Notes du cours de Théorie des Automates
Licence 3
Année 2012-2013

Gérard H. E. Duchamp*

15 octobre 2012

15-10-2012 06:38

Table des matières

* Prière de me signaler les erreurs ou bien à Julien David ou bien à Aloïs Brunel.

1 Introduction

1.1 Les différentes théories

Lorsqu'on parle d'*automate* en théorie des langages[1], on entend souvent *automate booléen*, c'est à dire essentiellement un accepteur, qui est une machine qui accepte ou non un mot. Nous verrons que ce type de machine est une partie d'une classe plus vaste qui comprend

- les automates booléens (ceux dont on vient de parler)
- les automates à ϵ-transitions
- les automates probabilistes, stochastiques et doublement stochastiques[2]
- les automates pour le calcul de longueur (ou de charge) de parcours
- les automates avec mémoire des adresses
- les transducteurs.

Nous avons résolument adopté ici le point de vue matriciel qui est, à notre connaissance le seul qui permette d'unifier les résultats obtenus dans les différentes théories (dont les précédentes) par des moyens spécifiques ou efficaces et, en même temps qui offre une implémentation rapide et naturelle.
Nous commençons par rappeler (ou exposer) la théorie classique à l'aide de ce point de vue matriciel, puis nous montrerons comment celle-ci prépare presque entièrement à la théorie générale par des conditions naturelles sur les scalaires qui sont appelés à remplacer le {0,1} booléen. Cette "variation des scalaires" permet d'aborder presque toutes les machines à nombre fini d'états connues.

1.2 Un calcul peut se terminer ou non

1.2.1 Un exemple classique.

Un algorithme se termine toujours (c'est dans la définition), mais il y a des procédés de calcul qui se terminent ou non selon les entrées que l'on leur soumet. Un exemple célèbre est donné par les fractions continues.
Fractions continues. —

Pour $x \in \mathbb{R}$ donné, on peut imaginer le procédé de calcul suivant.

1. Les langages sont simplement ls parties d'un monoïde libre.
2. Les deux premiers types se définissent par une condition sortante (la probablité totale de sortir d'un état - ou d'y faire une boucle - est égale à 1), le dernier type exige *aussi* une condition rentrante.

On applique tant que c'est possible, le calcul suivant.

$$x_0 = x \ ; \ a_n = \lfloor x_n \rfloor \ ; \ x_n = a_n + \frac{1}{x_{n+1}} \ . \tag{1}$$

```
frac_cont:=proc(x,n) option remember;
local res,an,xn,i;
xn:=x:an:=floor(x):res:=an:
for i to n while xn<>floor(xn)
do
xn:=1/(xn-an):an:=floor(xn): res:=res,an
od
:[res]
end;
```

Le domaine d'indexation de cette suite est, comme toujours

$$\{n \in \mathbb{N} | x_n \text{ est défini } \} \tag{2}$$

Il est évident que c'est un intervalle du type $[0, \cdots N]_{\overline{\mathbb{N}}}$ avec $N \in \mathbb{N}$ ou bien $N = +\infty$. son voit bien que ce calcul s'arrête (division par zéro) si, pour un n donné, $x_n \in \mathbb{N}$, sinon il se poursuit indéfiniment.
On présente la fraction continue ainsi

$$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \cdots}}}} \tag{3}$$

Exemple 1.1 *Développer* $x = \frac{\sqrt{3}}{2}$ *en fraction continue.*
Marche à suivre. —

1. $x_0 = x$ *et* $a0 = \lfloor x \rfloor$ *est ici* 0
2. $x_0 = \frac{\sqrt{3}}{2} = 0 + \frac{1}{x_1}$ *d'où* $x_1 = \frac{2}{\sqrt{3}}$ *et* $a_1 = \lfloor x_1 \rfloor = 1$
3. $x_1 = 1 + \frac{1}{x_2}$ *d'où* $x_2 = \frac{1}{\frac{2}{\sqrt{3}} - 1} = \frac{\sqrt{3}}{2-\sqrt{3}} = \frac{\sqrt{3}(2+\sqrt{3})}{4-3} = 2\sqrt{3}+3$ *(on a appliqué la quantité conjuguée) et* $a_2 = \lfloor x_2 \rfloor = 6$
4. $x_2 = 6 + \frac{1}{x_3}$ *d'où* $x_3 = \frac{1}{2\sqrt{3}-3} = \frac{2\sqrt{3}+3}{4.3-9} = \frac{2\sqrt{3}+3}{3}$ *(on applique encore la quantité conjuguée) et* $a_3 = \lfloor x_3 \rfloor = 2$
5. $x_3 = 2 + \frac{1}{x_4}$ *d'où* $x_4 = \frac{1}{\frac{2\sqrt{3}+3}{3} - 2} = \frac{3}{2\sqrt{3}+3-6} = \frac{3}{2\sqrt{3}-3} = 2\sqrt{3}+3$ *(on applique encore la quantité conjuguée encore et toujours !)*
6. $x_3 = x_1$, *les calculs se répètent et donc la fraction continue est périodique*

$$[0,1,6,2,6,2,6,2,6,2,6,\cdots]$$

7. *On a*

$$x = \frac{\sqrt{3}}{2} = 0 + \frac{1}{1 + \frac{1}{6 + \frac{1}{2 + \frac{1}{6 + \cdots}}}} \tag{4}$$

1.3 Décalages des langages.

1.3.1 Généralités.

Ici, les "quotients" analogues au procédé de calcul précédent seront donnés par les décalages. On rappelle que le décalage est défini par

Définition 1.2 *Soit $L \subset A^*$ un langage. Pour tout $w \in A^*$ et $L \subset A^*$,*

$$w^{-1}L = \{u | wu \in L\} \tag{5}$$

En fait, l'opérateur w^{-1} est adjoint de la multiplication à gauche par w comme la montre l'équivalence suivante[3]

$$\langle w^{-1}L | u\rangle = \langle L | wu\rangle \ . \tag{7}$$

Pour M,$L \subseteq A^*$; a,$b \in A$; u,$v \in A^*$ les formules suivantes

i) $a^{-1}(L+M) = a^{-1}(L) + a^{-1}(M)$ ii) $a^{-1}(LM) = a^{-1}(L)M + \langle L|\epsilon\rangle a^{-1}(M)$
iii) $a^{-1}(L^*) = a^{-1}(L)(L^*)$ iv) $a^{-1}(b) = \langle a|b\rangle\epsilon$; $a^{-1}(\epsilon) = \emptyset$
v) $u^{-1}v^{-1}(L) = (vu)^{-1}L$

on construit alors l'automate des décalés de la façon suivante

- Procédé(1.3.1)
  1. Données : Un alphabet (fini) A et un langage $L \subset A^*$
  2. État initial : L
  3. Transitions : $L_1 \xrightarrow{x} L_2$ si $L_2 = x^{-1}L_1$
  4. États : le plus petit ensemble qui puisse supporter les transitions ci-dessus
  5. États finaux : les L_i tels que $\epsilon \in L_i$

L'automate obtenu est un ADC (pas nécessairement fini !) qui reconnait le langage L.

1.3.2 Quelques exemples.

Commençons par l'automate des décalés de $abaA^*$ (Fig. 1).
Cet automate est un AFDC qui reconnaît $abaA^*$.
Une autre façon d'obtenir un automate (pas nécessairement déterministe) par décalages est de produire une famille finie dans laquelle est le langage donné et qui est stable par décalage. On entend par là que tout décalé de la famille est réunion d'éléments de la famille. Un exemple est donné par les décalés de $L = A^*(aba + aa)$.
On peut aussi produire un automate (non déterministe en général) en construisant une famille de langages $(L_i)_{i\in I=\{1..n\}}$

- dont fait partie L
- qui soit stable par décalage.

Le deuxième point veut dire que les décalés de tout L_i sont des unions des L_i. Soit

$$(\forall i \in I)(\forall a \in A)(a^{-1}L_i = \sum \mu_{ij}(a)L_j \tag{8}$$

3. On rappelle que le produit scalaire est défini, dans le contexte booléen par l'appartenance

$$\langle L|w\rangle = \begin{cases} 1 \text{ si } w \in L \\ 0 \text{ si } w \notin L \end{cases} \tag{6}$$

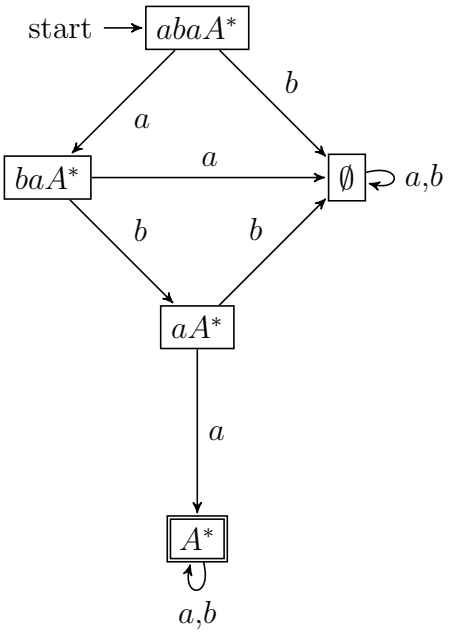

FIG. 1 – *Automate des décalés de* $L = abaA^*$.

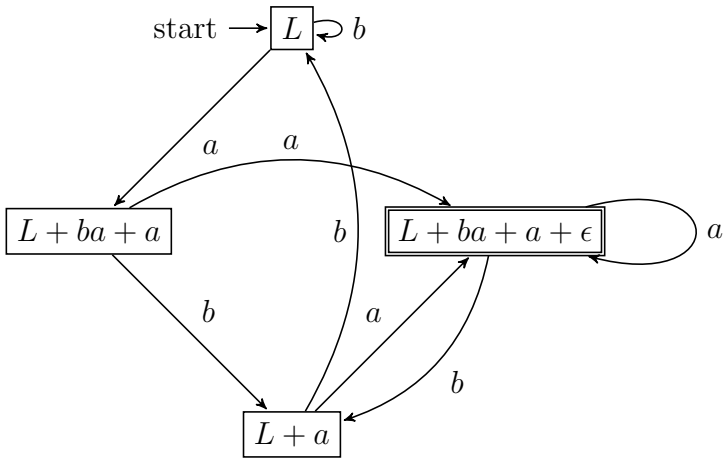

FIG. 2 – *Automate des décalés de* $L = A^*(aba + aa)$.

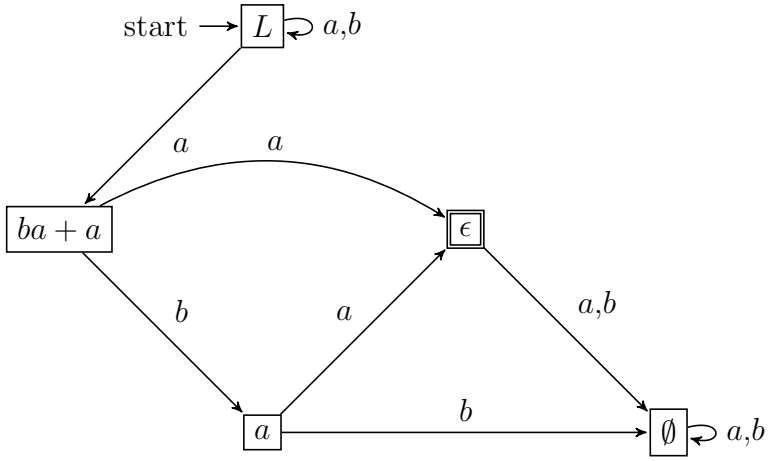

FIG. 3 – *Automate des décalés de $L = A^*(aba+aa)$ avec répartition des résultats (création d'une famille stable par décalage).*

Nous venons de créer la famille des 5 langages suivants $[L,ba+a,\epsilon,a,\emptyset]$ que l'on peut disposer sous forme d'un "vecteur de langages", la stabilité par décalage de la famille s'écrit alors

$$
\begin{aligned}
a^{-1}\begin{pmatrix} L \\ ba+a \\ a \\ \epsilon \\ \emptyset \end{pmatrix} &= \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} L \\ ba+a \\ a \\ \epsilon \\ \emptyset \end{pmatrix} \\
b^{-1}\begin{pmatrix} L \\ ba+a \\ a \\ \epsilon \\ \emptyset \end{pmatrix} &= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} L \\ ba+a \\ a \\ \epsilon \\ \emptyset \end{pmatrix}
\end{aligned}
\tag{9}
$$

Mais on peut, en remarquant que l'ensemble vide est l'union vide, se contenter d'une famille des 4 langages $[L,ba+a,\epsilon,a]$, avec les matrices de transition suivantes

$$
\begin{aligned}
a^{-1}\begin{pmatrix} L \\ ba+a \\ a \\ \epsilon \end{pmatrix} &= \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} L \\ ba+a \\ a \\ \epsilon \end{pmatrix} \\
b^{-1}\begin{pmatrix} L \\ ba+a \\ a \\ \epsilon \end{pmatrix} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} L \\ ba+a \\ a \\ \epsilon \end{pmatrix}
\end{aligned}
\tag{10}
$$

En appelant $M(x)$ la matrice de transition de la lettre x et en posant $M(u) = M(a_1)M(a_2)\cdots M(a_n)$ si $u = a_1a_2\cdots a_n$, on montre que $u^{-1}V = M(u)V$.

2 Graphes marqués

En fait, la repésentation graphique des automates finis est un cas particulier de la notion de *graphe marqué*.

Définition 2.1 *Un graphe marqué* $(S,E,L,\sigma,\beta,\lambda)$ *est la donnée de*

- S, *(comme "state"), un ensemble de sommets*
- E, *(comme "edge") un ensemble de flèches*
- L *(comme "label"), un ensemble d'étiquettes*
- σ,β *des applications* $E \to S$ *(σ est la "source" (resp. β le "but") de son argument, qui est une flèche).*
- $\lambda : E \to L$ *est l'application étiquette.*

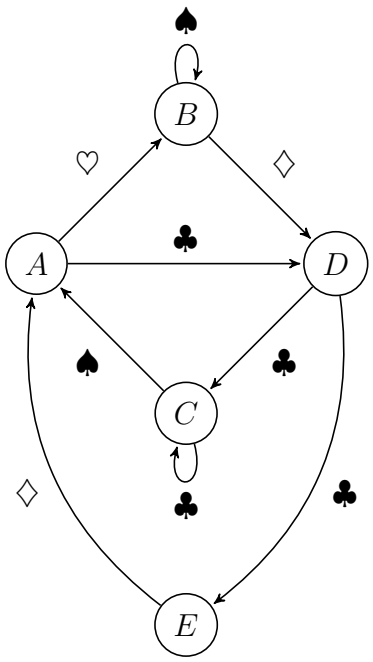

FIG. 4 – *Un graphe marqué avec, ici* $S = \{A,B,C,D,E\}$, $E \subset S^2$, $L = \{\heartsuit,\clubsuit,\clubsuit,\spadesuit\}$ *et ses applications* σ,β,λ.

Si on veut définir les éléments par un tableau on a

e	$\alpha(e)$	$\beta(e)$	$\lambda(e)$
(A,B)	A	B	♡
(B,B)	B	B	♠
(B,D)	B	D	♡
(C,A)	C	A	♠
(C,C)	C	C	♣
(D,E)	D	E	♣
(E,A)	E	A	♢

On remarquera que, dans l'exemple ci-dessus, les deux fonctions "source" et "but" sont respectivement les premières et deuxièmes projections $pr_1 : (x,y) \mapsto x$; $pr_2 : (x,y) \mapsto y$. C'est toujours possible quand $E \subset S^2$ (une ensemble de couple d'états), mais le concept de graphe marqué permet de couvrir avec une grande souplesse la situation des arcs multiples[4], comme le montre l'exemple suivant.

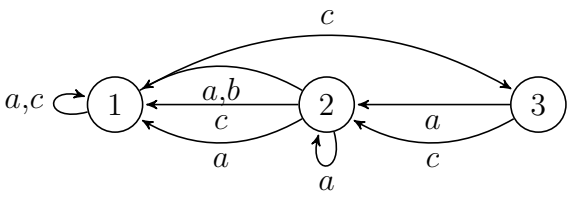

FIG. 5

e	$\alpha(e)$	$\beta(e)$	$\lambda(e)$
$(1,a,1)$	1	1	a
$(1,c,1)$	1	1	c
$(1,c,3)$	1	3	c
$(1,c,3)$	1	3	c
$(1,c,3)$	1	3	c
$(2,a,1)$	2	1	a
$(2,b,1)$	2	1	b
$(2,c,1)$	2	1	c
$(2,a,1,bis)$	1	3	c
$(2,a,2)$	2	2	a
$(3,a,2)$	3	2	a
$(3,c,2)$	3	2	c

Il y a une arête double de 3 vers 2 et une arête quadruple de 2 vers 1. Dans ce cas, il faut donner des noms à toutes les arêtes. Ici, le plus simple pour l'esprit est de nommer les arêtes comme des triplets ijk (source, lettre, but). On obtient alors le tableau suivant pour le graphe de la FIG. 5.
On remarquera qu'il y a deux arêtes de 2 vers 1 avec l'étiquette a, c'est donc ici que les triplets "(source, lettre, but)" ne séparent pas les arêtes. Ces cas se produisent lorsqu'on amalgame plusieurs lettres mais, dans la pratique, les triplets de $Q \times A \times Q$ suffiront à nos besoins.

4. Celle où il y a *plusieurs* arcs joignant deux sommets

3 Chemins

3.1 Les chemins, leur source et leur but

On appelle chemin dans un graphe marqué $(S,E,L,\sigma,\beta,\lambda)$, toute suite d'arêtes $e_1e_2\cdots e_n$ telle que pour tout $i<n$ le but de e_i soit la source de e_{i+1} ($\beta(e_i)=\sigma(e_{i+1})$).

Exercice Machine 3.1 *a) Prendre le graphe marqué de la* FIG. 4 *et faire des tirages aléatoires de suites de flèches de longueur N donnée. Sélectionner parmi ces tirages celles qui sont des chemins.*
b) Pour N petit, faire des tirages exhaustifs et déterminer la proportion de ceux qui sont des chemins.

Soit $c=e_1e_2\cdots e_n$ est un chemin, on prolonge les fonctions σ,β,λ comme suit.

$$\sigma(c)=\sigma(e_1)\ ;\ \beta(c)=\beta(e_n)\ ;\ \lambda(c)=\lambda(e_1)\lambda(e_2)\cdots\lambda(e_n)\in L^* \tag{11}$$

La source d'un chemin est son état de départ, son but est son état d'arrivée et son étiquette est la concaténation de ses étiquettes.

3.2 La matrice de transition

L'information utile pour calculer les étiquettes des chemins peut être codée dans une seule matrice (à coefficents symboliques). La matrice de transition. Cette matrice M est indexée à S^2 et le coefficient de $M[q_1,q_2]$ est la somme des étiquettes des flèches qui vont de q_1 à q_2.
Par exemple la matrice de transition du graphe de la FIG. 4 est, avec l'ordre $[A,B,C,D,E]$

$$\begin{pmatrix} 0 & \heartsuit & 0 & \clubsuit & 0 \\ 0 & \spadesuit & 0 & \diamondsuit & 0 \\ \spadesuit & 0 & \clubsuit & 0 & 0 \\ 0 & 0 & \clubsuit & 0 & \clubsuit \\ \diamondsuit & 0 & 0 & 0 & 0 \end{pmatrix} \tag{12}$$

lorsqu'il y a des arêtes multiples, on fait tout simplement la somme des transitions. Par exemple pour le graphe de la FIG. 5, on a la matrice de transition

$$\begin{pmatrix} a+c & 0 & c \\ a+b+c+a & a & 0 \\ 0 & a+c & 0 \end{pmatrix} \tag{13}$$

Nous verrons un peu plus bas quel sens donner au terme $M[2,1]$ qui devrait pouvoir s'écrire $2a+b+c$. Ce qui nous intéresse pour le moment est ce qui se passe lorsque l'on fait les puissances de la matrice de transition et c'est là que bifurquent les différentes théories.

4 Puissances de la matrice de transition

4.1 La théorie booléenne classique : Automates finis et structures de transition

Dans ce modèle, on veut un "accepteur", c'est à dire une machine qui dise si oui ou non un mot est reconnu. On n'a pas besoin de numtiplicités et le + est en réalité une union.

Qu'un état soit reconnu une ou deux (ou plus) de fois est équivalent et la matrice de transition (13) s'écrit

$$\begin{pmatrix} a+c & 0 & c \\ a+b+c & a & 0 \\ 0 & a+c & 0 \end{pmatrix} \tag{14}$$

Le calcul matriciel va donc se faire avec des scalaires dans {0,1} avec les lois suivantes

$$\begin{array}{c|c|c} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ \hline 1 & 1 & 1 \end{array} \qquad \begin{array}{c|c|c} \times & 0 & 1 \\ \hline 0 & 0 & 0 \\ \hline 1 & 0 & 1 \end{array} \tag{15}$$

Quand on multiple la matrice de transition par elle-même, on assiste à un phénomène intéressant ... la deuxième puissance donne les étiquettes des chemins de longueur 2

$$\begin{pmatrix} a+c & 0 & c \\ a+b+c & a & 0 \\ 0 & a+c & 0 \end{pmatrix} \begin{pmatrix} a+c & 0 & c \\ a+b+c & a & 0 \\ 0 & a+c & 0 \end{pmatrix} = \begin{pmatrix} aa+ac+ca+cc & ca+cc & ac+cc \\ aa+ac+ba+bc+ca+cc+aa+ab+ac & aa & ac+bc+cc \\ aa+ab+ac+ca+cb+cc & aa+ca & 0 \end{pmatrix}. \tag{16}$$

On voit que, dans $M^2[2,1]$ certains termes sont répétés (aa,ac), comme ce sont les ensembles qui nous intéressent, on peut réécrire la matrice

$$M^2 = \begin{pmatrix} aa+ac+ca+cc & ca+cc & ac+cc \\ aa+ac+ba+bc+ca+cc+ab & aa & ac+bc+cc \\ aa+ab+ac+ca+cb+cc & aa+ca & 0 \end{pmatrix} \tag{17}$$

Nous verrons plus tard les propriétés que doit vérifier un tel ensemble de scalaires pour que le calcul matriciel puisse se faire. Revenons pour le moment à la définition classique d'un (AF) et remarquons que, dans le graphe qui lui est associé les triplets $(q_1,x,q_2) \in Q\times A\times Q$ séparent les arêtes.

Définition 4.1 *Un* **AF** *(automate fini est une machine définie par un 5-uplet* $\mathbb{A} = (Q,A,\bullet,I,F)$ *où*

- Q *est un ensemble fini d'états*
- A *est un alphabet fini*
- $T \subset Q \times A \times Q$ *est un ensemble d'arêtes marquées par des lettres*
- $I \subseteq Q$ *est l'ensemble des entrées (i.e. états initiaux)*
- $F \subseteq Q$ *est l'ensemble des sorties (i.e. états finaux)*

Note 4.2 *i) Il est équivalent de se donner un ensemble d'arêtes comme ci-dessus ou bien une application* $\bullet : Q \times A \mapsto \mathcal{P}(Q)$. *S'entrainer à faire le passage.*
ii) Si on oublie les états initiaux et finaux, c'est une??.
On appelle donc?? la donnée d'un triplet $(Q,A,\bullet)$ *avec les caractéristiques du paragraphe précédent.*
iii) On dit que l'automate est déterministe *si* $|I| = 1$ *et que deux arêtes ayant même source et même étiquette ont nécessairement même but.*

On présentera donc un automate par un quintuplet (Q,A,T,I,F). Cette manière de faire facilite la traduction des données en la *représentation linéaire* de l'automate qui est celle que l'on implémente (voir T.D.).
Un *chemin* c dans le graphe de transition est donc ici une suite d'arêtes $h_i = (p_i,a_i,q_i)$; $i = 1..n$ telles que, pour tout $i < n$, on ait $q_i = p_{i+1}$ (les arêtes s'enchaînent). L'étiquette de c est le mot $a_1a_2\cdots a_n$. Le langage reconnu par un automate $\mathbb{A}$, noté $Ł(\mathbb{A})$, est l'ensemble des étiquettes des chemins qui mènent d'un état initial à un état final.

Définition 4.3 *La représentation linéaire d'un automate $\mathbb{A} = (Q,A,T,I,F)$ est la donnée des matrices suivantes associées à $\mathbb{A}$.*

- *Le vecteur initial $V_I \in \{0,1\}^{1\times Q}$ c'est un vecteur ligne (en général $Q = [1..n]$) défini par $V_I(q) = [q \in I]$ (symbole d'Iverson, on rappelle que $[P] = 1$ si P est vraie et 0 sinon). que*
- *Le vecteur final $V_F \in \{0,1\}^{Q\times 1}$ c'est un vecteur colonne (en général $Q = [1..n]$) défini par $V_F(q) = [q \in F]$.*
- *Pour chaque $a \in A$, une matrice $M(a) \in \{0,1\}^{Q\times Q}$ définie par $M(a)[q_1,q_2] = [(q_1,a,q_2) \in T]$*

En général on note, par abus de langage, I et F au lieu de V_I et V_F.

4.2 Comportement d'un automate : une fonction sur les mots

Dans ce chapitre, nous nous intéresserons plus spécialement aux fonctions sur A^* (A est un alphabet). C'est à dire, en ce qui concerne les sysèmes (informatiques ou électroniques) aux machines qui acceptent un mot en entrée et retournent un coefficient (un scalaire: un nombre, un booléen, un réel, un complexe ou même une matrice) en sortie.

$$w \to \boxed{\text{MACHINE}} \to M(w) \tag{18}$$

Ici on utilisera les scalaires de $B = \{0,1\}$ (les booléens) et $\mathbb{N}$ (les entiers naturels).
Dans le premier cas, on exprime seulement si le mot w est reconnu ou non. Dans le deuxième, on compte les chemins réussis d'étiquette w.
On a le lemme suivant.

Lemme 4.4 *Posons, pour $w = a_1a_2\cdots a_n$, $M(w) = M(a_1)M(a_2)\cdots M(a_n)$ (produit matriciel). Alors, on a*

$$[w \in Ł(\mathbb{A})] = IM(w)T. \tag{19}$$

Preuve — Elle se fait en remarquant, par récurrence que
$M(w)[q_1,q_2] =$ [il existe un chemin d'étiquette w qui joint q_1 à q_2]. □

Ce lemme permet d'exprimer $Ł(\mathbb{A})$ de faç on synthétique
Proposition 4.5 *Le langage reconnu par un automate $\mathbb{A}$ est bien*

$$Ł(\mathbb{A}) = \sum_{w\in A^*} (IM(w)T)w \tag{20}$$

4.3 Automates déterministes

TODO

4.4 Équivalence avec un AF d'un automate à ϵ-transitions

4.4.1 Généralités

Dans un automate à ϵ-transitions, on rajoute un symbole supplémentaire ϵ qui sera éliminé dans les étiquettes des chemins (ainsi l'étiquette d'un chemin est toujours la concaténation de ses étiquettes).
Le langage reconnu par un tel automate est toujours

$$\sum_{w \text{ est l'étiquette d'un chemin réussi de } \mathbb{A}} w \tag{21}$$

4.4.2 Suppression des ϵ-transitions

Les chemins réussis d'étiquette $w = a_1 a_2 \cdots a_n$ ont pour étiquette (avant supression des ϵ) $\epsilon^{k_0} a_1 \epsilon^{k_1} a_2 \epsilon^{k_2} \cdots a_n \epsilon^{k_n}$. Ceci montre que si $M(\epsilon^*)$ désigne la matrice de la clôture reflexive-transitive des ϵ-transitions, le nouvel autmate dont les éléments matriciels sont

- $I' = IM(\epsilon^*)$
- $M'(a) = M(a)M(\epsilon^*)$
- $F' = F$.

Proposition 4.6 *L'automate (sans ϵ-transitions) $\mathbb{A}'$ reconnait le même langage que $\mathbb{A}$.*

4.4.3 Application des ϵ-transitions

Les automates à ϵ-transitions sont commodes pouur construire des automates qui reconnaissent létoile et le produit de deux langages reconnus par un (ou deux) automates donnés.

5 Etoile d'une matrice

On va ici considérer des matrices (carrées) de langages. Le produit se fait comme d'habitude : si $U = (L_{ij})_{1 \leq i,j \leq n}$ et $V = (M_{ij})_{1 \leq i,j \leq n}$ on a $UV = (N_{ij})_{1 \leq i,j \leq n}$ avec

$$N_{ij} := \sum_{1 \leq k \leq n} M_{ik} N_{kj} \tag{22}$$

Rappel. — Dans $U = (L_{ij})_{1 \leq i,j \leq n}$, on a i qui est l'adresse de ligne, j l'adresse de colonne. Ainsi une matrice 3×3 se dispose

$$\begin{pmatrix} L_{11} & L_{12} & L_{13} \\ L_{21} & L_{22} & L_{23} \\ L_{31} & L_{32} & L_{33} \end{pmatrix} \tag{23}$$

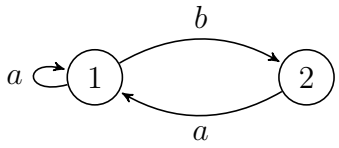

FIG. 6

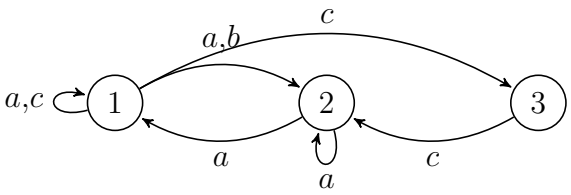

FIG. 7

Définition 5.1 *La* matrice de transtition "lettres" *(ou* matrice-lettres *tout court) d'une ?? est une matrice de langages (qui sont des sous-alphabets). C'est la matrice de format $Q\times Q$ (ses lignes et ses colonnes sont indexées par Q)*

$$T := \Big(\sum_{q_2 \in q_1.a} a \Big)_{q_1,q_2 \in Q} \tag{24}$$

étant entendu (par convention générale) que la somme est nulle s'il n'y pas d'arête entre q_1 et q_2.

Exemple 5.2 *1) La petite?? suivante:*
admet pour matrice-lettres $\begin{pmatrix} a & b \\ a & 0 \end{pmatrix}$.
admet pour matrice-lettres $\begin{pmatrix} a+c & a+b & c \\ a & a & 0 \\ 0 & c & 0 \end{pmatrix}$.

5.1 Étoile d'une matrice-lettres

Les puissances de la matrice-lettres d'une?? ont une propriété remarquable.

Proposition 5.3 *Soit T, la matrice-lettres d'une ?? $\mathcal{T} = (Q,A,\bullet)$. Pour toute paire d'états (q_1,q_2), on a*

$$(T^k)[q_1,q_2] = \{w \in A^k | q_1.w = q_2\} \tag{25}$$

autrement dit, l'entrée d'adresse $[q_1,q_2]$ de la puissance T^k est l'ensemble des mots de longueur k qui font passer de q_1 à q_2.

6 Fonctions sur les mots

Dans ce chapitre, nous nous intéresserons plus spécialement aux fonctions sur A^* (A est un alphabet). C'est à dire, en ce qui concerne les sysèmes (informatiques ou électroniques)

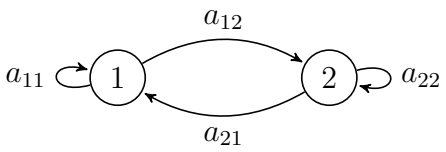

FIG. 8 – *Structure de transition générique sur 2 états*

aux machines qui acceptent un mot en entrée et retournent un coefficient (un scalaire: un nombre, un booléen, un réel, un complexe ou même une matrice) en sortie.

$$w \to \boxed{\text{MACHINE}} \to M(w) \tag{26}$$

On appellera *comportement* de la machine cette fonction $A^* \to K$ (K est l'ensemble des scalaires, voir chapitre (**??**)) et deux machines seront dites équivalentes ssi elles définisent la même fonction.

On peut composer les machines à l'aide des fonctions classiques (additionneurs, multiplieurs).

$$\begin{array}{cccccc} & \nearrow & \boxed{\text{MACHINE 1}} & \searrow & & \\ w & \to & \boxed{\text{MACHINE 2}} & \to & \bigoplus & \to M1(w) + M2(w) \end{array}$$

$$\begin{array}{cccccc} & \nearrow & \boxed{\text{MACHINE 1}} & \searrow & & \\ w & \to & \boxed{\text{MACHINE 2}} & \to & \bigotimes & \to M1(w) \times M2(w) \end{array}$$

c'est le produit (ou la somme) ponctuel(le) des fonctions correspondantes.
Il y a aussi un autre type de produit qui est très utile (nous verrons qu'il généralise la concaténation et qu'il éclaire les opérations sur les parties, c'est le produit défini par le formule

$$M1 * M2(w) = \sum_{uv=w} M1(u)M2(v) \tag{27}$$

il peut être réalisé par le système suivant

$$\begin{array}{cccccccc} & & \nearrow & u \to & \boxed{\text{MACHINE 1}} & \searrow & & \\ w = uv & \to & & & & & \bigotimes & \bigoplus_{uv=w} M1(u)M2(v) \\ & & \searrow & v \to & \boxed{\text{MACHINE 2}} & \nearrow & & \end{array}$$

6.1 Quelques exemples de machines

Toutes les machines considérées ici acceptent des mots en entrée et retournent des coefficients en sortie. Tout d'abord quelques machines de type "compteur".

Exemple 1: LONGUEUR D'UN MOT. — C'est une machine (ou un programme) qui lit un mot de gauche à droite (ou de droite à gauche peu importe ici) et qui incémente un compteur de +1 à chaque lettre (le compteur est initialisé à 0).
Le résultat est la longueur du mot.
Lorsque le mot est vide le compteur rest bien à son initialisation et le résultat est 0 (longueur du mot vide).

Exemple 2: NOMBRES D'OCCURENCES D'UNE LETTRE. — Soit $A = \{a,b\}$. C'est une machine (ou un programme) qui lit un mot de gauche à droite (ou de droite à gauche peu importe ici) et qui incémente un compteur de +1 à chaque lecture de a (le compteur est

initialisé à 0).
Le résultat est le nombre d'occurences de a.
Lorsque le mot est vide le compteur est bien à son initialisation et le résultat est 0 (longueur du mot vide).

Cette machine peut se réaliser matricellement. On pose

$$M(a) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix};\ M(b) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix};\ I = \begin{pmatrix} 1 & 0 \end{pmatrix};\ T = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{28}$$

puis $M(w) = M(a_1 a_2 \cdots a_n) = M(a_1)M(a_2)\cdots M(a_n)$ le résultat de la lecture d'un mot w est $IM(w)T$.
Montrons que cette machine compte bien le degré partiel en a

Exercice 6.1 *Montrer que cette machine compte bien le degré partiel en a.*

Dans la suite, une fonction $f : A^* \to K$ pourra aussi être noée $\sum_{u\in A^*} f(u)u$ (notation sommatoire). Cette notation permet de manipuler les fonctions comme des séries et les parties comme des sommes de mots.

7 Systèmes et Calcul

7.1 Introduction

Exemples d'automates booléens, stochastiques, de comptage, de plus courts chemins. Les semi-anneaux associés sont : $\mathbb{B}$, $\mathbb{R}_+$,$\mathbb{N}$,$([0, +\infty], min, +)$.

7.2 Description de la structure d'automate

7.2.1 Graphe pondéré

L'élément de base de ces graphes est la flêche $A = q_1 \xrightarrow{a|\alpha} q_2$ avec $q_i \in Q$, $a \in \S$, $\alpha \in k$ où Q est un ensemble d'états, $\S$ un alphabet et k, un semi-anneau[5]. Pour un tel objet, on définit, selon les conventions générales de la théorie des graphes,

- $t(A) := q_1$ ("tail": queue, source, origine)
- $h(A) := q_2$ ("head" tête, but, extrémité)
- $l(A) := a$ ("label" étiquette)
- $w(A) := \alpha$ ("weight" poids).

Un *chemin* est une suite d'arêtes $c = A_1 A_2 \cdots A_n$ (c'est un mot en les arêtes et sa longueur est n) telle que $h(A_k) = t(A_{k+1})$ pour $1 \leq k \leq n-1$ pour un tel chemin $t(c) = t(A_1)$, $h(c) = h(A_n)$, $l(c) = l(A_1)l(A_2)\cdots l(A_n)$ (concaténation), $w(c) = w(A_1)w(A_2)\cdots w(A_n)$ (produit dans le semi-anneau).
Par exemple pour le chemin de longueur 3 suivant ($k = \mathbb{N}$),

$$u = p \xrightarrow{a|2} q \xrightarrow{b|3} r \xrightarrow{c|5} s \tag{29}$$

5. Nous verrons plus bas que les axiomes de la structure de semi-anneau sont contraints par la définition même du système de transitions ainsi obtenu.

on a $t(u) = p$, $h(u) = s$, $l(u) = abc$, $h(u) = 30$.
Le poids d'un ensemble de chemins de même source, but et étiquette est la somme des poids des chemins de cet ensemble. Ainsi, si

$$\mathbf{q}1 \quad \begin{array}{c} \overset{u|\alpha}{\rightarrow} \\ \overset{u|\beta}{\rightarrow} \end{array} \quad \mathbf{q}2 \tag{30}$$

le poids de cet ensemble de chemins est $\alpha + \beta$. On a donc que les poids se multiplient en série et s'aditionnent en parallèle. Les diagrammes suivants montrent la nécessité des axiomes de semi-anneau.

Diagramme	Identité	Nom
$p \begin{array}{c} \overset{a\|\alpha}{\rightarrow} \\ \overset{a\|\beta}{\rightarrow} \\ \overset{a\|\gamma}{\rightarrow} \end{array} q$	$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$	Associativité de $+$
$p \begin{array}{c} \overset{a\|\alpha}{\rightarrow} \\ \underset{a\|\beta}{\rightarrow} \end{array} q$	$\alpha + \beta = \beta + \alpha$	Commutativité de $+$
$p \begin{array}{c} \overset{a\|\alpha}{\rightarrow} \\ \underset{a\|0}{\rightarrow} \end{array} q$	$\alpha + 0 = \alpha$	Élément neutre (droite) de $+$
$p \overset{a\|0}{} q \overset{b\|\beta}{\rightarrow} r$	$0 + \beta = \alpha$	Élément neutre (gauche) de $+$
$p \overset{a\|\alpha}{\rightarrow} q \overset{b\|\beta}{\rightarrow} r \overset{c\|\gamma}{\rightarrow} s$	$\alpha(\beta\gamma) = (\alpha\beta)\gamma$	Associativité de $\times$
$p \begin{array}{c} \overset{a\|\alpha}{\rightarrow} \\ \underset{a\|\beta}{\rightarrow} \end{array} q \overset{b\|\gamma}{\rightarrow} r$	$(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$	Distributivité (droite) de $\times$ sur $+$
$p \overset{a\|\alpha}{\rightarrow} q \begin{array}{c} \overset{b\|\beta}{\rightarrow} \\ \underset{b\|\gamma}{\rightarrow} \end{array} r$	$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$	Distributivité (gauche) de $\times$ sur $+$
$p \overset{a\|\alpha}{\rightarrow} q \overset{b\|1_k}{\rightarrow} r$	$\alpha \times 1_k = \alpha$	Élément neutre (droite) de $\times$
$p \overset{a\|1_k}{\rightarrow} q \overset{b\|\beta}{\rightarrow} r$	$1_k \times \beta = \beta$	Élément neutre (gauche) de $\times$

7.2.2 Structure et comportement des automates

Un automate à poids ou pondéré ("automaton with weights") est la donnée de trois éléments vectoriels (I,M,T):

- Un vecteur d'entrée $I \in k^{1\times Q}$
- Une famille (indexée à A) de matrices de transition $M : A \to k^{Q\times Q}$
- Un vecteur de sortie $T \in k^{Q\times 1}$

La donnée des transitions (M) est équivalente à celle d'un graphe pondéré dont les sommets sont Q, l'alphabet A et les poids sont pris dans k. De plus celle de I (resp. T) correspond à la donnée de flêches rentrantes (resp. sortantes) marquées avec des poids. Dans tout ce processus, on peut ne pas indiquer les flêches de poids nul.
Ce type d'automates généralise les automates (booléens) de la théorie des langages (que l'on obtient alors pour $k = \mathbb{B}$) est une machine qui prend un mot en entrée et retourne un coefficient (dans k) en sortie. Son comportement est donc une fonction $\mathcal{A} : A^* \to k$ (que l'on peut noter, de manière équivalente, comme une série $\mathcal{A} = \sum_{w\in A^*} \mathcal{A}(w)w$).

Calcul du poids $\mathcal{A}(w)$. —
On étend d'abord la fonction de transition M à A^* par

$$M(\epsilon) = I_{Q\times Q},\ M(w) = M(a_1a_2\cdots a_n) = M(a_1)M(a_2\cdots M(a_n) \tag{31}$$

où $I_{Q\times Q}$ est la matrice identité de format $Q \times Q$. Le calcul du poids d'un mot est alors, par définition,

$$\mathcal{A}(w) := IM(w)T \tag{32}$$

d'après la règle de multiplication des matrices, on a bien que $IM(w)T$ est une matrice de format 1×1 et donc un élément de k. Le lien avec le graphe de l'automate est donné par la proposition suivante :

Proposition 7.1 *Soit, pour deux états r,s et un mot $w \in A^*$*

$$\mathcal{A}^{r,s}(w) := I_r \left(\sum_{\substack{c,\ \text{chemin}\ \ l(c)=w \\ t(c)=r,\ h(c)=s}} weight(c) \right) T_s \tag{33}$$

alors

$$\mathcal{A}(w) = \sum_{r,s\in Q} \mathcal{A}^{r,s}(w) \tag{34}$$

Cette proposition a le sens intuitif suivant :

1. l'équation (33) donne le poids calculé comme au paragraphe précédent
   - on fait le bilan parallèle (c'est à dire une somme) des poids des chemins qui joingnent r à s
2. on multiplie (à gauche si c'est non commutatif) par le poids d'entrée en r
3. on multiplie (à droite si c'est non commutatif) par le poids de sortie en s

7.2.3 Premiers automates

1. Longueur totale $\sum_{w\in A^*} |w|w$
2. Comptage des a, $\sum_{w\in A^*} |w|_a w$ et des b, $\sum_{w\in A^*} |w|_b w$
3. Produit des degrés partiels $\sum_{w\in A^*} |w|_a|w|_b w$
4. Autres produits $\sum_{w\in A^*} F_{|w|}|w|w$, $\sum_{w\in A^*} F_{|w|_a}|w|_b w$

Fin du tronc commun

7.2.4 Composition des automates

Somme et multiplication par un coefficient constant

Produit de Hadamard

Produit (de concaténation)

Nous avons vu que nous pouvions coder de "l'infini dans du fini" en considérant les suites ultimement périodiques que sont les développements illimités des rationnels. Nous allons

voir qu'il en est de même pour la production des automates finis, en effet, un automate fini, dès qu'il possède un chemin réussi qui comporte un boucle, reconnaît un langage infini.

Exercice 7.2 *Montrer que cette condition est suffisante, autrement dit, si aucun chemin réussi ne comporte de boucle, alors le langage reconnu par l'automate est fini.*

Commençons par un exemple : On considère un automate (booléen), d'ensemble d'états Q et dont les transitions sont étiquetées par un alphabet A. Cet automate, via la correspondance (graphes $\leftrightarrow$ matrices) peut être vu comme un triplet (I,T,M) avec :

$$\begin{cases} \bullet \text{ Un vecteur d'entrée } I \in k^{1\times Q} \\ \bullet \text{ Une famille de matrices de transition } M : A \to k^{Q\times Q} \\ \bullet \text{ Un vecteur de sortie } T \in k^{Q\times 1} \end{cases}$$

Dans les automates usuels, les scalaires sont pris dans $\{0,1\}$. Si on considère ces nombres comme des entiers naturels, l'opération $w \to IM(w)T$ donne le nombre de chemins réussis. Une expression rationnelle du comportement de l'automate (tenant compte des multiplicités) résulte du calcul suivant

$$\sum_{w\in\Sigma^*} (IM(w)T)w = I(\sum_{w\in\Sigma^*} M(w)w)T = I(Id_n - \sum_{a\in\Sigma} M(a)a)^{-1}T$$

si on note $M_\Sigma = \sum_{a\in\Sigma} M(a)a$, on a $M_\Sigma^* = (Id_n - \sum_{a\in\Sigma} M(a)a)^{-1}$. C'est la matrice dont l'entrée d'adresse (i,j) est la somme

$$\sum_{\substack{w \text{ étiquette} \\ \text{un chemin de } i \text{ vers } j}} (\text{nb de chemins } i \to j \text{ d'étiquette } w)w$$

par exemple la matrice

$$M_\Sigma = \begin{pmatrix} a & a \\ b & 0 \end{pmatrix}$$

a pour étoile

$$M_\Sigma^* = \begin{pmatrix} (a+ab)^* & (a+ab)^*a \\ b(a+ab)^* & (ba^*a)^* \end{pmatrix}$$

il est facile de voir que les séries associées sont sans multiplicité (i.e. pour (i,j) et w donnés il existe au plus un chemin d'étiquette w), mais ce n'est pas le cas pour

$$Q_\Sigma = \begin{pmatrix} a & a \\ b & a \end{pmatrix}$$

qui a pour étoile

$$Q_\Sigma^* = (\ (a+aa^*b)^* \quad (a+aa^*b)a^*aa^*b(a+aa^*b)^* \quad (a+ba^*a)^*\ )$$

Exercice 7.3 *1) Dessiner les structures de transition (c'est à dire les automates sans vecteurs d'entrée et sortie) associés aux matrices M_Σ,Q_Σ.*
2) a) Montrer, en utilisant un raisonnement sur les chemins dans un graphe étiqueté convenable, que pour deux lettres, on a $(a+b)^* = (a^*b)a^*$ (élimination de Lazard monoïdale).
b) Appliquer cette identité pour trouver une autre forme de $(a+aa^*b)^*$.

c) Montrer que $a^*aa^* = a\frac{1}{(1-a)^2} = \sum_{n\geq 1} na^n$.
d) Si un mot ne se termine pas par b, sa multiplicité dans $(a^*aa^*b)^*$ *est nulle, mais s'il s'écrit* $w = a^{n_1}ba^{n_2}b\cdots a^{n_k}b$, *on a* $(w,(a^*aa^*b)^*) = n_1 + n_2 + \cdots n_k$. *En déduire le développement (i.e. les multiplicités des mots) de* $(a^*aa^*b)^*a^*$, *puis des 4 coefficients de la matrice* Q_Σ^*.
3) a) Soit l'alphabet à quatre lettres $\Sigma = \{a_{11},a_{12},a_{21},a_{22}\}$, *montrer directement en raisonnant sur les chemins, que si* $G = (\ a_{11} \quad a_{12}a_{21} \quad a_{22}\ )$ *on a*

$$G^* = \begin{pmatrix} A_{11} & A_{11}a_{12}a_{22}^* \\ a_{22}^*a_{21}A_{11} & A_{22} \end{pmatrix}$$

avec

$$A_{11} = (a_{11} + a_{12}a_{22}^*a_{21})^*,\ A_{22} = (a_{22} + a_{21}a_{11}^*a_{12})^*$$

b) Expliquer en quoi ces formules fournissent un algorithme permettant de calculer l'étoile de toute matrice de séries propres.

Exemple 7.4 *Soit* L_n *le langage fini formé des mots* w *tels que* $|w|_a + 2|w|_b = n$.
a) Écrire les premiers termes $L_0,L_1,L_2\cdots$.
b) Calculer $|L_n|$ *à l'aide d'une récurrence simple.*
c) Montrer que $SG = \sum_n |L_n|t^n = (t+t^2)^* = \frac{1}{1-t-t^2}$.
d) Faire le lien avec le nombre de pavages d'un rectangle $2\times n$ *par des dominos* 2×1 *([?] pp 321) comment coder les pavages, les énumérer, les générer.*
e) À l'aide des décalages, former l'automate qui reconnait la série S.

On a un analogue parfait de ce qui se passe pour les rationnels positifs. Plus précisément :

Exercice 7.5 *A) On considère les arbres* $1-2$ *qui sont les arbres à* 1 *ou deux fils.*
À chaque arbre $1-2$, *dont les noeuds internes sont signés par "+" s'ils ont deux fils et "*$()^{-1}$*" s'ils en ont un on fait correspondre une fraction (i.e. son évaluation avec les feuilles en* 1*) donnée par la règle récursive*

$$ev(\bullet) = 1;\ ev((\mathcal{A}_1,\mathcal{A}_2)) = ev((\mathcal{A}_1) + ev(\mathcal{A}_2);\ ev((\mathcal{A})) = \frac{1}{ev(\mathcal{A})}$$

montrer que l'ensemble des valeurs obtenues est $\mathbb{Q}_+^*$. *Est-ce que la représentation est unique ? Est-ce qu'elle englobe les fractions continues ? Comment caractériser les arbres qui les donnent ?*
B) On considère les séries sur un alphabet A *(i.e. fonctions* $A^* \to k$ *où* k *est un semi-anneau (i.e. suffisant pour faire la calcul matriciel).*
a) Montrer que les conditions suivantes sont équivalentes :
i) La série S *est l'évaluation d'une expression rationnelle.*
ii) La série S *est combinaison linéaire d'un ensemble de séries* $S_1,S_2,\cdots S_n$ *qui est (linéairement) stable par décalages soit*

$$(\forall x \in A)(\forall i \in [1..n])(x^{-1}S_i = \sum_{0\leq j\leq n} \mu_{i,j}(x)S_j$$

iii) Il existe $\lambda \in K^{1\times n}$, $\mu : A \to K^{n\times n}$,$\gamma \in K^{1\times n}$ *tels que pour tout* $w \in A^*$, $(S,w) = \lambda\mu(w)\gamma$ *(où* $\mu()$ *dénote encore l'extention de* μ *à* A^**).*

Lorsque l'on a une partie $X \in A^*$, on peut se demander :
Quel est le langage $L(X)$ engendré par X ?
c'est à dire les suites finies d'instructions (i.e. le sous-monoïde engendré). On a $L(X) = \sum_{n\geq 0} X^n$ à coefficients dans $\mathbb{B}$. La même somme à coefficients dans $\mathbb{N}$ contient plus d'informations (soit le nombre de façons d'obtenir w comme produit de facteurs dans X).
Automates. Automates à multiplicité (notion de coût). Comportement d'un automate. Séries (exemples), rationnelles.
Passage SGO $\leftrightarrow$ Aut $\leftrightarrow$ Exp. rat.
Exemples de $\mathbb{N}$ et $\mathbb{Z}$ automates.
Séries génératrices (rationnelles -arbres de Fibonacci- et non rationnelles -arbres binaires, chemins de Dyck-). Résolution des premières récurrences, décalage et Δ. Complexité du comptage des boucles. Arbres $1-2$.

Références

[1] Cohen H., *A Course in Computational Algebraic Number Theory*. Springer (1993)

[2] Char B.W., Geddes K.O., Gonnet G.H., ali.., *Maple V Library Reference Manual*, Springer (1992).

[3] Char B.W., Geddes K.O., Gonnet G.H., ali.., *Maple V Language Reference Manual*, Springer (1992).

[4] Davenport J., Siret Y., Tournier E., *Calcul formel*, Masson (1986)

[5] Demazure M., Cours d'algèbre : Divisiilité, Primalité, codes. Cassini (1997).

[6] von zur Gathen J. and Gerahrd J. Modern Computer Algebra. Cambridge (1999).

[7] Knuth D., *The art of computer programming* Tome I. Addison-Wesley (1981)

[8] Knuth D., *The art of computer programming* Tome II. Addison-Wesley (1981)

[9] Naudin P., Quitté C., *Algorithmique Algébrique* Masson (1992)