Informatique II

La notation tient compte de la rigueur des raisonnements et de la clarté des explications.
Chaque question peut être traitée en admettant le résultat des questions précédentes.

Notations et définitions

Dans tout le problème, A est un alphabet fini et non vide. Les lettres de A seront en général notées $a, b, \ldots$ ou $a_1, a_2, \ldots$ On notera $|X|$ le cardinal d'un ensemble fini X.

Un *semigroupe* S est un ensemble non vide muni d'une loi de composition interne associative. Cette loi sera notée multiplicativement : à un couple $(s,t) \in S \times S$, elle associe l'élément st de S. L'associativité s'écrit donc : pour tous $s, t, u \in S$, on a $(st)u = s(tu)$.

Un *morphisme* d'un semigroupe S dans un semigroupe T est une application $f : S \to T$ telle que $f(st) = f(s)f(t)$ pour tous $s, t \in S$. Un semigroupe T est un *sous-semigroupe* d'un semigroupe S s'il existe un morphisme injectif de T dans S.

Si Σ est un alphabet (fini ou non), Σ^* désigne le monoïde libre sur Σ, *i.e.*, l'ensemble des mots sur l'alphabet Σ ; le semigroupe libre sur Σ est noté Σ^+ : c'est l'ensemble des mots non vides sur l'alphabet Σ. Le mot vide est désigné par 1.

Une *relation* $\sim$ sur un ensemble X est une partie de $X \times X$. On notera $x \sim y$ plutôt que $(x,y) \in \sim$. Une *relation d'équivalence* est une relation réflexive, transitive et symétrique. Une relation d'équivalence $\sim$ sur un semigroupe S est une *congruence* si pour tous $s, t, u \in S$, on a $s \sim t \Longrightarrow (us \sim ut$ et $su \sim tu)$.

I Reconnaissance par semigroupe

On dit qu'un langage $L \subseteq A^+$ est *reconnu par un semigroupe fini* S s'il existe un morphisme $f : A^+ \longrightarrow S$ et une partie P de S telle que $L = f^{-1}(P)$.

Soit $\mathscr{A} = \langle A, Q, F, q_0, \delta \rangle$ un automate fini déterministe complet sur un alphabet A, où Q est l'ensemble des états de $\mathscr{A}$, F l'ensemble des états finals, q_0 l'état initial et $\delta : Q \to Q$ la fonction de transition. À tout mot $w \in A^+$, on associe l'application

$$\begin{aligned} f_w : Q &\longrightarrow Q \\ q &\longmapsto \delta(q, w) \end{aligned}$$

I.1 Montrer que l'ensemble $S_{\mathscr{A}} = \{f_w | w \in A^+\}$ muni de la loi $f \cdot g = g \circ f$ est un semigroupe fini.

Solution *C'est un semigroupe car la composition des applications est associative, il est fini car inclus dans l'ensemble des applications de Q dans Q.* □

On appelle $S_{\mathscr{A}}$ le *semigroupe de transitions* de l'automate $\mathscr{A}$.

I.2 Montrer que si $L \subseteq A^+$ est le langage accepté par un automate fini déterministe complet $\mathscr{A}$, alors le semigroupe de transitions de $\mathscr{A}$ reconnaît L.

Solution *Soit*

$$\begin{aligned} f : A^+ &\longrightarrow S_{\mathscr{A}} \\ w &\longmapsto f_w \end{aligned}$$

et soit $P = f(L)$. Pour $q \in Q$, on a $f_w f_v(q) = \delta(\delta(q,v), w) = \delta(q, vw) = f_{vw}(q)$. Donc $f(v)f(w) = f_w f_v = f_{vw} = f(vw)$ et l'application f est un morphisme. On a de façon évidente : $L \subseteq f^{-1}(P)$. Inversement, soit $w \in f^{-1}(P)$. Par définition de P, il existe un mot $v \in L$ tel que $f(v) = f(w)$, c'est-à-dire $f_v = f_w$. Comme $v \in L$, l'état $\delta(q_0, v)$ est final. Or $f_v(q_0) = f_w(q_0)$, soit $\delta(q_0, v) = \delta(q_0, w)$. L'état $\delta(q_0, w)$ est donc final, d'où $w \in L$. Donc $L = f^{-1}(P)$, et L est donc bien reconnu par $S_{\mathscr{A}}$. □

I.3 Montrer qu'un langage est rationnel si et seulement si il est reconnu par un semigroupe fini.

Solution *Soit $L \subseteq A^+$, soit S un semigroupe fini, $P \subseteq S$ et $f : A^+ \to S$ un morphisme tel que $L = f^{-1}(P)$. Soit S^1 le semigroupe obtenu en ajoutant à S un nouvel élément $1_S \notin S$, tel que : $1_S s = s 1_S = s$ pour tout $s \in S \cup \{1_S\}$. Soit $\mathscr{A}_S = \{A, S^1, P, 1_S, \delta\}$ l'automate sur A dont l'ensemble d'états est S^1, dont l'ensemble des états finals est P et dont l'état initial est 1_S. La fonction de transition δ est définie par*

$$\delta(s, a) = s \cdot f(a)$$

Par une récurrence facile sur $|w|$, on montre que $\delta(s, w) = s \cdot f(w)$ pour tout $w \in A^+$. Soit $w \in A^+$ un mot accepté par $\mathscr{A}_S$. On a donc $\delta(1_S, w) \in P$, soit $f(w) \in P$, donc $w \in L = f^{-1}(P)$. Inversement si $w \in L$, on a $\delta(1_S, w) = f(w) \in P$: w est donc bien accepté par $\mathscr{A}_S$.

Inversement, on a montré en I.2 que tout langage rationnel est reconnu par le semigroupe de transitions (fini) de n'importe quel automate qui le reconnaît. □

Si $L \subseteq A^+$, la *congruence syntaxique* de L est la relation $\sim_L$ sur A^+ définie par :

$$x \sim_L y \iff (\forall z, t \in A^*,\ zxt \in L \Leftrightarrow zyt \in L)$$

I.4 Montrer que la relation $\sim_L$ est bien une congruence.

Solution *Le fait que $\sim_L$ est une relation d'équivalence est immédiat. Supposons que $x \sim_L y$ et que $u(xz)v \in L$. Alors, $ux(zv) \in L$ donc, puisque $x \sim_L y$, on a $uy(zv) \in L$, soit $u(yz)v \in L$. On a donc bien $x \sim_L y \Longrightarrow xz \sim_L yz$. On montre de même que $x \sim_L y \Longrightarrow zx \sim_L zy$. La relation $\sim_L$ est donc bien une congruence.* □

Soit $x/{\sim_L} = \{y \in A^+ \mid x \sim_L y\}$ la classe d'équivalence de x. On pose également $A^+/{\sim_L} = \{x/{\sim_L} \mid x \in A^+\}$.

I.5 Soit L un langage rationnel de A^+. Montrer que

a. l'ensemble $A^+/{\sim_L}$ est fini.

b. on peut munir $A^+/{\sim_L}$ d'une structure de semigroupe.

c. $A^+/{\sim_L}$ est un semigroupe fini qui reconnaît L.

Solution

a. Puisque L est rationnel, les quotients $z^{-1}Lt^{-1}$ sont en nombre fini. Or, on a

$$x \sim_L y \iff (\forall z, t \in A^*,\ x \in z^{-1}Lt^{-1} \Leftrightarrow y \in z^{-1}Lt^{-1})$$

ce qui montre immédiatement que les classes d'équivalence sont en nombre fini.

b. Il suffit de vérifier que si $x' \sim_L x$ et $y' \sim_L y$, alors $xy \sim_L x'y'$. Ceci résulte du fait que $\sim_L$ est une congruence : $xy \sim_L x'y \sim_L x'y'$. Poser $(xy)/{\sim_L} = (x/{\sim_L})(y/{\sim_L})$ a donc un sens, et l'associativité de cette loi interne sur $A^+/{\sim_L}$ vient de celle de la concaténation sur A^+.

c. Il résulte des deux points précédents que $A^+/{\sim_L}$ est un semigroupe fini. Il reste à vérifier qu'il reconnaît L. D'après la définition de $(xy)/{\sim_L}$, la fonction f_L de A^+ dans $A^+/{\sim_L}$ qui à x associe $x/{\sim_L}$ est un morphisme. Par ailleurs, si $x \in L$ et si $y \sim_L x$, on a $1 \cdot x \cdot 1 \in L$, et donc $1 \cdot y \cdot 1 \in L$ par définition de la congruence syntaxique. Donc $L = f_L^{-1}(f_L(L))$, ce qui montre que $A^+/{\sim_L}$ reconnaît L. □

I.6 Soient $f : A^+ \to S$ et $g : A^+ \to T$ deux morphismes de semigroupes tels que

- f est surjectif ;
- pour tous $x, y \in A^+$, $f(x) = f(y) \Longrightarrow g(x) = g(y)$.

Montrer qu'il existe un morphisme $h : S \to T$ tel que $g = h \circ f$. Montrer de plus que si g est surjectif, alors h est surjectif.

Solution *Soient $x, y \in A^+$. Supposons que $f(x) = f(y)$. Ceci implique que $g(x) = g(y)$. La définition*

$$h(z) = g(x), \text{ où } x \text{ est choisi arbitrairement dans } A^+ \text{ tel que } z = f(x)$$

a donc un sens pour tout $z \in A^+$. On remarque que comme f est surjectif, l'existence de x est assurée et h est bien une application définie sur S. On a clairement $g(x) = h \circ f(x)$ pour tout $x \in f(A^+) = A^+$. Il reste à montrer que h est un morphisme. Soient $s, t \in S$. Comme f est surjectif, il existe $x, y \in A^+$ tels que $s = f(x)$ et $t = f(y)$. Puisque f est un morphisme, $st = f(xy)$. Donc $h(st) = h(f(xy)) = g(xy) = g(x)g(y) = h(f(x))h(f(y)) = h(s)h(t)$.

Enfin, supposons que g est surjectif. L'égalité $g = h \circ f$ montre alors que $h(f(A^+)) = g(A^+) = T$. Mais $f(A^+) = S$ car f est surjectif, donc $h(S) = T$ et h est surjectif. □

I.7 Soit S un semigroupe qui reconnaît un langage $L \subseteq A^+$. Soit $f : A^+ \to S$ un morphisme tel que $L = f^{-1}(P)$, où $P \subseteq S$. On note T le sous-semigroupe $f(A^+)$ de S. Montrer qu'il existe un morphisme surjectif de T dans $A^+/{\sim_L}$.

Solution *Le morphisme f est bien surjectif de A^+ dans T. D'après la question précédente, il suffit de montrer l'implication $f(x) = f(y) \Rightarrow f_L(x) = f_L(y)$, où $f_L : A^+ \to A^+/{\sim_L}$ est le morphisme (surjectif) qui envoie x sur $x/{\sim_L}$. Supposons donc que $f(x) = f(y)$. Soient $z, t \in A^*$. Puisque f est un morphisme, on a $f(zxt) = f(zyt)$. En particulier, $f(zxt) \in P$ si et seulement si $f(zyt) \in P$, et comme $L = f^{-1}(P)$, $zxt \in L$ si et seulement si $zyt \in L$. Donc $x \sim_L y$ et $f_L(x) = f_L(y)$.* □

II Semigroupes et langages apériodiques

On dit qu'un semigroupe S est *apériodique* s'il existe un entier $n \geqslant 1$ tel que pour tout $s \in S$, on a $s^n = s^{n+1}$. On dit qu'un langage est *apériodique* s'il est reconnu par un semigroupe apériodique.

II.1 Soit $A = \{a, b\}$. Montrer que le langage $(ab)^+ \subseteq A^+$ est apériodique.

Solution *On vérifie que le semigroupe de transitions de l'automate minimal de ce langage est apériodique.* □

Si $K \subseteq A^+$, on désigne par $A^+ \setminus K$ le complémentaire de K dans A^+.

II.2 Montrer que si $K, L \subseteq A^+$ sont apériodiques, alors $A^+ \setminus K$ et $K \cup L$ le sont aussi.

Solution *Soit $f : A^+ \to S$ et $g : A^+ \to T$ deux morphismes dans des semigroupes apériodiques et $P \subseteq S$, $Q \subseteq T$ tels que $K = f^{-1}(P)$ et $L = g^{-1}(Q)$. On constate d'abord que $A^+ \setminus K = f^{-1}(S \setminus P)$, donc $A^+ \setminus K$ est reconnu par S. Il est donc apériodique.*

D'autre part $S \times T$ muni de la loi $(s, t) \cdot (s', t') = (ss', tt')$ est clairement un semigroupe apériodique. Soit h le morphisme de A^+ dans $S \times T$ défini par $h(w) = (f(w), g(w))$. On a alors $K \cup L = h^{-1}((S \times Q) \cup (P \times T))$, donc $K \cup L$ est reconnu par $S \times T$, et $K \cup L$ est apériodique. □

II.3 Soit S un semigroupe apériodique. Montrer que si T est un sous-semigroupe de S et si $f : T \to T'$ est un morphisme surjectif, alors T' est apériodique. En déduire que si L est apériodique, alors $A^+/{\sim_L}$ est apériodique.

Solution *Il existe n tel que $s^n = s^{n+1}$ pour tout $s \in S$. Comme T est un sous-semigroupe de S, on a $t^n = t^{n+1}$ pour tout $t \in T$. Soit $u \in T'$. Comme f est surjectif, il existe $t \in T$ tel que $f(t) = u$. En utilisant le fait que f est un morphisme, on calcule donc $u^n = f(t)^n = f(t^n) = f(t^{n+1}) = f(t)^{n+1} = u^{n+1}$. Ceci montre que T' est apériodique.*

Soit maintenant S un semigroupe apériodique qui reconnaît L. D'après la question I.7, il existe un sous-semigroupe T de S et un morphisme surjectif de T dans $A^+/{\sim_L}$, et il suffit alors d'appliquer ce qui précède. $\square$

II.4 Déduire de la question précédente que si K et L sont deux langages apériodiques, alors KL est aussi apériodique.

Solution *Comme K et L sont apériodiques, $A^+/{\sim_L}$ et $A^+/{\sim_K}$ sont apériodiques d'après la question précédente. Il existe k et ℓ tels que pour tout $s \in A^+/{\sim_K}$ (resp. pour tout $s \in A^+/{\sim_L}$), on a $s^k = s^{k+1}$ (resp. on a $s^\ell = s^{\ell+1}$).*

D'après la question I.5 c, il suffit de montrer que $A^+/{\sim_{KL}}$ est apériodique. Soient $z, t \in A^*$ tels que le mot $w = zx^{k+\ell}t$ soit dans KL. On veut montrer que $w = zx^{k+\ell+1}t$ est aussi dans KL. Le mot w s'écrit uv avec $u \in K$ et $v \in L$, et soit x^k est un facteur de u, soit x^ℓ est un facteur de v. Supposons par exemple que x^k est un facteur de u. Alors $u = u_1x^ku_2$, mais comme $s^k = s^{k+1}$ pour tout s de $A^+/{\sim_K}$, $u_1x^{k+1}u_2$ est aussi dans K. On en déduit facilement que $w = zx^{k+\ell+1}t$ est aussi dans KL.

On montre de la même façon que si $w = zx^{k+\ell+1}t \in KL$, alors $w = zx^{k+\ell}t \in KL$. Ceci prouve que pour $s \in A^+/{\sim_{KL}}$, on a $s^{k+\ell} = s^{k+\ell+1}$. Donc $A^+/{\sim_{KL}}$ est bien apériodique. $\square$

III Logique temporelle linéaire et langages apériodiques

Soit A un alphabet. Les formules de la logique linéaire $\mathsf{LTL}(A)$ sont définies inductivement comme suit :

- Pour tout $a \in A$, a est une formule.
- Si φ et ψ sont des formules, alors $\varphi \vee \psi$ est une formule.
- Si φ est une formule, alors $\neg\varphi$ est une formule.
- Si φ est une formule, alors $\mathsf{X}\,\varphi$ est une formule.
- Si φ et ψ sont des formules, alors $\varphi \,\mathsf{U}\, \psi$ est une formule.

La *longueur* $|\varphi|$ d'une formule φ est le nombre de symboles de $A \cup \{\vee, \neg, \mathsf{X}, \mathsf{U}\}$ apparaissant dans son écriture.

Soit $u = a_1 \cdots a_n \in A^+$, où a_i désigne la $i^{\text{ème}}$ lettre de u. Pour $i = 1, \dots, n$ on définit l'expression « u satisfait φ à l'instant i », notée $u, i \models \varphi$, de la façon suivante :

- $u, i \models a$ (pour $a \in A$) si l'on a $a_i = a$;
- $u, i \models \varphi \vee \psi$ si l'on a $u, i \models \varphi$ ou $u, i \models \psi$;
- $u, i \models \neg\varphi$ si l'on n'a pas $u, i \models \varphi$;
- $u, i \models \mathsf{X}\,\varphi$ si $i \leqslant n - 1$ et $u, i + 1 \models \varphi$;
- $u, i \models \varphi \,\mathsf{U}\, \psi$ s'il existe un entier j qui satisfait les conditions suivantes :
  - $i \leqslant j \leqslant n$,
  - $u, j \models \psi$,
  - pour tout k tel que $i \leqslant k \leqslant j - 1$, on a : $u, k \models \varphi$.

On dit qu'un mot u satisfait une formule φ s'il la satisfait à l'instant 1, c'est-à-dire si $u, 1 \models \varphi$. Soit φ une formule de $\mathsf{LTL}(A)$. Le langage de A^+ défini par φ est

$$L_A(\varphi) = \{u \in A^+ \mid u, 1 \models \varphi\}$$

On dit que $L \subseteq A^+$ est *exprimable* dans $\mathsf{LTL}(A)$ s'il existe une formule φ de $\mathsf{LTL}(A)$ telle que $L = L_A(\varphi)$. On dit aussi que φ *définit* L.

III.1 Soit φ une formule de $\mathsf{LTL}(A)$. On pose

$$\mathsf{E}\,\varphi = (\bigvee_{a \in A} a)\ \mathsf{U}\ \varphi$$
$$\mathsf{G}\,\varphi = \neg(\mathsf{E}(\neg\varphi))$$

Décrire de façon informelle les langages définis par les formules $\mathsf{E}\,\varphi$ et $\mathsf{G}\,\varphi$.

Solution *On vérifie qu'un mot satisfait la formule $\mathsf{E}\varphi$ si et seulement s'il ce mot a un suffixe non vide qui satisfait φ. De même, un mot satisfait la formule $\mathsf{G}\varphi$ si et seulement si tous ses suffixes non vides satisfont φ.* □

III.2 Soit A un alphabet fini.

a. Trouver une formule de $\mathsf{LTL}(A)$ qui définit le langage A^+.

b. Trouver une formule de $\mathsf{LTL}(A)$ qui définit le langage aA^*, où $a \in A$.

c. Trouver une formule de $\mathsf{LTL}(A)$ qui définit le langage A^*b, où $b \in A$.

d. Trouver une formule de $\mathsf{LTL}(A)$ qui définit le langage $(ab)^+$, où $\{a, b\} \subseteq A$.

Solution *On utilise les abréviations suivantes : $\varphi \wedge \psi$ pour $\neg(\neg\varphi \vee \neg\psi)$; $\varphi \Rightarrow \psi$ pour $\neg\varphi \vee \psi$. Enfin, pour $B \subseteq A$, B est une abréviation de $\bigvee_{b \in B} b$. On constate que la formule A est satisfaite par n'importe quel mot u à tout instant $i \in [1, |u|]$. On vérifie alors facilement que*

a. $A^+ = L_A(A)$.

b. $aA^* = L_A(a)$.

c. $A^*b = L_A(\mathsf{E}(b \wedge \neg\,\mathsf{X}A))$.

d. $(ab)^+ = L_A(a \wedge (\mathsf{E}(b \wedge \neg\,\mathsf{X}A)) \wedge \mathsf{G}(a \Rightarrow \mathsf{X}b) \wedge \mathsf{G}(b \Rightarrow \neg\,\mathsf{X}(\neg a)))$. □

III.3 Montrer que

a. Si $\varphi = a$ $(a \in A)$, alors $L_A(\varphi)$ est apériodique.

b. Si $L_A(\varphi)$ est apériodique, alors $L_A(\neg\varphi)$ est apériodique.

c. Si $L_A(\varphi)$ et $L_A(\psi)$ sont apériodiques, alors $L_A(\varphi \vee \psi)$ est apériodique.

d. Si $L_A(\varphi)$ est apériodique, alors $L_A(\mathsf{X}\,\varphi)$ est apériodique.

Solution

a. On a $L_A(a) = aA^*$. On vérifie que le semigroupe de transitions de l'automate minimal de ce langage est apériodique.

b. *On a clairement* $L_A(\neg\varphi) = A^+ \setminus L_A(\varphi)$, *et comme la classe des langages apériodiques est fermée par complément (cf. question II.2),* $L_A(\neg\varphi)$ *est apériodique si* $L_A(\varphi)$ *l'est.*

c. *On a clairement* $L_A(\varphi \vee \psi) = L_A(\varphi) \cup L_A(\psi)$, *et comme la classe des langages apériodiques est fermée par union finie (cf. question II.2),* $L_A(\varphi \vee \psi)$ *est apériodique dès que* $L_A(\varphi)$ *et* $L_A(\psi)$ *le sont.*

d. *On a* $L_A(\mathsf{X}\varphi) = AL_A(\varphi)$. *Or, le langage* A *est apériodique (comme d'ailleurs tout langage fini), et la classe des langages apériodiques est fermée par produit (cf. question II.4). Donc* $L_A(\mathsf{X}\varphi)$ *est apériodique dès que* $L_A(\varphi)$ *l'est.* □

On rappelle qu'un mot u' est *suffixe* d'un mot $u \in A^+$ s'il existe $u'' \in A^*$ tel que $u = u''u'$.

III.4 Soient φ et ψ deux formules de $\mathsf{LTL}(A)$. On suppose que $L_A(\varphi)$ est reconnu par un semigroupe S. Soit $f : A^+ \to S$ un morphisme et $P \subseteq S$ tel que $L_A(\varphi) = f^{-1}(P)$. Pour $s \in S$, on pose $Ps^{-1} = \{t \in S \mid ts \in P\}$ et $L_s = f^{-1}(Ps^{-1})$. Prouver les égalités suivantes :

$$\begin{aligned} L_A(\varphi \,\mathsf{U}\, \psi) &= \{uv \in A^+ \mid u \in A^*, v \in L_A(\psi), \text{ et } u'v \in L_A(\varphi) \text{ pour tout suffixe } u' \neq 1 \text{ de } u\} \\ &= \bigcup_{s \in S} \left[A^+ \setminus \left(A^*(A^+ \setminus L_s)\right)\right] \left[L_A(\psi) \cap f^{-1}(s)\right] \end{aligned}$$

Solution *La première égalité est une conséquence immédiate de la définition de* $L_A(\varphi \,\mathsf{U}\, \psi)$.

Remarquons ensuite que pour tout $L \subseteq A^+$, *le langage* $A^+ \setminus (A^*(A^+ \setminus L))$ *est le langage des mots dont tous les suffixes non vides sont dans* L.

Montrons maintenant que $L_A(\varphi \,\mathsf{U}\, \psi) \subseteq \bigcup_{s \in S} (A^+ \setminus (A^*(A^+ \setminus L_s)))\,(L_A(\psi) \cap f^{-1}(s))$. *Soit* $uv \in L_A(\varphi \,\mathsf{U}\, \psi)$ *une factorisation donnée par la première égalité. Posons* $s = f(v)$. *On a bien* $v \in L_A(\psi) \cap f^{-1}(s)$. *Il suffit donc de montrer que* $u \in A^+ \setminus (A^*(A^+ \setminus L_s))$, *c'est-à-dire que tous les suffixes non vides* u' *de* u *s'envoient sur* Ps^{-1} *par* f. *Or,* $u'v \in L_A(\varphi)$ *implique que* $f(u'v) \in P$, *soit* $f(u') \in Ps^{-1}$.

Inversement, soit $s \in S$, *soit* $u \in A^+ \setminus (A^*(A^+ \setminus L_s))$ *et soit* $v \in L_A(\psi) \cap f^{-1}(s)$. *Pour montrer que* $uv \in L_A(\varphi \,\mathsf{U}\, \psi)$, *on a déjà* $v \in L_A(\psi)$. *Il reste à vérifier que pour tout suffixe non vide* u' *de* u, *on a* $u'v \in L_A(\varphi)$. *Mais comme* $u \in A^+ \setminus (A^*(A^+ \setminus L_s))$, *on a* $u' \in L_s$ *pour tout suffixe non vide* u' *de* u, *soit* $f(u')s \in P$, *donc* $f(u'v) \in P$, *soit encore* $u'v \in L_A(\varphi)$, *ce que l'on voulait.* □

III.5 Montrer que si $L_A(\varphi)$ et $L_A(\psi)$ sont apériodiques, alors $L_A(\varphi \,\mathsf{U}\, \psi)$ est apériodique.

Solution *Comme* $L_A(\varphi)$ *est apériodique, on peut donc supposer que le semigroupe* S *de la question précédente est apériodique. Comme la classe des langages apériodiques est fermée par union finie (cf. question II.2), il suffit de montrer que tout langage de la forme* $(A^+ \setminus (A^*(A^+ \setminus L_s)))\,(L_A(\psi) \cap f^{-1}(s))$ *est apériodique. Comme cette classe est fermée par produit (cf. question II.4), il suffit de montrer que*

i) $A^+ \setminus (A^*(A^+ \setminus L_s))$ *est apériodique ;*

ii) $L_A(\psi) \cap f^{-1}(s)$ *est apériodique.*

Mais L_s *est reconnu par* S *donc est apériodique. Donc* $A^+ \setminus L_s$ *est aussi apériodique. De plus, si* K *est apériodique,* $A^*K = A^+K \cup K$ *est une union de langages apériodiques, donc est apériodique. Le langage* $A^+ \setminus (A^*(A^+ \setminus L_s))$ *est donc bien apériodique.*

Enfin, la classe des langages apériodiques étant stable par union et complément, elle est stable par intersection, donc $L_A(\psi) \cap f^{-1}(s)$ *est apériodique.* □

III.6 Montrer que si φ est une formule de $\mathsf{LTL}(A)$, alors le langage $L_A(\varphi)$ est apériodique.

Solution *Les questions III.3 et III.5 permettent immédiatement de montrer que* $L_A(\varphi)$ *est apériodique, par induction structurelle sur* φ *(ou par récurrence sur la longueur de la formule* φ*).* □

III.7 Soit $A = \{a, b\}$. Montrer que le langage $(aa)^+$ n'est pas exprimable dans $\mathsf{LTL}(A)$.

Solution *Soit $L = (aa)^+$. Un calcul facile montre que le semigroupe $A^+/\sim_L$ n'est pas apériodique. Or, si L était reconnu par un semigroupe apériodique, $A^+/\sim_L$ serait apériodique d'après la question II.3. Le langage $(aa)^+$ n'est donc pas exprimable dans $\mathsf{LTL}(A)$.* □

IV Expressivité de la logique linéaire

Dans cette partie, on se propose de montrer que tout langage apériodique de A^+ est exprimable dans $\mathsf{LTL}(A)$. Soit L un langage apériodique de A^+ : on fixe un semigroupe fini apériodique S, une partie P de S et

$$h : A^+ \longrightarrow S$$

un morphisme tel que

$$L = h^{-1}(P)$$

IV.1 Montrer que si $h^{-1}(s)$ est exprimable dans $\mathsf{LTL}(A)$ pour tout $s \in S$, alors L est exprimable dans $\mathsf{LTL}(A)$.

Solution *Il suffit de remarquer que $L = h^{-1}(P) = \bigcup_{s \in P} h^{-1}(s)$ et d'utiliser le fait qu'une union de langages exprimables dans $\mathsf{LTL}(A)$ est exprimable dans $\mathsf{LTL}(A)$.* □

Dans toute la suite, on fixe un élément $s \in S$.

Pour tout ensemble Q, on note Q^Q l'ensemble des applications de Q dans Q.

IV.2 Vérifier que Q^Q muni de la composition des applications est un semigroupe. Montrer que pour tout semigroupe fini T, il existe un ensemble fini Q tel que T est un sous-semigroupe de Q^Q. On pourra commencer par traiter le cas où T a un élément neutre 1 (*i.e.*, tel que $1t = t1 = t$ pour tout $t \in T$), et montrer qu'alors, on peut choisir $Q = T$.

Solution *Le fait que Q^Q soit un semigroupe résulte immédiatement de l'associativité de la composition des applications de Q dans Q. Soit T^1 le semigroupe $T \cup \{1\}$, où 1 est un nouvel élément, qui agit comme un élément neutre ($1t = t1 = t$ pour tout élément t de T^1). Il est clair que T est un sous-semigroupe de T^1. Il suffit donc de montrer que T^1 est un sous-semigroupe de Q^Q, pour un certain ensemble Q. À chaque élément t de T^1, on peut associer l'application $\rho_t : T^1 \to T^1$ définie par $\rho_t(s) = ts$. L'application $t \mapsto \rho_t$ est un morphisme : $\rho_t \circ \rho_{t'}(s) = tt's = \rho_{tt'}(s)$; elle est injective : si $\rho_t = \rho_{t'}$, alors en particulier $\rho_t(1) = \rho_{t'}(1)$, soit $t = t'$. Finalement, S est un sous-semigroupe de Q^Q où $Q = T^1$.* □

IV.3 On suppose que pour tout $a \in A$, $h(a)$ est une bijection de Q dans Q. Montrer que $h^{-1}(s)$ est exprimable dans $\mathsf{LTL}(A)$.

Solution *Soit $w \in A^+$. Alors, $h(w)$ est une bijection, et comme S est apériodique, il existe n tel que $h(w)^{n+1} = h(w)^n$. En multipliant par $(h(w)^{-1})^n$, où $h(w)^{-1}$ désigne la bijection réciproque de $h(w)$, on obtient $h(w) = id_Q$. Ainsi, on a $h(w) = id_Q$ pour tout $w \in A^+$, et*

$$h^{-1}(s) = \begin{cases} \varnothing & si\ s \neq id_Q \\ A^+ & sinon \end{cases}$$

et $h^{-1}(s)$ est bien exprimable dans $\mathsf{LTL}(A)$. □

Dans la suite du problème, on suppose qu'il existe une lettre $a \in A$ telle que $h(a)$ n'est pas une bijection de Q dans Q. On pose alors :

$$\begin{aligned}
Q' &= h(a)(Q) \\
B &= A \setminus \{a\} \\
\Sigma &= B^* a \\
g &= h_{|B^+} : g \text{ est la restriction de } h \text{ à } B^+.
\end{aligned}$$

On se propose de montrer par récurrence sur $|Q|$ que $h^{-1}(s)$ est exprimable dans $\mathsf{LTL}(A)$.

IV.4 Vérifier que l'hypothèse de récurrence est vraie à l'ordre 1 :

$$\text{si } |Q| = 1, \text{ alors } h^{-1}(s) \text{ est exprimable dans } \mathsf{LTL}(A). \qquad (\mathscr{H}_1)$$

Solution *Si $|Q| = 1$, alors $|S| = 1$ donc tous les éléments de A^+ s'envoient sur l'unique élément de S par h. Donc $L = \varnothing$ ou $L = A^+$, qui sont tous deux exprimables dans $\mathsf{LTL}(A)$.* □

On suppose jusqu'à la fin du problème que l'hypothèse de récurrence suivante est vraie :

$$\text{si } |Q| \leqslant q, \text{ alors } h^{-1}(s) \text{ est exprimable dans } \mathsf{LTL}(A) \qquad (\mathscr{H}_q)$$

On fixe dans toute la suite du problème un ensemble Q de cardinal $q+1$, et on se propose maintenant de montrer $(\mathscr{H}_{q+1})$ par récurrence sur $|A|$.

IV.5 Montrer que $|Q'| < |Q|$, et que $S' = \{s_{|Q'} \mid s \in h(\Sigma^+)\}$ est un sous-semigroupe de ${Q'}^{Q'}$, où $s_{|Q'}$ désigne la restriction de s à Q'. Vérifier que S' est apériodique.

Solution *On ne peut avoir $|Q'| = |Q|$ que si $h(a)$ est une bijection, ce qui est exclu. Donc $|Q'| < |Q|$. Comme tout élément de Σ est un mot de A^*a, et comme $h(a)$ envoie Q sur Q', si $s \in h(\Sigma^+)$, alors s envoie Q sur Q'. On peut donc composer les restrictions à Q' d'éléments de $h(\Sigma)^+$. Il alors immédiat que les éléments de S' envoient Q' sur lui-même, et que S' est un sous-semigroupe de ${Q'}^{Q'}$.*

Le semigroupe $T = \{s \mid s \in h(\Sigma^+)\}$ est un sous-semigroupe de S, donc il est apériodique. On vérifie aisément que pour $s, t \in T$, on a $(st)_{|Q'} = s_{|Q'} t_{|Q'}$. L'application de T dans S' qui a t associe $t_{|Q'}$ est donc un morphisme, qui est bien sûr surjectif. D'après II.3, S' est apériodique. □

Si T est un semigroupe, on note T^1 le semigroupe obtenu en ajoutant à T un nouvel élément 1_T qui agit comme un élément neutre : $1_T t = t 1_T = t$ pour tout $t \in T \cup \{1_T\}$.

Soit $f : \Sigma^* \to S'^*$ le morphisme tel que $f(1) = 1$, et qui envoie $u_1 a \cdot u_2 a \cdots u_k a \in \Sigma^+$, avec $u_i \in B^*$, sur le mot de k lettres $[h(u_1 a)]_{|Q'} \cdot [h(u_2 a)]_{|Q'} \cdots [h(u_k a)]_{|Q'}$ de S'^+. On remarquera que dans cette définition, S'^+ désigne le semigroupe libre sur S', considéré comme un alphabet. Soit aussi $e : S'^* \to S'^1$ le morphisme qui envoie 1 sur $1_{S'}$ et le mot (de k lettres) $s_1 \cdot s_2 \cdots s_k$ de S'^+ sur l'élément $s_1 s_2 \cdots s_k$ de S'.

On prolonge g en un morphisme de B^* dans S^1 en posant $g(1) = 1_S$. On note encore g ce prolongement, et l'on pose alors pour $t \in S^1$ et $s' \in S'^1$:

$$\begin{aligned}
L_t &= g^{-1}(t) \\
K_{s'} &= f^{-1}(e^{-1}(s'))
\end{aligned}$$

IV.6 Montrer l'égalité

$$h^{-1}(s) \cap \Sigma^+ B^* = \bigcup_{\substack{t,u \in S^1, s' \in S'^1 \\ th(a)s'u = s}} L_t a K_{s'} L_u$$

Solution *Soit $x \in h^{-1}(s) \cap \Sigma^+ B^*$. D'après la définition de Σ, $x \in A^*aA^*$ et se factorise donc $x = x_1 a x_2 x_3$, où $x_1, x_3 \in B^*$ et $x_2 \in \Sigma^*$ (x_1 « s'arrête » juste avant le premier a et x_3 « commence » juste après le dernier). Soit $t \stackrel{def}{=} h(x_1) = g(x_1)$, $u \stackrel{def}{=} h(x_3) = g(x_3)$ et $s' \stackrel{def}{=} h(x_2) = e(f(x_2))$. On a $s = h(x) = h(x_1)h(a)h(x_2)h(x_3) = g(x_1)h(a)e(f(x_2))g(x_3) = th(a)s'u$, et on a bien $x \in L_t a K_{s'} L_u$. Ceci montre l'inclusion de gauche à droite.*

Inversement, si $x \in L_t a K_{s'} L_u$ où $th(a)s'u = s$, alors clairement $x \in A^*aA^* = \Sigma^+ B^*$. De plus $x = x_1 a x_2 x_3$, où $x_1, x_3 \in B^*$ et $x_2 \in \Sigma^*$ sont tels que $g(x_1) = t$, $e(f(x_2)) = s'$ et $g(x_3) = u$. Donc $h(x) = th(a)s'u = s$. □

Dans la suite, on fixe des éléments $t, u \in S^1$ et $s' \in S'^1$.

IV.7 Déduire de IV.5 qu'il existe une formule φ de $\mathsf{LTL}(S')$ qui définit $e^{-1}(s')$ si $s' \neq 1_{S'}$. Montrer par récurrence sur $|\varphi|$ que $K_{s'}$ est exprimable dans $\mathsf{LTL}(A)$.

Solution *Le langage $e^{-1}(s')$ de S'^+ est reconnu par S', qui est un sous-semigroupe apériodique de $Q'^{Q'}$. Comme $|Q'| < |Q|$, l'hypothèse de récurrence ($\mathscr{H}_q$) montre que $e^{-1}(s)$ est exprimable dans $\mathsf{LTL}(S')$. Soit φ une formule de $\mathsf{LTL}(S')$ telle que $L_{S'}(\varphi) = e^{-1}(s')$.*

- *Si $\varphi = t$, où $t \in S'$, alors $e^{-1}(s') = tS'^*$, donc $K_{s'} = \begin{cases} aA^* & \text{si } f(a) = t \\ \varnothing & \text{sinon} \end{cases}$, et ces langages sont exprimables dans $\mathsf{LTL}(A)$.*

  On raisonne maintenant par récurrence sur $|\varphi|$.

- *Si $\varphi = \neg\varphi_1$, on a $|\varphi_1| < |\varphi|$, et par récurrence, il existe ψ_1 telle que $f^{-1}(L_{S'}(\varphi_1)) = L_A(\psi_1)$. On a alors $K_{s'} = f^{-1}(L_{S'}(\neg\varphi_1)) = [A^+ \setminus f^{-1}(L_{S'}(\varphi_1))] = A^+ \setminus L_A(\psi_1) = L_A(\neg\psi_1)$.*

- *Si $\varphi = \varphi_1 \vee \varphi_2$, on a encore $|\varphi_1| < |\varphi|$ et $|\varphi_2| < |\varphi|$, donc il existe ψ_1 (resp. ψ_2) telle que $f^{-1}(L_{S'}(\varphi_1)) = L_A(\psi_1)$ (resp. $f^{-1}(L_{S'}(\varphi_2)) = L_A(\psi_2)$). On a donc $f^{-1}(L_{S'})(\varphi) = L_A(\psi_1 \vee \psi_2)$.*

- *Si $\varphi = \mathsf{X}\varphi_1$, on a $|\varphi_1| < |\varphi|$, et à nouveau il existe ψ_1 telle que $f^{-1}(L_{S'}(\varphi_1)) = L_A(\psi_1)$. On a $K_{s'} = f^{-1}(L_{S'}(\varphi)) = f^{-1}(S' L_{S'}(\varphi_1)) = af^{-1}(L_{S'}(\varphi_1)) = L_A(\mathsf{X}\psi_1)$.*

- *Enfin, si $\varphi = \varphi_1 \mathsf{U} \varphi_2$, avec $|\varphi_1| < |\varphi|$ et $|\varphi_2| < |\varphi|$, il existe ψ_1 (resp. ψ_2) telle que $f^{-1}(L_{S'}(\varphi_i)) = L_A(\psi_i)$. On a alors $K_{s'} = f^{-1}(L_{S'}(\varphi)) = f^{-1}(L_{S'}(\varphi_1 \mathsf{U} \varphi_2)) = L_A(\psi_1 \mathsf{U} \psi_2)$.*

Donc $K_{s'}$ est exprimable dans $\mathsf{LTL}(A)$. □

IV.8 Déduire de IV.6 et IV.7 que si $|A| = 1$, alors $h^{-1}(s)$ est exprimable dans $\mathsf{LTL}(A)$.

Solution *Pour $A = \{a\}$, on a $B = \varnothing$ et $B^* = \{1\}$, et $\Sigma^+ B^* = A^+$. Pour $t \in S^1$, $L_t = \varnothing$ sauf si $t = 1_S$, auquel cas $L_t = \{1\}$. Donc l'égalité de la question IV.6 s'écrit*

$$h^{-1}(s) = \Big[\bigcup_{\substack{s' \in S' \\ h(a)s' = s}} aK_{s'} \Big] \cup \begin{cases} \{a\} & \text{si } h(a) = s \\ \varnothing & \text{sinon} \end{cases}$$

Or $K_{s'}$ est exprimable dans $\mathsf{LTL}(A)$, donc $aK_{s'}$, et finalement $h^{-1}(s)$ le sont aussi. □

On suppose maintenant que

$$\text{si } |A| \leqslant p, \text{ alors } h^{-1}(s) \text{ est exprimable dans } \mathsf{LTL}(A) \qquad (\mathscr{H}'_p)$$

et on fixe un alphabet A de cardinal $p+1$.

IV.9 Soit φ est une formule de $\mathsf{LTL}(B)$.

a. Montrer que $L_B(\varphi)$ est exprimable dans $\mathsf{LTL}(A)$.

b. Montrer par récurrence sur la longueur de φ que $L_B(\varphi)aA^*$ est exprimable dans $\mathsf{LTL}(A)$.

En déduire que L_t $(t \in S)$ et L_taA^* $(t \in S^1)$ sont exprimables dans $\mathsf{LTL}(A)$.

Solution *On a $L_B(\varphi) = L_A(\varphi) \cap B^+ = L_A(\varphi \wedge \mathsf{G} B)$, donc $L_B(\varphi)$ est exprimable dans $\mathsf{LTL}(A)$.*

Soit φ une formule de $\mathsf{LTL}(B)$ qui définit L. Si $\varphi = b$, avec $b \in B$, on a $L = bB^*$ et $LaA^* = bB^*aA^* = L_A(b \wedge \mathsf{E} a)$. On suppose que pour toute formule φ telle que $|\varphi| < k$, $L_B(\varphi)aA^*$ est exprimable dans $\mathsf{LTL}(A)$; soit alors φ une formule de longueur k.

- *Si $\varphi = \neg\varphi_1$, on a $|\varphi_1| < k$, donc il existe ψ_1 telle que $L_B(\varphi_1)aA^* = L_A(\psi_1)$. On vérifie en utilisant $a \notin B$, que $L_B(\varphi)aA^* = B^+aA^* \setminus L_B(\varphi_1)aA^*$, donc $L_B(\varphi)aA^* = B^+aA^* \setminus L_A(\psi_1) = L_A(B \wedge \mathsf{E} a \wedge \neg\psi_1)$ est bien exprimable dans $\mathsf{LTL}(A)$.*

- *Si $\varphi = \varphi_1 \vee \varphi_2$, on a encore $|\varphi_1| < k$ et $|\varphi_2| < k$, donc il existe ψ_1 (resp. ψ_2) telle que $L_B(\varphi_1)aA^* = L_A(\psi_1)$ (resp. $L_B(\varphi_2)aA^* = L_A(\psi_2)$). On a donc $L_B(\varphi)aA^* = L_B(\varphi_1)aA^* \cup L_B(\varphi_2)aA^* = L_A(\psi_1 \vee \psi_2)$.*

- *Si $\varphi = \mathsf{X}\varphi_1$, on a $|\varphi_1| < k$, et à nouveau il existe ψ_1 telle que $L_B(\varphi_1)aA^* = L_A(\psi_1)$. On a $L_B(\varphi)aA^* = BL_A(\varphi_1)aA^* = L_A(B \wedge \mathsf{X}\psi_1)$.*

- *Enfin, si $\varphi = \varphi_1 \,\mathsf{U}\, \varphi_2$, avec $|\varphi_1| < k$ et $|\varphi_2| < k$, il existe ψ_1 (resp. ψ_2) telle que $L_B(\varphi_1)aA^* = L_A(\psi_1)$ (resp. $L_B(\varphi_2)aA^* = L_A(\psi_2)$). On a alors $L_B(\varphi)aA^* = L_B(\varphi_1 \,\mathsf{U}\, \varphi_2)aA^* = L_A(\psi_1 \,\mathsf{U}\, \psi_2)$.*

On a donc montré que $L_B(\varphi)aA^*$ est exprimable dans $\mathsf{LTL}(A)$.

Comme $|B| < |A|$, $g^{-1}(t) \setminus \{1\}$ est exprimable dans $\mathsf{LTL}(B)$ d'après ($\mathscr{H}'_p$). On déduit de a que L_t ($t \in S$) est exprimable dans $\mathsf{LTL}(A)$ et de b que L_taA^* ($t \in S^1$) l'est aussi. □

IV.10 Montrer que si $L_1, L_2 \subseteq B^*$ et $K \subseteq \Sigma^*$, on a $L_1aKL_2 = L_1aA^* \cap B^*aKL_2$. En déduire que l'on a

$$L_taK_{s'}L_u = L_taA^* \cap B^*aK_{s'}L_u$$

Solution *L'inclusion de gauche droite est triviale. Soit $x \in L_1aA^* \cap B^*aKL_2$. On peut écrire, avec des notations évidentes : $x = x_1ax' = x_Bax_Kx_2$. Comme $x_1 \in B^*$, l'occurrence de a qui apparaît dans ces deux factorisations est la même (c'est la première). On a donc $x' = x_Kx_2 \in KL_2$. La deuxième égalité demandée est triviale.* □

IV.11 Montrer que

$$B^*aK_{s'}L_u = B^*aK_{s'}B^* \cap \Sigma^+L_u$$

Montrer par ailleurs que Σ^+L_u est exprimable dans $\mathsf{LTL}(A)$.

Solution *On a $\Sigma^+ = B^*a\Sigma^*$. À nouveau l'inclusion de gauche droite est triviale. Soit $x \in B^*aK_{s'}B^* \cap B^*a\Sigma^*L_u$. Avec des notations évidentes, x admet deux décompositions $x = x_Bax_{s'}y_B = x'_Bax_\Sigma x_u$. Comme la lettre a n'apparaît ni dans x_B ni dans x'_B, l'occurrence de a qui apparaît dans les deux* *factorisations est la même. Donc $x_{s'}y_B = x_\Sigma x_u$. En remarquant de même que $y_B, x_u \in B^*$ et que si $x_{s'}$ et x_Σ ne sont pas vides, ils se terminent par a, on en déduit que $x_{s'} = x_\Sigma$ et $y_B = x_u$. On a donc bien $x \in B^*aK_{s'}L_u$.*

Montrons maintenant que $\Sigma^+L_u = B^*a\Sigma^*L_u$ est exprimable dans $\mathsf{LTL}(A)$. Si $u = 1$, $\Sigma^+L_u = A^*a$ est exprimable (cf. III.2). Supposons $u \neq 1$. On sait par l'hypothèse de récurrence ($\mathscr{H}'_p$) que $g^{-1}(u)$ est exprimable dans $\mathsf{LTL}(B)$ et donc dans $\mathsf{LTL}(A)$. Soit φ une formule de $\mathsf{LTL}(A)$ telle que $L(\varphi) = g^{-1}(u)$. La formule $\mathsf{E}(a \wedge \mathsf{X}\varphi)$ définit alors Σ^+L_u. □

IV.12 Montrer que l'on a : $h^{-1}(s) = (h^{-1}(s) \cap \Sigma^+B^*) \cup L_s$.

Solution *L'égalité demandée résulte trivialement de $A^+ = \Sigma^+B^* \cup B^+$ et du fait que $L_s = h^{-1}(s) \cap B^+$. Pour $|A| = 1$, $B = \varnothing$, donc $B^* = \{1\}$ et cette égalité s'écrit simplement $h^{-1}(s) = h^{-1}(s) \cap a^+$.* □

IV.13 On suppose que si $s' \neq 1_{S'}$, alors $K_{s'}B^*$ est exprimable dans $\mathsf{LTL}(A)$ (ceci sera montré en IV.14). Montrer que $B^*aK_{s'}L_u$ est exprimable dans $\mathsf{LTL}(A)$, puis déduire des questions précédentes que $h^{-1}(s)$ est exprimable dans $\mathsf{LTL}(A)$. En déduire que tout langage apériodique de A^+ est exprimable dans $\mathsf{LTL}(A)$.

Solution *D'après la question IV.14, le langage $K_{s'}B^*$ est exprimable dans $\mathsf{LTL}(A)$, disons par φ. Mais alors, le langage $B^*aK_{s'}B^*$ est lui aussi exprimable, par $B\,\mathsf{U}\,(a \wedge \mathsf{X}\varphi)$. D'après la question IV.11, le langage $B^*aK_{s'}L_u$ est donc lui aussi exprimable. D'après IV.10 et IV.9, le langage $L_taK_{s'}L_u$ est donc exprimable, et d'après l'expression de $h^{-1}(s)$ de la question IV.6, $h^{-1}(s)$ est exprimable dans $\mathsf{LTL}(A)$. Il reste à utiliser IV.1 pour conclure.* □

IV.14 Soit $s' \neq 1_{S'}$. Montrer par récurrence sur la longueur d'une formule définissant $e^{-1}(s')$ que $K_{s'}B^*$ est exprimable dans $\mathsf{LTL}(A)$.

Solution *On sait que $e^{-1}(s)$ est exprimable dans $\mathsf{LTL}(S')$ (cf. IV.7). Soit φ une formule de $\mathsf{LTL}(S')$ telle que $L_{S'}(\varphi) = e^{-1}(s')$.*

- *Si $\varphi = t$, où $t \in S'$, alors $e^{-1}(s') = tS'^*$, donc $K_{s'}B^* = \bigcup_{\substack{u \in S^1 \\ uh(a)=t}} L_uaA^*B^*$ On a $L_uaA^*B^* = L_uaA^*$, donc ce langage est exprimable dans $\mathsf{LTL}(A)$ d'après IV.9, et $K_{s'}B^*$ l'est donc aussi.*

  On raisonne maintenant par récurrence sur $|\varphi|$.

- *Si $\varphi = \neg\varphi_1$, on a $|\varphi_1| < |\varphi|$, donc il existe ψ_1 telle que $f^{-1}(L_{S'}(\varphi_1))B^* = L_A(\psi_1)$. Alors, $K_{s'}B^* = f^{-1}(L_{S'}(\neg\varphi_1))B^* = [A^+ \setminus f^{-1}(L_{S'}(\varphi_1))]B^* = L_A(\neg\psi_1)$, la dernière égalité provenant de ce que pour $K \subseteq \Sigma^*$, on a $(A^+ \setminus K)B^* = A^+ \setminus (KB^*)$.*

- *Si $\varphi = \varphi_1 \vee \varphi_2$ avec $|\varphi_i| < |\varphi|$, il existe ψ_i telles que $f^{-1}(L_{S'}(\varphi_i))B^* = L_A(\psi_i)$. On a donc $K_{s'} = [f^{-1}(L_{S'}(\varphi_1)) \cup f^{-1}(L_{S'}(\varphi_2))]B^* = f^{-1}(L_{S'}(\varphi_1))B^* \cup f^{-1}(L_{S'}(\varphi_2))B^* = L_A(\psi_1 \vee \psi_2)$.*

- *Si $\varphi = \mathsf{X}\varphi_1$, on a $|\varphi_1| < |\varphi|$, et à nouveau il existe ψ_1 telle que $f^{-1}(L_{S'}(\varphi_1))B^* = L_A(\psi_1)$. On a $f^{-1}(L_{S'}(\varphi)B^*) = f^{-1}(S'L_{S'}(\varphi_1))B^* = \bigcup_{u \in S^1} L_uaf^{-1}(L_{S'}(\varphi_1))B^* = \bigcup_{u \in S^1} L_uaL_A(\psi_1)$. Mais d'après IV.10, on a $L_uaL_A(\psi_1) = L_uaA^* \cap B^*aL_A(\psi_1)$, Or L_uaA^* est exprimable dans $\mathsf{LTL}(A)$ d'après IV.9, et $B^*aL_A(\psi_1) = L_A(B\,\mathsf{U}\,(a \wedge \mathsf{X}\psi_1))$.*

- *Enfin, si $\varphi = \varphi_1\,\mathsf{U}\,\varphi_2$ avec $|\varphi_i| < |\varphi|$, il existe ψ_i telles que $f^{-1}(L_{S'}(\varphi_i))B^* = L_A(\psi_i)$. On a alors $K_{s'}B^* = f^{-1}(L_{S'}(\varphi))B^* = f^{-1}(L_{S'}(\varphi_1\,\mathsf{U}\,\varphi_2))B^*$. Soit $\chi_i = B\,\mathsf{U}\,(a \wedge \mathsf{X}\psi_i))$, de sorte que $L_A(\chi_i) = B^*af^{-1}(L_{S'}(\varphi_i))B^*$. On vérifie facilement que*

$$\begin{aligned} f^{-1}(L_{S'}(\varphi_1\,\mathsf{U}\,\varphi_2))B^* &= f^{-1}(L_{S'}(\varphi_1))B^* \cup [f^{-1}(L_{S'}(\varphi_2))B^* \cap L_A(\chi_1\,\mathsf{U}\,\chi_2)] \\ &= L_A(\psi_1) \cup [L_A(\psi_2) \cap L_A(\chi_1\,\mathsf{U}\,\chi_2)] \\ &= L_A(\psi_1 \vee (\psi_2 \wedge (\chi_1\,\mathsf{U}\,\chi_2))) \end{aligned}$$

On a donc montré que $K_{s'}B^*$ est exprimable dans $\mathsf{LTL}(A)$. $\square$

IV.15 Montrer que sur l'alphabet $A = \{a, b\}$, le langage $(ab \cup ba)^+$ est exprimable dans $\mathsf{LTL}(A)$. On ne cherchera pas à expliciter une formule qui définit ce langage.

Solution *Il suffit de calculer le semigroupe de transitions de l'automate minimal de $(ab \cup ba)^+$, et de vérifier que ce semigroupe est apériodique.* $\square$