Outils mathématiques pour l'Informatique
notes de cours

Géraud Sénizergues

Année 2002-2003 [1]

[1] dernière mise à jour : 25 septembre 2003

Table des matières

Chapitre 1

Introduction

Ce texte est un document de soutien du cours d' OMI de la Licence Informatique. La durée de l'enseignement est de 24 heures de cours et 36 heures de TD.

Sujet Nous présentons ici divers "outils" mathématiques couramment utilisés en informatique.
Ces outils comprennent certains procédés calculatoires apparus dans les mathématiques du dix-huitième siècle (les séries génératrices), certaines structures algébriques apparues au dix-neuvième siècle (les anneaux, les algèbres), une théorie qui a contribué à l' éclosion puis au développement de l'informatique (la logique mathématique) et enfin une théorie partiellement suscitée par le développement de l'informatique (la théorie des langages formels, apparue dans les années 1950-1960).

Quelques problèmes
En guise de provocation, nous soumettons à la sagacité du lecteur les problèmes qui suivent.
PROBLÈME 1
On considère l'ensemble L des mots sur l' alphabet $\{0, 1\}$ défini par la for-

mule suivante :

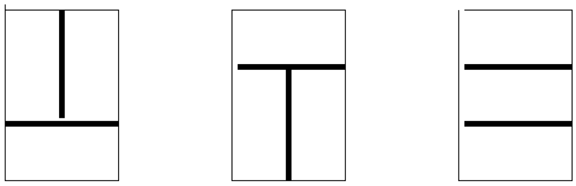
$$L = \overline{(0 \cdot \{0,11\}^* \cdot 1)} \cdot 1 \cap \{01,1\}^*.$$

Dans cette formule,pour tout ensemble de mots M on note :
$\overline{M} = \{u \text{ mot sur l'alphabet } 0,1 \mid u \notin M\}$
$M^* = \{u = u_1 \cdot u_2 \cdots u_n \mid n \in \mathbb{N}, u_1, u_2, \ldots, u_n \in M\}$.
QUESTION : Construire un circuit séquentiel à une seule entrée, et une seule sortie, tel que, après avoir lu une suite quelconque u de symboles $0, 1$, le circuit renvoie la sortie 1 si et seulement si le mot u appartient à L.

PROBLÈME 2
Soit $F = \{a, b, c\}$ un ensemble de trois symboles.
On considère deux ensembles d'arbres :
$M(\{\cdot\} \cup F)$: c'est l'ensemble des "termes bien formés" sur le symbole binaire $\cdot$ et les symboles 0-aires (les "constantes") a, b, c.
$\mathcal{A}(F)$: c'est l'ensemble des arbres planaires à sommets étiquetés sur F.
QUESTION :
Définir une bijection $\varphi : M(\{\cdot\} \cup F) \to \mathcal{A}(F)$, "calculable" (en un sens intuitif). On doit, en particulier, pouvoir calculer "à la main" $\varphi(t)$ pour t terme à au plus 10 noeuds.

PROBLÈME 3 (***)
On considère l'ensemble des "théorèmes vrais" d'une théorie mathématique. Après s'être donné des définitions suffisamment précises, on devrait pouvoir distinguer les énoncés mathématiques "bien-formés" (peut-être faux mais syntaxiquement corrects), des énoncés "mal-formés" (tellement bizarres qu'on dirait familièrement qu'ils n'ont "ni queue ni tête"). A l'intérieur des énoncés bien-formés on souhaiterait découvrir ceux qui sont *vrais*.
QUESTION Pour quelles théories le langage des énoncés *vrais* peut-il être engendré mecaniquement, par un nombre fini de règles simples ?

PROBLÈME 4
On cherche à déterminer le nombre de façons différentes de paver un rectangle de dimension $3 \times n$ par des rectangles de dimension 1×2 ou 2×1. Un rectangle de dimension 1×2 sera nommé "domino horizontal", un rectangle de dimension 2×1 sera nommé "domino vertical" (voir figure 2.2.3). Pour tout entier $n \geq 0$ nous notons u_n le nombre de pavages d'un rectangle de dimension $3 \times n$ par des dominos (chaque domino peut être vertical ou horizontal)



Pavages du rectangle 3×2

Pavages du rectangle 3×3, privé de son carré NO.

FIG. 1.1 –

QUESTION :
Donner une formule (simple) exprimant u_n en fonction de n.

Sources
Ce cours polycopié est exempt de toute originalité. Les résultats exposés font partie de ce que l'on pourrait appeler le "noyau dur" de l'informatique théorique. L'exposition elle-même suit essentiellement les références suivantes :

1. [Aut94, pages 11-17,41-65] a inspiré
   Monoïde libre, expressions rationnelles et automates finis.
2. [AG93, pages 24-32] a inspiré
   Ensembles ordonnés- Treillis
3. [AG93, pages 33-48] a inspiré

Construction par induction- Induction structurelle.
Exception : la preuve du théorème 4.2.5.

4. [Jac85, pages 474-479] a inspiré
   Algèbres de Boole et anneaux de Boole.

5. [AG93, pages 59-61] et [Xuo92, pages 140-146] ont inspiré Fonctions booléennes
   Exception : la preuve du théorème 6.4.9.

6. [AG93, pages 66-68] a inspiré
   Formules propositionnelles : syntaxe et sémantique

7. [Hue86, pages 8-17] a inspiré
   Un premier système formel
   [Lal90, pages 113-114,125] a inspiré
   Un second système formel

8. [Car61, pages 9-14] a inspiré
   Séries formelles.
   [BBC94, pages 20-26] a inspiré
   Récurrences linéaires.

Chapitre 2

Monoïde libre, expressions rationnelles et automates finis.

2.1 Monoïdes

Définition 2.1.1 *Un monoïde est un triplet $\mathcal{M} = (M, \cdot, e)$, où M est un ensemble M, $\cdot$ est une opération associative sur M et e est l' élément neutre de M pour cette loi.*

Soit X un ensemble. Un *mot* sur l'alphabet X est, par définition, une application partant d'un intervalle $[1, n]$ de $\mathbb{N}$ et arrivant dans l'ensemble X : $u : [1, n] \to X$.
Le mot particulier correspondant à l'application vide est dénommé le "mot vide" et noté ϵ.
On dénote par X^*, l'ensemble des mots écrits sur l'alphabet X.
Soient $u : [1, n] \to X, v : [1, m] \to X$ deux mots. Le *produit de concaténation* de u par v est le mot w obtenu en juxtaposant u et v. Formellement, $w = u \cdot v$ est défini par :

$$\mathrm{dom}(w) = [1, n + m], \ \ \forall i \in [1, n], w[i] = u[i]; \ \ \forall j \in [1, m], w[i + j] = v[j].$$

Remarquons que, pour tout $u \in X^*$
$$u \cdot \epsilon = \epsilon \cdot u = u.$$

Définition 2.1.2 *Pour tout alphabet X, $(X^*, \cdot, \epsilon)$ est un monoïde. On l'appelle le "monoïde libre engendré par X".*

Définition 2.1.3 *Soit $\mathcal{M} = (M, \cdot, e)$. Un* sous-monoïde *de $\mathcal{M}$ est un triplet $\mathcal{M}' = (M^{'}, \odot, e')$ tel que :*
- $M' \subseteq M$
- $e' = e$
- $\forall m, m^{'} \in M', m \odot m' = m \cdot m'$.

Si I est un ensemble d' indice et si $\forall i \in I, \mathcal{M}_i = (M_i, \cdot, e)$ est un sous-monoïde de $\mathcal{M}$, alors $(\bigcap_{i \in I} M_i, \cdot, e)$ est un sous-monoïde de $\mathcal{M}$.

Définition 2.1.4 *Soit Y une partie d'un monoïde M. On appelle* sous-monoïde engendré par *Y, le plus petit sous-monoïde de $\mathcal{M}$ contenant Y. On le note Y^*.*

D'après ce qui précède, Y^* est l'intersection de tous les sous-monoïdes de $\mathcal{M}$ qui contiennent Y.

Exemple 2.1.5 *Soit $\mathcal{N} = (\mathbb{N}, +, 0)$. Soit A l' ensemble des nombres pairs et B l' ensemble des nombres impairs. $(A, +, 0)$ est le sous-monoïde de $\mathcal{N}$ engendré par $\{2\}$ tandis que $(B, +, 0)$ n' est pas un sous-monoïde de $\mathcal{N}$.*

Définition 2.1.6 *Soient $\mathcal{M} = (M, \cdot, e)$,$\mathcal{M}^{'} = (M^{'}, \times, e^{'})$ des monoïdes. On appelle* homomorphisme *(de monoïde) allant de $\mathcal{M}$ dans $\mathcal{M}'$, toute application h de M dans M' verifiant :*
- $h(e) = e'$
- $\forall m, m' \in \mathcal{M}, h(m \cdot m') = h(m) \times h(m')$

Exemple 2.1.7 *L' application qui à un mot u associe sa longueur $|u|$ est un homomorphisme de $(X^*, \cdot, \varepsilon)$ dans $(\mathbb{N}, +, 0)$.*

L'application $n \mapsto 2^n$ est un homomorphisme de $(\mathbb{N}, +, 0)$ dans $(\mathbb{N}, \times, 1)$.

Théorème 2.1.8 *Soit X un alphabet. Soit $(M, \cdot, e)$ un monoïde et soit h une application de X dans M. Il existe un et un seul homomorphisme $\tilde{h}$: $X^* \longrightarrow M$ tel que $\forall x \in X, \tilde{h}(x) = h(x)$.*

Le monoïde X^* est appelé le monoïde *libre* engendré par X. La propriété énoncée dans le théorème 2.1.8 est la *propriété universelle* du monoïde libre sur X. On peut démontrer qu'elle caractérise (à isomorphisme près) le couple (X, X^*).
Preuve : Existence : Posons $\tilde{h}(\varepsilon) = e$ et $\tilde{h}(x_1...x_n) = h(x_1) \cdot ... \cdot h(x_n)$. Il est facile de voir que $\tilde{h}$ est bien un homomorphisme.

Unicité :Soient g et $g^{'}$ deux homomorphismes de X^* dans M tels que $\forall x \in X, g(x) = g'(x)$. Alors $g(\varepsilon) = g^{'}(\varepsilon) = e$ et pour tout mot $u = x_1...x_n$,

$$g(u) = g(x_1) \cdot ... \cdot g(x_n) = g^{'}(x_1) \cdot ... \cdot g^{'}(x_n) = g^{'}(u). \tag{2.1}$$

C' est à cause de ce théorème que le monoïde X^* est appelé le monoïde *libre* engendré par X. $\square$

On appelle *langage* sur l'alphabet X, toute partie de X^* .

2.2 Langages reconnaissables

Définition 2.2.1 *Un* automate *est un 5-uplet, $\mathcal{A} =< X, Q, D, A, \delta >$ où*
- *X est un ensemble fini,l'alphabet d' entrée*
- *Q est un ensemble, l' ensemble des états*
- *$D \subset Q$ est l' ensemble des etats de départ*
- *$A \subset Q$ est l' ensemble des etats d'arrivée*
- *$\delta \subset Q \times X \times Q$ est l' ensemble des transitions*

Définition 2.2.2 *Un automate* fini *est un automate $\mathcal{A} =< X, Q, D, A, \delta >$ dont l'ensemble d' états, Q, est fini.*

Exemple 2.2.3 *Posons*

$X = \{a, b\}, Q_1 = \{1, 2\}, D_1 = \{1\}, A_1 = \{2\}, \delta_1 = \{(1, a, 1), (1, b, 2), (2, b, 2)\}.$

$\mathcal{A}_1 =< X, Q_1, D_1, A_1, \delta_1 >$ *est un automate fini.*

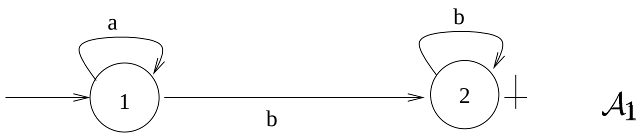


FIG. 2.1 – representation graphique.

Exemple 2.2.4 *Soit*

$$Q_2 = \{1,2,3,4,5\}, D_2 = \{1,4\}, A_2 = \{3,5\},$$

$$\delta_2 = \{(1,a,1),(1,b,1),(1,a,2),(2,a,3),(4,a,5),(5,b,4)\}.$$

$\mathcal{A}_2 =< X, Q_2, D_2, A_2, \delta_2 >$ *est un automate fini.*

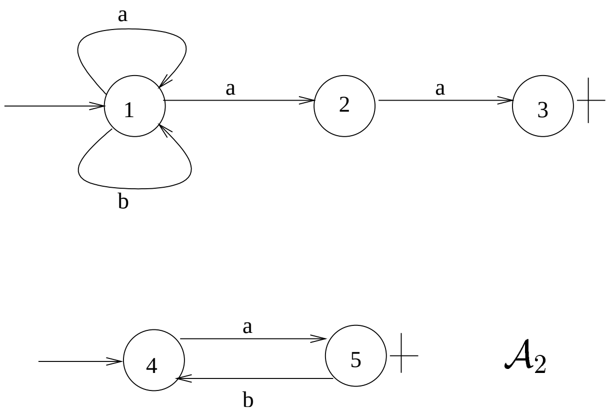


FIG. 2.2 – representation graphique.

Soit $\mathcal{A} =< X, Q, D, A, \delta >$ un automate fini.
Un mot w de δ^* est un *chemin* dans $\mathcal{A}$ ssi il s'écrit

$$w = (q_1, x_1, q_1^{'})(q_2, x_2, q_2^{'})...(q_i, x_i, q_i^{'})...(q_n, x_n, q_n^{'}) \tag{2.2}$$

et il vérifie la condition :

$$w = \varepsilon \text{ ou } \forall i \in [1, n-1], q_i^{'} = q_{i+1}$$

– n est la longueur du chemin
– ce chemin mène de l'état q_1 à l'état q_n
– on convient que ε mène de q à q (pour tout $q \in Q$)

Définition 2.2.5 *On appelle* trace *l'homomorphisme* $t : \delta^* \longrightarrow X^*$ *tq*

$$\forall (q, x, q^{'}) \in \delta, t((q, x, q^{'})) = x$$

Définition 2.2.6 *Un mot* $u \in X^*$ *est accepté (ou reconnu) par* $\mathcal{A}$, *ssi il existe un chemin* w *dans* $\mathcal{A}$ *menant d'un état* $q_d \in D$ *à un état* $q_a \in A$ *et tel que* $t(w) = u$.

Définition 2.2.7 *On appelle langage accepté (ou reconnu) par* $\mathcal{A}$, *noté* $L_{\mathcal{A}}$, *l' ensemble des mots acceptés (ou reconnnus) par* $\mathcal{A}$.

Exemple 2.2.8 *(suite des exemples 2.2.3,2.2.4).*

$$L_{\mathcal{A}_1} = \{a^n b^m | n \geq 0, m \geq 1\}; \quad L_{\mathcal{A}_2} = \{uaa | u \in \{a, b\}^*\} \cup \{a(ba)^n | n \geq 0\}$$

Notation :

$$\mathcal{A} < p, q > = < X, Q, \{p\}, \{q\}, \delta >$$

$$L_{\mathcal{A}} = \cup_{(p,q) \in D \times A} L_{\mathcal{A}<p,q>}$$

□

Définition 2.2.9 *Un langage* $L \subset X^*$ *est dit* reconnaissable *ssi, il existe un automate fini* $\mathcal{A}$ *sur* X, *tq* $L = L_{\mathcal{A}}$. *On note* $Rec(X^*)$ *l'ensemble des langages reconnaissables sur* X^*.

Exemple 2.2.10 $\mathcal{A}_1$ *est un automate deterministe (localement il n'a qu'un choix par lettre). Ce n'est pas le cas de* $\mathcal{A}_2$.

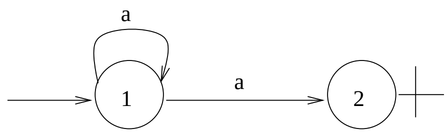


FIG. 2.3 – 2 choix possibles dans l'état 1 pour lire a

Définition 2.2.11 *Un automate $\mathcal{A} =< X, Q, D, A, \delta >$ est* déterministe *ssi*

- *(1)* $Card(D) = 1$
- *(2)* $\forall q \in Q, \forall x \in X, Card(\{q^{'} \in Q, (q, x, q^{'}) \in \delta\}) \leq 1$

$\mathcal{A}$ *est dit* déterministe complet *ssi*
- *(1)* $Card(D) = 1$
- *(2)* $\forall q \in Q, \forall x \in X, Card(\{q' \in Q | (q, x, q') \in \delta\}) = 1$

Remarque 2.2.12 *La simulation d'un automate fini déterministe complet par un programme est très simple.*

Notation :
Lorsque $\mathcal{A}$ est déterministe, on utilise la notation fonctionnelle

$$\delta : Q \times X \longrightarrow Q$$

La fonction δ s'étend en une unique fonction $\tilde{\delta} : Q \times X \longrightarrow Q$ vérifiant :
- $\forall q \in Q, \tilde{\delta}(q, \epsilon) = q$
- $\forall q \in Q, \forall u \in X^*, \forall x \in X, \tilde{\delta}(q, u, x) = \delta(\tilde{\delta}(q, u), x)$

Si $\mathcal{A}$ est déterministe complet, alors $\tilde{\delta}$ est une application.

Proposition 2.2.13 *Un langage est reconnaissable ssi il est reconnu par un automate fini déterministe complet.*

Preuve : Soit $L = L_{\mathcal{A}}$ où $\mathcal{A} =< X, Q, D, A, \delta >$. Construisons un automate fini déterministe complet $\mathcal{B}$ tel que $L_{\mathcal{A}} = L_{\mathcal{B}}$. Posons

$$\mathcal{B} =< X, \mathcal{P}(Q), \{D\}, \mathcal{R}, \triangle >$$

où $\mathcal{R} = \{P \in \mathcal{P}(Q), P \cap A \neq \emptyset\}$

$$\triangle : \mathcal{P}(Q) \times X \longrightarrow \mathcal{P}(Q)$$

$$(P, x) \longrightarrow \{q \in Q, \exists p \in P, (p, x, q) \in \delta\}$$

On démonte par récurrence sur $|u|$ que : $\forall u \in X^*, \forall P \in \mathcal{P}(Q)$,

$$\tilde{\triangle}(P, u) = \{q \in Q, \exists p \in P, \exists w \in \delta^*, t(w) = u \text{ et } w \text{ mène de } p \text{ à } q\}$$

$$\begin{aligned}
u \in L_{\mathcal{A}} &\Leftrightarrow \exists w \in \delta^*, \exists q_d \in D, \exists q_a \in A, t(w) = u \text{ et } w \text{ est un chemin qui mène de } q_d \text{ à } q_a \\
&\Leftrightarrow \exists q_a \in A, \tilde{\triangle}(D, u) \ni q_a \\
&\Leftrightarrow \tilde{\triangle}(D, u) \cap A \neq \emptyset \\
&\Leftrightarrow \tilde{\triangle}(D, u) \in \mathcal{R}.
\end{aligned}$$

$\mathcal{B}$ est déterministe complet car $\triangle$ est une application. □

Remarque 2.2.14 *Si $\mathcal{A}$ a n états, alors $\mathcal{B}$ a 2^n états*

Proposition 2.2.15 *Si $L \subseteq X^*$ est reconnaissable alors $X^* - L$ est reconnaissable.*

Preuve : Soit $L = L_{\mathcal{A}}$, où

$$\mathcal{A} =< X, Q, d, A, \delta >$$

(δ application).
Posons

$$\mathcal{B} =< X, Q, d, Q - A, \delta > .$$

Montrons que $X^* - L_{\mathcal{A}} = L_{\mathcal{B}}$ Soit $u \in X^*$. On a la suite d' équivalences :
$u \in X^* - L_{\mathcal{A}} \Leftrightarrow \tilde{\triangle}(d, u) \notin A \Leftrightarrow \tilde{\triangle}(d, u) \in Q - A$. □

Proposition 2.2.16 *Si $L \subseteq X^*$ est fini, alors L est reconnaissable.*

Preuve : Soit $L \subset X^*, Card(L) < +\infty$ Soit $\mathcal{A} =< X, Q, d, A, \delta >$ où

$$Q = Pref(L) = \{u \in X^*, \exists v \in X^*, u \cdot v \in L\}$$

$$\delta : Q \times X \longrightarrow Q$$

$$(u, x) \mapsto ux$$

si $ux \in Pref(L)$, sinon (u, x) n'a pas d'image par δ.

$$d = \varepsilon$$

$$A = L$$

On a bien :

$$\forall u \in X^*, \tilde{\delta}(\varepsilon, u) \in L \Leftrightarrow u \in L.$$

□

Exemple 2.2.17 *Lorsque* $L = \{a, aa, aab, ab, ba, bba\}$, $\mathcal{A}$ *est l'automate représenté sur la figure 2.4.*

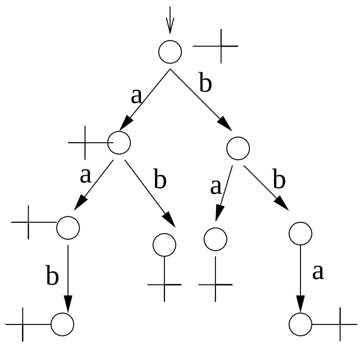


FIG. 2.4 –

Proposition 2.2.18 *$Rec(X^*)$ est fermé par union.*

Preuve : Soient $L_1 = L_{\mathcal{A}_1}, L_2 = L_{\mathcal{A}_2}$

$$\mathcal{A}_1 =< X, Q, D_1, A_1, \delta_1 >, \mathcal{A}_2 =< X, Q, D_2, A_2, \delta_2 >$$

On suppose que $Q_1 \cap Q_2 = \emptyset$. Posons :

$$\mathcal{A} =< X, Q_1 \cup Q_2, D_1 \cup D_2, A_1 \cup A_2, \delta_1 \cup \delta_2 > .$$

On vérifie que $L_{\mathcal{A}} = L_{\mathcal{A}_1} \cup L_{\mathcal{A}_2}$. $\square$

Proposition 2.2.19 *$Rec(X^*)$ est fermé par produit.*

Idée naïve : supposons que $L_1 = L_{\mathcal{A}_1}, L_2 = L_{\mathcal{A}_2}$. On construit l'union des deux automates $\mathcal{A}_1, \mathcal{A}_2$, dans laquelle on fusionne l'état final de $\mathcal{A}_1$ avec l'état initial de $\mathcal{A}_2$.

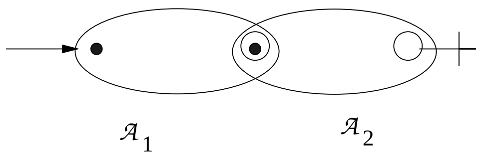


FIG. 2.5 – L' idée ...

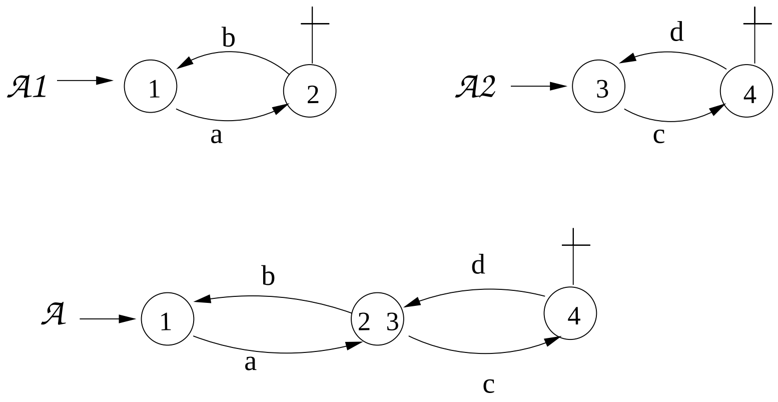


FIG. 2.6 – ... et son contre-exemple !

Dans l'exemple de la figure 2.6, on obtient un automate $\mathcal{A}$ tel que :

$$acdbac \in L_{\mathcal{A}} - L_{\mathcal{A}_1} \cdot L_{\mathcal{A}_2}$$

Il faut donc améliorer cette idée de départ.

Preuve de la proposition 2.2.19 : Considérons des automates finis $\mathcal{A}_1$, $\mathcal{A}_2$ tels que $L_1 = L_{\mathcal{A}_1}, L_2 = L_{\mathcal{A}_2}$.

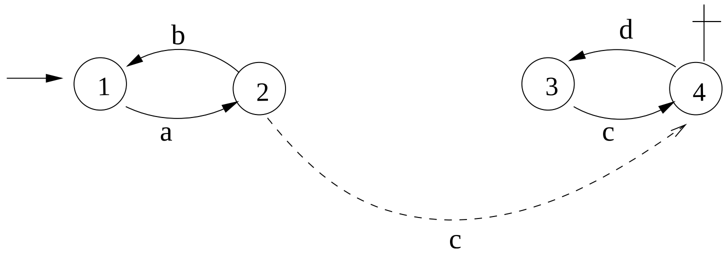


FIG. 2.7 – Exemple de produit (de concaténation).

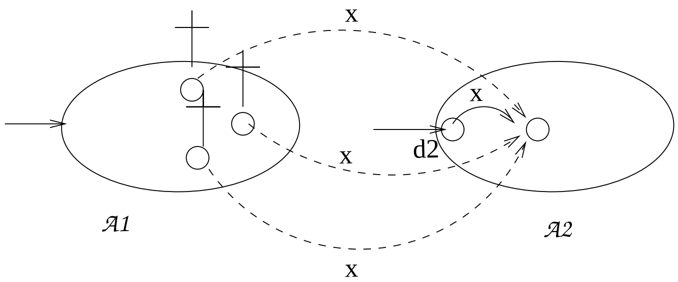


FIG. 2.8 – Produit (de concaténation)

$$\mathcal{A}_1 =< X, Q_1, D_1, A_1, \delta_1 >$$
$$\mathcal{A}_2 =< X, Q_2, D_2, A_2, \delta_2 >$$
$$\mathcal{A} =< X, Q_1 \cup Q_2, D_1, A, \delta >$$
$$\delta = \delta_1 \cup \delta_2 \cup \{(q, x, q') \in A_1 \times X \times Q_2 | \exists d_2 \in D_2, (d_2, x, q') \in \delta_2\}$$
$$A = A_2 \text{ si } D_2 \cap A_2 = \emptyset; \;\; A = A_1 \cup A_2 \text{ si } D_2 \cap A_2 \neq \emptyset.$$

On vérifie que $L_{\mathcal{A}} = L_{\mathcal{A}_1} \cdot L_{\mathcal{A}_2}$. □

Définition 2.2.20 *Soit $L \subseteq X^*$. On note $L^* = \bigcup_{n \geq 0} L^n$.*

Remarquons que L^* est bien le sous-monoïde de X^* engendré par L (voir la définition 2.1.4).

Proposition 2.2.21 *$Rec(X^*)$ est fermé par l'opération *.*

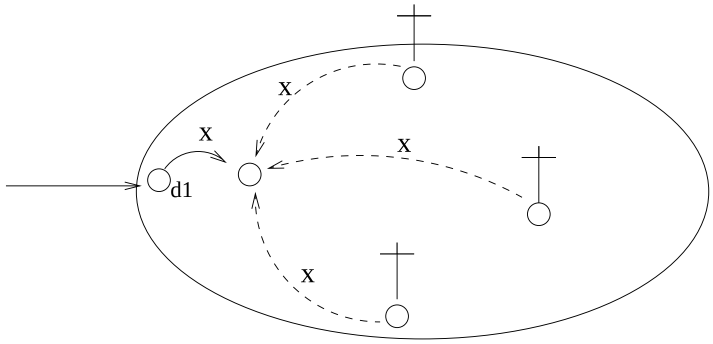


FIG. 2.9 – Opération étoile

Preuve : Soit $L = L_{\mathcal{A}_1}$:

$$\mathcal{A}_1 = < X, Q_1, D_1, A_1, \delta_1 >$$

$$\mathcal{A} = < X, Q_1, \{d_1\}, A, \delta >$$

$$\delta = \delta_1 \cup \{(q, x, q^{'}) \in A_1 \times X \times Q_1 | \exists d_1 \in D_1, (d_1, x, q^{'}) \in \delta_1\}$$

$$A = A_1 \cup D_1.$$

On vérifie que $L_{\mathcal{A}} = (L_{\mathcal{A}_1})^*$. □

Remarque 2.2.22 *Si $X \subseteq Y$ alors $Rec(X^*) \subseteq Rec(Y^*)$.*

2.3 Langages rationnels

Définition 2.3.1 *$Rat(X^*)$ est la plus petite partie de $\mathcal{P}(X^*)$ contenant les langages finis et stable par les opération $\cup, \cdot, *$.*

Notion d'expression rationnelle :

$$\mathcal{X} = \{(,), \cdot, +, *\} \cup X \cup \{\varepsilon\}$$

où

$$Y = \{(,), \cdot, +, *\}$$

On suppose $X \cap (Y \cup \{\varepsilon\}) = \emptyset$

L'ensemble ER (X) des expressions rationnelles sur X est le plus petit langage sur $\mathcal{X}^*$ verifiant :

- (0) $\epsilon \in$ ER (X)
- (1) $\forall x \in X, x \in$ ER (X)
- (2) si $e_1, e_2 \in$ ER (X) alors $(e_1 \cdot e_2) \in$ ER (X)
- (3) si $e_1, e_2, \in$ ER (X) alors $(e_1 + e_2) \in$ ER (X)
- (4) si $e \in$ ER (X) alors $e* \in$ ER (X).

Le fait qu'il existe un *plus petit* langage sur $\mathcal{X}^*$ vérifiant ces conditions n'est pas tout à fait évident ; nous en donnerons une justification, sous une forme plus générale, après la définition 4.2.1.
Le langage dénoté par une expression rationnelle est défini récursivement par :

$$\Pi : \text{ ER } (X) \longmapsto \mathcal{P}(X^*)$$

$$\epsilon \longmapsto \{\epsilon\}$$

$$x \in X \longmapsto \{x\}$$

$$(e_1 \cdot e_2) \longmapsto \Pi(e_1) \cdot \Pi(e_2)$$

$$(e_1 + e_2) \longmapsto \Pi(e_1) \cup \Pi(e_2)$$

$$e* \longmapsto \Pi(e*) = (\Pi(e))^*$$

Là aussi, l'existence et l'unicité d'une application Π satisfaisant ces conditions n'est pas tout à fait évidente ; elle repose sur le fait qu'un mot de ER (X) a une décomposition *unique* sous l'une des formes (0),(1),(2),(3) ou (4). Nous en donnerons une justification, sous une forme plus générale, après la définition 4.2.5.

Remarque 2.3.2 *Un langage rationnel est décrit par un infinité d'expressions rationnelles. Par exemple :*

$$(a + b)^* = (a^*b)^*a^*$$

Proposition 2.3.3 *: Soit X un alphabet fini. Alors $Rat(X^*)$ est exactement l' ensemble des langages sur X qui sont de la forme $\Pi(e)$ pour une expression rationnelle $e \in ER(X)$.*

Théorème 2.3.4 *(Kleene) : Soit X un alphabet fini,alors $Rat(X^*) = Rec(X^*)$*

Preuve : 1- $Rec(X^*)$ contient les parties finies et est fermée par $\cup, \cdot, *$. Donc $Rat(X^*) \subseteq Rec(X^*)$.
2-Soit $\mathcal{A} =< X, Q, D, A, \delta >$ un automate fini tel que $L = L_{\mathcal{A}}$.

$$\mathcal{A} =< X, Q, D, A, \delta >$$

$$Q = [1, n]$$

Pour tout calcul w de l'automate $\mathcal{A}$, on note $I(w)$ l'intérieur de ce calcul :
si $w = (q_1, x_1, q_1')(q_2, x_2, q_2')...(q_i, x_i, a_i')...(q_n, x_n, q_n')$ alors $I(w) = \{q_2, \ldots, q_n\}$.
Pour tous $i, j, k \in [1, n]$, on pose alors :

$$L_{i,j}^{(k)} = \{u \in X^* | \exists w \in \delta^*, \text{ chemin de } i \text{ à } j, I(w) \subseteq [1, k]\}.$$

Les formules suivantes sont vraies :

$$\begin{aligned} L_{i,j}^{(0)} &= \{x \in X, (i, x, j) \in \delta\} (\text{si } i \neq j) \\ L_{i,j}^{(0)} &= \{x \in X, (i, x, j) \in \delta\} \cup \{\epsilon\} (\text{si } i = j) \\ L_{i,j}^{(k)} &= L_{i,j}^{(k-1)} \cup L_{i,k}^{(k-1)} (L_{k,k}^{(k-1)})^* L_{k,j}^{(k-1)}. \end{aligned}$$

On prouve ainsi par récurrence sur k :

$$\forall i, j \in [1, n], L_{i,j}^{(k)} \in Rat(X^*).$$

D'où

$$L_{\mathcal{A}} = \bigcup_{(i,j) \in D \times A} L_{\mathcal{A}<i,j>} = \bigcup_{(i,j) \in D \times A} L_{i,j}^{(n)} \in Rat(X^*).$$

□
Question : Les langages suivants sont-ils rationnels ?

$$\begin{aligned} L_1 &= \{a^n b^n | n \geq 1\}, \\ L_2 &= \{f \in \{a, b, c\}^* || f|_a = |f|_b\} \\ L_3 &= \{f \in \{a, b\}^* || f|_a = |f|_b \text{ et pour tout } g \leq f, |g|_a \geq |g|_b\}. \end{aligned}$$

Supposons que $\mathcal{A} =< X, Q, D, A, \delta >$ reconnaît L_1.

Soit $N = Card(Q)$, soit w un calcul de $\mathcal{A}$ sur le mot $a^N b^N$

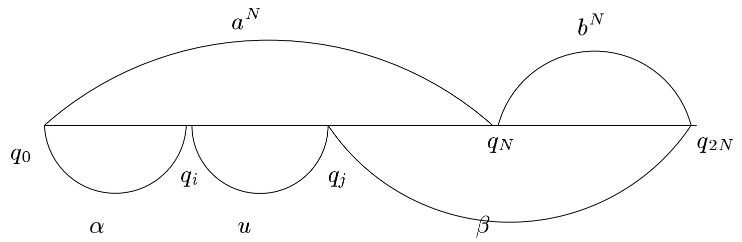


FIG. 2.10 – q_i est répété

$$w = (q_0, x_1, q_1)...(q_{i-1}, x_i, q_i)...(q_{2N-1}, x_{2N}, q_{2N})$$
$$\exists i, j \in \mathbb{N}, 0 \leq i < j \leq N, q_i = q_j.$$

$a^N b^N = \alpha u \beta$ où $q_1 \xrightarrow{\alpha}_{\mathcal{A}} q_i$, $q_i \xrightarrow{u}_{\mathcal{A}} q_j$, $q_j \xrightarrow{\beta}_{\mathcal{A}} q_{2N}$ On en déduit que : $\forall k \in \mathbb{N}, \alpha u^k \beta \in L_{\mathcal{A}}$, en vertu du calcul :

$$q_1 \xrightarrow{\alpha}_{\mathcal{A}} q_i, q_i \xrightarrow{u^k}_{\mathcal{A}} q_i = q_j, q_j \xrightarrow{\beta}_{\mathcal{A}} q_{2N}.$$

Mais $\alpha u^2 \beta \notin L_{\mathcal{A}}$, car $|\alpha u^2 \beta|_a > |\alpha\beta|_b$. L'existence de $\mathcal{A}$ conduit donc à une contradiction.

Lemme 2.3.5 *(de l'étoile) Soit L un langage rationnel.Alors il existe une constante $N > 0$, t.q. pour tout mot $v \in L$,si $|v| \geq N$ alors il existe des mots $\alpha, u, \beta \in X^*$ tq.*
- *(1) $v = \alpha u \beta$*
- *(2) $0 < |u| < N$*
- *(3) $\alpha u^* \beta \subseteq L$*

Preuve : Supposons que $\mathcal{A} =< X, Q, D, A, \delta >$ reconnaît L. Soit $N = Card(Q)$. Soit $v \in L, |u| \geq N$. Soit w un calcul réussi de $\mathcal{A}$ sur le mot v :
- $w = (q_0, x_1, q_1)...(q_{i-1}, x_i, q_i)...(q_{n-1}, x_n, q_n)$ où $n = |u|$
- w est un chemin
- $q_0 \in D, q_n \in A$

– $t(w) = v$.
Comme $n+1 \geq N+1 = Card(Q)+1$, $\exists i, j \in \mathbb{N}, 0 \leq i < j \leq n$ tels que $q_i = q_j$. Soit $(k,\ell) \in [0,n]^2, k < \ell$, tels que $q_k = q_\ell$ et $\forall (i,j) \in [0,n]^2$
Si $i < j$ et $q_i = q_j$ alors $\ell - k < j - i$. On a $\ell - k < N$. Posons :

$$\alpha = t((q_0, x_1, q_1)...(q_{k-1}, x_k, q_k))$$

$$u = t((q_k, x_{k+1}, q_{k+1})...(q_{\ell-1}, x_\ell, q_\ell))$$

$$\beta = t((q_\ell, x_{\ell+1}, q_{\ell+1})...(q_{n-1}, x_n, q_n))$$

On vérifie alors que $\alpha u \beta = t(w) = v$, i.e. le point (1) est vrai.
$\ell > k \Rightarrow |u| > 0, \ell - k < N \Rightarrow |u| < N$, ce qui prouve le point (2).
Pour tout entier $m \geq 0$:

$$q_0 \xrightarrow{\alpha}_{\mathcal{A}} q_k, q_k \xrightarrow{u^m}_{\mathcal{A}} q_k = q_\ell, q_\ell \xrightarrow{\beta}_{\mathcal{A}} q_n.$$

Donc $\alpha u^* \beta \subseteq L$, i.e. (3). $\square$

2.4 Automate minimal

Notation : Soient $u \in X^*, L \subset X^*$

$$u^{-1}L = \{v \in X^* | uv \in L\}$$

$$Lu^{-1} = \{v \in X^* | vu \in L\}$$

On appelle “résiduel”du langage L, tout langage de la forme $u^{-1}L$.

$$\mathbb{Q}(L) = \{u^{-1}L | u \in X^*\}$$

Théorème 2.4.1 *(Myhill-Nerode) :* $L \in Rec(X^*) \Leftrightarrow \mathbb{Q}(L)$ *est fini.*

Preuve : 1)Supposons que $L \in Rec(X^*)$. Soit $\mathcal{A} =< X, Q, \{d\}, A, \delta >$ un automate déterministe complet reconnaissant L. Considérons les trois applications :

$$\varphi : u \mapsto u^{-1}L; \quad \tau : u \mapsto \tilde{\delta}(d,u); \quad \bar{\varphi} : q \mapsto L_{\mathcal{A}<q,A>}$$

$$\begin{tikzcd}
X^* \arrow[d, "\bar{\iota}"'] \arrow[dr, "\varphi"] & \\
Q \arrow[r, "\bar{\varphi}"] & Q(L)
\end{tikzcd}$$

FIG. 2.11 – Diagramme 1

Le diagramme précédent est commutatif. Comme φ est surjective, $\bar{\varphi}$ l'est aussi. Donc $\mathbb{Q}(L) = \mathrm{im}(\bar{\varphi})$ et $\mathrm{Card}(\mathbb{Q}(L)) \leq \mathrm{Card}(Q)$.

2)Supposons que $\mathbb{Q}(L)$ est fini.

Considérons l'automate fini déterministe, complet : $\mathcal{M} =< X, \mathbb{Q}(L), \{L\}, R, \theta >$ défini par

$$R = \{P \in \mathbb{Q}(L) | \epsilon \in P\} \text{ et } \theta(P, u) = x^{-1}P.$$

Pour tout $u \in X^*, \tilde{\theta}(L, u) = u^{-1}L$. Donc $L_{\mathcal{M}} = L$. □

Définition 2.4.2 *Soient* $\mathcal{A} =< X, Q, \{d\}, A, \delta >$,$\mathcal{A}' =< X, Q', \{d'\}, A', \delta' >$*deux automates déterministes,complets. Un* homomorphisme *de* $\mathcal{A}$ *dans* $\mathcal{A}'$ *est une application* $h : Q \to Q'$ *vérifiant les propriétés :*
- *(H1)* $h(d) = d'$
- *(H2)* $\forall q \in Q, \forall x \in X, h(\delta(q, x) = \delta'(h(q), x)$
- *(H3)* $q \in A \Leftrightarrow h(q) \in A'$

Propriété 2.4.3 *Si* $h : \mathcal{A} \to \mathcal{A}'$ *est un homorphisme, alors* $L_{\mathcal{A}} = L_{\mathcal{A}'}$.

Preuve : On prouve, à partir de $(H2)$, par récurrence sur $|u|$, que

$$\forall q \in Q, \forall u \in X^*, h(\tilde{\delta}(q, u)) = \tilde{\delta}'(h(q), u) \tag{2.3}$$

□

Théorème 2.4.4 *Soit* $L \in Rec(X^*)$. *Il existe un a.f déterministe complet* $\mathcal{M}$ *vérifiant :*

– *(MIN1)* $L_{\mathcal{M}} = L$
– *(MIN2) pour tout a.f.déterministe complet* $\mathcal{A}$*, si* $L_{\mathcal{A}} = L$*, alors il existe un homomorphisme surjectif* $h : \mathcal{A} \to \mathcal{M}$*.*

Cet automate $\mathcal{M}$ *est unique, à isomorphisme près. On l'appelle* l'automate minimal *de* L*.*

Preuve : **Existence**
Soit $\mathcal{M}$ l'automate défini dans la preuve du Théorème 2.4.1.
(MIN1)est vraie.
(MIN2) : montrons que $\bar{\varphi}$ est un homomorphisme d'automates :
$\bar{\varphi}(d) = L$, donc (H1) est vraie.
Soient $q \in Q, x \in X$. Alors

$$\bar{\varphi}(\delta(q,x)) = L_{\mathcal{A}<\delta(q,x),A>} = x^{-1}L_{\mathcal{A}<q,A>} = \theta(L_{\mathcal{A}<q,A>}, x)$$

donc (H2) est vraie.
$q \in A \Leftrightarrow \epsilon \in L_{\mathcal{A}<q,A>} \Leftrightarrow \epsilon \in \bar{\varphi}(q) \Leftrightarrow \bar{\varphi}(q) \in R$, donc (H3) est vraie.
Unicité
Soit $\mathcal{M} = \mathcal{M}_1$ et soit $\mathcal{M}_2$ un automate déterministe, complet, vérifiant (MIN1),(MIN2).
On considère les applications $\tau_i : u \mapsto \tilde{\delta}_i(d_i, u)$ et les homorphismes surjectifs $h_i : \mathcal{M}_{3-i} \to \mathcal{M}_i$, fournis par la propriété (MIN2). Le fait que h_i est un homorphisme entraîne que :

$$h_2 \circ \tau_1 = \tau_2 \text{ et } h_1 \circ \tau_2 = \tau_1,$$

(d'après l' équation (2.3)). On en déduit que, pour tout $u \in X^*$:

$$h_1 \circ h_2 \circ \tau_1(u) = h_1 \circ \tau_2(u) = \tau_1(u) \tag{2.4}$$

Mais τ_1 est surjective (voir la définition de $\mathcal{M} = \mathcal{M}_1$). De (2.4) on tire donc que $h_1 \circ h_2 = \mathrm{Id}_{Q_1}$.
Comme h_2 et τ_1 sont surjectives, τ_2 (qui est leur composée) l'est aussi. On peut donc utiliser le même raisonnement que ci-dessus pour montrer que $h_2 \circ h_1 = \mathrm{Id}_{Q_2}$. Les applications h_i sont donc des isomorphismes réciproques. Donc $\mathcal{M}_1 \approx \mathcal{M}_2$. □
Congruence d'automate :
Une relation d'équivalence $\sim$ sur Q est une *congruence* de $\mathcal{A}$ ssi,
– (C2) $\forall q, q' \in Q, \forall x \in X, q \sim q' \Rightarrow \delta(q,x) \sim \delta(q',x)$
– (C3) $\sim$ sature A.

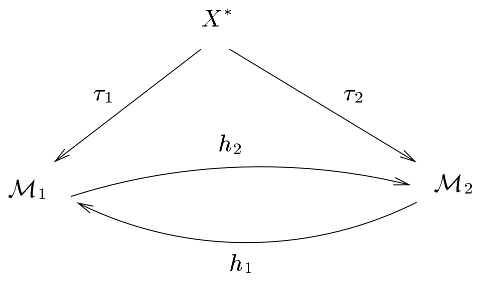


FIG. 2.12 –

Automate quotient :
Soit $\sim$ une congruence sur l'automate d.c. $\mathcal{A} =< X, Q, \{d\}, A, \delta >$. L'automate *quotient* de $\mathcal{A}$ par la congruence $\sim$ est défini par

$$\mathcal{A}/\sim =< X, Q/\sim, \{[d]_\sim\}, A/\sim, \bar{\delta} >$$

où

$$A/\sim = \{[a]_\sim | a \in A\} \text{ et } \bar{\delta}([q]_\sim, x) = [\delta(q, x)]_\sim.$$

La projection $\Pi : Q \to Q/\sim$ est définie par :

$$\forall q \in Q, \Pi(q) = [q]_\sim.$$

Proposition 2.4.5 *1- $\Pi : \mathcal{A} \to \mathcal{A}/\sim$ est un homomorphisme d'automates.*
2- $L_\mathcal{A} = L_{\mathcal{A}/\sim}$

Lemme 2.4.6 (Factorisation des homomorphismes)
Soient $\mathcal{A} =< X, Q, \{d\}, A, \delta >$ et $\mathcal{B} =< X, Q', \{d'\}, A', \delta' >$ deux automates déterministes complets. Soit $h : \mathcal{A} \longrightarrow \mathcal{B}$ un homorphisme d'automates surjectif. Définissons une relation d' équivalence Ker$h$ *sur Q par :*
$q(\text{Ker}h)r \Leftrightarrow h(q) = h(r)$.
Définissons une application $\bar{h} : Q/\text{Ker}h \to Q'$ par : $\bar{h}([q]_{\text{Ker}h}) = h(q)$. Alors $h = \bar{h} \circ \Pi$ et $\bar{h}$ est un isomorphisme d'automates.

Définition 2.4.7 *Soit $\mathcal{A} =< X, Q, \{d\}, A, \delta >$ un a.d.c. La congruence de Nerode de $\mathcal{A}$, notée $\equiv$, est définie par :*

$$q \equiv r \Leftrightarrow L_{\mathcal{A}<q,A>} = L_{\mathcal{A}<r,A>}.$$

$$\begin{tikzcd} \mathcal{A} \arrow[d] \arrow[dr, "h"] & \\ \mathcal{A}/\mathrm{Ker}h \arrow[r, "\bar{h}"] & \mathcal{B} \end{tikzcd}$$

FIG. 2.13 – Factorisation de h

Proposition 2.4.8 *L'automate $\mathcal{A}/\equiv$ est isomorphe à l'automate $\mathcal{M}$.*

Preuve : Dans le diagramme 1, $\mathrm{Ker}\bar{\varphi} = \equiv$. Par le lemme de factorisation, $\mathcal{A}/\equiv$ est isomorphe à $\mathcal{M}$. □

$$\begin{tikzcd} \mathcal{A} \arrow[r, dash, "\overline{\varphi}"] \arrow[d, dash, "\Pi"'] & \mathcal{M} \\ \mathcal{A}/\equiv \arrow[ur, dash, "\overline{\overline{\varphi}}", "\approx"'] & \end{tikzcd}$$

FIG. 2.14 – factorisation de $\bar{\varphi}$

Construction de l'automate minimal : Soit $\mathcal{A} =< X, Q, \{d\}, A, \delta >$ un automate fini d.c. On définit une suite d'approximations de la congruence de Nerode, $(\equiv_i)_{i\geq 0}$ par : $q \equiv_i r$ ssi

$$\forall u \in X^*, |u| \leq i \Rightarrow [\tilde{\delta}(q,u) \in A \Leftrightarrow \tilde{\delta}(r,u) \in A].$$

Lemme 2.4.9 $\forall i \in \mathbb{N}, \equiv_{i+1} \subseteq \equiv_i$.

Lemme 2.4.10 $\equiv = \bigcap_{i\geq 0} \equiv_i$.

Lemme 2.4.11 *Si $\equiv_k = \equiv_{k+1}$ alors $\equiv = \equiv_k$.*

Preuve :
$$q \equiv_{i+1} r \Leftrightarrow (\forall x \in X \cup \{\epsilon\}, \delta(q,x) \equiv_i \delta(r,x)).$$
Donc
$$\equiv_k = \equiv_{k+1} \Rightarrow \forall \lambda \geq 1, \equiv_k = \equiv_{k+\lambda} .$$
Ce qui entraîne que $\bigcap_{i\geq 0} \equiv_i = \equiv_k$ et donc $\equiv = \equiv_k$. □

Lemme 2.4.12 *Il existe un entier $k \leq \mathrm{Card}(Q) - 1$, tel que $\equiv_k = \equiv_{k+1}$*

Preuve : D'après le lemme 2.4.9 on a les inégalités :
$$1 \leq \ldots \leq \mathrm{Card}(Q/\equiv_i) \leq \mathrm{Card}(Q/\equiv_{i+1}) \leq \ldots \leq \mathrm{Card}(Q).$$
Mais la suite d'inégalités obtenues ne peuvent être strictes plus de $\mathrm{Card}(Q)-1$ fois. □
Algorithme :

$\sim$: $=$ $\equiv$ _0 ; `FINI := faux;`
`tant que (not FINI) faire`
`debut`
`soit` $\simeq$ `définie par:`

$q \simeq r$ `ssi` [$\forall\ x \in X \cup \{\epsilon\},\ \tilde{\delta}(q,x) \sim \tilde{\delta}(r,x)$]
`si` $\simeq = \sim$ `alors FINI := vrai;`
`fin`

Théorème 2.4.13 *L'algorithme précédent calcule pour tout a.f.d.c $\mathcal{A}$, son équivalence de Nerode $\equiv$.*

- l'algorithme précédent est polynomial
- Il existe un algorithme en O(nlog(n)), "l'algorithme de Hopcroft", voir [BBC94, th.6.16 p.333]

Définition 2.4.14 *Soit $\mathcal{M} = (M, \cdot, e)$ un monoïde. On appelle* congruence à droite *(resp. à gauche) sur $\mathcal{M}$, toute relation d' équivalence R sur M telle que, $\forall u, v, \beta \in M$,*
$$uRv \Rightarrow u \cdot \beta \ R \ v \cdot \beta$$

(resp. $uRv \Rightarrow \beta \cdot u \ R \ \beta \cdot v$*).*
R est une congruence *si et seulement si, R est à la fois une congruence à droite et à gauche.*
On appelle index *d'une congruence à droite (resp. à gauche) R, le cardinal de M/R.*

Définition 2.4.15 *On appelle congruence syntaxique à droite de L la relation $\equiv_L$ définie par :*

$$u \simeq_L v \Leftrightarrow [\forall \beta \in X^*, u\beta \in L \Leftrightarrow v\beta \in L]$$

Théorème 2.4.16 *Soit $L \in X^*$.*
(1) L est rationnel ssi $\simeq_L$ est d'index fini.
(2) $\mathcal{M} \approx < X, X^*/\simeq_L, \{[\epsilon]_{\simeq_L}\}, R, \delta >$ où

$$R = \{[u]_{\simeq_L} | u \in L\}; \quad \delta([u]_{\simeq_L}, x) = [ux]_{\simeq_L}.$$

Preuve : Reprenons l'application $\varphi : X^* \to \mathbb{Q}(L)$ définie dans la preuve du théorème 2.4.1. Considérons l'automate déterministe complet (infini) $\mathcal{X} =< X, X^*, \{\epsilon\}, L, \delta_X >$ où

$$\forall u \in X^*, \forall x \in X, \delta_X(u, x) = u \cdot x.$$

φ est un homorphisme surjectif de l'automate $\mathcal{X}$ dans $\mathcal{M}$. Par le lemme de factorisation, $\mathcal{X}/\mathrm{Ker}\varphi$ est isomorphe à $\mathcal{M}$. Mais $\mathrm{Ker}\varphi$ n'est autre que l' ́quivalence syntaxique à droite $\simeq_L$. Donc $\mathcal{X}/\simeq$ est isomorphe à $\mathcal{M}$, ce qui prouve le point (2).
D'après le point (2), $\mathrm{Card}(X^*/\simeq) = \mathrm{Card}(\mathbb{Q}(L))$. Donc L est rationnel ssi $\mathrm{Card}(\mathbb{Q}(L)) < \infty$ (par le théorème 2.4.1) ssi $\mathrm{Card}(X^*/\simeq) < \infty$ (par l' égalité ci-dessus). Le point (1) est prouvé. □

Définition 2.4.17 *On appelle* congruence syntaxique *de L la relation $\equiv_L$ définie par :*

$$u \equiv_L v \Leftrightarrow [\forall \alpha \in X^*, \forall \beta \in X^*, \alpha u\beta \in L \Leftrightarrow \alpha v\beta \in L]$$

Proposition 2.4.18 *Soit $L \subseteq X^*$. Les conditions suivantes sont équivalentes.*
(1) il existe un monoïde fini N, un homomorphisme $\varphi : X^* \to N$ et $P \subseteq N$, tels que $L = \varphi^{-1}(P)$
(2) il existe un monoïde fini N, un homomorphisme $\varphi : X^* \to N$ tels que $L = \varphi^{-1}(\varphi(L))$
(3) il existe une congruence d'index fini $\equiv$ sur X^* qui sature L,
(4) $\equiv_L$ est d'index fini.
Dans ce cas on dit que L est m-reconnaissable.

Preuve : (1) $\Rightarrow$ (2) : selon l'égalité (1),

$$\varphi^{-1}(\varphi(L)) = \varphi^{-1}(\varphi(\varphi^{-1}(P))) = \varphi^{-1}(P) = L.$$

(2) $\Rightarrow$ (3) : considérons la congruence $\equiv = Ker\varphi$. Un "lemme de factorisation" analogue au lemme 2.4.6, mais où la structure d'automate est remplacée par la structure de monoïde, reste valide. En appliquant ce lemme 2.4.6, "version monoïdes", à $\varphi : X^* \to \mathrm{im}\varphi \subseteq N$, on obtient que $X^*/\mathrm{Ker}\varphi$ est isomorphe à $\mathrm{im}\varphi$. Donc $\mathrm{Card}(X^*/\mathrm{Ker}\varphi) \leq \mathrm{Card}(N) < \infty$.

(3) $\Rightarrow$ (4) : comme $\equiv$ sature L, on a l'inclusion $\equiv \subset \equiv_L$. L'application $h : X^*/\equiv \to X^*/\equiv_L$ définie par $h([u]_\equiv) = [u]_{\equiv_L}$ est bien définie (c'est en fait un homomorphisme) et elle est surjective.
Donc $\mathrm{Card}(X^*/\equiv_L) \leq \mathrm{Card}(X^*/\equiv) < \infty$.

(4) $\Rightarrow$ (1) : posons $N = X^*/\equiv$, $\varphi : u \mapsto [u]_{\equiv_L}$ et $P = \varphi(L)$. On a bien $L = \varphi^{-1}(P)$. $\square$

Théorème 2.4.19 *Soit $L \subseteq X^*$. L est reconnaissable $\Leftrightarrow$ L est m-reconnaissable.*

Preuve : (1)Supposons que L est m-reconnaissable. Soit $\varphi : X^* \to N$, $P \subseteq N$ tels que $L = \varphi^{-1}(P)$.
Définissons $\mathcal{A} = < X, N, \{1_N\}, P, \delta >$ où

$$\delta(n, x) = n \cdot \varphi(x).$$

Cet automate fini (d'ailleurs déterministe et complet) reconnaît L.
(2)Supposons que L est reconnaissable. Soit $\mathcal{A} =< X, Q, \{d\}, A, \delta >$ un automate fini déterministe complet, le reconnaissant. Définissons $\mathcal{N} = (Q^Q, \otimes, I)$ où $\otimes$ dénote la composition des applications, notée "à l'envers" :

$$\forall q \in Q, \ \ (f \otimes g)(q) = g(f(q)).$$

Soit $\varphi : X^* \to Q^Q$ définie par $u \mapsto (q \mapsto \tilde{\delta}(q, u))$ et soit
$P = \{f \in Q^Q | f(d) \in A\}$.
On vérifie que $L = \varphi^{-1}(P)$. $\square$

Chapitre 3

Ensembles ordonnés - Treillis

3.1 Ensembles bien-fondés - Induction

Définition 3.1.1 *Une relation d'ordre $\leq$ sur un ensemble E est* <u>*bien-fondée*</u> *s'il n'y a pas de suite infinie strictement décroissante d'éléments de E.*
Un <u>*bon*</u> *ordre est un ordre total et bien-fondé.*

Proposition 3.1.2 *Soit $(E, \leq)$ un ensemble ordonné. $\leq$ est bien-fondé ssi toute partie non-vide admet au moins un élément minimal.*

Preuve : Montrons que $\leq$ n'est pas bien fondé $\Leftrightarrow$ $\exists\, A$, partie non vide de E, sans élement minimal.

(1) Supposons que $\leq$ n'est pas bien-fondé.
Soit $x_0 > x_1 > \ldots > x_n > x_{n+1} > \ldots$
une suite infinie, strictement décroissante.
Posons $A = \{x_n \mid n \in \mathbb{N}\}$. A n'a pas d'élément minimal.

(2) Soit $A \subseteq E$, $A \neq \emptyset$, A sans élément minimal.
Pour tout $x \in A$, $\{y \in A \mid y < x\} \neq \emptyset$

Soit $\varphi : \quad A \to \bigcup_{x \in A} \{y \in A \mid y < x\}$

$x \mapsto \varphi(x) \in \{y \in A \mid y < x\}$

(φ est une "fonction de choix")

Soit $x_0 \in A$.
Posons $x_{n+1} = \varphi(x_n) \ \ (n \geq 0)$:
$x_0 > x_1 > \ldots > x_n > x_{n+1} > \ldots$
Donc l'ordre $\leq$ n'est pas bien-fondé.

Exemples :	$(\mathbb{N}, \leq)$	bien-fondé
	$(\mathbb{Z}, \leq)$	pas bien-fondé
	$(\mathbb{N} \times \mathbb{N}, \leq_{lex})$	bien-fondé

□

Théorème 3.1.3 *Soit $(E, \leq)$ un ensemble ordonné, où $\leq$ est un ordre bien-fondé.*
Soit P une propriété dépendant d'un élément x de F.
Si P vérifie :
$(I) \quad \forall x \in E, \ \ ((\forall y \in E, \ y < x \ \Rightarrow P(y)) \ \Rightarrow \ P(x))$
alors $\forall x \in E, \ P(x)$.

Preuve : Considérons P vérifiant (I).
Soit $A = \{x \in E, \ P(x) \text{ est faux}\}$.
Si $A \neq \emptyset$, A admet un élément minimal, x_0.
$\forall y < x_0$, $y \notin A$, donc $y < x_0 \ \Rightarrow \ P(y)$.
D'après (I), on a alors : $P(x_0)$ est vraie.
Contradiction. Donc $A = \emptyset$.
□

3.2 Treillis

Définition 3.2.1 *Soit* $(E, \leq)$ *un ensemble ordonné.*
$(E, \leq)$ *est un* <u>*treillis*</u> *ssi :*
– *toute paire d'éléments admet une borne supérieure*
– *et toute paire d'éléments admet une borne inférieure.*

<u>**Notation :**</u> $x, y \in E, \quad x \sqcap y = \inf(\{x, y\})$
$$x \sqcup y = \sup(\{x, y\})$$

Exemple 3.2.2 * $(\mathbb{N}, \leq)$ *est un treillis*

* $(\mathbb{N}, |\,)$ *est un treillis*
$(x \sqcup y = ppcm(\{x, y\}),\ x \sqcap y = pgcd(\{x, y\})$

* $\left(\mathbb{N} \times \mathbb{N} \times \ldots \times \mathbb{N} \times \ldots, \quad \underset{\substack{\uparrow \\ \textit{ordre produit}}}{\leq} \right)$
i. e. $(x_n)_{n \in \mathbb{N}} \leq (y_n)_{n \in \mathbb{N}} \Leftrightarrow \forall n \in \mathbb{N}, x_n \leq y_n$ *est un treillis.*

* $(\mathcal{P}(E), \subseteq)$ *est un treillis.*

Proposition 3.2.3 *idempotence :* $x \sqcup x = x,\ x \sqcap x = x$
commutativité : $x \sqcup y = y \sqcup x, \quad x \sqcap y = y \sqcap x$
associativité : $(x \sqcup y) \sqcup z = x \sqcup (y \sqcup z), \quad (x \sqcap y) \sqcap z = x \sqcap (y \sqcap z)$
absorption : $x \sqcap (x \sqcup y) = x = (y \sqcap x) \sqcup x$

Preuve : facile (seule l'associativité demande une petite vérification).
□

Théorème 3.2.4 *Soit* $(E, \sqcup, \sqcap)$ *un ensemble muni de deux lois binaires qui vérifient les propriétés d'idempotence, commutativité, associativité et absorption.*
Posons $x \leq y \Leftrightarrow x \sqcup y = y$.

Alors $\leq$ est un ordre, $(E, \leq)$ est un treillis et $\sqcup$, $\sqcap$ sont le sup et l'inf dans ce treillis.

Preuve :

Ordre : - *réflexivité* $x \leq x$ car $x \sqcup x = x$ (idempotence)

- *transitivité* $x \leq y$ et $y \leq z$: $x \sqcup y = y$, $y \sqcup z = z$
  donc $x \sqcup z = x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z = y \sqcup z = z$
  i. e. $x \leq z$.
- *antisymétrie* $x \leq y$, $y \leq x$
  $x \sqcup y = y = x \Rightarrow x = y$

Opérateur sup : Soit $x \sqcup y = z$

$x \sqcup z = x \sqcup (x \sqcup y) = (x \sqcup x) \sqcup y = x \sqcup y = z$
Donc $x \leq z$
de même $y \leq z$.
Soit $t \mid x \leq t$, $y \leq t$
$x \sqcup t = t$, $y \sqcup t = t$
$\underbrace{(x \sqcup y)}_{z} \sqcup t = x \sqcup (y \sqcup t) = x \sqcup t = t$
Donc $z \leq t$.
Finalement : $z = \sup(\{x, y\})$.

Opérateur inf : * On remarque tout d'abord que : $x \sqcup y = y \Leftrightarrow x \sqcap y = x$

$$\left\{ \begin{array}{l} x \sqcup y = y \\ x \sqcap y = x \sqcap (x \sqcup y) \underset{\text{(absorption)}}{=} x \end{array} \right.$$

$$\left\{ \begin{array}{l} x \sqcap y = x \\ x \sqcup y = (x \sqcap y) \sqcup y \underset{\text{(absorption)}}{=} y \end{array} \right.$$

* Donc l'ordre $\leq$ peut être défini, de façon équivalente, par
$x \leq y \Leftrightarrow x \sqcap y = x$
On prouve alors que $\inf(\{x, y\}) = x \sqcap y$, par les mêmes arguments que $\sup(\{x, y\}) = x \sqcup y$ (interchanger $\sqcap$ et $\sqcup$).

$\square$

Définition 3.2.5 *Un treillis est distributif si $\sqcap$ et $\sqcup$ distribuent l'une par*

rapport à l'autre,
i. e.
(1) $x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z)$
(2) $x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z)$

Proposition 3.2.6 (1) $\Leftrightarrow$ (2), *dans la définition 3.2.5.*

Preuve :
(1)

$$\begin{array}{rcll} (x \sqcap y) \sqcup (x \sqcap z) & = & ((x \sqcap y) \sqcup x) \sqcap ((x \sqcap y) \sqcup z) & \text{(par (1))} \\ & = & x \sqcap ((x \sqcap y) \sqcup z) & \text{(par absorption)} \\ & = & x \sqcap ((x \sqcup z) \sqcap (y \sqcup z)) & \text{(par (1))} \\ & = & (x \sqcap (x \sqcup z)) \sqcap (y \sqcup z) & \text{(associativité)} \\ & = & x \sqcap (y \sqcup z) & \text{(absorption)} \end{array}$$

Donc (2) est prouvée.
L'implication (2) $\Rightarrow$ (1) s'obtient par la même méthode (intervertir $\sqcap$ et $\sqcup$).
$\square$

Définition 3.2.7 *Un treillis* $(E, \leq)$ *est dit* complémenté *ssi*
1-il a un élément minimum $\perp$ *et un élément maximum* $\top$
2-il existe un application $\nu : E \to E$ *telle que*

$$\forall x \in E, \;\; x \sqcap \nu(x) = \perp, \;\; x \sqcup \nu(x) = \top$$

Proposition 3.2.8 *Soit* $(E, \leq)$ *un treillis distributif.*
Il existe au plus une application $\nu : E \to E$ *qui en fasse un treillis complémenté.*
Si $(E, \leq, \nu)$ *est un treillis distributif complémenté :*
$\nu(\nu(x)) = x$ *(involution)*
$\nu(x \sqcup y) = \nu(x) \sqcap \nu(y)$
$\nu(x \sqcap y) = \nu(x) \sqcup \nu(y)$ *(lois de Morgan)*
$x \leq y \;\Leftrightarrow\; \nu(x) \geq \nu(y)$

Preuve :
* Propriété (Q) :
$(x \sqcap y = \perp \text{ et } x \sqcup z = \top) \;\Rightarrow\; y \leq z.$

preuve de (Q) :

$$\begin{aligned} z &= z \sqcup \bot \\ &= z \sqcup (x \sqcap y) \\ &= (z \sqcup x) \sqcap (z \sqcup y) \\ &= \top \sqcap (z \sqcup y) \\ &= z \sqcup y \end{aligned}$$

Donc $y \leq z$.

* Unicité de $x' \mid x \sqcap x' = \bot,\ x \sqcup x' = \top$:
si $\begin{cases} x \sqcap x' = x \sqcap x'' = \bot \\ x \sqcup x' = x \sqcup x'' = \top \end{cases}$
par (Q) $\quad x' \leq x''$ et $x'' \leq x'$ donc $x' = x''$.

* Involution :
$x \sqcap \nu(x) = \bot$, $\nu(x) \sqcup \nu(\nu(x)) = \top$, donc $x \leq \nu(\nu(x))$ $\quad$ (par (Q))
$x \sqcup \nu(x) = \top$, $\nu(x) \sqcap \nu(\nu(x)) = \bot$, donc $\nu(\nu(x)) \leq x$
Donc $x = \nu(\nu(x))$

* Lois de Morgan :
Montrons que
$(x \sqcup y) \sqcap (\nu(x) \sqcap \nu(y)) = \bot$, $(x \sqcup y) \sqcup (\nu(x) \sqcap \nu(y)) = \top$
(par la propriété d'unicité, on pourra conclure que $\nu(x \sqcup y) = \nu(x) \sqcap \nu(y)$)

$$\begin{aligned} (x \sqcup y) \sqcap (\nu(x) \sqcap \nu(y)) &= (x \sqcap \nu(x) \sqcap \nu(y)) \sqcup (y \sqcap \nu(x) \sqcap \nu(y)) \\ &= (\bot \sqcap \nu(y)) \sqcup (\nu(x) \sqcap \bot) \\ &= \bot \sqcup \bot \\ &= \bot \end{aligned}$$

$$\begin{aligned} (x \sqcup y) \sqcup (\nu(x) \sqcap \nu(y)) &= (x \sqcup y \sqcup \nu(x)) \sqcap (x \sqcup y \sqcup \nu(y)) \\ &= (\top \sqcup y) \sqcap (x \sqcup \top) \\ &= \top \sqcap \top \\ &= \top \end{aligned}$$

(la deuxième loi de Morgan se démontre de façon analogue, ou alors, se déduit de la première, en appliquant ν et en sachant que $\nu^2 = \mathrm{Id}$).

* Renversement de l'ordre :

$$\begin{aligned} x \leq y &\Leftrightarrow x \sqcup y = y \\ &\Leftrightarrow \nu(x \sqcup y) = \nu(y) \\ &\Leftrightarrow \nu(x) \sqcap \nu(y) = \nu(y) \\ &\Leftrightarrow \nu(y) \leq \nu(x). \end{aligned}$$

□

3.3 Treillis complets - Points fixes

Définition 3.3.1 *Un ensemble ordonné* $(E, \leq)$ *est un* treillis complet *(ou sup-complet), si toute partie de* E *admet une borne supérieure.*

Exemple : $(\mathcal{P}(F), \subseteq)$ est un treillis complet.

Remarque 3.3.2 *Si* $(E, \leq)$ *vérifie la définition 3.3.1 alors,*
** il s' agit bien d' un treillis :*

$$a \sqcup b = \sup(\{a, b\}); \quad a \sqcap b = \sup(\{m \in E, m \leq a \text{ et } m \leq b\}).$$

** il admet un plus petit élément,* $\perp = \sup\,(\emptyset)$
** il admet un plus grand élément,* $\top = \sup\,(E)$

Définition 3.3.3 *Une application* $f : (E_1, \leq_1) \to (E_2 \leq_2)$ *est dite continue ssi, pour toute partie* $A \subseteq E_1$*, admettant une borne supérieure* $a = \sup(A)$*,* $\{f(x) \mid x \in A\}$ *admet aussi une borne supérieure et elle est égale à* $f(a)$*.*

Remarque 3.3.4 ** Lorsque les* $(E_i, \leq_i)$ $(1 \leq i \leq 2)$ *sont des treillis complets,* f *est continue ssi, pour toute partie* $A \subseteq E_1$*,* $f(\sup A) = \sup(f(A))$

* *Si f est continue, f est croissante.*

On appelle "point fixe" de $f : E \to E$, tout $x \in E$ tel que $f(x) = x$.

Théorème 3.3.5 *Si f est une application croissante d'un treillis complet $(E, \leq)$ dans lui-même, alors f a un plus grand point fixe.*

Preuve : Soit $X = \{x \in E \mid x \leq f(x)\}$. Posons $z = \sup(X)$.
$\forall x \in X$, $x \leq f(x) \leq f(z)$, donc $\forall x \in X$, $x \leq f(z)$.
Comme $f(z)$ est un majorant de X, $\underline{z \leq f(z)}$ (J1)
$f(z) \leq f(f(z))$ (croissance de f)
Donc, $f(z) \in X$, d'où $\underline{f(z) \leq z}$ (J2)
Par (J1) (J2), $z = f(z)$
et comme $z \in X$, z est le plus grand "sous point-fixe"
$\Rightarrow$ z est le plus grand point-fixe.
□

Théorème 3.3.6 *Si f est une application continue d'un treillis complet dans lui-même, alors f a un plus petit point fixe. Ce plus petit point fixe est égal à*

$$\sup(\{f^n(\perp) \mid n \in \mathbb{N}\}).$$

Preuve : Posons $x = \sup(\{f^n(\perp) \mid n \in \mathbb{N}\})$
Comme f est continue, $f(x) = \sup(\{f^{n+1}(\perp) \mid n \in \mathbb{N}\})$.
Mais $\{f^n(\perp) \mid n \in \mathbb{N}\}$ et $\{f^{n+1}(\perp) \mid n \in \mathbb{N}\}$ ont les mêmes majorants, donc la même borne supérieure. Donc $f(x) = x$.
Soit $y = f(y)$
$\perp \leq y \Rightarrow \forall n \in \mathbb{N}$, $f^n(\perp) \leq f^n(y) = y$
Donc y est un majorant de $\{f^n(\perp) \mid n \in \mathbb{N}\}$, donc $x \leq y$.
□

Chapitre 4

Construction par induction - Induction structurelle

4.1 Récurrence sur $\mathbb{N}$

Théorème 4.1.1 *Soit $P(n)$ une propriété dépendant de l'entier n. Si les deux conditions suivantes sont réalisées*

(B) $P(0)$
(I) $\forall\, n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$

alors, $\forall\, n \in \mathbb{N}, P(n)$.

Théorème 4.1.2 *Soit $P(n)$ une propriété dépendante de l'entier n. Si P vérifie*

$$(I)\ \forall\, n \in \mathbb{N}, ((\forall\, m \in \mathbb{N}, m < n \Rightarrow P(m)) \Rightarrow P(n))$$

alors, $\forall\, n \in \mathbb{N}, P(n)$.

Preuve : $(\mathbb{N}, \leq)$ est bien-fondé. Il s'agit donc de l'induction bien-fondée. □

4.2 Induction structurelle

Définition 4.2.1 *Soit E un ensemble, $B \subseteq E$, et K un ensemble d'opérations, $\Phi : E^{a(\Phi)} \to E$.*
Soit X le plus petit sous-ensemble de E tel que

(B) $B \subseteq X$
(I) $\forall\, \Phi \in K, \forall\, x_1, \ldots, x_{a(\Phi)} \in X, \Phi(x_1, \ldots, x_{a(\Phi)}) \in X$

On dit que X est l'ensemble défini inductivement par les conditions (B), (I).

Preuve : Prouvons l'existence d'un tel X :

$$\text{soit} \quad \begin{array}{rrcl} H: & \mathcal{P}(E) & \to & \mathcal{P}(E) \\ & Y & \mapsto & B \cup \{\Phi(x_1, \ldots, x_{a(\Phi)}) \mid x_1, \ldots, x_{a(\Phi)} \in Y\} \end{array}$$

H est croissante.
Posons
$$X = \bigcup_{n \geq 0} H^n(\emptyset)$$
Si
$$Y_0 \subseteq Y_1 \subseteq \ldots \subseteq Y_n \subseteq Y_{n+1} \subseteq \ldots$$
alors
$$H(\bigcup_{n \geq 0} Y_n) = \bigcup_{n \geq 0} H(Y_n)$$
(N.B. quoique H ne soit pas continue au sens de la def 3.3.3)
Donc
$$H(X) = \bigcup_{n \geq 0} H^{n+1}(\emptyset) = \bigcup_{n \geq 0} H^n(\emptyset) = X.$$
D'autre part, si $H(X') \subseteq X'$, alors
$$\emptyset \subseteq X', H(\emptyset) \subseteq X', \ldots, H^n(\emptyset)) \subseteq X', \ldots$$
donc
$$X \subseteq X'.$$
$\Box$

Remarque 4.2.2

1 - Si X est défini inductivement par (B), (I), tout élément de X est de l'une des formes :

$$x \in B$$

ou

$$x = \Phi(x_1, \ldots, x_{a(\Phi)}) \text{ où } x_i \in X$$

2 - $H^n(\emptyset)$ s'interprète comme l'ensemble des éléments obtenus à partir de B à l'aide d'au plus n étapes d'applications d'opérations Φ.

Théorème 4.2.3 *Soit X un ensemble défini inductivement (comme en 4.2.1) et soit $P(x)$ un prédicat exprimant une propriété de x. Si P vérifie*

(B') $\forall\, x \in B, P(x)$
(I') $\forall\, \Phi \in K, \forall\, x_1, \ldots, x_{a(\Phi)} \in X, (P(x_1) \text{ et } P(x_2) \text{ et } \ldots \text{ et } P(x_{a(\Phi)})) \Rightarrow P(\Phi(x_1, \ldots, x_{a(\Phi)}))$

alors,

$$\forall\, x \in X, P(x).$$

Preuve : Posons $Y = \{x \in E | P(x)\}$.

$$B \subseteq Y$$

et

$$\forall\, \Phi \in K, \forall\, x_1, \ldots, x_{a(\Phi)} \in Y, \Phi(x_1, \ldots, x_{a(\Phi)}) \in Y$$

donc

$$X \subseteq Y.$$

□

Définition 4.2.4 *Soient (E, B, K) un ensemble de base $B \subseteq E$ et un ensemble K d'opérations sur E (comme dans la définition 4.2.1). La définition inductive associée à (E, B, K) est dite non-ambiguë si et seulement si :*

$$\forall\, n \geq 0, \forall\, x \in H^{n+1}(\emptyset), \text{ un et un seul des cas suivants est réalisé :}$$

(cas B) : $x \in B$
(cas I) : $\exists\, \Phi \in K, \exists\, (x_1, \ldots, x_{a(\Phi)}) \in (H^n(\emptyset))^{a(\Phi)}$*, tels que* $x = \Phi(x_1, \ldots, x_{a(\Phi)})$.
et si, lorsque (n, x) est dans le cas (I), l'opérateur Φ et le vecteur $(x_1, \ldots, x_{a(\Phi)})$ sont uniques.

Définition 4.2.5 (définition de fonction) *Soit X la plus petite partie de E telle que*

(0) $B \subseteq X$
(1) $\forall\, \Phi \in K, \forall\, x_1, \ldots, x_{a(\Phi)} \in X, \Phi(x_1, \ldots, x_{a(\Phi)}) \in X$

On suppose que cette définition inductive est non-ambiguë.

$$\textit{Soient} \left\{ \begin{array}{lll} g_0 & : & B \longrightarrow E' \\ g_\Phi & : & {E'}^{a(\Phi)} \longrightarrow E' \end{array} \right. \quad \textit{des applications.}$$

Alors il existe une unique application $f : X \longrightarrow E'$ telle que

$(0')$ $\forall\, x \in B, f(x) = g_0(x)$
$(1')$ $\forall \Phi \in K, \forall x_1, \ldots, x_{a(\Phi)} \in X, f(\Phi(x_1, \ldots, x_{a(\Phi)})) = g_\Phi(f(x_1), \ldots, f(x_{a(\Phi)}))$.

Preuve : Soit F la plus petite partie de $E \times E'$ telle que

$(0'')$ $\{(x, g_0(x)) \mid x \in B\} \subseteq F$
$(1'')$ $\forall\, \Phi \in K, \forall\, (x_1, y_1), \ldots, (x_{a(\Phi)}, y_{a(\Phi)}) \in F$,
$(\Phi(x_1, \ldots, x_{a(\Phi)}), g_\Phi(y_1, \ldots, y_{a(\Phi)})) \in F$.

* F existe (relation binaire, définie par induction structurelle)
* F est unique (idem)
* Montrons que $\mathrm{dom}(F) = X$: la preuve du principe de définition inductive montre que

$$\begin{array}{rcl} F & = & \bigcup_{n \geq 0} F_n \text{ avec} \\ F_0 & = & \emptyset \\ F_1 & = & \{(x, g_0(x)) \mid x \in B\} \\ & \vdots & \\ F_{n+1} & = & F_1 \cup \{(\Phi(x_1, \ldots, x_{a(\Phi)}), g_\Phi(y_1, \ldots, y_{a(\Phi)})) \mid (x_1, y_1), \ldots, (x_{a(\Phi)}, y_{a(\Phi)}) \in F_n, \Phi \in K\} \end{array}$$

$$\begin{array}{rcl}
\mathrm{dom}(F_0) & = & \emptyset \\
\mathrm{dom}(F_1) & = & B \\
& \vdots & \\
\mathrm{dom}(F_{n+1}) & = & B \cup \{(\Phi(x_1, \ldots, x_{a(\Phi)}) \mid x_1, \ldots, x_{a(\Phi)} \in \mathrm{dom}(F_n), \Phi \in K\}
\end{array}$$

Donc

$$\mathrm{dom}(F_{n+1}) = H(\mathrm{dom}(F_n))$$

Par récurrence :

$$\mathrm{dom}(F_{n+1}) = H^{n+1}(\emptyset),$$

$$\mathrm{dom}(F) = \bigcup_{n \geq 0} \mathrm{dom}(F_n) = \bigcup_{n \geq 0} H^n(\emptyset) = X.$$

* F est fonctionnelle :
  comme $\mathrm{dom}(F_n) \subseteq \mathrm{dom}(F_{n+1})$, il suffit de prouver que chaque F_n est fonctionnelle.

$$\begin{array}{rcl}
n = 0 & : & \emptyset \text{ est fonctionnelle.} \\
n = 1 & : & F_1 = g_{0|B} \text{ est fonctionnelle.} \\
& \vdots & \\
n + 1 & : & \text{On suppose que } F_n \text{ est fonctionnelle.}
\end{array}$$

Soient $(x, y), (x, z) \in F_{n+1}$

cas 1 : $x \in B, y = g_0(x)$
$x = \Phi(x_1, \ldots, x_{a(\Phi)}), z = g_\Phi(y_1, \ldots, y_{a(\Phi)}), (x_i, y_i) \in F_n$
Impossible car $x \in \Phi((H^n(\emptyset))^{a(\Phi)} \cap B = \emptyset$.

cas 2 : $x = \Phi(x_1, \ldots, x_{a(\Phi)}), y = g_\Phi(y_1, \ldots, y_{a(\Phi)})$
$x = \Phi'(x'_1, \ldots, x'_{a(\Phi')}), z = g_{\Phi'}(y'_1, \ldots, y'_{a(\Phi')})$
$(x_i, y_i) \in F_n, (x'_j, y'_j) \in F_n$.

La non-ambiguité de la définition entraîne :

$$\Phi = \Phi', \forall\, i \in [1, a(\Phi)], x_i = x'_i.$$

Par hypothèse de récurrence : F_n est fonctionnelle, donc $y_i = y'_i$, or g_Φ est fonctionnelle, donc :

$$y = z.$$

□

4.3 Les termes

Définition 4.3.1 *Une* signature *est un ensemble F de symboles, muni d' une application* $\mathbf{ar} : F \to \mathbb{N}$.

L' application **ar** associe à chaque symbole $f \in F$ son *arité* $\mathbf{ar}(f)$. Intuitivement, f est un symbole de fonction et $\mathbf{ar}(f)$ le nombre d' arguments de cette fonction. Etant donnés une signature $(F, \mathbf{ar})$ et un alphabet de variables V, on définit l' ensemble des termes $T(F, V)$ comme suit.

Définition 4.3.2 $T(F, V)$ *est l'ensemble des mots sur l'alphabet* $F \cup V$ *défini inductivement par*
(i) si $v \in V$, *alors* $v \in T(F, V)$

(ii) si $f \in F$ *et* $\mathbf{ar}(f) = 0$, *alors* $f \in T(F, V)$

(iii) si $f \in F$ *et* $\mathbf{ar}(f) = n \geq 1$, *et si* $t_1, \ldots, t_n \in T(F, V)$, *alors* $f \cdot t_1 \cdots t_n \in T(F, V)$.

Théorème 4.3.3 *(décomposition des termes) Si* $t \in T(F, V)$, *alors* t *s'écrit sous une et une seulement des formes suivantes :*

(i)	$t = v$	*où* $v \in V$
(ii)	$t = f$	*où* $f \in F$ *et* $\mathbf{ar}(f) = 0$
(iii)	$t = f \cdot t_1 \cdots t_n$	*où*$f \in F, \mathbf{ar}(f) = n \geq 1$ *et* $t_1, \ldots, t_n \in F$

De plus, dans le cas (iii), le n*-uple* $(t_1, \cdots, t_n)$ *est unique.*

Autrement dit : la définition inductive 4.3.2 est *non-ambiguë* (au sens de la définition 4.2.4).
Critère de bonne formation des termes :
Soit $\pi : (F \cup V)^* \to (\mathbb{Z}, +, 0)$ l'unique homomorphisme tel que :

$$\begin{cases} \pi(v) = -1 & (\text{si } v \in V) \\ \pi(f) = \mathbf{ar}(f) - 1 & (\text{si } f \in F). \end{cases}$$

Soit $u \in (F \cup V)^*$. Le mot u est un terme correctement formé ssi :
(1) $\pi(u) = -1$

(2) $\forall u' <_{pref} u,\ \pi(u') \geq 0$

Preuve du critère :
Soit $\mathcal{C} = \{u \in (F \cup V)^* \mid u$ vérifie le critère$\}$. On montre successivement que $T(F,V) \subseteq \mathcal{C}$ (partie A) puis que $\mathcal{C} \subseteq T(F,V)$ (partie B).
A :
* $V \subseteq \mathcal{C}$
* $\{f \in F \mid \mathbf{ar}(f) = 0\} \subseteq \mathcal{C}$
* $\mathcal{C}$ est stable par les opérations :
$(t_1, \ldots, t_n) \mapsto f \cdot t_1 \cdots t_n$,
Donc, $\mathcal{C}$ vérifie les points (i)-(iii) de la définition inductive de $T(F,V)$, donc $T(F,V) \subseteq \mathcal{C}$.
B :
Démontrons par récurrence sur $|u|$ que : $u \in \mathcal{C} \Rightarrow u \in T(F,V)$.
* $|u| = 0$: vrai (car $u \notin \mathcal{C}$)
* $|u| = 1$, $u \in \mathcal{C}$.
Comme u vérifie le critère, u est une variable $v \in V$ ou bien u est un symbole f d' arité 0.
* $|u| = n+1$, $n \geq 1$ et $u \in \mathcal{C}$. Comme u vérifie le critère et a une longueur ≥ 2, il est de la forme :

$$u = f \cdot v$$

où $\pi(f) = n-1, n \geq 1, v \in (F \cup V)^*, \pi(v) = -n$. On considère les plus courts préfixes $v_1, v_2, \ldots v_n$ de v de poids $-1, -2, \ldots, -n$. Soient $u_1, u_2, \ldots u_n$ les mots tels que

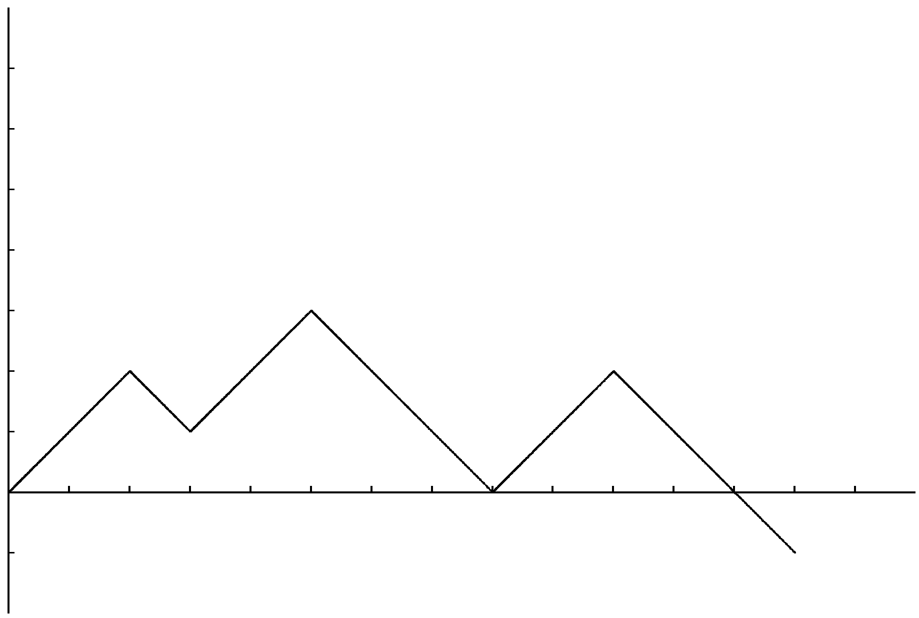
$$v_1 = u_1,\ v_2 = v_1 \cdot u_2,\ v_{i+1} = v_i \cdot u_{i+1},\ v_n = v_{n-1} \cdot u_n.$$

Les mots u_i vérifient alors que :

$$u = f \cdot u_1 \cdot u_2 \cdots u_n$$

et ces mots sont eux-aussi dans $\mathcal{C}$. Par hypothèse de récurrence, $\forall i \in [1,n], u_i \in T(F,V)$. Et par le point (iii), $u \in T(F,V)$.

Schéma :



Preuve du théorème 4.3.3 :

- L' *existence* de la décomposition résulte de la définition inductive des termes.
- *Unicité* :
  Supposons $t = f \cdot t_1 \cdot t_2 \cdots t_n = g \cdot u_1 \cdot u_2 \cdots u_m$.
  Comme $f = g$, les entiers n, m sont égaux. Les mots t_1, u_1 sont comparables pour l'ordre préfixe et vérifient le critère. Donc ils sont égaux (en vertu de la condition (2) du critère).

Les mots t_2, u_2 sont donc comparables pour l'ordre préfixe et vérifientle critère ...
On démontre ainsi que, pour tout $i \in [1,n], t_i = u_i$.

□

Substitution :
Soit t, u_1, ..., u_n des termes, v_1, v_2, ..., $v_n \in V$.
On note $t[u_1/v_1, u_2/v_2, \dots, u_n/v_n]$ le terme obtenu en "substituant u_i à v_i dans F ".

$$\begin{tikzcd}
F \cup V \arrow[d, "i"'] \arrow[dr, "\varphi"] & \\
(F \cup V)^* \arrow[r, "\tilde{\varphi}"'] & (F \cup V)^*
\end{tikzcd}$$

$$\begin{array}{lll}
\varphi: & v_i \mapsto u_i & (i \in [1,n]) \\
 & f \mapsto f & (f \in F) \\
 & v \mapsto v & (v \in V - \{v_1, v_2, \dots, v_n\})
\end{array}$$

Elle est définie par :
$t[u_1/v_1, u_2/v_2, \dots, u_n/v_n] = \tilde{\varphi}(t)$.

Proposition 4.3.4 *Si $t, u_1, \dots, u_n$ sont des termes et $v_1, v_2, \dots, v_n$ sont des variables alors $t[u_1/v_1, u_2/v_2, \dots, u_n/v_n]$ est un terme.*

Preuve : Posons $\mathcal{C} = \{t \in (F \cup V)^* \quad | \quad \tilde{\varphi}(t) \text{ est un terme}\}$
(i) $\forall v \in V$, $\tilde{\varphi}(v) \in \mathcal{C}$
car $\tilde{\varphi}(v) \in \{u_1, \dots, u_n\} \subseteq T(F,V)$

(ii) Supposons $f \in F$ tel que $\mathbf{ar}(f) = 0$.
$\tilde{\varphi}(f) = f$. Donc $f \in \mathcal{C}$.

(iii) Supposons $f \in F, \mathbf{ar}(f) = p \geq 1$ et $t_1, \dots, t_p \in \mathcal{C}$
$\tilde{\varphi}(f \cdot t_1 \cdots t_p) = f \cdot \tilde{\varphi}(t_1) \cdots \tilde{\varphi}(t_p)$ et les $\tilde{\varphi}(t_i)$ appartiennent à $T(F,V)$
donc $\tilde{\varphi}(ft_1 \dots t_p) \in T(F,V)$
donc $ft_1 \dots, t_p \in \mathcal{C}$.

Comme $\mathcal{C}$ vérifie les points (i),(ii),(iii) de la définition 4.3.2, on peut conclure que $T(F,V) \subseteq \mathcal{C}$.

□

On appelle *instance* du terme t, tout terme de la forme $t[u_1/v_1, u_2/v_2, \ldots, u_n/v_n]$ pour des termes $u_1, \ldots, u_n$.

Exemple 4.3.5 *Hauteur d'un terme.*

Exemple 4.3.6 *Nombre de Strahler d'un terme.*

Exemple 4.3.7 *Expressions arithmétiques avec* $+, \times, a, b, c, (,)$.

Exemple 4.3.8 *Expressions rationnelles.*

Exemple 4.3.9 *Hauteur d' étoile d'une expression rationnelle.*

Chapitre 5

Algèbres de Boole et anneaux de Boole

5.1 Des algèbres vers les anneaux

Définition 5.1.1 *Une algèbre de Boole est un treillis distributif complémenté* $(E, \sqcup, \sqcap, \perp, \top, \bar{})$
On note $x \mapsto \bar{x}$ l'application "complément" (qui était notée $x \mapsto \nu(x)$ au chapitre 3).

Historiquement :

* G. Boole a inventé les "algèbres de Boole" pour ramener les lois du raisonnement (les syllogismes) à des règles de calcul en petit nombre ([1847]).
* M. H. Stone a montré que les "algèbres de Boole" correspondent à des sortes particulières "d'anneaux", au sens de l'Algèbre (comme pour les anneaux de polynômes, les anneaux $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}[\sqrt{5}]$, $\mathbb{Z}[[X]]$, etc ...).

Partons d'une algèbre de Boole : $(E, \sqcup, \sqcap, 0, 1, \bar{})$
Posons $a \oplus b = (a \sqcap \bar{b}) \sqcup (\bar{a} \sqcap b)$
(la "différence symétrique de a et b").
On vérifie que :

$$\begin{aligned}
(a \sqcup b) \sqcap \overline{(a \sqcap b)} &= (a \sqcup b) \sqcap (\bar{a} \sqcup \bar{b}) \quad \text{(Morgan)} \\
&= ((a \sqcup b) \sqcap \bar{a}) \sqcup ((a \sqcup b) \sqcap \bar{b}) \quad \text{Distribution)} \\
&= ((a \sqcap \bar{a}) \sqcup (b \sqcap \bar{a})) \sqcup ((a \sqcap \bar{b}) \sqcup (b \sqcap \bar{b})) \\
&= (b \sqcap \bar{a}) \sqcup (a \sqcap \bar{b}) \\
&= a \oplus b
\end{aligned}$$

Remarque 5.1.2 *Lorsque* $E = \mathcal{P}(F)$, $\sqcup = \cup$, $\sqcap = \cap$, $\bar{x} = \complement x$
$a \oplus b$ *est la différence symétrique de* a *et* b.

Montrons que $(E, \oplus, \cdot, 0, 1)$ est un anneau commutatif unitaire
(où $\cdot = \sqcap$, $0 = \bot$, $1 = \top$).
i. e. : $(E, \oplus)$ est un groupe, $(E, \cdot, 1)$ est un monoïde commutatif, $\cdot$ est distributive sur $\oplus$.

* Associativité de $\oplus$

$$\begin{aligned}
(a \oplus b) \oplus c &= ([(a \sqcap \bar{b}) \sqcup (\bar{a} \sqcap b)] \sqcap \bar{c}) \sqcup (\overline{[(a \sqcap \bar{b}) \sqcup (\bar{a} \sqcap b)]} \sqcap c) \\
&= [(a \sqcap \bar{b} \sqcap \bar{c}) \sqcup (\bar{a} \sqcap b \sqcap \bar{c})] \sqcup ([(\bar{a} \sqcup b) \sqcap (a \sqcup \bar{b})] \sqcap c) \\
&= (a \sqcap \bar{b} \sqcap \bar{c}) \sqcup (\bar{a} \sqcap b \sqcap \bar{c}) \sqcup (\bar{a} \sqcap \bar{b} \sqcap c) \sqcup (a \sqcap b \sqcap c)
\end{aligned}$$

Par substitution :
$(c \oplus b) \oplus a = (c \sqcap \bar{b} \sqcap \bar{a}) \sqcup (\bar{c} \sqcap b \sqcap \bar{a}) \sqcup (\bar{c} \sqcap \bar{b} \sqcap a) \sqcup (c \sqcap b \sqcap a)$
On vérifie que, étant donnée la commutativité-associativité de $\sqcup$, $\sqcap$:
$(c \oplus b) \oplus a = (a \oplus b) \oplus c$
Donc l'associativité résultera de la commutativité de $\oplus$.

* Commutativité de $\oplus$
On a vu que : $a \oplus b = (a \sqcup b) \sqcap \overline{(a \sqcap b)}$
Comme $\sqcup$, $\sqcap$ sont commutatives, $\oplus$ est aussi commutative.

* Elément neutre 0
(rappel : $0 = \bot$) (remarquons que $\bar{0} = 1$)
$a \oplus 0 = (a \sqcap 1) \sqcup (\bar{a} \sqcap 0) = a \sqcup 0 = a$
Donc $(E, \oplus, 0)$ est un groupe commutatif.

* Elément neutre 1
$a \cdot 1 = a \sqcap \top = a$
Donc $(E, \cdot, 1)$ est un monoïde commutatif.

* Distributivité

$$\begin{aligned}(a \oplus b) \cdot c &= ((a \sqcap \bar{b}) \sqcup (\bar{a} \sqcap b)) \sqcap c \\ &= (a \sqcap \bar{b} \sqcap c) \sqcup (\bar{a} \sqcap b \sqcap c)\end{aligned}$$

$$\begin{aligned}(a \cdot c) \oplus (b \cdot c) &= ((a \sqcap c) \sqcap \overline{(b \sqcap c)}) \sqcup (((\overline{(a \sqcap c)} \sqcap (b \sqcap c)) \\ &= ((a \sqcap c) \sqcap (\bar{b} \sqcup \bar{c})) \sqcup ((\bar{a} \sqcup \bar{c}) \sqcap (b \sqcap c)) \\ &= (a \sqcap c \sqcap \bar{b}) \sqcup (\bar{a} \sqcap b \sqcap c) \\ &= (a \sqcap \bar{b} \sqcap c) \sqcup (\bar{a} \sqcap b \sqcap c)\end{aligned}$$

Donc $(E, \oplus, \cdot, 0, 1)$ est un anneau, commutatif, unitaire.

* Idempotence
$a \sqcap a = a$

On appelle *anneau de Boole* un anneau unitaire où tout élément est idempotent.

Théorème 5.1.3 *Si $(E, \sqcup, \sqcap, 0, 1, \bar{\ })$ est une algèbre de Boole alors $(E, \oplus, \cdot, 0, 1)$ est un anneau de Boole.*
(où $a \oplus b = (a \sqcap \bar{b}) \sqcup (\bar{a} \sqcap b)$, $a \cdot b = a \sqcap b$).

Remarque 5.1.4 *Si $(E, \oplus, \cdot, 0, 1)$ est un anneau unitaire où tout élément est idempotent,*
alors il est commutatif et $\forall x \in E$, $2x = 0$.

Preuve : $a \oplus b \oplus ab \oplus ba = a^2 \oplus b^2 \oplus ab \oplus ba = (a \oplus b)^2 = a \oplus b$
donc $ab \oplus ba = 0$. Donc $2a = 2a^2 = aa \oplus aa = 0$. Donc $a = -a$.
D'où $ab - ba = 0$ et l'anneau est commutatif.
□

5.2 Des anneaux vers les algèbres

Partons maintenant d'un anneau de Boole : $(E, \oplus, \cdot, 0, 1)$.
Posons :
$$\begin{cases} a \sqcup b = a \oplus b - ab = 1 - (1-a)(1-b) \\ \sigma(x) = 1 - x \end{cases}$$

Donc $a \sqcup b = \sigma^{-1}(\sigma(a) \cdot \sigma(b))$
L'associativité de $\cdot$ entraîne donc l'associativité de $\sqcup$,
et la commutativité de $\cdot$ entraîne la commutativité de $\sqcup$.

$a \sqcup a = 2a - a^2 = -a^2 = a$

Posons : $a \sqcap b = a \cdot b$
$a \sqcap a = a$ (car anneau idempotent)

– Absorption

$$\begin{aligned} (a \sqcup b) \sqcap a &= (a \oplus b - ab)a \\ &= aa \oplus ba - aba \\ &= a \oplus ba - ab \\ &= a \end{aligned}$$

$$\begin{aligned} (a \sqcap b) \sqcup a &= ab \oplus a - aab \\ &= ab \oplus a - ab \\ &= a \end{aligned}$$

Donc, $(E, \sqcup, \sqcap)$ est un treillis.
Comme $a \sqcup 0 = a \oplus 0 - a \cdot 0 = a$ $0 \leq a$
$a \sqcup 1 = a \oplus 1 - a = 1$ $a \leq 1$
Donc 0 est le plus petit élément, 1 est le plus grand élément.

– Complément :
$a \sqcup (1-a) = a \oplus (1-a) - a(1-a) = 1 - a \oplus a^2 = 1$
$a \sqcap (1-a) = a - a^2 = 0$
Donc $\bar{a} = (1-a)$ est un complément.

– Distributivité :

$$\begin{aligned}(a \sqcup b) \sqcap c &= (a \oplus b - ab) \cdot c \\ &= ac \oplus bc - abc \\ &= ac \oplus bc - acbc \\ &= (a \sqcap c) \sqcup (b \sqcap c)\end{aligned}$$

Théorème 5.2.1 *Si $(E, \oplus, \cdot, 0, 1)$ est un anneau de Boole, alors $(E, \sqcup, \sqcap, 0, 1, \bar{\ })$ est une algèbre de Boole.*
(où $a \sqcup b = a \oplus b - ab$, $a \sqcap b = a \cdot b$, $\bar{a} = 1 - a$)

5.3 Réciprocité

Montrons que les deux constructions des sections précédentes :

(1) Algèbre de Boole → Anneau de Boole
(2) Anneau de Boole → Algèbre de Boole
sont inverses l'une de l'autre.

– (1)(2) :
Soit $(E, \sqcup, \sqcap, 0, 1, \bar{\ })$ une Algèbre de Boole.
Alors $(E, \oplus, \cdot, 0, 1)$ est un Anneau de Boole, avec :
$\begin{cases} a \oplus b = (a \sqcap \bar{b}) \sqcup (\bar{a} \sqcap b) \\ a \cdot b = a \sqcap b. \end{cases}$
On obtient ensuite une Algèbre de Boole :
$(E, \sqcup', \sqcap', 0, 1, \bar{\ }')$ avec
$\begin{cases} \bar{a}' = 1 - a = 1 \oplus a = (1 \sqcap \bar{a}) \sqcup (0 \sqcap a) = \bar{a} \\ a \sqcup' b = a \oplus b - ab \\ a \sqcap' b = a \cdot b = a \sqcap b \end{cases}$
$a \sqcup' b = 1 - (1-a)(1-b) = \overline{(\bar{a}' \sqcap' \bar{b}')}' = \overline{(\bar{a} \sqcap \bar{b})} = a \sqcup b$
Donc on ré-obtient l'Algèbre de Boole de départ.

– (2)(1) :
Soit $(E, \oplus, \cdot, 0, 1)$ un anneau de Boole

soit $(E, \sqcup, \sqcap, 0, 1, \bar{})$ l'algèbre de Boole associée.
où $a \sqcup b = a \oplus b - ab$, $a \sqcap b = a \cdot b$, $\bar{a} = 1 - a$.
on obtient $(E, \oplus, \cdot, 0, 1)$ avec

$$\begin{aligned} a \cdot b &= a \sqcap b \\ &= a \cdot b \end{aligned}$$

$$\begin{aligned} a \oplus b &= (a \sqcap \bar{b}) \sqcup (\bar{a} \sqcap b) \\ &= (a \sqcap (1 - b)) \sqcup ((1 - a) \sqcap b) \\ &= a \cdot (1 - b) \sqcup (1 - a) \cdot b \\ &= (a - ab) \sqcup (b - ab) \\ &= (a - ab) \oplus (b - ab) - (a - ab) \cdot (b - ab) \\ &= a \oplus b \oplus ab \oplus aab \oplus abb \oplus aabb \\ &= a \oplus b \oplus 4ab \\ &= a \oplus b \end{aligned}$$

Théorème 5.3.1 *Les transformations (1) et (2) sont inverses l'une de l'autre.*

Chapitre 6

Fonctions booléennes

6.1 Algèbre des fonctions booléennes

Soit $(\mathbb{B}, +, ., 0, 1, -)$ l'algèbre de Boole à 2 éléments. Une fonction booléenne à n arguments est une application de $\mathbb{B}^n$ dans $\mathbb{B}$. On note $\mathcal{B}_n$ l'ensemble des applications de $\mathbb{B}^n$ dans $\mathbb{B}$.

Définition 6.1.1 *Soient $f, g \in \mathcal{B}_n$. On pose $f \leq g$ si et seulement si $\forall \overrightarrow{x} \in \mathbb{B}^n, f(\overrightarrow{x}) \leq g(\overrightarrow{x})$.*

On vérifie que $(\mathcal{B}_n, \leq)$ est un treillis distributif, que la fonction constante 0 (resp. 1) est un plus petit (resp. plus grand) élément. Pour tout $f \in \mathcal{B}_n$, on définit $\bar{f} \in \mathcal{B}_n$ par :

$$\forall \overrightarrow{x} \in \mathbb{B}^n, \bar{f}(\overrightarrow{x}) = \overline{f(\overrightarrow{x})}.$$

On vérifie que $f \mapsto \bar{f}$, est une complémentation du treillis distributif $(\mathcal{B}_n, \leq)$.

6.2 Fonctions et polynômes

Définition 6.2.1 *L'ensemble des fonctions booléennes polynomiales à n arguments $(n \geq 0)$ est défini inductivement par*

(0) $(x_1, x_2, \ldots, x_n) \mapsto 0$ *et* $(x_1, x_2, \ldots, x_n) \mapsto 1$ *sont polynomiales*
(1) $\forall\, i \in [1, n], (x_1, x_2, \ldots, x_n) \mapsto x_i$ *est polynomiale*
(2) si f, g *sont polynomiales alors* $f + g$, $f \,.\, g$, $\overline{f}$ *sont polynomiales.*

Exemple 6.2.2

$$\begin{array}{llll} f: & \mathbb{B}^3 & \to & \mathbb{B} \\ & (x_1, x_2, x_3) & \mapsto & (\overline{(x_1 + x_2)} \,.\, (\overline{x_1} \,.\, x_2)) + x_3 \,.\, x_3 \end{array}$$

est polynomiale.

Remarque 6.2.3

$$f(\overrightarrow{x}) = (\overline{x_1} \,.\, \overline{x_2}) \,.\, \overline{x_1} \,.\, x_2 + x_3 = x_3$$

Théorème 6.2.4 *Toute fonction booléenne est polynomiale.*

Preuve : Soit $f : \mathbb{B}^n \to \mathbb{B}$

$$\forall\, x \in \mathbb{B} \text{ et } \epsilon \in \{0, 1\}, \text{ posons :} \qquad x^\epsilon = \left\{ \begin{array}{ll} x & \text{si } \epsilon = 1 \\ \overline{x} & \text{si } \epsilon = 0 \end{array} \right.$$

Considérons :

$$g(x_1, x_2, \ldots, x_n) = \sum_{f(b_1, b_2, \ldots, b_n) = 1} x_1^{b_1} x_2^{b_2} \ldots x_n^{b_n}$$

1 - g est polynomiale
2 - si $f(b_1, b_2, \ldots, b_n) = 1$ alors $g(b_1, b_2, \ldots, b_n) = 1$
3 - suppons $f(b_1, b_2, \ldots, b_n) = 0$

$$\forall\, b'_1, b'_2, \ldots, b'_n \mid f(b'_1, b'_2, \ldots, b'_n) = 1,$$

$$\exists\, i \in [1, n], b_i \neq b'_i, \text{ donc } b_i^{b'_i} = 0, \text{ donc } b_1^{b'_1} b_2^{b'_2} \ldots b_n^{b'_n} = 0$$

Donc

$$g(b_1, b_2, \ldots, b_n) = 0.$$

Les points (2)(3) montrent que :

$$f = g$$

□
Une autre preuve du théorème 6.2.4 repose sur le lemme suivant

Lemme 6.2.5 *Soit $f : \mathbb{B}^n \to \mathbb{B}$ avec $n \geq 1$. Alors, pour tout $\overrightarrow{y} \in \mathbb{B}^{n-1}$,*

$$f(x_1, \overrightarrow{y}) = x_1 \cdot f(1, \overrightarrow{y}) + \bar{x_1} \cdot f(0, \overrightarrow{y})$$

Preuve : On vérifie successivement que le membre gauche et le membre droit de cette égalité prennent la même valeur :
1- sur les arguments de la forme $(1, \overrightarrow{y})$
2- sur les arguments de la forme $(0, \overrightarrow{y})$. □
Le théorème 6.2.4 peut alors être prouvé par récurrence sur n (nous laissons en exercice le détail de cette seconde preuve).

Définition 6.2.6 *Soit $f : \mathbb{B}^n \to \mathbb{B}$. La fonction duale de f, $\tilde{f}$, est définie par :*

$$\tilde{f}(x_1, x_2, \ldots, x_n) = \overline{f(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n})}$$

Théorème 6.2.7 *Toute fonction booléenne est de la forme :*

$$f(x_1, x_2, \ldots, x_n) = \sum_{(\epsilon_1, \epsilon_2, \ldots, \epsilon_n) \in E} x_1^{\epsilon_1} x_2^{\epsilon_2} \ldots x_n^{\epsilon_n}$$

où E est une partie de $\{0,1\}^n$.

Preuve : Résulte de la preuve du théoreme 6.2.4 □

Théorème 6.2.8 *Toute fonction booléenne est de la forme*

$$f(x_1, x_2, \ldots, x_n) = \prod_{(\epsilon_1, \epsilon_2, \ldots, \epsilon_n) \in E} (x_1^{\epsilon_1} + x_2^{\epsilon_2} + \ldots + x_n^{\epsilon_n})$$

où E est une partie de $\{0,1\}^n$

Preuve : $\tilde{f}$ est de la forme $\sum_{(\epsilon_1,\epsilon_2,\ldots,\epsilon_n)\in E} x_1^{\epsilon_1}x_2^{\epsilon_2}\ldots x_n^{\epsilon_n}$

Donc

$$f(x_1,x_2,\ldots,x_n) = \prod_{(\epsilon_1,\epsilon_2,\ldots,\epsilon_n)\in E} (x_1^{\epsilon_1}+x_2^{\epsilon_2}+\ldots+x_n^{\epsilon_n})$$

□

6.3 Décompositions en sommes

Notons $X = \{x_1,\ldots,x_n\}$ un alphabet de variables et soit $\bar{X} = \{\bar{x_1},\ldots,\bar{x_n}\}$ un alphabet disjoint, en bijection avec X. On appelle *monôme* tout mot $m = x_{i_1}^{\epsilon_1}\cdot x_{i_2}^{\epsilon_2}\cdots x_{i_p}^{\epsilon_p}$ écrit sur l'alphabet $X\cup\bar{X}$, tel que : $0\leq p\leq n,\ \ 1\leq i_1 < i_2 < \cdots < i_p \leq n$. On note $\mathcal{M}(X)$ l'ensemble des monômes sur l'alphabet des variables X. La *fonction monômiale* associée à m est, $\tilde{m} : \mathbb{B}^n \to \mathbb{B}$, définie par :

$$\tilde{m}(x_1,x_2,\ldots,x_n) = x_{i_1}^{\epsilon_1}\cdot x_{i_2}^{\epsilon_2}\cdots x_{i_p}^{\epsilon_p}$$

Lorsque $p = 0$, $m = \epsilon$ et la fonction associée vaut 1. Dans ce qui suit on confond souvent [1] un monôme m et la fonction monomiale $\tilde{m}$ associée.

Le théorème 6.2.7 montre que toute fonction booléenne f est la somme de fonctions monomiales. On s'intéresse maintenant à la *minimisation* du *nombre* et de la *longueur* des monômes intervenant dans une décomposition de f en somme de monômes. La restriction de l'ordre (voir définition 6.1.1) à l'ensemble des fonctions monomiales s'interprète comme suit sur les monômes :

$$\tilde{m_1} \leq \tilde{m_2} \Leftrightarrow \text{ toute variable dans } m_2 \text{ figure sous la même forme dans } m_1$$

Autrement dit,

$$\tilde{m_1} \leq \tilde{m_2} \Leftrightarrow \text{ le mot } m_2 \text{ est sous-mot du mot } m_1.$$

Définition 6.3.1 *On appelle* monôme premier *d'une fonction booléenne f, un monôme m tel que*
1- $m \leq f$
2- $\forall m' \in \mathcal{M}(X), (m \leq m' \leq f) \Rightarrow m = m'$.

[1] abusivement, sans doute !

Théorème 6.3.2 *Toute fonction est somme de ses monômes premiers.*

Preuve : Soit $f : \mathbb{B}^n \to \mathbb{B}$ et soient $m_1, m_2, \ldots, m_p$ ses monômes premiers. D'après le théorème 6.2.7, f admet au moins une décomposition en somme de monômes :

$$f = \sum_{j=1}^{q} \mu_j.$$

Considérons

$$g = \sum_{i=1}^{p} m_i.$$

1-Puisque $\forall i \in [1,p], m_i \leq f$, on a $g \leq f$.
2-Soit $j \in [1,q]$. L'ensemble de monômes

$$\{m' \in \mathcal{M}(X) \mid \mu_j \leq m' \leq f\},$$

est non-vide, puisqu'il possède μ_j, et a un cardinal fini. Donc il admet au moins un élément maximal m. Cet élément maximal est un monôme premier : $\exists i \in [1,p], \mu_j \leq m_i$. Donc

$$\mu_j \leq \sum_{i=1}^{p} m_i = g$$

d' où $f \leq g$. □
D'après ce théorème 6.3.2, la somme des monômes premiers fournit une expression de la fonction. En général, cette représentation n'est pas minimale.

Définition 6.3.3 *Une* base *d'une fonction est un ensemble de monômes premiers dont la somme est égale à la fonction.*
Une base est dite irrédondante *lorsqu'elle est minimale relativement à l'inclusion.*

Proposition 6.3.4 *Soit* $f = \sum_{j=1}^{q} \mu_j$ *une décomposition d'une fonction booléenne* f *en somme de monômes. Alors, il existe une base irrédondante*

de f, $\{\nu_1, \nu_2, \ldots, \nu_r\}$ *telle que*
1- $r \leq q$
2- $\sum_{k=1}^{r} |\nu_k| \leq \sum_{j=1}^{q} |\mu_j|$

Preuve : Soit $M = \{m_1, m_2, \ldots, m_p\}$ l'ensemble des monômes premiers de f. La preuve du théorème 6.3.2 montre que,

$$\forall j \in [1, q], \exists i \in [1, p], \mu_j \leq m_i.$$

Choisissons, pour chaque j, un indice $i_j \in [1, p]$, tel que $\mu_j \leq m_{i_j}$. On a alors

$$f = \sum_{j=1}^{q} m_{i_j}.$$

Extrayons de $\{m_{i_j} \mid 1 \leq j \leq q\}$ une partie minimale pour l'inclusion, $N = \{\nu_k \mid 1 \leq k \leq r\}$, dont la somme soit encore égale à f.
N est bien une base irrédondante. Comme $N \subseteq M$, $r \leq q$.
Comme $\mu_j \leq m_{i_j}$, leurs longueurs vérifient l'inégalité opposée : $\mid \mu_j \mid \geq \mid m_{i_j} \mid$.
Donc

$$\sum_{j=1}^{q} |\mu_j| \geq \sum_{j=1}^{q} |m_{i_j}| \geq \sum_{k=1}^{r} |\nu_k|,$$

ce qui établit le point (2). □
Ainsi, la simplification d'une fonction passe pas la détermination de l'ensemble de ses monômes premiers, puis de ses bases irrédondantes.

6.4 Calcul des décompositions minimales

Nous exposons ici une méthode de calcul des bases irrédondantes d'une fonction booléenne. Cette méthode est basée sur l'opération de *consensus* entre monômes. Elle s'applique aux fonctions représentées sous une forme polynomiale arbitraire.

6.4.1 Tous les monômes premiers

Définition 6.4.1 *On dit que deux monômes m_1 et m_2 forment une paire productive lorsqu'une et une seule des variables apparaissant dans m_1 et m_2 est biforme.*
Dans ce cas, on appelle consensus *de m_1 et m_2 le monôme, noté* $\mathrm{cons}(m_1, m_2)$, *qui est le produit des variables monoformes de m_1 et m_2.*

Exemple 6.4.2 *Soient quatre monômes :*

$$m_1 = xy\bar{z} \qquad m_2 = x\bar{y}zt \qquad m_3 = \bar{x}yz \qquad m_4 = x\bar{t}$$

Les deux seules paires productives sont :$\{m_2, m_4\}, \{m_3, m_4\}$. *Leurs consensus sont :*

$$\mathrm{cons}(m_2, m_4) = x\bar{y}z; \;\; \mathrm{cons}(m_3, m_4) = yz\bar{t}.$$

Donnée : une liste de monômes U.
À calculer : l'ensemble des monômes premiers de la fonction somme des éléments de U.
Algorithme :

```
procedure  PREMIER(U: ensemble de monômes; var M: ensemble de monomes);
var: C,N: ensemble de monômes;
    FINI: booléen;
début
    M:=U; FINI:=0;
    tantque (not(FINI)) faire
        C:={ cons(m,m') | m ∈ M,m' ∈ M, (m,m') paire productive }
        N:= M ∪ C
        N:= {m ∈ N | ∀ m' ∈ N, m ≤ m' ⇒ m = m'}
        si N=M alors FINI:=1 sinon M := N;
    eriaf
fin
```

Exemple 6.4.3 *Soit la fonction*

$$f(x, y, z, t) = \bar{x}\bar{z} + xyt + \bar{x}yz + \bar{x}\bar{y}\bar{z} + \bar{y}z\bar{t}$$

Ligne 1 : Valeur initiale de M :

$\bar{x}\bar{z}$	xyt	$\bar{x}yz$	$\bar{x}\bar{y}\bar{z}$	$\bar{y}z\bar{t}$
1	2	3	4	5

Ligne 3 : Valeur de C (la liste des consensus)

$y\bar{z}t$	$\bar{x}y$	$\bar{x}\bar{y}\bar{t}$	yzt	$\bar{x}z\bar{t}$
1, 2	1, 3	1, 5	2, 3	3, 5

Ligne 5 : Valeur de N (la nouvelle liste de monômes)

$\bar{x}y$	$\bar{x}\bar{z}$	xyt	$\bar{x}\bar{y}\bar{t}$	$\bar{x}z\bar{t}$	yzt	$y\bar{z}t$	$\bar{y}z\bar{t}$
1	2	3	4	5	6	7	8

(la deuxième ligne du tableau attribue un nouveau numéro à chaque monôme).
Ligne 3 : Valeur de C

yt	$\bar{x}\bar{t}$	$\bar{x}z\bar{t}$	$y\bar{z}t$	$\bar{x}yt$	$\bar{x}\bar{y}\bar{t}$	$\bar{x}yz$
1, 3	1, 4	1, 8	2, 3	2, 6	2, 8	5, 6

Ligne 5 : Valeur de N

$\bar{x}y$	$\bar{x}\bar{z}$	$\bar{x}\bar{t}$	yt	$\bar{y}z\bar{t}$
1	2	3	4	5

Ligne 3 : Valeur de C

$\bar{x}z\bar{t}$	$\bar{x}\bar{y}\bar{t}$	$\bar{x}y$
1, 5	2, 5	3, 4

Ligne 5 : Valeur de N

$\bar{x}y$	$\bar{x}\bar{z}$	$\bar{x}\bar{t}$	yt	$\bar{y}z\bar{t}$
1	2	3	4	5

Comme $N = M$, l'algorithme s'arrête. La liste des monômes premiers de f est donc :

$$(\bar{x}y, \bar{x}\bar{z}, \bar{x}\bar{t}, yt, \bar{y}z\bar{t})$$

Preuve de l'algorithme du consensus

Lemme 6.4.4 *Soit (m_1, m_2) une paire de monômes productive.*
Alors $\mathrm{cons}(m_1, m_2) \leq m_1 + m_2$.

Preuve : Soient $m_1 = m'_1 x, m_2 = m'_2 \bar{x}$ où $m'_1, m'_2 \in \mathcal{M}(X), x \in X$.
Alors

$$\mathrm{cons}(m_1, m_2) = m'_1 \cdot m'_2 = m'_1 \cdot m'_2 \cdot x + m'_1 \cdot m'_2 \cdot \bar{x} \leq m'_1 \cdot x + m'_2 \cdot \bar{x} = m_1 + m_2.$$

□
Dans ce qui suit on note $f = \sum_{u \in U} u$ et l'on énonce des propriétés de l'algorithme appliqué à cet ensemble de monômes U.

Lemme 6.4.5 *En fin d'exécution de la ligne 1 (resp. 6), les propriétés suivantes sont vraies :*
(I1) $f = \sum_{m \in M} m$
(I2) $\forall m, m' \in M, m \leq m' \Rightarrow m = m'$
Si de plus, $FINI = 1$, *alors la propriété suivante est vraie :*
(I3) $\forall m, m' \in M$, *si* (m, m') *est productive, alors* $\exists m'' \in M, \mathrm{cons}(m, m') \leq m''$.

Lemme 6.4.6 *En fin d'exécution de la ligne 5, la propriété suivante est vraie : (I4)* $N \neq M \Rightarrow mr(N) \supset mr(M)$.

où $mr(P)$ désigne l'ensemble des monômes minorants de P :

$$mr(P) = \{m \in \mathcal{M}(X) \mid \exists m' \in P, m \leq m'\}.$$

On cherche maintenant à tirer des invariants (I1,I2,I3) la correction de l'algorithme. Donnons un lemme qui permet de raisonner par récurrence sur le nombre de variables. On particularise la variable x_1 et l'on note : $g(1), g(0) : \mathbb{B}^{n-1} \to \mathbb{B}$ les applications partielles

$$g(1) : \overrightarrow{y} \mapsto g(1, \overrightarrow{y}); \quad g(0) : \overrightarrow{y} \mapsto g(0, \overrightarrow{y}).$$

Lemme 6.4.7 *Soit* $M = \{m_1, m_2, \ldots, m_p\}$ *un ensemble de monômes. Notons* $I_+ = \{i \in [1, p] \mid m_i \leq x_1\}, I_- = \{i \in [1, p] \mid m_i \leq \bar{x_1}\}, I_0 = [1, p] - (I_+ \cup I_-)$.
Alors, pour tous $i, j \in [1, p]$, *on a :*
1-si $m_i \leq m_j$ *alors* $m_i(1) \leq m_j(1)$ *et* $m_i(0) \leq m_j(0)$
2-si $i, j \in I_+ \cup I_0$ *et* $(m_i(1), m_j(1))$ *est productive, alors* (m_i, m_j) *est productive et* $\mathrm{cons}(m_i(1), m_j(1)) = \mathrm{cons}(m_i, m_j)(1)$.

2'-si $i, j \in I_- \cup I_0$ et $(m_i(0), m_j(0))$ est productive, alors (m_i, m_j) est productive et $\mathrm{cons}(m_i(0), m_j(0)) = \mathrm{cons}(m_i, m_j)(0)$.

Preuve : 1- Evident.
2- Supposons que : $m_i(1) = \alpha x$; $m_j(1) = \beta \bar{x}$ où x est une variable autre que x_1 et la paire (α, β) ne présente que des variables monoformes.
Dans la paire (m_i, m_j) la variable x_1 est encore monoforme (elle ne peut apparaître que positivement). Donc (m_i, m_j) est productive.
Si $i, j \in I_0$, alors

$$\mathrm{cons}(m_i, m_j) = \alpha \cdot \beta; \text{ donc } \mathrm{cons}(m_i, m_j)(1) = \alpha \cdot \beta = \mathrm{cons}(m_i(1), m_j(1)).$$

Si $i \in I_+$ ou $j \in I_+$, alors

$$\mathrm{cons}(m_i, m_j) = \alpha \cdot \beta \cdot x_1; \text{ et on a encore } \mathrm{cons}(m_i, m_j)(1) = \alpha \cdot \beta = \mathrm{cons}(m_i(1), m_j(1)).$$

2'- Calcul analogue où l'on remplace x_1 par $\bar{x_1}$ et 1 par 0. □

Lemme 6.4.8 *Soit f une fonction booléenne et $M = \{m_1, m_2, \ldots, m_p\}$ un ensemble de monômes tels que :*
H1 : $f = \sum_{i=1}^{p} m_i$
H2 : pour tous $1 \leq i < j \leq p$, les monômes (m_i, m_j) sont incomparables.
H3 : pour tous $1 \leq i < j \leq p$, si (m_i, m_j) est productive, alors il existe $k \in [1, p]$ tel que $\mathrm{cons}(m_i, m_j) \leq m_k$.
Alors l'ensemble des monômes premiers de f est exactement $\{m_1, m_2, \ldots, m_p\}$.

Preuve : 1- Montrons, par récurrence sur le nombre de variables n, que tout monôme premier de f est l'un des m_i.
Base : $n = 0$
Dans ce cas, les deux seuls ensembles M possibles sont $\emptyset$ et $\{1\}$.Ce sont bien les ensembles de monômes premiers respectivement de la fonction 0 et de la fonction 1.
Induction : $n \geq 1$
Posons

$$J_+ = \{i \in I_+ \cup I_0 \mid \forall j \in I_+ \cup I_0, m_i(1) \leq m_j(1) \Rightarrow m_i(1) = m_j(1)\};$$

$$J_- = \{i \in I_- \cup I_0 \mid \forall j \in I_- \cup I_0, m_i(0) \leq m_j(0) \Rightarrow m_i(0) = m_j(0)\}.$$

1.1- Les ensembles $M_+ = \{m_i(1) \mid i \in J_+\}$, $M_- = \{m_i(0) \mid i \in J_-\}$ vérifient clairement (H1,H2) vis à vis de $f(1)$ (resp. $f(0)$). Montrons qu'ils vérifient aussi (H3).
Soient $i, j \in J_+$ tels que $(m_i(1), m_j(1))$ soit productive. D' après le lemme 6.4.7, point 2, (m_i, m_j) est productive et

$$\text{cons}(m_i(1), m_j(1)) = \text{cons}(m_i, m_j)(1). \tag{6.1}$$

D'après l'hypothèse (H3) sur M,

$$\exists k \in [1, p], \text{cons}(m_i, m_j) \leq m_k \tag{6.2}$$

et en appliquant le lemme 6.4.7, point 1,

$$\text{cons}(m_i, m_j)(1) \leq m_k(1). \tag{6.3}$$

La majoration (6.2) montre que $k \in I_0$. Donc il existe $\ell \in J_+$ tel que

$$m_k(1) \leq m_\ell(1) \tag{6.4}$$

Les équations (6.1,6.3,6.4) montrent que

$$\text{cons}(m_i(1), m_j(1)) \leq m_\ell(1)$$

où $\ell \in J_+$, donc la condition (H3) est remplie par M_+.
De façon analogue, la condition (H3) est remplie par M_-.
1.2-Soit m un monôme premier de f. Montrons que $m \in M$.
cas 1 :$m \leq x_1$
$m(1)$ est un monôme qui minore $f(1)$. Donc, il existe un monôme premier μ de $f(1)$ tel que

$$m(1) \leq \mu.$$

Par hypothèse de récurrence, comme M_+ vérifie (H1,H2,H3), M_+ possède tous les monômes premiers de $f(1)$. Donc il existe $i \in J_+$, tel que

$$\mu = m_i(1).$$

Remarquons que $m(0) \leq x_1(0) = 0$, donc

$$m(1) \leq m_i(1) \text{ et } m(0) \leq m_i(0)$$

d'où (en appliquant le lemme 6.2.5),

$$m \leq m_i$$

et comme m est premier

$$m = m_i,$$

donc m est bien un élément de M.

cas 2 :$m \leq \bar{x_1}$

Même type d'argumentation que dans le cas 1, en remplaçant $(1, 0, M_+, J_+)$ par $(0, 1, M_-, J_-)$.

cas 3 :$m \not\leq x_1$ et $m \not\leq \bar{x_1}$

On applique ici aussi l' hypothèse de récurrence à M_+ et à M_- : il existe $i \in J_+, j \in J_-$ tels que

$$m = m(1) \leq m_i(1); \;\; m = m(0) \leq m_j(0).$$

On a donc

$$m_i \in \{\alpha, x_1\alpha\}, \;\; m_j \in \{\beta, \bar{x_1}\beta\}, \;\; m \leq \alpha, \;\; m \leq \beta.$$

Comme $m \leq \alpha \cdot \beta$ et $m \neq 0$ (on vérifie que 0 n'est pas une fonction monomiale), nécessairement $\{\alpha, \beta\}$ est une paire ne contenant que des variables monoformes. L'une des équations suivantes est donc vraie :

$$m \leq \alpha = m_i \tag{6.5}$$

ou

$$m \leq \beta = m_j \tag{6.6}$$

ou

$$m \leq \alpha \cdot \beta = \mathrm{cons}(m_i, m_j). \tag{6.7}$$

Si (6.5) se produit alors $m = m_i$.
Si (6.6) se produit alors $m = m_j$.
Si (6.7) se produit alors, par (H3), il existe $k \in [1, p]$ tel que

$$\mathrm{cons}(m_i, m_j) \leq m_k. \tag{6.8}$$

Par (6.7,6.8), $m \leq m_k$ et finalement $m = m_k$.

2- L'ensemble $\{m_i \mid 1 \leq i \leq p\}$ contient l'ensemble des monômes premiers de f. Soit $i \in [1, p]$:

m_i est majoré par un monôme premier, qui est donc un m_j ($j \in [1, p]$). Mais d'après (H2), $i = j$, donc m_i est premier. □

Théorème 6.4.9 *Soit $f = \sum_{u \in U} u$ une somme de monômes. La procédure PREMIER(U,M) se termine et affecte à M l'ensemble des monômes premiers de f.*

Preuve :
Terminaison :
D'après le lemme 6.4.6, chaque passage dans la boucle 2-6 augmente la cardinalité de $mr(M)$ d'au moins 1, sauf le dernier passage. L'exécution de PREMIER passe donc au plus Card$(\{m \in \mathcal{M}(X) \mid m \leq f\}) + 1$ fois dans cette boucle.
Correction :
D'après le lemme 6.4.5, en fin d'exécution de PREMIER, les invariants $(I1, I2, I3)$ sont valides. L'ensemble M vérifie donc les hypothèses du lemme 6.4.8, donc M est exactement l'ensemble des monômes premiers de f. □

6.4.2 Les bases irrédondantes

Une méthode élémentaire pour obtenir les bases irrédondantes d'une fonction $f$consiste à couvrir de façon minimale ses monômes canoniques par ses monômes premiers.
Soient $m_1, m_2, \ldots, m_p$ ses monômes premiers et $\mu_1, \mu_2, \ldots, \mu_q$ ses monômes canoniques. On associe à chaque monôme canonique μ_j, $1 \leq j \leq q$, de f, le produit

$$\Pi_j = \Pi_{k=1}^{\ell(j)} m_{\alpha(j,k)}$$

où $1 \leq \alpha(j,1) < \ldots < \alpha(j,k) < \ldots < \alpha(j,\ell(j)) \leq p$
sont les indices des monômes premiers qui majorent μ_j. On a alors

$$f = \sum_{j=1}^{q} \mu_j \leq \sum_{j=1}^{q} \Pi_j.$$

En développant la somme $\sum_{j=1}^{q} \Pi_j$ en un produit de sommes de monômes premiers, et en ne gardant que les sommes S_k qui sont minimales pour l' inclusion, on obtient :

$$f = \sum_{j=1}^{q} \mu_j \leq \sum_{j=1}^{q} \Pi_j = \Pi_{k=1}^{r} S_k.$$

Pour tout k on a bien

$$f = S_k.$$

On peut montrer que $\{S_k \mid 1 \leq k \leq r\}$ est exactement l'ensemble des bases irrédondantes de f.

Exemple 6.4.10 *Les monômes premiers de la fonction* $f(x,y,z) = x\bar{y} + y\bar{z} + z\bar{x}$ *sont* $m_1 = x\bar{y}$, $m_2 = y\bar{z}$, $m_3 = \bar{x}z$, $m_4 = \bar{x}y$, $m_5 = \bar{y}z$, $m_6 = x\bar{z}$. *Les monômes canoniques de* f *sont :*

$$\mu_1 = \bar{x}\bar{y}z \quad \mu_2 = \bar{x}y\bar{z} \quad \mu_3 = x\bar{y}\bar{z} \quad \mu_4 = xy\bar{z} \quad \mu_5 = x\bar{y}z \quad \mu_6 = \bar{x}yz$$

La couverture des μ_j *par les* m_i *est donnée par le tableau*

μ_1	μ_2	μ_3	μ_4	μ_5	μ_6
$m_3 \cdot m_5$	$m_2 \cdot m_4$	$m_1 \cdot m_6$	$m_2 \cdot m_6$	$m_1 \cdot m_5$	$m_3 \cdot m_4$

Le développement de la somme

$$(m_3 \cdot m_5) + (m_2 \cdot m_4) + (m_1 \cdot m_6) + (m_2 \cdot m_6) + (m_1 \cdot m_5) + (m_3 \cdot m_4),$$

où l'on ne garde que les sommes minimales, donne

$$(m_1+m_2+m_3)\cdot(m_2+m_3+m_5+m_6)\cdot(m_1+m_3+m_4+m_6)\cdot(m_1+m_2+m_4+m_5)\cdot(m_4+m_5+m_6)$$

D'où les bases irrédondantes : $\{m_1, m_2, m_3\}, \{m_2, m_3, m_5, m_6\}, \{m_1, m_3, m_4, m_6\}, \{m_1, m_2, m_4, m_5\}, \{m_4, m_5, m_6\}$.
On peut aussi visualiser la majoration des μ_j *par les* m_i *au moyen du tableau ci-dessous. Une base irrédondante correspond à un ensemble minimal de lignes qui contient au moins un* $\bullet$ *par colonne.*

	μ_1	μ_2	μ_3	μ_4	μ_5	μ_6
m_1			$\bullet$		$\bullet$	
m_2		$\bullet$		$\bullet$		
m_3	$\bullet$					$\bullet$
m_4		$\bullet$				$\bullet$
m_5	$\bullet$				$\bullet$	
m_6			$\bullet$	$\bullet$		

Chapitre 7

Logique propositionnelle

7.1 Formules propositionnelles : syntaxe

On étudie les formules logiques construites à partir :
- d'un ensemble dénombrable $\mathcal{P} = \{\ p,\ q,\ r,\ \ldots\}$ de variables propositionnelles
- de l'ensemble de connecteurs $\mathcal{C} = \{\neg,\ \wedge,\ \vee,\ \rightarrow,\ \leftrightarrow\}$

Définition 7.1.1 *L'ensemble des formules propositionnelles construites sur $\mathcal{P}$ et $\mathcal{C}$, $\mathcal{F}(\mathcal{C}, \mathcal{P})$, est l'ensemble des termes correctement formés sur l' ensemble de variables $\mathcal{P}$ et sur la signature $(\mathcal{C}, \mathbf{ar})$ définie par :*
$\mathbf{ar}(\neg) = 1, \mathbf{ar}(\wedge) = \mathbf{ar}(\vee) = \mathbf{ar}(\rightarrow) = \mathbf{ar}(\leftrightarrow) = 2.$

7.2 Formules propositionnelles : sémantique

Une interprétation est une application $I : \mathcal{P} \rightarrow \mathbb{B}$.
On définit alors l'application "valeur de vérité", $\tilde{I} : \mathcal{F}(\mathcal{C}, \mathcal{P}) \rightarrow \mathbb{B}$ par la définition inductive suivante.

Définition 7.2.1 *(i) si $v \in \mathcal{P}$, alors $\tilde{I}(v) = I(v)$*

(ii) si $G \in \mathcal{F}(\mathcal{P}, \mathcal{C})$, $\tilde{I}(\neg G) = \overline{\tilde{I}(G)}$

(iii) si $F, G \in \mathcal{F}(\mathcal{P}, \mathcal{C})$
$\tilde{I}(\wedge FG) = \tilde{I}(F) \,.\, \tilde{I}(G)$
$\tilde{I}(\vee FG) = \tilde{I}(F) \,+\, \tilde{I}(G)$
$\tilde{I}(\rightarrow FG) = \overline{\tilde{I}(F)} \,+\, \tilde{I}(G)$
$\tilde{I}(\leftrightarrow FG) = \tilde{I}(F) \,.\, \tilde{I}(G) \,+\, \overline{\tilde{I}(F)} \,.\, \overline{\tilde{I}(G)}$

Définition 7.2.2 *(i) Si I est une interprétation et F une formule, F est satisfaite par I signifie :* $\tilde{I}(F) = 1$.
On dit encore que F "est vraie" dans I.
(ii) F est satisfaisable ssi il existe une interprétation I qui satisfait F.
(iii) F est une tautologie ssi, pour toute interprétation I, $\tilde{I}(F) = 1$.

Enrichissons $\mathcal{C}$ d'un connecteur ff (constante "faux").
On adapte la définition inductive de $\mathcal{F}(\mathcal{C}, \mathcal{P})$ en posant :
(i) $\forall v \in \mathcal{P} \cup \{ff\}$, $v \in \mathcal{F}(\mathcal{C}, \mathcal{P})$
$\vdots$

On adapte $\tilde{I}$ en posant :
(i) $\tilde{I}(ff) = 0$.

Soit $\mathcal{P}_n = \{p_1, p_2, \ldots, p_n\} \subseteq \mathcal{P}$.
On définit une application $\varphi : \mathcal{F}(\mathcal{P}_n, \mathcal{C}) \longrightarrow \mathcal{B}_n = \{0,1\}^{\{0,1\}^n}$
($\mathcal{B}_n$ est l'ensemble des fonctions booléennes à n arguments) par :

$$\forall F \in \mathcal{F}(\mathcal{C}, \mathcal{P}), \forall \overrightarrow{b} \in \{0,1\}^n, \ \ (\varphi(F))(\overrightarrow{b}) = \tilde{I}_{\overrightarrow{b}}(F)$$

où $I_{\overrightarrow{b}}$ est l'interprétation définie par $I_{\overrightarrow{b}}(\pi) = b_i$.

Théorème 7.2.3 *Toute fonction booléenne de n variables est la fonction associée à une formule propositionnelle sur n variables.*

Preuve : Pour tout $p \in \mathcal{P}$, $\varepsilon \in \{0,1\}$, notons

$$p^\varepsilon = \begin{cases} p & \text{si } \varepsilon = 1 \\ \neg p & \text{si } \varepsilon = 0 \end{cases}$$

Remarquons que :

$\varphi(p_i) = x_i$
$\varphi({p_i}^{\varepsilon_i}) = {x_i}^{\varepsilon_i}$
$\varphi(\wedge FG) = \varphi(F) \, . \, \varphi(G)$
$\varphi(\vee FG) = \varphi(F) \ + \ \varphi(G)$

Par le théorème 6.2.7, toute fonction $f \in \mathcal{B}_n$ est de la forme :

$$f(x_1, \ldots, x_n) = \sum_{(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) \in E} {x_1}^{\varepsilon_1} {x_2}^{\varepsilon_2} \ldots {x_n}^{\varepsilon_n}$$

Donc, $f = \varphi(\bigvee_{(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) \in E} (\bigwedge_{i=1}^n \ {p_1}^{\varepsilon_1} {p_2}^{\varepsilon_2} \ldots {p_n}^{\varepsilon_n}))$

$\square$

Notations :

$\bigvee_{i=1}^n \ F_1 F_2 \ldots F_p$ est une abréviation de

$\vee F_1 (\vee F_2 (\vee \ldots (\vee F_{p-1} F_p \underbrace{) \ldots)}_{p-1 \text{ parenthèses.}}$

$\bigwedge_{i=1}^n \ F_1 F_2 \ldots F_p$ est une abréviation de

$\wedge F_1 (\wedge F_2 (\wedge \ldots (\wedge F_{p-1} F_p \underbrace{) \ldots)}_{p-1 \text{ parenthèses.}}$

$\square$

Notations :
Pour toutes formules F, G,

$$\models F$$

se lit, “F est valide” et signifie : $\forall I \in \{0,1\}^{\mathcal{P}}, \quad \tilde{I}(F) = 1$

$$F \models G$$

se lit, "F implique sémantiquement G" et signifie : $\forall I \in \{0,1\}^{\mathcal{P}}$, $\tilde{I}(F) = 1 \Rightarrow \tilde{I}(G) = 1$.

$$F \models\!\mid G$$

se lit "F est sémantiquement équivalente à G" et signifie : $\forall I \in \{0,1\}^{\mathcal{P}}$, $\tilde{I}(F) = \tilde{I}(G)$).

Si $\mathcal{E}$ est une ensemble de formules,

$$\mathcal{E} \models F$$

se lit, "$\mathcal{E}$ implique sémantiquement G" et signifie :
$\forall I \in \{0,1\}^{\mathcal{P}}$, $[\forall G \in \mathcal{E},\ \tilde{I}(G) = 1] \Rightarrow \tilde{I}(F) = 1$.

On dit qu'une formule F est :
* en forme normale disjonctive ssi F s'écrit sous la forme :
  $F = \bigvee_{i=1}^{m} (\bigwedge_{j=1}^{n_i} p_{i,j}^{\varepsilon_{i,j}})$ où $p_{i,j} \in \mathcal{P}_n$, $\varepsilon_{i,j} \in \{0,1\}$.
  ($m = 0$ correspond à $F = ff$)

* en forme normale disjonctive canonique ssi F s'écrit sous la forme :
  $F = \bigvee_{i=1}^{m} (\bigwedge_{j=1}^{n_i} p_{i,j}^{\varepsilon_{i,j}})$ où $\forall i$, $\{p_{i,j}\}_{1\le j\le n_i} = \{p_k\}_{1\le k\le n}$ et $n = n_i$

* en forme normale conjonctive ssi F s'écrit sous la forme :
  $F = \bigwedge_{i=1}^{m} (\bigvee_{j=1}^{n_i} p_{i,j}^{\varepsilon_{i,j}})$ où $p_{i,j} \in \mathcal{P}_n$, $\varepsilon_{i,j} \in \{0,1\}$.
  ($m = 0$ correspond à $F = p_1 \cup \bar{p_1}$)

* en forme normale conjonctive canonique ssi F s'écrit sous la forme :
  $F = \bigwedge_{i=1}^{m} (\bigvee_{j=1}^{n_i} p_{i,j}^{\varepsilon_{i,j}})$ où $\forall i$, $\{p_{i,j}\}_{1\le j\le n_i} = \{p_k\}_{1\le k\le n}$ et $n = n_i$

Théorème 7.2.4 *(1) Pour toute formule $F \in \mathcal{F}(\mathcal{C}, \mathcal{P}_n)$, il existe $F^c \in \mathcal{F}(\mathcal{C}\mathcal{P}_n)$ telle que, F^c est en forme normale conjonctive canonique et $F \mid\!=\!\mid F^c$*
(2) Pour toute formule $F \in \mathcal{F}(\mathcal{C}, \mathcal{P}_n)$, il existe $F^d \in \mathcal{F}(\mathcal{C}, \mathcal{P}_n)$ telle que, F^d est en forme normale disjonctive canonique et $F \models\!\mid F^d$.

Preuve : La preuve du théorème 7.2.3 montre l'existence de F^d.
Utilisons le théorème 6.2.8 :

la fonction $\varphi(F)$ est de la forme $\prod_{\vec{\varepsilon} \in E} (x_1^{\varepsilon_1} + x_2^{\varepsilon_2} + \ldots + x_n^{\varepsilon_n})$

Posons $F^c = \bigwedge_{\vec{\varepsilon} \in E} (\bigvee_{i=1}^{n} p_i^{\varepsilon_i})$.

Comme $\varphi(F) = \varphi(F^c)$, $\quad F \models\!\mid F^c$
et F^c est en forme normale conjonctive canonique.
□

7.3 Un premier système formel

Un système formel est constitué d'un *langage*, d'un ensemble d'*axiomes* pris parmi les mots du langage et d'un ensemble de *règles de déduction*. (Les mots du langage sont aussi appelés les *jugements* du système formel). Les mots que l'on peut obtenir à partir des axiomes par application, un nombre fini de fois, de règles de déduction, sont les *théorèmes* du sytème formel.
Nous examinons dans ce paragraphe un sytème formel dont le langage est l'ensemble de toutes les formules propositionnelles et où les théorèmes sont les *tautologies*.
Langage :
$\mathcal{F}(\mathcal{C}, \mathcal{P})$ où $\mathcal{C} = \{\rightarrow, ff\}$

Axiomes : toutes les instances des schémas d'axiomes A1, A2, A3
A1 : $p \rightarrow (q \rightarrow p)$
A2 : $(p \rightarrow (q \rightarrow r)) \rightarrow ((p \rightarrow q) \rightarrow (p \rightarrow r))$
A3 : $((p \rightarrow ff) \rightarrow ff) \rightarrow p$

On note $\mathcal{A}$ l'ensemble des axiomes.
Règle de déduction : Modus Ponens

$$\text{i. e.} \qquad \frac{\mathrm{p} \qquad \mathrm{p} \rightarrow \mathrm{q}}{\mathrm{q}}$$

Preuve, dérivation : On appelle preuve (ou dérivation) toute suite finie de formules, $(F_i)_{1 \leq i \leq n}$, telle que
$\forall i$, F_i est un axiome ou $\exists j \leq k < i \quad | \quad (F_j, F_k, F_i)$ est une instance de MP

ou (F_k, F_j, F_i) est une instance de MP.
Exemple
Voici une preuve de $p \to p$:

1	$p \to [(p \to p) \to p)]$	$A1$
2	$p \to [(p \to p) \to p)] \to [p \to (p \to p)] \to (p \to p)]$	$A2$
3	$[p \to (p \to p)] \to (p \to p)]$	$MP1, 2$
4	$p \to (p \to p)$	$A1$
5	$p \to p$	$MP\ 4, 3$

Donnons maintenant une preuve de $\mathrm{ff} \to p$:

1	$\mathrm{ff} \to [(p \to \mathrm{ff}) \to \mathrm{ff}]$	$A1$
2	$[(p \to \mathrm{ff}) \to \mathrm{ff}] \to p$	$A3$
3	$[((p \to \mathrm{ff}) \to \mathrm{ff}) \to p] \to [\mathrm{ff} \to [((p \to \mathrm{ff}) \to \mathrm{ff}) \to p]]$	$A1$
4	$[\mathrm{ff} \to [((p \to \mathrm{ff}) \to \mathrm{ff}) \to p]]$	$MP2, 3$
5	$\{\mathrm{ff} \to [((p \to \mathrm{ff}) \to \mathrm{ff}) \to p]\} \to \{[\mathrm{ff} \to ((p \to \mathrm{ff}) \to \mathrm{ff})] \to [\mathrm{ff} \to p]\}$	$A2$
6	$[\mathrm{ff} \to ((p \to \mathrm{ff}) \to \mathrm{ff})] \to [\mathrm{ff} \to p]$	$MP\ 4, 5$
7	$\mathrm{ff} \to p$	$MP\ 1, 6$

□
Relation $\vdash$:

$$\vdash F$$

se lit "F est démontrable" et signifie : "il existe une preuve $(F_i)_{1 \leq i \leq n}$ aboutissant à $F_n = F$".
Relativisation à un ensemble de formules $\mathcal{E}$:

$$\mathcal{E} \vdash F$$

se lit "F est démontrable à partir de $\mathcal{E}$" et signifie : "il existe une preuve $(F_i)_{1 \leq i \leq n}$, dans le système formel $\langle \mathcal{F}, \mathcal{A} \cup \mathcal{E}, MP \rangle$ aboutissant à $F_n = F$". Une telle suite $(F_i)_{1 \leq i \leq n}$ est aussi appelée une preuve relativement à $\mathcal{E}$.

7.3.1 Théorème de déduction

Lemme 7.3.1 $\forall F, G \in \mathcal{F}$,
$\vdash (F \to G) \Leftrightarrow F \vdash G$

1) $\Rightarrow$ *immédiat*

2) $\Leftarrow$ *supposons* $F \vdash G$
Soit $D = (G_1, G_2, \ldots, G_n)$ *une preuve relativement à* F *telle que* $G_n = G$.
Montrons par récurrence sur $k \in [1, n]$ *la propriété* $\mathcal{P}(k)$ *:*

$$\vdash\ F \to G_k.$$

a) $G_k = F$
Dans ce cas, il existe bien une preuve de $F \to F$ *(exemple vu plus haut).*
b) G_k *est un axiome* $(G_k,\ G_k \to (F \to G_k),\ F \to G_k)$

c) $G_i,\ G_j = G_i \to G_k$ *où* $i, j \leq k$

1	$F \to (G_i \to G_k)$	*(hypothèse de récurrence)*
2	$F \to G_i$	*(hypothèse de récurrence)*
3	$[F \to (G_i \to G_k)] \to [(F \to G_i) \to (F \to G_k)]$	
4	$(F \to G_i) \to (F \to G_k)$	*MP 1, 3*
5	$F \to G_k$	*MP 2, 4*

Théorème 7.3.2 (de déduction) *Soient* $P \subseteq \mathcal{F}$, *et* $F, G \in \mathcal{F}$.
$P\ \vdash\ F \to G \quad \Leftrightarrow \quad P, F \vdash G$

Preuve :
$\Rightarrow$ vrai, en utilisant MP
$\Leftarrow$ soit $D = (G_1, G_2, \ldots, G_n)$ une preuve de $G_n = G$ relativement à $\mathcal{A} \cup P \cup \{F\}$. On argumente comme pour le lemme 1, en traitant P de la même manière que $\mathcal{A}$.
$\square$

Corollaire 7.3.3 *Pour tout* $P \subseteq \mathcal{F}$ *et* $G \in \mathcal{F}$,
$P \vdash G \ \Leftrightarrow\ P \cup \{G \to \mathrm{ff}\} \vdash \mathrm{ff}$
(trivial pour $\models$*)*

Adéquation :

Théorème 7.3.4 (de validité) $\forall F \in \mathcal{F}, \vdash F\ \Rightarrow \models F$

Preuve : Par récurrence sur la longueur des preuves.
□

7.3.2 Complétude

Définition 7.3.5 *Soit I une interprétation quelconque.*
On pose $F^I = \begin{cases} F & si\, I(F) = 1 \\ F \rightarrow \text{ff} & si\, I(F) = 0 \end{cases}$

Lemme 7.3.6 *Soit $F \in \mathfrak{F}$ et $\{p_1, p_2, \ldots, p_n\}$ l'ensemble des variables apparaissant dans F. $\forall I \in \mathfrak{I}$,* $p_1^I, \ldots, p_n^I \vdash F^I$

Preuve : Récurrence sur le nombre de "$\rightarrow$" dans F.
i) 0 :
- $F = p_i$ $\quad F^I = p_i^I$
- $F = \text{ff}$ $\quad F^I = (\text{ff} \rightarrow \text{ff})$ $\quad$ or $\vdash (\text{ff} \rightarrow \text{ff})$

ii) $F = (G \rightarrow H)$
$p_1^I, \ldots, p_n^I \vdash G^I$ (Hypothèse de récurrence)
$p_1^I, \ldots, p_n^I \vdash r^I$ (Hypothèse de récurrence)

cas 1 : $G^I = G$, $H^I = H$
1− $H \rightarrow (G \rightarrow H)$ (A1)
2− H
3− $G \rightarrow H$ (MP 1, 2)
$= (G \rightarrow H]^I$

cas 2 : $G^I = G \rightarrow \text{ff}$, $H^I = H$
même preuve

cas 3 : $G^I = G \rightarrow \text{ff}$, $H^I = H \rightarrow \text{ff}$ $\quad (G \rightarrow H)^I = G \rightarrow H$
Montrons que $G \rightarrow \text{ff} \vdash G \rightarrow H$

0−	$G \to \mathrm{ff}$	
1−	$\mathrm{ff} \to H$	(voir l'exemple plus haut, preuve de longueur 7)
2−	$(\mathrm{ff} \to H) \to (G \to (\mathrm{ff} \to H))$	A1
3−	$G \to (\mathrm{ff} \to H)$	MP 1, 2
4−	$[G \to (\mathrm{ff} \to H)] \to [(G \to \mathrm{ff}) \to (G \to H)]$	$A2$
5−	$(G \to \mathrm{ff}) \to (G \to H)$	MP 3, 4
6−	$G \to H$	MP 0, 5

cas 4 : $G^I = G$, $H^I = H \to \mathrm{ff}$, $(G \to H)^I = (G \to H) \to \mathrm{ff}$
$G, H \to \mathrm{ff} \vdash (G \to H) \to \mathrm{ff}$
$\Leftrightarrow \quad G, H \to \mathrm{ff}, (G \to H) \quad \vdash \mathrm{ff}$
(par le théorème de déduction)

1−	G	
2−	$G \to H$	
3−	H	MP 1, 2
4−	$H \to \mathrm{ff}$	
5−	ff	MP 3, 4

□

Lemme 7.3.7 *Si* $\models F$ *alors* $\forall I, \quad p_1^I, \ldots, p_n^I \vdash F$.

Preuve : résulte du lemme précédent, puisque $F^I = F$.
□

Lemme 7.3.8 *Supposons* $\models F$. *Soit* $p'_i \in \{p_i, \neg p_i\}$ $(1 \le i \le n)$.
Alors, pour tout $k \le n$, $\quad p'_1, p'_2, \ldots, p'_k \vdash F$

Preuve :
1) Montrons que $G \to F, \quad (G \to \mathrm{ff}) \to F \vdash F$
revient à : $G \to F, \quad (G \to \mathrm{ff}) \to F, \quad F \to \mathrm{ff} \vdash \mathrm{ff}$

1−	$F \to \mathrm{ff}$	Hypothèse
2−	$(F \to \mathrm{ff}) \to (G \to (F \to \mathrm{ff}))$	A1
3−	$G \to (F \to \mathrm{ff})$	MP 1, 2
4−	$[G \to (F \to \mathrm{ff})] \to [(G \to F) \to (G \to \mathrm{ff})]$	A2
5−	$(G \to F) \to (G \to \mathrm{ff})$	MP 3, 4
6−	$G \to F$	Hypothèse
7−	$G \to \mathrm{ff}$	MP 5, 6
8−	$(G \to \mathrm{ff}) \to F$	Hypothèse
9−	F	MP 7, 8
10−	$F \to \mathrm{ff}$	Hypothèse
11−	ff	MP 9, 10

2) Par récurrence descendante sur k :

- vrai si $k = n$
- $\left\{ \begin{array}{l} p'_1, p'_2, \ldots, p'_k, p'_{k+1} \vdash F \\ p'_1, p'_2, \ldots, p'_k, \neg p'_{k+1} \vdash F \quad \text{(Hypothèse de récurrence)} \end{array} \right.$ Ici $\neg p'_i$ désigne $p_i \to \mathrm{ff}$ (respectivement p_i)si $p'_i = p_i$ (resp. si $p'_i = p_i \to \mathrm{ff}$).
- donc, par le théorème de déduction :

$$p'_1, p'_2, \ldots, p'_k \vdash p'_{k+1} \to F \text{ et } p'_1, p'_2, \ldots, \neg p'_{k+1} \to F$$

- donc $p'_1, p'_2, \ldots, p'_k \vdash F$ (d' après la partie 1)

□

Théorème 7.3.9 (de complétude) *Pour toute formule $F \in \mathcal{F}$, si $\models F$ alors $\vdash F$.*

La conjonction des théorèmes 7.3.4 (validité) et 7.3.9 (complétude), montre que les théorèmes du sytème formel étudié dans ce paragraphe sont exactement les tautologies. Autrement dit : une formule est *vraie* si et seulement si elle est *prouvable* dans ce système.
C'est cette propriété qui est remarquable et que l'on souhaiterait vérifiée par chaque système formel.
Nous désignons désormais par SH ce premier système formel (qui est un **S**ystème **H**ilbertien, selon la terminologie en vigueur). Nous noterons $\vdash_{\mathrm{SH}}$ la relation de déduction dans ce système formel.

7.4 Un second système formel

Nous examinons maintenant un second système formel dont les jugements sont les mots sur l' alphabet $\mathcal{C} \cup \mathcal{P} \cup \{\vdash\} \cup \{,\}$ de la forme

$$F_1,F_2,\ldots,F_n \vdash G \tag{7.1}$$

où $F_1, F_2, \ldots, F_n, G \in \mathcal{F}(\mathcal{C}, \mathcal{P})$.
Le cas $n = 0$ correspond à un mot de la forme $\vdash G$. On appelle *séquent* un tel jugement [1]. On notera $\mathcal{S}(\mathcal{C}, \mathcal{P})$ l'ensemble des séquents [2].

Axiome : toutes les instances du schéma d'axiome :

$$\Gamma, F, \Delta \vdash F$$

où Γ, Δ sont des suites finies (éventuellement vides) de formules et F est une formule.

Règles de déduction :

$$\textbf{introduction} \quad \frac{\Gamma, F, \Delta \quad \vdash G}{\Gamma, \Delta \quad \vdash F \to G}$$

$$\textbf{élimination} \quad \frac{\Gamma \quad \vdash F \qquad \Gamma \quad \vdash F \to G}{\Gamma \quad \vdash G}$$

$$\textbf{double négation} \quad \frac{\Gamma \quad \vdash (F \to \mathrm{ff}) \to \mathrm{ff}}{\Gamma \quad \vdash F}$$

où Γ, Δ sont des listes finies (éventuellement vides) de formules. On appelle *déduction naturelle* le système formel ainsi défini. Nous le noterons DN .
Notons $\mathcal{L}$ l' ensemble des listes finies de formules. Considérons l' application φ, de $\mathcal{L}$ dans l' ensemble des parties de $\mathcal{F}(\mathcal{C}, \mathcal{P})$:

$$\varphi(F_1, F_2, \ldots, F_n) = \{F_1, F_2, \ldots, F_n\}.$$

[1] la notion "standard" de séquent est plus large : il s' agit des mots de la forme $F_1,F_2,\ldots,F_n \vdash G_1,G_2,\ldots,G_m$ où $m, n \in \mathbb{N}$ et F_i, G_j sont des formules ; le système DN ne manipule que des séquents où $m = 1$

[2] au sens restrictif de la formule (8.3)

Théorème 7.4.1 (Simulation) *Soient* Γ *une liste finie de formules et* H *une formule. Le séquent* $\Gamma \vdash H$ *est prouvable dans* DN *, si et seulement si,* $\varphi(\Gamma) \vdash_{\mathrm{SH}} H$

La preuve que nous donnons de ce théorème fournit une méthode de *simulation* de DN par SH et inversement. Plus précisément : nous donnons deux algorithmes $A, \bar{A}$. L'algorithme A permet de calculer, à partir d'une preuve de $\Gamma \vdash F$ dans DN , une preuve (relative) de F à partir de $\varphi(\Gamma)$, dans SH . L'algorithme $\bar{A}$ permet de calculer, à partir d'une preuve (relative) de F à partir de $\varphi(\Gamma)$, dans SH , une preuve de $\Gamma \vdash F$ dans DN .
Preuve : 1- Montrons que si $\Gamma \vdash F$ est prouvable dans DN , alors $\varphi(\Gamma) \vdash_{\mathrm{SH}} F$.
On vérifie que, pour tous Γ, Δ, F, G
Axiome :
$\varphi(\Gamma, F, \Delta) \vdash_{\mathrm{SH}} F$
introduction :
si $\varphi(\Gamma, F, \Delta) \vdash_{\mathrm{SH}} G$ alors $\varphi(\Gamma, \Delta) \vdash_{\mathrm{SH}} F \rightarrow G$ (d' après le théorème 7.3.2).
élimination :
si $\Gamma \vdash_{\mathrm{SH}} F$ et $\varphi(\Gamma) \vdash_{\mathrm{SH}} F \rightarrow G$ alors $\varphi(\Gamma) \vdash_{\mathrm{SH}} G$ (en utilisant le MP).
double négation :
si $\varphi(\Gamma) \vdash_{\mathrm{SH}} (F \rightarrow \mathrm{ff}) \rightarrow \mathrm{ff}$ alors $\varphi(\Gamma) \vdash_{\mathrm{SH}} F$ (en utilisant l' axiome A3 de SH).
On a ainsi prouvé par induction sur la structure des preuves dy sytème DN , que, pour tout séquent $\Gamma \vdash F$ prouvable dans DN , on a aussi $\varphi(\Gamma) \vdash_{\mathrm{SH}} F$.
2- Montrons que, si $\vdash_{\mathrm{SH}} F$ alors le séquent $\vdash F$ est prouvable dans DN .
Axiome A1 :
1- $p, q \vdash p$ (Axiome)
2- $p \vdash q \rightarrow p$ (introduction,1)
3- $\vdash p \rightarrow q \rightarrow p$ (introduction,2)
Axiome A2 :
Notons $\Gamma = p, p \rightarrow q, p \rightarrow (q \rightarrow r)$
1- $\Gamma \vdash p$ (Axiome)
2- $\Gamma \vdash p \rightarrow q$ (Axiome)
3- $\Gamma \vdash q$ (elimination,1,2)
4- $\Gamma \vdash q \rightarrow r$ (Axiome)
5- $\Gamma \vdash r$ (elimination,3,4)
6- $p \rightarrow q, p \rightarrow (q \rightarrow r) \vdash p \rightarrow r$ (introduction 5)
7- $p \rightarrow (q \rightarrow r) \vdash (p \rightarrow q) \rightarrow (p \rightarrow r)$ (introduction 6)
8- $\vdash (p \rightarrow (q \rightarrow r)) \rightarrow [(p \rightarrow q) \rightarrow (p \rightarrow r)]$ (introduction 7)
Axiome A3 :

1- $(p \to \text{ff}) \to \text{ff} \vdash (p \to \text{ff}) \to \text{ff}$ (Axiome)
2- $(p \to \text{ff}) \to \text{ff} \vdash p$ (double négation)
3- $\vdash ((p \to \text{ff}) \to \text{ff}) \to p$
MP :
Supposons que $\vdash F$ et $\vdash F \to G$ sont prouvables dans DN .
Alors, en utilisant la règle d' élimination $\vdash F \to G$ est prouvable dans DN .
On a ainsi prouvé, par induction sur la structure des preuves de SH , la propriété annoncée.
3- Montrons que, si $\varphi(\Gamma) \vdash_{\text{SH}} F$ alors le séquent $\Gamma \vdash F$ est prouvable dans DN .
Soit $\Gamma = F_1, F_2, \ldots, F_n$ tel que

$$F_1, F_2, \ldots, F_n \vdash_{\text{SH}} F.$$

Alors , en utilisant n fois le théorème de déduction (th. 7.3.2) on obtient :
$F_2, \ldots, F_n \vdash_{\text{SH}} F_1 \to F$,
$\vdots$
$F_n \vdash_{\text{SH}} F_{n-1} \to (\ldots \to (F_1 \to F) \ldots)$,
$\vdash_{\text{SH}} F_n \to (F_{n-1} \to (\ldots \to (F_1 \to F) \ldots))$,
d'après l 'etape 2 de cette preuve, le séquent suivant est prouvable dans DN

$$\vdash F_n \to (F_{n-1} \to (\ldots \to (F_1 \to F) \ldots)) \tag{7.2}$$

On peut montrer que, pour tout séquent $\Delta \vdash H$ et toute formule G , si $\Delta \vdash H$ est prouvable dans DN alors $\Delta, G \vdash H$ est prouvable dans DN . Donc les séquents

$$F_n \vdash F_n \text{ et } F_n \vdash F_n \to (F_{n-1} \to (\ldots \to (F_1 \to F) \ldots)) \tag{7.3}$$

sont aussi prouvables dans DN . En utilisant la règle d'élimination de DN , on obtient une preuve du séquent

$$F_n \vdash F_{n-1} \to (\ldots \to (F_1 \to F) \ldots) \tag{7.4}$$

et en ré-itérant $n-1$ fois ce procédé on montre que le séquent

$$F_1, F_2, \ldots, F_n \vdash F \tag{7.5}$$

est prouvable dans DN . □

Corollaire 7.4.2 (Adéquation de DN **)** *Un séquent* $\Gamma \vdash F$ *est prouvable dans le système* DN *si et seulement si* $\varphi(\Gamma) \models F$.

Chapitre 8

Séries génératrices - Récurrences linéaires

8.1 Un exemple

On considère la suite $(u_n)_{n\geq 0}$ définie par :

$$\begin{cases} u_0 = u_1 = 1 \\ u_{n+2} - 4u_{n+1} + 4u_n = 0 \qquad (\forall\, n \geq 0) \qquad (\mathcal{E}_1) \end{cases}$$

On souhaite résoudre le PROBLÈME :
exprimer "directement" u_n en fonction de n.

Méthode : on pose $u(z) = \sum_{n\geq 0} u_n\, z^n \qquad (z \in \mathbb{C}, |z| < \rho)$

$(E1)$ Traduire $(\mathcal{E}_1)$ en une équation fonctionnelle sur $u(z)$.
$(E2)$ Résoudre l'équation fonctionnelle : on obtient $u(z)$ en fonction de z.
$(E3)$ Développer $u(z)$ en série entière : on obtient u_n en fonction de n.

$\underline{(E1)}$:

$$u_{n+2}\, z^{n+2} - 4u_{n+1}\, z^{n+2} + 4u_n\, z^{n+2} = 0 \qquad (\forall\, z, |z| < \rho)$$

(où ρ est le rayon de convergence de la série $\sum\, u_n\, z^n$)

$$(u_{n+2}\, z^{n+2}) \times 1 + (u_{n+1}\, z^{n+1}) \times (-4z) + (u_n\, z^n) \times (4z^2) = 0$$

$$(\text{pour } |z| < \rho,\ n \geq 0)$$

$$\underline{u(z) \times (1 - 4z + 4z^2) = (u_1 - 4u_0)z + u_0} \qquad (\text{pour } |z| < \rho)$$

$\underline{(E2)}$:

$$u(z) = \frac{u_0 + (u_1 - 4u_0)z}{1 - 4z + 4z^2}$$

$$u(z) = \frac{-3z + 1}{(1 - 2z)^2}$$

Décomposons $u(z)$ en éléments simples :

$$-3z + 1 = \frac{3}{2}(-2z + 1) - \frac{1}{2} \qquad (\text{division Euclidienne})$$

$$u(z) = \frac{3}{2} \times \frac{1}{1 - 2z} - \frac{1}{2} \times \frac{1}{(1 - 2z)^2}$$

Rappelons le développement en série entière :

$$(1 - v)^{-p} = \sum_{n \geq 0} \complement_{n+p-1}^{p-1}\, v^n \qquad (|v| < 1)$$

D'où

$$(1 - 2z)^{-1} = \sum_{n \geq 0} 2^n \times z^n \qquad (|z| < \frac{1}{2})$$

$$(1 - 2z)^{-2} = \sum_{n \geq 0} (n + 1) \times 2^n \times z^n \qquad (|z| < \frac{1}{2})$$

$$u(z) = \sum_{n\geq 0}[\frac{3}{2}\times 2^n - \frac{1}{2}(n+1)\times 2^n]z^n \qquad (\text{pour } |z| < \rho \text{ et } |z| < \frac{1}{2})$$

<u>$(E3)$:</u>

Supposons que $\rho \neq 0$.
Dans ce cas : $\forall\, n \geq 0$

$$\frac{u^{(n)}}{n!}(0) = u_n \qquad \text{et} \qquad \frac{u^{(n)}}{n!}(0) = \frac{3}{2}\times 2^n - \frac{1}{2}(n+1)\times 2^n$$

Donc :

$$\underline{\forall\, n \geq 0, \qquad u_n = \frac{3}{2}\times 2^n - \frac{1}{2}(n+1)\times 2^n} \qquad \mathcal{E}_2$$

Remarque 8.1.1 *pour achever la preuve de ($\mathcal{E}_2$), il faut :*
- soit démontrer que $\rho \neq 0$
- soit vérifier que le membre droit de ($\mathcal{E}_2$) est solution de ($\mathcal{E}_1$)
- soit ...

Un autre point de vue consiste à remplacer la manipulation de la fonction : $z \longmapsto \sum_{n=0}^{+\infty} u_n\, z^n$ par la manipulation de la "série formelle $\displaystyle\sum_{n=0}^{+\infty} u_n\, X^n$".

8.2 Séries formelles

Soit K un corps commutatif (nous nous placerons dans le cas $K = \mathbb{C}$ pour les exemples et les applications).

On définit l'ensemble des séries formelles à une indéterminée X, à coefficients dans K, noté $K[[X]]$, comme l'ensemble des applications de $\mathbb{N}$ dans K :

$$\text{si } a \in K[[X]], \qquad a = (a_n)_{n\geq 0}$$

On définit trois opérations : $\qquad$ pour $a = (a_n)_{n\geq 0}$, $b = (b_n)_{n\geq 0}$

somme : $a+b=c$ où

$$\forall\, n \in \mathbb{N},\ c_n = a_n + b_n$$

produit de convolution : $a.b=c$ où

$$\forall\, n \in \mathbb{N},\ c_n = \sum_{i=0}^{n} a_i\, b_{n-i}$$

produit par un scallaire : si $\lambda \in K$, $\lambda \otimes a = c$ où

$$\forall\, n \in \mathbb{N},\ c_n = \lambda \cdot a_n$$

Indéterminée : on définit l'indéterminée X par

$$X = (0, 1, 0, \ldots, 0, \ldots)$$

i.e.

$$X = (\delta_{1,n})_{n\geq 0}$$

$$\text{où} \quad \delta_{i,j} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases} \qquad \text{(symbole de Kronecker)}$$

Fait 8.2.1

$$\forall p \in \mathbb{N} - \{0\}, X^p = (\underbrace{0, 0, \ldots, 0}_{p \text{ termes nuls}}, 1, 0, \ldots) = (\delta_{p,n})_{n\geq 0}$$

On pose, par convention,

$$X^0 = (1, 0, \ldots, 0, \ldots) = (\delta_{0,n})_{n\geq 0}$$

Définition 8.2.2 *On appelle ordre d'une suite $a = (a_n)_{n\geq 0}$, $a \neq 0$, le nombre entier $\omega(a) = \min\{n \in \mathbb{N} \mid a_n \neq 0\}$ (on peut convenir que $\omega(a) = +\infty$, si $a = 0$).*

Définition 8.2.3 *Une famille $(S_i)_{i\in I}$ de séries formelles est dite sommable si et seulement si, pour tout $n \geq 0$, $\{i \in I, \omega(S_i) \leq n\}$ est fini.*

$$\textit{Dans ce cas, si} S_i = (s_{i,n})_{n\geq 0}, \quad \textit{on définit } T = \sum_{i\in I} S_i \qquad \textit{par}$$

$$T = (t_n)_{n\geq 0} \quad \textit{et} \quad t_n = \sum_{i\in I} s_{i,n} \quad (\forall\, n \geq 0).$$

Proposition 8.2.4 *Soit $a = (a_n)_{n\geq 0}$. La famille $(a_n\, X^n)_{n\geq 0}$ est sommable et $a = \sum_{n=0}^{+\infty} a_n X^n$.*

Proposition 8.2.5 *$(K[[X]], +, \cdot, \otimes)$ est une algèbre sur K possédant une unité (pour le produit de convolution)*

$$\mathbb{1} = (1, 0, \ldots, 0, \ldots)$$

Détaillons cette propriété

(1) $(K[[X]], +, .)$ est un anneau commutatif, unitaire, intègre, d'unité
$\mathbb{1} = (1, 0, \ldots, 0, \ldots)$.
(*rappel* : intègre signifie $S \cdot T = 0 \Rightarrow (S = 0 \text{ ou } T = 0)$)

(2) $(K[[X]], +, \otimes)$ est un K-espace vectoriel

(3) $\forall\, S, T \in K[[X]], \forall\, \lambda \in K$
$\lambda \otimes (S \cdot T) = (\lambda \otimes S) \cdot T = S \cdot (\lambda \otimes T)$.

<u>Substitution</u> d'une série dans une autre :

Soit $S = \sum_{n\geq 0} a_n\, X^n$ et $T \in K[[X]]$. On souhaite définir

$$S \circ T = \sum_{n\geq 0} a_n T^n$$

Définition 8.2.6 *Soit* $S = \sum_{n \geq 0} a_n X^n$ *et* $T \in K[[X]]$, *avec* $\omega(T) \geq 1$. *Alors* $(a_n T^n)_{n \geq 0}$ *est sommable et l'on définit*

$$S \circ T = \sum_{n=0}^{\infty} a_n T^n$$

Proposition 8.2.7
(1) Pour tous $S_1, S_2, T \in K[[X]]$ *tels que* $\omega(T) \geq 1$
on a :

$$\begin{aligned} (S_1 + S_2) \circ T &= (S_1 \circ T) + (S_2 \circ T) \\ (S_1 \cdot S_2) \circ T &= (S_1 \circ T) \cdot (S_2 \circ T) \\ 1\!\!1 \circ T &= 1\!\!1 \end{aligned}$$

(2) Pour tous $U, S, T \in K[[X]]$ *tels que* $\omega(S) \geq 1$, $\omega(T) \geq 1$,

$$(U \circ S) \circ T = U \circ (S \circ T)$$

Remarque 8.2.8 *Le point (1) revient à dire que* $S \mapsto S \circ T$ *(*T *fixé,* S *variable) est un homomorphisme d'anneau unitaire.*

Proposition 8.2.9 *Les éléments inversibles de* $K[[X]]$ *sont exactement les séries d'ordre* 0.

Preuve :
(1) Supposons que $S \cdot T = 1\!\!1$. Alors $s_0 \,.\, t_0 = 1$, donc $s_0 \neq 0$, $t_0 \neq 0$ et $\omega(S) = \omega(T) = 0$.

(2) Supposons que $\omega(S) = 0$

Cas particulier 1 : $S = 1 - X$
Posons $T = \sum_{n \geq 0} X^n$ et vérifions que $S \cdot T = 1\!\!1$.
Posons $S \cdot T = U$. On obtient :
$u_0 = s_0 \,.\, t_0 = 1$
$u_n = \sum_{i=0}^{n} s_i \, t_{n-i} = s_0 \, t_n + s_1 \, t_{n-1} = t_n - t_{n-1} = 0 \quad (n \geq 0)$

Donc $U = \mathbb{1}$.

Cas particulier 2 : $S = \mathbb{1} - U$ avec $\omega(U) \geq 1$.

Posons $S' = \sum_{n\geq 0} U^n$.

$$\begin{aligned} S \cdot S' &= [(\mathbb{1} - X) \circ U] \cdot [T \circ U] \\ &= [(\mathbb{1} - X) \cdot T] \circ U \\ &= \mathbb{1} \circ U && \text{(d'après la proposition 8.2.7)} \\ &= \mathbb{1} && \text{(d'après le cas 1)} \end{aligned}$$

Cas général : $S = s_0 + V$ où $s_0 \neq 0 \quad \omega(V) \geq 1$.

$S = s_0 \otimes (1 - U)$ où $U = -\frac{1}{s_0} \otimes V$ Soit $S' = \frac{1}{s_0} \otimes \sum_{n\geq 0} U^n$

$$\begin{aligned} S \cdot S' &= [s_0 \otimes (1 - U)] \cdot [\frac{1}{s_0} \otimes \sum_{n\geq 0} U^n] \\ &= (s_0 \cdot \frac{1}{s_0}) \otimes ([1 - U] \cdot [\sum_{n\geq 0} U^n]) && \text{(car algèbre sur } K \text{)} \\ &= 1 \times \mathbb{1} && \text{(d'après le cas 2)} \\ &= \mathbb{1} \end{aligned}$$

□

Exemple 8.2.10

$$S = (1 - 2X)^2 \quad \omega(S) = 0.$$

Donc, S est inversible : $\frac{1}{(1-2X)^2}$ est une série formelle bien définie.

Formule 8.2.11 *Pour tout entier $p \geq 1$, la série $S = (1-X)^p$ est inversible et son inverse est donné par :*

$$\frac{1}{S} = \sum_{n\geq 0} C_{n+p-1}^{p-1} X^n$$

8.3 Récurrences linéaires

8.3.1 Récurrences linéaires à coefficients constants

Considérons les suites $(u_n)_{n\geq 0}$ de nombres complexes vérifiant :

$$\forall\, n \geq 0\,, \quad u_{n+h} = a_{h-1}\, u_{n+h-1} + a_{h-2}\, u_{n+h-2} + \ldots + a_0\, u_n \quad (\mathcal{E})$$

avec $h \geq 1,\ a_0 \neq 0$
$(\mathcal{E})$ est une relation de récurrence linéaire à coefficients constants, d'ordre h.
Le polynôme caractéristique de la récurrence est :

$$G(X) = X^h - a_{h-1}\, X^{h-1} - a_{h-2}\, X^{h-2} - \ldots - a_{h-i}\, X^{h-i} - \ldots - a_0$$

On note :

$$B(X) = 1 - a_{h-1}\, X - a_{h-2}\, X^2 - \ldots - a_{h-i}\, X^i - \ldots - a_0\, X^h$$

(B est le polynôme réciproque de G).
Posons :

$$u(X) = \sum_{n=0}^{+\infty} u_n\, X^n$$
$$A(X) = B(X)\,.\,u(X)$$

Notons $[X^m]A(X)$ le coefficient de X^m dans $A(X)$.
Soit $m \geq h$:

$$\begin{aligned}
[X^m]A(X) &= \sum_{i=0}^{m} b_i\, u_{m-i} \\
&= \sum_{i=0}^{h} b_i\, u_{m-i} \\
&= u_m - a_{h-1}\, u_{m-1} - a_{h-2}\, u_{m-2} - \ldots - a_0\, u_{m-h} \\
&= u_{n+h} - a_{h-1}\, u_{n+h-1} - a_{h-2}\, u_{n+h-2} - \ldots - a_0\, u_n \quad \text{(pour } n = m-h \geq 0) \\
&= 0 \quad \text{(par } \mathcal{E})
\end{aligned}$$

Donc A est un polynôme et $d^\circ(A) \leq h-1$.

$$\boxed{u(X) = \frac{A(X)}{B(X)}}$$

Comme $\mathbb{C}$ est algébriquement clos :

$$\begin{aligned} G(X) &= \prod_{i=1}^{r}(X-\omega_i)^{n_i} \qquad \text{avec } \sum_{i=1}^{r} = h,\ \omega_i \in \mathbb{C} \\ B(X) &= \prod_{i=1}^{r}(1-\omega_i\,X)^{n_i} \end{aligned}$$

Comme $d^\circ(A) < d^\circ(B)$, la décomposition en éléments simples de $u(X)$ est de la forme :

$$u(X) = \sum_{i=1}^{r}\sum_{j=1}^{n_i} \frac{\beta_{i,j}}{(1-\omega_i\,X)^j}$$

$$(1-\omega_i\,X)^{-j} = \sum_{n=0}^{+\infty} \mathrm{C}_{n+j-1}^{j-1}\,\omega_i^n\,X^n$$

$$u(X) = \sum_{i=1}^{r}\sum_{j=1}^{n_i}\sum_{n=0}^{+\infty} \beta_{i,j}\ \mathrm{C}_{n+j-1}^{j-1}\,\omega_i^n$$

D'où

$$u_n = \sum_{i=1}^{r}\sum_{j=1}^{n_i} \beta_{i,j}\ \mathrm{C}_{n+j-1}^{j-1}\,\omega_i^n$$

Remarquons que, pour j fixé, $n \mapsto \mathrm{C}_{n+j-1}^{j-1}$ est une fonction polynômiale de degré $(j-1)$ de la variable n.

$$\boxed{u_n = \sum_{i=1}^{r} P_i(n)\,\omega_i^n}$$

où P_i est un polynôme de degré $d^\circ(P_i) \leq n_i - 1$.
Cette forme de u_n s'appelle un "polynôme exponentiel".

Proposition 8.3.1 *Soient $a_0, a_1, \ldots, a_h \in \mathbb{C}, a_0 \neq 0$ et $(u_n)_{n\geq 0}$ une suite complexe. Les conditions suivantes sont équivalentes.*
(1) $\forall\, n \geq 0 \quad u_{n+h} = a_{h-1}\,u_{n+h-1} + a_{h-2}u_{n+h-2} + \ldots + a_0\,u_n$

(2) $u(X) = \dfrac{A(X)}{B(X)}$ *où* $\left\{ \begin{array}{lcl} B(X) &=& 1 - a_{h-1}\,X - a_{h-2}\,X^2 - \ldots - a_0\,X^h \\ d^\circ(A) &\leq& h-1 \end{array} \right.$

(3) $\forall\, n \geq 0,\ u_n = \displaystyle\sum_{i=1}^{r} P_i(n)\,\omega_i^n$ *où* $\left\{\begin{array}{rcl} B(X) & = & \displaystyle\prod_{i=1}^{r}(1-\omega_i\,X)^{n_i} \\ P_i & \in & \mathbb{C}\,[X] \\ d^\circ(P_i) & \leq & n_i - 1 \end{array}\right.$

Preuve : (1) $\Rightarrow$ (2) $\Rightarrow$ (3) voir ci-dessus.

(2) $\Rightarrow$ (1) : comme $d^\circ(u\,.\,B) \leq h-1$,

$\forall\, m \geq h,$	$[X^m]\,(B\,.\,u) = 0$
i.e.	$u_m - a_{h-1}\,u_{m-1} - \ldots - a_0\,u_{m-h} = 0$
d'où	$u_{n+h} - a_{h-1}\,u_{n+h-1} - \ldots - a_0\,u_n = 0 \quad (\forall\, n \geq 0)$
donc	(1) est vraie.

(3) $\Rightarrow$ (2) : comme $d^\circ(\subset_{X+j-1}^{j-1}) = j-1$,
$(\subset_{X+j-1}^{j-1})_{1\leq j\leq n_i}$ forment une base de l'espace vectoriel $\mathbb{C}_{n_i}\,[X]$ (l'espace des polynômes de degré $\leq n_i - 1$).
Donc, $\forall\, i \in [1,r]$, $\exists\, \beta_{i,1},\ldots,\beta_{i,n_i}$ tels que

$$P_i(n) = \sum_{j=1}^{n_i} \beta_{i,j}\ \subset_{n+j-1}^{j-1} \qquad (4)$$

$$\begin{array}{rcll}
u(X) & = & \displaystyle\sum_{n=0}^{+\infty}\sum_{i=1}^{r} P_i(n)\,\omega_i^n\,X^n & \text{(par (3))} \\
& = & \displaystyle\sum_{n=0}^{+\infty}\sum_{i=1}^{r}\sum_{j=1}^{n_i} \beta_{i,j}\ \subset_{n+j-1}^{j-1}\,\omega_i^n\,X^n & \text{(par (4))} \\
& = & \displaystyle\sum_{i=1}^{r}\sum_{j=1}^{n_i}(\beta_{i,j}\sum_{n=0}^{+\infty}\subset_{n+j-1}^{j-1}\,\omega_i^n\,X^n) & \text{car même coefficient de } X^n \\
& = & \displaystyle\sum_{i=1}^{r}\sum_{j=1}^{n_i}\frac{\beta_{i,j}}{(1-\omega_i\,X)^j} & \\
& = & \dfrac{A(X)}{B(X)} & \text{avec } d^\circ(A) \leq h-1
\end{array}$$

□

8.3.2 Récurrences linéaires, à coefficients constants avec second membre

Considérons les suites $(u_n)_{n\geq 0}$ de nombres complexes vérifiant :

$$\forall\, n \geq 0, \qquad u_{n+h} = (a_{h-1}\, u_{n+h-1} + a_{h-2}\, u_{n+h-2} + \ldots + a_0\, u_n) + v_n \qquad (\mathcal{E})$$

avec $a_0 \neq 0$.
$(\mathcal{E})$ est une relation de récurrence linéaire, à coefficients constants, d'ordre h, de second membre v_n. Posons

$$v(X) = \sum_{n=0}^{+\infty} v_n\, X^n \qquad u(X) = \sum_{n=0}^{+\infty} u_n\, X^n$$

Comme dans la partie 8.3.1, l'équation $(\mathcal{E})$ peut s'interpréter par :

$$\begin{array}{lll} \forall\, m \geq h, & [X^m] & B(X)\,.\,u(X) = v_{m-h} \\ \text{D'où} & & B(X)\,.\,u(X) = A(X) + X^h\,.\,v(X) \\ \text{avec} & & A(X) \in \mathbb{C}\,[X]\,,\ d^\circ(A) \leq h-1 \end{array}$$

$$\text{d'où} \qquad \boxed{u(X) = \frac{A(X) + X^h\,.\,v(X)}{B(X)}}$$

On en déduit que $(u_n)_{n\geq 0}$ est solution de $(\mathcal{E})$ si et seulement si

$$u_n = \sum_{i=1}^{r} P_i(n)\,\omega_i^n + w_n$$

avec $d^\circ(P_i) \leq n_i - 1$, $(w_n)_{n\geq 0}$ solution particulière de $(\mathcal{E})$.

<u>Cas où $v(X)$ est rationnelle :</u>

$$v(X) = \frac{P(X)}{Q(X)} \qquad d^\circ(P) < d^\circ(Q)$$

alors,

$$u(X) = \frac{A(X)\,Q(X) + X^h\,P(X)}{B(X)\,Q(X)}$$

où

$$d^\circ(AQ+X^h P) \leq \max\{d^\circ(A)+d^\circ(Q), h+d^\circ(P)\} \leq h-1+d^\circ(Q) = d^\circ(BQ)-1$$

Donc

$$u_n = \sum_{j=1}^{q} Q_j(n)\ \theta_j^n$$

où

$$B(X)\ .\ Q(X) = \prod_{j=1}^{q} (1 - \theta_j\ X)^{mj}$$

Exemple 8.3.2

$$\begin{cases} t_{n+1} - 2t_n &= n + 2^n \\ t_0 &= 0 \end{cases}$$

La proposition 8.3.1 nous garantit que la série $v(X) = \sum_{n \geq 0} v_n X^n$ est une fraction rationnelle $\dfrac{P(X)}{Q(X)}$. Calculons les polynômes P et Q.

$$\begin{aligned}
\frac{P(X)}{Q(X)} &= \sum_{n \geq 0} (n + 2^n)\ X^n \\
&= \sum_{n \geq 0} (n+1)\ X^n - \sum_{n \geq 0} X^n + \sum_{n \geq 0} 2^n\ X^n \\
&= \frac{1}{(1-X)^2} - \frac{1}{(1-X)} + \frac{1}{(1-2X)} \\
&= \frac{(1-2X) - (1-X)\ (1-2X) + (1-X)^2}{(1-X)^2\ (1-2X)} \\
&= \frac{1 - 2X - 1 + 2X + X - 2X^2 + 1 - 2X + X^2}{(1-X)^2\ (1-2X)} \\
&= \frac{1 - X - X^2}{(1-X)^2\ (1-2X)} \\
&= \frac{1 - X - X^2}{(1 - 2X + X^2)\ (1-2X)} \\
&= \frac{1 - X - X^2}{1 - 4X + 5X^2 - 2X^3}
\end{aligned}$$

Solution 1 :

Exprimons maintenant u_n *en fonction de* n *en suivant pas à pas la méthode (et les notations) du paragraphe 8.3.2.*

$G(X) = X - 2$

$B(X) = 1 - 2X$

$A(X) = 0$

$P(X) = 1 - X - X^2$

$Q(X) = (1 - X)^2\,(1 - 2X)$

$$t_1(X) = \frac{X\,(1 - X - X^2)}{(1 - X)^2\,(1 - 2X)^2}$$

Bezout :

$$t_1 = \frac{X - X^2 - X^3}{(1 - X)^2\,(1 - 2X)^2}$$

$((1 - 2X) - 2(1 - X))^3 = -1$

$(2(1 - X) - (1 - 2X))^3 = 1$

$8(1 - X)^3 - 3 \times 4(1 - X)^2\,(1 - 2X) + 3 \times 2(1 - X)\,(1 - 2X)^2 - (1 - 2X)^3 = 1$

$(1 - X)^2\,[8(1 - X) - 12(1 - 2X)] + (1 - 2X)^2\,[6(1 - X) - (1 - 2X)] = 1$

$(1 - X)^2\,[-4 + 16X] + (1 - 2X)^2\,[5 - 4X] = 1$

$$t_1(X) = \frac{(5 - 4X)\,(X - X^2 - X^3)}{(1 - X)^2} - \frac{(4 - 16X)\,(X - X^2 - X^3)}{(1 - 2X)^2}$$

$$t_1(X) = \frac{5X - 9X^2 - X^3 + 4X^4}{(1 - X)^2} - \frac{4X - 20X^2 + 12X^3 + 16X^4}{(1 - 2X)^2}$$

$$\begin{array}{r|l} 4X^4 - X^3 - 9X^2 + 5X & X^2 - 2X + 1 \\ \cline{2-2} 7X^3 - 13X^2 + 5X & 4X^2 + 7X + 1 \\ X^2 - 2X & \\ -1 & \end{array}$$

$$\begin{array}{r|l} 16X^4 + 12X^3 - 20X^2 + 4X & 4X^2 - 4X + 1 \\ \cline{2-2} 28X^3 - 24X^2 + 4X & 4X^2 + 7X + 1 \\ 4X^2 - 3X & \\ X - 1 & \end{array}$$

$$t_1(X) = -\frac{1}{(1-X)^2} + \frac{-X+1}{(1-2X)^2}$$

$$\boxed{t_1(X) = -\frac{1}{(1-X)^2} + \frac{1}{2}\,\frac{(1-2X)^1}{(1-2X)^2} + \frac{1}{2}\,\frac{1}{(1-2X)^2}}$$

Vérification :

$$\begin{aligned} N(X) &= -(1-2X)^2 + (1-X)^3 \\ &= -1 + 4X - 4X^2 + 1 - 3X + 3X^2 - X^3 \\ &= X - X^2 - X^3 \qquad \rightarrow \textit{correct} \end{aligned}$$

Développement en série :

$$t_n = -\binom{n+1}{1} + \frac{1}{2}\,2^n + \frac{1}{2}\binom{n+1}{1}\,2^n$$

$$\boxed{t_n = -(n+1) + (n+2)\,2^{n-1}}$$

$t_0 = 0 \qquad t_1 = 1 \qquad t_2 = -3 + 8 = 5 \qquad t_3 = -4 + 5 \times 4 = 16 \qquad \rightarrow\ OK$

Solution2 (variante) :

Relation de récurrence vérifiée par $v_n = (n + 2^n)$:

$$v(X) \times (1 - 4X + 5X^2 - 2X^3) = 1 - X - X^2$$

$$v_{n+3} - 4v_{n+2} + 5v_{n+1} - 2v_n = 0 \qquad \textit{(coeff de } X^{n+3}\textit{)}$$

Relation de récurrence vérifiée par t_n :

$$t_{n+4} - 2t_{n+3} = 4v_{n+2} - 5v_{n+1} + 2v_n$$

$$t_{n+4} - 2t_{n+3} = 4(t_{n+3} - 2t_{n+2}) - 5(t_{n+2} - 2t_{n+1}) + 2(t_{n+1} - 2t_n)$$

$$\boxed{t_{n+4} - 6t_{n+3} + 13t_{n+2} - 12t_{n+1} + 4t_n = 0}$$

$$\begin{aligned} B'(X) &= 1 - 6X + 13X^2 - 12X^3 + 4X^4 \\ &= (1-2X)\,(1 - 4X + 5X^2 - 2X^3) \\ &= (1-2X)\,(1-X)\,(1 - 3X + 2X^2) \\ &= (1-2X)^2\,(1-X)^2 \end{aligned}$$

$t_0 = 0,\ t_1 = 1,\ t_2 = 5,\ t_3 = 16$

$$\begin{aligned} A'(X) &= t(X)\,B'(X) \\ &= (1X + 5X^2 + 16X^3 + \ldots)\,(1 - 6X + 13X^2 - 12X^3 + \ldots) \\ &= 1X - X^2 + \underbrace{\ldots\ldots\ldots}_{\textit{ces termes s'annulent}} - X^3 \end{aligned}$$

$t_2(X) = \dfrac{X - X^2 - X^3}{(1-2X)^2\,(1-X)^2}$.

On constate que cette fraction rationnelle est bien égale à celle qui avait été calculée par la méthode 1.

On termine, comme dans la solution1, par la décomposition en éléments simples de t_2 , puis le "développement en série" de t_2 (i.e. l'application de la formule 8.2.11 à chaque élément simple).

Bibliographie

[AG93] A. Arnold and I. Guessarian. *Mathématiques pour l'informatique.* MASSON, 1993.

[Aut94] J.M. Autebert. *Théorie des langages et des automates.* MASSON, 1994.

[BBC94] D. Beauquier, J. Berstel, and P. Chrétienne. *Eléments d'algorithmique.* MASSON, 1994.

[Car61] H. Cartan. *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes.* HERMANN, 1961.

[Hue86] G. Huet. *Inititation à la Logique Mathématique.* Notes de Cours du DEA d'Informatique, université Paris 9, 1986.

[Jac85] N. Jacobson. *Basic Algebra I.* FREEMAN, 1985.

[Lal90] R. Lalement. *Logique, réduction, résolution.* MASSON, 1990.

[Xuo92] N.H. Xuong. *Mathématiques discrètes et Informatique.* MASSON, 1992.

Annexe 1 : Problèmes

Examen de Mai 2001

Exercice

On considère l'automate fini $\mathcal{A} =< X, Q, D, A, \delta >$ où $X = \{a, b\}, Q = \{0, 1, 2, 3, 4\}$, $D = \{0\}$,$A = \{0\}$ et δ est donnée par la table suivante :

$x \setminus q$	0	1	2	3	4
a	1	4	2,3	4	4
b	4	2	4	0	4

On remarquera que $\mathcal{A}$ n'est pas déterministe ($\delta(2, a)$ contient 2 éléments).
1-Calculer l'automate déterministe complet minimal qui reconnaît le langage $L = \mathrm{L}_{\mathcal{A}}$.
2-On considère les langages rationnels suivants :

$$R_1 = ab(ab)^*, R_2 = ba(ba)^*, R_3 = aba(aba)^*.$$

Pour chaque valeur de l'entier $i \in [1, 3]$, déterminer si

$$L \cap R_i = \emptyset ?, \quad L \cap R_i \text{ a un nombre fini d'éléments ?}$$

3- On considère l'automate fini $\mathcal{A}' =< X, Q', D', A', \delta' >$ où $X = \{a, b\}, Q' = \{0, 1, 2, 3, 4, 5, 6\}$, $D' = \{0\}$,$A' = \{0\}$ et δ' est donnée par la table suivante :

$x \setminus q$	0	1	2	3	4	5	6
a	1	6	3	3	5	5	6
b	6	2	6	4	6	0	6

Vérifier que cette automate est déterministe, complet. Est-il minimal ?
4- Calculer l'automate fini déterministe minimal reconnaissant le langage $\mathrm{L}_{\mathcal{A}} \cap \mathrm{L}_{\mathcal{A}'}$.
5-Pour chacune des affirmations qui suivent, dire si elle est juste ou fausse (en justifiant la réponse) :
"$\mathrm{L}_{\mathcal{A}} = \mathrm{L}_{\mathcal{A}'}$", "$\mathrm{L}_{\mathcal{A}} \subseteq \mathrm{L}_{\mathcal{A}'}$", "$\mathrm{L}_{\mathcal{A}} \supseteq \mathrm{L}_{\mathcal{A}'}$", "$\mathrm{L}_{\mathcal{A}} \cap \mathrm{L}_{\mathcal{A}'} = \emptyset$", "$\mathrm{L}_{\mathcal{A}} \cap \mathrm{L}_{\mathcal{A}'} \subseteq R_1$".
6-Posons $M = \{u \in \{a, b\}^*, |u|_a = |u|_b\}$. Autrement dit, M est l'ensemble des mots sur $\{a, b\}$ qui ont le même nombre d'occurrences de la lettre a et de la lettre b.
M est-il rationnel ? $L \cap M$ est-il rationnel ?

Exercice

On considère l'ensemble de connecteurs $\mathcal{C} = \{\rightarrow, ff\}$ et l'ensemble de variables propositionnelles $\mathcal{P} = \{p, q, r, \ldots\}$. On considère les formules :

$$F_1 = (p \rightarrow q) \rightarrow p; \quad F_2 = (q \rightarrow p) \rightarrow p;$$

$$F_3 = q \rightarrow (p \rightarrow q); \quad F_4 = [p \rightarrow (q \rightarrow r)] \rightarrow [(p \rightarrow q) \rightarrow (p \rightarrow r)]$$

$$F_5 = [(p \rightarrow ff) \rightarrow ff] \rightarrow [p \rightarrow ff].$$

Pour chacune d'elles :
1- dire si elle est *satisfaisable* ? (et dans l'affirmative, donner une interprétation qui rend vraie la formule)
2- dire si c'est une *tautologie* (en justifiant la réponse).

Exercice

Soit $(u_n)_{n\geq 0}$ la suite d'entiers définie par :

$$u_n = u_{n-1} + 2u_{n-2} \ \ (n \geq 2) \text{ et } u_0 = 1, u_1 = 2.$$

1- On note $u(X) = \sum_{n=0}^{\infty} u_n X^n$. Montrer que

$$u(X) = \frac{1}{1-2X}$$

2- En déduire une expression de u_n en fonction de n.
3- Soit $(v_n)_{n\geq 0}$ la suite d'entiers définie par :

$$v_n = v_{n-1} + 2v_{n-2} + (-1)^n \ \ (n \geq 2) \text{ et } v_0 = v_1 = 1.$$

On note $v(X) = \sum_{n=0}^{\infty} v_n X^n$. Donner une expression de $v(X)$ en fonction de X.
(On remarquera que $\sum_{n=0}^{\infty} (-1)^n X^n = \frac{1}{1+X}$).
4- En déduire une expression de v_n en fonction de n.

Problème

On considère $E = \{0, 1, 2\}$, et $\mathcal{F}_k$ $(k \geq 1)$ l'ensemble des applications de E^k dans E ($\mathcal{F}_k$ est l'ensemble des applications à k arguments prenant leurs valeurs dans E et à valeurs dans E). On note $\mathcal{F}_{\leq 2} = \mathcal{F}_1 \cup \mathcal{F}_2$. On considère les deux applications particulières $\lambda, \mu \in \mathcal{F}_2$, données par leur table de valeurs :

$$\lambda : \begin{array}{c||c|c|c|} x \setminus y & 0 & 1 & 2 \\ \hline 0 & 1 & 0 & 2 \\ 1 & 0 & 0 & 1 \\ 2 & 1 & 0 & 2 \end{array} \qquad \mu : \begin{array}{c||c|c|c|} x \setminus y & 0 & 1 & 2 \\ \hline 0 & 1 & 0 & 0 \\ 1 & 0 & 2 & 0 \\ 2 & 0 & 0 & 0 \end{array}$$

On note P_1, P_2 les éléments de $\mathcal{F}_2$ définis par :

$$P_1(x, y) = x; \ \ P_2(x, y) = y.$$

1- Soit $\mathcal{L}$ le sous-ensemble de $\mathcal{F}_{\leq 2}$ défini inductivement par :

(0) $P_1, P_2 \in \mathcal{L}$

(1) $\lambda \in \mathcal{L}$

(2) si $G, H \in \mathcal{L} \cap \mathcal{F}_2$ et $F \in \mathcal{L} \cap \mathcal{F}_2$ alors la fonction $(x,y) \mapsto F(G(x,y), H(x,y))$ appartient à $\mathcal{L}$

(3) si $G \in \mathcal{L} \cap \mathcal{F}_2$ et $F \in \mathcal{L} \cap \mathcal{F}_1$ alors la fonction $(x,y) \mapsto F(G(x,y))$ appartient à $\mathcal{L}$

(4) si $G \in \mathcal{L} \cap \mathcal{F}_2$ alors la fonction $x \mapsto G(x,x)$ appartient à $\mathcal{L}$

Montrer, par induction structurelle, que, pour toute fonction $F \in \mathcal{L}$:

$$\text{si } F \in \mathcal{F}_1, \forall x \in \{0,1\}, F(x) \in \{0,1\} \text{ et } \text{ si } F \in \mathcal{F}_2, \forall x \in \{0,1\}, \forall y \in \{0,1\}, F(x,y) \in \{0,1\}.$$

2-En déduire que $\mathcal{L} \neq \mathcal{F}_{\leq 2}$.
3- Soit $\mathcal{M}$ le sous-ensemble de $\mathcal{F}_{\leq 2}$ défini inductivement par :

(0) $P_1, P_2 \in \mathcal{M}$

(1) $\mu \in \mathcal{M}$

(2) si $G, H \in \mathcal{M} \cap \mathcal{F}_2$ et $F \in \mathcal{M} \cap \mathcal{F}_2$ alors la fonction $(x,y) \mapsto F(G(x,y), H(x,y))$ appartient à $\mathcal{M}$

(3) si $G \in \mathcal{M} \cap \mathcal{F}_2$ et $F \in \mathcal{M} \cap \mathcal{F}_1$ alors la fonction $(x,y) \mapsto F(G(x,y))$ appartient à $\mathcal{M}$

(4) si $G \in \mathcal{M} \cap \mathcal{F}_2$ alors la fonction $x \mapsto G(x,x)$ appartient à $\mathcal{M}$.

Montrer que les applications $\delta_0, \delta_1, \delta_2$ suivantes sont dans $\mathcal{M}$:

$$\delta_0(x) = x; \quad \delta_1(x) = x+1(\text{ si } x < 2), \delta_1(2) = 0; \quad \delta_2(0) = 2, \delta_2(1) = 0, \delta_2(2) = 1.$$

4- On pose $\mathrm{Z}(x) = 0(\text{ pour tout } x \leq 2)$. Vérifier que

$$\mathrm{Z}(x) = \mu(x, \delta_1(x)).$$

En déduire que $\mathrm{Z} \in \mathcal{M}$.
5- On pose $\mathrm{Not}(x) = 1(\text{ si } x = 0), \mathrm{Not}(x) = 0(\text{ si } x \neq 0)$. Montrer que $\mathrm{Not} \in \mathcal{M}$.
6- Déterminer des applications $\mathrm{Xor}, \mathrm{And} \in \mathcal{M}$ telles que :

$$\mathrm{Xor}(0,0) = \mathrm{Xor}(1,1) = 0 \text{ et } \mathrm{Xor}(0,1) = \mathrm{Xor}(1,0) = 1,$$

$$\mathrm{And}(0,0) = \mathrm{And}(1,0) = \mathrm{And}(0,1) = 0 \text{ et } \mathrm{And}(1,1) = 1.$$

7- Pour tout $i \in E$ on pose

$$\mathrm{Test}_i(x) = 1 \text{ si } x = i, \mathrm{Test}_i(x) = 0 \text{ si } x \neq i.$$

Montrer que les applications Test_i $(i \in E)$ sont dans $\mathcal{M}$.
8-Pour tout $(i,j) \in E \times E$ on pose

$$\text{Test}_{i,j}(x,y) = 1 \text{ si } (x,y) = (i,j), \text{Test}_{i,j}(x,y) = 0 \text{ si } (x,y) \neq (i,j).$$

Montrer que les applications $\text{Test}_{i,j}$ $((i,j) \in E \times E)$ sont dans $\mathcal{M}$.
9-Soit $F : E \times E \to \{0,1\}$. Montrer, par récurrence sur l'entier $\text{Card}(\{(x,y) \in E \times E | F(x,y) = 1\})$ que $F \in \mathcal{M}$.
10- Soit $G : E \times E \to E$. On pose :

$$G_0(x,y) = G(x,y) - 1 \text{ si } G(x,y) \geq 1, G_0(x,y) = 0 \text{ si } G(x,y) = 0;$$

$$G_1(x,y) = G(x,y) - 1 \text{ si } G(x,y) \geq 1, G_1(x,y) = 1 \text{ si } G(x,y) = 0.$$

En appliquant le résultat de la question 9 à G_0, G_1, montrer que $G \in \mathcal{M}$.
11-Que pouvons nous en conclure sur l'ensemble $\mathcal{M}$?

Corrigé de l'examen de Mai 2001

Exercice

1- On retire de $\mathcal{A}$ l' état "poubelle" 4. Puis on déterminise l'automate ainsi obtenu. On obtient :

$x \setminus q$	0	1	2	2,3	$\emptyset$
a	1	$\emptyset$	2,3	2,3	$\emptyset$
b	$\emptyset$	2	$\emptyset$	0	$\emptyset$

En renommant les états de cet automate, on obtient l'automate $\bar{\mathcal{A}} =< X, \bar{Q}, \bar{D}, \bar{A}, \bar{\delta} >$, dont la table des transitions est :

$x \setminus q$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
a	$\bar{1}$	$\bar{4}$	$\bar{3}$	$\bar{3}$	$\bar{4}$
b	$\bar{4}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{4}$

et où $\bar{D} = \bar{A} = \{\bar{0}\}$. Cet automate est déterministe et complet. Calculons la partition de son ensemble d'états induite par l'équivalence de Nérode.
$\pi_0 = \{\{\bar{0}\}, \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}\}$
$\pi_1 = \{\{\bar{0}\}, \{\bar{1}, \bar{2}, \bar{4}\}, \{\bar{3}\}\}$
$\pi_2 = \{\{\bar{0}\}, \{\bar{1}, \bar{4}\}, \{\bar{2}\}, \{\bar{3}\}\}$
$\pi_3 = \{\{\bar{0}\}, \{\bar{1}\}, \{\bar{2}\}, \{\bar{3}\}, \{\bar{4}\}\}$.
Donc π, la partition en classes pour l'équivalence de Nérode, est la partition en singletons. Donc $\bar{\mathcal{A}}$ est minimal.
2-$\forall n \geq 0, \bar{\delta}(\bar{0}, (ab)^{2n}) = \bar{0} \in \bar{A}, \bar{\delta}(\bar{0}, (ab)^{2n+1}) = \bar{2} \notin \bar{A}$.
Donc $L \cap R_1 = \{(ab)^{2n}, n \geq 1\}$ est non-vide et a un nombre infini d'éléments.
$\forall n \geq 1, \bar{\delta}(\bar{0}, (ba)^n) = \bar{4} \notin \bar{A}$, donc $L \cap R_2 = \emptyset$.
$\bar{\delta}(\bar{0}, aba) = \bar{3}, \bar{\delta}(\bar{0}, abaaba) = \bar{1}$, $\forall n \geq 3, \bar{\delta}(\bar{0}, (aba)^n) = \bar{4} \notin \bar{A}$,
donc $L \cap R_3 = \emptyset$.
3- Comme dans la question 1, le calcul des partitions de Q' pour les équivalences successives $\equiv_i$ $(0 \leq i \leq 5)$ donne :

$$\Pi_5 = \{\{0\}, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}\}$$

4- Supprimons les états inaccessibles des automates $\bar{\mathcal{A}}$,$\mathcal{A}'$, puis formons leur produit direct. On obtient la table de transitions :

$x \setminus q$	$\bar{0},0$	$\bar{1},1$	$\bar{2},2$	$\bar{3},3$	$\bar{0},4$	$\bar{1},5$	$\bar{2},0$	$\bar{3},1$	$\bar{0},2$	$\bar{1},3$	$\bar{2},4$	$\bar{3},5$
a	$\bar{1},1$	$-$	$\bar{3},3$	$\bar{3},3$	$\bar{1},5$	$-$	$\bar{3},1$	$-$	$\bar{1},3$	$-$	$\bar{3},5$	$\bar{3},5$
b	$-$	$\bar{2},2$	$-$	$\bar{0},4$	$-$	$\bar{2},0$	$-$	$\bar{0},2$	$-$	$\bar{2},4$	$-$	$\bar{0},0$

Après ajout d'un état "poubelle" P et renommage des autres états,on obtient :

$x \setminus q$	0	1	2	3	4	5	6	7	8	9	10	11	P
a	1	P	3	3	5	P	7	P	9	P	11	11	P
b	P	2	P	4	P	6	P	8	P	10	P	0	P

où l'état de départ est 0 et l' état d'arrivée est 0.
On vérifie que :
$\forall i \in \{0, 1, 2, \ldots, 11\}, i \not\equiv P$: en effet aucun mot n'est reconnu à partir de l' état P alors qu'au moins un mot est reconnu à partir de i ;
$\forall i, j \in \{0, 1, 2, \ldots 11\}, i \neq j \Rightarrow i \not\equiv j$:
en effet la longueur minimale d'un mot reconnu à partir de i (resp. j) est $12 - i$ (resp. $12 - j$). Donc l'équivalence de Nérode de cet automate est réduite à l'égalité. C'est donc l'automate minimal reconnaissant $\mathrm{L}_{\mathcal{A}} \cap \mathrm{L}_{\mathcal{A}'}$.
5-
5.1 Par unicité de l'automate minimal (à isomorphisme près), on conclut de la question 4 que $\mathrm{L}_{\bar{\mathcal{A}}} \cap \mathrm{L}_{\mathcal{A}'} \neq \mathrm{L}_{\bar{\mathcal{A}}}$. Donc

$$\mathrm{L}_{\mathcal{A}} \neq \mathrm{L}_{\mathcal{A}'}.$$

5.2 De même, $\mathrm{L}_{\bar{\mathcal{A}}} \cap \mathrm{L}_{\mathcal{A}'} \neq \mathrm{L}_{\mathcal{A}'}$.Donc

$$\mathrm{L}_{\mathcal{A}} \not\subseteq \mathrm{L}_{\mathcal{A}'}.$$

5.3 $\mathrm{L}_{\mathcal{A}} \cap \mathrm{L}_{\mathcal{A}'} \neq \mathrm{L}_{\mathcal{A}}$. Donc

$$\mathrm{L}_{\mathcal{A}} \not\supseteq \mathrm{L}_{\mathcal{A}'}.$$

5.4 $\mathrm{L}_{\mathcal{A}} \cap \mathrm{L}_{\mathcal{A}'}$ possède le mot $(ab)^6$, donc

$$\mathrm{L}_{\mathcal{A}} \cap \mathrm{L}_{\mathcal{A}'} \neq \emptyset.$$

5.5 $\mathrm{L}_{\mathcal{A}} \cap \mathrm{L}_{\mathcal{A}'}$ possède le mot $(ab)^5aab$ et $(ab)^5aab \notin ab(ab)^*$, donc

$$\mathrm{L}_{\mathcal{A}} \cap \mathrm{L}_{\mathcal{A}'} \not\subseteq R_1.$$

6-Pour tout entier $n \geq 0$:

$$(a^n)^{-1}M \cap b^* = \{b^n\}$$

donc $n \neq m \Rightarrow (a^n)^{-1}M \neq (a^m)^{-1}M$. Le langage M a donc une *infinité* de résiduels, donc M n'est pas rationnel.
$L \cap M = ((ab)^2)^*$, donc c'est un langage rationnel.

Exercice

1- Considérons les interprétations suivantes :

$I \setminus \mathcal{P}$	p	q	r
I_1	1	1	1
I_2	0	0	0

$$\tilde{I}_1(F_1) = \tilde{I}_1(F_2) = \tilde{I}_1(F_3) = \tilde{I}_1(F_4) = 1; \;\; \tilde{I}_2(F_5) = 1$$

Donc toutes les formules données sont *satisfaisables.*
2- F_3, F_4 sont des instances des schémas d'axiomes du système formel étudié en cours. Ce sont donc des tautologies.D'autre part

$$\tilde{I}_2(F_1) = \tilde{I}_2(F_2) = 0; \;\; \tilde{I}_1(F_5) = 0$$

donc F_1, F_2, F_5 ne sont pas des tautologies.

Exercice

1- De la relation de récurrence

$$u_n = u_{n-1} + 2u_{n-2} \quad (n \geq 2) \text{ et } u_0 = 1, u_1 = 2. \tag{8.1}$$

on tire successivement :

$$u_n X^n = u_{n-1} X^n + 2u_{n-2} X^n \quad (n \geq 2)$$

$$\sum_{n=0}^{\infty} u_n X^n = (1 + 2X) + \sum_{n=2}^{\infty} u_{n-1} X^n + \sum_{n=2}^{\infty} 2u_{n-2} X^n,$$

$$u(X) = (1 + 2X) + (u(X) - 1)X + 2u(X)X^2,$$

$$u(X) \cdot (1 - X - 2X^2) = 1 + X$$

$$u(X) = \frac{1 + X}{1 - X - 2X^2} = \frac{1}{1 - 2X}.$$

2-Comme $\frac{1}{1-2X} = \sum_{n=0}^{\infty}(2X)^n = \sum_{n=0}^{\infty} 2^n \cdot X^n$, on enconclut que

$$u_n = 2^n \quad (n \geq 0).$$

3-De la relation de récurrence

$$v_n = v_{n-1} + 2v_{n-2} + (-1)^n \quad (n \geq 2) \text{ et } v_0 = v_1 = 1, \tag{8.2}$$

on tire successivement :

$$v_n X^n = v_{n-1} X^n + 2v_{n-2} X^n + (-1)^n X^n \quad (n \geq 2)$$

$$\sum_{n=0}^{\infty} v_n X^n = [1+X] + [(\sum_{n=2}^{\infty} v_{n-1} X^{n-1})X] + [(\sum_{n=2}^{\infty} 2v_{n-2} X^{n-2})X^2] + [\sum_{n=2}^{\infty} (-1)^n X^n]$$

$$v(X) = [1 + X] + [(v(X) - 1)X] + [(2v(X))X^2] + [\frac{1}{1 + X} - 1 + X]$$

$$v(X)[1 - X - 2X^2] = [1 + X] + [-X] + [0] + [\frac{1}{1 + X} - 1 + X] = \frac{1 + X + X^2}{1 + X}$$

$$v(X) = \frac{1 + X + X^2}{(1 + X)^2(1 - 2X)}$$

4-v_n est donc un “polynôme exponentiel” de n, de la forme :

$$v_n = \alpha 2^n + \beta(-1)^n + \gamma n(-1)^n$$

les valeurs $v_0 = 1, v_1 = 1, v_2 = 4$ entrainent que :

$$\alpha + \beta = 1; \;\; 2\alpha - \beta - \gamma = 1; \;\; 4\alpha + \beta + 2\gamma = 4,$$

soit, finalement que :

$$\alpha = 7/9, \beta = 2/9, \gamma = 1/3$$

d'où

$$v_n = \frac{7}{9}2^n + \frac{2}{9}(-1)^n + \frac{1}{3}n(-1)^n.$$

Problème

1- Considérons la propriété $\mathsf{P}(F)$:

si $F \in \mathcal{F}_1, \forall x \in \{0,1\}, F(x) \in \{0,1\}$ et si $F \in \mathcal{F}_2, \forall x \in \{0,1\}, \forall y \in \{0,1\}, F(x,y) \in \{0,1\}$.

On vérifie :

$$\mathsf{P}(P_1), \mathsf{P}(P_2), \mathsf{P}(\lambda).$$

Supposons que $F, G, H \in \mathcal{F}_2$ sont telles que $\mathsf{P}(F), \mathsf{P}(G), \mathsf{P}(H)$ soient vraies et soient $x, y \in \{0,1\}$. Alors $G(x,y), H(x,y) \in \{0,1\}$. Et comme $\mathsf{P}(F)$ est vraie, $F(G(x,y), H(x,y)) \in \{0,1\}$.
De même, si $G \in \mathcal{L} \cap \mathcal{F}_2$, $F \in \mathcal{L} \cap \mathcal{F}_1$ et $\mathsf{P}(F), \mathsf{P}(G)$, alors la fonction $(x,y) \mapsto F(G(x,y))$ vérifie P.
Si $G \in \mathcal{L} \cap \mathcal{F}_2$ et $\mathsf{P}(G)$ alors la fonction $x \mapsto G(x,x)$ vérifie P.
Donc, par induction structurelle, on a démontré que toute fonction de $\mathcal{L}$ vérifie P.
2- La fonction $\mu \in \mathcal{F}_2$ ne vérifie pas P, puisque $\mu(1,1) = 2$. Donc $\mathcal{L} \neq \mathcal{F}_{\leq 2}$.
3- $\delta_0(x) = P_1(x,x)$, donc par les points (0) puis (4) de la définition inductive de $\mathcal{M}$, $\delta_0 \in \mathcal{M}$.
$\delta_1(x) = \mu(x,x)$, donc par les points (1) puis (4) de la définition inductive de $\mathcal{M}$, $\delta_1 \in \mathcal{M}$.
$\delta_2(x) = \mu(\mu(x,x), \mu(x,x))$, donc par les points (1) puis (2) puis (4) de la définition inductive de $\mathcal{M}$, $\delta_2 \in \mathcal{M}$.
4-Comme pour tout $x \in E, x \neq \delta_1(x)$, la formule

$$\forall x \in E, \mathrm{Z}(x) = \mu(x, \delta_1(x))$$

est vraie. En utilisant le point (3) : $(x,y) \mapsto \delta_1(P_1(x,y))$ est dans $\mathcal{M}$; en utilisant le point (2) : $(x,y) \mapsto \mu(P_1(x,y), \delta_1(P_1(x,y)))$ est dans $\mathcal{M}$; en

utilisant le point (4) : $x \mapsto \mu(P_1(x,x), \delta_1(P_1(x,x)))$ est dans $\mathcal{M}$;c'est à dire $Z \in \mathcal{M}$.
5- $\forall x \in E, \mathrm{Not}(x) = \mu(x, \mathrm{Z}(x))$, donc Not $\in \mathcal{M}$.
6- Considérons les applications suivantes :

$$\mathrm{Xor}(x,y) = \mathrm{Not}(\mu(x,y)); \quad \mathrm{And}(x,y) = \mu(\delta_2(x), \delta_2(y)).$$

Comme $\mu, \mathrm{Not}, \delta_2 \in \mathcal{M}$, les formules ci-dessus montrent que $\mathrm{Xor}, \mathrm{And} \in \mathcal{M}$. On vérifie que les valeurs prises sur $\{0,1\} \times \{0,1\}$ sont les suivantes :

(x,y)	Xor	$\delta_2(x)$	$\delta_2(y)$	And
$0,0$	0	2	2	0
$0,1$	1	2	0	0
$1,0$	1	0	2	0
$1,1$	0	0	0	1

Donc Xor et And répondent bien à la question.
7- Les formules suivantes décrivent les fonctions Test_i à partir des fonctions δ_j et Not, qui sont dans $\mathcal{M}$:

$$\mathrm{Test}_0(x) = \mathrm{Not}(x); \quad \mathrm{Test}_i(x) = \mathrm{Test}_0(\delta_{3-i}(x)) \text{ pour } 1 \leq i \leq 2.$$

Donc $\forall i \in \{0,1,2\}, \mathrm{Test}_i \in \mathcal{M}$.
8-

$$\mathrm{Test}_{i,j}(x,y) = \mathrm{And}(\mathrm{Test}_i(x), \mathrm{Test}_j(y)).$$

Comme on a vu que And et $\mathrm{Test}_i, \mathrm{Test}_j$ appartiennent à $\mathcal{M}$, on conclut que $\mathrm{Test}_{i,j} \in \mathcal{M}$.
9- Soit $F : E \times E \to \{0,1\}$. Notons $\|F\| = \mathrm{Card}(\{(x,y) \in E \times E | F(x,y) = 1\})$.
Si $\|F\| = 0$, alors $F = \mathrm{Z}$ et d'après la question 4, $F \in \mathcal{M}$.
Si $\|F\| \geq 1$, fixons un argument $(x_1, y_1) \in E \times E$ tel que $F(x_1, y_1) = 1$.
Posons :

$$F_1(x_1, y_1) = 0 \text{ et } F_1(x,y) = F(x,y) \text{ pour tout } (x,y) \in E \times E - \{(x_1, y_1)\}.$$

Comme $\|F_1\| \leq \|F\| - 1$, par hypothèse de récurrence, $F_1 \in \mathcal{M}$.
Mais :

$$F(x,y) = \mathrm{Xor}(F_1(x,y), \mathrm{Test}_{x_1,y_1}(x,y))$$

comme Xor et Test_{x_1,y_1} appartiennent à $\mathcal{M}$, $F \in \mathcal{M}$.
10- Comme G_0, G_1 sont des applications de $E \times E$ dans $\{0,1\}$, d'après la question 9, $G_0, G_1 \in \mathcal{M}$. Mais

$$G(x,y) = \mu(G_0(x,y), G_1(x,y))$$

donc $G \in \mathcal{M}$.
11- On conclut de la question 10 que $\mathcal{M} = \mathcal{F}_{\leq 2}$. La fonction μ *engendre toutes* les applications de $\{0,1,2\}^2$ dans $\{0,1,2\}$. C'est un analogue de l'application *nor* qui engendre toutes les applications de $\{0,1\}^2$ dans $\{0,1\}$.

Examen, OMI, session de Septembre 2001.

Exercice 1

1-On considère le langage $L_2 = \{a,b\}^* abb \{a,b\}^* \subseteq \{a,b\}^*$. Calculer un automate fini, déterministe, sur l'alphabet $X = \{a,b\}$, qui reconnaît L_2.
2-Calculer l'automate déterministe, complet, minimal, de L_2.
3-Calculer une expression rationnelle décrivant le langage $X^* - L_2$.
4-Plus généralement, pour tout entier $n \geq 1$ on pose

$$L_n = \{a,b\}^* ab^n \{a,b\}^*.$$

Combien d' états possède l'automate déterministe minimal de L_n ?
5-Considérons les langages :

$$L = \cup_{n\geq 1} L_n; \quad S_n = L_n \cdot L_{n+1} (\text{ pour } n \geq 1); \quad S = \cup_{n \geq 1} S_n$$

Le langage L est-il rationnel ?
Est-il vrai que, pour tout $n \geq 1$, S_n est rationnel ?
Le langage S est-il rationnel ?

Exercice 2

Soit $\mathbb{N}$ l'ensemble des entiers positifs ou nuls et $\mathcal{E} = \mathcal{P}(\mathbb{N})$ l'ensemble des parties de $\mathbb{N}$. On considère l'ensemble ordonné $(\mathcal{E}, \subseteq)$, où $\subseteq$ est la relation d'inclusion.
On rappelle qu'un ensemble ordonné $\mathcal{E}$ est dit *complet* lorsque toute partie de $\mathcal{E}$ admet une borne supérieure.
1-Vérifier que $(\mathcal{E}, \subseteq)$ est complet. Rappeler l'expression de la borne supérieure (respectivement inférieure) d'un ensemble $\mathcal{A} \subseteq \mathcal{E}$ à l'aide de l'opération de réunion (resp. d'intersection).

On considére les applications $f_i : \mathcal{E} \to \mathcal{E}$
$f_1 : A \mapsto A \cup \{0\}$
$f_2 : A \mapsto A \cap (2 \cdot \mathbb{N})$
(la notation $2 \cdot \mathbb{N}$ désigne l'ensemble des entiers pairs)
$f_3 : A \mapsto A \cup \{0\}$ (si $\mathrm{Card}(A)$ est un entier pair); $A \mapsto A \cup \{1\}$ (si $\mathrm{Card}(A)$ est un entier impair); $A \mapsto A \cup \{0, 1\}$ (si $\mathrm{Card}(A)$ est infini);
$f_4 : A \mapsto \{a - 1 \mid a \in A - \{0\}\}$ i.e. $f_4(A)$ est l'ensemble des prédécesseurs des éléments de A.
$f_5 : A \mapsto \mathbb{N} - A$ i.e. $f_5(A)$ est le complémentaire de A dans $\mathbb{N}$.
$f_6 : A \mapsto \{x \in \mathbb{N} \mid x + 1 \in A \text{ et } x \in A\} \cup \{0\}$
2-Déterminer, pour chaque indice $i \in [1, 6]$, si f_i est croissante ? si f_i est continue ?
3-f_5 admet-elle au moins un point fixe ?
4-f_6 admet-elle un plus grand point fixe ?
5-Quels sont les points fixes de f_3 ? f_3 admet-elle un plus petit point fixe ? un plus grand point fixe ?
6-Soit $\mathcal{Q} \subseteq \mathcal{E}$ un ensemble de parties de $\mathbb{N}$. Donner un exemple d'application $f : \mathcal{E} \to \mathcal{E}$, dont l'ensemble des points fixes soit exactement $\mathcal{Q}$.
Indication : on pourra distinguer, dans la définition de $f(A)$, le cas $A \in \mathcal{Q}$ du cas $A \notin \mathcal{Q}$ et s'inspirer de f_5.
7-Soit $f : \mathcal{E} \to \mathcal{E}$ une application continue. Notons $\mathcal{PF}(f) \subseteq \mathcal{E}$ l'ensemble des points fixes de f. Montrer que $\mathcal{PF}(f)$ est clos par borne supérieure c'est à dire :

$$\forall \mathcal{G} \subseteq \mathcal{PF}(f), \sup(\mathcal{G}) \in \mathcal{PF}(f).$$

8-Soit $\mathcal{Q} \subseteq \mathcal{E}$ un ensemble de parties de $\mathbb{N}$, clos par borne supérieure. Montrer qu'il existe une application continue $f : \mathcal{E} \to \mathcal{E}$, dont l'ensemble des points fixes soit exactement $\mathcal{Q}$.

Exercice 3

1-Soit $(u_n)_{n\geq 0}$ la suite d'entiers définie par :

$$u_n - 4u_{n-1} - 4u_{n-2} = 0 \ \ (n \geq 2) \text{ et } u_0 = 1, u_1 = 1.$$

Donner une expression de u_n en fonction de n.
2-Soit $(v_n)_{n\geq 0}$ la suite d'entiers définie par :

$$v_n - 4v_{n-1} - 4v_{n-2} = n \ \ (n \geq 2) \text{ et } v_0 = 1, v_1 = 1.$$

Donner une expression de v_n en fonction de n.

Examen de Mai 2002

Durée : 3 heures.
Tous documents autorisés.
Le problème et l'exercice sont *indépendants*. Les questions précédées d'une $*$ sont *difficiles*. Le candidat peut, bien sûr, admettre les résultats de certaines questions, puis les utiliser dans la suite de l' épreuve. La note obtenue (entre 0 et 20), est le minimum entre 20 et le total de points obtenus (entre 0 et 35).

Problème (sur 27 points)

I-Sous-mots

On s'intéresse à l'ensemble X^* des mots sur un alphabet fini X. Soient u, v deux mots de X^* :

$u = x_1 \cdots x_i x_{i+1} \cdots x_l$ avec $x_1, \cdots, x_i, x_{i+1}, \cdots, x_l \in X$ et $v = y_1 \cdots y_j y_{j+1} \cdots y_m$ avec $y_1, \cdots, y_j, y_{j+1}, \cdots, y_m \in X$.
On dit que u est *sous-mot de* v ssi il existe une suite strictement croissante $1 \leq j_1 < \cdots < j_i < j_{i+1} < \cdots < j_l \leq m$ telle que

$$x_1 = y_{j_1}, \cdots, x_i = y_{j_i}, x_{i+1} = y_{j_{i+1}}, \cdots, x_l = y_{j_l}.$$

(Dans le cas particulier où $l = 0$, $u = \epsilon$ et u est sous-mot de v).
On note alors $u \leq_{\mathrm{sm}} v$.
Par exemple $aab \leq_{\mathrm{sm}} bababb$ mais $aaa \not\leq_{\mathrm{sm}} bababb$.
1-Vérifier que la relation binaire $\leq_{\mathrm{sm}}$ est un ordre. Est-il total ? Est-il bien-fondé ?
2-L'ordre $\leq_{\mathrm{sm}}$ est-il compatible avec le produit à gauche, c'est à dire, vérifie-t-il que :
$\forall u, v, w \in X^*, u \leq_{\mathrm{sm}} v \Rightarrow w \cdot u \leq_{\mathrm{sm}} w \cdot v$?
3.1-Montrer que, $\forall u, v \in X^*, \forall x \in X, \;\; x \cdot u \leq_{\mathrm{sm}} x \cdot v \Rightarrow u \leq_{\mathrm{sm}} v$.
3.2-L'ordre $\leq_{\mathrm{sm}}$ est-il simplifiable à gauche, c'est à dire, vérifie-t-il que :
$\forall u, v, w \in X^*, w \cdot u \leq_{\mathrm{sm}} w \cdot v \Rightarrow u \leq_{\mathrm{sm}} v$?

On considère $X = \{a, b\}$ et $L = \{u \in X^* \mid aba \leq_{\mathrm{sm}} u\}$.

4-Donner une expression rationnelle de L.
5-Donner une expression rationnelle de $X^* - L$.
6-Calculer un automate déterministe reconnaissant L. En déduire l'automate minimal de L.
7-Montrer que, pour tout langage rationnel $K \subseteq X^*$, les langages suivants sont rationnels :

$$M(K) = \{u \in X^* \mid \exists v \in K, v \leq_{\mathrm{sm}} u\}; \;\; m(K) = \{u \in X^* \mid \exists v \in K, u \leq_{\mathrm{sm}} v\}.$$

II-Beaux-ordres

Soit $(E, \preceq)$ un ensemble ordonné (N.B : $\preceq$ est une relation d'ordre, mais on ne suppose pas que $\preceq$ est un ordre *total*). On note $\prec$ la relation : $x \prec y \Leftrightarrow (x \preceq y$ et $x \neq y)$.
Rappel :$\preceq$ est un ordre *bien-fondé* ssi il n'existe pas de suite $(u_n)_{n \geq 0}$ telle que $\forall n \in \mathbf{N}, u_{n+1} \prec u_n$.
(*)8- Montrer que les conditions suivantes sur l'ordre $\preceq$ sont équivalentes :

(i) toute partie non-vide de E a un nombre fini, non-nul, d'éléments minimaux

(ii) $\preceq$ est bien-fondé et, pour toute partie infinie P de E , il existe $x, y \in P$ tels que $x \prec y$

(iii) pour toute suite $(u_n)_{n\geq 0}$ d'éléments de E, il existe une suite strictement croissante d'entiers $n_0 < n_1 < \cdots < n_i < n_{i+1} < \cdots$ telle que $u_{n_0} \preceq u_{n_1} \preceq \cdots \preceq u_{n_i} \preceq u_{n_{i+1}} \preceq \cdots$

(iv) pour toute suite $(u_n)_{n\geq 0}$ d'éléments de E, il existe $i < j$ tels que $u_i \preceq u_j$.

Lorsque l'une de ces propriétés est vérifiée on dit que $\preceq$ est un *bel* ordre.
9- On considère l'ensemble ordonné $(\mathbf{N} \times \mathbf{N}, \leq_{\mathrm{p}})$, où $\leq_{\mathrm{p}}$ est l'ordre produit défini par :

$$(n, m) \leq_{\mathrm{p}} (n', m') \Leftrightarrow (n \leq n' \text{ et } m \leq m').$$

L'ordre $\leq_{\mathrm{p}}$ est-il bien-fondé ? Est-il un bel ordre ?
10- On considère l'ensemble ordonné $(\mathbf{N} \times \mathbf{N}, \leq_{\mathrm{lx}})$, où $\leq_{\mathrm{lx}}$ est l'ordre lexicographique défini par :

$$(n, m) \leq_{\mathrm{lx}} (n', m') \Leftrightarrow (n < n' \text{ ou } (n = n' \text{ et } m \leq m')).$$

L'ordre $\leq_{\mathrm{lx}}$ est-il bien-fondé ? Est-il un bel ordre ?
11- On considère l'ensemble ordonné $(X^* \times X^*, \leq_{\mathrm{f}})$, où $\leq_{\mathrm{f}}$ est l'ordre "être facteur de", défini par :

$$u \leq_{\mathrm{f}} v \Leftrightarrow \exists \alpha, \beta \in X^*, \alpha \cdot u \cdot \beta = v.$$

Par exemple $aab \not\leq_{\mathrm{f}} bababb$, mais $bab \leq_{\mathrm{f}} bababb$.
L'ordre $\leq_{\mathrm{f}}$ est-il bien-fondé ? Est-il un bel ordre ?
12- On considère l'ensemble ordonné $(\{a, b\}^*, \leq_{\mathrm{lx}})$, où $\leq_{\mathrm{lx}}$ est l'ordre lexicographique sur les mots, défini par :

$$u \leq_{\mathrm{lx}} v \Leftrightarrow \exists \alpha, \beta, \gamma \in X^*, (u = \alpha a \beta \text{ et } v = \alpha b \gamma) \text{ ou } (\exists \gamma \in X^*, u \cdot \gamma = v).$$

(Cet ordre correspond à l'ordre de présentation des mots dans un dictionnaire).
Par exemple $aab \leq_{\mathrm{lx}} aabba$, $aab \leq_{\mathrm{lx}} abaaa$, $aaaaaab \leq_{\mathrm{lx}} ab$.
L'ordre $\leq_{\mathrm{lx}}$ est-il bien-fondé ? Est-il un bel ordre ?

III-Induction

On réfléchit ici, aux preuves par induction dans l'ensemble ordonné $(\Omega, \leq_{\mathrm{lx}})$, où Ω est l'ensemble des suites d' éléments de X^* et l'ordre lexicographique, noté $\leq_{\mathrm{lx}}$, est défini par :
pour toutes suites $U = (u_n)_{n \geq 0}$, $V = (v_n)_{n \geq 0}$, on pose $U \leq_{\mathrm{lx}} V$ ssi

$$U = V \text{ ou } (\exists n_0 \in \mathbf{N}, \forall n < n_0, u_n = v_n \text{ et } u_{n_0} \leq_{\mathrm{sm}} v_{n_0} \text{ et } u_{n_0} \neq v_{n_0}).$$

13- L'ordre $\leq_{\mathrm{lx}}$ sur Ω est-il bien-fondé ?
On rappelle que, dans ce contexte, une propriété $\mathcal{P}$ est *inductive* ssi

$$\forall x \in \Omega, (\forall y \in \Omega, (y \leq_{\mathrm{lx}} x \text{ et } y \neq x) \Rightarrow \mathcal{P}(y)) \Rightarrow \mathcal{P}(x).$$

On considère la propriété $\mathcal{P}_0$ définie par : pour toute suite $U = (u_n)_{n \geq 0}$,

$$\mathcal{P}_0(U) : \ \forall n \in \mathbb{N}, \exists n' \geq n, u_{n'} = \epsilon.$$

Autrement dit, la suite U vérifie la propriété $\mathcal{P}_0$ ssi elle comporte un nombre infini de termes égaux au mot vide.
14- Vérifier que la propriété $\mathcal{P}_0$ est inductive.
15- La propriété $\mathcal{P}_0$ est-elle vérifiée par tous les éléments de Ω ? Ce résultat est-il contradictoire avec le "principe d'induction bien-fondée" vu en cours ?
(*)16- Montrer que toute partie non-vide de Ω admet une borne inférieure (pour l'ordre $\leq_{\mathrm{lx}}$).
Une propriété $\mathcal{P}$ est dite inf-compatible, si, pour toute partie non-vide P de Ω, si $\mathcal{P}(\inf(P))$ est vraie alors, il existe $U \in P$, telle que $\mathcal{P}(U)$ est vraie.
17- Montrer que, si une propriété $\mathcal{P}$ est à la fois inductive et inf-compatible, alors :

$$\forall U \in \Omega, \mathcal{P}(U).$$

18- La propriété $\mathcal{P}_0$ est-elle inf-compatible ?

IV-Théorème de Higman

On utilise ici le principe d'induction mis au point dans la partie III (question 17), pour démontrer que l'ordre des sous-mots est beau.
Soit $\mathcal{P}_1$ la propriété suivante sur les éléments de Ω : pour toute suite $U = (u_n)_{n \geq 0}$

$$\mathcal{P}_1(U) : \text{ il existe } i < j \text{ tels que } u_i \leq_{\mathrm{sm}} u_j.$$

Montrer que $\mathcal{P}$ est inductive et inf-compatible.
19- Soit $U \in \Omega$ une suite ne vérifiant pas $\mathcal{P}_1$. Vérifier qu'il existe une lettre $x \in X$ et une suite strictement croissante d'entiers $(n_i)_{i \geq 0}$ telle que chaque mot u_{n_i} s'écrit sous la forme $x \cdot u'_{n_i}$. Construire à partir de U et de $(u'_{n_i})_{i \geq 0}$ une suite $U' \leq_{\mathrm{lx}} U, U' \neq U$ qui ne vérifie pas $\mathcal{P}_1$.
20- Montrer que $\mathcal{P}_1$ est inductive.
(*)21- Monter que $\mathcal{P}_1$ est inf-compatible.
22- Montrer le "théorème de Higman" : $\leq_{\mathrm{sm}}$ est un bel ordre sur X^*.

V-Calcul des minimaux

On se place maintenant dans l'ensemble ordonné $(X^*, \leq_{\mathrm{sm}})$. On appelle *idéal* toute partie $I \subseteq X^*$ telle que $\forall u, v \in X^*, u \in I$ et $u \leq_{\mathrm{sm}} v \Rightarrow v \in I$. Pour toute partie P de X^* on note $\mathrm{I}(P) = \{v \in X^* | \exists u \in P, u \leq_{\mathrm{sm}} v\}$. On dit qu'un idéal J est *finiment engendré* ssi il existe une partie finie $P \subseteq X^*$ telle que $J = \mathrm{I}(P)$.
23- Étant donnée une partie L de X^*, l'ensemble de ses mots minimaux est :

$$\mathrm{Min}(L) = \{u \in L \mid \forall v \in L, v \leq_{\mathrm{sm}} u \Rightarrow v = u\}.$$

Montrer que, pour tout $L \subseteq X^*$, $\mathrm{Min}(L)$ est *fini*.
Indication : utiliser le théorème de Higman (question 22).
24- En déduire que tout idéal de $(X^*, \leq_{\mathrm{sm}})$ est finiment engendré.
25- Donner un algorithme résolvant le problème suivant :

> *Instance :* Un automate fini $\mathcal{A}$ (sur l'alphabet d'entrée X).
> *Question :* Le langage $\mathrm{L}(\mathcal{A})$ est-il un idéal ?

26- Donner un algorithme résolvant le problème suivant :

> *Instance :* Un automate fini $\mathcal{A}$ (sur l'alphabet d'entrée X).
> *À calculer :* L'ensemble (fini) des mots minimaux de $\mathrm{I}(\mathrm{L}(\mathcal{A}))$.

27- Le langage $L = b^*aa^*b(a+b)^*$ est-il un idéal de $(\{a,b\}^*, \leq_{\mathrm{sm}})$? Calculer l'ensemble des mots minimaux de $\mathrm{I}(L)$.

Exercice (sur 8 points)

1-On note $S(X) = \sum_{n=0}^{\infty} n \cdot X^n$.
Exprimer $S(X)$ sous la forme $\frac{P(X)}{Q(X)}$ pour des polynômes $P, Q \in \mathbb{Q}[X]$.
Soit $(u_n)_{n\geq 0}$ la suite d'entiers définie par :

$$u_n = u_{n-1} + 2u_{n-2} + \ldots + nu_0 \ \ (n \geq 1) \text{ et } u_0 = 1.$$

2-Calculer les valeurs de u_n pour $0 \leq n \leq 5$.
On note $u(X) = \sum_{n=0}^{\infty} u_n \cdot X^n$.
3-Déduire de l'équation de récurrence ci-dessus une expression de $u(X)$ en fonction de $S(X)$ et de $u(X)$.
4- En déduire que $u(X) = 1 + \frac{X}{X^2-3X+1}$.
5- Exprimer u_n en fonction de n.
6- Trouver une équation linéaire à coefficients constants, d'ordre 2, vérifiée par la suite $(u_{n+1})_{n\geq 0}$.
7- On considère la suite de Fibonacci $(F_n)_{n\geq 0}$ définie par

$$F_n = F_{n-1} + F_{n-2} \ \ (n \geq 2) \text{ et } F_0 = 0,\ F_1 = 1.$$

Trouver une équation linéaire à coefficients constants, d'ordre 2, vérifiée par la suite $(F_{2n})_{n\geq 0}$.
8- En déduire une expression de u_n en fonction de F_{2n}.

Examen de Septembre 2002

Tous documents autorisés
Durée : 3 heures
Les exercices et le problème sont *indépendants*.

Exercice 1 (sur 3 points)

On considère le langage $L = a^*b \cdot (\{a,b\}^* - (ab)^*) \cdot abb$.
1- Calculer un automate fini, sur l'alphabet $X = \{a,b\}$, qui reconnaît L.
2- Déterminiser et minimiser cet automate.

Exercice 2 (sur 2 points)

Calculer l'ensemble des monômes premiers du polynôme booléen :

$$P = x\bar{y}\bar{z} + xzt + \bar{x}y\bar{t} + \bar{x}\bar{y}z + \bar{y}\bar{z}.$$

Exercice 3 (sur 2 points)

Soit $(u_n)_{n\geq 0}$ la suite d'entiers définie par :

$$u_0 = 0, u_1 = 3 \text{ et } \forall n \geq 2, u_n - 6u_{n-1} + 9u_{n-2} = 0.$$

Donner une expression de u_n en fonction de n.

Problème (sur 15 points)

Dans tout ce problème, on considère deux joueurs, $J1$ et $J2$, qui jouent à déplacer un pion (le même pour les deux joueurs) le long des arcs d'un graphe orienté fini $\mathcal{G}$. Les sommets de $\mathcal{G}$ sont partitionnés en deux sous-ensembles : S_1 (respectivement S_2) est l'ensemble des sommets où J1 (resp. J2) choisit le déplacement du pion. Le jeu s'arrête lorsque le pion est bloqué sur un sommet sans successeur. Une *partie* est une suite p de déplacements du pion. La notion de partie *gagnée* ou *perdue* par $J1$, est fixée par la donnée d'un ensemble de parties $\mathcal{F}_1$: si la partie p appartient à $\mathcal{F}_1$, elle est gagnées par J1 (et perdue par J2), sinon elle est gagnée par J2 (et perdue par J1. Remarquons qu'il n'y a donc pas de partie nulle.

Formellement : $\mathcal{G} = (S_1, S_2, E)$ où $S_1 \cap S_2 = \emptyset$ et $E \subseteq S_1 \times S_2 \cup S_2 \times S_1$. $\mathcal{G}$ peut être vu comme un graphe bi-parti sur l'ensemble de sommets $S = S_1 \cup S_2$. Une *partie* est une suite $p = (s_k)_{k \in K}$ telle que :
(P1)- $K = [1, n]$ (pour un entier $n \in \mathbb{N}$) ou bien $K = [1, +\infty[$
(P2)- $\forall k \in K$, si $k + 1 \in K$, alors $(s_k, s_{k+1}) \in E$
(P3)- si $K = [1, n]$, alors s_n n'a aucun successeur dans $\mathcal{G}$.
On dit que la partie p *commence* en s si $s_1 = s$.

Une *stratégie* pour le joueur Ji ($i = 1$ ou $i = 2$) est une application $\sigma : S \to \mathcal{P}(S)$, associant à tout sommet $s \in S$ un sous-ensemble de sommets $\sigma(s)$, vérifiant les conditions
(ST1)- $\forall s' \in \sigma(s), (s, s') \in E$
(σ spécifie un choix de "coups prometteurs" pour J1)
(ST2)- si $s \in S_{3-i}$, alors $\sigma(s) = \{s' \in S \mid (s, s') \in E\}$ (cas où c'est le tour de l'adversaire)
(ST3)- $\sigma(s) = \emptyset$ seulement si s n'a aucun successeur. (i.e. on est obligé de jouer tant que cela est possible)

Une partie $(s_k)_{k \in K}$ *respecte la stratégie* σ ssi,

$$\forall k \in K, \text{ tel que } k + 1 \in K, \text{ on a toujours : } s_{k+1} \in \sigma(s_k).$$

La stratégie du joueur Ji est *gagnante* (pour Ji), depuis le sommet s, ssi toute partie commençant en s et respectant la stratégie σ, est gagnée par Ji.

Exemple : on choisit pour $\mathcal{G}$ le graphe de la figure 1, et la partition $S_1 = \{1, 4\}, S_2 = \{2, 3, 5\}$. On définit l'ensemble $\mathcal{F}_1$ des parties gagnantes (pour $J1$), comme l'ensemble des parties qui passent par le sommet 5. Soit σ la stratégie pour le joueur $J1$, depuis le sommet 1, définie par :

$$\sigma(1) = \{2\}; \;\; \sigma(4) = \{5\}$$

et bien sûr

$$\sigma(2) = \{4\}; \;\; \sigma(3) = \{1, 4\}; \;\; \sigma(5) = \{1, 4\};$$

(ces 3 dernières conditions sont imposées par ST2).
1- Vérifier que cette stratégie est gagnante pour $J1$, depuis le sommet 1.
2- On définit σ' la stratégie pour le joueur $J1$, définie par :

$$\sigma'(1) = \{2, 3\}; \;\; \sigma'(4) = \{5\}$$

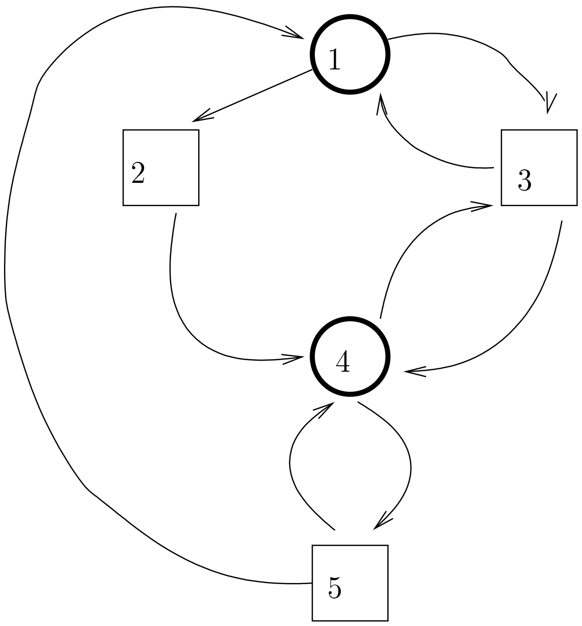


FIG. 8.1 – Le graphe $\mathcal{G}$.

et

$$\sigma'(2) = \{4\}; \;\; \sigma'(3) = \{1, 4\}; \;\; \sigma'(5) = \{1, 4\};$$

Vérifier que cette stratégie est gagnante pour $J1$, depuis le sommet 4.
3- Exhiber une partie c qui respecte σ', qui commence en 1, mais qui est perdue par $J1$. En déduire que σ' n'est pas une stratégie gagnante pour $J1$ depuis le sommet 1.
4- On conserve le graphe de la figure 1, mais on définit maintenant $\mathcal{F}_1$ comme l'ensemble des parties qui passent *infiniment souvent* par le sommet 2.
Montrer que $J2$ a une stratégie gagnante depuis le sommet 1.
On suppose, dans les questions 5 et 6, que $\mathcal{G} = (S, E)$ est un arbre orienté, non-réduit à sa racine.
5- Soit $r \in S$ la racine de cet arbre.
Montrer qu'il existe une unique partition (S_1, S_2) de l'ensemble des sommets S, telle que $r \in S_1$ et $E \subseteq S_1 \times S_2 \cup S_2 \times S_1$.
6- Soit F un sous-ensemble des feuilles de $\mathcal{G}$. On définit $\mathcal{F}_1$ comme l'ensemble des parties qui se terminent dans F.
6.1- Montrer que, soit $J1$ a une stratégie gagnante depuis r, soit $J2$ a une stratégie gagnante depuis r.

6.2- Ecrire un algorithme qui, à partir de $\mathcal{G}$ et F, détermine si $J1$ (ou, au contraire, $J2$), a une stratégie gagnante depuis r.
Quelle est la complexité de votre algorithme ?

On considère maintenant un graphe bi-parti $\mathcal{G}$ fini et un sous-ensemble de ses sommets $F \subseteq S$. On définit $\mathcal{F}_1$ comme l'ensemble des parties qui passent par au moins un sommet de F.
On note $F_i = F \cap S_i$, pour $i \in \{1, 2\}$. Pour tout $X \subseteq S$ on note :

$$p(X) = \{s \in S \mid \exists s' \in X, (s, s') \in E\}; \;\; q(X) = p(X) - p(S - X).$$

7- Montrer que l'application $f : \mathcal{P}(S) \to \mathcal{P}(S)$ définie par :

$$\forall X \subseteq S, \;\; f(X) = F \cup (p(X) \cap S_1) \cup (q(X) \cap S_2)$$

est croissante pour l'inclusion.
8- f est-elle une application continue de l'ensemble ordonné complet $(\mathcal{P}(S), \subseteq)$ dans lui-même ?
9- Montrer que f admet un plus petit point fixe, (que l'on notera X_1).
10- Montrer que $J1$ a une stratégie gagnante depuis chaque sommet de X_1.
11- Montrer que $J2$ a une stratégie gagnante depuis chaque sommet de $S - X_1$. En déduire que X_1 est exactement l'ensemble des sommets depuis lesquels $J1$ a une stratégie gagnante (on les appelle les *positions gagnantes* de $J1$).
12- Donner un algorithme de calcul des positions gagnantes de $J1$ à partir de $\mathcal{G}$ et F. Quelle est la complexité de votre algorithme ?
13- On note $\varphi : \mathcal{P}(S) \to \mathcal{P}(S)$ l'application associant à F le sous-ensemble X_1.
L'application φ est-elle croissante ?

On définit maintenant les parties gagnantes (pour $J1$) comme celles qui passent infiniment souvent dans F.
14- Montrer que l'application $g : \mathcal{P}(S) \to \mathcal{P}(S)$ définie par :

$$\forall X \subseteq S, \;\; g(X) = [p(\varphi(F \cap X)) \cap S_1] \cup [q(\varphi(F \cap X)) \cap S_2]$$

est croissante pour l'inclusion.
15- Montrer que g admet un plus grand point fixe, (que l'on notera Y_1).
16- Montrer que tout sommet de Y_1 est une position gagnante de $J1$.

17- Montrer que l'ensemble des positions gagnantes pour $J1$ est un point fixe de g.
18- Donner un algorithme de calcul des positions gagnantes de $J1$ à partir de $\mathcal{G}$ et F. Quelle est la complexité de votre algorithme ?

Examen de Mai 2003

Durée : 3 heures.
Tous documents autorisés.
Les deux exercices et le problème sont *indépendants*. La note obtenue (entre 0 et 20), est le minimum entre 20 et le total de points obtenus (entre 0 et 28).

Exercice (sur 5 points)

On considère, dans cet exercice, divers langages formels définis sur l' alphabet $X = \{a, b, c\}$.
1- Soit $R_0 = a^+ \cdot b^+ \cdot c^+$.
Donner un automate complet déterministe reconnaissant R_0.
2- Soit $R_1 = \{u \in X^*, \exists\lambda \in \mathbb{N}, |u| = 1 + 3\lambda\}$.
Donner un automate complet déterministe reconnaissant R_1.
3-Soit $L_0 = \{a^p \cdot b^q \cdot c^r \mid p, q, r \in \mathbb{N} - \{0\}, \exists\lambda \in \mathbb{N}, p + q + r = 1 + 3\lambda\}$.
3.1 Donner un automate complet déterministe reconnaissant L_0.
3.2 Minimiser cet automate.
4- Soit $L_1 = \{a^n \cdot b \cdot u \mid n \in \mathbb{N}, u \in L_0, \exists\mu \in \mathbb{N}, |u| = n + 3\mu\}$.
L_1 est-il rationnel ?
5- Soit $L_2 = \{a^n \cdot b \cdot u \mid n \in \mathbb{N}, u \in L_0, |u| = n\}$.
L_2 est-il rationnel ?

Exercice (sur 8 points)

Soit $(u_n)_{n\geq 0}$ la suite définie par :

$$u_{n+2} = 4u_{n+1} - u_n \quad \text{pour tout } n \geq 0 \quad \text{et } u_0 = 2, \;\; u_1 = 4.$$

1- Calculer les valeurs de u_n pour $n \in \{2, 3\}$.
On note $u(X) = \sum_{n=0}^{\infty} u_n \cdot X^n$.
2- Exprimer $u(X)$ sous la forme $\frac{P(X)}{Q(X)}$ pour des polynômes $P, Q \in \mathbb{Q}[X]$.
3- Exprimer u_n en fonction de n.
Soit $(v_n)_{n\geq 0}$ la suite définie par :

$$v_{n+1} = \sum_{k=0}^{n} u_{n-k} v_k \quad \text{pour tout } n \geq 0 \quad \text{et } v_0 = 1.$$

4- Calculer les valeurs de v_n pour $n \in \{1, 2, 3\}$.
On note $v(X) = \sum_{n=0}^{\infty} v_n \cdot X^n$.
5- Écrire une équation (algébrique), à coefficients dans $\mathbb{Q}[X]$, qui relie les deux séries $u(X)$ et $v(X)$.
6- En déduire une expression de $v(X)$ en fonction de $u(X)$, puis une expression de $v(X)$ sous la forme $\frac{R(X)}{S(X)}$ pour des polynômes $R, S \in \mathbb{Q}[X]$.
7- Exprimer v_n en fonction de n.

Problème (sur 15 points)

Nous étudions un système formel, appelé “calcul de Lambek”.

Partie I : syntaxe On considère l'ensemble de connecteurs $\mathcal{C} = \{\backslash, /\}$, qui sont tous les deux d'arité deux. On note $\mathcal{P}$ un ensemble dénombrable de variables propositionnelles et $\mathcal{F}(\mathcal{C}, \mathcal{P})$ l' ensemble des formules construites avec les connecteurs de $\mathcal{C}$ et les variables de $\mathcal{P}$. Les jugements sont les mots sur l'alphabet $\mathcal{C} \cup \mathcal{P} \cup \{\vdash\} \cup \{,\}$ de la forme

$$F_1, F_2, \ldots, F_n \vdash G \tag{8.3}$$

où $n \geq 1, F_1, F_2, \ldots, F_n, G \in \mathcal{F}(\mathcal{C}, \mathcal{P})$.
On appelle *séquent* un tel jugement. On notera $\mathcal{S}(\mathcal{C}, \mathcal{P})$ l'ensemble des séquents.
Exemples : $p\backslash q$; p/q ; $(p/q)\backslash p$; $(p\backslash q)\backslash(p\backslash q)$ sont des formules de $\mathcal{F}(\mathcal{C}, \mathcal{P})$.
$p\backslash(q/r) \vdash (p\backslash q)/r$ et $p,(p\backslash q)/r \vdash q/r$ sont des séquents de $\mathcal{S}(\mathcal{C}, \mathcal{P})$.
Axiome : toutes les instances du schéma d'axiome :

$$F \vdash F$$

où F est une formule.
Règles de déduction :

introduction à gauche $\dfrac{F, \Delta \quad \vdash G}{\Delta \quad \vdash F\backslash G}$

introduction à droite $\dfrac{\Gamma, F \quad \vdash G}{\Gamma \quad \vdash G/F}$

élimination à gauche $\dfrac{\Gamma \quad \vdash F \qquad \Delta \quad \vdash F\backslash G}{\Gamma, \Delta \quad \vdash G}$

élimination à droite $\dfrac{\Gamma \quad \vdash G/F \qquad \Delta \quad \vdash F}{\Gamma, \Delta \quad \vdash G}$

où, dans les quatre règles, Γ, Δ sont des listes non-vides de formules et F, G sont des formules.
1- On considère l'esquisse d'une preuve dans le calcul de Lambek, du séquent S_1 :

$$p\backslash(q/r) \vdash (p\backslash q)/r$$

1- $p \vdash p$ (Axiome)
2- $p\backslash(q/r) \vdash p\backslash(q/r)$ (?)
3- $p, p\backslash(q/r) \vdash (q/r)$ (élimination gauche, 1,2)
4- $r \vdash r$ (Axiome)
5- $p, p\backslash(q/r), r \vdash q$ (élimination droite, 3,4)
6- $p\backslash(q/r), r \vdash p\backslash q$ (introduction gauche, 5)
7- $p\backslash(q/r) \vdash (p\backslash q)/r$ (?)
Vérifier que cette suite de 7 séquents est bien une preuve en remplaçant chaque point d'interrogation par une justification précise.
2- Construire une preuve, dans le calcul de Lambek, du séquent S_2 :

$$(p\backslash q)/r \vdash p\backslash(q/r).$$

On se demande si les séquents $S_3 = p\backslash(q\backslash r) \vdash (p\backslash q)\backslash r$ et $S_4 = p \vdash q/q$ sont prouvables. Considérons l'application

$$\tau : \mathcal{F}(\mathcal{C},\mathcal{P}) \rightarrow \mathcal{F}(\mathcal{C}',\mathcal{P}) \qquad (\text{ où } \mathcal{C}' = \{\rightarrow\})$$

définie inductivement par : pour toute variable $p \in \mathcal{P}$ et toutes formules $F, G \in \mathcal{F}(\mathcal{C},\mathcal{P})$,

$$\tau(p) = p;\ \ \tau(G/F) = F \rightarrow G;\ \ \tau(F\backslash G) = F \rightarrow G.$$

3- Montrer que si un séquent de Lambek, S, est prouvable dans le calcul de Lambek, alors $\tau(S)$ est prouvable en déduction naturelle.
4- Montrer que S_3 n'est pas prouvable dans le calcul de Lambek.

Afin de traiter S_4 on définit inductivement, pour toute variable $p \ \in \mathcal{P}$ la notion de valuation $\nu_p(*) : \mathcal{F}(\mathcal{C},\mathcal{P}) \rightarrow \mathbb{Z}$ d' une formule :

$\nu_p(p) = 1;\ \ \nu_p(q) = 0($ pour toute variable $q \neq p);\ \ \nu_p(G/F) = \nu_p(F\backslash G) = \nu_p(G) - \nu_p(F).$

On étend la valuation ν_p aux séquents en posant :

$$\nu_p(F_1, F_2, \ldots, F_n \vdash G) = -\nu_p(F_1) - \nu_p(F_2) - \ldots - \nu_p(F_n) + \nu_p(G).$$

Exemple :
Pour la formule $H = (((p/p)\backslash p)\backslash(p/p))/(q/q)$, on a $\nu_p(H) = -1;\ \ \nu_q(H) = 0$.
Pour le séquent $S = H, p/p \vdash q/p$ on a $\nu_p(S) = 0;\ \ \nu_q(S) = 1$.
5- Montrer que, si S est un séquent prouvable dans le calcul de Lambek,alors,

$$\forall p \in \mathcal{P}, \nu_p(S) = 0.$$

6- Montrer que S_4 n'est pas prouvable dans le calcul de Lambek.

Partie II : sémantique Nous définissons maintenant une *sémantique* pour les séquents. Soit X un alphabet dénombrable. Notons 2^{X^*} l' ensemble des parties de X^*. Nous définissons trois opérations binaires sur 2^{X^*} : pour toutes les parties $U, V \in 2^{X^*}$

$$U \circ V = \{u \cdot v \mid u \in U, v \in V\}$$

$U//V = \{w \in X^*, \forall v \in V, w{\cdot}v \in U\}$; $V\backslash\backslash U = \{w \in X^*, \forall v \in V, v{\cdot}w \in U\}$;

7- Vérifier que $(2^{X^*}, \circ, \{\epsilon\})$ est un monoïde.

8- 8.1 Vérifier que, en général,

$$U//V = \bigcap_{v \in V} Uv^{-1}; \quad V\backslash\backslash U = \bigcap_{v \in V} v^{-1}U;$$

8.2 Considérons par exemple : $X = \{a, b\}, U = \{ab, aab, aaab\}, V = \{b, ab\}$. Calculer les résiduels Uv^{-1} et $v^{-1}U$ pour chaque $v \in V$ de l'exemple ; en déduire les valeurs de $U//V$ et $V\backslash\backslash U$ pour cet exemple.

9- Vérifier que, pour tous $U, V, W \in 2^{X^*}$ les trois propriétés suivantes sont équivalentes :

(P1) $U \subseteq (W//V)$

(P2) $(U \circ V) \subseteq W$

(P3) $V \subseteq (U\backslash\backslash W)$

On appelle *interprétation* toute application $\mathrm{I} : \mathcal{P} \to 2^{X^*}$. Une telle application est alors étendue à toute formule par :

$$\mathrm{I}(G/F) = \mathrm{I}(G)//\mathrm{I}(F); \quad \mathrm{I}(F\backslash G) = \mathrm{I}(F)\backslash\backslash \mathrm{I}(G)$$

puis à toute liste non-vide $\Gamma = F_1, F_2, \cdots, F_n$ de formules par :

$$\mathrm{I}(\Gamma) = \mathrm{I}(F_1) \circ \mathrm{I}(F_2) \circ \ldots \circ \mathrm{I}(F_n).$$

10- Montrer que, si le séquent $\Gamma \vdash G$ est prouvable dans le calcul de Lambek, alors, pour toute interprétation I,

$$\mathrm{I}(\Gamma) \subseteq \mathrm{I}(G).$$

11- On considère le séquent $S_5 : p/q \vdash q\backslash p$.
Son image $\tau(S_5)$ est-elle prouvable en déduction naturelle ?
La condition énoncée dans la question 5 est-elle vérifiée par S_5 ?
Déduire de la question 10 que S_5 n'est pas prouvable dans le calcul de Lambek.

12- Montrer le théorème de complétude du calcul de Lambek :
Soit X un alphabet dénombrable. Pour tout séquent $\Gamma \vdash G$, si pour toute interprétation $\mathrm{I} : \mathcal{P} \to 2^{X^*}$, $\mathrm{I}(\Gamma) \subseteq \mathrm{I}(G)$, alors $\Gamma \vdash G$ est prouvable dans le calcul de Lambek.
Indication : poser $X = \mathcal{F}(\mathcal{C}, \mathcal{P})$ (cet ensemble est dénombrable), considérer l'interprétation particulière J définie par :

$$\forall p \in \mathcal{P}, \mathrm{J}(p) = \{F_1 \cdot F_2 \cdots F_n \mid F_1, F_2, \cdots, F_n \vdash p \text{ est prouvable}\},$$

puis montrer que,

$$\forall G \in \mathcal{F}(\mathcal{C},\mathcal{P}), \mathrm{J}(G) = \{F_1 \cdot F_2 \cdots F_n \mid F_1, F_2, \cdots, F_n \vdash G \text{ est prouvable}\}.$$

13- Le théorème de complétude du calcul de Lambek reste-t-il vrai pour l'alphabet fini $X = \{a, b\}$?

Examen de Septembre 2003

Durée : 3 heures.
Tous documents autorisés.
Les questions précédées d'une $*$ sont *difficiles*. Le candidat peut, bien sûr, admettre les résultats de certaines questions, puis les utiliser dans la suite de l'épreuve. La note obtenue (entre 0 et 20), est le minimum entre 20 et le total de points obtenus (entre 0 et 40).

Problème (sur 40 points)

On rappelle qu'un *mot fini* u sur l'alphabet X est, par définition, une application partant d'un intervalle $[0, n-1]$ de $\mathbb{N}$ et arrivant dans l'ensemble X : $u : [0, n-1] \to X$.
Plus généralement, on appelle *mot* (fini ou infini) sur l'alphabet X, une application $u : D \to X$, dont le domaine de définition D vérifie :

$$D = [0, n-1] \text{ pour un entier } n \geq 0 \text{ ou bien } D = \mathbb{N}.$$

Lorsque $D = \mathbb{N}$, on dit que u est un mot *infini*. On note $u[k]$ l'image de l'entier k par u. Ainsi

$$u = u[0]u[1]\ldots u[k]\ldots u[n-1] \text{ si } u \text{ est fini ou bien } u = u[0]u[1]\ldots u[k]\ldots \text{ si } u \text{ est infini.}$$

On note X^∞ l'ensemble de tous les mots sur l'alphabet X.
Exemples :

$u_1 = ababb$ est un mot fini de longueur 5 ;
$u_1[0] = a, u_1[1] = b, u_1[2] = a, u_1[3] = b, u_1[4] = b$, la longueur de u, $|u|$ vaut 5.
$u_2 = ababbbbbbbbbbb\ldots$ est un mot infini ;
$u_2[0] = a, u_2[1] = b, u_2[2] = a,\ \ \forall k \geq 3, u_2[k] = b.$
$u_3 = abaaaaaaaaaa\ldots$ est un mot infini ;
$u_3[0] = a, u_3[1] = b,\ \ \forall k \geq 2, u_3[k] = a.$

I : Ordre sur les mots Soient $u : D \to X, v : E \to X$ deux mots. On dit que u est préfixe de v si et seulement si,

$$u = v \text{ ou } \exists n \in \mathbb{N}, |u| = n \text{ et } \forall k \in [0, n-1] u[k] = v[k].$$

On note alors

$$u \leq v.$$

Exemple(suite) : $u_1 \leq u_2$, $u_1 \not\leq u_3$.
On examine ici quelques propriétés de l'ensemble ordonné $(X^\infty, \leq)$.
1- Montrer que deux mots $u, v \in X^\infty$ admettent toujours une borne inférieure.
2- À quelle condition deux mots $u, v \in X^\infty$ admettent-ils une borne supérieure ?
3- Montrer que toute suite croissante admet une borne supérieure.
4- Montrer que tout mot infini u est la borne supérieure d'une suite strictement croissante de mots finis.

II : Mot de Thue-Morse On considère l'homomorphisme $\varphi : \{a, b\}^* \to \{a, b\}^*$ défini par :

$$\varphi(a) = ab,\ \varphi(b) = ba.$$

Soit u_n la suite de mots sur $\{a, b\}$ définie par

$$u_0 = a, \forall n \geq 0, u_{n+1} = \varphi(u_n).$$

5- Vérifier que $u_1 = ab, u_2 = abba, u_3 = abbabaab$; calculer u_4, u_5, u_6.
Montrer que u_n est une suite croissante (pour l'ordre $\leq$).
On considère le mot $u \in \{a, b\}^\infty$ défini par

$$u = \sup\{u_n \mid n \geq 0\}.$$

C'est le "mot de Thue-Morse".
6- Montrer que, pour tout entier $n \geq 0$

6.1- le mot aaa n'est pas facteur de $u_{n+1} = \varphi(u_n)$
6.2- le mot bbb n'est pas facteur de $u_{n+1} = \varphi(u_n)$
6.3- tout facteur de longueur 5 de u_{n+2} contient aa ou bb en facteur.
7- Montrer que, pour tout entier $n \geq 0$ et tout mot $f \in \{a, b\}^*$
7.1- le mot $afafa$ n'est pas facteur de u_n
7.2- le mot $bfbfb$ n'est pas facteur de u_n
Indication : on établira (7.1) par récurrence sur n en distinguant les quatre cas :
cas 1 : $afafa$ est en position paire et f est de longueur paire
cas 2 : $afafa$ est en position paire et f est de longueur impaire
cas 3 : $afafa$ est en position impaire et f est de longueur paire
cas 4 : $afafa$ est en position impaire et f est de longueur impaire

Soit $Y = \{x, y, z, t\}$. On définit une application $C : \{a, b\}^* \to Y^*$ par : $C(\epsilon) = C(a) = C(b) = \epsilon$ et, pour tout $u \in \{a, b\}^*$

$$C(aa \cdot u) = x \cdot C(a \cdot u); \quad C(ab \cdot u) = y \cdot C(b \cdot u);$$

$$C(ba \cdot u) = z \cdot C(a \cdot u); \quad C(bb \cdot u) = t \cdot C(b \cdot u).$$

($C(u)$ est la suite des facteurs de longueur 2 de u).
Exemples :
$C(aababb) = xyzyt, C(aababbb) = xyzytt, C(aaaab) = xxxy$.
8- Montrer que le mot $u' = \sup\{C(u_n) \mid n \geq 0\}$ est bien défini ($u' \in Y^\infty$) et montrer qu'il n'admet aucune décomposition sous la forme

$$u' = \alpha \cdot f \cdot f \cdot \beta$$

avec $\alpha \in Y^*, f \in Y^+, \beta \in Y^\infty$.
(On dit que u' est un mot infini “sans carré”).
9- Soit $u(n)$ le préfixe de longueur n du mot u. Montrer que, pour tout $p \geq 0$, $|u(2p)|_a = |u(2p)|_b$.
En déduire que $\lim_{n\to+\infty} \frac{|u(n)|_a}{n} = \frac{1}{2}$.

III : Série S. On étudie ici une première série formelle S associée au mot de Thue-Morse.
10- Montrer que, pour $n \geq 0$,

$$u[n] = a \Rightarrow (u[2n] = a \text{ et } u[2n+1] = b).$$

$$u[n] = b \Rightarrow (u[2n] = b \text{ et } u[2n+1] = a).$$

On note $\nu : \{0,1\}^* \to \mathbb{N}$ l'application associant à tout mot binaire l'entier qu'il représente. Formellement :

$$\nu(w) = w[0]2^{\ell-1} + w[1]2^{\ell-2} + \ldots + w[k]2^{\ell-k-1} + w[\ell-1]2^0 \text{ où} \ell = |w|,$$

$$\text{et } \nu(\epsilon) = 0.$$

On définit les langages

$$L_a = \{w \in \{0,1\}^* \mid u[\nu(w)] = a\}; \quad L_b = \{w \in \{0,1\}^* \mid u[\nu(w)] = b\}.$$

Exemples : comme $u = abbabaab\ldots$, $\{\epsilon, 0, 00, 11, 000, 011, 101, 110\} \subseteq L_a$ et $\{1, 01, 10, 001, 010, 100, 111\} \subseteq L_b$.
11- Donner des automates finis déterministes reconnaissant les langages L_a, L_b.
Pour tout $n \geq 0$ on pose

$$s_n = \text{Card}\{w \in \{0,1\}^* \mid |w| = n \text{ et } w \in L_a\}.$$

On considère la série formelle $S \in \mathbb{Q}[[X]]$ définie par :

$$S(X) = \sum_{n=0}^{\infty} s_n X^n.$$

12- Montrer que la suite s_n vérifie une récurrence linéaire, à coefficients constants.
13- Montrer que $S \in \mathbb{Q}((X))$. Calculer explicitement deux polynômes $P, Q \in \mathbb{Q}[X]$ tels que $S = \frac{P}{Q}$.

IV : Série U. On étudie ici une seconde série formelle U associée au mot de Thue-Morse.
On considère l'ensemble $\mathbb{F}_2 = \{0,1\}$ muni des opérations $\oplus$ (l'addition modulo 2 ou encore, le connecteur "ou exclusif") , $\times$ (le produit modulo 2 ou encore, le connecteur "et"). On rappelle que $(\mathbb{F}_2, \oplus, \times)$ est un corps commutatif.
Soit $\Psi : \{a,b\} \to \mathbb{F}_2$ l'application définie par :

$$\Psi(a) = 0, \quad \Psi(b) = 1.$$

La série $U \in \mathbb{F}_2[[X]]$ est définie par

$$U(X) = \sum_{n=0}^{\infty} \Psi(u[n])X^n.$$

14- Montrer que $\sum_{n=0}^{\infty} \Psi(u[2n])X^{2n} = U(X^2)$.
15- Déterminer deux polynômes $H, K \in \mathbb{F}_2[X]$ tels que
$\sum_{n=0}^{\infty} \Psi(u[2n+1])X^{2n+1} = U(X^2)X + \frac{H}{K}$.
16- Vérifier que, dans l'anneau $\mathbb{F}_2[[X]]$ on a "$1 + 1 = 0$". En déduire que, $\forall A, B \in \mathbb{F}_2[[X]], (A+B)^2 = A^2 + B^2$ et $A(X^2) = (A(X))^2$.
17- Écrire une équation de degré 2, à coefficients dans $\mathbb{F}_2[X]$, et dont U est une solution.

V : Suite de Fibonacci On note $(F_n)_{n\in\mathbb{N}}$ la suite de Fibonacci, définie par

$$F_0 = 1, F_1 = 2 \text{ et } F_{n+2} = F_{n+1} + F_n (\text{ pour tout } n \geq 0).$$

18- Calculer, pour tout nombre entier n, F_n en fonction de n.
19- Montrer que tout nombre entier n s'écrit de manière unique sous la forme

$$n = \sum_{i\geq 0} n_i F_i$$

avec $n_i \in \{0,1\}$ et $n_i n_{i+1} = 0$ pour tout nombre entier $i \geq 0$. En posant $k = \sup\{i \in \mathbb{N}, n_i = 1\}$, on dit que $n_k n_{k-1} \ldots n_0 \in \{0,1\}^{k+1}$ est l'écriture du nombre entier non nul en base de Fibonacci, et on note $n_k n_{k-1} \ldots n_0 = Fib(n)$. Par convention $0 = Fib(0)$.
20- Ecrire un programme, en PASCAL libre, donnant l'écriture de tout nombre entier en base de Fibonacci.

VI : Mot de Fibonacci On considère l'homomorphisme $\sigma : \{a,b\}^* \to \{a,b\}^*$ défini par :

$$\varphi(a) = ab,\ \varphi(b) = a.$$

Soit v_n la suite de mots sur $\{a,b\}$ définie par

$$v_0 = a, \forall n \geq 0, v_{n+1} = \sigma(v_n).$$

21- Montrer que v_n est une suite croissante (pour l'ordre $\leq$).
On considère le mot $v \in \{a,b\}^\infty$ défini par

$$v = \sup\{v_n \mid n \geq 0\}.$$

C'est le “mot de Fibonacci”.
22- Montrer que, pour tout $n \geq 0, v_{n+2} = v_{n+1} \cdot v_n$.
23- Exprimer les nombres $|v_n|, |v_n|_a, |v_n|_b$ à l'aide de la suite de Fibonacci (voir partie V).
24- Montrer que

$$\lim_{n \to +\infty} \frac{|v_n|_a}{v_n} = \frac{1}{\Phi},$$

où Φ est la racine positive de l' équation $X^2 - X - 1 = 0$ (Φ est le “nombre d'or”).
*25- Soit $v(n)$ le préfixe de longueur n du mot v. Montrer que

$$\lim_{n \to +\infty} \frac{|v(n)|_a}{n} = \frac{1}{\Phi}.$$

***VII : Automates et densité.** Soit $(c_n)_{n \in \mathbb{N}}$ une suite de nombres complexes vérifiant

$$\sum_{n=0}^{\infty} c_n = s \in \mathbb{C}$$

autrement dit, la série est convergente et sa somme est s.
On rappelle que, dans ce cas, le rayon de convergence ρ de la série entière $z \mapsto \sum_{n=0}^{\infty} c_n z^n$ vérifie alors :

$$\rho \geq 1.$$

*26- Montrer que, pour tous $m_1, m_2 \in \mathbb{N}, r \in [0, 1]$,

$$|\sum_{n=m_1}^{m_2} c_n \cdot r^n| \leq 2 \cdot \max\{|\sum_{n=m}^{m_2} c_n|, m_1 \leq m \leq m_2\}.$$

*27- Notons $f : [0, 1] \to \mathbb{C}$ l'application définie par

$$\forall r \in [0, 1], f(r) = \sum_{n=0}^{\infty} c_n r^n.$$

Montrer que $\lim_{r \to 1^-} f(r) = s$.
*28- Montrer que, si $\sum_{n=0}^{\infty} c_n X^n \in \mathbb{Q}((X))$ et si $\sum_{n=0}^{\infty} c_n = s \in \mathbb{C}$, alors

$$s \in \mathbb{Q}.$$

Un mot $g \in \{a, b\}^{\infty}$ est dit *automatique* si et seulement si le langage

$$L_a(g) = \{w \in \{0, 1\}^* \mid g[\nu(w)] = a\}$$

est rationnel. Pour tout $n \geq 0$ on pose

$$t_n = \text{Card}\{w \in \{0,1\}^* \mid |w| = n \text{ et } w \in L_a(g)\}.$$

On considère la série formelle $G \in \mathbb{Q}[[X]]$ définie par :

$$G(X) = \sum_{n=0}^{\infty} t_n X^n.$$

*29- Montrer que, si le mot g est automatique, alors la série G est une fraction rationnelle.
*30- On suppose que $\lim_{n\to+\infty} \frac{t_n}{2^n} = d \in \{0,1\}$. (Le nombre d est la “densité” du langage $L_a(g)$ dans $\{a,b\}^*$). Montrer que, si g est automatique, alors $d \in \mathbb{Q}$.
*31- En déduire que le mot de Fibonacci n'est pas automatique.