TD 3 – Rationalité, minimisation et monoïdes

1 Rationalité

Exercice 1. Les langages suivants sont-ils rationnels ? Justifier.

1. $\{a^n b^n \mid n \in \mathbb{N}\}$.
2. $\{a^m b^n \mid n \equiv m \pmod d\}$ pour un $d \in \mathbb{N}_{>0}$ donné.
3. $\{a^p \mid p \text{ premier}\}$.
4. $\{a^{P(n)} \mid n \in \mathbb{N}\}$ pour P un polynôme à coefficients dans $\mathbb{N}$.
5. $\{w \in \{a, b, c\}^* \mid (|w|_a = 0) \Rightarrow (|w|_b = 0)\}$.
6. $\{w \in \{a, b\}^* \mid |w|_a < |w|_b\}$.
7. $\{w \in \{a, b\}^* \mid 7 \text{ divise } |w|_a, 3 \text{ divise } |w|_b\}$.
8. $\{w \in \{(,)\}^* \mid w \text{ est bien parenthésé}\}$.

2 Non équivalence des lemmes de pompage

Soit les trois versions qui suivent du lemme de pompage.

1. Soit L un langage rationnel sur un alphabet Σ. Alors
$$\exists n \in \mathbb{N}_{>0}, \forall u \in L : |u| \geq n \Rightarrow \exists v, t, w \in \Sigma^* \quad u = vtw \quad |t| > 0 \quad \forall m \in \mathbb{N} \quad vt^m w \in L\ .$$
2. Soit L un langage rationnel sur un alphabet Σ. Alors
$$\exists n \in \mathbb{N}_{>0}, \forall rus \in L : |u| \geq n \Rightarrow \exists v, t, w \in \Sigma^* \quad u = vtw \quad |t| > 0 \quad \forall m \in \mathbb{N} \quad rvt^m ws \in L\ .$$
3. Soit L un langage rationnel sur un alphabet Σ. Alors
$$\begin{aligned}&\exists n \in \mathbb{N}_{>0}, \forall r u_1 \cdots u_n s \in L :\\ &(\forall i, |u_i| \geq 1) \Rightarrow \exists 1 \leq i < j \leq n \quad \forall m \in \mathbb{N} \quad r u_1 \cdots u_i (u_{i+1} \cdots u_j)^m u_{j+1} \cdots u_n s \in L\ .\end{aligned}$$

Exercice 2. Montrer que $L = \{w \in \{a, b\}^* \mid |w|_a = |w|_b\}$ vérifie le lemme 1 mais pas le lemme 2.

Exercice 3. Montrer que $L = \{(ab)^n (cd)^n \mid n \in \mathbb{N}\} \cup \mathcal{L}(\Sigma^*(aa + bb + cc + dd + ac + bd)\Sigma^*)$ vérifie le lemme 2 mais pas le lemme 3.

3 Quotients, théorème de Myhill-Nerode

Soit Σ un alphabet. Étant donné un langage L sur Σ et $u \in \Sigma^*$ on définit :

— le *quotient à gauche de* L *par* u, noté $u^{-1}L$, comme étant le langage sur Σ tel que $u^{-1}L = \{w \in \Sigma^* \mid uw \in L\}$;

— le *quotient à droite de* L *par* u, noté Lu^{-1}, comme étant le langage sur Σ tel que $Lu^{-1} = \{w \in \Sigma^* \mid wu \in L\}$.

Exercice 4. Montrer qu'un langage L sur un alphabet Σ est rationnel si et seulement s'il a un nombre fini de quotients à gauche, c'est-à-dire que $\{u^{-1}L \mid u \in \Sigma^*\}$ est fini.

Exercice 5. Montrer que pour tout langage rationnel L sur un alphabet Σ, tout AFD le reconnaissant contient au moins $\left|\{u^{-1}L \mid u \in \Sigma^*\}\right|$ états, que ce minorant est atteint et que tous les AFD avec ce nombre minimal d'états sont équivalents à « renommage » des états près (ce qui nous autorise à parler de « l'automate minimal de L »).

4 Algorithme de Brzozowski

Soit Σ un alphabet.

Étant donné un mot $w \in \Sigma^*$, on définit le *mot renversé de* w, noté $w^{\mathcal{R}}$, comme étant $w^{\mathcal{R}} = \varepsilon$ si $w = \varepsilon$ et $w^{\mathcal{R}} = a_n \cdots a_1$ si $w = a_1 \cdots a_n$ pour $n \in \mathbb{N}_{>0}$.

Étant donné un langage L sur Σ, le *renversé de* L, noté $L^{\mathcal{R}}$, est simplement le langage $L^{\mathcal{R}} = \{w^{\mathcal{R}} \mid w \in L\}$.

Pour tout AFD $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$, on définit l'AFN $\mathcal{A}^{\mathcal{R}} = (Q, \Sigma, \delta^{\mathcal{R}}, F, \{q_0\})$ où $\delta^{\mathcal{R}} \colon Q \times \Sigma \to \mathfrak{P}(Q)$ est telle que $\delta^{\mathcal{R}}(q, a) = \{p \in Q \mid \delta(p, a) = q\}$ pour tous $q \in Q$ et $a \in \Sigma$. (Précisons que, dans cette section, nous autoriserons les AFN à avoir un ensemble non vide d'états initiaux au lieu d'uniquement un seul et que nous les interdirons d'avoir des ε-transitions).

On dira enfin qu'un AFD est *émondé* lorsque chacun de ses états est accessible depuis l'état initial.

Exercice 6. Soit L un langage sur Σ et $\mathcal{A}$ un AFD émondé le reconnaissant. Montrer que $\mathcal{A}^{\mathcal{R}}$ est un AFN reconnaissant $L^{\mathcal{R}}$.

Pour tout AFN $\mathcal{B} = (Q, \Sigma, \delta, S, F)$, on notera $\mathcal{B}^{\mathcal{D}}$ l'AFD obtenu de $\mathcal{B}$ par la construction par sous-ensembles, c'est-à-dire la version émondée de l'AFD $(\mathfrak{P}(Q), \Sigma, \delta', S, \{P \subseteq Q \mid P \cap F \neq \emptyset\})$, où δ' est telle que $\delta'(P, a) = \bigcup_{q \in P} \delta(q, a)$ pour tous $P \subseteq Q$ et $a \in \Sigma$.

Exercice 7. Soit L un langage sur Σ et $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$ un AFD émondé le reconnaissant. Considérons l'AFD $(\mathcal{A}^{\mathcal{R}})^{\mathcal{D}} = (Q', \Sigma, \delta', q'_0, F')$, qui reconnaît $L^{\mathcal{R}}$. Montrer que pour tous $u, v \in \Sigma^*$, $Lu^{-1} = Lv^{-1}$ implique que $\hat{\delta}'(q'_0, u^{\mathcal{R}}) = \hat{\delta}'(q'_0, v^{\mathcal{R}})$.

Exercice 8. En déduire que pour tout langage L sur Σ et AFD émondé $\mathcal{A}$ le reconnaissant, $(\mathcal{A}^{\mathcal{R}})^{\mathcal{D}}$ est l'automate minimal reconnaissant $L^{\mathcal{R}}$.

Exercice 9. Proposer un algorithme de minimisation se basant sur le résultat précédent et en discuter la complexité.

5 Reconnaissance par monoïdes

Un *monoïde* est la donnée $(M, \star)$ d'un ensemble M et d'une loi de composition interne $\star \colon M \times M \to M$ tels que

— $\star$ est associative : $\forall x, y, z \in M, (x \star y) \star z = x \star (y \star z)$;

— $\star$ a un élément neutre : $\exists e \in M, \forall m \in M, e \star m = m \star e = m$.

Il est classique de montrer que cet élément neutre est unique, et on le notera donc $1_{(M,\star)}$.

Si Σ est un alphabet, l'ensemble de tous les mots Σ^* muni de la concaténation $\cdot$ forme un monoïde $(\Sigma^*, \cdot)$ dont l'élément neutre est le mot vide, appelé le *monoïde libre engendré par* Σ.

Étant donné deux monoïdes $(M, \star)$ et $(N, \perp)$, un *morphisme de* $(M, \star)$ *dans* $(N, \perp)$ est une application $\varphi \colon M \to N$ telle que :

— $\forall m_1, m_2 \in M, \varphi(m_1) \perp \varphi(m_2) = \varphi(m_1 \star m_2)$;

— $\varphi(1_{(M,\star)}) = 1_{(N,\perp)}$.

Si Σ est un alphabet, on dira qu'un monoïde $(M, \star)$ *reconnaît* un langage L sur Σ si et seulement s'il existe un morphisme $\varphi \colon \Sigma^* \to M$ de $(\Sigma^*, \cdot)$ dans $(M, \star)$ tel que $L = \varphi^{-1}(P)$ pour un certain $P \subseteq M$.

Exercice 10. Montrer que si un langage est reconnu par un monoïde fini, alors il est rationnel.

Exercice 11. Montrer que si un langage est rationnel, alors il est reconnu par un monoïde fini.

Exercice 12. Montrer, en utilisant ce résultat, que le langage $\{w \in \{a, b\}^* \mid |w|_a = |w|_b\}$ n'est pas rationnel. Donner un monoïde permettant de le reconnaître.