Table des matières

— ∘ —

Chapitre 1

Notions fondamentales

Une tourniquette
Pour fair' la vinaigrette
Un bel aérateur
Pour bouffer les odeurs
Des draps qui chauffent
Un pistolet à gaufres
Un avion pour deux
Et nous serons heureux

B. Vian, *La complainte du progrès*

1 Notations et généralités

Les notions introduites dans ce chapitre ne sont que des rappels. On peut donc sans dommage passer au chapitre suivant. Toutefois, avant ces diverses définitions, voici un certain nombre de conventions typographiques que j'ai essayé de respecter dans ce rapport.

Un ensemble est désigné par une lettre majuscule, ainsi qu'un monoïde, dont la multiplication (interne) est notée par un point. Un semi-anneau est noté par une majuscule ajourée ($\mathbb{K}$), son addition et sa multiplication sont notées respectivement $\oplus$ et $\otimes$, sauf si l'instance de semi-anneau qu'on considère a des lois usuellement désignées par d'autres symboles. Les éléments de ces structures sont notés par des minuscules.

L'action (à droite) d'un élément x d'un monoïde sur un élément p d'un ensemble est notée $p \cdot x$. De même, l'action à gauche est notée $x \cdot p$; le contexte permet de différencier ces deux opérations.

Les fonctions sont désignées par des minuscules grecques.

Les automates et les graphes sont notés par des majuscules « calligraphiées ». La majuscule $\mathcal{L}$ désigne un langage. Les expressions rationnelles sont désignées par des majuscules « droites ».

Si X est un ensemble, on note $\mathcal{P}(X)$ l'ensemble des parties de X :

$$\mathcal{P}(X) = \{Y \mid Y \subseteq X\}.$$

Une **relation** α sur $X \times Y$ est un sous-ensemble de $X \times Y$. On note $x\alpha = \{y \mid (x,y) \in \alpha\}$. Une relation est une **fonction** si pour tout x dans X, il existe au plus un élément y dans Y tel que (x,y) appartient à α; l'élément y est alors appelé image de x par α et on note $y = x\alpha$[1]. Toute relation de X dans Y peut être vue comme une fonction de X dans $\mathcal{P}(Y)$.

On note Y^X l'ensemble des fonctions de X dans Y. Si X est un ensemble fini, une telle fonction peut être vue comme un vecteur. Le **support** d'une fonction α de Y^X, noté $\mathsf{Supp}(\alpha)$, est l'ensemble des éléments de X qui ont une image par α. Une **application** est une fonction dont le support est X.

Dans certains cas, il est plus commode de travailler avec des applications. On adjoint alors à Y un zéro (0_Y) et, à toute fonction α de Y^X, on associe l'application α' de $(Y \cup \{0_Y\})^X$ qui est égale à α sur le support de α et dont l'image est 0_Y ailleurs. Dans ce contexte, le support de α' est l'ensemble des éléments de X dont l'image est différente de 0_Y par α'.

— ∘ —

2 Graphes orientés

Un automate est avant tout un graphe orienté. Nous allons donc présenter ces objets.

DÉFINITION 1.1 *Un **graphe orienté** est un ensemble de sommets (Q) reliés par un ensemble de flèches ou arcs (orientés). Chaque arc est désigné par un couple formé de son sommet de départ et de celui d'arrivée. Formellement un graphe orienté $\mathcal{G}$ est donc un couple $\langle Q,E \rangle$ tel que E est un sous-ensemble de $Q \times Q$. Le graphe $\mathcal{G}$ est fini si Q est un ensemble fini.*

DÉFINITION 1.2 *Soit $\mathcal{G} = \langle Q,E \rangle$ un graphe orienté. Un **sous-graphe** de $\mathcal{G}$ est un graphe $\mathcal{G}' = \langle Q',E' \rangle$ tel que $Q' \subseteq Q$ et $E' \subseteq E \cap Q' \times Q'$.*

DÉFINITION 1.3 *Soit $\mathcal{G} = \langle Q,E \rangle$ un graphe orienté. Soit n un entier positif. Un **chemin** de $\mathcal{G}$ de longueur n est un $(n+1)$-uplet de sommets $(p_0,p_1,\ldots,p_n)$ tel que, pour tout i dans $[1;n]$, (p_{i-1},p_i) est un arc de $\mathcal{G}$. Le sommet p_0 est le **sommet de départ** du chemin, p_n est le **sommet d'arrivée**. Un chemin est un circuit (ou une **boucle**) s'il est de longueur non nulle et que $p_0 = p_n$. C'est un **circuit élémentaire** si, pour tout $i < j$ dans $[0;n]$, $p_i = p_j$ entraîne $i = 0$ et $j = n$.*

1. On note la fonction *à droite* de l'élément sur lequel elle s'applique (par exemple $x\alpha$ est l'image de x par la fonction α). Ceci permet (entre autre) de noter $\alpha\beta$ la fonction qui consiste à appliquer d'abord α puis β.

DÉFINITION 1.4 *Un graphe orienté est un* ***graphe acyclique*** *s'il ne contient aucune boucle. Un graphe orienté est un* ***graphe fortement connexe*** *si, pour tout couple de sommets (p,q), il existe un chemin de p à q. Une* ***composante fortement connexe*** *d'un graphe orienté est un sous-graphe fortement connexe maximal. Une* ***pelote*** *est une composante fortement connexe non triviale, c'est-à-dire contenant au moins un arc.*

DÉFINITION 1.5 *Soit $\mathcal{G} = \langle Q,E \rangle$ un graphe orienté. Soit $\overline{E} = \{(p,q) \mid (q,p) \in E\}$. Le graphe $\mathcal{G}$ est* ***connexe*** *si le graphe $\langle Q,E \cup \overline{E} \rangle$ est fortement connexe. Une* ***composante connexe*** *d'un graphe orienté est un sous-graphe connexe maximal.*

EXEMPLE 1.1 Le graphe présenté figure 1 contient trois composantes fortement connexes : $\langle \{p\},\{(p,p)\} \rangle$, $\langle \{q\},\emptyset \rangle$ et $\langle \{r\},\{(r,r)\} \rangle$; la première et la troisième sont des pelotes. D'autre part, le graphe, bien qu'il ne soit pas fortement connexe, est connexe.

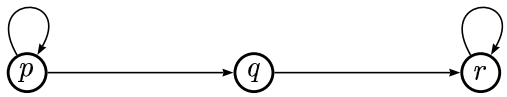

FIG. 1 – *Un graphe orienté à trois sommets*

DÉFINITION 1.6 *Un graphe $\mathcal{G} = \langle Q,E \rangle$ est* ***étiqueté*** *par un ensemble X s'il existe une application de E dans X. L'image d'un arc e par cette application est appelée* ***étiquette*** *de E. On notera alors $\mathcal{G} = \langle Q,E' \rangle$, avec $E' = \{(p,x,q) \mid x \in X$ étiquette de $(p,q) \in E\}$.*

DÉFINITION 1.7 *Soit $\mathcal{G} = \langle Q,E \rangle$ et $\mathcal{H} = \langle R,F \rangle$ deux graphes. Une application μ de Q dans R est un* ***morphisme de graphes*** *de $\mathcal{G}$ dans $\mathcal{H}$ si, quel que soit (p,q) dans E, $(p\mu,q\mu)$ appartient à F. Par extension, on dit que $(p\mu,q\mu)$ est l'image de (p,q) par μ. Si $\mathcal{G}$ et $\mathcal{H}$ sont des graphes étiquetés, l'application μ est un morphisme de $\mathcal{G}$ dans $\mathcal{H}$ si, quel que soit (p,x,q) dans E, $(p\mu,x,q\mu)$ appartient à F.*

— ∘ —

3 Structures algébriques

3.1 Monoïdes

DÉFINITION 1.8 *Un ensemble X, muni d'une loi associative et qui contient un élément neutre noté 1_X est un* ***monoïde.***[2] *On appelle généralement cette loi la multiplication du monoïde. Lorsqu'on veut préciser que X est muni de la loi « . », on désigne le monoïde par $(X,.)$.*

2. Une telle structure sans élément neutre est appelée semi-groupe.

Évidemment, les axiomes de monoïde sont beaucoup plus faibles que ceux de groupe. Toutefois, l'associativité est une contrainte forte qui conduit les monoïdes à avoir des structures très particulières (voir [40, 52]).

Un monoïde peut contenir un élément absorbant. On appelle alors celui-ci le zéro du monoïde.

Dans la plupart des cas, les ensembles classiques munis d'une loi vérifient les axiomes de monoïde. Ainsi, $(\mathbb{N},+)$, $(\mathbb{N},*)$, $(\mathbb{Z},*)$, $(\mathcal{M}_n(\mathbb{R}),*)$, *etc.* sont des monoïdes. Les groupes sont eux aussi des monoïdes.

DÉFINITION 1.9 *Soit $(M,.)$ un monoïde. Pour tout couple (x,y) d'éléments de M, le* ***quotient à gauche*** *de x par y noté $y^{-1}x$ est l'ensemble $\{z \in M \mid y.z = x\}$. Le quotient à gauche d'un sous-ensemble de M par y est l'union des quotients des éléments du sous-ensemble par y.*

DÉFINITION 1.10 *Soit M un monoïde et A un ensemble de générateurs de M. Le* ***graphe de Cayley*** *(droit) de M par rapport à A est le graphe étiqueté $\langle M,E \rangle$, où*

$$E = \{(x,a,y) \in M \times A \times M \mid y = x.a\}.$$

EXEMPLE 1.2 Dans la suite, on utilisera beaucoup les monoïdes finis. Soit M_1 le monoïde donné par la table ci-dessous. On note 1 pour 1_{M_1} et 0 pour 0_{M_1}.

.	1	x	y	t	0
1	1	x	y	t	0
x	x	x	0	0	0
y	y	t	y	t	0
t	t	t	0	0	0
0	0	0	0	0	0

Quelques quotients à gauche de ce monoïde :

$$y^{-1}t = \{x,t\}, \qquad x^{-1}0_{M_1} = \{y,t,0_{M_1}\}, \qquad \text{et} \qquad x^{-1}t = \emptyset.$$

Les éléments x et y engendrent le monoïde M_1. Le graphe de Cayley de M_1 par rapport à ces éléments est représenté figure 2.

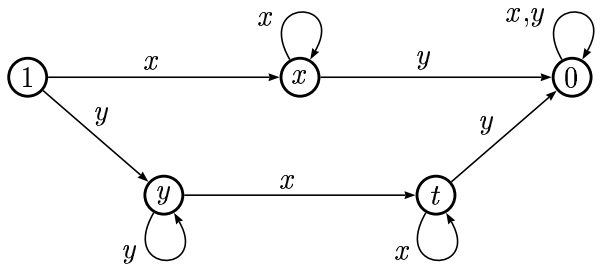

FIG. 2 – *Graphe de Cayley de M_1.*

DÉFINITION 1.11 *Soit $\sim$ une équivalence sur un monoïde M. Cette équivalence est* ***régulière à droite*** *(on dit aussi que c'est une congruence droite) si*

$$\forall x,y \in M \; x \sim y \Rightarrow \forall z \; x.z \sim y.z.$$

De même, c'est une congruence gauche, ou une relation d'équivalence régulière à gauche si

$$\forall x,y \in M \; x \sim y \Rightarrow \forall z \; z.x \sim z.y.$$

Si une relation d'équivalence est régulière à gauche et à droite, c'est une congruence. Les classes de M modulo cette équivalence forment alors un monoïde.

DÉFINITION 1.12 *Soit X un ensemble et M un monoïde. Une application μ de M dans X^X est une* ***action*** *à droite de M sur X si:*

$$\begin{aligned} \forall p \in X, \forall x,y \in M, \qquad p(1_M\mu) &= p, \\ (p(x\mu))(y\mu) &= p((x.y)\mu). \end{aligned}$$

On note alors $p \cdot x = p(x\mu)$. Symétriquement, une telle application est une action à gauche de M sur X si:

$$\begin{aligned} \forall p \in X, \forall x,y \in M, \qquad p(1_M\mu) &= p, \\ (p(x\mu))(y\mu) &= p((y.x)\mu). \end{aligned}$$

On note alors $x \cdot p = p(x\mu)$.

— ∘ —

Une famille de monoïdes tient une place particulière parmi les monoïdes; ce sont les monoïdes libres, et, en ce qui nous concerne, les monoïdes libres finiment engendrés.

DÉFINITION 1.13 *On désigne par* ***alphabet*** *un ensemble fini A non vide de symboles appelées* ***lettres****. On peut former des* ***mots*** *par concaténation de ces lettres. L'opération de concaténation, associative, fait de l'ensemble des mots sur A, noté A^*, un monoïde: le* ***monoïde libre engendré par*** *A. Le mot vide, élément neutre de ce monoïde est noté 1_{A^*}. On notera A^+ l'ensemble des mots de A^* différents du mot vide. Un sous-ensemble de A^* est appelé un* ***langage****. La* ***longueur d'un mot*** *est le nombre de lettres qu'il comporte; on note la longueur d'un mot u par $|u|$, de même, pour toute lettre a de A, on note le nombre d'occurrences de a dans u, $|u|_a$. On notera par ailleurs u_i la i-ème lettre du mot u.*

La métaphore linguistique qui guide cette définition ne doit pas induire en erreur. Il n'est *a priori* nullement question de sémantique dans la définition des mots. Ainsi, sur l'alphabet latin des majuscules (non accentuées) qui compte vingt-six éléments, $JRASKDFW$ est un mot, bien qu'on puisse douter qu'il ait un sens dans une des langues utilisant cet alphabet.

La taille des alphabets qu'on considère peut varier selon les emplois. Ainsi, traditionnellement, en informatique, l'alphabet a deux lettres, 0 et 1 (nous utiliserons plutôt a et b

pour ne pas confondre avec d'autres usages de 0 et 1). En bio-informatique, il compte généralement 4 lettres (les bases du code génétique) ou 20 (les acides aminés). En linguistique, il peut en compter des centaines (alphabets, sons, nature des mots, *etc.*).

On peut définir sur le monoïde libre, à cause de l'unicité de la décomposition de chaque élément, certaines notions qui n'auraient pas de sens dans d'autres structures.

DÉFINITION 1.14 *Soit $u = u_1u_2\dots u_k$ un mot de A^*. L'**image miroir** de u est le mot $u_ku_{k-1}\dots u_1$. L'image miroir d'un langage est l'ensemble des images miroir de ses éléments.*

Ordres et distances sur le monoïde libre

DÉFINITION 1.15 *Soit u et v deux mots de A^*.*

- *u est un **préfixe** de v s'il existe w dans A^* tel que $v = u.w$.*
- *u est un **suffixe** de v s'il existe w dans A^* tel que $v = w.u$.*
- *u est un **facteur** de v s'il existe w et t dans A^* tels que $v = w.u.t$.*

On peut, à partir de ces notions, définir des relations d'ordre partiel sur le monoïde libre. Ainsi, un mot u est plus petit qu'un mot v selon la relation « préfixe » si et seulement si u est un préfixe de v, et on peut définir de la même manière des relations à l'aide du suffixe ou du facteur. On préfère parfois utiliser des relations d'ordre total sur A^*; nous allons ici en définir deux.

DÉFINITION 1.16 *On suppose l'alphabet A totalement ordonné. L'**ordre lexicographique** sur A^* est défini comme suit :*

- *Le mot vide est inférieur à tout mot de A^+.*
- *Quels que soient $u = a.u'$ et $v = b.v'$,*

$$u <_{\mathsf{lex}} v \Leftrightarrow ou \begin{cases} a < b, \\ a = b \text{ et } u' <_{\mathsf{lex}} v'. \end{cases}$$

*L'**ordre radiciel** (ou ordre militaire) est défini sur A^* par :*

$$u <_{\mathsf{rad}} v \Leftrightarrow ou \begin{cases} |u| < |v|, \\ |u| = |v| \text{ et } u <_{\mathsf{lex}} v. \end{cases}$$

REMARQUE 1.1 Pour l'ordre radiciel, un mot n'a qu'un nombre fini de mots qui lui sont inférieurs, ce qui n'est pas le cas pour l'ordre lexicographique.

Le monoïde A^* peut être muni d'une distance;

DÉFINITION 1.17 *Soit u et v deux mots de A^*. On note $u \wedge v$ le plus grand préfixe commun à u et v.*

DÉFINITION 1.18 *La **distance préfixe** est définie sur A^* par :*

$$d_{\mathsf{pref}}(u,v) = |u| + |v| - 2|u \wedge v|.$$

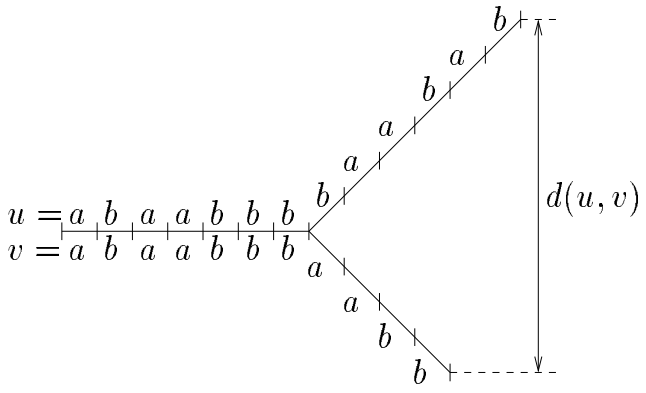

FIG. 3 – *Distance préfixe.*

EXEMPLE 2 La distance préfixe peut être vue comme l'indique la figure 3.

— ∘ —

3.2 Semi-anneaux

DÉFINITION 1.19 *Un* ***semi-anneau*** *est un ensemble* $\mathbb{K}$*, muni de deux lois associatives et d'un élément neutre pour chaque loi. La première loi* ($\oplus$) *est commutative, la seconde* ($\otimes$) *est distributive sur la première. On les appellera respectivement addition et multiplication. L'élément neutre de l'addition* ($0_{\mathbb{K}}$) *doit de plus être absorbant pour la multiplication. Dans le cas où l'on souhaite préciser quelles sont les lois du semi-anneau, on note* $(\mathbb{K}, \oplus, \otimes)$*. On note* $\mathbb{K}_*$ *l'ensemble des éléments de* $\mathbb{K}$ *différents de* $0_{\mathbb{K}}$*.*

EXEMPLE 3 Les nombres entiers positifs, ou naturels, $(\mathbb{N}, +, *)$ forment un semi-anneau : les deux lois sont associatives, l'addition est commutative et la multiplication est distributive sur l'addition. Comme la multiplication est elle aussi commutative, on dit que $\mathbb{N}$ est un semi-anneau commutatif. L'ensemble $\mathbb{N}$ n'est un groupe ni par rapport à son addition ni par rapport à sa multiplication. $\mathbb{N}$ peut cependant être plongé dans un anneau (les entiers relatifs $\mathbb{Z}$) et même dans un corps (les rationnels $\mathbb{Q}$). On verra toutefois qu'on ne peut pas faire de même avec n'importe quel semi-anneau.

En revanche, $(\mathbb{N}, \mathsf{max}, +)$ n'est pas un semi-anneau, bien que les deux lois soient associatives et que la seconde soit distributive sur la première; l'élément neutre de max, 0, n'est pas absorbant pour $+$, puisque c'est aussi son élément neutre.

DÉFINITION 1.20 *Soit* $(M, .)$ *un monoïde. Un élément* x *de* M *tel que* $x.x = x$ *est appelé* ***idempotent****. Si chaque élément de* M *est idempotent,* M *est un monoïde idempotent. Un semi-anneau* $(\mathbb{K}, \oplus, \otimes)$ *est idempotent si* $(\mathbb{K}, \oplus)$ *est un monoïde idempotent.*

REMARQUE 1.2 Un élément idempotent d'un monoïde M différent de 1_M n'est pas inversible. En effet, soit x un élément idempotent et y inverse de x, alors $x = x.x.y = x.y = 1_M$.

Un monoïde idempotent non trivial ne peut donc pas être plongé dans un groupe. Les semi-anneaux idempotents ne peuvent donc en particulier pas être plongés dans des anneaux et encore moins dans des corps.

EXEMPLE 4 Un autre exemple connu est le semi-anneau de Boole, c'est-à-dire l'ensemble {0,1} muni des lois :

$\oplus$	0	1
0	0	1
1	1	1

$\otimes$	0	1
0	0	0
1	0	1

On peut voir ce semi-anneau comme l'ensemble {VRAI,FAUX} muni des lois « OU » et « ET ». Pour définir un semi-anneau à deux éléments en respectant les axiomes, le seul choix possible porte sur la valeur de $1 \oplus 1$. Si on fixe $1 \oplus 1 = 1$, on obtient le semi-anneau de Boole, sinon $1 \oplus 1 = 0$ et le semi-anneau construit est en fait le corps $\mathbb{Z}/2\mathbb{Z}$. Ce sont les représentants de deux types de semi-anneaux. D'une part, $\mathbb{Z}/2\mathbb{Z}$ fait partie des semi-anneaux qu'on peut plonger dans un corps (c'est un corps lui-même), d'autre part, le semi-anneau de Boole est un semi-anneau non-plongeable dans un corps (c'est plus particulièrement un semi-anneau idempotent).

REMARQUE 1.3 Soit $(M,.)$ un monoïde. On définit la multiplication de deux sous-ensembles X et Y de M par $X.Y = \{x.y \mid x \in X \text{ et } y \in Y\}$. Alors $(\mathcal{P}(M), \cup, .)$ est un semi-anneau idempotent. Dans ce qui suit, il arrivera que l'identification soit faite entre un monoïde et le semi-anneau des parties qui lui correspond.

Nous aurons besoin de factoriser des éléments de semi-anneaux. Cette factorisation n'est pas toujours unique, sauf dans un semi-anneau **factoriel**. Ce n'est pas exactement de cette propriété dont nous aurons besoin.

DÉFINITION 1.21 *Soit $\mathbb{K}$ un semi-anneau. Un **idéal** (droit) de $\mathbb{K}$ est un sous-ensemble $\mathcal{I}$ tel que $\mathcal{I} \oplus \mathcal{I} \subseteq \mathcal{I}$ et $\mathcal{I} \otimes \mathbb{K} \subseteq \mathcal{I}$. Un idéal est finiment engendré s'il existe un ensemble fini X dans $\mathbb{K}$ tel que $\mathcal{I} = X \otimes \mathbb{K}$. Un idéal $\mathcal{I}$ est **principal** s'il existe un élément x de $\mathbb{K}$ tel que $\mathcal{I} = x \otimes \mathbb{K}$. On dira qu'un semi-anneau est un **semi-anneau principal** si, pour tout idéal $\mathcal{I}$, il existe un unique idéal principal minimum qui contient $\mathcal{I}$.*

Soit $\mathbb{K}$ un semi-anneau principal, X un ensemble d'éléments de $\mathbb{K}$ et $\mathcal{I}$ le plus petit idéal principal qui contient X. Tout élément z qui engendre l'idéal $\mathcal{I}$ est un pgcd *de X.*

REMARQUE 1.4 D'un point de vue effectif, la non unicité du pgcd peut poser un problème. Nous verrons le moment voulu comment le résoudre. On peut dès à présent remarquer qu'il est possible de passer d'un pgcd à un autre par multiplication à droite, puisque chacun appartient à l'idéal engendré par l'autre.

EXEMPLE 5 Le semi-anneau $(\mathbb{R}_+ \cup \{-\infty\}, \max, +)$ est principal. En effet, pour tout ensemble X, l'adhérence (pour la topologie usuelle) de l'idéal engendré par X est l'idéal principal engendré par $\inf\{x \in X \mid x \neq -\infty\}$.

Le semi-anneau $(\mathbb{R}\cup\{-\infty\}, \max, +)$ est lui aussi principal. Les deux seuls idéaux de ce semi-anneau sont le semi-anneau lui-même, engendré par n'importe quel élément différent de $-\infty$ et $\{-\infty\}$.

En revanche, le semi-anneau $(\mathcal{P}(B^*), \cup, .)$, avec $B = \{a,b\}$ n'est pas principal. Par exemple, soit $x = \{a,b,a^2,ab,ba,aba\}$ et $y = \{a,b,ab,a^2,ba,b^2,aba,ab^2\}$. Ces deux ensembles admettent $\{1_{B^*},a\}$ et $\{a,b,ab\}$ pour facteurs maximaux gauches communs :

$$x = \{1_{B^*},a\}.\{a,b,ba\} \qquad x = \{a,b,ab\}.\{1_{B^*},a\}$$
$$y = \{1_{B^*},a\}.\{a,b,ba,bb\} \qquad y = \{a,b,ab\}.\{1_{B^*},a,b\}$$

Aucun de ces facteurs ne divise l'autre, il n'y a donc pas unicité de l'idéal principal minimal qui contient x et y.

DÉFINITION 1.22 *Soit $(\mathbb{K},\oplus,\otimes)$ un semi-anneau. Pour tout x dans $\mathbb{K}$, pour tout n dans $\mathbb{N}$, x^n est défini inductivement par $x^0 = 1_{\mathbb{K}}$ et $x^n = x \otimes x^{n-1}$. On pose la quantité suivante, pour n dans $\mathbb{N}$:*

$$X_n = \bigoplus_{k=0}^{n} x^k$$

Si X_n admet une limite dans $\mathbb{K}$ lorsque n tend vers l'infini, cette limite est appelée ***étoile*** *de x et notée x^*. Dans ce cas, on note*

$$x^* = \bigoplus_{k=0}^{\infty} x^k, \quad x^+ = \bigoplus_{k=1}^{\infty} x^k.$$

REMARQUE 1.5 Puisqu'on parle de limite dans $\mathbb{K}$, ce semi-anneau est implicitement muni d'une topologie. Il peut, par défaut, être muni de la topologie discrète, mais il est plus naturel de munir certains semi-anneaux ($\mathbb{R}$,$\mathbb{Q}$, ...) de leur topologie habituelle. Le choix de celle-ci n'est pas sans conséquence sur la définition de l'étoile.

EXEMPLE 6 Dans $\mathbb{Q}$, l'étoile de $1/2$ est la limite, lorsque n tend vers l'infini, de la somme :

$$X_n = \sum_{i=0}^{n} \left(\frac{1}{2}\right)^i = 2 - \left(\frac{1}{2}\right)^n.$$

Cette suite converge pour la topologie habituelle mais pas pour la topologie discrète.

REMARQUE 1.6 L'étoile d'un élément x d'un monoïde M est toujours définie. En effet les sous-ensembles X_n forment dans ce cas une suite croissante dont la limite est :

$$X = \{y \in M \mid \exists n, y = x^n\}.$$

Plus généralement, l'étoile de n'importe quel sous-ensemble de M est définie.

DÉFINITION 1.23 *Soit $\mathbb{K}$ un semi-anneau et P un sous-ensemble de $\mathbb{K}$. Un élément x de $\mathbb{K}$ est* ***rationnel*** *par rapport à P s'il peut être obtenu à partir d'éléments de P et des opérations d'addition, de multiplication et d'étoile.*

REMARQUE 1.7 L'ensemble des éléments de $\mathbb{R}$ rationnels par rapport à $\mathbb{Z}$ n'est pas $\mathbb{Q}$! Avec la topologie usuelle, le seul élément de $\mathbb{Z}$ auquel on peut appliquer l'opération étoile est 0, donc l'ensemble des éléments de $\mathbb{R}$ rationnels par rapport à $\mathbb{Z}$ est $\mathbb{Z}$.

En revanche, munissons $\mathbb{Z}$ de la norme 2-adique : pour tout entier n qui s'écrit $n = 2^k m$, avec $\mathsf{pgcd}(2,m) = 1$, $|n|_2 = 2^{-k}$. Alors l'ensemble des éléments de $\mathbb{Q}_2$ (clôture 2-adique de $\mathbb{Q}$) rationnels par rapport à $\mathbb{Z}$ contient par exemple $-1/3$, car la suite $\sum_{k=0}^{n} 4^k = \frac{4^{(n+1)}-1}{3}$ est une suite de Cauchy, donc converge dans $\mathbb{Q}_2$ et 4^* vérifie $1 + 4.4^* = 4^*$, donc $4^* = -1/3$.

Nous emploierons parfois le terme de semi-module. Il s'agit de la généralisation du concept de module.

DÉFINITION 1.24 *Soit $\mathbb{K}$ un semi-anneau, V est un $\mathbb{K}$-**semi-module** (à gauche) si V est muni d'une loi $\oplus$ telle que $(V,\oplus)$ est un monoïde d'élément neutre 0_V et s'il existe une action (à gauche) de $(\mathbb{K},\otimes)$ sur V (notée par simple concaténation d'un élément de $\mathbb{K}$ avec un élément de V) telle que :*

$$\begin{aligned} \forall x \in V,\ 0_{\mathbb{K}}\, x &= 0_V \\ \forall k,k' \in \mathbb{K}, \forall x,y \in V,\ (k \oplus k')\, x &= k\, x \oplus k'\, x \\ k\,(x \oplus y) &= k\, x \oplus k\, y. \end{aligned}$$

*Un semi-module est dit finiment engendré, ou de **type fini**, s'il existe un ensemble fini $\{x_1,x_2,\ldots,x_n\}$ tel que, pour tout x, il existe $(k_1,k_2,\ldots,k_n)$ dans $\mathbb{K}^n$ tel que*

$$x = \bigoplus_{r=1}^{n} k_r x_r.$$

Nous nous intéresserons aussi à des sous-ensembles particuliers de semi-modules : les faisceaux finis de droites, que nous appellerons aussi $\mathbb{K}$-cônes finiment engendrés.

DÉFINITION 1.25 *Soit V un semi-module et X un sous-ensemble de V. L'ensemble X est un $\mathbb{K}$-**cône** finiment engendré s'il existe un ensemble fini d'éléments de V, $\{x_i \mid i \in I\}$, tel que :*

$$X = \bigcup_{i \in I} \mathbb{K} x_i.$$

— ∘ —

3.3 Polynômes et séries formelles

Par souci de simplification, on définit ici uniquement les polynômes et séries formelles sur A^*. On trouvera une étude plus complète des séries sur un monoïde dans [55].

DÉFINITION 1.26 *Soit A un alphabet et $(\mathbb{K},\oplus,\otimes)$ un semi-anneau. On appelle semi-anneau des **series** (formelles) sur A^* à coefficients (ou à multiplicité) dans $\mathbb{K}$, qu'on note $\mathbb{K}\langle\langle A^* \rangle\rangle$,*

l'ensemble des applications de A^* dans $\mathbb{K}$ muni des opérations :

$$\textit{d'addition : } \alpha \oplus \beta : x \mapsto x\alpha \oplus x\beta,$$
$$\textit{et de multiplication : } \alpha \otimes \beta : x \mapsto \bigoplus_{y.z=x} y\alpha \otimes z\beta.$$

Pour une série α, on utilise de préférence la notation suivante : pour tout mot u de A^*, $\langle \alpha,u \rangle = u\alpha$. On note formellement la série comme une somme infinie :

$$\alpha = \bigoplus_{u \in A^*} \langle \alpha,u \rangle u.$$

Si on identifie un scalaire k de $\mathbb{K}$ à la série $k\,1_{A^*}$, on définit du même coup la multiplication d'une série par un scalaire. Les séries sont donc un $\mathbb{K}$-semi-module.

Remarque 1.8 Comme on se place dans le monoïde libre, la somme effectuée dans la définition de la multiplication est une somme finie. On peut définir les séries sur d'autres monoïdes que le monoïde libre. Toutefois, si celui-ci n'est pas gradué, c'est-à-dire s'il existe des éléments admettant un nombre infini de factorisations, la multiplication peut ne pas être définie partout. Les séries ne forment alors pas un semi-anneau.
La multiplication des séries faisant intervenir la multiplication du monoïde libre, elle n'est pas commutative, même si le semi-anneau l'est (sauf si l'alphabet n'a qu'une lettre).

Définition 1.27 *Le **support d'une série** s de $\mathbb{K}\langle\langle A^* \rangle\rangle$, noté $\mathsf{Supp}(s)$ est l'ensemble des mots dont les coefficients sont non nuls :*

$$\mathsf{Supp}(s) = \{u \in A^* \mid \langle s,u \rangle \neq 0_{\mathbb{K}}\}.$$

*Une série dont le support est fini est un **polynôme**. L'ensemble des polynômes forme un sous-semi-anneau de $\mathbb{K}\langle\langle A^* \rangle\rangle$ noté $\mathbb{K}\langle A^* \rangle$.*

Remarque 1.9 L'ensemble des polynômes en variables commutatives est généralement noté $\mathbb{K}[A]$, où A est l'alphabet de variables. On préfère utiliser la notation $\mathbb{K}\langle M \rangle$, où M est le monoïde des variables. Dans le cas des variables commutatives, on noterait le semi-anneau des polynômes $\mathbb{K}\langle A^{\oplus} \rangle$, où $A^{\oplus}$ est le monoïde *commutatif* libre engendré par A. Cette notation inclut non seulement les variables, mais les relations éventuelles qui existent entre elles.

Définition 1.28 *On appelle **terme constant de la série** s et on note $\mathsf{c}(s)$ le coefficient du mot vide dans s : $\langle s,1_{A^*} \rangle$. La **partie propre d'une série** s est la série s_p définie par :*

$$\langle s_p,1_{A^*} \rangle = 0_{\mathbb{K}}\,, \quad \forall u \in A^+,\ \langle s_p,u \rangle = \langle s,u \rangle.$$

On peut donc écrire $s = \mathsf{c}(s)1_{A^*} \oplus s_p$.

Comme dans tout semi-anneau, on peut vouloir calculer l'étoile d'une série. La définition d'une telle quantité est fortement liée à la définition de l'étoile dans le semi-anneau $\mathbb{K}$:

PROPOSITION 1.1 *[8] L'étoile d'une série s de $\mathbb{K}\langle\langle A^*\rangle\rangle$ est définie si et seulement si l'étoile du terme constant de s est définie dans $\mathbb{K}$. On a alors l'égalité suivante :*

$$s^* = (\mathsf{c}(s)^*\, s_p)^*\, \mathsf{c}(s)^*.$$

REMARQUE 1.10 L'étoile d'une série propre est toujours définie, en effet :

$$\begin{aligned}\langle s_p^*, u\rangle &= \bigoplus_{\substack{u=v_1v_2\cdots v_n \\ v_1,v_2,\ldots,v_n\in A^*}} \langle s_p^*, v_1\rangle \otimes \ldots \otimes \langle s_p^*, v_n\rangle \\ &= \bigoplus_{\substack{u=v_1v_2\cdots v_n \\ v_1,v_2,\ldots,v_n\in A^+}} \langle s_p^*, v_1\rangle \otimes \ldots \otimes \langle s_p^*, v_n\rangle.\end{aligned}$$

Le membre droit de cette équation est une somme finie.

REMARQUE 1.11 Si l'étoile est toujours définie sur le semi-anneau $\mathbb{K}$, elle est d'après la proposition, toujours définie sur $\mathbb{K}\langle\langle A^*\rangle\rangle$. Ainsi, si $\mathbb{K}$ est le semi-anneau de Boole, on retrouve le cas particulier de la remarque 1.3, puisque $\mathbb{B}\langle\langle A^*\rangle\rangle$ est isomorphe à $\mathcal{P}(A^*)$.

DÉFINITION 1.29 *Le* ***quotient à gauche d'une série*** *s par un mot u de A^* est la série*

$$u^{-1}s = \bigoplus_{v\in A^*} \langle s, uv\rangle v.$$

Il n'est pas difficile de voir que le quotient ainsi défini est une action (à droite) des mots sur les séries.

— ∘ —

3.4 Ensembles et séries rationnels

DÉFINITION 1.30 *Soit M un monoïde. L'ensemble* $\mathrm{Rat}\, M$ *des* ***ensembles rationnels*** *de M est la clôture des ensembles finis de M par les opérations de produit, d'union et d'étoile. Ce qui revient à dire que les ensembles rationnels de M sont les éléments de $\mathcal{P}(M)$ rationnels par rapport aux ensembles finis. Si M est le monoïde libre, on parle de* ***langage rationnel****.*

DÉFINITION 1.31 *Le semi-anneau des* ***séries rationnelles*** $\mathbb{K}\mathrm{Rat}\, A^*$ *de $\mathbb{K}\langle\langle A^*\rangle\rangle$ est la clôture du semi-anneau des polynômes par les opérations d'addition, de multiplication et d'étoile, si cette dernière est définie.*

Les ensembles rationnels d'un monoïde M et les séries rationnelles forment des sous-semi-anneaux de $\mathcal{P}(M)$ et des séries formelles respectivement.

EXEMPLE 1.3 Soit $A = \{a,b\}$ un alphabet. Formons un langage rationnel dans le monoïde libre A^*. Le langage ab (en fait le singleton $\{ab\}$) est un langage fini, le langage $a+b$ aussi. Le langage $(a+b)^*$ est l'étoile d'un langage fini, donc il est rationnel. En fait, il s'agit de A^* tout entier. Le langage $\mathcal{L}_1 = (a+b)^*ab(a+b)^*$ est un produit de langages rationnels ; il

est donc aussi rationnel. Intuitivement ce langage contient tous les mots qui contiennent le facteur ab. Pour former un mot qui appartient à ce langage, on peut en effet mettre ce que l'on veut au début ou à la fin ($(a+b)^*$) à condition d'insérer ab au milieu.

On peut analyser un peu plus finement ce que représente cette description. Plaçons nous dans le cadre des séries à multiplicité dans $\mathbb{N}$. Le mot ab est alors vu comme un polynôme formé d'un seul monôme dont le coefficient est 1. La série $\chi_{A^*} = (a+b)^*$ est la série caractéristique de A^*, c'est-à-dire que pour tout mot u de A^*, $\langle \chi_{A^*}, u \rangle = 1$. La série $s_1 = (a+b)^*ab(a+b)^*$ est donc une série rationnelle. La multiplicité d'un mot u dans s_1 est le nombre de façons dont u se factorise en $u = v.ab.w$, c'est donc le nombre de facteurs ab qui apparaissent dans u.

— ∘ —

3.5 Ensembles reconnaissables

DÉFINITION 1.32 *Soit M un monoïde. Un sous-ensemble $\mathcal{L}$ de M est un* ***ensemble reconnaissable*** *(par morphisme) s'il existe un monoïde fini N, un morphisme φ de M dans N tel que $\mathcal{L} = (\mathcal{L}\varphi)\varphi^{-1}$ (en d'autres termes, le sous-ensemble $\mathcal{L}$ est l'image inverse par φ d'une partie de N). Un langage $\mathcal{L}$ de A^* est un* ***langage reconnaissable*** *si c'est un sous-ensemble reconnaissable de A^*.*

EXEMPLE 7.1 Soit $A = \{a,b\}$ et $N_3 = (\mathbb{Z}/3\mathbb{Z},+)$. Soit $\varphi : A^* \to N_3$ le morphisme défini par $a\varphi = 1$ et $b\varphi = -1$. L'image d'un mot de A^* dans N_3 par φ est donc la différence modulo 3 entre le nombre de a et le nombre de b. Le langage $\mathcal{L}_3 = \{-1,1\}\varphi^{-1}$ est un langage reconnaissable; c'est l'ensemble des mots de A^* dont le nombre de a est différent du nombre de b modulo 3.

EXEMPLE 1.4 Soit φ le morphisme de A^* dans le monoïde M_1 (présenté page 22) défini par $a\varphi = x$ et $b\varphi = y$. Un examen attentif (d'autres techniques nous permettront de le vérifier) nous permet de voir que :

$$\begin{aligned} 1_{M_1}\varphi^{-1} &= 1_{A^*}, & t\varphi^{-1} &= b^+a^+, \\ x\varphi^{-1} &= a^+, & 0_{M_1}\varphi^{-1} &= A^*abA^* = \mathcal{L}_1. \\ y\varphi^{-1} &= b^+, \end{aligned}$$

Le langage $\mathcal{L}_1$, image inverse de 0_{M_1} par φ est donc un langage reconnaissable de A^*.

— ∘ —

4 Automates

4.1 Automates sur un semi-anneau

DÉFINITION 1.33 *Un* ***automate $\mathcal{A}$ sur un semi-anneau*** $\mathbb{K}$ *est défini comme un quintuplet $\langle Q,\mathbb{K},E,I,T \rangle$, où Q est un ensemble fini d'****états****, E une matrice de $\mathbb{K}^{Q\times Q}$, I et T deux*

vecteurs (respectivement ligne et colonne) de $\mathbb{K}^Q$. E est la matrice de transition de $\mathcal{A}$, I et T sont respectivement les vecteurs initial et final de $\mathcal{A}$.
Les éléments des supports de E, I et T sont respectivements appelés ***transitions****, états initiaux et états finals (ou terminaux).*

DÉFINITION 1.34 *Le* ***graphe sous-jacent à un automate*** $\mathcal{A} = \langle Q,\mathbb{K},E,I,T \rangle$ *est le graphe orienté* $\mathcal{G}_\mathcal{A} = \langle Q, \mathsf{Supp}(E) \rangle$.

DÉFINITION 1.35 *Soit $\mathcal{A} = \langle Q,\mathbb{K},E,I,T \rangle$. Un chemin de $\mathcal{A}$ de longueur k est une suite d'états $(p_0,p_1,\ldots,p_k)$ telle que, pour tout i dans $[1;k]$, (p_{i-1},p_i) est une transition. L'étiquette d'un chemin $\mathcal{C}$ est l'élément $E_\mathcal{C} = E_{p_0,p_1} \otimes E_{p_1,p_2} \otimes \ldots \otimes E_{p_{k-1},p_k}$. Ce chemin est* ***réussi*** *si p_0 est un état initial et p_k est un état final. Le* ***calcul*** *correspondant à un chemin réussi $\mathcal{C}$ est $I_{p_0} \otimes E_\mathcal{C} \otimes T_{p_k}$. L'élément de $\mathbb{K}$* ***reconnu*** *par l'automate est la somme des calculs des chemins réussis de l'automate, si elle est définie. Deux automates sont* ***équivalents*** *s'ils reconnaissent le même élément de $\mathbb{K}$.*

DÉFINITION 1.36 *Un automate $\mathcal{A} = \langle Q,\mathbb{K},E,I,T \rangle$ est* ***normalisé*** *s'il ne comporte qu'un état initial i et un état final t avec $I_i = T_t = 1_\mathbb{K}$, que ces états sont distincts, et que, pour tout p dans Q, $E_{p,i} = E_{t,p} = 0_\mathbb{K}$.*

PROPOSITION 1.2 *Tout automate est équivalent à un automate normalisé.*

Démonstration. Soit $\mathcal{A} = \langle Q,\mathbb{K},E,I,T \rangle$ un automate. Soit i et t deux états qui n'appartiennent pas à Q. On pose $Q' = Q \cup \{i,t\}$ et on définit E' dans $\mathbb{K}^{Q' \times Q'}$ par :

$$E'_{p,q} = \begin{cases} E_{p,q} & \text{si } p,q \in Q \\ I_q & \text{si } p = i \text{ et } q \in Q \\ T_p & \text{si } q = t \text{ et } p \in Q \\ 0_\mathbb{K} & \text{si } p = t,\ q = i \text{ ou } (p,q) = (i,t) \end{cases}$$

L'automate $\mathcal{A}' = \{Q',\mathbb{K},E',i,t\}$ [3] est normalisé. Il y a une bijection entre les chemins réussis de $\mathcal{A}$ et ceux de $\mathcal{A}'$:

$$(p_0,\ldots,p_k) \longmapsto (i,p_0,p_1,\ldots,p_k,t)$$

De plus, le calcul correspondant à un chemin réussi de $\mathcal{A}$ et celui correspondant à son image dans $\mathcal{A}'$ sont égaux. La somme des calculs des deux automates est donc la même; ils sont équivalents. □

— ∘ —

Examinons le rapport entre les produits matriciels qu'on peut effectuer sur E, I ou T et les étiquettes des chemins.

Le produit $I \otimes T = \bigoplus_{p \in Q} I_p \otimes T_p$ est la somme des calculs de longueur 0 de l'automate.

3. Pour alléger l'écriture, on note i (*resp.* t) le vecteur caractéristique de i (*resp.* de t).

La matrice E représente les étiquettes des transitions, c'est-à-dire des chemins de longueur 1; le produit $I \otimes E \otimes T = \bigoplus_{p,q \in Q} I_p \otimes E_{p,q} \otimes T_q$ est donc la somme des calculs de longueur 1 de l'automate.

On peut généraliser cette constatation :

PROPOSITION 1.3 *Soit $\mathcal{A} = \langle Q, \mathbb{K}, E, I, T \rangle$ un automate. La somme des calculs de longueur k de l'automate est $I \otimes E^k \otimes T$. L'élément reconnu par l'automate, s'il est défini, est $I \otimes E^* \otimes T$.*

Démonstration. On montre par récurrence sur la longueur des chemins que $(E^k)_{p,q}$ est la somme des étiquettes des chemins de longueur k entre p et q. C'est trivialement vrai pour $k = 0$. Si le résultat est vrai pour k, tout chemin de p à q de longueur $k+1$ se décompose en un chemin de p à r, pour un certain état r, et une transition de r à q. La somme des étiquettes des chemins de longueur $k+1$ entre p et q est donc

$$\bigoplus_{r \in Q} (E^k)_{p,r} \otimes E_{r,q} = (E^{k+1})_{p,q},$$

ce qui montre le résultat. La somme des calculs de longueur k entre p et q est donc $I_p \otimes E^k_{p,q} \otimes T_q$ et la somme des calculs de longueur k de l'automate est

$$\bigoplus_{p,q \in Q} I_p \otimes (E^k)_{p,q} \otimes T_q = I \otimes E^k \otimes T.$$

La somme des calculs de l'automate est

$$\bigoplus_{k \in \mathbb{N}} I \otimes E^k \otimes T = I \otimes \left(\bigoplus_{k \in \mathbb{N}} E^k \right) \otimes T = I \otimes E^* \otimes T$$

□

PROPOSITION 1.4 *Les coefficients de l'étoile d'une matrice sont rationnels par rapport aux coefficients de la matrice.*

— ∘ —

4.2 Automates sur un monoïde

La définition d'un automate sur un monoïde découle de l'identification du monoïde M avec les singletons du semi-anneau $\mathcal{P}(M)$. On va donner explicitement les définitions que l'on obtient.

DÉFINITION 1.37 *Un **automate $\mathcal{A}$ sur un monoïde** M est défini comme un quintuplet $\langle Q, M, E, I, T \rangle$, où Q est un ensemble fini d'**états**, où E est une matrice de $(\mathrm{Rat}\, M)^{Q \times Q}$ et I et T des vecteurs de $(\mathrm{Rat}\, M)^Q$.*

Les chemins, étiquettes des chemins et calculs d'un automate sont définis de la même façon que dans le cas des semi-anneaux.

DÉFINITION 1.38 *Soit $\mathcal{A}$ un automate sur M. Un élément de M est* ***accepté*** *par $\mathcal{A}$ s'il appartient à un calcul de $\mathcal{A}$. L'élément de $\mathcal{P}(M)$ reconnu par $\mathcal{A}$ est l'***ensemble reconnu par l'automate***. L'addition du semi-anneau $\mathcal{P}(M)$ étant l'union, l'ensemble reconnu par l'automate $\mathcal{A}$ est l'ensemble des mots acceptés par $\mathcal{A}$.*

La proposition 1.4 a pour corollaire immédiat que l'ensemble reconnu par un automate est rationnel. Réciproquement, à partir d'une expression rationnelle, il existe plusieurs méthodes classiques pour construire un automate qui dénote le même ensemble. Nous n'y revenons pas ici, mais nous aurons l'occasion d'en décrire plusieurs dans les chapitres suivants.

THÉORÈME 1.1 *Un ensemble est rationnel si et seulement s'il peut être reconnu par un automate fini.*

REMARQUE 1.12 Il convient de souligner la différence entre un ensemble reconnaissable (reconnu par un morphisme) et un ensemble rationnel (reconnu par un automate). Un ensemble rationnel peut ne pas être reconnaissable. Par exemple, dans le monoïde $(\mathbb{N}^2,+)$, l'ensemble $\{(x,y) \mid x \leqslant y\}$ peut être reconnu par un automate et n'est pourtant pas reconnaissable. Nous verrons cependant que dans le monoïde libre ces deux notions coïncident.

DÉFINITION 1.39 *Soit $\mathcal{A} = \langle Q,M,E,I,T \rangle$ un automate. Pour tout état p de Q, le* ***passé*** *de p dans $\mathcal{A}$, noté $\mathsf{Past}_{\mathcal{A}}(p)$, est l'ensemble reconnu par l'automate $\langle Q,M,E,I,p \rangle$. De même, le* ***futur*** *de p dans $\mathcal{A}$, noté $\mathsf{Fut}_{\mathcal{A}}(p)$, est l'ensemble reconnu par l'automate $\langle Q,M,E,p,T \rangle$ et, pour tout couple d'états (p,q), l'ensemble de transition $\mathsf{Trans}_{\mathcal{A}}(p,q)$ est l'ensemble reconnu par l'automate $\langle Q,M,E,p,q \rangle$.*

Le passé (*resp.* le futur) est donc l'ensemble des éléments qui étiquettent des débuts de calculs menant en p (*resp.* des fins de calculs venant de p). Le produit d'un élément du passé par un élément du futur étiquette donc un calcul de l'automate passant par p. Donc $\mathsf{Past}_{\mathcal{A}}(p).\mathsf{Fut}_{\mathcal{A}}(p)$ est inclus dans l'ensemble reconnu par $\mathcal{A}$.
De même, $\mathsf{Past}_{\mathcal{A}}(p).\mathsf{Trans}_{\mathcal{A}}(p,q).\mathsf{Fut}_{\mathcal{A}}(q)$ est inclus dans cet ensemble.

DÉFINITION 1.40 *Soit $\mathcal{A} = \langle Q,M,E,I,T \rangle$ et $\mathcal{B} = \langle R,M,F,J,U \rangle$ deux automates. Une application μ de Q dans R est un morphisme d'automates de $\mathcal{A}$ dans $\mathcal{B}$, si*

- *pour tout élément p de Q, I_p est inclus dans $J_{p\mu}$ et T_p est inclus dans $U_{p\mu}$,*
- *pour tout couple (p,q) de $Q \times Q$, $E_{p,q}$ est inclus dans $F_{p\mu,q\mu}$.*

PROPOSITION 1.5 *Soit $\mathcal{A}$ et $\mathcal{B}$ deux automates sur un monoïde M. S'il existe un morphisme de $\mathcal{A}$ dans $\mathcal{B}$, l'ensemble reconnu par $\mathcal{A}$ est inclus dans celui reconnu par $\mathcal{B}$.*

DÉFINITION 1.41 *Un automate $\mathcal{A} = \langle Q,M,E,I,T \rangle$ est* ***non-ambigu*** *si, pour tout élément x de M, il existe au plus un seul chemin réussi de $\mathcal{A}$, $(p_0,p_1,\ldots,p_k)$, au calcul duquel appartient x, et, le cas échéant, une seule factorisation de $x = x_0.x_1.x_2 \ldots x_k.x_{k+1}$ telle*

que :

$$\forall i \in [1;k],\ x_i \in E_{p_{i-1},p_i},$$
$$x_0 \in I_{p_0} \qquad et \qquad x_{k+1} \in T_{p_k}.$$

Cette dernière notion est globale, ce qui permet de la définir dans n'importe quel monoïde, ce qui n'est pas le cas du *déterminisme* qui n'a un sens que dans le monoïde libre.

— ∘ —

4.3 Automates sur un alphabet

Lorsqu'on travaille dans le monoïde libre (A^*), on préfère manipuler des automates dans lesquels chaque transition correspond à une seule lettre. Ces automates particuliers, « temps-réel » (puisqu'à chaque opération représentée par une lettre, on effectue une transition), sont les automates classiques. Ils permettent d'établir le lien entre les langages rationnels et reconnaissables.

DÉFINITION 1.42 *Un* ***automate*** $\mathcal{A}$ *est un quintuplet* $\langle Q,A,E,I,T \rangle$*, où* Q *est un ensemble fini d'états,* A *un alphabet fini,* E *un sous-ensemble de* $Q \times A \times Q$ *appelé ensemble des* ***transitions*** *et* I *(resp.* T*) un sous-ensemble de* Q *regroupant les* ***états initiaux*** *(resp.* ***terminaux****).*
L'étiquette d'une transition (p,a,q) *de* E *est* a*; pour tout* e *dans* E*,* $|e|$ *représente l'étiquette de* e*.*

EXEMPLE 1.5 Soit $\mathcal{A}_1 = \langle Q,A,E,I,T \rangle$ l'automate défini par :

$$\begin{aligned} Q &= \{p,q,r\}, \\ A &= \{a,b\}, \\ E &= \{(p,a,p),(p,b,p),(p,a,q),(q,b,r),(r,a,r),(r,b,r)\}, \\ I &= \{p\}, \\ T &= \{r\}. \end{aligned}$$

La représentation graphique de cet automate est donnée figure 4. Les états initiaux sont indiqués par une flèche entrante et les états terminaux par une flèche sortante. Le graphe sous-jacent de cet automate est celui de la figure 1.

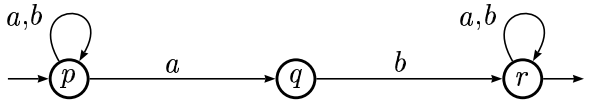

FIG. 4 – *Un automate à trois états*

DÉFINITION 1.43 *Soit $\mathcal{A} = \langle Q,A,E,I,T \rangle$. Un* ***chemin*** *de $\mathcal{A}$ est une suite de transitions dont les images dans le graphe sous-jacent forment un chemin. L'****étiquette d'un chemin*** *est le mot formé par la concaténation des étiquettes des transitions qui le constituent. Un* ***chemin réussi*** *(aussi appelé* ***calcul****) de $\mathcal{A}$ est un chemin dont l'état de départ appartient à I et celui d'arrivée à T.*

DÉFINITION 1.44 *Un mot de A^* est* ***accepté*** *par un automate $\mathcal{A}$ s'il existe un calcul de $\mathcal{A}$ dont ce mot est l'étiquette. Le* ***langage reconnu*** *par un automate est l'ensemble des mots qu'il accepte. Deux automates sont* ***équivalents*** *s'ils reconnaissent le même langage.*

THÉORÈME 1.2 *Un langage est rationnel si et seulement s'il existe un automate qui reconnaît ce langage.*

On verra en effet dans le chapitre 6 qu'à partir d'une expression rationnelle, on peut construire un automate qui reconnaît le langage représenté par l'expression.

EXEMPLE 1.6 On voit facilement que l'automate de la figure 4 accepte tous les mots de $\{a,b\}^*$ qui contiennent un facteur ab et que ce sont les seuls mots acceptés. Le langage reconnu par cet automate est donc $\mathcal{L}_1 = \{a,b\}^*ab\{a,b\}^*$.

Pour des raisons de facilité, ou pour obtenir une description plus compacte, on peut parfois recourir à l'utilisation dans les automates de transitions qui ne sont pas étiquetées par des lettres mais par le mot vide. Ces transitions que nous appelons **transitions spontanées**, parce qu'elles correspondent au passage d'un état dans un autre sans qu'aucune opération ne soit effectuée, sont parfois appelées ε-transitions. Nous renonçons à cette appellation qui fait référence au symbole ε qui dénote alors le mot vide et auquel nous préférons 1_{A^*}.

DÉFINITION 1.45 *Un état q d'un automate est un* ***état accessible*** *s'il existe un chemin d'un état initial vers q; il est* ***co-accessible*** *s'il existe un chemin de q vers un état terminal. Un automate est* ***émondé*** *si tous ses états sont accessibles et co-accessibles.*

PROPOSITION 1.6 *Tout automate est équivalent à un automate émondé.*

En effet, si un état d'un automate n'est pas à la fois accessible et co-accessible, on peut le supprimer sans changer le langage reconnu par l'automate.

DÉFINITION 1.46 *Un automate sur un alphabet A est* ***déterministe*** *s'il n'a qu'un état initial et si, de chaque état, part au plus une transition étiquetée par chaque lettre. De même, il est* ***co-déterministe*** *s'il n'a qu'un état final et si, dans chaque état, arrive au plus une transition étiquetée par chaque lettre.*

DÉFINITION 1.47 *Un automate sur un alphabet A est* ***complet*** *si de chaque état part au moins une transition étiquetée par chaque lettre.*

On considère généralement cette notion dans le cadre des automates déterministes. De chaque état part alors une et une seule transition étiquetée par chaque lettre. On peut toujours rendre un automate complet en ajoutant un état non co-accessible dans lequel arrive les transitions qu'on rajoute pour obtenir un automate complet.

DÉFINITION 1.48 *Pour tout état p de Q, pour toute lettre a de A, on note*

$$p \cdot a = \{q \in Q \mid (p,a,q) \in E\}$$

l'ensemble des ***successeurs*** *de p par a.*
Si X est un sous-ensemble de Q,

$$X \cdot a = \bigcup_{p \in X} p \cdot a.$$

Les successeurs d'un état p ou d'un ensemble X par un mot $u = u'a$ sont définis récursivement par :

$$p \cdot u = (p \cdot u') \cdot a\,, \quad X \cdot u = (X \cdot u') \cdot a.$$

Le monoïde libre A^* agit ainsi à droite sur l'ensemble $\mathcal{P}(Q)$. Si $\mathcal{A}$ est un automate déterministe, A^* agit à droite sur Q.
On peut symétriquement définir l'ensemble des ***prédécesseurs*** *de p par a et étendre cette notion aux prédécesseurs d'un sous-ensemble X de Q par un mot u. On définit ainsi une action à gauche de A^* sur $\mathcal{P}(Q)$ qui, si l'automate est co-déterministe, est plus particulièrement une action à gauche de A^* sur Q.*

— ∘ —

On l'a vu, les transitions peuvent être considérées comme une matrice de $\mathcal{P}(A)^{Q \times Q}$. Dans les automates sur A, l'accent est mis sur les générateurs. Au lieu d'utiliser la matrice de transition E, on préfère considérer la fonction $\mu : A \mapsto \mathbb{B}^{Q \times Q}$ telle que :

$$E = \sum_{a \in A^*} (a\mu)a$$

DÉFINITION 1.49 *La* ***représentation linéaire*** *d'un automate $\mathcal{A} = \langle\, Q,A,E,I,T \,\rangle$ est un triplet (λ,μ,ν), où λ et ν sont respectivement des vecteurs ligne et colonne de $\mathbb{B}^Q$, et μ un morphisme de A^* dans $\mathbb{B}^{Q \times Q}$ tels que :*

$$\forall p \in Q,\ \lambda_p = 1_{\mathbb{B}} \Leftrightarrow p \in I\,, \quad \nu_p = 1_{\mathbb{B}} \Leftrightarrow p \in T,$$
$$\forall p,q \in Q,\ \forall a \in A,\ (a\mu)_{p,q} = 1_{\mathbb{B}} \Leftrightarrow (p,a,q) \in E.$$

PROPOSITION 1.7 *Soit $\mathcal{A}$ un automate et (λ,μ,ν) sa représentation linéaire. Le monoïde (fini) engendré par $A\mu$ est appelé* ***monoïde de transition*** *de $\mathcal{A}$. Il reconnaît le langage reconnu par $\mathcal{A}$.*

En effet, les mots u acceptés par $\mathcal{A}$ sont exactement ceux pour lesquels il existe un couple $(i,t) \in I \times T$ tel que $(u\mu)_{i,t} \neq 0_{\mathbb{B}}$.

THÉORÈME 1.3 *(Kleene) Soit A un alphabet fini. Un langage de A^* est rationnel si et seulement s'il est reconnaissable.*

La proposition 1.7 montre qu'un langage rationnel est reconnaissable. Réciproquement, soit $\mathcal{L}$ un langage reconnu par le morphisme μ de A^* sur un monoïde fini M. A partir du **graphe de Cayley** de M, on peut facilement construire un automate déterministe qui accepte $\mathcal{L}$:

$$\mathcal{A} = \langle M,A,\{(x,a,y) \mid y = x.(a\mu)\},1_M,\mathcal{L}\mu \rangle.$$

COROLLAIRE 1.8 *Tout automate est équivalent à un automate déterministe.*

Il suffit en effet de considérer le graphe de Cayley du monoïde de transition de l'automate de départ $\mathcal{A}$. Le monoïde de transition $M_{\mathcal{A}}$ est, rappelons-le, un ensemble de relations de Q dans Q, où Q est l'ensemble des états de $\mathcal{A}$. En fait, on peut obtenir à partir de $\mathcal{A}$ un automate plus petit que ce graphe de Cayley. La seule chose qui importe pour savoir si un élément α de $M_{\mathcal{A}}$ est final, est le fait que $I\alpha$ contienne ou non un état final de $\mathcal{A}$. On peut donc définir la relation d'équivalence sur $M_{\mathcal{A}}$: $\alpha \sim \beta \Leftrightarrow I\alpha = I\beta$. Attention, cette relation n'est qu'une congruence *droite*[4], ce qui permet de quotienter le graphe de Cayley (à droite) du monoïde. Le calcul de l'automate qui en résulte ne nécessite pas le calcul du monoïde de transition. C'est ce qu'on appelle la construction des sous-ensembles[5]. On appelle l'automate obtenu le **déterminisé** de $\mathcal{A}$. .

DÉFINITION 1.50 *Soit $\mathcal{A} = \langle Q,A,E,I,T \rangle$ un automate. On définit l'automate **déterminisé** de $\mathcal{A}$, $\mathcal{D} = \langle R,A,F,J,U \rangle$ par :*

$$\begin{aligned} R &= \{I \cdot u \mid u \in A^*\}, \\ J &= \{I\}, \\ U &= \{X \in R \mid X \cap T \neq \emptyset\}, \\ F &= \{(X,a,Y) \in R \times A \times R \mid Y = X \cdot a\}. \end{aligned}$$

*De façon duale, on définit l'automate **co-déterminisé** de $\mathcal{A}$, $\mathcal{C} = \langle S,A,G,H,V \rangle$ par :*

$$\begin{aligned} S &= \{u \cdot T \mid u \in A^*\}, \\ H &= \{X \in S \mid X \cap I \neq \emptyset\}, \\ V &= \{T\}, \\ G &= \{(X,a,Y) \in R \times A \times R \mid X = a \cdot Y\}. \end{aligned}$$

Le déterminisme d'un automate lui confère quelques propriétés :

PROPOSITION 1.9 *Soit $\mathcal{A}$ un automate déterministe qui reconnaît un langage $\mathcal{L}$. Alors, pour tout état p,*

4. Ce n'est pas forcément la plus grossière qui sature l'image de $\mathcal{L}$ dans $M_{\mathcal{A}}$.

5. « subset construction » en anglais, voir [23]

i) *pour tout état q distinct de p,* $\mathsf{Past}_{\mathcal{A}}(p) \cap \mathsf{Past}_{\mathcal{A}}(q) = \emptyset$.

ii) *pour tout mot u de* $\mathsf{Past}_{\mathcal{A}}(p)$, *on a* $\mathsf{Fut}_{\mathcal{A}}(p) = u^{-1}\mathcal{L}$.

Démonstration. Soit i l'état initial de $\mathcal{A}$. Le premier point est trivial, à cause du déterminisme, un mot donné ne peut mener au plus qu'en un seul état à partir de i et ne peut donc appartenir qu'au passé de cet état. Quant au second point, tout mot du langage qui accepte u comme préfixe se décompose en $u.v$, avec v qui appartient à $\mathsf{Fut}_{\mathcal{B}}(i \cdot u)$. Réciproquement, pour tout mot v de $\mathsf{Fut}_{\mathcal{B}}(i \cdot u)$, le mot $u.v$ est dans le langage. □

Voyons la relation entre les futurs des états d'un automate et ceux de son déterminisé.

LEMME 1.10 *Soit $\mathcal{A}$ un automate et $\mathcal{D}$ son déterminisé. Alors, pour tout état X de $\mathcal{D}$, on a :*

$$\mathsf{Fut}_{\mathcal{D}}(X) = \bigcup_{p \in X} \mathsf{Fut}_{\mathcal{A}}(p).$$

Démonstration. La preuve est par récurrence sur la longueur des mots. Par définition du déterminisé, le mot vide appartient au futur de X (en d'autres termes, X est final) si et seulement si il appartient au futur d'un des états de $\mathcal{A}$ qui sont dans X. Soit u un mot de longueur non nulle; u s'écrit $u = a.u'$. On obtient :

$$\begin{aligned} u \in \mathsf{Fut}_{\mathcal{D}}(X) &\iff u' \in \mathsf{Fut}_{\mathcal{D}}(X \cdot a) \\ &\iff u' \in \bigcup_{q \in X \cdot a} \mathsf{Fut}_{\mathcal{A}}(q) \\ &\iff u' \in \bigcup_{p \in X} \bigcup_{q \in p \cdot a} \mathsf{Fut}_{\mathcal{A}}(q) \\ &\iff u = a.u' \in \bigcup_{p \in X} \mathsf{Fut}_{\mathcal{A}}(p). \end{aligned}$$

□

On voit que les quotients du langage jouent un rôle particulier. Dans un automate déterministe quelconque, il se peut que deux états aient le même futur et correspondent donc au même quotient. On peut définir un automate déterministe canonique dans lequel chaque quotient correspond à un seul état :

DÉFINITION 1.51 *L'automate minimal d'un langage $\mathcal{L}$ sur A^* est l'automate déterministe $\mathcal{A}_{\mathcal{L}} = \langle Q, A, E, \{i\}, T \rangle$, défini par :*

$$\begin{aligned} Q &= \{u^{-1}\mathcal{L} \mid u \in A^*\} \setminus \{\emptyset\} \\ i &= \mathcal{L} \\ T &= \{p \in Q \mid 1_{A^*} \in p\} \\ E &= \{(p, a, q) \mid a^{-1}p = q\} \end{aligned}$$

REMARQUE 1.13 L'automate ainsi défini est émondé. On peut définir l'automate minimal comme l'automate des quotients gauches de $\mathcal{L}$, éventuellement ensemble vide compris, ce qui donne un automate qui, le cas échéant, a un état de plus qui n'est pas co-accessible, mais l'automate est alors complet. Cependant, dans la suite, nous utiliserons essentiellement l'automate minimal émondé.

Par construction, le futur d'un état étiqueté par un quotient $u^{-1}\mathcal{L}$ est égal à ce quotient.

Il est facile de montrer que tout automate déterministe $\mathcal{A}$ émondé qui accepte un langage $\mathcal{L}$ s'envoie par quotient surjectif sur l'automate minimal de $\mathcal{L}$. Il suffit d'associer à un état p l'état de l'automate minimal qui correspond à $\mathsf{Fut}_{\mathcal{A}}(p)$ (qui est un quotient de $\mathcal{L}$).

On peut construire l'automate minimal par raffinement successif de partitions d'états sur lesquelles on examine l'action des lettres. Nous ne reviendrons pas ici sur cet algorithme dû à Moore et dont une version donnée par Hopcroft est en $O(n \log n)$. On pourra aussi consulter [50] pour une analyse en moyenne de cet algorithme sur certaines classes de langages.

On s'intéresse ici à une autre méthode, algorithmiquement moins performante mais qui nous donnent certaines informations sur des classes d'automates que nous étudierons plus tard. Elle est due à Brzozowski.

PROPOSITION 1.11 *Le déterminisé d'un automate co-déterministe est un automate minimal.*

Démonstration. Si un automate $\mathcal{A}$ est co-déterministe, les futurs de ses états sont disjoints deux à deux. Le futur d'un état du déterminisé $\mathcal{D}$, est, par construction, l'union des futurs des états de $\mathcal{A}$ auquel il correspond. Les futurs des états de $\mathcal{D}$ sont donc distincts. L'automate $\mathcal{D}$ est par conséquence minimal. □

COROLLAIRE 1.12 *Si un automate est à la fois déterministe et co-déterministe, il est minimal.*

La portée de ce corollaire est relativement faible, puisque nous verrons que de tels automates ne peuvent reconnaître qu'une classe restreinte de langages; ce résultat nous sera toutefois utile lorsque nous étudierons les langages à groupe ou réversibles.

Examinons maintenant le monoïde de transition de l'automate minimal d'un langage. Comme l'automate minimal est un quotient de tout automate déterministe qui reconnaît le langage, son monoïde de transition est un quotient du monoïde de transition de chacun de ces automates déterministes.

D'autre part, on a vu qu'on peut construire un automate déterministe qui reconnaît le langage à partir de n'importe quel monoïde qui reconnaît le langage. Il s'agit du graphe de Cayley, dont le monoïde de transition est le monoïde lui-même (puisque l'action des générateurs à droite sur les états est la multiplication du monoïde).

On obtient donc la proposition suivante :

PROPOSITION 1.13 *Le monoïde de transition de l'automate minimal d'un langage sur A^*, appelé* ***monoïde syntaxique*** *du langage est un quotient de n'importe quel monoïde qui reconnaît le langage. Il existe un morphisme canonique de A^* dans ce monoïde; nous l'appellerons le* ***morphisme syntaxique****.*

Nous avons vu que dans le monoïde libre existe la notion d'image miroir d'un mot. On peut appliquer aux automates une transformation en correspondance avec cette opération.

DÉFINITION 1.52 *Soit $\mathcal{A}$ un automate dont la représentation linéaire est (λ,μ,ν). L'automate* ***transposé*** *de $\mathcal{A}$ est l'automate $\mathcal{A}^t$ défini par la représentation linéaire (ν^t,μ^t,λ^t) où λ^t et ν^t sont les vecteurs transposés respectifs de λ et ν et où μ^t est un morphisme qui, à tout mot u de A^* associe la matrice transposée de $\overline{u}\mu$.*

L'automate transposé de $\mathcal{A}$ reconnaît l'image miroir de $\mathcal{L}$ (puisque $\lambda \otimes u\mu \otimes \nu = \nu^t \otimes \overline{u}\mu^t \otimes \nu^t$).

Pour conclure, on va rappeler une construction classique sur les automates. Étant donné deux automates $\mathcal{A}$ et $\mathcal{B}$, calculer un automate qui reconnaît l'union des langages reconnus par $\mathcal{A}$ et $\mathcal{B}$ est très simple, il suffit de considérer l'union des deux automates. Calculer l'automate qui reconnaît l'intersection des langages est un peu plus compliqué. Cette opération s'appelle le produit. Il faut souligner ici que le langage que reconnaît le produit de deux automates n'est pas le produit des langages mais leur intersection.

DÉFINITION 1.53 *Soit $\mathcal{A} = \langle\, Q,A,E,I,T \,\rangle$ et $\mathcal{B} = \langle\, R,A,F,J,U \,\rangle$ deux automates. Le* ***produit*** *de $\mathcal{A}$ et de $\mathcal{B}$ est l'automate $\mathcal{C} = \langle\, Q \times R,A,G,I \times J,T \times U \,\rangle$, avec*

$$K = \{((p,q),a,(p',q')) \mid (p,a,q) \in E,(p',a,q') \in F\}.$$

En pratique, on ne construit que la partie accessible du produit. Il peut parfois être intéressant de calculer le produit d'un automate par lui-même (qu'on appelle son **carré**). En effet, chaque chemin du carré correspond à deux chemins de l'automate; ceci permet d'effectuer certaines comparaisons.

— ∘ —

4.4 Automates à multiplicité

On peut définir les automates sur A à multiplicité dans un semi-anneau $\mathbb{K}$, comme des automates sur le semi-anneau $\mathbb{K}\langle\langle A^* \rangle\rangle$. Toutefois, là encore, on s'intéressera aux automates « temps-réel », c'est-à-dire les automates dont les transitions sont étiquetées par des lettres pondérées, donc par des sommes de monômes de degré 1 :

DÉFINITION 1.54 *Un* ***automate à multiplicité*** *dans un semi-anneau $\mathbb{K}$ sur un alphabet A est un sextuplet $\mathcal{A} = \langle\, Q,A,\mathbb{K},E,I,T \,\rangle$, où Q est un ensemble fini d'états, E un sous-ensemble fini de $Q \times A \times \mathbb{K}_* \times Q$ qui sont les transitions de $\mathcal{A}$, et I et T deux vecteurs*

de $\mathbb{K}^Q$.
On suppose qu'entre deux états p *et* q*, il n'y a au plus qu'une transition par lettre de* A*. Au besoin, on remplace deux transitions* (p,a,k,q) *et* (p,a,k',q) *par la transition* $(p,a,k \oplus k',q)$.

On peut remarquer que les transitions sont étiquetées par des éléments de $\mathbb{K}_*$. En effet, ajouter une transition étiquetée par $0_\mathbb{K}$ ne change pas la série reconnue (ou *réalisée*).

DÉFINITION 1.55 *L'**automate sous-jacent** d'un automate* $\mathcal{A} = \langle Q,A,\mathbb{K},E,I,T \rangle$ *à multiplicité est un automate* $\mathcal{B} = \langle Q,A,F,J,U \rangle$ *(sans multiplicité) tel que*

$$\begin{aligned} F &= \{(p,a,q) \mid \exists k \in \mathbb{K}_*, (p,a,k,q) \in E\}, \\ J &= \{p \mid I_p \neq 0_\mathbb{K}\}, \\ U &= \{p \mid T_p \neq 0_\mathbb{K}\}. \end{aligned}$$

On dira qu'un automate à multiplicité est déterministe, co-déterministe ou complet si son automate sous-jacent l'est.

On peut définir une représentation linéaire pour les automates avec multiplicité de la même manière que pour les automates « classiques ».

DÉFINITION 1.56 *La **représentation linéaire** d'un automate* $\mathcal{A} = \langle Q,A,\mathbb{K},E,I,T \rangle$ *est un triplet* (λ,μ,ν)*, où* λ *et* ν *sont respectivement des vecteurs ligne et colonne de* $\mathbb{K}^Q$*, et* μ *un morphisme de* A^* *dans* $\mathbb{K}^{Q\times Q}$ *tels que :*

$$\begin{gathered} \forall p \in Q,\ \lambda_p = I_p\ , \quad \nu_p = T_p, \\ \forall p,q \in Q,\ \forall a \in A,\ (a\mu)_{p,q} = k \Leftrightarrow (p,a,k,q) \in E. \end{gathered}$$

Si (p,a,q) *n'est pas une transition de l'automate sous-jacent de* $\mathcal{A}$*,* $(a\mu)_{p,q} = 0_\mathbb{K}$.

REMARQUE 1.14 Si α est réalisé par un automate dont la représentation linéaire est (λ,μ,ν), pour tout mot u de A^*, la série $u^{-1}\alpha$ est réalisée par un automate dont la représentation linéaire est $(\lambda \otimes u\mu,\mu,\nu)$.

Le problème de la déterminisation des automates à multiplicité est de loin beaucoup plus délicat que dans le cas des automates sans multiplicité. On a en effet, un lien similaire entre les futurs des états d'un automate déterministe et les quotients de la série.

PROPOSITION 1.14 *Soit* $\mathcal{A}$ *un automate déterministe à multiplicité dans* $\mathbb{K}$ *qui réalise une série* s*. Alors, pour tout état* p *de* $\mathcal{A}$*, pour tout mot* u *de* $\mathsf{Past}_\mathcal{A}(p)$,

$$\langle \mathsf{Past}_\mathcal{A}(p),u \rangle \otimes \mathsf{Fut}_\mathcal{A}(p) = u^{-1}s.$$

Démonstration. Comme $\mathcal{A}$ est déterministe, pour tout mot dont u est un préfixe, et qu'on peut écrire $u.v$,

$$\langle s,u.v \rangle = \langle \mathsf{Past}_\mathcal{A}(p),u \rangle \otimes \langle \mathsf{Fut}_\mathcal{A}(p),v \rangle.$$

On obtient donc directement le résultat. □

On le voit, chaque quotient d'une série réalisée par un automate déterministe est multiple (dans $\mathbb{K}$) d'une série prise dans un ensemble fini. Toute série rationnelle ne respecte pas cette propriété. Par exemple, la série $a^* + (2a)^*$ sur $\mathbb{N}$ a pour quotients $\{a^* + 2^n(2a)^* \mid n \in \mathbb{N}\}$. On peut vérifier qu'il n'y a pas d'ensemble fini de séries tel que chacun de ces quotients est un multiple d'un élément de cet ensemble. Les séries réalisables par un automate fini sont donc un sous-ensemble strict des séries rationnelles.

DÉFINITION 1.57 *Soit s un série de $\mathbb{K}\mathrm{Rat}\, A^*$. On dit que s est une* ***série séquentielle***[6] *si s peut être réalisée par un automate déterministe.*

On l'a vu, les quotients d'une série séquentielle appartiennent à un cône finiment engendré et ce n'est en général pas le cas des séries rationnelles. Toutefois, les quotients des séries rationnelles respectent la propriété suivante qui est caractéristique :

THÉORÈME 1.4 *Une série formelle sur A^* à coefficients dans $\mathbb{K}$ est rationnelle si et seulement si elle appartient à un $\mathbb{K}$-semi-module de type fini clos par quotient (par rapport aux mots de A^*).*

Démonstration. Soit s une série formelle et $g = (g_1, g_2, \ldots, g_n)$ un système générateur d'un semi-module clos par quotient contenant s. On considère g comme un vecteur colonne. Comme il s'agit d'un système générateur, il existe un vecteur ligne λ de $\mathbb{K}^n$ et une application μ de A^* dans $\mathbb{K}^{n\times n}$ tels que :

$$\begin{aligned} s &= \lambda \otimes g \\ \forall u \in A^*, u^{-1}g &= (u\mu) \otimes g \end{aligned}$$

Comme le quotient est une action à droite des mots sur les séries, μ est un morphisme. On pose $\nu = (\nu_1, \ldots, \nu_n)$, vecteur colonne tel que, pour tout i de $[1; n]$, $g_i = \langle s_1, 1_{A^*}\rangle$. Le triplet (λ,μ,ν) est la représentation linéaire d'un automate. Pour tout mot u,

$$\begin{aligned} \langle s,u\rangle &= \langle \lambda \otimes g, u\rangle \\ &= \lambda \otimes \langle g,u\rangle \\ &= \lambda \otimes \langle u^{-1}g, 1_{A^*}\rangle \\ &= \lambda \otimes (u\mu) \otimes \nu \end{aligned}$$

L'automate ainsi construit reconnaît s qui est donc rationnelle.

Considérons à présent une série rationnelle s réalisée par un automate $\mathcal{A} = \langle\, Q, A, \mathbb{K}, E, I, T\,\rangle$ à n états. Pour tout mot u de A^*,quel que soit le mot w acceptant u comme préfixe $(w = u.v)$, on a :

$$\langle u^{-1}s, v\rangle = \langle s, w\rangle = \bigoplus_{q\in Q} \langle \mathsf{Past}_{\mathcal{A}}(p), u\rangle \otimes \langle \mathsf{Fut}_{\mathcal{A}}(p), v\rangle.$$

6. On appelle série séquentielle ce qui était traditionnellement appelé série sous-séquentielle.

Donc, on a la relation

$$u^{-1}s = \bigoplus_{q \in Q} \langle \mathsf{Past}_{\mathcal{A}}(p), u \rangle \otimes \mathsf{Fut}_{\mathcal{A}}(p).$$

Les futurs des états de l'automate engendrent donc un $\mathbb{K}$-semi-module de type fini clos par quotient et qui contient s. □

On peut revenir aux séries séquentielles et en donner une caractérisation :

THÉORÈME 1.5 *Une série formelle sur A^* à coefficients dans $\mathbb{K}$ est rationnelle si et seulement si ses quotients appartiennent à un $\mathbb{K}$-cône finiment engendré.*

Démonstration. Le fait qu'une série séquentielle respecte cette propriété est un corollaire immédiat de la proposition 1.14.
Si les quotients d'une série formelle appartiennent à un cône finiment engendré par une famille $(g_1, g_2, \ldots, g_n)$, ils appartiennent au sous-module engendré par les mêmes générateurs, qui est stable pour l'opération quotient, et la série est donc rationnelle. Dire que les quotients appartiennent à un cône signifie que pour toute lettre a, pour tout i de $[1; n]$, il existe j dans $[1; n]$ et $k_{i,j}$ dans $\mathbb{K}$ tel que $a^{-1}g_i = k_{i,j}g_j$. On peut donc trouver un morphisme μ de A^* dans $\mathbb{K}^{n \times n}$ tel que, pour toute lettre a de A, chaque ligne de $a\mu$ n'a qu'un coefficient non nul. Comme, de même, la série s est proportionnelle à l'un des g_i, l'automate correspondant à la représentation linéaire (λ, μ, ν) ainsi construite est déterministe. □

De même qu'on a défini l'action des lettres sur les états d'un automate, dans le cas d'un automate avec multiplicité, on peut définir la **fonction de production** d'un mot sur un état :

DÉFINITION 1.58 *Soit $\mathcal{A} = \langle Q, A, \mathbb{K}, E, I, T \rangle$ un automate à multiplicité et (λ, μ, ν) sa représentation linéaire. Pour tout état p de Q, on pose $\chi^{(p)}$ le vecteur de $\mathbb{K}^Q$ caractéristique de p ($\chi^{(p)}_p = 1_{\mathbb{K}}$ et pour tout $q \neq p$, $\chi^{(p)}_q = 0_{\mathbb{K}}$). Pour tout mot u, on définit la **production** de u à partir d'un état p par :*

$$p * u = \chi^{(p)}.(u\mu).$$

Si X est un sous-ensemble de Q,

$$X * a = \bigoplus_{p \in X} p * a.$$

Parmi les automates à multiplicité, citons deux familles particulières. Premièrement, ceux dont les coefficients appartiennent à $\mathrm{Rat}\, B^*$, où B est un alphabet fini. Il s'agit alors de **transducteurs**; ils ont été largement étudiés dans le passé. C'est le même type de questions que celles qui ont été résolues pour les transducteurs que nous allons nous poser au sujet d'une seconde famille, celle des automates à coefficients dans un semi-anneau $(\mathsf{max}, +)$.

— ∘ —

Table des exemples

Index

Bibliographie

[1] A. Ambainis et R. Freivalds, 1-way quantum finite automata: strengths, weaknesses and generalizations. In *39th Ann. Symposium on FOCS* (1998), 332–342.

[2] D. Angluin, Inference of reversible languages. *J. of the ACM* **29** (1982), 741–765.

[3] V. Antimirov, Partial derivatives of regular expressions and finite automaton constructions. *Theoret. Comput. Sci.* **155** (1996), 291–319.

[4] A. Arnold, A. Dicky, et M. Nivat, A note about minimal non-deterministic automata. *Bull ot the EATCS* **47** (1992), 166–169.

[5] M.-P. Béal, O. Carton, C. Prieur, et J. Sakarovitch, Squaring transducers. *Proc. of Latin 2000, Lect. Notes in Comp. Sci.* **1776** (2000), 397–406.

[6] G. Berry et R. Sethi, From regular expressions to deterministic automata, *Theoret. Comput. Sci.* **48** (1986), 117–126.

[7] J. Berstel et J.-E. Pin, Local languages and the Berry-Sethi algorithm, *Theoret. Comput. Sci.* **155** (1996), 439–446.

[8] J. Berstel et Ch. Reutenauer, *Les séries rationnelles et leurs langages.* Masson, 1984. Traduction: *Rational Series and their Languages.* Springer, 1986.

[9] J. A. Brzozowski, Derivatives of regular expressions. *J. Assoc. Comput. Mach.* **11** (1964), 481–494.

[10] A. Buchsbaum, R. Giancarlo, et J. Westbrook, On the Determinization of Weighted Finite Automata. *Proc. of ICALP'98, Lect. Notes in Comp. Sci.* **1443** (1998), 482–493.

[11] P. Caron et M. Flouret, Glushkov construction for multiplicities. *Pre-Proceedings of CIAA'00*, M. Daley, M. Eramian and S. Yu, eds, Univ. of Western Ontario, (2000), 52–61.

[12] O. Carton, Factorisations et matrice des facteurs. Manuscrit (1994).

[13] J.-M. Champarnaud et D. Ziadi, New finite automaton constructions based on canonical derivatives. *Pre-Proceedings of CIAA'00*, M. Daley, M. Eramian and S. Yu, eds, Univ. of Western Ontario, (2000), 36–43.

[14] Ch. Choffrut, Une caractérisation des fonctions séquentielles et des fonctions sous-séquentielles en tant que relations rationnelles. *Theoret. Comput. Sci.* **5** (1977), 325–337.

[15] M. Chrobak, Finite Automata and Unary Languages. *Theoret. Comput. Sci.* **47** (1986), 149–158.

[16] G. Cohen, P. Moller, J.-P. Quadrat, et M. Viot, Algebraic Tools for the Performance Evaluation of Discrete Event Systems. *IEEE Proc.: Special issue on D.E.S.* **77.1** (1989).

[17] R. Cohen, Star height of certain families of regular events. *J. Computer System Sci.* **4** (1970), 281–297.

[18] R. Cohen et J. A. Brzozowski, General properties of star height of regular events. *J. Computer System Sci.* **4** (1970), 260–280.

[19] J. H. Conway, *Regular algebra and finite machines.* Chapman and Hall, 1971.

[20] B. COURCELLE, D. NIWINSKI, A. PODELSKI, A geometrical view of the dererminization ond minimization of finite-state automata. *Math. Systems Theory* **24** (1991), 117–146.

[21] F. DEJEAN ET M.-P. SCHÜTZENBERGER, On a question of Eggan. *Inform. and Control* **9** (1966), 23–25.

[22] L. C. EGGAN, Transition graphs and the star-height of regular events. *Michigan Mathematical J.* **10** (1963), 385–397.

[23] S. EILENBERG, *Automata, Languages and Machines, volume A.* Academic Press, 1974.

[24] S. GAUBERT, Rational Series over Dioids and Discrete Event Systems. *Proc. of the 11th Conf. on Anal. and Opt. of Systems, Lect. Notes in Contr. and Inf. Sci.* **199** (1994).

[25] S. GAUBERT, On the Burnside problem for Semigroups of Matrices in the (max,+) Algebra. *Semigroup Forum* **52** (1996), 271–292.

[26] S. GAUBERT, Methods and applications of (max,+) linear algebra. *rapport de recherche INRIA* **3088** (1997).

[27] V. GLUSHKOV, The abstract theory of automata. *Russian Mathematical Surveys 16* (1961), 1–53.

[28] CH. HAGENAH ET A. MUSCHOLL, Computing ε-Free NFA from regular expressions in $O(n\log^2(n))$ time. *R.A.I.R.O. Inf. Théorique* **34**, (2000), 257–277.

[29] T.E. HALL, Biprefix codes, inverse semigroups and syntactic monoids of injective automata. *Theoret. Comput. Sci.* **32** (1984), 201–213.

[30] T. HARJU ET J. KARHUMÄKI, The equivalence problem of multitape finite automata. *Theoret. Comput. Sci.* **78** (1991), 347–355.

[31] K. HASHIGUCHI ET N. HONDA, The star height of reset-free events and strictly locally testable events. *Inform. and Control* **40** (1979), 267–284.

[32] K. HASHIGUCHI, Limitedness theorem on finite automata with distance functions. *J. of Comput. Syst. Sci.* **24** (1982), 233–244.

[33] K. HASHIGUCHI, Algorithms for determining relative star height and star height. *Inform. and Computation* **78** (1988), 124–169.

[34] K. HASHIGUCHI, Improved limitedness theorem on finite automata with distance functions. *Theoret. Comput. Sci.* **72** (1990), 27–38.

[35] P.-C. HÉAM, A lower bound for reversible automata. *Theoret. Informatics Appl.* **34** (2000), 331–341.

[36] P.-C. HÉAM, Contribution à l'algorithmique des automates : complexité et aspects topologiques. *Thèse de doctorat*, Université Paris 7, 2001.

[37] J. HROMKOVIČ, S. SEIBERT, ET T. WILKE, Translating regular expressions into small ε-free nondeterministic finite automata. *Proc. of STACS'97, Lect. Notes in Comp. Sci.* **1200** (1997), 55–66.

[38] D. KROB, Differentiation of K-rational expressions. *Int. J. of Algebra and Computation 2* (1992), 57–87.

[39] W. KUICH ET A. SALOMAA, *Semirings, Automata, Languages.* Springer, 1986.

[40] G. LALLEMENT, *Semigroups and combinatorial applications.* Wiley, 1979.

[41] H. LEUNG, Limitedness theorem on finite automata with distance functions: an algebraic proof *Theoret. Comput. Sci.* **81** (1991), 137–145.

[42] S. LOMBARDY ET J. SAKAROVITCH, On the star height of rational languages, a new presentation for two old results *Proc. of 3rd ICLWC, Kyoto* (2000) (M. Ito, ed.), World Scientific, *à paraître.*

[43] S. LOMBARDY ET J. SAKAROVITCH, Star height of reversible languages and universal automata, *accepté à Latin'02.*

[44] S. LOMBARDY, Sequentialization and unambiguity of (max, +) rational series over one letter. *Pre-Proc. of Workshop on Max-plus algebra, Prague* (2001) (S. Gaubert, ed.).

[45] O. MATZ ET A. POTTHOFF, Computing small nondeterministic finite automata. *proc. of TACAS'95, BRICS Notes Series* (1995), 74–88.

[46] R. MCNAUGHTON ET H. YAMADA, Regular expressions and state graphs for automata. *IRE Trans. on electronic computers* **9** (1960), 39–47.

[47] R. MCNAUGHTON, The loop complexity of pure-group events. *Inform. and Control* **11** (1967), 167–176.

[48] MOEBIUS, *Sur l'étoile.* Gentiane, 1983, Rééd. Casterman, 1990.

[49] M. MOHRI, Finite-State Transducers in Language and Speech Processing. *Computat. Ling.* **23.2** (1997), 269–311.

[50] C. NICAUD, Étude du comportement en moyenne des automates finis et des langages rationnels. *Thèse de doctorat*, Université Paris 7, 2000.

[51] J.-E. PIN, On reversible automata. In *Proc. 1st LATIN Conf., (I. Simon, Ed.), Lecture Notes in Comput. Sci.* **583** (1992), 401–416.

[52] J.-E. PIN, Variétés de langages formels. Masson, 1984. Traduction: *Varieties of formal languages* North Oxford Acad. Pub., 1986.

[53] G. RANEY, Sequential functions. *J. Assoc. Comput. Mach.* **5** (1958) 177–180.

[54] J. SAKAROVITCH, A construction on automata that has remained hidden. *Theoret. Comput. Sci.* **204** (1998), 205–231.

[55] J. SAKAROVITCH, *Éléments de théorie des automates.* Vuibert, *à paraître.*

[56] A. SALOMAA, *Jewels of formal language theory.* Computer Science Press, 1981.

[57] P.V. SILVA, On free inverse monoid languages. *Theoret. Informatics and Appl.* **30** (1996), 349–378.

[58] I. SIMON, Recognizable sets with multiplicities in the tropical semiring. *Proc. of MFCS'88, Lect. Notes in Comp. Sci.* **324** (1988), 107–120.

[59] I. SIMON, The non deterministic complexity of a finite automaton. *Mots (M. Lothaire)*, Hermès (1990) 384–400.

[60] I. SIMON, On semigroups of matrices over the tropical semiring. *R.A.I.R.O. Inf. Théorique*, (1994), 277–294.

[61] N.J.A. SLOANE, *The On-Line Encyclopedia of Integer Sequences.* `http://www.research.att.com/~njas/sequences/`

[62] J.B. STEPHEN, Presentations of inverse monoids. *J. Pure Appl. Alg.* **63** (1990), 81–112.

[63] M. SZALAY, On the maximal order in S_n and S_n^*. *Acta arithm.* **37** (1980), 321–331.