TD9 – Monoïdes

Margot Catinaud margot.catinaud@lmf.cnrs.fr

Dans tout ce TD, on note Σ un alphabet fini.

Exercice 1

Soit u et v deux mots de Σ^*. Démontrer par récurrence sur $|u|+|v|$ la propriété suivante :

$$uv = vu \implies \exists\, w \in \Sigma^*,\ \{u, v\} \subset w^*$$

Exercice 2

Soient $n, m \in \mathbb{N}^*$ deux entiers naturels non nuls. Résoudre dans Σ^* l'équation

$$u^m = v^n \tag{$\mathcal{E}$}$$

Exercice 3

Soient $u, v \in \Sigma^*$ deux mots.

Définition 1 : Mots conjugués

Les mots u et v sont dits *conjugués* lorsqu'il existe deux mots $x, y \in \Sigma^*$ tels que $u = xy$ et $v = yx$.

Montrer l'équivalence suivante :

$$u \text{ et } v \text{ sont conjugués} \iff \exists\, z \in \Sigma^*,\ uz = zv.$$

Exercice 4

On considère trois mots $x, y, z \in \Sigma^*$ vérifiant l'égalité $x^2y^2 = z^2$. Justifier qu'il existe un mot $w \in \Sigma^*$ et deux entiers $p, q \in \mathbb{N}$ tels que $x = w^p$, $y = w^q$ et $z = w^{p+q}$.

Exercice 5

Soit $\mathbb{M}$ est un monoïde. Soient K, L deux parties de $\mathbb{M}$. On note

$$L^{-1}K = \left\{ x \in \mathbb{M} \mid \exists y \in L,\ yx \in K \right\}$$

1. Soit $\mathbb{L}$ un sous-monoïde de Σ^*. Démontrer que $\mathbb{L}$ est un monoïde libre si et seulement si $\mathbb{L}^{-1}\mathbb{L} \cap \mathbb{L}\mathbb{L}^{-1} = \mathbb{L}$.
2. Soit $\mathbb{L}$ un sous-monoïde de Σ^*. On définit par récurrence la suite $\left(\mathbb{M}_n\right)_{n\in\mathbb{N}}$ par
   - $\mathbb{M}_0 \overset{\text{def}}{=} \mathbb{L}$ et
   - Pour $n \in \mathbb{N}$, $\mathbb{M}_{n+1} \overset{\text{def}}{=} {\mathbb{M}_n}^{-1}\mathbb{M}_n \cap \mathbb{M}_n{\mathbb{M}_n}^{-1}$

   Démontrer que l'on définit ainsi une suite croissante de monoïdes et que $\bigcup_{n\in\mathbb{N}} \mathbb{M}_n$ est le plus petit sous-monoïde libre contenant $\mathbb{L}$.

Monoïdes finis

Exercice 6

Démontrer qu'un monoïde fini est le quotient d'un monoïde libre.

Exercice 7

Soit $\mathbb{M}$ un monoïde fini et soit $x \in \mathbb{M}$.

1. Démontrer qu'il existe deux entiers naturels $n, m \in \mathbb{N}$ avec $m < n$ et $x^m = x^n$.
2. On définit $l \overset{\text{def}}{=} \min\Big\{n \in \mathbb{N} \;\Big|\; \exists\, m \in [\![0; n-1]\!],\ x^m = x^n\Big\}$.
   (a) Démontrer que les éléments de $\{x^i\}_{i=0}^{l-1}$ sont des éléments distincts.
   (b) Démontrer que le monoïde $\langle x \rangle$ est de cardinal l.
   (c) Soit $k \in [\![0; l-1]\!]$ un entier tel que $x^k = x^l$. Soit $r \in \mathbb{N}$ l'unique entier compris entre k et $l-1$ divisible par $l-k$. Démontrer que $\langle x \rangle$ est un groupe cyclique d'ordre $l-k$ d'élément neutre x^r.
   (d) Démontrer que x admet une puissance qui est un idempotent(*i.e.* un élément y tel que $y^2 = y$). Y en a-t-il plusieurs ?

1 Monoide syntaxique et Langages sans étoile

Exercice 8 (Définition du monoïde syntaxique)

Soit $\mathcal{L} \subset \Sigma^*$ un langage. $\mathcal{L}$ induit alors une relation d'équivalence sur Σ^* :

$$w \sim_{\mathcal{L}} w' \overset{\text{def}}{\iff} \forall\, u, v \in \Sigma^*,\ \Big[uvw \in L \iff uw'v \in \mathcal{L}\Big].$$

Justifier que $\sim_{\mathcal{L}}$ est une congruence sur Σ^*. On définit alors le monoïde syntaxique $\mathbb{M}_{\mathcal{L}}$ comme le quotient $\Sigma^*\big|_{\sim_{\mathcal{L}}}$.

Exercice 9 (Langage reconnu par un monoïde)

Soit $\mathcal{L} \subset \Sigma^*$ un langage. Soit $\mathbb{M}$ un monoïde.

Définition 2 : Langage reconnu par un monoïde

On dit que le langage $\mathcal{L}$ est *reconnu par le monoïde* $\mathbb{M}$ lorsqu'il existe $\varphi : \Sigma^* \longrightarrow \mathbb{M}$ un morphisme de monoïdes et une partie $\mathbb{X} \subseteq \mathbb{M}$ tels que $\mathcal{L} = \varphi^{-1}(\mathbb{X})$.

1. Démontrer qu'un langage reconnu par un monoïde fini est rationnel.
2. Démontrer qu'un langage $\mathcal{L}$ est reconnu par son monoïde syntaxique.
3. Démontrer qu'un langage $\mathcal{L}$ est reconnu par un monoïde $\mathbb{M}$ si et seulement si $\mathbb{M}_{\mathcal{L}}$ est isomorphe à un quotient d'un sous-monoïde de $\mathbb{M}$.
4. En déduire une caractérisation des langages rationnels portant sur leurs monoïdes syntaxiques.

Exercice 10 (Langages sans étoile)

La famille des langages sans étoile est la plus petite famille contenant le langage vide, les singletons et stable par union, passage au complémentaire et concaténation.

1. Démontrer que l'intersection de deux langages sans étoile est sans étoile.
2. Démontrer que Σ^* est sans étoile.
3. Soient $a, b \in \Sigma$ deux lettres distinctes. Démontrer que $(ab)^*$ est sans étoile.

On dit qu'un monoïde fini est *apériodique* lorsque le seul groupe qu'il contient est le groupe trivial $\{1\}$.

4. Soit $\mathbb{M}$ un monoïde fini. Démontrer l'équivalence des assertions suivantes :
   (i) Le monoïde $\mathbb{M}$ est apériodique ;
   (ii) $\forall\, m \in \mathbb{M},\ \exists\, n \in \mathbb{N}^*,\ m^{n+1} = m^n$;
   (iii) $\exists\, n_0 \in \mathbb{N}^*,\ \forall\, m \in \mathbb{M},\ m^{n_0+1} = m^{n_0}$.
5. Soit $\mathcal{L}$ un langage rationnel et soit $\mathbb{M}_{\mathcal{L}}$ son monoïde syntaxique associé. Par définition du monoïde syntaxique, on déduit de la question précédente que les deux propriétés suivantes sont équivalentes :
   (i) $\mathbb{M}_{\mathcal{L}}$ est apériodique ;
   (ii) $\forall\, u \in \Sigma^*,\ \exists\, n_u \in \mathbb{N}^*,\ \forall\, v, w \in \Sigma^*,\ \Big[vu^{n_u}w \in L \iff vu^{n_u+1}w \in L\Big]$

   Dans ce cas, on appelle *indice du langage* $\mathcal{L}$, noté $i(\mathcal{L})$, le plus petit entier naturel non nul n_u vérifiant la propriété (ii).
   (a) Démontrer les propriétés suivantes :
   (i) $i(\{a\}) = 1$,

(*ii*) $i(\mathcal{L} \cup \mathcal{L}') \leqslant \max\big(i(\mathcal{L}), i(\mathcal{L}')\big)$,
(*iii*) $i(\mathcal{L}\mathcal{L}') \leq i(\mathcal{L}) + i(\mathcal{L}') + 1$,
(*iv*) $i\big(\Sigma^* \setminus \mathcal{L}\big) = i(\mathcal{L})$.

(b) En déduire que le monoïde syntaxique d'un langage sans étoile est apériodique.

6. Soit $\mathbb{M}$ un monoïde fini apériodique. Démontrer les propriétés suivantes :
   (a) **(Règles de simplification)** $\forall\, u, v, w \in \mathbb{M},\ \big[w = uwv \Rightarrow w = uw = wv\big]$.
   (b) 1 est le seul élément inversible à droite ou à gauche
   (c) $\forall m \in \mathbb{M},\ \big(m\mathbb{M} \cap \mathbb{M}m\big) \setminus \Big\{u \in \mathbb{M} \;\Big|\; m \notin \mathbb{M}u\mathbb{M}\Big\} = \{m\}$.
7. Soit $\mathbb{M}$ un monoïde fini apériodique. Soit $m \in \mathbb{M}$. On définit $\rho(m) = \mathrm{Card}(\mathbb{M}m\mathbb{M})$.
   (a) Démontrer que le seul m tel que $\rho(m) = \mathrm{Card}(\mathbb{M})$ est $m = 1$.
   (b) Soient $u, v \in \mathbb{M}$. Si $u \in vM$ et $v \notin uM$, alors $\rho(v) > \rho(u)$.
   (c) Soient $u, v \in \mathbb{M}$. Supposons qu'il existe $w, z \in \mathbb{M}$ tels que $u \in \mathbb{M}wv\mathbb{M} \cap \mathbb{M}vz\mathbb{M}$ et $u \notin \mathbb{M}wvz\mathbb{M}$. Montrer que, dans ce cas, $\rho(v) > \rho(u)$.
8. Soit $\mu : \Sigma^* \longrightarrow \mathbb{M}$ un morphisme de Σ^* dans un monoïde apériodique fini $\mathbb{M}$. Soit $m \in \mathbb{M}$. On pose :

$$U_\mu(m) \overset{\text{def}}{=} \bigcup_{\substack{(a,n) \in \Sigma \times \mathbb{M} \\ n\mu(a)\mathbb{M} = m\mathbb{M} \\ n \notin m\mathbb{M}}} \mu^{-1}(n)a \qquad V_\mu(m) \overset{\text{def}}{=} \bigcup_{\substack{(a,n) \in \Sigma \times \mathbb{M} \\ \mathbb{M}\mu(a)n = \mathbb{M}m \\ n \notin \mathbb{M}m}} a\mu^{-1}(n)$$

$$W_\mu(m) \overset{\text{def}}{=} \Big\{a \in \Sigma \;\Big|\; m \notin \mathbb{M}a\mathbb{M}\Big\} \cup \left(\bigcup_{\substack{(a,b,n) \in \Sigma \times \Sigma \times \mathbb{M} \\ m \in \mathbb{M}\mu(a)n\mathbb{M} \cap \mathbb{M}n\mu(b)\mathbb{M} \\ m \notin \mathbb{M}\mu(a)n\mu(b)\mathbb{M}}} a\mu^{-1}(n)b \right)$$

   (a) Soit $m \in \mathbb{M}$ tel que $m \neq 1$. Soit $x \in \Sigma^*$ tel que $\mu(x) \in mM$. Démontrer que x se factorise sous la forme uay, avec $\mu(u) \notin m\mathbb{M}, \mu(ua) \in m\mathbb{M}$. On pose $n \overset{\text{def}}{=} \mu(u)$. Établir une réciproque.
   (b) On démontre de la même façon que $x \in \Sigma^*$ est tel que $\mu(x) \in \mathbb{M}m$ si et seulement s'il se factorise sous la forme $u'a'v'$ avec $\mu(v') \notin \mathbb{M}m$ et $\mu(a'v') \in \mathbb{M}m$. Démontrer que $m \notin \mathbb{M}\mu(x)\mathbb{M}$ si et seulement si $x \notin \Sigma^* W \Sigma^*$.
   (c) Conclure par récurrence sur $\rho(\mathbb{M})$.

Exercice 11 (Groupes libres)

On note $\overline{\Sigma}$ une copie de Σ définie par $\overline{\Sigma} \overset{\text{def}}{=} \big\{\overline{a} \mid a \in \Sigma\big\}$. Pour chaque lettre $a \in \Sigma$, on note $\overline{\overline{a}} = a$. L'application $x \longrightarrow \overline{x}$ ainsi définit une involution de $\Sigma \sqcup \overline{\Sigma}$ qui échange Σ et $\overline{\Sigma}$.

On note $\mathbb{L}$ le monoïde libre sur l'alphabet $\Sigma \sqcup \overline{\Sigma}$.

On définit les deux *opérations élémentaires* sur un mot $u = u_1 u_2 \dots u_p$, avec $u_i \in \Sigma \sqcup \overline{\Sigma}$ suivantes :

- **(Insertion)** $I(u, a, i) \overset{\text{def}}{=} u_1 u_2 \dots u_i\, a\overline{a}\, u_{i+1} \dots u_p$ pour $i \in [\![0; p]\!]$ et $a \in \Sigma \sqcup \overline{\Sigma}$.
- **(Suppression)** $S(u) = u_1 u_2 \dots u_{i-1} u_{i+2} \dots u_p$ pour $i \in [\![1; p-1]\!]$ tel que $u_{i+1} = \overline{u_i}$.

1. On définit sur $\mathbb{L}$ une relation en posant, pour $w, w' \in \mathbb{L}$ $w \sim_{\mathbb{L}} w'$ lorsqu'il existe une suite finie de mots $(w_i)_{i=1}^n$ tels que $w_1 = w$, $w_n = w'$ et, pour $i \in [\![1; n-1]\!]$, w_{i+1} est obtenu à partir de w_i par une opération élémentaire. Démontrer que $\sim_{\mathbb{L}}$ est une congruence.
2. On dit qu'un mot $w \in \big(\Sigma \sqcup \overline{\Sigma}\big)^*$ est *réduit* lorsque l'on ne peut pas faire de suppression.
   (a) Démontrer que toute classe de congruence contient un mot réduit.
   (b) On se propose de justifier que toute classe de congruence contient un unique mot réduit. Soient w et w' deux mots réduits congruents. Soit $(w_i)_{i=1}^n$ une suite de la définition de la relation de congruence $\sim_{\mathbb{L}}$ et telle que $\sum_{i=1}^{n} |w_i|$ est minimal parmi les suites finies de mots vérifiant cette propriété. On suppose $w \neq w'$ *i.e.* $n > 1$.

(*i*) Justifier que $|w| < |w_2|$ et $|w'| < |w_{n-1}|$.

(*ii*) En déduire qu'il existe $i \in [\![2; n-1]\!]$ tel que w_i obtenu à partir de w_{i-1} à partir d'une insertion et w_{i+1} est obtenu à partir de w_i à partir d'une suppression.

(*iii*) Soient $a, b \in \Sigma \sqcup \overline{\Sigma}$ et $k, j \in [\![1; p-1]\!]$ tels que : $w_{i-1} = u_1 \dots u_p$, $w_i = u_1 \dots u_k a\overline{a} u_{k+1} \dots u_p = v_1 \dots v_{p+2}$ et $w_{i+1} = v_1 \dots v_{j-1} v_{j+1} \dots v_{p+2}$ avec $v_j = b$ et $V_{j+1} = \overline{b}$. En étudiant les cas où ces deux opérations se chevauchent ou non, aboutir à une contradiction.

3. On note $\mathbb{GF}$ le monoïde $\mathbb{L}/\sim_{\mathbb{L}}$ et σ la surjection canonique de $\mathbb{L}$ sur $\mathbb{GF}$.
   (a) Démontrer que σ injecte Σ dans $\mathbb{GF}$.
   (b) Démontrer que $\mathbb{GF}$ est le groupe engendré par $\sigma(\Sigma)$.
   (c) Quel est ce groupe lorsque Σ est un singleton ?
4. Soit $\phi : \Sigma \longrightarrow \mathbb{G}$ avec $\mathbb{G}$ un groupe. On étend ϕ sur $\overline{\Sigma}$ en posant $\phi(\overline{u}) = \phi(u)^{-1}$, pour tout $u \in \Sigma$. Démontrer qu'il existe un unique morphisme de groupes de $\mathbb{GF}$ dans $\mathbb{G}$ prolongeant ϕ.
5. On note $\mathbb{L}_R$ l'ensemble des mots réduits.
   (a) Démontrer que tout facteur d'un mot réduit est réduit.
   (b) Soit $u \in \Sigma$. Justifier que l'on peut définir une application π_u de $\mathbb{L}_R$ dans lui-même en posant :

$$\begin{array}{cccc} \pi_u & \mathbb{L}_R & \longrightarrow & \mathbb{L}_R \\ & w & \longmapsto & \begin{cases} uw & \textbf{si } uw \in \mathbb{L}_R, \\ v & \textbf{si } w = \overline{u}v. \end{cases} \end{array}$$

   (c) Démontrer que π_u est une permutation de $\mathbb{L}_R$.
   (d) Soit $\pi : \Sigma \longrightarrow \mathfrak{S}(\mathbb{L}_R)$ l'application définie par, pour tout $u \in \Sigma$, $\pi(u) = \pi_u$. On note $\hat{\pi}$ le morphisme de groupes prolongeant π à $\mathbb{L}$. Si $w \in \mathbb{L}_R$, démontrer que $\pi_w(\varepsilon) = w$.
   (e) Retrouver ainsi l'unicité du mot réduit dans une classe de congruence.