un morphisme $\phi : \Sigma^* \to M$ reconnaissant L. Alors il existe une congruence $\sim$ sur $\phi[\Sigma^*]$ telle que $\phi[\Sigma^*]/\sim$ soit isomorphe à $\Sigma^*/\approx_L$. De plus, $[\cdot]_{\approx_L}$ se factorise en $[\cdot]_\sim \circ \phi$ (à isomorphisme près du codomaine)

Preuve

ϕ reconnaît L, donc $\sim_\phi$ est une congruence compatible avec L, donc $\sim_\phi \subseteq \approx_L$. Soit donc la congruence $\sim_0$ telle que $\Sigma^*/\approx_L$ est isomorphe à $(\Sigma^*/\sim_\phi)/\sim_0$. Or $\phi_{\sim_\phi} : \Sigma^*/\sim_\phi \to \phi[\Sigma^*]$ tel que $\phi_{\sim_\phi}([u]_{\sim_\phi}) := \phi(u)$ est un isomorphisme de monoïdes. On écrit $\phi_{\sim_\phi}([u]_{\sim_\phi}) \sim \phi_{\sim_\phi}([v]_{\sim_\phi})$ si $[u]_{\sim_\phi} \sim_0 [v]_{\sim_\phi}$, i.e. si $u \approx_L v$. Ainsi, $\phi[\Sigma^*]/\sim$ est isomorphe à $(\Sigma^*/\sim_\phi)/\sim_0$, donc à $\Sigma^*/\approx_L$. De plus, $\sim$ est une congruence en tant qu'"image" de $\sim_0$ par un (iso)morphisme. (2ème point à vérifier.)

Le plus petit monoïde reconnaissant L, i.e. $\Sigma^*/\approx_L$, est donc "caché" dans tout monoïde reconnaissant L : on le "découvre" en prenant le bon sous-monoïde puis en en faisant le quotient par la bonne congruence.

Monoïde syntaxique et reconnaissance par morphisme

Lemme

Le monoïde syntaxique de L est isomorphe au monoïde des transitions de l'automate des résiduels de L.

Preuve : Soit $\mathcal{A} = (Q, \delta, i, F)$ un automate minimal reconnaissant L. On sait que le morphisme $\delta^c : \Sigma^* \to (Q \to Q)$, une curryfication de δ^*, reconnaît L. On veut montrer que $\Sigma^* / \approx_L$ est isomorphe à $\delta^c[\Sigma^*]$. Or $\delta^c_{\sim_{\delta^c}} : \Sigma^* / \sim_{\delta^c} \to \delta^c[\Sigma^*]$ tel que $\delta^c_{\sim_{\delta^c}}([u]_{\sim_{\delta^c}}) := \delta^c(u)$ est un isomorphisme. Il suffit donc de montrer $\approx_L = \sim_{\delta^c}$. On sait que $\sim_{\delta^c}$ est une congruence compatible avec L, car δ^c reconnaît L. Or $\approx_L$ est la plus grande congruence compatible avec L, donc $\sim_{\delta^c} \subseteq \approx_L$. Mq $\approx_L \subseteq \sim_{\delta^c}$. Soit $u \approx_L v$. On veut montrer que $\delta^c(u) = \delta^c(v)$, i.e. que $\forall q \in Q, \delta^*(q, u) = \delta^*(q, v)$. Comme $\mathcal{A}$ est minimal, il suffit de montrer que $\forall q \in Q, \mathcal{L}(\delta^*(q, u)) = \mathcal{L}(\delta^*(q, v))$, i.e. $\forall q \in Q, \delta^*(\delta^*(q, u), y) \in F \Leftrightarrow \delta^*(\delta^*(q, v), y) \in F$. Étant minimal, $\mathcal{A}$ est accessible, donc ceci équivaut à $\forall x, y \in \Sigma^*, \delta^*(\delta^*(\delta^*(i, x), u), v) \in F \Leftrightarrow \delta^*(\delta^*(\delta^*(i, x), v), v) \in F$, équivalent à $\forall x, y \in \Sigma^*, xuy \in L \Leftrightarrow xvy \in L$, i.e. à $u \approx_L v$.

Résumé

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

1. L est reconnu par un AFD (ou AFN, etc)
2. L a un nombre fini de résiduels
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 $vu_1 \ldots u_j u_{k+1} \ldots u_N w \in L$ (+ variantes)
4. L est produit par une expression rationnelle.
5. L est reconnu par un morphisme de monoïdes dans un monoïde fini.
6. La congruence syntaxique de L a un nombre fini de classes.