	ANNÉE UNIVERSITAIRE 2009/2010 1ÈRE SESSION DE PRINTEMPS **Parcours :** CSB6 **Code UE :** INF253 **Corrigé de l'Épreuve :** Informatique Théorique 2 **Date :** 04 Mai 2011	

Exercice 1 [5 points]

1- K_1 est algébrique. Il est engendré par la grammaire algébrique suivante :
$G_1 := \langle X, \{S_0, S_1\}, P_1, S_0\rangle$, où P_1 est constitué des règles :

$$\begin{array}{lcl} S_0 & \rightarrow & aS_0c \ + \ S_1 \\ S_1 & \rightarrow & bS_1c \ + \ \varepsilon \end{array}$$

2- K_2 est algébrique. Il est engendré par la grammaire algébrique suivante :
$G_2 := \langle X, \{S_0, S_1\}, P_2, S_0\rangle$, où P_1 est constitué des règles :

$$\begin{array}{lcl} S_0 & \rightarrow & aS_0c \ + \ aS_0 \ + \ S_1 \\ S_1 & \rightarrow & bS_1c \ + \ bS_1 \ + \ \varepsilon \end{array}$$

3- Montrons que K_3 n'est pas algébrique. Si K_3 était algébrique, alors il vérifierait le lemme d'itération , pour une certaine constante k. Considérons le mot

$$w := a^k b^k c^k$$

et une décomposition de ce mot sous la forme $w = \alpha u \beta v \gamma$ de telle manière que

(1) $\forall n \in \mathbb{N}, \alpha u^n \beta v^n \gamma \in K_3$
(2) $|uv| \geq 1$
(3) $|u\beta v| \leq k - 1$.

Si $u \in a^+b^+$ ou $u \in b^+c^+$ ou $v \in a^+b^+$ ou $v \in b^+c^+$ alors $\alpha u^2 \beta v^2 \gamma \notin a^+b^+c^+$, donc $\alpha u^2 \beta v^2 \gamma \notin K_3$, ce qui contredit (1).
Si $u \in a^*b^+c^*$ ou $v \in a^*b^+c^*$ alors $|uv| \geq k$ ce qui contredit (3).
Si, pour une lettre $x \in \{a, b\}$, $u \in x^*$ et $v \in x^*$, alors $\alpha\beta\gamma \notin K_3$ (trop peu de lettres x), ce qui contredit (1).
Si $u \in c^*$ et $v \in c^*$, alors $\alpha u^2 \beta v^2 \gamma \notin K_3$ (trop de lettres c),ce qui contredit (1).
Si $u \in a^+$ et $v \in b^+$, alors $\alpha\beta\gamma \notin K_3$ (trop de lettres c), ce qui contredit (1).
Si $u \in a^+$ et $v \in c^+$, alors $\alpha\beta\gamma \notin K_3$ (trop peu de lettres a par rapport aux lettres b), ce qui contredit (1).
Si $u \in b^+$ et $v \in c^+$, alors $\alpha u^2 \beta v^2 \gamma \notin K_3$ (trop peu de lettres a), ce qui contredit (1).
Nous aboutissons à une contradiction. QED

4- $K_4 = \{a^p b^q \mid p \geq q\} \cdot c^* \cup a^* \cdot \{b^q c^r \mid q \geq r\}$ Chacun des quatre langages $\{a^p b^q \mid p \geq q\}, c^*, a^*, \{b^q c^r \mid q \geq r\}$ est algébrique (on peut donner, pour le premier et le quatrième, des grammaires analogues à celle donnée pour K_2). Or l'ensemble des langage algébriques est clos par produit et par union finie. Donc K_4 est algébrique.

5- Considérons l'homorphisme $\varphi : \{a, b, c, \#\}^* \to \{a, b, c, \#\}^*$ défini par

$$\varphi(a) = a, \;\; \varphi(b) = b, \;\; \varphi(c) = c, \;\; \varphi(\#) = \varepsilon.$$

On alors

$$\varphi(K_5) \cap a^* b^* c^* = K_3$$

Comme les opérations "homorphisme de monoides libres"et "intersection avec un rationnel" conservent l'algébricité, si K_5 est algébrique alors K_3 est algébrique. Or K_3 n'est pas algébrique. Donc K_5 n'est pas algébrique.

Exercice 2 [5 points]

1-

$$t_1 = f(a, a), \;\; t_2 = m(f(a, a)), \;\; t_3 = f(a, m(f(a, a))), \;\; t_4 = m(f(a, m(f(a, a)))).$$

2- L_1 est reconnu par l'a.f.t. $\mathcal{A}_1 := \langle F, Q_1, Q_{1,+}, \delta_1 \rangle$ où $Q_1 = \{0, 1, 2\}, Q_{1,+} = \{0, 1, 2\}$ et δ_1 est formé des transitions suivantes :

$$a \to 0, \;\; f(0, 0) \to 1, \;\; m(1) \to 2, \;\; f(0, 2) \to 1.$$

On vérifie que

$$t \to^* 0 \Leftrightarrow t = t_0$$

$$t \to^* 1 \Leftrightarrow \exists n \in \mathbb{N}, t = t_{2n+1}$$

$$t \to^* 2 \Leftrightarrow \exists n \in \mathbb{N}, t = t_{2n+2}$$

Il en découle que $L_{\mathcal{A}_1} = \{t_n \mid n \in \mathbb{N}\}$.
3- Les feuilles de $f(a, b)$ sont 0 et 1 et elles ont longueur 2. Donc $f(a, b) \in L_2$.
Les sommets 0 et 10 sont des feuilles de $f(a, m(b))$ qui n'ont pas la même longueur. Donc $f(a, m(b)) \notin L_2$.
Les sommets 0 et 10 sont des feuilles de $f(a, m(b))$ et ils ont des étiquettes différentes. Donc $f(a, m(b)) \in L_3$.
Le terme $f(a, f(a, a))$ a toutes ses feuilles étiquetées par la même lettre a, donc $f(a, f(a, a)) \notin L_3$.
4- Raisonnons par l'absurde.
Supposons que L_2 est reconnaissable. Soit k un entier tel que L_2 satisfait le lemme d'itération pour k.
Considérons le terme

$$t := f(m^k(a), m^k(a)) \in L_2$$

D'après le lemme d'itération, t se factorise en $t = B[C[d]]$ avec B, C contextes, $d \in \mathrm{T}(F)$ et
(1) $\forall n \in \mathbb{N}, B[C^n[d]] \in L$
(2) $\|C\| \geq 2$
(3) $\|C[d]\| \leq k - 1$.
La condition (3) entraîne qu'il existe $\ell \in [0, k]$ tel que

$$C[d] = m^\ell(a),$$

et la condition (2) montre que

$$C = m^{\ell'}, \text{ avec } 0 < \ell' \leq \ell \leq k.$$

Donc
$$B[C^2[d]] = f(m^{k+\ell'}(a), m^k(a)) \text{ ou } B[C^2[d]] = f(m^k(a), m^{k+\ell'}(a))$$
alors qu'aucun de ces deux termes n'appartient à L_2 : contradiction !
Donc L_2 n'est pas reconnaissable.
5- L_3 est reconnu par l'a.f.t. $\mathcal{A}_3 := \langle F, Q_3, Q_{3,+}, \delta_3 \rangle$ où $Q_3 = \{0,1,2\}, Q_{3,+} = \{2\}$ et δ_3 est formé des transitions suivantes :

$$a \to 0, \;\; b \to 1, \;\; m(0) \to 0, \;\; m(1) \to 1, \;\; f(0,1) \to 2, \;\; f(1,0) \to 2, \;\; f(1,1) \to 1, \;\; f(0,0) \to 0,$$

$$f(2,q) \to 2, \;\; f(q,2) \to 2 \;\; (\text{ pour tout } q \in Q).$$

On vérifie que :
$t \to^* 0$ ssi toutes les feuilles de t sont étiquetées par a.
$t \to^* 1$ ssi toutes les feuilles de t sont étiquetées par b.
$t \to^* 2$ ssi il existe deux feuilles de t qui sont étiquetées, l'une par a , l'autre par b.
Il en découle que $L_{\mathcal{A}_3} = L_3$.

Exercice 3 [5 points]

1- Φ peut être traduite en langage informel par :
tout a est suivi d'un a (ou bien est en dernière position) et tout b est suivi d'un b (ou bien est en dernière position). Donc
$$\mathrm{L}(\Phi) = \mathrm{a}^* + \mathrm{b}^*.$$

2- Ψ peut être traduite en langage informel par :
tout facteur aa est suivi d'un b (ou bien est en dernière position) et tout facteur ab est suivi d'un b (ou bien est en dernière position) et tout facteur bb est suivi d'un b (ou bien est en dernière position).

Remarquons que tout mot de longueur ≤ 2 est modèle de Ψ. Décrivons ensuite les modèles de Ψ, de longueur ≥ 2, en fonction de leur préfixe de longueur 2. On obtient :

$$aab^*, \;\; abb^*, \;\; ba + baab^*, \;\; bbb^*.$$

L'union de tous ces langages forme le langage des modèles de Ψ i.e.

$$\mathrm{L}(\Psi) = \varepsilon + \mathrm{a} + \mathrm{b} + \mathrm{aa} + \mathrm{ab} + \mathrm{ba} + \mathrm{bb} + \mathrm{aab}^* + \mathrm{abb}^* + \mathrm{baab}^* + \mathrm{bbb}^*$$

ou encore, après simplification :

$$\mathrm{L}(\Psi) = \varepsilon + \mathrm{a} + \mathrm{b} + \mathrm{ba} + \mathrm{aab}^* + \mathrm{abb}^* + \mathrm{baab}^* + \mathrm{bbb}^*.$$

3- Notons C1,C2,...,C6 chacune des conditions de l'énoncé (dans leur ordre d'écriture).
On vérifie aisément que tout mot de L satisfait les conditions (C1-C6).
Soit $w \in \{a,b\}^*$ un mot satisfaisant les conditions (C1-C6).
Par C1 : $u = bu_1$. Par C2 : $u = bau_2$. Par C3 : $u = baau_3$. Par C4 : $u = baabu_4$. Par C5 : $u = baabbu_5$. Par C6 : $u = baabbu_5$ et $u_5 \in b^*$.
Finalement : $u \in L$.
4- Les conditions (C1-C6) peuvent être traduites en MSO par :

$$
\begin{aligned}
\theta \quad := \quad & \forall x \cdot \forall y \cdot \\
& [(\forall t \cdot \neg S(t,x)) \to P_b(x)] \wedge \\
& [(\forall t \cdot (\neg S(t,x)) \wedge S(x,y)) \to P_a(y)] \wedge \\
& [(P_b(x) \wedge P_a(y) \wedge S(x,y)) \to (\exists z \cdot S(y,z) \wedge P_a(z))] \wedge \\
& [(P_a(x) \wedge P_a(y) \wedge S(x,y)) \to (\exists z \cdot S(y,z) \wedge P_b(z))] \wedge \\
& [(P_a(x) \wedge P_b(y) \wedge S(x,y)) \to (\exists z \cdot S(y,z) \wedge P_b(z))] \wedge \\
& [(P_b(x) \wedge P_b(y) \wedge S(x,y)) \to (\forall z \cdot S(y,z) \to P_b(z))]
\end{aligned}
$$

PROBLÈME [20 points]

PARTIE 1 : le langage de Dyck.

1- Nous exhibons, pour chaque mot, une dérivation de la grammaire G, qui a pour origine l'axiome S et pour extrémité ce mot :

$$S \to aS\bar{a} \to a\bar{a}$$

$$S \to bS\bar{b} \to b\bar{b}$$

$$S \to SS \to aS\bar{a}S \to a\bar{a}S \to a\bar{a}bS\bar{b} \to a\bar{a}b\bar{b}$$

$$S \to aS\bar{a} \to abS\bar{b}\bar{a} \to ab\bar{b}\bar{a}.$$

2- Pour tout mot $w \in (X \cup \{S\})^*$, posons $\|w\|_a := |w|_a - |w|_{\bar{a}}$. Chaque règle de P conserve la norme i.e.

$$w \to_G w' \Rightarrow \|w\|_a = \|w'\|_a.$$

Or $\|S\|_a = 0$, donc tout mot w de N_2 vérifie que $\|w\|_a = 0$. On en conclut que : $aa \notin N_2, a\bar{b} \notin N_2$. Remarquons que la norme $\|w\|_b := |w|_b - |w|_{\bar{b}}$ peut être utilisée pour montrer que $ab\bar{a} \notin N_2$.

La grammaire G peut être transformée en la grammaire propre :

$$G' := \langle X, \{S\}, P', S\rangle,$$

où P' est constitué des règles :

$$S \to SS \;+\; aS\bar{a} \;+\; \bar{a}Sa \;+\; bS\bar{b} \;+\; \bar{b}Sb \;+\; a\bar{a} \;+\; \bar{a}a \;+\; b\bar{b} \;+\; \bar{b}b$$

et $L_{G'} = L_G - \{\varepsilon\}$.

Soit

$$S \to w_1 \to^* ab\bar{a}\bar{b} \tag{1}$$

une dérivation dans G'. Si $w' = SS$, alors, par le lemme fondamental , il existe $u_1, u_2 \in N_2 - \{\varepsilon\}$ tels que

$$ab\bar{a}\bar{b} = u_1 \cdot u_2. \tag{2}$$

Mais $a \notin N_2, ab \notin N_2, ab\bar{a} \notin N_2$, donc $u_1 \notin \{a, ab, ab\bar{a}\}$, ce qui montre que $ab\bar{a}\bar{b}$ n'a aucune décomposition de la forme (2). Si $w' = aS\bar{a}$ alors, par le lemme fondamental , il existe $u_1 \in N_2 - \{\varepsilon\}$ tel que

$$ab\bar{a}\bar{b} = au_1\bar{a}. \tag{3}$$

ce qui est impossible puisque les deux mots ci-dessus n'ont pas la même dernière lettre. On élimine, par des arguments similaires les possibilités : $w' \in \{\bar{a}Sa, bS\bar{b}, \bar{b}Sb\}$ et les possibilités $w' \in \{a\bar{a}, \bar{a}a, b\bar{b}, \bar{b}b\}$ sont éliminées par le fait que ces mots sont différents de $ab\bar{a}\bar{b}$. La dérivation (1) n'existe donc pas.
3- On remarque tout d'abord que :

$$\forall u \in X^*, \theta(\tilde{u}) = \widetilde{\theta(u)}, \;\; \theta(\theta(u) = u, \;\; \tilde{\tilde{u}} = u.$$

Donc

$$\mathrm{I}(\mathrm{I}(u)) = \theta(\widetilde{\theta(\tilde{u})}) = \theta(\theta(\tilde{\tilde{u}})) = u.$$

On remarque ensuite que

$$\forall u, v \in X^*, \widetilde{u \cdot v} = \tilde{v} \cdot \tilde{u}.$$

Donc

$$\mathrm{I}(u \cdot v) = \theta(\widetilde{u \cdot v}) = \theta(\tilde{v} \cdot \tilde{u})$$

et comme θ est un homomorphisme

$$\mathrm{I}(u \cdot v) = \theta(\tilde{v}) \cdot \theta(\tilde{u})$$

i.e.

$$\mathrm{I}(u \cdot v) = \mathrm{I}(v) \cdot \mathrm{I}(u).$$

4- Supposons que $u \in N_2, v \in N_2$. Cela signifie que $S \to_G^* u$ et $S \to_G^* v$. Donc, par le lemme fondamental,

$$S \to SS \to_G^* uv,$$

i.e. $uv \in N_2$.
5- Remarquons que l'ensemble des membres droits de règles $\{m \in (X \cup \{S\})^* \mid (S, m) \in P\}$ est clos par les opérations $u \mapsto \tilde{u}, \;\; u \mapsto \theta(u), \;\; u \mapsto \mathrm{I}(u)$. Par récurrence sur la longueur des dérivations, on en déduit que

$$u \to_G^* v \Rightarrow \tilde{u} \to_G^* \tilde{v}, \;\; u \to_G^* v \Rightarrow \theta(u) \to_G^* \theta(v), \;\; u \to_G^* v \Rightarrow \mathrm{I}(u) \to_G^* \mathrm{I}(v).$$

En prenant $u = S$, on obtient que N_2 est clos par ces trois opérations.
6- Supposons que $x \in X, u, v \in N_2$. Remarquons que $S \to xS\theta(x)$ est une règle de la grammaire G. Alors $S \to SS \to xS\theta(x)S \to^* xu\theta(x)S \to^* xu\theta(x)v$.
7- Montrons, par récurrence sur $|w|$, que si $w \in N_2 - \{\varepsilon\}$, alors w est de la forme demandée. Soit $w \in N_2 - \{\varepsilon\}$ et $|w| = n$. Alors w est engendré par la grammaire G' :

$$S \to w' \to_{G'}^* w \tag{4}$$

Cas 1 : w' est terminal.
Alors w est de la forme $x\theta(x)$ pour une lettre $x \in X$. Choisissons $u := \varepsilon$ et $v := \varepsilon$. On a bien $w = xu\theta(x)v$ et $u, v \in N_2$.
Cas 2 :$w' = SS$. Par le lemme fondamental $w = w_1 w_2$ avec $w_1 \in N_2 - \{\varepsilon\}, w_2 \in N_2 - \{\varepsilon\}$. Comme G' est propre, $|w_1| < n$ et $|w_2| < n$. Par hypothèse de récurrence, il existe $x \in X, u_1, v_1 \in N_2$ tels que

$$w_1 = x \cdot u_1 \cdot \theta(x) \cdot v_1$$

Posons $u := u_1, v := v_1 \cdot w_2$. Par la question 4, $v \in N_2$. On a bien $w = x \cdot u \cdot \theta(x) \cdot v$.
Cas 3 :$w' = xS\theta(x)$ où $x \in X$.

Par le lemme fondamental $w = xu\theta(x)$ avec $u \in N_2$. Posons $v := \varepsilon \in N_2$. On a bien $w = x \cdot u \cdot \theta(x) \cdot v$.
8- Supposons que $x \in X, v \in X^*, x \cdot v \in N_2$.
D'après la question 7, il existe des mots $u', v' \in N_2$ tels que $x \cdot v = x \cdot u' \cdot \theta(x) \cdot v'$. Considérons le mot

$$v \cdot x = u' \cdot \theta(x) \cdot v' \cdot x$$

On a

$$S \to SS \to^* u'S \to u'\ \theta(x)Sx \to^* u'\theta(x)v'x.$$

Donc $v \cdot x \in N_2$.
9- Supposons que $|u| = 0$:
$u \cdot v \in N_2 \Rightarrow v \in N_2 \Rightarrow v \cdot u \in N_2$.
Supposons que $|u| = n + 1$:
Alors $u = xu'$ avec $x \in X$. Si $(xu') \cdot v \in N_2$ alors, par la question 8, $u' \cdot (vx) \in N_2$. Et comme $u' \leq n$, par hypothèse de récurrence,$(vx) \cdot u' \in N_2$, i.e. $v \cdot u \in N_2$.
Image mentale : Écrivons un mot w de longueur ℓ sur un cercle, et supposons que w appartient à N_2. Par la qu. 8, en faisant tourner le cercle de $2\pi/\ell$, on obtient encore un mot de N_2. En faisant tourner le cercle de $2 \cdot |u| \cdot \pi/\ell$ on obtient un mot de N_2, puisque l'on itère $|u|$ fois la rotation précédente.

PARTIE 2 : le groupe libre.

10- Montrons, par récurrence sur n, la propriété $REF(n)$

$$\forall u \in X^*, |u| \leq n \Rightarrow u \cdot \mathrm{I}(u) \in N_2.$$

Base :$n = 0$.
Comme $\varepsilon \in N_2$, $REF(0)$ est vraie.
Induction : soit $n > 0$
$u = xv$ et $|v| \leq n$.

$$u\mathrm{I}(u) = xv\mathrm{I}(v)\theta(x)$$

Par hypothèse de récurrence $v\mathrm{I}(v) \in N_2$ et par la question 6,

$$x \cdot (v\mathrm{I}(v)) \cdot \theta(x) \cdot \varepsilon \in N_2$$

i.e. $u\mathrm{I}(u) \in N_2$.
Donc pour tout $u \in X^*, u \equiv u$.
11- Supposons que $u \equiv v$.
Par définition de $\equiv$ on a donc :

$$u \cdot \mathrm{I}(v) \in N_2.$$

Comme N_2 est clos par I (qu. 5) :

$$\mathrm{I}(u \cdot \mathrm{I}(v)) \in N_2,$$

et par les propriétés de I vues à la question 3 :

$$v \cdot \mathrm{I}(u) \in N_2,$$

ce qui montre, par définition de $\equiv$ que :

$$v \equiv u.$$

12-

12.1- Si $v \in N_2$, par la qu. 6, $x\theta(x)v \in N_2$.
Prouvons par récurrence sur $|v|$ que $x\theta(x)v \in N_2 \Rightarrow v \in N_2$.
Supposons que $x\theta(x)v \in N_2$.
Base : $|v| = 0$.
Dans ce cas $v \in N_2$.
Induction : $|v| = n + 1$.
Il existe une dérivation dans la grammaire G' de la forme :

$$S \to w' \to^*_{G'} x\theta(x)v \tag{5}$$

Cas 1 : $w' = SS$
Par le lemme fondamental, $x\theta(x)v = w_1w_2$ avec $w_1, w_2 \in N_2 - \{\varepsilon\}$. Comme w_1 ne peut être réduit à x, on doit avoir :

$$w_1 = x\theta(x)v_1 \quad \text{et } v = v_1w_2$$

(voir la figure 1) Par hypothèse de récurrence, $v_1 \in N_2$ et par la qu. 4, $v = v_1w_2 \in N_2$.

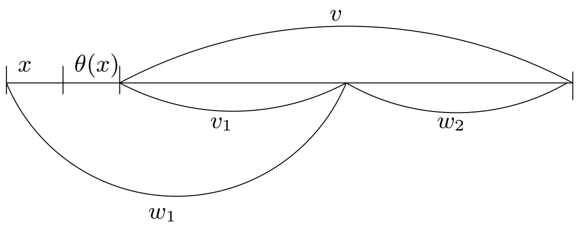

Fig. 1 – q.12, cas 1

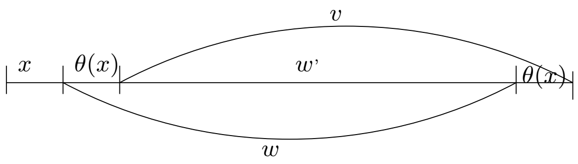

Fig. 2 – q.12, cas 2

Cas 2 : $w' = xS\theta(x)$
Par le lemme fondamental, $x\theta(x)v = xw\theta(x)$ avec $w \in N_2 - \{\varepsilon\}$. Donc, le mot w est de la forme $\theta(x)w'$ et on a :

$$\theta(x)w' \in N_2, \;\; w'\theta(x) = v$$

(voir la figure 2). Par la question 8, il suit que $v \in N_2$. Seuls ces deux cas de règles de G' sont possibles car le mot v est non-vide.

12.2- Soient $x \in X, u, v \in X^*$.

$$\begin{aligned} u \cdot x\theta(x) \cdot v \in N_2 \quad &\Leftrightarrow x\theta(x) \cdot v \cdot u \in N_2 && \text{par la qu. 9} \\ &\Leftrightarrow v \cdot u \in N_2 && \text{par la qu. 12.1} \\ &\Leftrightarrow u \cdot v \in N_2 && \text{par la qu. 9 .} \end{aligned}$$

12.3- Par récurrence sur la longueur de w, [on décompose w en $w' \cdot x$] on déduit de la qu. 12.2 que : pour tous $w, u, v \in X^*$,

$$u \cdot w\mathrm{I}(w) \cdot v \in N_2 \Leftrightarrow u \cdot v \in N_2.$$

13- Supposons que $u \equiv v$ et $v \equiv w$. Alors

$$u \cdot \mathrm{I}(v) \in N_2 \text{ et } v \cdot \mathrm{I}(w) \in N_2.$$

Comme N_2 est clos par produit (qu. 4),

$$u \cdot \mathrm{I}(v) \cdot v \cdot \mathrm{I}(w) \in N_2,$$

En posant $w_1 := \mathrm{I}(v)$ et en tenant compte du fait que $\mathrm{I}(\mathrm{I}(v)) = v$ (qu. 3), on obtient :

$$u \cdot (w_1\mathrm{I}(w_1)) \cdot \mathrm{I}(w) \in N_2,$$

ce qui, d'après la qu. 12.3, entraîne que

$$u \cdot \mathrm{I}(w) \in N_2,$$

i.e. $u \equiv w$.
14- Soient $\alpha, u, v \in X^*$ tels que $u \equiv v$.
Alors $u\mathrm{I}(v) \in N_2$. Par ailleurs $\mathrm{I}(\alpha) \equiv \mathrm{I}(\alpha)$ (qu. 10), donc $\mathrm{I}(\alpha)\alpha \in N_2$. Comme N_2 est clos par produit (qu. 4)

$$\mathrm{I}(\alpha)\alpha u\mathrm{I}(v) \in N_2$$

et par la qu.9

$$\alpha u\mathrm{I}(v)\mathrm{I}(\alpha) \in N_2$$

i.e. $\alpha u \equiv \alpha v$.
15- Soient $\beta, u, v \in X^*$ tels que $u \equiv v$.
Alors $u\mathrm{I}(v) \in N_2$. Par la qu. 12.3 on a :

$$u\beta\mathrm{I}(\beta)\mathrm{I}(v) \in N_2$$

i.e. $u\beta \equiv v\beta$.
16- Supposons que $u \equiv u', v \equiv v'$.

$$\begin{aligned} u \equiv u' \quad &\Rightarrow uv \equiv u'v && \text{par la qu. 15} \\ v \equiv v' \quad &\Rightarrow u'v \equiv u'v' && \text{par la qu. 14} \end{aligned}$$

et par transitivité de $\equiv$ (qu. 13), on obtient : $uv \equiv u'v'$.
17- Supossons que $u \equiv v$. Alors $u\mathrm{I}(v) \in N_2$, donc $\mathrm{I}(u\mathrm{I}(v)) \in N_2$ (qu. 5), donc $\mathrm{I}(\mathrm{I}(v))\mathrm{I}(u) \in N_2$

(par la qu. 3), donc $\mathrm{I}(u)\mathrm{I}(\mathrm{I}(v)) \in N_2$ (par la qu. 9) i.e. $\mathrm{I}(u) \equiv \mathrm{I}(v)$.
18- Il découle de la question 16 que la classe produit ne dépend que des classes arguments (et non des représentants choisis u, v).
19.1- L'associativité du produit de classes découle de l'associativité du produit de concaténation. On vérifie aussi que, puisque ε est élément neutre pour le produit de concaténation, sa classe est élément neutre pour le produit des classes.
19.2- Par définition :

$$[u]_{\equiv} \cdot [\mathrm{I}(u)]_{\equiv} = [u \cdot \mathrm{I}(u)]_{\equiv}.$$

Or $u\mathrm{I}(u) \in N_2$ (par la qu. 10, par exemple), donc $(u\mathrm{I}(u)) \cdot \mathrm{I}(\varepsilon) \in N_2$ i.e. $u\mathrm{I}(u) \equiv \varepsilon$. Donc

$$[u]_{\equiv} \cdot [\mathrm{I}(u)]_{\equiv} = [\varepsilon]_{\equiv}.$$

Comme $\mathrm{I}(\mathrm{I}(u)) = u$ (qu.3), l'égalité précédente, pour $\mathrm{I}(u)$, s'écrit

$$[\mathrm{I}(u)]_{\equiv} \cdot [u]_{\equiv} = [\varepsilon]_{\equiv}.$$

Les deux égalités précédentes montrent que $[\mathrm{I}(u)]_{\equiv}$ est un inverse pour $[u]_{\equiv}$ dans le monoide F_2. Donc F_2 est un groupe (i.e. un monoïde dont tout élément est inversible).
20- Soit $u \in X^*$.

$$\begin{aligned} u \in N_2 \quad &\Leftrightarrow u \cdot \mathrm{I}(\varepsilon) \in N_2 && \text{car } \mathrm{I}(\varepsilon) = \varepsilon \\ &\Leftrightarrow u \equiv \varepsilon && \text{definition de } \equiv \\ &\Leftrightarrow u \in [\varepsilon]_{\equiv} && . \end{aligned}$$

PARTIE 3 : le problème de l'inclusion.

21- On vérifie que, dans tout groupe G :

$$(xy) = (xy')(x'y')^{-1}(x'y)$$

En se plaçant dans F_2 :

$$[uv] = [uv'][u'v']^{-1}[u'v]$$

(on a omis les indices $\equiv$ dans cette notation pour les classes). Dans le cas où $[uv'] = [u'v'] = [u'v] = [\varepsilon]$ on obtient que

$$[uv] = [\varepsilon]^3 = [\varepsilon]$$

donc $uv \equiv \varepsilon$.
22- Notons $\mathcal{A} =< X, Q, D, A, \delta >$. Choisissons $K := 2Card(Q)$. Soit $w \in L_{\mathcal{A}}, |w| \geq K$. Soit c un calcul réussi de $\mathcal{A}$ sur le mot w :

$$c = (q_0, x_1, q_1)...(q_{i-1}, x_i, q_i)...(q_{n-1}, x_n, q_n) \text{ où } n = |w|.$$

Comme $n+1 \geq 2Card(Q)+1$, l'un au moins des états de Q apparaît trois fois dans ce calcul :

$$\exists i, j, k \in \mathbb{N}, 0 \leq i < j < k \leq n, \quad q_i = q_j = q_k.$$

Posons :

$$\alpha = t((q_0, x_1, q_1)...(q_{i-1}, x_k, q_i)), \quad u_1 = t((q_i, x_{i+1}, q_{i+1})...(q_{j-1}, x_j, q_j)), \quad u_2 = t((q_j, x_{j+1}, q_{j+1})...(q_{k-1}, x_k, q_k)),$$

(on rappelle que t est l'application *trace* qui efface les états dans le calcul). On vérifie le point (1) aisément.
Comme $i < j < k$ les mots u_1, u_2 ne sont pas vides (point (2)).
Comme $q_i = q_j = q_k$ on obtient que :

$$\alpha\{u_1, u_2\}^*\beta \subseteq L_{\mathcal{A}}.$$

23- En posant : $u := \alpha, u' := \alpha u_1, v := \beta, v' := u_2\beta$ et en appliquant le résultat de la qu. 21, on obtient que :

$$(\alpha\beta \equiv \varepsilon \quad \wedge \quad \alpha u_1\beta \equiv \varepsilon \quad \wedge \quad \alpha u_2\beta \equiv \varepsilon) \Rightarrow \alpha u_1 u_2\beta \equiv \varepsilon.$$

24- Soit w un mot de longueur minimale de $L_{\mathcal{A}} - N_2$. Si $|w| \geq K$ alors w a une factorisation de la forme donnée à la qu. 22. Comme $\alpha\beta, \alpha u_1\beta, \alpha u_2\beta$ sont dans $L_{\mathcal{A}}$ (condition (3) de la qu. 22) et comme ils sont strictement plus courts (condition (2)), par minimalité de w, ils appartiennent à N_2. Mais, par la qu. 23, on en déduit que $w \in N_2$, ce qui est contraire à notre hypothèse. Un tel mot w n'existe donc pas. Autrement dit :

$$L_{\mathcal{A}} - N_2 = \emptyset \Leftrightarrow \{w \in L_{\mathcal{A}} - N_2 \mid |w| < K\} = \emptyset.$$

Pour tester si $L_{\mathcal{A}} \subseteq N_2$ il suffit donc de tester si

$$\forall w \in X^*, (|w| < K \text{ et } w \in L_{\mathcal{A}}) \quad \Rightarrow \quad w \in N_2.$$

Schéma d'algorithme :
- Énumérer les mots de longueur $< K$
- pour chacun d'eux : tester si $w \in L_{\mathcal{A}} \Rightarrow w \in N_2$
- si l'un deux ne vérifie pas cette inmplication , alors $L_{\mathcal{A}} \not\subseteq N_2$, sinon $L_{\mathcal{A}} \subseteq N_2$.