3e ANNÉE

INFORMATIQUE II

DURÉE : 5 heures

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.

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.

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

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.

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.

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.

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 $A^+/\sim_L$.

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.

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.

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.

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

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 $i = 1, \ldots, n$ 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 $\mathsf{G}\,\varphi$.

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 $\{a,b\} \subseteq A$.

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.

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 :

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

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

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

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

Dans toute la suite, on fixe un élément $s \in S$.
Pour tout ensemble E, on note E^E l'ensemble des applications de E dans E.

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

Dans la suite, on identifiera tout élément t de S avec l'application induite par t sur Q, et le produit tu $(t, u \in S)$ avec l'application composée $u \circ t$.

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 $\mathsf{LTL}(A)$.

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 :

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

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 :

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

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.

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 $s' \in S'^1$:

$$L_t = g^{-1}(t)$$
$$K_{s'} = f^{-1}(e^{-1}(s'))$$

IV.6 Montrer l'égalité

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

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 $\mathsf{LTL}(A)$.

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

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 $L_t a A^*$ $(t \in S^1)$ sont exprimables dans $\mathsf{LTL}(A)$.

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

$$L_t a K_{s'} L_u = L_t a A^* \cap B^* a K_{s'} L_u$$

IV.11 Montrer que

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

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

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

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 $B^* a K_{s'} L_u$ 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 $\mathsf{LTL}(A)$.

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 $\mathsf{LTL}(A)$.

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.

FIN DE L'ÉNONCÉ