DM Langages Formels

À rendre le jeudi 14 mars

Soit Σ un alphabet fini. On considère une extension des expressions régulières avec l'opération d'inverse : soit $\mathrm{Reg}(\Sigma, {}^{-1})$ l'ensemble des expressions

$$e ::= 0 \mid 1 \mid a \mid e + e \mid e \cdot e \mid e^* \mid e^{-1}\,, \qquad \text{où } a \in \Sigma\,.$$

On note aussi $\mathrm{Reg}(\Sigma)$ l'ensemble des expressions qui n'utilisent pas ${}^{-1}$, i.e., des expressions régulières usuelles.

Une expression e est interprétée comme une *relation* sur un ensemble E. Plus précisément, étant donné un ensemble E et une interprétation $\sigma : \Sigma \to \mathcal{P}(E \times E)$ qui associe à chaque lettre une relation binaire sur E, on définit inductivement une extension $\sigma : \mathrm{Reg}(\Sigma, {}^{-1}) \to \mathcal{P}(E \times E)$ de σ aux expressions comme suit :

$$\begin{aligned}
\sigma(0) &= \emptyset \\
\sigma(1) &= \{(x, x) \mid x \in E\} \\
\sigma(a) &= \sigma(a) \\
\sigma(e + f) &= \sigma(e) \cup \sigma(f) \\
\sigma(e \cdot f) &= \sigma(e) \cdot \sigma(f) = \{(x, z) \in E \times E \mid \exists y, (x, y) \in \sigma(e) \wedge (y, z) \in \sigma(f)\} \\
\sigma(e^*) &= \sigma(e)^* = \{(x, y) \in E \times E \mid \exists n \geq 0, \exists x_0 = x, x_1, \ldots, x_n = y, \\
&\qquad\qquad \forall\, 0 \leq i < n, (x_i, x_{i+1}) \in \sigma(e)\} \\
\sigma(e^{-1}) &= \sigma(e)^{-1} = \{(x, y) \in E \times E \mid (y, x) \in \sigma(e)\}\,.
\end{aligned}$$

En particulier, pour un mot $u = a_0 a_1 \cdots a_{n-1} \in \Sigma^*$, $\sigma(u) = \sigma(a_0) \cdot \sigma(a_1) \cdots \sigma(a_{n-1})$.

On dit que deux expressions e et f sont équivalentes, noté $e \equiv f$, si pour tout ensemble E et pour toute interprétation $\sigma : \Sigma \to \mathcal{P}(E \times E)$, on a $\sigma(e) = \sigma(f)$. On note également $e \subseteq f$ si pour tous E et $\sigma : \Sigma \to \mathcal{P}(E \times E)$, on a $\sigma(e) \subseteq \sigma(f)$.

On s'intéresse au problème de décider si deux expressions sont équivalentes.

1 Expressions régulières

On considère d'abord le cas d'expressions régulières construites sans l'opérateur ${}^{-1}$. On définit le langage $L(e) \subseteq \Sigma^*$ d'une expression de manière usuelle :

$$\begin{array}{ccc}
L(0) = \emptyset & L(1) = \{\varepsilon\} & L(a) = \{a\} \\
L(e_1 + e_2) = L(e_1) \cup L(e_2) & L(e_1 \cdot e_2) = L(e_1) \cdot L(e_2) & L(e^*) = L(e)^*\,.
\end{array}$$

Question 1.

(a) Montrer que pour tout ensemble E et pour toute interprétation $\sigma : \Sigma \to \mathcal{P}(E \times E)$, pour toute expression régulière $e \in \mathrm{Reg}(\Sigma)$, on a

$$\sigma(e) = \bigcup_{v \in L(e)} \sigma(v)\,.$$

Correction :
On prouve le résultat par induction sur e :

— $\sigma(0) = \emptyset = \bigcup_{v\in\emptyset} \sigma(v)$

— $\sigma(1) = \{(x,x) \mid x \in E\} = \sigma(\varepsilon) = \bigcup_{v\in\{\varepsilon\}} \sigma(v)$

— $\sigma(a) = \bigcup_{v\in\{a\}} \sigma(v)$

— $\sigma(e_1 + e_2) = \sigma(e_1) \cup \sigma(e_2) = \bigcup_{v\in L(e_1)} \sigma(v) \cup \bigcup_{v\in L(e_2)} \sigma(v) = \bigcup_{v\in L(e_1+e_2)} \sigma(v)$

— $\sigma(e_1 \cdot e_2) = \sigma(e_1) \cdot \sigma(e_2) = \left(\bigcup_{v\in L(e_1)} \sigma(v)\right) \cdot \left(\bigcup_{v\in L(e_2)} \sigma(v)\right)$
$= \bigcup_{v_1\in L(e_1), v_2\in L(e_2)} \sigma(v_1) \cdot \sigma(v_2)$
$= \bigcup_{v_1\in L(e_1), v_2\in L(e_2)} \sigma(v_1 \cdot v_2) = \bigcup_{v\in L(e_1\cdot e_2)} \sigma(v)$

— $\sigma(e^*) = \sigma(e)^* = \left(\bigcup_{v\in L(e)} \sigma(v)\right)^*$
$= \bigcup_{n\geq 0, v_1,\ldots,v_n\in L(e)} \sigma(v_1)\cdots\sigma(v_n) = \bigcup_{v\in L(e^*)} \sigma(v)\,.$

(b) Montrer que pour toutes expressions régulières $e, f \in \mathrm{Reg}(\Sigma)$, on a $e \equiv f$ si et seulement si $L(e) = L(f)$.

Correction :
Si $L(e) = L(f)$, alors pour tout σ, $\sigma(e) = \bigcup_{v\in L(e)} \sigma(v) = \bigcup_{v\in L(f)} \sigma(v) = \sigma(f)$.
Réciproquement, supposons que $e \equiv f$. Soit $u = a_0 \ldots a_{n-1} \in L(e)$. On pose $E = \{0, \ldots, n\}$, et on définit $\sigma : \Sigma \to \mathcal{P}(E \times E)$ par

$$\sigma(a) = \{(i, i+1) \mid 0 \leq i < n \wedge a_i = a\}\,.$$

On a $(0,n) \in \sigma(u) \subseteq \sigma(e) = \sigma(f)$, donc il existe $v = b_0 \ldots b_{k-1} \in L(f)$ tel que $(0,n) \in \sigma(v) = \sigma(b_0)\cdots\sigma(b_{k-1})$. Par définition, il existe $(i_0, i_1) \in \sigma(b_0), (i_1, i_2) \in \sigma(b_1), \ldots, (i_{k-1}, i_k) \in \sigma(b_{k-1})$ tels que $i_0 = 0$ et $i_k = n$. On a alors nécessairement $i_{j+1} = i_j + 1$ pour tout j, i.e., $i_j = j$ pour tout $0 \leq j \leq k$, et $k = n$. De plus $(j, j+1) \in \sigma(b_j)$ implique que $b_j = a_j$. Donc $v = u$.

2 Expressions avec inverse

On dit qu'une expression $e \in \mathrm{Reg}(\Sigma, {}^{-1})$ est *normalisée* si l'utilisation de ${}^{-1}$ est restreinte aux expressions atomiques, i.e., si e est de la forme :

$$e ::= 0 \mid 1 \mid a \mid a^{-1} \mid e + e \mid e \cdot e \mid e^* \,, \qquad \text{où } a \in \Sigma \,.$$

Question 2. Montrer que pour toute expression $e \in \mathrm{Reg}(\Sigma, {}^{-1})$, il existe une expression normalisée $e' \in \mathrm{Reg}(\Sigma, {}^{-1})$ telle que $e \equiv e'$.

Correction :
On montre le résultat par induction sur la taille de e, en utilisant les équivalences ci-dessous :

$$0^{-1} \equiv 0 \qquad 1^{-1} \equiv 1 \qquad (f^{-1})^{-1} \equiv f$$
$$(f \cdot g)^{-1} \equiv g^{-1} \cdot f^{-1} \qquad (f^*)^{-1} \equiv (f^{-1})^* \qquad (f + g)^{-1} \equiv f^{-1} + g^{-1} \,.$$

Question 3. On considère les expressions

$$e_1 = a \qquad e_2 = aa^{-1}a \qquad e_3 = bb^{-1}a$$

Pour tous $i, j \in \{1, 2, 3\}$, a-t-on $e_i \subseteq e_j$? Dans chaque cas, donner une preuve que l'inclusion est valide ou un contre-exemple.

Correction :
On a trivialement $e_i \subseteq e_i$ pour tout i. La seule autre inclusion valide est $e_1 \subseteq e_2$. En effet, pour tout $\sigma : \Sigma \to \mathcal{P}(E \times E)$ et $(x, y) \in \sigma(e_1)$, on a $(x, y) \in \sigma(a)$ et $(y, x) \in \sigma(a^{-1})$, donc $(x, x) \in \sigma(a) \cdot \sigma(a^{-1})$, et à nouveau $(x, y) \in \sigma(a)$ donc $(x, y) \in (\sigma(a) \cdot \sigma(a^{-1})) \cdot \sigma(a) = \sigma(e_2)$.
Pour montrer que les autres inclusions ne sont pas valides, on peut prendre par exemple $E = \{0, \ldots, 6\}$, $\sigma(a) = \{(0, 1), (2, 1), (2, 3), (5, 6))\}$, et $\sigma(b) = \{(3, 4), (5, 4)\}$:

$$0 \xrightarrow{a} 1 \xleftarrow{a} 2 \xrightarrow{a} 3 \xrightarrow{b} 4 \xleftarrow{b} 5 \xrightarrow{a} 6$$

On a $(0, 1) \in \sigma(e_1)$ mais $(0, 1) \notin \sigma(e_3)$; $(0, 3) \in \sigma(e_2)$ mais $(0, 3) \notin \sigma(e_1)$ et $(0, 3) \notin \sigma(e_3)$; et $(3, 6) \in \sigma(e_3)$ mais $(3, 6) \notin \sigma(e_1)$ et $(3, 6) \notin \sigma(e_2)$.

On définit une copie $\overline{\Sigma}$ de Σ, qu'on suppose disjointe de Σ :

$$\overline{\Sigma} = \{\overline{a} \mid a \in \Sigma\} \,.$$

Pour $a \in \Sigma$, on notera $\overline{(\overline{a})} = a$. Pour tous E et $\sigma : \Sigma \to \mathcal{P}(E \times E)$, on définit une extension $\overline{\sigma} : (\Sigma \cup \overline{\Sigma}) \to \mathcal{P}(E \times E)$ de σ à $\Sigma \cup \overline{\Sigma}$, en posant, pour tout $a \in \Sigma$,

$$\overline{\sigma}(a) = \sigma(a)\,, \quad \text{et} \quad \overline{\sigma}(\overline{a}) = (\sigma(a))^{-1}\,.$$

Pour toute expression $e \in \mathrm{Reg}(\Sigma, {}^{-1})$, on fixe une expression normalisée e' telle que $e \equiv e'$. On note $\tau(e) \in \mathrm{Reg}(\Sigma \cup \overline{\Sigma})$ l'expression régulière sur $\Sigma \cup \overline{\Sigma}$ obtenue en substituant toute occurence de a^{-1} dans e' par $\overline{a}$. Par exemple, $\tau((a + b^{-1})b(b^{-1}a^{-1})^*ab) = (a + \overline{b})b(\overline{b}\overline{a})^*ab$.

Question 4. Soit E un ensemble, et $\sigma : \Sigma \to \mathcal{P}(E \times E)$. Montrer que pour tout $e \in \mathrm{Reg}(\Sigma, {}^{-1})$,

$$\sigma(e) = \overline{\sigma}(\tau(e)) = \bigcup_{u \in L(\tau(e))} \overline{\sigma}(u)\,.$$

Correction :
Par induction immédiate sur e', on a $\sigma(e') = \overline{\sigma}(\tau(e))$, d'où $\sigma(e) = \overline{\sigma}(\tau(e))$. On obtient la seconde égalité en appliquant la question 1 à $\tau(e)$.

Question 5. Montrer que si $\tau(e) \equiv \tau(f)$ alors $e \equiv f$, mais que la réciproque n'est pas vraie : donner un exemple d'expressions e et f telles que $e \equiv f$, mais $\tau(e) \not\equiv \tau(f)$.

Correction :
Si $\tau(e) \equiv \tau(f)$, alors pour tout $\sigma : \Sigma \to \mathcal{P}(E \times E)$, on a $\overline{\sigma}(\tau(e)) = \overline{\sigma}(\tau(f))$, et d'après la question 4, $\sigma(e) = \sigma(f)$. Par contre, on a $aa^{-1}a + a \equiv aa^{-1}a$, mais $a\overline{a}a + a \not\equiv a\overline{a}a$ car $a \notin L(a\overline{a}a)$.

Soit $u = a_0 \dots a_{n-1} \in (\Sigma \cup \overline{\Sigma})^*$, où $a_i \in \Sigma \cup \overline{\Sigma}$ pour tout $0 \leq i < n$. On peut voir u comme un mot ou comme une expression sur $\Sigma \cup \overline{\Sigma}$, mais aussi comme un modèle dans lequel on pourra évaluer les expressions. Plus précisément, on associe à e l'ensemble $E_u = \{0, \dots, n\}$, et l'interprétation $\sigma_u : \Sigma \to \mathcal{P}(E_u \times E_u)$ définie par

$$\sigma_u(a) = \{(i, i+1) \mid 0 \leq i < n \wedge a_i = a\} \cup \{(i+1, i) \mid 0 \leq i < n \wedge a_i = \overline{a}\}\,.$$

Comme au dessus, on notera $\overline{\sigma_u} : \Sigma \cup \overline{\Sigma} \to \mathcal{P}(E_u \times E_u)$ son extension à $\Sigma \cup \overline{\Sigma}$: pour tout $a \in \Sigma$,

$$\overline{\sigma_u}(a) = \{(i, i+1) \mid 0 \leq i < n \wedge a_i = a\} \cup \{(i+1, i) \mid 0 \leq i < n \wedge a_i = \overline{a}\}$$
$$\overline{\sigma_u}(\overline{a}) = \{(i, i+1) \mid 0 \leq i < n \wedge a_i = \overline{a}\} \cup \{(i+1, i) \mid 0 \leq i < n \wedge a_i = a = \overline{(\overline{a})}\}\,.$$

Question 6. Soit $u = ab\overline{b}\overline{a}ab$, et $e = (a+b^{-1})b(b^{-1}a^{-1})^*ab$. Que vaut $\sigma_u(e)$? Aucune justification n'est demandée.

Correction :
$\sigma_u(e) = \{(0,2),(0,6),(2,2),(2,6),(4,2),(4,6),(6,2),(6,6)\}$.

Question 7. Soit $u, v \in (\Sigma \cup \overline{\Sigma})^*$. Montrer que les propositions suivantes sont équivalentes :

1. Pour tous E et $\sigma : \Sigma \to \mathcal{P}(E \times E)$, $\overline{\sigma}(u) \subseteq \overline{\sigma}(v)$.
2. $(0, |u|) \in \overline{\sigma_u}(v)$.

Correction :
On note $u = a_0 \dots a_{n-1}$, et $v = b_0 \dots b_{k-1}$.
Si (1) est vrai, alors en particulier $\overline{\sigma_u}(u) \subseteq \overline{\sigma_u}(v)$. Or pout tout $0 \leq i < n$, on a $(i, i+1) \in \overline{\sigma_u}(a_i)$, donc $(0,n) \in \overline{\sigma_u}(a_0) \cdots \overline{\sigma_u}(a_{n-1}) = \overline{\sigma_u}(u)$. Donc $(0,n) \in \overline{\sigma_u}(v)$.
Réciproquement, supposons que $(0,n) \in \overline{\sigma_u}(v)$, i.e., il existe $i_0 = 0, i_1, \dots, i_k = n$ tels que pour tout $0 \leq j < k$, on a $(i_j, i_{j+1}) \in \overline{\sigma_u}(b_j)$. Soit E un ensemble, et $\sigma : \Sigma \to \mathcal{P}(E \times E)$.
Soit $(x,y) \in \overline{\sigma}(u) = \overline{\sigma}(a_0) \cdots \overline{\sigma}(a_{n-1})$. Il existe $x_0 = x, x_1, \dots, x_n = y$ tels que pour tout $0 \leq i < n$, $(x_i, x_{i+1}) \in \overline{\sigma}(a_i)$. Pour tout $0 \leq j \leq k$, on pose $y_j = x_{i_j}$. En particulier, $y_0 = x$ et $y_k = y$. Soit $0 \leq j < k$. Montrons que $(y_j, y_{j+1}) \in \overline{\sigma}(b_j)$. On sait que $(i_j, i_{j+1}) \in \overline{\sigma_u}(b_j)$. Par définition de $\overline{\sigma_u}(b_j)$, on a

— soit $(i_j, i_{j+1}) = (i_j, i_j + 1)$ et $a_{i_j} = b_j$,

— soit $(i_j, i_{j+1}) = (i_{j+1} + 1, i_{j+1})$ et $a_{i_{j+1}} = \overline{b_j}$.

Dans le premier cas, on a

$$(y_j, y_{j+1}) = (x_{i_j}, x_{i_j+1}) \in \overline{\sigma}(a_{i_j}) = \overline{\sigma}(b_j)\,.$$

Dans le second cas, on a

$$(y_j, y_{j+1}) = (x_{i_{j+1}+1}, x_{i_{j+1}}) \in (\overline{\sigma}(a_{i_{j+1}}))^{-1} = \overline{\sigma}(\overline{a_{i_{j+1}}}) = \overline{\sigma}(b_j)\,.$$

D'où $(y_j, y_{j+1}) \in \overline{\sigma}(b_j)$, et $(x,y) = (y_0, y_k) \in \overline{\sigma}(b_0) \cdots \overline{\sigma}(b_{k-1}) = \overline{\sigma}(v)$.

Question 8. Soit $e, f \in \mathrm{Reg}(\Sigma, {}^{-1})$. Montrer que les propositions suivantes sont équivalentes :

1. $e \equiv f$.
2. Pour tout $u \in (\Sigma \cup \overline{\Sigma})^*$, $\sigma_u(e) = \sigma_u(f)$.
3. Pour tout $u \in (\Sigma \cup \overline{\Sigma})^*$, $(0, |u|) \in \sigma_u(e)$ si et seulement si $(0, |u|) \in \sigma_u(f)$.

Correction :
On a triviallement (1) $\implies$ (2) $\implies$ (3). Montrons (3) $\implies$ (1). Supposons que pour tout $u \in (\Sigma \cup \overline{\Sigma})^*$, $(0, |u|) \in \sigma_u(e)$ si et seulement si $(0, |u|) \in \sigma_u(f)$. Soit E un ensemble, et $\sigma : \Sigma \to \mathcal{P}(E \times E)$. On veut montrer que $\sigma(e) = \sigma(f)$.
Soit $(x, y) \in \sigma(e)$. D'après la question 4, il existe $u \in L(\tau(e))$ tel que $(x, y) \in \overline{\sigma}(u)$. D'après la question 7, on a $(0, |u|) \in \overline{\sigma_u}(u) \subseteq \overline{\sigma_u}(e)$. Par hypothèse, on a donc aussi $(0, |u|) \in \overline{\sigma_u}(f)$, i.e., il existe $v \in L(\tau(f))$ tel que $(0, |u|) \in \overline{\sigma_u}(v)$. D'après la question 7, on a alors $\overline{\sigma}(u) \subseteq \overline{\sigma}(v)$. Donc $(x, y) \in \overline{\sigma}(v) \subseteq \sigma(f)$. Donc $\sigma(e) \subseteq \sigma(f)$, et par symétrie, $\sigma(e) = \sigma(f)$.

Un *automate à double sens* (ou *automate boustrophédon*) est un automate fini non-déterministe qui, à chaque transition, peut déplacer sa tête de lecture vers la droite ou vers la gauche. Avant une transition, la tête de lecture de l'automate se situe entre deux lettres, et, selon qu'il se déplace vers la gauche ou vers la droite, l'automate va lire la lettre située à sa gauche ou à sa droite. [1]

Plus formellement, un automate à double sens sur un alphabet Σ est un quadruplet $\mathcal{B} = (Q, T, I, F)$, où

— Q est un ensemble fini d'états,

— $I \subseteq Q$ est un ensemble d'états initiaux,

— $F \subseteq Q$ est un ensemble d'états acceptants,

— $T \subseteq Q \times \{\rightarrow, \leftarrow\} \times \Sigma \times Q$ est un ensemble de transitions.

Soit $u = a_0 \dots a_{n-1} \in \Sigma^*$. Un *calcul* de $\mathcal{B}$ sur u est une suite $(q_0, i_0), \dots, (q_k, i_k)$ telle que pour tout $0 \leq j \leq k$, $(q_j, i_j) \in Q \times \{0, \dots, n\}$, et si $j < k$:

— soit $i_{j+1} = i_j + 1$ et $(q_j, \rightarrow, a_{i_j}, q_{j+1}) \in T$,

— soit $i_{j+1} = i_j - 1$ et $(q_j, \leftarrow, a_{i_j - 1}, q_{j+1}) \in T$.

Un calcul de $\mathcal{B}$ est *acceptant* si $i_0 = 0$, $i_k = n$, $q_0 \in I$, et $q_k \in F$. Le langage accepté par $\mathcal{B}$, noté $L(\mathcal{B})$, est l'ensemble des mots $u \in \Sigma^*$ tels que $\mathcal{B}$ a un calcul acceptant sur u.

On admet temporairement le résultat suivant (prouvé dans la section 3) :

Théorème 1. *Pour tout automate à double sens $\mathcal{B}$ avec n états, on peut construire effectivement un automate déterministe classique $\mathcal{A}$ avec $2^{O(n^2)}$ états tel que $L(\mathcal{A}) = L(\mathcal{B})$. De plus, la construction de $\mathcal{A}$ est dans* PSPACE.

1. Remarque : une autre définition, plus usuelle, consiste à considérer que la tête de lecture de l'automate est positionnée sur une lettre, et que la lettre lue ne dépend pas de la direction de déplacement (comme dans une machine de Turing). On peut aussi ajouter des marqueurs de début et de fin pour permettre à l'automate de tester s'il a atteint le début ou la fin du mot. Toutefois, toutes ces définitions ont le même pouvoir d'expression.

Pour tout $e \in \mathrm{Reg}(\Sigma, {}^{-1})$, on note $\mathcal{A}_e = (Q_e, T_e, I_e, F_e)$ un automate fini sur $\Sigma \cup \overline{\Sigma}$ tel que $L(\mathcal{A}_e) = L(\tau(e))$. On lui associe un automate à double sens $\mathcal{B}_e = (Q_e, U_e, I_e, F_e)$ sur $\Sigma \cup \overline{\Sigma}$, défini par

$$U_e = \{(q, \to, a, q') \mid (q, a, q') \in T_e\} \cup \{(q, \leftarrow, \overline{a}, q') \mid (q, a, q') \in T_e\}\,.$$

Chaque transition de $\mathcal{A}_e$ sur une lettre $a \in \Sigma \cup \overline{\Sigma}$ donne donc lieu à deux transitions dans $\mathcal{B}_e$: une transition vers la droite sur a, et une transition vers la gauche sur $\overline{a}$.

Question 9. Montrer que

$$L(\mathcal{B}_e) = \{u \in (\Sigma \cup \overline{\Sigma})^* \mid (0, |u|) \in \sigma_u(e)\}\,.$$

Correction :
Soit $u = a_0 \dots a_{n-1} \in (\Sigma \cup \overline{\Sigma})^*$.
Supposons que $u \in L(\mathcal{B}_e)$. Soit $(q_0, i_0), \dots, (q_k, i_k)$ un calcul acceptant de $\mathcal{B}_e$ sur u. En particulier, $i_0 = 0$, $q_0 \in I_e$, $i_k = |u|$, et $q_k \in F_e$. Pour tout $j \in \{0, \dots, k-1\}$, on note

$$b_j = \begin{cases} a_{i_j} & \text{si } i_{j+1} = i_j + 1 \\ \overline{a_{i_j - 1}} & \text{si } i_{j+1} = i_j - 1\,. \end{cases}$$

Par définition de $\mathcal{B}_e$, pour tout $j \in \{0, \dots, k-1\}$, on a :

— soit $i_{j+1} = i_j + 1$, et $(q_j, \to, a_{i_j}, q_{j+1}) \in U_e$, i.e., $(q_j, a_{i_j}, q_{j+1}) \in T_e$,

— soit $i_{j+1} = i_j - 1$, et $(q_j, \leftarrow, a_{i_j - 1}, q_{j+1}) \in U_e$, i.e., $(q_j, \overline{a_{i_j - 1}}, q_{j+1}) \in T_e$.

Dans les deux cas, on a $(q_j, b_j, q_{j+1}) \in T_e$. Donc

$$q_0 \xrightarrow{b_0} \cdots \xrightarrow{b_{k-1}} q_k$$

est un calcul acceptant de $\mathcal{A}_e$, et $b_0 \dots b_{k-1} \in L(\tau(e))$. De plus, pour tout $0 \leq j < k$, on a $(i_j, i_{j+1}) \in \overline{\sigma_u}(b_j)$ par définition de σ_u et b_j. On a donc $(0, n) = (i_0, i_k) \in \overline{\sigma_u}(b_0 \dots b_{k-1}) \subseteq \sigma_u(e)$.

Réciproquement, supposons que $(0,n) \in \sigma_u(e)$. Il existe $v = b_0 \cdots b_{k-1} \in L(\tau(e))$ tel que $(0,n) \in \overline{\sigma_u}(v)$. Il existe $i_0 = 0, i_1, \ldots, i_k = n$ tels que pour tout $0 \leq j < k$, $(i_j, i_{j+1}) \in \overline{\sigma_u}(b_j)$. Soit

$$q_0 \xrightarrow{b_0} \cdots \xrightarrow{b_{k-1}} q_k$$

un calcul acceptant de $\mathcal{A}_e$ sur v. Montrons que

$$(q_0, i_0), \ldots, (q_k, i_k)$$

est un calcul acceptant de $\mathcal{B}_e$ sur u. On a $q_0 \in I_e$, $q_k \in F_e$, $i_0 = 0$, et $i_k = n$, donc il suffit de montrer que c'est un calcul de $\mathcal{B}_e$ sur u. Pour tout j, on a $(i_j, i_{j+1}) \in \overline{\sigma_u}(b_j)$, donc soit $i_{j+1} = i_j + 1$ et $a_{i_j} = b_j$, soit $i_{j+1} = i_j - 1$ et $a_{i_{j+1}} = \overline{b_j}$. Dans le premier cas, on a $(q_j, a_{i_j}, q_{j+1}) \in T_e$ et $(q_j, \rightarrow, a_{i_j}, q_{j+1}) \in U_e$. Dans le second cas, on a $(q_j, \overline{a_{i_{j+1}}}, q_{j+1}) \in T_e$, et $(q_j, \leftarrow, a_{i_{j+1}}, q_{j+1}) \in U_e$. D'où le résultat.

Question 10. Montrer que le problème de l'équivalence de deux expressions dans $\mathrm{Reg}(\Sigma, {}^{-1})$ est décidable. Quelle est sa complexité ?

Correction :
Pour tout $e, f \in \mathrm{Reg}(\Sigma, {}^{-1})$, on a

$$\begin{aligned} e \equiv f \quad &\underset{\text{(Q8)}}{\iff} \quad \{u \in (\Sigma \cup \overline{\Sigma})^* \mid (0, |u|) \in \sigma_u(e)\} = \{u \in (\Sigma \cup \overline{\Sigma})^* \mid (0, |u|) \in \sigma_u(f)\} \\ &\underset{\text{(Q9)}}{\iff} \quad L(\mathcal{B}_e) = L(\mathcal{B}_f)\,. \end{aligned}$$

À partir des expressions e et f, on peut construire en temps linéaire $\tau(e)$, $\mathcal{A}_e$, puis $\mathcal{B}_e$, et similairement, $\mathcal{B}_f$. D'après le Théorème 1, on peut alors construire un automate fini déterministe complet $\mathcal{A}'_e$ (resp. $\mathcal{A}'_f$) équivalent à $\mathcal{B}_e$ (resp. $\mathcal{B}_f$) de taille exponentielle. Finalement, on teste si $L(\mathcal{A}'_e) = L(\mathcal{A}'_f)$. Comme $\mathcal{A}'_e$ et $\mathcal{A}'_f$ sont déterministes et complets, il suffit de construire l'automate produit de $\mathcal{A}'_e$ et $\mathcal{A}'_f$, et de tester s'il contient un état accessible (p, q) tel que p est final dans $\mathcal{A}'_e$ mais q n'est pas final dans $\mathcal{A}'_f$, ou inversement. On obtient un algorithme en temps $2^{O(n^2)}$.
Plus précisément, le problème est en fait PSPACE-complet. La borne inférieure vient du problème de l'équivalence de deux expressions régulières classiques qui est déjà PSPACE-dur. Pour la borne supérieure, on n'a pas besoin de construire explicitement les automates $\mathcal{A}'_e$ puis $\mathcal{A}'_f$, puis leur produit ; on peut simplement deviner "au vol" un chemin dans l'automate produit, de longueur bornée par le nombre $(2^{O(n^2)})$ d'états, et tester s'il atteint un état (p, q) comme décrit au dessus. Pour cela, on maintient un compteur du nombre de transitions empruntées, et l'état courant de $\mathcal{A}'_e$ et $\mathcal{A}'_f$, ce qui nécessite un espace polynomial. On obtient une procédure dans NPSPACE = PSPACE.

3 Automates à double sens

On va maintenant prouver le Théorème 1.

Soit $\mathcal{B} = (Q, T, I, F)$ un automate à double-sens sur un alphabet Σ. Pour tout $u \in \Sigma^*$, on appelle

- $\lambda(u)$ l'ensemble des paires d'états $(q, q') \in Q \times Q$ telles qu'il existe un calcul de $\mathcal{B}$ sur u qui commence à gauche de u et finit à droite de u et va de l'état q à l'état q', i.e., un calcul de $\mathcal{B}$ sur u de la forme $(q_0, i_0), \ldots, (q_k, i_k)$ tel que $q_0 = q$, $i_0 = 0$, $q_k = q'$, et $i_k = |u|$; similairement,
- $\mu(u)$ l'ensemble des $(q, q') \in Q \times Q$ tels qu'il existe un calcul de $\mathcal{B}$ sur u de la forme $(q_0, i_0), \ldots, (q_k, i_k)$ avec $q_0 = q$, $i_0 = |u|$, $q_k = q'$, et $i_k = |u|$.

Pour $u, v \in \Sigma^*$, on note $u \sim v$ quand $(\lambda(u), \mu(u)) = (\lambda(v), \mu(v))$.

Question 11. Montrer que $\sim$ est une congruence à droite, c'est-à-dire une relation d'équivalence telle que pour tous $u, v, w \in \Sigma^*$, $u \sim v$ implique $uw \sim vw$.

Correction :
Soit $u, v, w \in \Sigma^*$ tels que $u \sim v$. Montrons que $\lambda(uw) \subseteq \lambda(vw)$. Par symétrie, on aura $\lambda(uw) = \lambda(vw)$. Soit $(q, q') \in \lambda(uw)$, et $\rho = (q_0, i_0), \ldots, (q_n, i_n)$ un calcul de $\mathcal{B}$ sur uw tel que $q_0 = q$, $i_0 = 0$, $q_n = q'$, $i_n = |uw|$. On peut décomposer ρ en

$$(q, 0), \rho_1, (q'_1, |u|), \rho_2, (q'_2, |u|), \cdots, \rho_n, (q'_n, |u|), \rho_{n+1}, (q', |uw|)$$

où ρ_k ne contient que des paires (q_j, i_j) telles que $0 \leq i_j \leq |u|$ si k est impair, ou $|u| \leq i_j \leq |uw|$ si k est pair (en particulier, $n + 1$ est pair). Pour tout k, on définit un calcul $\widetilde{\rho_k}$ de $\mathcal{B}$ sur vw comme suit :

- $(q, q'_1) \in \lambda(u) = \lambda(v)$, donc il existe un calcul de $\mathcal{B}$ sur v de la forme $(q, 0), \widetilde{\rho_1}, (q'_1, |v|)$.
- pour tout k pair, on peut définir un calcul $\widetilde{\rho_k}$ de $\mathcal{B}$ sur vw en remplaçant chaque paire (q_j, i_j) dans ρ_k par $(q_j, i_j - |u| + |v|)$ (car $|u| \leq i_j \leq |u| + |w|$).
- Pour tout $k \geq 3$ impair, $(q'_{k-1}, |u|), \rho_k, (q'_k, |u|)$ est un calcul de $\mathcal{B}$ sur u, donc $(q'_{k-1}, q'_k) \in \mu(u) = \mu(v)$, donc il existe un calcul $(q'_{k-1}, |v|), \widetilde{\rho_k}, (q'_k, |v|)$ de $\mathcal{B}$ sur v.

Alors

$$(q, 0), \widetilde{\rho_1}, (q'_1, |v|), \widetilde{\rho_2}, (q'_2, |v|), \cdots, \widetilde{\rho_n}, (q'_n, |v|), \widetilde{\rho_{n+1}}, (q', |vw|)$$

est un calcul de $\mathcal{B}$ sur vw. Donc $(q, q') \in \lambda(vw)$.
Similairement, $\mu(uw) = \mu(vw)$, donc $uw \sim vw$.

Question 12. Prouver le Théorème 1. On pourra construire un automate dont les états sont des classes d'équivalence de $\sim$.

Correction :
On note $[u]$ la classe d'équivalence d'un mot $u \in \Sigma^*$ par $\sim$. Soit $\mathcal{A} = (Q', \delta, i, F')$, avec

$$\begin{aligned} Q' &= \{[u] \mid u \in \Sigma^*\} & I' &= \{[\varepsilon]\} \\ \delta([u], a) &= [ua] & F' &= \{[u] \mid u \in L(\mathcal{B})\}\,. \end{aligned}$$

D'après la question 11, pour tout v tel que $[u] = [v]$, pour tout $a \in \Sigma$, on a $[ua] = [va]$, donc δ est bien définie. De plus, la fonction $[u] \mapsto (\lambda(u), \mu(u))$ est une injection de Q' dans $\mathcal{P}(Q \times Q)^2$, donc $Q' \leq 2^{2|Q|^2}$.
Montrons que $L(\mathcal{A}) = L(\mathcal{B})$. On remarque d'abord que $\sim$ sature $L(\mathcal{B})$: pour tout u, on a $u \in L(\mathcal{B})$ ssi $\lambda(u) \cap (I \times F) \neq \emptyset$, donc pour tout $u' \sim u$, $u \in L(\mathcal{B})$ ssi $u' \in L(\mathcal{B})$. De plus, par récurrence immédiate sur $|u|$, pour tout $u \in \Sigma^*$, on a $\delta(i, u) = [u]$. Donc

$$\begin{aligned} u \in L(\mathcal{A}) &\iff [u] \in F' \\ &\iff \exists u' \in L(B), [u] = [u'] \\ &\iff u \in L(\mathcal{B})\,. \end{aligned}$$

Finalement, pour construire $\mathcal{A}$ à partir de $\mathcal{B}$, on représente un état $[u]$ par le couple $(\lambda(u), \mu(u))$. On a $i = [\varepsilon] = (\{(q,q) \mid q \in Q\}, \{(q,q) \mid q \in Q\})$, et pour $(X, Y) \in Q'$, on peut vérifier que

$$\begin{aligned} \delta((X,Y), a) &= (X \cdot T_a^{\rightarrow} \cdot (T_a^{\leftarrow} \cdot Y \cdot T_a^{\rightarrow})^*,\ (T_a^{\leftarrow} \cdot Y \cdot T_a^{\rightarrow})^*) \\ &= (X \cdot T_a^{\rightarrow} \cdot (T_a^{\leftarrow} \cdot Y \cdot T_a^{\rightarrow})^{\leq |Q|},\ (T_a^{\leftarrow} \cdot Y \cdot T_a^{\rightarrow})^{\leq |Q|})\,. \end{aligned}$$

où $T_a^{\rightarrow} = \{(p,q) \mid (p, \rightarrow, a, q) \in T\}$ et $T_a^{\leftarrow} = \{(p,q) \mid (p, \leftarrow, a, q) \in T\}$.