UNIVERSITÉ DU QUÉBEC À MONTRÉAL

SÉRIES RATIONNELLES ET MATRICES GÉNÉRIQUES NON COMMUTATIVES

THÈSE

PRÉSENTÉE

COMME EXIGENCE PARTIELLE

DU DOCTORAT EN MATHÉMATIQUES

PAR

SYLVAIN LAVALLÉE

JUILLET 2009

À Jeanne

REMERCIEMENTS

Je tiens à remercier mon directeur, le professeur Christophe Reutenauer, qui, dans un premier temps a accepté de me diriger et ce, sans me connaître. Sa patience et sa confiance à mon égard sont tout simplement exceptionnelles. Il a toujours su trouver la façon de me motiver malgré les nombreuses difficultés rencontrées. Son expérience et sa notoriété furent pour moi des atouts indispensables à l'obtention de ce diplôme. Finalement, je le remercie pour son support financier.

Je tiens à remercier Nathalie de m'avoir soutenue tout au long de cette quête ; merci pour tes petits lunchs et surtout à ta patience, ta compréhension et tes sacrifices étant donné mes absences fréquentes.

Merci à Mélanie et Jean-François qui m'ont offert le gîte et le support moral pendant ces belles années.

Un gros merci à l'équipe du LACIM pour leur dynamisme et leur côté humain, en particulier à Lise, sans oublier Manon.

Merci à ma mère Thérèse, à ma soeur Nathalie, à Jacinthe, Paul, Michaël et Paméla pour tout ce que vous avez fait pour moi.

Merci à mes amis Benoit, Mathieu, Mathieu, Mélanie et Caroline qui ont toujours été là quand venait le temps de relaxer.

TABLE DES MATIÈRES

LISTE DES FIGURES

RÉSUMÉ

Dans ce travail, nous nous intéressons aux séries rationnelles et aux matrices génériques non commutatives.

Dans le premier chapitre, on étudiera les polynômes de cliques du graphe pondéré. Soit C un graphe simple non orienté (sans boucles), on lui associe la somme des monômes $(-1)^i c_i x^i$ où c_i est le nombre de sous-graphes complets (cliques) sur i sommets. En pondérant les sommets par des entiers non négatifs, on définit les polynômes de cliques du graphe pondéré C comme étant la somme des monômes $(-1)^{|B|} x^{\deg(B)}$, où B est un sous-graphe complet de C. On va montrer que l'ensemble de tels polynômes coïncide avec l'ensemble des polynômes réciproques des polynômes caractéristiques de matrices à coefficients entiers non négatifs.

Au chapitre 2, on va généraliser ce polynôme une fois de plus en pondérant les sommets du graphe simple par des monômes de la forme αx^d, où α est un réel positif et d, un entier non négatif. On va lui associer le polynôme de cliques généralisé comme la somme $(-1)^{|B|} \left(\prod_{s\in B} \alpha_s x^{d_s}\right)$, où B est un sous-ensemble commutatif de C et s est un sommet de B. On va montrer que l'ensemble de ces polynômes coïncide exactement avec l'ensemble des polynômes réciproques des polynômes caractéristiques à coefficients réels non négatifs.

Le troisième chapitre porte sur la $\mathbb{N}$-rationalité de certaines classes de séries. Tout d'abord, on va établir les conditions nécessaires et suffisantes nous permettant de décider de la $\mathbb{N}$-rationalité d'une série de la forme $(1 - ax + bx^k)^{-1}$, où $a \in \mathbb{N}$, $b \in \mathbb{Z}$, $k \geq 2$. Par la suite, on fera de même pour les séries de la forme $(1 - ax + bx^2 + cx^3)^{-1}$, où $a \in \mathbb{N}$ et b, $c \in \mathbb{Z}$.

Au Chapitre 4, on étudiera les propriétés des fonctions zêta associées aux automates et aux codes. On va montrer que le nombre de chemins bi-infinis dans $\mathcal{A}$ dont la période est n est égal au rang stable d'un certain mot non vide w ; i.e. le rang de w^n pour un n suffisamment grand. Par ailleurs, on montrera plusieurs propriétés de cette série telles la $\mathbb{N}$-rationalité, l'apériodicité ou la divergence. Étant donné que plusieurs de ces résultats sont valides pour des automates non ambigus, ceux-ci s'appliqueront aux codes. On y présentera les propriétés de la fonction zêta des codes complets, des codes purs, des codes circulaires et des codes bifixes.

Le chapitre 5 portera sur les matrices génériques stochastiques, i.e. les matrices à variables non commutatives soumises aux conditions stochastiques (somme des éléments de chaque ligne vaut 1). Il est bien connu dans la littérature que toute matrice stochastique a 1 comme valeur propre dont le vecteur propre à droite associé est ${}^t(1, \ldots, 1)$.

Mais qu'en est-il du vecteur propre à gauche associé à cette même valeur propre ? Dans le cas commutatif, on montrera que ce vecteur de la matrice M est le vecteur ligne des mineurs principaux $M - I_n$. Dans le cas non-commutatif, on montrera que les éléments de ce vecteur sont les inverses des dérivations des codes reconnus par l'automate dont M est la matrice associée, évalués dans un corps libre.

Mots clés : Séries rationnelles, codes à longueurs variables, fonction zêta, automate, corps libre, matrices génériques, polynômes de cliques.

INTRODUCTION

Les séries formelles sont utilisées dans plusieurs branches des mathématiques incluant la combinatoire algébrique et énumérative. Les séries rationnelles en variables non commutatives comportent plusieurs propriétés similaires à celles des langages rationnels. Citons par exemple le théorème fondamental de Schützenberger qui est l'analogie du théorème de Kleene, (Kleene, 1956). On peut consulter (Salomaa et Soittola, 1978), (Berstel et Reutenauer, 1984) ou (Berstel et Reutenauer, 2008b).

Parmi ces séries, on retrouve les séries rationnelles à coefficients entiers non négatifs dites les séries $\mathbb{N}$-rationnelles. On verra que ces séries sont complètement caractérisées par les théorèmes de Berstel (Berstel, 1971) et Soittola (Soittola, 1976). Dans (Gessel, 2003), on trouve une façon combinatoire d'obtenir une telle série, notamment la théorie des monoïdes partiellement commutatifs libres de Cartier-Foata (Cartier et Foata, 1969). Dans (Barcucci et al., 2001), on retrouve un algorithme nous permettant de décider si une série est $\mathbb{N}$-rationnelle. Finalement, C. Koutschan (Koutschan, 2005), (Koutschan, 2008), a implémenté l'algorithme décrit dans la preuve du théorème de Soittola. Ce package, RLangGFun (Maple), est disponible sur à l'adresse http ://www.risc.uni-linz.ac.cat/research/combinat/software/RLangGFun/.

L'importance de ces séries vient en partie du fait que les séries $\mathbb{N}$-rationnelles sont précisément les séries génératrices des langages rationnels ((Berstel et Reutenauer, 2008b), Lemme 2.1.4, (Salomaa et Soittola, 1978), Cor. II. 5.4).

La première partie de ce travail portera sur l'études de certaines classes de séries $\mathbb{N}$-rationnelles. Tout d'abord, on caractérisera les séries de la forme $(\det(1 - xM))^{-1}$, où M est une matrice à coefficients entiers non négatifs. Ces séries sont $\mathbb{N}$-rationnelles étant donné qu'elles coïncident avec les séries génératrices des monoïdes gradués partiellement commutatifs libres. On montrera que les polynômes $\det(1 - xM)$ coïncident avec les polynômes de cliques pondérés.

Par la suite, on étudiera les séries de la forme $(\det(1 - xM))^{-1}$, où M est une matrice à coefficients réels non négatifs. On montrera que les polynômes de la forme $\det(1 - xM)$ coïncident avec les polynômes de cliques généralisés.

Ensuite, on s'intéresse aux conditions nécessaire et suffisante permettant de décider de la $\mathbb{N}$-rationalité des séries de la forme $(1 - ax + bx^k)^{-1}$, où $a \in \mathbb{N}$, $b \in \mathbb{Z}$, $k \geq 2$ et $(1 - ax + bx^2 + cx^3)^{-1}$, où $a \in \mathbb{N}$ et b, $c \in \mathbb{Z}$.

Finalement, on étudiera les propriétés de la fonction zêta d'un automate. Ceux-ci étant valides pour des automates non ambigus, on pourra les appliquer aux codes.

La seconde partie porte sur les matrices génériques stochastiques, des matrices dont les entrées sont des variables non commutatives dont la somme des éléments de chaque ligne vaut 1. Il est connu dans la littérature que toute matrice stochastique a le vecteur propre à droite ${}^t(1, \ldots, 1)$ associé à la valeur propre 1. On s'intéressera au vecteur propre à gauche associé à 1, tout d'abord dans le cas commutatif et par la suite, dans le cas non commutatif. Dans ce dernier cas, on aura recours à la théorie des corps libres (au sens de Cohn) puisque les entrées de la matrice ; des expressions rationnelles, seront plongées dans un corps libre.

Ce travail est divisé comme suit. Au Chapitre 1, on fera une introduction à la théorie des langages et des séries rationnelles en variables non commutatives (voir (Eilenberg, 1974), (Salomaa et Soittola, 1978) ou (Berstel et Reutenauer, 1984)).

Au Chapitre 2, on définira le polynôme de cliques. On va généraliser ce polynôme une première fois en pondérant les sommets du graphe simple non orienté C par des monômes de la forme x^d, où $d \in \mathbb{N}$. Afin de simplifier l'écriture, on va étiqueter les sommets de C par d. On va lui associer le polynôme de cliques du graphe pondéré défini comme la somme des monômes $(-1)^{|B|} x^{\deg(B)}$, où B est un sous-graphe complet du graphe simple pondéré. On va montrer que l'ensemble de tels polynômes coïncide avec l'ensemble des polynômes réciproques des polynômes caractéristiques de matrices à coefficients entiers non négatifs. L'inclusion d'un sens nécessite la théorie des monoïdes partiellement commutatifs, introduite par Cartier et Foata (Cartier et Foata, 1969), où on utilisera la construction du graphe des circuits. Cette construction n'étant pas surjective, pour montrer l'inclusion dans l'autre sens, on va devoir utiliser un théorème de Kim, Ormes et Roush (Kim, Ormes et Roush, 2000) établissant les conditions nécessaire et suffisante pour qu'un ensemble de nombres complexes soit le spectre d'une matrice à coefficients entiers non négatifs. Entre autres, on va utiliser un résultat de Lalonde (Lalonde, 1995) pour montrer que le polynôme de cliques pondéré satisfasse l'une des conditions de ce théorème.

Au Chapitre 3, on va généraliser une fois de plus le polynôme de cliques en pondérant les sommets par des monômes de la forme αx^d, où α est un réel positif et d, un entier non négatif. On va lui associer le polynôme défini comme la somme des monômes $(-1)^{|B|}\left(\prod_{s\in B}\alpha_s x^{d_s}\right)$, où B est un sous-ensemble commutatif du graphe et s est un sommet de B. Ces polynômes seront appelés polynômes de cliques généralisés. On va montrer que l'ensemble de ces polynômes coïncide exactement avec l'ensemble des polynômes réciproques des polynômes caractéristiques de matrices à coefficients réels non négatifs. L'idée de la preuve est exactement la même que la démonstration du théorème principal du Chapitre 2 à l'exception qu'on va utiliser le théorème spectral de Boyle et Handelman (Boyle et Handelman, 1991) (au lieu du théorème de Kim, Ormes et Roush) afin de montrer l'inclusion dans l'autre sens. Afin de montrer que le polynôme de cliques généralisé vérifie l'une des conditions du théorème spectral, on va utiliser un résultat provenant de la théorie des empilements de Viennot (Viennot, 1986).

Au Chapitre 4, on va s'intéresser aux conditions nécessaire et suffisante permettant de décider si une série de la forme $(1-ax+bx^k)^{-1}$, où $a\in\mathbb{N}$, $b\in\mathbb{Z}$, $k\geq 2$ est $\mathbb{N}$-rationnelle. La motivation de ce problème provient du fait que $(1-ax+bx^2)^{-1}$ est $\mathbb{N}$-rationnelle si et seulement si $a^2\geq 4b$. Cette condition est reliée à la théorie des graphes extrémaux ; en effet, Mantel (voir (Bollobas, 1998)) a démontré qu'il existe un graphe simple non orienté ayant a sommets et b arêtes sans triangle si et seulement si $4b\leq a^2$. On va démontrer qu'une telle série est $\mathbb{N}$-rationnelle si et seulement si $k^k b \leq (k-1)^{k-1}\, a^k$. La condition nécessaire se base sur le nombre de racines réelles du polynôme réciproque du dénominateur, $x^k - a\, x^{k-1} + b$. La condition suffisante se démontre directement par calculs. Par la suite, on fera de même pour les séries de la forme $(1 - ax + bx^2 + cx^3)^{-1}$, où $a \in \mathbb{N}$ et $b, c \in \mathbb{Z}$. On va séparer ce problème en deux parties : $a^2 \geq 3b$ et $a^2 < 3b$. Dans le premier cas, on a que le polynôme réciproque du dénominateur $p(x)$ possède un maximum et un minimum locaux. Par la suite, on applique les Théorèmes de Berstel et Soittola selon le nombre de racines réelles de ce polynôme. Dans le second cas, on a que $p(x)$ est strictement croissant sur tout son domaine. Ce cas se restreint uniquement à la situation où $b > 0$ et $c < 0$. En effet, si $b < 0$, la condition $3b > a^2$ n'est jamais satisfaite et si $c > 0$, $p(x)$ a une seule racine réelle qui est négative, donc $(1 - ax + bx^2 + cx^3)^{-1}$, n'est jamais $\mathbb{N}$-rationnelle.

Dans le Chapitre 5, on va démontrer plusieurs propriétés de la fonction zêta d'un automate définie comme la série $\exp\left\{\sum_{n=1}^{\infty} a_n \frac{z^n}{n}\right\}$, où a_n est le nombre de chemins bi-infinis dans $\mathcal{A}$ dont la période est n. On va montrer que a_n est égal au rang stable d'un certain mot non vide w ; i.e. le rang de w^n pour un n suffisamment grand. Par ailleurs, on montrera plusieurs propriétés de cette série telles la $\mathbb{N}$-rationalité ou concernant l'apériodicité ou la divergence. Étant donné que plusieurs de ces résultats sont valides pour des automates non ambigus, ceux-ci s'appliqueront aux codes, en particulier aux codes complets, aux codes purs, aux codes circulaires et aux codes bifixes. Finalement, on va montrer que $\zeta(\mathcal{A})$ est une spécialisation de la fonction zêta Z_ϕ d'un morphisme de systèmes dynamiques définie dans (Boyle, 1989).

Au Chapitre 6, on va identifier le vecteur propre à gauche associé à la valeur propre 1 d'une matrice générique stochastique. Dans le cas commutatif, on va montrer que les éléments de ce vecteur sont les mineurs principaux de la matrice. Ce résultat est bien connu en probabilités puisqu'il permet de calculer la probabilité limite d'un procédé de Markov fini, en remplaçant la matrice stochastique M par $M - I$. On peut calculer ces probabilités en utilisant le théorème des arbres des chaînes de Markov (Markov chain trees theorem), voir (Leighton et Rivest, 1983), (Broder, 1989), (Anantharam et Tsoucas, 1989) ou (Aldous, 1990) où ce calcul est donné en termes d'arbres générateurs. La preuve du cas commutatif qu'on retrouve dans ce travail est entièrement algébrique étant donné qu'elle se base uniquement sur la formule du déterminant impliquant les matrices adjointes.

Dans le cas non commutatif, les éléments de ce vecteur propre sont les inverses des dérivations des codes reconnus par l'automate dont M est la matrice de cet automate. Pour ce faire, on va utiliser des résultats provenant de la théorie des corps libres, l'analogue non commutatif du corps des fractions. Il existe plusieurs constructions du corps libre, (voir (Amitsur, 1966), (Bergman, 1970), (Malcolmson, 1978), (Cohn, 1971) et (Cohn, 1995)). Les éléments inversibles d'un corps libre sont les matrices pleines ; i.e. soit M une telle matrice, il n'existe pas de matrices P et Q de dimensions $n \times (n-1)$ et $(n-1) \times n$ respectivement telles que $M = PQ$. Par la suite, on va construire une certaine matrice F et suite à des transformations élémentaires de lignes et de colonnes, on va montrer que F est équivalente à une matrice creuse.

CHAPITRE I

LANGAGES ET SÉRIES FORMELLES

Ce chapitre est une introduction aux langages et aux séries rationnelles en un nombre fini de variables non commutatives. La dernière section de ce chapitre portera sur la classe des séries $\mathbb{N}$-rationnelles, une sous-classe des séries rationnelles. Tous les résultats concernant les séries proviennent du livre de Berstel et Reutenauer (Berstel et Reutenauer, 1984) ; il est possible de consulter la version électronique de ce livre, disponible sur la page web de Jean Berstel.

1.1 Langages

Soit A un ensemble fini appelé *alphabet*, les éléments sont appelés des *lettres*. Un *mot* w est une suite finie de lettres et la *longueur* de w, notée $|w|$ est égale à la longueur de cette suite. On note 1 le mot vide. Soit $u = a_1 \dots a_n$ et $v = b_1 \dots b_m$ deux mots ; on définit le *produit* (concaténation) comme étant le mot $w = uv = a_1 \dots a_n b_1 \dots b_m$. Ainsi, l'ensemble des mots, muni de ce produit est un monoïde, appelé le *monoïde libre* engendré par A. On le note A^*.

Un *langage* L est un sous-ensemble de A^* ; L est *fini* s'il contient un nombre fini d'éléments. Soient L_1 et L_2 deux langages. On définit le produit de L_1 et L_2 comme le langage $\{w_1 w_2 \mid w_1 \in L_1,\, w_2 \in L_2\}$. On appelle l'*étoile* de L le langage

$$L^* = \{w_1 \dots w_n \mid w_i \in L, n \geq 0\} = \bigcup_{n \geq 0} L^n, \qquad L^0 = \phi.$$

Un langage est *rationnel* s'il est obtenu à partir des langages finis par les opérations rationnelles : union, produit et étoile.

Les *opérations rationnelles non ambiguës* sont l'union disjointe, le produit non ambigu (i.e. tout mot $w \in L_1L_2$ a une unique factorisation $w = w_1w_2$ telle que $w_1 \in L_1$ et $w_2 \in L_2$) et l'étoile non ambiguë (i.e. tout mot de L^* a une seule factorisation $w_1w_2 \ldots w_n$, $w_i \in L$). On montre qu'un langage rationnel peut être obtenu en utilisant seulement des opérations rationnelles non ambiguës ((Eilenberg, 1974) Thm. VII.8.2).

1.2 Séries formelles

Définition 1.1. Un demi-anneau est un ensemble $\mathbb{K}$ muni de deux opérations binaires, la somme ($+$) et le produit ($\cdot$) et deux éléments notés 0 et 1 ayant les propriétés suivantes :

(i) $\langle \mathbb{K}, +, 0 \rangle$ est un monoïde commutatif,

(ii) $\langle \mathbb{K}, \cdot, 1 \rangle$ est un monoïde,

(iii) le produit est distributif en respect de l'addition,

(iv) $0 \cdot x = x \cdot 0 = 0$, pour tout $x \in \mathbb{K}$.

Un demi-anneau est commutatif si le produit l'est.

Définition 1.2. Soit A un alphabet et $\mathbb{K}$ un demi-anneau. Une série formelle S est une fonction

$$S : A^* \to \mathbb{K}.$$

L'image d'un mot w par S est appelée le coefficient de w dans S et est dénoté (S, w). La série S s'écrit elle-même comme la somme formelle

$$S = \sum_{w \in A^*} (S, w)\, w.$$

L'ensemble de toutes les séries formelles sur A^* ayant des coefficients dans $\mathbb{K}$ est dénoté $\mathbb{K}\langle\langle A \rangle\rangle$.

Sur l'ensemble $\mathbb{K}\langle\langle A \rangle\rangle$, on définit la somme et le produit (de Cauchy) des séries $S =$

$\sum_{w \in A^*} (S, w)\, w$ et $T = \sum_{w \in A^*} (T, w)\, w$ par :

$$\begin{aligned} S + T &= \sum_{w \in A^*} ((S, w) + (T, w))\, w, \\ ST &= \sum_{w \in A^*} \left(\sum_{uv = w} (S, u)\, (T, v) \right) w \end{aligned}$$

respectivement. L'addition dans $\mathbb{K}$ étant commutative, $S + T = T + S$. Cependant, le produit n'est généralement pas commutatif.

Définition 1.3. Soit L un langage. La série caractéristique $\underline{L}$ de L est la série formelle $\underline{L} = \sum_{w \in L} w$.

L'ensemble $\mathbb{K}\langle\langle A \rangle\rangle$, muni de l'addition et de la multiplication est un demi-anneau dont l'élément neutre pour la somme est la série $0 = \sum_{w \in A^*} 0w$ et l'élément neutre du produit est la série $\underline{1} = 1$, où 1 est le mot vide.

Définition 1.4. Une série $S \in \mathbb{K}\langle\langle A \rangle\rangle$ est dite propre (ou quasi-régulière) si le coefficient du mot vide est nul ; i.e. $(S, 1) = 0$.

On peut munir $\mathbb{K}\langle\langle A \rangle\rangle$ d'une structure topologique au sens de la convergence d'une suite $S_1, S_2, \ldots$ d'éléments de $\mathbb{K}\langle\langle A \rangle\rangle$. La suite converge à la limite S ; i.e.

$$\lim_{i \to \infty} S_i = S \Leftrightarrow \forall n \in \mathbb{N},\ \exists M \in \mathbb{N},\ \forall w \in A^n,\ \forall m > M, (S_m, w) = (S, w).$$

Soit S une série propre. On s'intéresse à la suite des puissances de S : $S^0 = 1$, $S^1 = S$, $S^2 = S \cdot S$, ..., qui converge à 0 puisque le coefficient pour tout mot w de longueur n vaut 0 dans toute série S^m, $m > n$. Ainsi, la série

$$S^* = \lim_{m \to \infty} \sum_{n=0}^{m} S^n$$

existe et est nommée l'*étoile* de S. De façon similaire, on définit

$$S^+ = \lim_{m \to \infty} \sum_{n=1}^{m} S^n.$$

Ces deux séries sont liées via les relations

$$S^* = 1 + S^+, \qquad S^+ = S\,S^* = S^*\,S.$$

Donc, si $\mathbb{K}$ est un anneau, on a $S^* = (1-S)^{-1}$ puisque

$$S^*(1-S) = S^* - S^+ = 1.$$

Définition 1.5. Les opérations rationnelles dans $\mathbb{K}\langle\langle A\rangle\rangle$ sont la somme, le produit et l'étoile. Un sous-demi-anneau de $\mathbb{K}\langle\langle A\rangle\rangle$ est rationnellement fermé s'il est fermé sous les opérations rationnelles. La clôture rationnelle d'un sous-ensemble $M \subseteq \mathbb{K}\langle\langle A\rangle\rangle$ est le plus petit sous-ensemble de $\mathbb{K}\langle\langle A\rangle\rangle$ contenant M et qui est rationnellement fermé. Une série formelle $S \in \mathbb{K}\langle\langle A\rangle\rangle$ est $\mathbb{K}$-rationnelle si c'est un élément de la clôture rationnelle de $\mathbb{K}\langle\langle A\rangle\rangle$. L'ensemble de toutes les séries $\mathbb{K}$-rationnelles est dénoté par $\mathbb{K}^{rat}\langle\langle A\rangle\rangle$.

Proposition 1.6. *(voir (Berstel et Reutenauer, 2008b), Prop. III.2.1) La série caractéristique d'un langage rationnel est une série rationnelle.*

Définition 1.7. Une série formelle $S \in \mathbb{K}\langle\langle A\rangle\rangle$ est dite reconnaissable s'il existe un entier $n \geq 1$, un morphisme de monoïdes

$$\mu = A^* \to K^{n\times n},$$

et deux matrices $\lambda \in K^{1\times n}$ et $\gamma \in K^{n\times 1}$ telles que pour tout mot w, le coefficient de w dans S, noté (S, w) est égal à

$$(S,\, w) = \lambda\,\mu(w)\,\gamma.$$

Dans ce cas, le triplet (λ, μ, γ) est appelé la représentation linéaire de S et n, sa dimension.

Le résultat fondamental suivant est dû à Schützenberger (Schützenberger, 1961).

Théorème 1.8 (Schützenberger). *Une série formelle est rationnelle si et seulement si elle est reconnaissable.*

1.3 Séries rationnelles en une variable

Soit $\mathbb{K}$ un corps. Lorsqu'on se restreint à une seule variable, on a $\mathbb{K}\langle\langle A\rangle\rangle = \mathbb{K}[[x]]$ ($\mathbb{K}\langle A\rangle = \mathbb{K}[x]$), l'anneau des séries (polynômes) en une variable.

Proposition 1.9. *(voir (Berstel et Reutenauer, 2008b), Prop. V.1.1) Une série S est rationnelle si et seulement s'il existe deux polynômes $P(x)$ et $Q(x)$ dans $\mathbb{K}[x]$ tels que $Q(0) = 1$ et que S est la série obtenue en développant la fraction rationnelle $P(x)/Q(x)$.*

Théorème 1.10. *(voir (Berstel et Reutenauer, 2008b), Prop. V.1.2) Soit $S = \sum_{n=0}^{\infty} a_n\, x^n$. S est rationnelle si et seulement s'il existe $q_1, q_2, \ldots, q_k \in \mathbb{K}$ tels que pour n suffisamment grand, $a_{n+k} = q_1\, a_{n+k-1} + \ldots + q_k\, a_n$.*

À la relation de récurrence linéaire $a_{n+k} = q_1\, a_{n+k-1} + \ldots + q_k\, a_n$ la plus courte correspond le polynôme $x^k - q_1 x^{k-1} - \ldots - q_k$, appelé le polynôme minimal de $S = \sum_{n=0}^{\infty} a_n x^n$.

Définition 1.11. Une série rationnelle est régulière si elle admet une représentation linéaire $(\lambda,\, \mu,\, \gamma)$ telle que $\mu(x)$ est une matrice inversible.

Définition 1.12. Le produit de Hadamard de deux séries formelles S et T est la série $S \odot T$ définie par

$$(S \odot T,\, w) = (S,\, w)\,(T,\, w).$$

Définition 1.13. Supposons que $\mathbb{K}$ soit de caractéristique 0. Soit Λ le groupe multiplicatif $\mathbb{K} \setminus 0$ et soit x une variable. Considérons l'algèbre $\mathbb{K}[x][\Lambda]$ du groupe Λ sur l'anneau $\mathbb{K}[x]$. C'est en particulier une algèbre sur $\mathbb{K}$. Un élément de $\mathbb{K}[x][\Lambda]$ est appelé un polynôme exponentiel.

Théorème 1.14. *(voir (Berstel et Reutenauer, 2008b), Prop. V.2.1) Soit $\mathbb{K}$ un corps algébriquement clos. La fonction qui associe à un polynôme exponentiel*

$$\sum_{\lambda \in \Lambda} P_\lambda(x)\, \lambda \in \mathbb{K}[x][\Lambda]$$

la série rationnelle régulière

$$\sum_{n=0}^{\infty} a_n\, x^n$$

définie par

$$a_n = \sum_{\lambda \in \Lambda} P_\lambda(n)\, \lambda^n$$

est un isomorphisme de $\mathbb{K}$-algèbres de $\mathbb{K}[x][\Lambda]$ vers l'algèbre de Hadamard des séries rationnelles régulières.

Définition 1.15. Soit $f(x) = \frac{P(x)}{Q(x)}$ une série rationnelle, où $Q(x) = 1 - q_1\, x - q_2\, x^2 - \ldots - q_k\, x^k$. Les racines de $Q(x)$ sont appelées les pôles de $f(x)$ tandis que les racines du polynôme réciproque $\overline{Q}(x)$ sont appelées les *valeurs propres* de $f(x)$.

Remarque 1.16. La multiplicité de la valeur propre λ est égale à $1 + \deg(P_\lambda)$, où P_λ est le polynôme associé à λ défini au Théorème précédent.

Corollaire 1.17. *Soit $S = \sum a_n\, x^n$ une série rationnelle sur un corps algébriquement clos de caractéristique nulle $\mathbb{K}$.*

(i) Pour un n suffisamment grand, on a

$$a_n = \sum_{i=1}^{p} P_i(n)\, \lambda_i^n, \tag{1.1}$$

où $\lambda_1, \ldots, \lambda_p \in \mathbb{K} \setminus \{0\}$ et $P_i(x) \in \mathbb{K}[x]$.

(ii) L'expression (1.1) est unique si les valeurs propres λ_i sont distinctes. En particulier, les valeurs propres non nulles de S sont les λ_i telles que $P_i \neq 0$.

1.4 Séries $\mathbb{N}$-rationnelles

On va s'intéresser à une sous-classe particulière des séries rationnelles en une variable : les séries $\mathbb{N}$-rationnelles ; i.e. les séries à coefficients entiers non négatifs obtenues par une suite finie d'opérations rationnelles de polynômes à coefficients entiers non négatifs.

Définition 1.18. Une série est $\mathbb{N}$-rationnelle (en une variable) si elle est obtenue par un nombre fini de sommes, de produits et d'étoiles de polynômes à coefficients dans $\mathbb{N}$.

Définition 1.19. Soit $Q(x)$ un polynôme de degré k, on définit le polynôme réciproque de $Q(x)$ comme étant le polynôme $\overline{Q}(x) = x^k\, Q(x^{-k})$.

Le théorème suivant, dû à Berstel (Berstel, 1971), établit une condition nécessaire des séries $\mathbb{N}$-rationnelles.

Théorème 1.20 (Berstel). *Soit $f(x)$ une fonction $\mathbb{N}$-rationnelle qui n'est pas un polynôme. Soit ρ le minimum des modules des pôles de $f(x)$. Alors ρ est un pôle de $f(x)$ et tout pôle de f de module ρ est de la forme $\rho\theta$, où θ est une racine de l'unité.*

On remarque que le minimum des modules des pôles d'une série rationnelle est le rayon de convergence de la série associée. Une conséquence directe de ce théorème nous assure qu'une série $\mathbb{N}$-rationnelle a un pôle réel positif qui est de module minimum.

Définition 1.21. Une valeur propre de $f(x)$ est dite dominante si elle est unique, réelle, positive et strictement plus grande que le module de toute autre valeur propre de $f(x)$.

Le théorème suivant, dû à Soittola (Soittola, 1976) énonce une condition suffisante assurant la $\mathbb{N}$-rationalité d'une série formelle.

Théorème 1.22 (Soittola). *Une série $\mathbb{Z}$-rationnelle ayant une valeur propre dominante et tous ses coefficients positifs ou nuls est $\mathbb{N}$-rationnelle.*

On retrouve une autre démonstration dans (Katayama, O. et Enomoto, 1978) et plus récemment, dans (Berstel et Reutenauer, 2008a). Par définition, une série $\mathbb{N}$-rationnelle a nécessairement des coefficients dans $\mathbb{N}$ mais une série à coefficients entiers non négatifs n'est pas en général $\mathbb{N}$-rationnelle. Par exemple, considérons la série suivante due à Gessel (Gessel, 2003)

$$f(x) = x + 4\,x^2 + x^3 + 144\,x^4 + 361\,x^5 + 484\,x^6 + 19321\,x^7 + 28224x^8 + 128881\,x^9 + \ldots$$

est une série à coefficients entiers non négatifs engendrée par la fraction

$$\frac{x + 5\,x^2}{1 + x - 5\,x^2 - 125\,x^3},$$

n'étant pas une série $\mathbb{N}$-rationnelle. En effet, les valeurs propres sont 5, $-3 + 4\,i$ et $-3 - 4\,i$; ces 3 valeurs propres sont toutes de module 5 ; ainsi, il n'y a donc pas de valeur propre dominante. On trouve d'autres exemples dans (Eilenberg, 1974), Exemple VIII.6.1, (Salomaa et Soittola, 1978) Exercice II.10.2 ou (Berstel et Reutenauer, 1984) Exercice V.2.2.

CHAPITRE II

POLYNÔMES DE CLIQUES DE GRAPHES PONDÉRÉS

La caractérisation des polynômes caractéristiques, connue dans la littérature sous l'appellation (N)IEP ((nonnegative) inverse eigenvalue problem) est un problème qui perdure depuis longtemps. Ce problème consiste à déterminer les conditions nécessaires et suffisantes afin qu'un ensemble de nombres complexes soit le spectre d'une matrice. Particulièrement, on s'intéresse au cas où les matrices doivent être non négatives. Boyle et Handelman (Boyle et Handelman, 1991) ont défini ces conditions permettant de nous garantir qu'un ensemble de nombres complexes soit le spectre d'une matrice carrée à coefficients *réels* non négatifs. Kim, Ormes et Roush (Kim, Ormes et Roush, 2000) ont établi et démontré les conditions nous assurant qu'un ensemble de nombres complexes soit le spectre d'une matrice carrée à coefficients *entiers* non négatifs.

On va rappeler la définition d'un polynôme de cliques associé à un graphe simple non orienté C et on va généraliser ce polynôme en pondérant chaque sommet de C par des entiers positifs. On appelle ce polynôme le *polynôme de cliques de graphes pondérés.* Le Théorème 2.4 stipule que l'ensemble des polynômes de cliques pondérés coïncide avec l'ensemble des polynômes de la forme $\det(1 - x\,M)$, où M est une matrice à coefficients entiers non négatifs.

2.1 Polynômes de cliques et polynômes caractéristiques

Soit C un graphe simple non orienté. Le *polynôme de cliques*, également appelé *polynôme de dépendance*, a été introduit par Fisher (Fisher, 1989) et est défini comme la somme des monômes $(-1)^i x^i$, où i est une *clique* de degré i de C ; i.e. un sous-graphe complet sur i éléments de C.

Exemple 2.1. Le polynôme de cliques du graphe suivant vaut $1 - 4x + 4x^2 - x^3$.

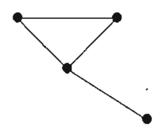
$C =$ 

Figure 2.1 Graphe simple.

Pour connaître des propriétés et résultats concernant ce polynôme on peut consulter (Hajialbolhassan et Mehrabadi, 1998), (Goldwurm et Santini, 2000), (Goldwurm et Saporiti, 1998) et (Levit et Mandrescu, 2005).

On va généraliser ce polynôme en pondérant chaque sommet s de C par un entier positif d_s dit *degré* de s. Soit B une clique, on définit le *degré* de B : $\deg(B)$=la somme des degrés des sommets de B.

Définition 2.2. Soit C un graphe simple dont les sommets sont pondérés par des entiers positifs. Le *polynôme de cliques du graphe pondéré* C, noté $P_C(x)$, est la somme des monômes $(-1)^{|B|} x^{\deg(B)}$, où B est une clique de C. Si tous les $d_s = 1$, on est ramené au polynôme de cliques.

Exemple 2.3. Reprenons l'exemple précédent et pondérons chaque sommet par un entier positif

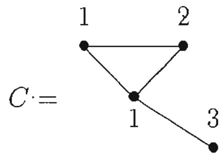


Figure 2.2 Graphe simple pondéré.

Le polynôme de cliques du graphe pondéré C est

$$\begin{aligned} P_C(x) &= 1-(2x+x^2+x^3)+(x^2+2x^3+x^4)-x^4 \\ &= 1-2x+x^3. \end{aligned}$$

Considérons maintenant une autre classe de polynômes. Soit M une matrice carrée à coefficients entiers non négatifs, considérons le polynôme $\det(1-x\,M)$, où 1 est la matrice identité de la taille appropriée. Ce polynôme est le *polynôme réciproque du polynôme caractéristique de* M.

Théorème 2.4. *Les polynômes de cliques pondérés coïncident avec les réciproques de polynômes caractéristiques de matrices carrées à coefficients entiers non négatifs. Autrement dit, les séries génératrices des monoïdes gradués partiellement commutatifs libres coïncident avec les séries de la forme* $\det(1-x\,M)^{-1}$, *où* M *est une matrice à coefficients dans* $\mathbb{N}$.

Remarque 2.5. On sait par la théorie de Cartier-Foata que si $f = 1/\det(1-x\,M)$, où M est une matrice à coefficients entiers non négatifs, alors $F(x)$ est $\mathbb{N}$-rationnelle. La réciproque n'est pas valide. En effet, soit

$$F(x) = \frac{1}{1-3x+5x^2-8x^3}.$$

Cette série, provenant de (Barcucci et al., 2001), est $\mathbb{N}$-rationnelle puisque

$$\begin{aligned} F(x) \;=\;& 1 + 3\,x + 4\,x^2 + 5\,x^3 + 19\,x^4 + 64\,x^5 + 137\,x^6 + 243\,x^7 + 17745\,x^{12} \\ & + A\,B\,\big(2287904\,x^{18} + 171059648\,x^{24} + 33080\,x^{13} + 2637120\,x^{19} + 392\,x^8 + 50944\,x^{14} \\ & + 1344\,x^9 + 70848\,x^{15} + 3032\,x^{10} + 144704\,x^{16} + 5512\,x^{11} + 487424\,x^{17}\big) \\ & + A\,\big(727545\,x^{18} + 9963\,x^{13} + 164\,x^8 + 205\,x^9 + 779\,x^{10} + 2624\,x^{11}\big) \\ & + A^2\,B\,\big(10192728000\,x^{30} + 139579200\,x^{25} + 2297600\,x^{20} + 2872000\,x^{21} + 10913600\,x^{22} \\ & + 36761600\,x^{23}\big)\,, \end{aligned}$$

où

$$\begin{aligned} A &= (41\,x^6)^*, \\ B &= (81\,x^6 + 7616\,x^{12} + 574400\,x^{18}\,A)^*. \end{aligned}$$

Cette expression rationnelle a été obtenue à l'aide du paquetage *RLangGFun* (Maple), créé par C. Koutschan (Koutschan, 2005) ou (Koutschan, 2008). Il est impossible de construire un graphe simple ayant 3 sommets tous pondérés par 1, et 5 arêtes. Ainsi, par le Théorème 2.4, il n'y a pas équivalence entre l'ensemble des séries de la forme $(\det(1 - x\,M))^{-1}$, où M est une matrice à coefficients dans $\mathbb{N}$ et l'ensemble des séries $\mathbb{N}$-rationnelles qui sont des inverses de polynômes.

2.2 Monoïdes partiellement commutatifs libres

On va introduire la théorie des monoïdes partiellement commutatifs libres de Cartier et Foata (Cartier et Foata, 1969). On peut consulter la version électronique de ce livre sur le site du séminaire lotharingien de combinatoire.

Définition 2.6. Un *circuit* est une classe de conjugaison de chemins fermés sans point double dans un graphe orienté.

Soient C un graphe simple non orienté et A l'ensemble des sommets de C. Considérons le monoïde libre A^* sur A. On définit la congruence $\sim_C$ engendrée par les relations $ab \sim_C ba$

si $\{a, b\}$ est une arête de C. On définit ainsi le *monoïde partiellement commutatif libre* $A^*/\sim_C$. On note $[a]$ la classe d'équivalence de la lettre a.

Un sous-ensemble B de A est une *partie commutative* si elle est finie, non vide et si deux de ses éléments commutent deux à deux modulo $\sim_C$. On pose alors $[B] = \prod_{a \in B} [a]$ et $[1] = 1$.

Définition 2.7. Soit $\mathbb{K}\langle\langle A^*/\sim_C\rangle\rangle$ la $\mathbb{K}$-algèbre des séries partiellement commutatives. On définit les séries partiellement commutatives

$$\begin{aligned} \zeta &= \sum_{u \in A^*/\sim_C} u, \\ \mu &= \sum_{B \subseteq A} (-1)^{|B|} [B], \end{aligned}$$

où la somme est sur toutes les parties commutatives B de A.

Théorème 2.8 (Cartier-Foata).

$$\mu\,\zeta = \zeta\,\mu = 1. \tag{2.1}$$

Soit D un graphe orienté, on construit le *graphe des circuits* C (graphe non orienté) de D comme suit : les sommets de C sont les circuits de D et deux sommets sont reliés par une arête si les circuits correspondants sont disjoints dans D. On pondère chaque sommet de C par la longueur du circuit de D correspondant à ce sommet. Nous noterons $C = \pi(D)$.

Soit M la matrice d'adjacence de D. En développant le déterminant $\det(1 - x\,M)$ en utilisant la formule impliquant les permutations et en décomposant celles-ci en cycles, on a

$$\det(1 - x\,M) = \sum_{\{c_1, \ldots, c_k\}} x^{|c_1| + \ldots + |c_k|},$$

où $k \in \mathbb{N}$, $\{c_1, \ldots, c_k\}$ est un ensemble de k circuits, où $|c_i|$ représente la longueur de c_i.

Ainsi, $\det(1 - x\,M)$ est le polynôme de cliques du graphe pondéré C.

Exemple 2.9. Considérons le graphe orienté D ci-dessous :

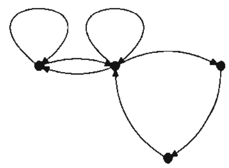


Figure 2.3 Graphe orienté D.

Son graphe des circuits C est

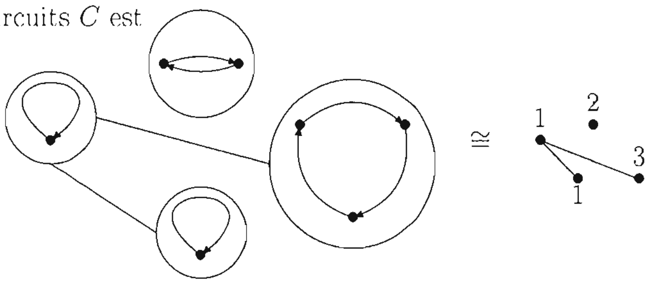


Figure 2.4 Graphe des circuits C.

Son polynôme de cliques de graphe pondéré est $P_C(x) = 1 - 2x - x^2 - x^3 + x^2 + x^4 =$ $1 - 2x - x^3 + x^4 = \det(1 - xM)$, où $M = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$ la matrice d'adjacence de D.

Dans le but de prouver que tout polynôme de cliques de graphes pondérés est de la forme $\det(1 - xM)$, on ne peut pas inverser la dernière construction. En effet, l'application $\pi : D \to C$ de l'ensemble des graphes orientés vers l'ensemble des graphes simples n'est pas surjective, comme le montre l'exemple suivant.

Exemple 2.10. Soit C le graphe

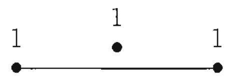


Figure 2.5 Graphe simple.

dont les sommets sont tous de degré 1. Son polynôme de cliques vaut $1 - 3\,x + x^2$. Or, il n'y a pas de graphe orienté D tel que $\pi(D) = C$; sinon D aurait 3 boucles de longueur 1 tel qu'exactement 2 d'entre elles seraient disjointes, ce qui est impossible. Cependant, on a $1 - 3\,x + x^2 = \det\left(1 - x\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}\right)$.

2.3 Théorème de Kim, Ormes et Roush

Dans leur caractérisation des polynômes de la forme $\det(1 - xM)$, où M est une matrice primitive à coefficients dans $\mathbb{N}$, Kim, Ormes et Roush (Kim, Ormes et Roush, 2000) ont démontré en particulier le théorème suivant.

Théorème 2.11 (KOR). *Un polynôme* $P(x) = \prod_{i=1}^{k} (1 - \lambda_i\, x)$, *où les* λ_i *sont des nombres complexes non nuls, est de la forme* $\det(1 - x\,M)$ *où* M *est une matrice carrée à coefficients entiers non négatifs si les conditions suivantes sont satisfaites :*

(1) les coefficients de $P(x)$ *sont tous entiers ;*

(2) il y a un indice i *tel que* $\lambda_i > |\lambda_j|$, *pour tout* $j \neq i$;

(3) $tr_n(\lambda_1, \ldots, \lambda_k) \geq 0$, *pour tout* $n \geq 1$, *où*

$$tr_n(\lambda_1, \ldots, \lambda_k) = \sum_{d\,|\,n} \mu\left(\frac{n}{d}\right) \left(\lambda_1^d + \ldots + \lambda_k^d\right).$$

On va démontrer que $P_C(x)$ vérifie ces trois conditions afin de démontrer qu'il est le polynôme réciproque de $\det(1 - xM)$. Par sa construction, $P_C(x)$ satisfait la première condition.

Soient B un sous-ensemble commutatif de A et $\deg(B)$ son degré. En appliquant la transformation $a \to x^{\deg(a)}$ à l'équation (2.1), on obtient

$$\sum_{u \in A^*/\sim_C} x^{|u|} = \frac{1}{\sum_B (-1)^{|B|} x^{\deg(B)}} = \frac{1}{P_C(x)}. \tag{2.2}$$

Ainsi, $\frac{1}{P_C(x)}$ est une série génératrice d'un monoïde partiellement commutatif libre. Lalonde (Lalonde, 1995) a démontré que tout monoïde partiellement commutatif libre se factorise en éléments de Lyndon.

Théorème 2.12. *Soit M un monoïde partiellement commutatif libre. Il existe un sous-ensemble L de M totalement ordonné tel que que tout élément $m \in M$ a une unique factorisation $m = \ell_1 \dots \ell_n$, où , $\ell_i \in L$, $i \in [n]$ et $\ell_1 \geq \dots \geq \ell_n$.*

Corollaire 2.13. *La série génératrice d'un monoïde partiellement commutatif libre M s'écrit*

$$\prod_{n=1}^{\infty} \left(\frac{1}{1 - x^n} \right)^{\alpha_n},$$

où α_n est le nombre de $\ell \in L$ de degré n.

Démonstration. Du théorème précédent, on a

$$\begin{aligned} \sum_{u \in A^*/\sim_C} u &= \prod_{\ell \in L} (1 + \ell + \ell^2 + \dots) \\ &= \left(\frac{1}{1 - \ell_1} \right) \left(\frac{1}{1 - \ell_2} \right) \dots \end{aligned}$$

En envoyant chaque lettre de ℓ sur x, on a

$$\sum_{u \in A^*/\sim_C} u = \prod_{n=1}^{\infty} \left(\frac{1}{1 - x^n} \right)^{\alpha_n},$$

où α_n est le nombre de mots de L de degré n.

Corollaire 2.14.

$$\alpha_n = \frac{1}{n} tr_n(\lambda_1, \dots, \lambda_k), \tag{2.3}$$

où

$$tr_n(\lambda_1, \dots, \lambda_k) = \sum_{d \mid n} \mu \left(\frac{n}{d} \right) \left(\lambda_1^d + \dots + \lambda_k^d \right).$$

Démonstration. Du corollaire précédent, on a

$$\sum_{u\in A^*/\sim_C} u = \frac{1}{\prod_{i=1}^{d}(1-\lambda_i\, x)} = \prod_{n=1}^{\infty}\left(\frac{1}{1-x^n}\right)^{\alpha_n}. \tag{2.4}$$

Du côté gauche de l'équation (2.4) on a

$$\begin{aligned}
\frac{1}{\prod_{i=1}^{d}(1-\lambda_i\, x)} &= \exp\left\{\ln\frac{1}{\left(\prod_{i=1}^{d}(1-\lambda_i\, x)\right)}\right\} = \exp\left\{\sum_{i=1}^{d}\ln\frac{1}{(1-\lambda_i\, x)}\right\}\\
&= \exp\left\{\sum_{i=1}^{d}\sum_{j=1}^{\infty}\lambda_i^j\,\frac{x^j}{j}\right\} = \exp\left\{\sum_{j=1}^{\infty}\left(\sum_{i=1}^{d}\lambda_i^j\right)\frac{x^j}{j}\right\}\\
&= \exp\left\{\sum_{j=1}^{\infty} tr^j(\lambda_1,\, \ldots,\, \lambda_k)\,\frac{x^j}{j}\right\} = \prod_{n=1}^{\infty}\left(\frac{1}{1-x^n}\right)^{\alpha_n},
\end{aligned} \tag{2.5}$$

où $tr^j(\lambda_1,\, \ldots,\, \lambda_k) = \sum_{d=1}^{k}\lambda_d^j$. Prenons la dérivée logarithmique et multiplions par x de part et d'autre de l'équation (2.5). Du côté gauche on a

$$\begin{aligned}
& x\,\frac{d}{dx}\left(\ln\left(\exp\left\{\sum_{j=1}^{\infty} tr^j(\lambda_1,\, \ldots,\, \lambda_k)\,\frac{x^j}{j}\right\}\right)\right) = x\,\frac{d}{dx}\left(\sum_{j=1}^{\infty} tr^j(\lambda_1,\, \ldots,\, \lambda_k)\,\frac{x^j}{j}\right)\\
&= x\left(\sum_{j=1}^{\infty} tr^j(\lambda_1,\, \ldots,\, \lambda_k)\,\frac{d}{dx}\,\frac{x^j}{j}\right) = x\left(\sum_{j=1}^{\infty} tr^j(\lambda_1,\, \ldots,\, \lambda_k)\,\frac{j\,x^{j-1}}{j}\right)\\
&= \sum_{j=1}^{\infty} tr^j(\lambda_1,\, \ldots,\, \lambda_k)\, x^j.
\end{aligned} \tag{2.6}$$

Du côté droit on a

$$\begin{aligned}
& x\,\frac{d}{dx}\left(\ln\left(\prod_{n=1}^{\infty}\left(\frac{1}{1-x^n}\right)^{\alpha_n}\right)\right) = x\,\frac{d}{dx}\left(\sum_{n=1}^{\infty}\ln\left((1-x^n)^{-\alpha_n}\right)\right)\\
&= x\,\frac{d}{dx}\left(\sum_{n=1}^{\infty}-\alpha_n\ln(1-x^n)\right) = x\sum_{n=1}^{\infty}-\alpha_n\,\frac{d}{dx}\left(\ln(1-x^n)\right)\\
&= x\sum_{n=1}^{\infty}-\alpha_n\,\frac{-n\,x^{n-1}}{1-x^n} = \sum_{n=1}^{\infty}\alpha_n\,\frac{n\,x^n}{1-x^n}\\
&= \sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\alpha_m\, m\, x^{m\,n}.
\end{aligned} \tag{2.7}$$

En combinant les équations (2.6) et (2.7), on obtient

$$\sum_{j=1}^{\infty} tr^j(\lambda_1, \ldots, \lambda_k)\, x^j = \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} \alpha_m\, m\, x^{m\,n}.$$

En comparant les coefficients de x^n de part et d'autre, on a

$$tr^j(\lambda_1, \ldots, \lambda_k) = \sum_{d\,|\,n} d\, \alpha_d.$$

En utilisant la formule d'inversion de Möbius, on a

$$\begin{aligned} n\,\alpha_n &= \sum_{d\,|\,n} \mu \binom{n}{d} \left(\lambda_1^d + \ldots + \lambda_k^d\right) \\ \Leftrightarrow \alpha_n &= \frac{1}{n}\, tr_n(\lambda_1, \ldots, \lambda_k). \end{aligned}$$

Du Corollaire 2.14, on a

$$\alpha_n = \frac{1}{n} \sum_{d\,|\,n} \mu \binom{n}{d} \left(\lambda_1^d + \ldots + \lambda_k^d\right),$$

où α_n désigne un certain nombre de mots ; d'où $\alpha_n \geq 0$. Ainsi, le polynôme de cliques pondéré satisfait la 3^e condition du Théorème 2.11.

La vérification que $P_C(x)$ satisfasse la seconde condition nécessite certains résultats provenant notamment de la théorie des séries rationnelles, de la théorie des graphes, de la théorie de Perron-Frobenius ainsi que du résultat suivant que nous démontrerons plus loin.

Proposition 2.15. *Soit la série formelle* $F(x) = \sum_{n=0}^{\infty} f_n\, x^n = \dfrac{1}{P_C(x)}$. *Si le graphe complémentaire* C *est connexe et si les degrés* d_s *des sommets* s *de* C *sont relativement premiers, alors cette série a une racine dominante unique qui est simple.*

Une lettre a est *liée* à une partie B de A si soit $a \in B$, soit il existe une lettre de B avec laquelle a ne commute pas. Si B_1 et B_2 sont 2 sous-ensembles commutatifs de A, on dit que B_2 est lié à B_1 si toute lettre de B_2 est liée à B_1.

Définition 2.16. Le *graphe de Cartier-Foata* D est le graphe orienté dont les sommets sont les sous-ensembles commutatifs de A, avec une arête $B_1 \to B_2$ si B_2 est lié à B_1.

L'ensemble des chemins de ce graphe s'identifie à l'ensemble des *formes normales de Cartier-Foata* (voir la notion de V-décomposition dans (Cartier et Foata, 1969), Section I.3).

Théorème 2.17 (Cartier-Foata). *Tout élément* $w \in A^*/\sim_C$ *admet une unique forme normale de Cartier-Foata* $w = [B_1][B_2]\dots[B_k]$, *où* B_{i+1} *est lié à* B_i, $i = 1, \dots, k-1$.

Définition 2.18. Un graphe orienté est *fortement connexe* si pour tous sommets s et t de ce graphe, il existe un chemin de s vers t.

Lemme 2.19. *Soit* C *le graphe des non commutations. Si* C *est connexe,* D *est un graphe fortement connexe.*

Démonstration. Il suffit de montrer que le graphe orienté D de Cartier-Foata a un sous-graphe D_1 tel que D_1 soit fortement connexe et que pour tout sommet s de D, il existe un chemin de s à D_1 et un chemin de D_1 à s.

Construisons D_1 à partir de l'ensemble B de tous les singletons de D : $B = \{a\}$, $a \in A$. Notons que si $a, b \in A$ ne commutent pas modulo la congruence $\sim_C$ ou si $a = b$, alors $\{b\}$ est lié avec $\{a\}$. Ainsi, D_1 a des arêtes $a \to b$ et $b \to a$ pour toutes lettres $a, b \in A$ telles que $a - b$ soit une arête de C. Donc, si C est connexe, D_1 est fortement connexe.

Maintenant, soit B un sommet de D. Si $b \in B$, alors $\{b\}$ est lié à B, donc, il y a une arête $B \to \{b\}$ dans D. Il reste à montrer qu'il y a un chemin dans D de D_1 vers B. On peut supposer que $|B| \geq 2$. On le démontre par récurrence sur $|B|$ et sur $d(B) = \min\{d(b_1, b_2) \mid b_1, b_2 \in B, b_1 \neq b_2\}$, où d est la distance dans le graphe C ; puisque B est un sous-ensemble commutatif de A, $d(B) \geq 2$.

Soit $a \in A$. Définissons $B_1 = \{b \in B \mid a - b \in C\}$ et $B' = (B \setminus B_1) \cup \{a\}$. Donc B' est commutatif. De plus B est lié avec B' : en effet, si $b \in B$ alors soit $b \in B \setminus B_1 \subseteq B'$, soit $b \in B_1$ et b ne commutent pas avec a par construction. D'où $B' \to B$ dans D.

Supposons tout d'abord que $d(B) = 2$. Alors, il existe 2 sommets b_1, $b_2 \in B$ tels que $d(b_1, b_2) = 2$ et on peut trouver $a \in A$ et les arêtes $b_1 - a - b_2$ dans $\overline{C}$. Alors B_1 ci-dessus satisfait $|B_1| \geq 2 \Rightarrow |B'| < |B|$ et on peut conclure par induction sur $|B|$.

Supposons que $d(B) \geq 3$. On peut trouver 2 sommets b_1, $b_2 \in B$ tels que $d(b_1, b_2) = d(B)$ et d'où $a \in A$ tel que $a - b_1$ dans $\overline{C}$ et $d(a, b_2) = d(b_1, b_2) - 1 \geq 2$. Alors B_1 satisfait $|B_1| \geq 1$, d'où $|B'| \leq |B|$. De plus, a, $b_2 \in B'$ (puisque $b_2 \notin B_1$, autrement $d(a, b_2) = 1$), donc $d(B') < d(B)$. Et on conclut par récurrence sur $d(B)$. □

Exemple 2.20. Soit C le graphe

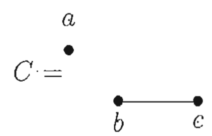


Figure 2.6 Graphe des commutations.

Son graphe complémentaire est

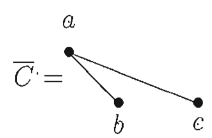


Figure 2.7 Graphe complémentaire.

Les sous-ensembles commutatifs de C sont $B_1 = \{a\}$, $B_2 = \{b\}$, $B_3 = \{c\}$ et $B_4 = \{b, c\}$.
Le graphe de Cartier-Foata est

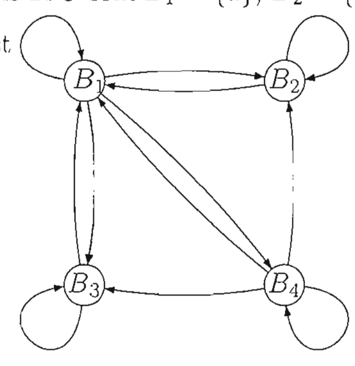


Figure 2.8 Graphe de Cartier-Foata.

Définition 2.21. Une *matrice entière non négative polynomiale* est une matrice carrée dont les entrées sont dans $x\,\mathbb{N}(x)$; i.e. les entrées sont des polynômes en la variable x de terme constant nul à coefficients entiers non négatifs.

Soit $M = M_{i,j}$ une telle matrice, on va construire une matrice N à coefficients entiers non négatifs. Cette construction est appelée le *procédé de linéarisation*. Soit r la dimension de M, on construit r sommets étiquetés de 1 à r. Prenons l'entrée $M_{i,j}$ qui est de la forme $a_1\,x + a_2\,x^2 + \ldots a_k\,x^k$. En rajoutant des nouveaux sommets entre i et j, on construit a_h chemins de longueur h entre les sommets i et j, $h = 1, \ldots, k$. On obtient ainsi un graphe orienté dont la matrice d'adjacence est N.

Proposition 2.22. *(voir (Boyle, 1993), Section 5.3) Soient M et N deux matrices définies au paragraphe précédent, alors* $\det(1 - M) = \det(1 - x\,N)$.

Exemple 2.23. Soit $M = \begin{bmatrix} 0 & x^2 \\ 2\,x^3 & x + x^3 \end{bmatrix}$. On a $\det(1 - M) = 1 - x - x^3 - 2\,x^5$. On lui associe le graphe

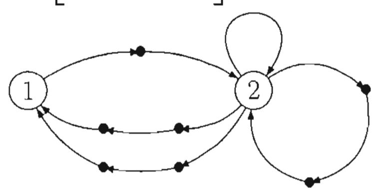


Figure 2.9 Graphe orienté obtenu par le procédé de linéarisation.

Sa matrice d'adjacence N est

$$N = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

On a $\det(1 - x\,N) = 1 - x - x^3 - 2\,x^5 = \det(1 - M)$.

Définition 2.24. Une matrice M est dite *réductible* s'il existe une matrice de permutations P telle que

$$P\,M\,P^{-1} = \begin{bmatrix} A & B \\ 0 & C \end{bmatrix},$$

où A et C sont des matrices carrées de dimensions supérieures ou égales à 1. S'il n'existe pas une telle matrice de permutations, alors M est dite *irréductible*.

Définition 2.25. Un graphe orienté est dit *irréductible* si sa matrice d'adjacence est une matrice irréductible.

Le résultat suivant est bien connu.

Lemme 2.26. *Soit M une matrice, M est irréductible si et seulement si le graphe G dont M est sa matrice d'adjacence est fortement connexe.*

Définition 2.27. Une matrice non négative M est dite *primitive* s'il existe un entier $k \geq 1$ tel que tous les coefficients de M^k soient strictement positifs. Il s'ensuit qu'une matrice primitive est irréductible. Un graphe est *primitif* si et seulement si la matrice d'adjacence est primitive.

Définition 2.28. L'*indice d'imprimitivité* d'un graphe fortement connexe est le plus grand commun diviseur des longueurs des chemins fermés de ce graphe.

Théorème 2.29. *(Voir (Marcus, Roth et Siegel, 2001), Prop. 3.8) Un graphe irréductible est primitif si et seulement si l'indice d'imprimitivité est égal à 1.*

Définition 2.30. On appelle *rayon spectral* d'une matrice carrée le maximum des modules des valeurs propres.

Théorème 2.31 (Perron). *(voir (Boyle, 2005), Thm 2.2) Soit M une matrice primitive à coefficients dans $\mathbb{R}_+$ de rayon spectral λ. Alors λ est une racine simple du polynôme caractéristique qui est strictement supérieure au module de toute autre valeur propre. De plus, le vecteur propre associé à λ comporte uniquement des valeurs strictement positives.*

Démonstration de la Proposition 2.15.

1. Soient A l'ensemble des lettres et D le graphe de Cartier-Foata. À ce graphe, on associe la matrice d'adjacence M, où les lignes et les colonnes sont indexées par les sous-ensembles commutatifs de A, et la donnée en la position (B_1, B_2) est $x^{deg(B_2)}$. Cette matrice est une matrice non négative polynomiale. Soit λ_B le vecteur ligne ayant des 1 en position B et 0 ailleurs, et γ le vecteur colonne ayant seulement des 1.

2. Soit σ un nouveau symbole et définissons un nouveau graphe orienté E' en ajoutant le sommet σ et les arêtes $\sigma \to B$ pour tout sommet B dans D'. Clairement, l'ensemble des formes normales de Cartier-Foata est en bijection avec l'ensemble des chemins dans E' débutant en σ.

3. Il s'ensuit que la série de Hilbert de $A^*/\sim_C$ est

$$1 + \sum_B x^{\deg(B)}\, \lambda_B\, M^*\, \gamma,$$

où B parcourt l'ensemble de tous les sous-ensembles commutatifs de A.

4. Par le procédé de linéarisation, on associe à M une matrice carrée N à coefficients dans $\mathbb{N}$ telle que tout coefficient de M^* est égal à la somme des coefficients de $(xN)^*$. Puisque

$\overline{C}$ est connexe, on a du Lemme 2.19 que D est fortement connexe. Par conséquent, N est une matrice irréductible par le Théorème 2.26. De plus, comme les entrées de la diagonale de M contiennent x^{d_s} et comme les d_s sont supposés relativement premiers, alors N est une matrice primitive par le Théorème 2.29.

5. On en déduit que cette série formelle s'écrit comme 1+ une somme non triviale de termes de la forme $x^k\,(xN)^*_{i\,j}$, $k \in \mathbb{N}$.

6. Comme N est primitive, on a du théorème de Perron que ses valeurs propres, comptées avec leurs multiplicités sont $\lambda_1, \ldots, \lambda_m$, avec $\lambda_1 > |\lambda_2|, \ldots, |\lambda_m|$ et λ_1 est simple. Par la forme normale de Jordan et du Théorème de Schützenberger, chaque série $(xN)^*_{i\,j}$ est rationnelle. Du Corollaire 1.17, ces séries sont de de la forme $\sum_{n\geq 0} a_n\, x^n$, avec

$$a_n = h\,\lambda_1^n + \sum_{s=2}^{m} P_s(n)\,\lambda_s^n,$$

pour n suffisamment grand.

7. Le coefficient dominant h, doit être positif. En effet, comme N est primitive, on a N^q strictement positif pour une certaine puissance q. Alors, pour tous indices u, v, $a_{n+2q} = (N^{n+2q})_{i,j} \geq (N^q)_{i,u}\,(N^n)_{u,v}\,(N^q)_{v,j}$; donc $(N^n)_{u,v} \leq C\,a_{n+2q}$, pour une certaine constante C. Donc, si $h = 0$, alors R^n s'accroît plus lentement que λ_1^n, contradiction. Donc $h \neq 0$ et $h > 0$ puisque $a_n \geq 0$ et $a_n \sim h\,\lambda_1^n$, lorsque $n \to \infty$.

8. Notons que si a_n a un coefficient dominant positif, alors $x^k\,a_n$ également. Ce qui implique par l'étape 5 que (f_n) a λ_1 comme racine dominante, qui est simple.

□

On peut maintenant démontrer que $P_C(x)$ vérifie la condition (ii) du Théorème de Kim, Ormes et Roush. Supposons d'abord que les deux conditions de la Proposition 2.15 soient satisfaites : i.e. C est connexe et les degrés d_s des monômes x^{d_s}, où s est un sommet, sont relativement premiers. La Proposition 2.15 implique que $\frac{1}{P_C(x)} = \sum_{n\geq 0} f_n\, x^n$ et pour un n suffisamment grand,

$$f_n = h\,\lambda_1^n + \sum_{i=2}^{\ell} P_i(n)\,\lambda_i^n,$$

avec $\lambda_1 > |\lambda_2|, \ldots, |\lambda_\ell|$ et $h \neq 0$. Il s'ensuit que $\sum_{n\geq 0} f_n\,x^n$ est la somme d'un polynôme, de $\frac{h}{1-\lambda_1 x}$ et d'une combinaison $\mathbb{C}$-linéaire de fractions de la forme $\frac{x^s}{(1-\lambda_i x)^t}$, $i \geq 2$. Donc, le dénominateur $P_C(x)$, est un produit de $(1-\lambda_1 x)$ avec des facteurs de la forme $(1-\lambda_i x)^t$, ce qui démontre (ii).

Il reste à relaxer les deux hypothèses de la Proposition 2.15. Si $\overline{C}$ n'est pas connexe, alors le polynôme de cliques pondéré de C est un produit de plus petits polynômes de cliques pondérés. Il suffit alors de prendre pour M la somme diagonale des matrices correspondantes.

Si les entiers d_s ne sont pas relativement premiers, soit p leur plus grand diviseur commun et on prend comme nouveau degré $\frac{1}{p}\,d_s$. Cela suffit pour montrer que toute matrice carrée M ayant des coefficients entiers non négatifs, $\det(1 - x\,M)\,|_{x\to x^p}$ est aussi de la forme $\det(1-x\,M')$, pour une quelconque matrice M' sur $\mathbb{N}$. Ce qui est démontré en appliquant une fois de plus le procédé de linéarisation.

CHAPITRE III

POLYNÔMES DE CLIQUES GÉNÉRALISÉS

On va définir les polynômes de cliques généralisés et on va montrer que l'ensemble de ces polynômes coïncide avec les polynômes de la forme $\det(1 - x\,M)$, où M est une matrice à coefficients réels non négatifs (Théorème 3.3). La démonstration de ce résultat est similaire à celle du Théorème 2.4 sauf qu'on va utiliser le théorème spectral de Boyle et Handelman (Boyle et Handelman, 1991) au lieu de celui de Kim, Ormes et Roush (Kim, Ormes et Roush, 2000). Par ailleurs tous les résultats utilisant les monoïdes partiellement commutatifs libres (Cartier et Foata, 1969) seront utilisés de manière analogue en appliquant la spécialisation $a \mapsto \alpha_a\, x^{d_a}$ à toute lettre du monoïde $A^*/\sim_C$.

3.1 Polynômes de cliques généralisés

Nous avons vu au Chapitre 2 le polynôme de cliques associé à un graphe simple C. On va généraliser ce polynôme en associant à tout sommet s de C un monôme de la forme $\alpha_s\, x^{d_s}$, $\alpha_s \in \mathbb{R}_+$ et $d_s \in \mathbb{N}$. Si tous les α_s valent 1, on est ramené au polynôme de cliques de graphes pondérés $P_C(x)$. De plus, si tous les $d_s = 1$, on retrouve le polynôme de cliques. Soit B un sous-ensemble de sommets, on définit le *degré* de B par $\prod_{s \in B} \alpha_s\, x^{d_s}$.

Définition 3.1. Soit C un graphe simple dont les sommets sont pondérés par des monômes de la forme $\alpha_s\, x^{d_s}$, $\alpha_s \in \mathbb{R}_+$ et $d_s \in \mathbb{N}$. Le *polynôme de cliques généralisé de C* est défini par

$$PG_C(x) = 1 + \sum_{B} (-1)^{|B|} \left(\prod_{s \in B} \alpha_s\, x^{d_s} \right),$$

où la somme parcourt tous les sous-graphes complets B de C.

Exemple 3.2. Le polynôme de cliques généralisé du graphe pondéré suivant

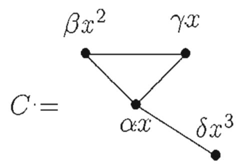


Figure 3.1 Graphe simple pondéré

est $PG_C(x) = 1 - \alpha\, x - \beta\, x^2 - \gamma\, x - \delta\, x^3 + \alpha\, \delta\, x^4 + \alpha\, \beta\, x^3 + \beta\, \gamma\, x^3 + \alpha\, \gamma\, x^2 - \alpha\, \beta\, \gamma\, x^4$.

Considérons maintenant une autre classe de polynômes. Soit M une matrice carrée à coefficients réels non négatifs et soit le polynôme $\det(1 - x\, M)$, où 1 est la matrice identité de la taille appropriée. Ce polynôme est le polynôme réciproque du polynôme caractéristique de M.

Théorème 3.3. *Les polynômes de cliques généralisés coïncident avec les réciproques de polynômes caractéristiques de matrices carrées à coefficients réels non négatifs.*

Soit M une matrice à coefficients réels non négatifs ; on va montrer que $\det(1 - xM)$ est un polynôme de cliques généralisé.

Soient D un graphe orienté et M sa matrice d'adjacence. On construit le graphe des circuits C de D de la même manière qu'au chapitre précédent. On pondère chaque sommet s de C par $\alpha_s\, x^{d_s}$, où $\alpha_s \in \mathbb{R}_+$ est le produit des poids de chaque arête du circuit correspondant à s et d_s est la longueur du circuit.

En développant le déterminant $\det(1 - x\, M)$ par la formule impliquant les permutations et en décomposant celles-ci en cycles, on a

$$\det(1 - x\, M) = \sum_{\{c_1, \ldots, c_k\}} (-1)^k \left(\prod_{i=1}^{k} \alpha_{c_i} \right) x^{|c_1| + \ldots + |c_k|},$$

où $k \in \mathbb{N}$, $\{c_1, \ldots, c_k\}$ est un ensemble de k circuits simples (sans sommet répété) disjoints, où $|c_i|$ représente la longueur de c_i et où $\prod_{i=1}^{k} \alpha_{c_i}$ est le poids total des circuits composant la permutation. Par définition du polynôme de cliques généralisé, on a $\det(1-xM) = PG_C(x)$. Ce qui démontre que $\det(1-xM)$ est un polynôme de cliques généralisé.

Exemple 3.4. Soit $M = \begin{bmatrix} \alpha & \beta & 0 & 0 \\ 1 & \gamma & \delta & 0 \\ 0 & 0 & 0 & 1 \\ 0 & \epsilon & 0 & 0 \end{bmatrix}$, où α, β, γ, δ, $\epsilon \in \mathbb{R}_+$. M est la matrice d'adjacence du graphe D suivant.

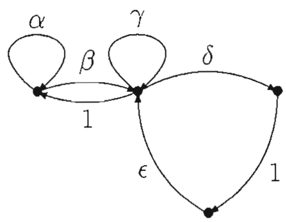


Figure 3.2 Graphe orienté pondéré.

Son graphe des circuits C est

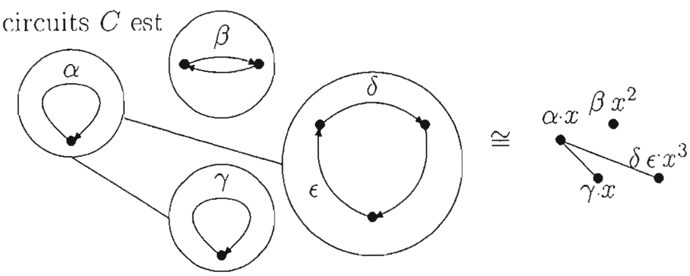


Figure 3.3 Graphe des circuits.

Son polynôme de cliques généralisé vaut

$$\begin{aligned} PG_C(x) &= 1 - \alpha\, x - \gamma\, x - \beta\, x^2 - \delta\, \epsilon\, x^3 + \alpha\, \gamma\, x^2 + \alpha\, \delta\, x^4 \\ &= \det(1 - x\, M). \end{aligned}$$

Dans le but de prouver que tout polynôme de cliques généralisé est de la forme $\det(1 - x\,M)$, il ne suffit pas d'inverser la dernière construction. L'exemple 2.10 montre qu'un graphe simple n'est pas toujours le graphe des circuits d'un graphe orienté.

3.2 Théorème de Boyle et Handelman

Ainsi, afin de que le polynôme de cliques généralisé est le polynôme réciproque de $\det(1 - xM)$, où M est une matrice à coefficients réels non négatifs, on va utiliser le résultat fondamental suivant de Boyle et Handelman (Boyle et Handelman, 1991).

Théorème 3.5 (Boyle et Handelman). *Un polynôme* $P(x) = \prod_{i=1}^{k}(1 - \lambda_i\,x)$, *où les* λ_i *sont des nombres complexes non nuls, est de la forme* $\det(1 - x\,M)$ *où* M *est une matrice carrée à coefficients réels non négatifs si les conditions suivantes sont satisfaites :*

(1) les coefficients de $P(x)$ *sont tous réels ;*

(2) il y a un indice i *tel que* $\lambda_i > |\lambda_j|$, *pour tout* $j \neq i$ *;*

(3) soient $n \geq 1$ *et* $m \geq 1$ *deux entiers positifs,*

(i) $tr^n(\lambda_1, \ldots, \lambda_k) = \sum_{i=1}^{k} \lambda_i^n \geq 0$,

(ii) $tr^n(\lambda_1, \ldots, \lambda_k) > 0 \Rightarrow tr^{nm}(\lambda_1, \ldots, \lambda_k) > 0$.

On va démontrer que $PG_C(x)$ vérifie ces trois conditions.

Remarque 3.6. Il est connu qu'une série $F(x)$ de la forme $(\det(1 - x\,M))^{-1}$ avec M une matrice carrée réelle non négative, est $\mathbb{R}_+$-rationnelle. Cependant, la réciproque n'est pas vraie. En effet, soit

$$F(x) = \frac{1}{1 - 3\,x + 5\,x^2 - 8\,x^3}.$$

Au chapitre 2, on a vu que cette série est $\mathbb{N}$-rationnelle. On a

$$PG_C(x) = 1 + \sum_{i=1}^{\infty} (-1)^i\, e_i\, x^i,$$

où e_i est la i^e *fonction symétrique élémentaire* (voir (Macdonald, 1995)). Puisque $p_n = tr^n(\lambda_1, \ldots, \lambda_k) = \sum_{i=1}^{k} \lambda_i^n$, où p_n est la n^e *fonction symétrique somme de puissances*, si on suppose que $1 - 3x + 5x^2 - 8x^3$ est de la forme $\det(1 - xM)$, on aurait que

$$p_2 = e_1^2 - 2\,e_2 = 3^2 - 2 \cdot 5 = -1 < 0.$$

Du Théorème 3.5, $1 - 3\,x + 5\,x^2 - 8\,x^3$ n'est pas le spectre d'une matrice carrée à coefficients réels non négatifs.

Par construction de $PG_C(x)$, la première condition du Théorème 3.5 est satisfaite. Pour vérifier que le spectre de $PG_C(x)$ satisfasse la seconde condition du Théorème 3.5, il va falloir utiliser un résultat suivant qui est une généralisation de la Proposition 2.15 et que nous démontrerons plus loin.

Proposition 3.7. *Soit* $F(x) = \sum_{n=0}^{\infty} f_n\,x^n = \dfrac{1}{PG_C(x)}$ *une série formelle. Si le graphe complémentaire* $\overline{C}$ *est connexe et si les degrés* d_s *des poids* $\alpha_s\,x^{d_s}$ *des sommets* s *de* C *sont relativement premiers, alors cette série a une racine dominante unique qui est simple.*

Remarque 3.8. Le procédé de linéarisation défini au chapitre précédent s'applique également à une *matrice réelle non négative polynomiale*. En effet, soit M une telle matrice, on va construire une matrice à coefficients réels non négatifs.

Soit r la dimension de M, on construit r sommets étiquetés de 1 à r. Prenons l'entrée $M_{i,j}$ qui est de la forme $a_1\,x + a_2\,x^2 + \ldots a_k\,x^k$. En ajoutant des nouveaux sommets, on construit k chemins entre les sommets i et j comme suit. Chaque chemin sera de longueur h, $h = 1, \ldots, k$, la première arête de ce chemin aura le poids a_h tandis que les autres arêtes seront toutes de poids 1. On obtient ainsi un graphe orienté dont la matrice adjacente est N.

Proposition 3.9. *Soient* M *et* N *deux matrices définies au paragraphe précédent, alors* $\det(1 - M) = \det(1 - x\,N)$.

La preuve est identique à celle de la démonstration de la Proposition 2.22.

Exemple 3.10. Soit $M = \begin{bmatrix} 0 & \alpha\, x^2 \\ \beta\, x^3 & \gamma\, x + \delta\, x^3 \end{bmatrix}$. On lui associe le graphe

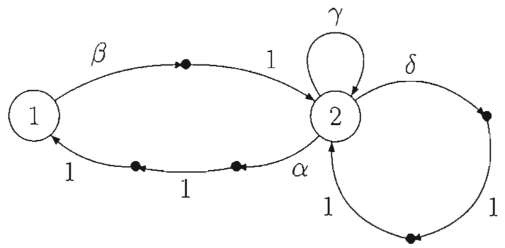


Figure 3.4 Graphe orienté pondéré obtenu par le procédé de linéarisation.

Sa matrice d'adjacence N est

$$N = \begin{bmatrix} 0 & \beta & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \gamma & \delta & 0 & \alpha & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

On a $\det(1 - M) = \det(1 - x\, N) = 1 - \gamma\, x - \delta\, x^3 - \alpha\, \beta\, x^5$.

Démonstration de la Proposition 3.7.

Soit C le graphe simple non orienté pondéré associé à $PG_C(x)$. Soit C' le graphe obtenu de C en étiquetant chaque sommet par une lettre. Supposons C connexe, alors C' est connexe. Supposons également que les d_s sont relativement premiers. Soient D' le graphe de Cartier-Foata associé à C' et M' sa matrice d'adjacence. On applique la spécialisation $a \mapsto \alpha_a\, x^{d_a}$ à M' et on obtient une matrice M. La suite de la démonstration est identique à celle de la Proposition 2.15 à la différence qu'on utilise le procédé de linéarisation défini ci-haut.

□

On peut maintenant démontrer la condition (2) du théorème 3.5. On peut supposer que les 2 conditions de la Proposition 3.7 sont satisfaites : i.e. $\overline{C}$ est connexe et les degrés d_s des monômes $\alpha_s\, x^{d_s}$, où s est un sommet, sont relativement premiers. La Proposition 3.7 implique que $\frac{1}{PG_C(x)} = \sum_{n\geq 0} f_n\, x^n$ et pour un n suffisamment grand,

$$f_n = h\,\lambda_1^n + \sum_{i=2}^{\ell} P_i(n)\,\lambda_i^n,$$

avec $\lambda_1 > |\lambda_2|, \ldots, |\lambda_\ell|$ et $h \neq 0$. Il s'ensuit que $\sum_{n\geq 0} f_n\, x^n$ est la somme d'un polynôme, de $\frac{h}{1-\lambda_1\, x}$ et d'une combinaison $\mathbb{C}$-linéaire de fractions de la forme $\frac{x^s}{(1-\lambda_i\, x)^t}$, $i \geq 2$. Donc, le dénominateur $P(x)$ est un produit de $(1-\lambda_1\, x)$ avec des facteurs de la forme $(1-\lambda_i\, x)^t$, ce qui démontre (2).

Il reste à montrer qu'on peut se ramener aux deux hypothèses de la Proposition 3.7. Si $\overline{C}$ n'est pas connexe, alors le polynôme de cliques généralisé de C est un produit de plus petits polynômes de cliques généralisés. Il suffit alors de prendre pour M la somme diagonale des matrices correspondantes.

Si les entiers d_s ne sont pas relativement premiers, soit p leur plus grand diviseur commun et on prend comme nouveau degré $\frac{1}{p}\, d_s$. Cela suffit pour montrer que toute matrice carrée M ayant des coefficients réels non négatifs, $\det(1 - x\,M)\ |_{x\to x^p}$ est aussi de la forme $\det(1 - x\,M')$, pour une quelconque matrice M' sur $\mathbb{R}_+$. Ce qui est démontré en appliquant une fois de plus le procédé de linéarisation.

Il reste à démontrer que le polynôme de cliques généralisé vérifie la troisième condition du théorème 3.5.

Définition 3.11. Dans $A^*/\sim_C$, une *pyramide à gauche* est un élément $p \neq 1$ tel que :

1) il existe une lettre $a \in A$ et un élément $u \in A^*/\sim_C$ tels que $p = au$;

2) pour toute lettre $b \in A$ et tout élément $v \in A^*/\sim_C$ tels que $p = bv$, on a $a = b$.

Cette définition est équivalente à celle de Viennot (Viennot, 1986) ; en effet, une pyramide à gauche est l'image miroir d'une pyramide de Viennot, qui a donné cette définition dans le cadre des empilements, dont la théorie est équivalente à celles des monoïdes partiellement commutatifs libres.

Théorème 3.12 (Viennot). *La série formelle indexée par les pyramides est donnée par*

$$\sum_{p} \frac{1}{|p|} p =_{comm} \ln\left(\frac{1}{\sum_{B}(-1)^{|B|} B}\right), \tag{3.1}$$

où $=_{comm}$ *signifie que l'identité a lieu dans le monoïde commutatif libre sur* A.

Voir (Viennot, 1986) ou (Krattenthaler, 2006).

Vérifions que $PG_C(x)$ vérifie la condition 3(i). Puisque $P(0) = 1$, on a $P(x) = \prod_{i=1}^{k}(1 - \lambda_i x)$, où $\lambda_i \in \mathbb{C}$; ainsi

$$\begin{aligned} \ln\left(\frac{1}{\prod_{i=1}^{k}(1-\lambda_i x)}\right) &= \sum_{i=1}^{k} \ln\left(\frac{1}{1-\lambda_i x}\right) = \sum_{i=1}^{k}\sum_{n=1}^{\infty} \lambda_i^n \frac{x^n}{n} \\ &= \sum_{n=1}^{\infty}\sum_{i=1}^{k} \lambda_i^n \frac{x^n}{n} = \sum_{n=1}^{\infty} tr^n(\lambda_1, \ldots, \lambda_k)\frac{x^n}{n}. \end{aligned}$$

Appliquons la spécialisation $\psi : a \mapsto \alpha_a x^{d_a}$ de chaque côté de l'équation (3.1). Du côté droit, on a

$$\ln\left(\frac{1}{PG_C(x)}\right) = \sum_{n=1}^{\infty} tr^n(\lambda_1, \ldots, \lambda_k)\frac{x^n}{n}.$$

Du côté gauche, on a

$$\sum_{p} \frac{1}{|\psi(p)|}\psi(p),$$

où $\psi(p) = \prod_{a\in p} \alpha_a x^{d_a}$. Définissons le *degré d'une pyramide* par $\deg(P) = \prod_{a \in p} x^{d_a}$. On a donc

$$\begin{aligned} \sum_{p} \frac{1}{|\psi(p)|}\psi(p) &= \sum_{p}\frac{1}{|p|}\prod_{a\in p}\alpha_a x^{d_a} \\ &= \sum_{p}\frac{1}{|p|} x^{\deg(p)} \prod_{a\in p}\alpha_a. \end{aligned}$$

En combinant ces résultats, on a l'égalité

$$\begin{aligned}\sum_{n=1}^{\infty} tr^n(\lambda_1, \ldots, \lambda_k)\,\frac{x^n}{n} &= \sum_{p} \frac{1}{|p|}\, x^{\deg(p)} \prod_{a\in p} \alpha_a \\ &= \sum_{n=1}^{\infty} x^n \sum_{p,\, \deg(p)=n} \frac{1}{|p|} \prod_{a\in p} \alpha_a.\end{aligned}$$

Pour tout $n \geq 1$, comparons les coefficients de x^n de part et d'autre, on a

$$tr^n(\lambda_1, \ldots, \lambda_k) = n \sum_{p,\, |p|=\deg(p)=n} \prod_{a\in p} \alpha_a \geq 0.$$

Pour vérifier la condition 3 (ii), on va utiliser le résultat suivant.

Proposition 3.13. *p est une pyramide gauche si et seulement si dans sa forme normale de Cartier-Foata, $p = [B_1][B_2]\ldots[B_k]$, on a $|B_1| = 1$.*

Démonstration. ($\Rightarrow$) Supposons que $p = [B_1][B_2]\ldots[B_k]$ est une pyramide à gauche. Alors nécessairement $|B_1| = 1$. En effet, si $|B_1| \geq 2$, alors pour tout a, $b \in B_1$ tels que $a \neq b$, on aurait $p = au = bv$, contradiction car p est une pyramide à gauche.

($\Leftarrow$) Supposons $p = [B_1][B_2]\ldots[B_k]$ où $|B_1| = 1$. Écrivons $B_1 = \{a\}$, on a $p = a[B_2]\ldots[B_k]$. Par l'unicité de la forme normale de Cartier-Foata (Théorème 2.17), si $p = au = bv$, alors $a = b$. Donc p est une pyramide gauche. □

Vérifions maintenant la condition 3(ii). Supposons $tr^n(\lambda_1, \ldots, \lambda_k) > 0$, il existe donc une pyramide gauche p de degré n. Alors, pour tout $m \geq 1$, on peut construire une pyramide gauche de degré nm en concaténant m pyramides gauches p.

En effet, soit $p = [B_1][B_2]\ldots[B_k]$ une telle pyramide gauche, on peut supposer $k \geq 2$. De la proposition 3.13, $B_1 = \{a\}$. Considérons les deux cas suivants.

1. Si a est liée à B_k, p^m a la forme normale de Cartier-Foata

$$p^m = \underbrace{[B_1][B_2]\ldots[B_k] \quad [B_1][B_2]\ldots[B_k] \quad \ldots \quad [B_1][B_2]\ldots[B_k]}_{m\, fois}.$$

2. Si a n'est pas lié à B_k, alors $a \notin B_k$ et $B_k \cup \{a\}$ est un ensemble commutatif. On a que B_2 lié à $B_k \cup \{a\}$; en effet, si $b \in B_2$, b est lié à $B_1 = \{a\}$, donc soit $b = a$, soit b ne commute pas avec a. Dans les deux cas, b est lié avec $B_k \cup \{a\}$. Donc, p^m a la forme normale de Cartier-Foata

$$p^m = [B_1] \underbrace{[B_2] \dots [B_k \cup \{a\}] \quad [B_2] \dots [B_k \cup \{a\}] \quad \dots \quad [B_2] \dots [B_k \cup \{a\}]}_{m-1\, fois} \quad [B_2] \dots [B_k].$$

Dans les deux cas, puisque $B_1 = \{a\}$, on a de la Proposition 3.13 que p^m est une pyramide gauche de degré nm. Ainsi, on a $tr^{nm}(\lambda_1, \dots, \lambda_k) > 0$.

CHAPITRE IV

$\mathbb{N}$-RATIONALITÉ DE CERTAINES SÉRIES.

Au premier paragraphe, on va déterminer une condition nécessaire et suffisante pour qu'une série de la forme $(1 - ax + bx^k)^{-1}$ soit $\mathbb{N}$-rationnelle, $a \in \mathbb{N}$, $b \in \mathbb{Z}$ et $k \geq 2$ (Théorème 4.3). À la deuxième section on fera de même pour les séries de la forme $(1 - ax + bx^2 + cx^3)^{-1}$, $a \in \mathbb{N}$, $b, c \in \mathbb{Z}$ (Théorème 4.12).

4.1 $\mathbb{N}$-rationalité des séries de la forme $(1 - ax + bx^k)^{-1}$

Théorème 4.1 (Mantel). *Soient a, $b \in \mathbb{N}$. Alors il existe un graphe simple non orienté ayant a sommets et b arêtes sans triangle si et seulement si $4b \leq a^2$.*

On peut consulter (Bollobas, 1998), Théorème I.2 pour la démonstration. Ce résultat a été généralisé par Turan dans la théorie des graphes extrémaux ; (voir (Bollobas, 1998), Chapitre 4).

La condition du Théorème de Mantel est liée à la $\mathbb{N}$-rationalité des séries de la forme $(1 - ax + bx^2)^{-1}$, où $a \in \mathbb{N}$ et $b \in \mathbb{Z}$.

Théorème 4.2. *Soit $f(x) = (1 - ax + bx^2)^{-1}$, où $a \in \mathbb{N}$ et $b \in \mathbb{Z}$; alors $f(x)$ est $\mathbb{N}$-rationnelle si et seulement si $4b \leq a^2$.*

Démonstration. ($\Leftarrow$) Supposons $4b \leq a^2$. Si a est pair,

$$\frac{1}{1 - ax + bx^2} = \frac{1}{1 - 2\left(\frac{ax}{2}\right) + \frac{a^2}{4}x^2 - \frac{a^2}{4}x^2 + bx^2} = \frac{1}{\left(1 - \frac{ax}{2}\right)^2 - \left(\frac{a^2}{4} - b\right)x^2}$$

$$= \frac{\left(\left(\frac{ax}{2}\right)^*\right)^2}{1-\left(\left(\frac{ax}{2}\right)^*\right)^2\left(\frac{a^2}{4}-b\right)x^2} = \left(\left(\frac{ax}{2}\right)^*\right)^2 + \left(\left(\left(\frac{ax}{2}\right)^*\right)^2\left(\frac{a^2}{4}-b\right)x^2\right)^*.$$

Comme $4b \leq a^2$ par hypothèse, tous les coefficients de la série sont non négatifs. Donc $f(x)$ est $\mathbb{N}$-rationnelle.

Si a est impair, l'hypothèse devient $4b \leq a^2 - 1$.

$$\begin{aligned}
\frac{1}{1-ax+bx^2} &= \frac{1}{\left(1-\frac{a-1}{2}x\right)\left(1-\frac{a+1}{2}x\right)-\left(\frac{a^2-1}{4}-b\right)x^2} \\
&= \frac{\left(\frac{a-1}{2}x\right)^*}{1-\frac{a+1}{2}x-\left(\frac{a^2-1}{4}-b\right)\left(\frac{a-1}{2}x\right)^*x^2} \\
&= \left(\frac{a-1}{2}x\right)^*\left(\frac{a+1}{2}x+\left(\frac{a^2-1}{4}-b\right)\left(\frac{a-1}{2}x\right)^*x^2\right)^*
\end{aligned}$$

Comme $4b \leq a^2 - 1$ par hypothèse, tous les coefficients de la série sont non négatifs. Donc $f(x)$ est $\mathbb{N}$-rationnelle.

($\Rightarrow$) Supposons que $f(x)$ soit $\mathbb{N}$-rationnelle. Soit $p(x) = x^2 - ax + b$ le polynôme réciproque du dénominateur de $f(x)$. Puisque $f(x)$ est $\mathbb{N}$-rationnelle, du Théorème de Berstel, on a que le module maximal des racines de $p(x)$ est une racine de $p(x)$. Il s'ensuit que $p(x)$ a deux racines réelles. Il s'ensuit que le discriminant $a^2 - 4b$ de $p(x)$ est non négatif, d'où $4b \leq a^2$. □

On va généraliser ce résultat en déterminant une condition nécessaire et suffisante pour qu'une série de la forme $(1 - ax + bx^k)^{-1}$, où $a \in \mathbb{N}$, $b \in \mathbb{Z}$ et $k \geq 2 \in \mathbb{N}$ soit $\mathbb{N}$-rationnelle (Théorème 4.3). Ce résultat nous a été suggéré par des expérimentations par ordinateur en utilisant le paquetage RLangGFun (Maple) de Koutschan (Koutschan, 2005) ou (Koutschan, 2008)

Posons $\Delta = (k-1)^{k-1}a^k - k^k b$.

Théorème 4.3. *Soit*

$$f(x) = \frac{1}{1 - a\,x + b\,x^k}, \quad a \in \mathbb{N},\ b \in \mathbb{Z},\ k \geq 2.$$

$f(x)$ est $\mathbb{N}$-rationnelle si et seulement si $\Delta \geq 0$.

Remarque 4.4. Le *discriminant* du polynôme réciproque du dénominateur de $f(x)$ est

$$\begin{cases} -b^{k-2}\,\Delta, & \text{si } k \equiv 0 \mod 4 \text{ ou } k \equiv 1 \mod 4, \\ b^{k-2}\,\Delta, & \text{si } k \equiv 2 \mod 4 \text{ ou } k \equiv 3 \mod 4. \end{cases}$$

Démonstration. Soient $p = p(x) = a_n\,x^n + \ldots + a_1\,x + a_0$ et $q = q(x) = b_m\,x^m + \ldots + b_1\,x + b_0$ deux polynômes de degré n et m respectivement. *La matrice de Sylvester* de p et q, notée $S(p, q)$ est la matrice carrée de dimension $n + m$ définie par

$$S(p,\,q) = \begin{bmatrix} a_n & a_{n-1} & \ldots & \ldots & \ldots & a_0 & 0 & \ldots & \ldots & 0 \\ 0 & a_n & a_{n-1} & \ldots & \ldots & \ldots & a_0 & 0 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & a_n & a_{n-1} & \ldots & \ldots & \ldots & \ldots & a_0 \\ b_m & b_{m-1} & \ldots & b_1 & b_0 & 0 & \ldots & \ldots & \ldots & 0 \\ 0 & b_m & b_{m-1} & \ldots & b_1 & b_0 & 0 & \ldots & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \ldots & \ldots & \ldots & 0 & b_m & b_{m-1} & \ldots & b_1 & b_0 \end{bmatrix}.$$

Il est connu dans la littérature que

$$disc(p(x)) = (-1)^{\frac{n\,(n-1)}{2}}\ \det(S(p,\,p')).$$

On peut consulter (Coste, 2001) pour la démonstration de ce résultat. Posons $p = x^k - ax^{k-1} + b$, on a $p' = kx^{k-1} - a\,(k-1)x^{k-2}$. Calculons tout d'abord le déterminant. On a $\det(S(p,\,p')) =$

$$
\begin{array}{cccccccccccccc}
1 & -a & 0 & & \dots & & 0 & b & 0 & 0 & \dots & 0 & 0 & 0 \\
0 & 1 & -a & 0 & & \dots & & 0 & b & 0 & \dots & 0 & 0 & 0 \\
\vdots & & & & & & & \vdots & & & \ddots & & & \\
0 & & \dots & & 0 & 1 & -a & 0 & 0 & 0 & \dots & 0 & b & 0 \\
0 & & \dots & & & 0 & 1 & -a & 0 & 0 & \dots & 0 & 0 & b \\
k & -(k-1)a & 0 & & \dots & & 0 & 0 & 0 & & \dots & & & 0 \\
0 & k & -(k-1)a & 0 & & \dots & & 0 & & & & & & \\
\vdots & & & & & & & \vdots & \vdots & & & & & \vdots \\
0 & & \dots & & 0 & k & -(k-1)a & 0 & & & & & & \\
0 & & \dots & & & 0 & k & -(k-1)a & 0 & & \dots & & & 0
\end{array}.
$$

Considérons tous les b situés dans le bloc supérieur droit. Pour chaque b, considérons la matrice cofacteur qui lui est associée. Étant donné que tous les b se situent sur la même diagonale, toutes les matrices cofacteurs associées aux b sont de même signe. Considérons le b situé dans la dernière colonne. Puisqu'il est situé à la position $(2k+1,\, k+1)$, le signe de sa matrice cofacteur associée est $(-1)^{(2k-1)+(k-1)} = (-1)^{3k-2} = (-1)^{3k} = (-1)^k$. Comme il y a exactement $(k-2)$ éléments b sur cette diagonale, on a $((-1)^k)^{k-2} = (-1)^{k^2} = (-1)^k$. En utilisant la formule du déterminant impliquant les matrices cofacteurs, le déterminant vaut

$$
(-1)^k\, b^{k-2}\underbrace{\begin{vmatrix}
1 & -a & 0 & & \dots & & 0 & b \\
k & -(k-1)a & 0 & & \dots & & 0 & 0 \\
0 & k & -(k-1)a & 0 & & \dots & & 0 \\
\vdots & & & & & & & \vdots \\
0 & & \dots & & 0 & k & -(k-1)a & 0 \\
0 & & \dots & & & 0 & k & -(k-1)a
\end{vmatrix}}_{A},
$$

où A est une matrice carrée d'ordre $k+1$. Appliquons l'opération $L_2 - k\,L_1$, on a

$$= \quad (-1)^k\, b^{k-2} \begin{vmatrix} 1 & -a & 0 & & \dots & & 0 & b \\ 0 & a & 0 & & \dots & & 0 & -kb \\ 0 & k & -(k-1)a & 0 & & \dots & & 0 \\ 0 & 0 & k & -(k-1)a & 0 & & \dots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & & \dots & & 0 & k & -(k-1)a & 0 \\ 0 & & \dots & & & 0 & k & -(k-1)a \end{vmatrix}$$

$$= \quad (-1)^k\, b^{k-2} \underbrace{\begin{vmatrix} a & 0 & & \dots & & 0 & -kb \\ k & -(k-1)a & 0 & & \dots & & 0 \\ 0 & k & -(k-1)a & 0 & & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & & \dots & 0 & k & -(k-1)a & 0 \\ 0 & & \dots & & 0 & k & -(k-1)a \end{vmatrix}}_{B},$$

où B est une matrice carrée d'ordre k. Appliquons l'opération

$$L_1 - \frac{a}{k}\, L_2 - \frac{(k-1)\, a^2}{k^2}\, L_3 - \frac{(k-1)^2\, a^3}{k^3}\, L_4 - \dots - \frac{(k-1)^{k-3}\, a^{k-2}}{k^{k-2}}\, L_{k-1}.$$

On obtient

$$(-1)^k\, b^{k-2} \begin{vmatrix} 0 & 0 & & \dots & 0 & \frac{(k-1)^{k-2}\, a^{k-1}}{k^{k-2}} & -kb \\ k & -(k-1)a & 0 & & \dots & & 0 \\ 0 & k & -(k-1)a & 0 & & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & & \dots & 0 & k & -(k-1)a & 0 \\ 0 & & \dots & & 0 & k & -(k-1)a \end{vmatrix}.$$

Considérons les $(k-2)$ entrées k situées sur les lignes $L_2, \dots, L_{k-1}$. Chacune d'entre elles a une matrice cofacteur associée de signe négatif puisque tous les k sont situés directement sous la diagonale principale. Il s'ensuit que

$$\begin{aligned}
\det(S(p,\,p')) &= (-1)^k\,(-1)^{k-2}\,b^{k-2}\,k^{k-2} \begin{bmatrix} (k-1)^{k-2}\,a^{k-1} & -kb \\ k^{k-2} & \\ k & -(k-1)a \end{bmatrix} \\
&= b^{k-2}\,k^{k-2}\left(-\frac{(k-1)^{k-1}\,a^k}{k^{k-2}} + k^2\,b\right) \\
&= -b^{k-2}\left((k-1)^{k-1}\,a^k - k^k\,b\right) \\
&= -b^{k-2}\,\Delta.
\end{aligned}$$

Il reste à évaluer le signe de $(-1)^{\frac{k\,(k-1)}{2}}$. Soit $m \in \mathbb{N}$

1) Si $k \equiv 0 \mod 4$, $k = 4m$ et $(-1)^{\frac{4m\,(4m-1)}{2}} = 1$.

2) Si $k \equiv 1 \mod 4$, $k = 4m+1$ et $(-1)^{\frac{(4m+1)\,(4m)}{2}} = 1$.

3) Si $k \equiv 2 \mod 4$, $k = 4m+2$ et $(-1)^{\frac{(4m+2)\,(4m+1)}{2}} = -1$.

4) Si $k \equiv 3 \mod 4$, $k = 4m+3$ et $(-1)^{\frac{(4m+3)\,(4m+2)}{2}} = -1$.

□

Lemme 4.5. *Soit $p(x) = x^k - a\,x^{k-1} + b$, un polynôme unitaire de degré $k \geq 3$, où $a \in \mathbb{N}$ et $b \in \mathbb{N}$.*

(i) Si k est pair,

(1) $\Delta \geq 0 \Leftrightarrow p(x)$ a 2 racines réelles positives.

(2) $\Delta < 0 \Leftrightarrow p(x)$ n'a aucune racine réelle.

(ii) Si k est impair,

(1) $\Delta \geq 0 \Leftrightarrow p(x)$ a 3 racines réelles dont une est négative et deux sont positives.

(2) $\Delta < 0 \Leftrightarrow p(x)$ a une seule racine réelle et celle-ci est négative.

Démonstration. Dérivons $p(x)$ par rapport à x, on a $p'(x) = k\,x^{k-1} - (k-1)a\,x^{k-2}$. Les deux seuls zéros de ce polynôme sont $x_1 = 0$ et $x_2 = \frac{(k-1)\,a}{k}$. Comme

$$\begin{aligned}
p''(x_2) &= k\,(k-1)\left(\frac{(k-1)\,a}{k}\right)^{k-1} - a\,(k-1)\,(k-2)\left(\frac{(k-1)\,a}{k}\right)^{k-3} \\
&= \frac{(k-1)^{k-1}\,a^{k-2}}{k^{k-3}} - \frac{(k-2)\,(k-1)^{k-2}\,a^{k-2}}{k^{k-3}}
\end{aligned}$$

$$
\begin{aligned}
&= \frac{(k-1)^{k-1}\,a^{k-2}}{k^{k-3}}\,((k-1)-(k-2)) \\
&= \frac{(k-1)^{k-1}\,a^{k-2}}{k^{k-3}} > 0,
\end{aligned}
$$

on a un minimum local en x_2. Comme $p''(x_1) = 0$, on ne peut pas conclure par le test de la dérivée seconde. Or, au voisinage de 0, $p(x) = b - a\,x^{k-1} + O(x^k)$.

(i) Si k pair, $k-1$ est impair, on a un point d'inflexion en $x = 0$. Ainsi le graphique de $p(x)$ est de la forme

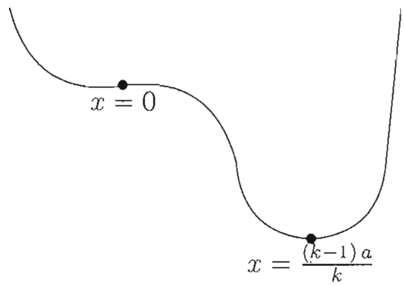


Figure 4.1 Graphique de $p(x) = x^k - a\,x^{k-1} + b$, k pair.

Puisque x_1 et x_2 sont les uniques racines de $p'(x)$, il s'ensuit que le minimum est un minimum global. Si $p(x_2) = \frac{-(k-1)^{k-1}\,a^k}{k^k} + b > 0$, alors $p(x)$ n'a aucune racine réelle. Si $p(x_2) \leq 0$, alors $p(x)$ a exactement deux racines réelles. Celles-ci sont positives car pour tout $x \leq 0$, $p(x) > p(0) = b > 0$.

(ii) Si k est impair, $k-1$ est pair. Comme $-a < 0$, on a un maximum local en $x = 0$; donc, le graphique de $p(x)$ est de la forme

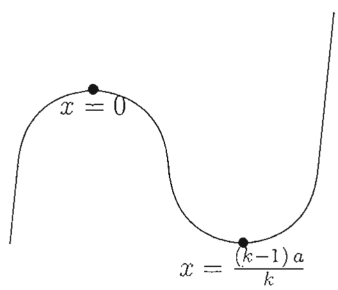


Figure 4.2 Graphique de $p(x) = x^k - a\,x^{k-1} + b$, k impair.

Étant donné que x_1 et x_2 sont les 2 seules racines de $p'(x)$, le minimum local en x_2 est le seul de $p(x)$. Si $p(x_2) > 0$, alors $p(x)$ a une unique racine réelle, qui est négative. Si $p(x_2) \leq 0$, alors $p(x)$ a 3 racines réelles, 2 positives et une négative. $\square$

Démonstration du Théorème 4.3

$\Rightarrow$) Supposons que $f(x)$ soit $\mathbb{N}$-rationnelle. Si $b \leq 0$, on a $k^k b \leq (k-1)^{k-1} a^k$. Pour le reste de la preuve, on va supposer $b > 0$.

Soient $p(x) = x^k - a\,x^{k-1} + b$ le polynôme réciproque du dénominateur de $f(x)$ et ρ le module maximal de ses racines. Comme $f(x)$ est $\mathbb{N}$-rationnelle, on a du Théorème de Berstel que $\rho \in \mathbb{R}_+$ est une racine de $f(x)$. Il s'ensuit du Lemme 4.5 que $\Delta \geq 0$.

$\Leftarrow$) Supposons que pour tout $k \geq 2$, $\Delta \geq 0$. On a $f(x) = (a\,x + (-b)\,x^k)^*$ est $\mathbb{Z}$-rationnelle. Par ailleurs, $f(x)$ est $\mathbb{R}_+$-rationnelle puisque

$$\begin{aligned} p &= 1 - ax + bx^k \\ &= \left(1 - \frac{k-1}{k}ax\right)\left(1 - \sum_{i=1}^{k-2}\frac{(k-1)^{i-1}}{k^i}a^i x^i - \frac{kb}{(k-1)a}x^{k-1}\right) - \frac{\Delta}{k^{k-1}(k-1)a}x^{k-1} \end{aligned}$$

En inversant tout, on a

$$\begin{aligned} f(x) &= \frac{1}{\left(1 - \frac{k-1}{k}ax\right)\left(1 - \sum_{i=1}^{k-2}\frac{(k-1)^{i-1}}{k^i}a^i x^i - \frac{kb}{(k-1)a}x^{k-1}\right) - \frac{\Delta}{k^{k-1}(k-1)a}x^{k-1}} \\ &= \frac{\left(\frac{k-1}{k}ax\right)^*}{\left(1 - \sum_{i=1}^{k-2}\frac{(k-1)^{i-1}}{k^i}a^i x^i - \frac{kb}{(k-1)a}x^{k-1}\right) - \left(\frac{k-1}{k}ax\right)^*\left(\frac{\Delta}{k^{k-1}(k-1)a}\right)x^{k-1}} \\ &= \left(\frac{k-1}{k}ax\right)^* g^*, \end{aligned}$$

où

$$g = \sum_{i=1}^{k-2}\frac{(k-1)^{i-1}}{k^i}a^i x^i + \frac{kb}{(k-1)a}x^{k-1} + \left(\frac{k-1}{k}ax\right)^*\left(\frac{\Delta}{k^{k-1}(k-1)a}\right)x^{k-1}.$$

Comme $f(x)$ est une série $\mathbb{R}_+$ à coefficients entiers, elle est $\mathbb{N}$-rationnelle ; ceci découle des Théorèmes de Berstel et Soittola.

□

Remarque 4.6. La démonstration de la condition suffisante montre que $1 - ax + bx^k$ est un *dénominateur de Soittola* (voir (Perrin, 1992) ou (Berstel et Reutenauer, 2008b) Chap. VIII Exercice 3.3).

4.2 $\mathbb{N}$-rationalité des séries de la forme $(1 - ax + bx^2 + cx^3)^{-1}$

On va déterminer les conditions nécessaire et suffisante caractérisant la $\mathbb{N}$-rationalité de toute série de la forme $(1 - ax + bx^2 + cx^3)^{-1}$, où $a \in \mathbb{N}$ et b, $c \in \mathbb{Z}$.

Contrairement à la décidabilité de la $\mathbb{N}$-rationalité des séries de la forme $(1-ax+bx^k)^{-1}$, le discriminant de $x^3 - ax^2 + bx + c$ ne suffit pas pour décider si une série de la forme $(1 - ax + bx^2 + cx^3)^{-1}$ est $\mathbb{N}$-rationnelle. Les deux exemples suivants illustrent cette situation lorsque $b > 0$ et $c < 0$.

Exemple 4.7. $f(x) = (1 - x + x^2 - x^3)^{-1}$. Le discriminant $x^3 - x^2 + x - 1$ vaut -16. Cette série est $\mathbb{N}$-rationnelle puisque

$$\frac{1}{1 - x + x^2 - x^3} = \frac{1}{(1-x)(1+x^2)} = \frac{1+x}{(1-x^2)(1+x^2)} = \frac{1+x}{1-x^4} = (1+x)(x^4)^*.$$

Exemple 4.8. $f(x) = (1 - 4x + 4x^2 - x^3)^{-1}$. Le discriminant $x^3 - 4x^2 + 4x - 1$ vaut 5. La série $f(x)$ est $\mathbb{N}$-rationnelle puisque

$$f(x) = 1 + 2Ax(B+1) + A^2Bx^3, \qquad A = (2x)^*, \qquad B = (2x + Ax^3)^*.$$

Cette expression rationnelle a été obtenue à l'aide du paquetage *RLangGFun*.

Lemme 4.9. *Soit* $p(x) = x^3 - ax^2 + bx + c$, *où* $a \in \mathbb{N}$, b, $c \in \mathbb{Z}$. *Si* $a^2 \geq 3b$, $p(x)$ *a un maximum local en* $x_1 = \frac{a-\sqrt{a^2-3b}}{3}$ *et un minimum local en* $x_2 = \frac{a+\sqrt{a^2-3b}}{3}$. *Si* $a^2 < 3b$, $p(x)$ *est strictement croissante sur tout son domaine.*

Démonstration. Supposons $a^2 \geq 3b$. Dérivons $p(x)$ par rapport à x, on a

$$p'(x) = 3x^2 - 2ax + b.$$

Les zéros de la dérivée sont

$$x = \frac{2a \pm \sqrt{4a^2 - 12b}}{6} = \frac{2a \pm 2\sqrt{a^2 - 3b}}{6} = \frac{a \pm \sqrt{a^2 - 3b}}{3}.$$

Posons $x_1 = \frac{a - \sqrt{a^2-3b}}{3}$ et $x_2 = \frac{a + \sqrt{a^2-3b}}{3}$. Étudions la nature de ces racines, en utilisant le test de la concavité. La dérivée seconde de $p(x)$ par rapport à x est $p''(x) = 6x - 2a$.

$$\begin{aligned} p''(x_1) &= 2a - 2\sqrt{a^2 - 3b} - 2a = -2\sqrt{a^2 - 3b} < 0, \\ p''(x_2) &= 2\sqrt{a^2 - 3b} > 0. \end{aligned}$$

On a donc un maximum local en x_1 et un minimum local en x_2. Ainsi, $p(x)$ se comporte selon le graphique

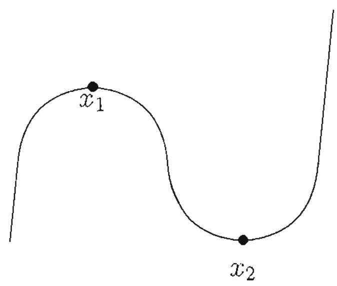


Figure 4.3 Graphique de $p(x) = x^3 - a\,x^2 + bx + c$ lorsque $a^2 \geq 3b$.

Si $a^2 < 3b$, la dérivée ne possède aucun zéro. Il s'ensuit que $p(x)$ est strictement croissante sur tout son domaine car $p(x)$ est un polynôme de degré 3. □

Lemme 4.10. *Si $a^2 < 3b$, l'unique racine réelle de $p(x)$ sera négative si $c > 0$ et positive si $c < 0$.*

Démonstration. Du Lemme précédent, $p(x)$ est strictement croissant sur $\mathbb{R}$. Comme $p(0) = c$, la racine réelle sera négative si $c > 0$ et positive si $c < 0$.

Posons $\delta = a^2 - 3b$ et supposons $\delta \geq 0$. Évaluons le polynôme au point $x_2 = \dfrac{a+\sqrt{\delta}}{3}$,

$$\begin{aligned}
p(x_2) &= (x_2)^3 - a(x_2)^2 + bx_2 + c \\
&= \left(\frac{a+\sqrt{\delta}}{3}\right)^3 - a\left(\frac{a+\sqrt{\delta}}{3}\right)^2 + b\left(\frac{a+\sqrt{\delta}}{3}\right) + c \\
&= \frac{4a^3}{27} + \frac{4a^2}{27}\sqrt{\delta} - \frac{b}{9}\sqrt{\delta} - \frac{ab}{3} - \frac{2a^3}{9} + \frac{ab}{3} - \frac{2a^2}{9}\sqrt{\delta} + \frac{ab}{3} + \frac{b}{3}\sqrt{\delta} + c \\
&= \frac{-2a^3}{27} - \frac{2a^2}{27}\sqrt{\delta} + \frac{2b}{9}\sqrt{\delta} + \frac{ab}{3} + c \\
&= \frac{-2a^3}{27} - \frac{2a^2}{27}(\delta)^{3/2} + \frac{ab}{3} + c.
\end{aligned}$$

Posons $\Delta = \dfrac{-2a^3}{27} - \dfrac{2a^2}{27}(\delta)^{3/2} + \dfrac{ab}{3} + c$.

Du Lemme 4.9 et du calcul de Δ, on en déduit le résultat suivant.

Lemme 4.11. *Soit $p(x) = x^3 - ax^2 + bx + c$, $a \in \mathbb{N}$, b, $c \in \mathbb{Z}$ tel que $a^2 \geq 3b$.*

(1) Si $c > 0$,

(i) $\Delta \leq 0 \Leftrightarrow p(x)$ a 3 racines réelles, 1 négative et 2 positives.

(ii) $\Delta > 0 \Leftrightarrow p(x)$ a une seule racine réelle qui est négative.

(2) Si $c < 0$,

(i) $\Delta \leq 0 \Leftrightarrow p(x)$ a 3 racines réelles positives.

(ii) $\Delta > 0 \Leftrightarrow p(x)$ a une seule racine réelle qui est positive.

Théorème 4.12. *Soit $f(x) = \dfrac{1}{1 - a\,x + b\,x^2 + c\,x^3} = \sum_{n=0}^{n} f_n x^n$, $a \in \mathbb{N}$, b, $c \in \mathbb{Z}$.*

(1) Si $a^2 \geq 3b$,

(i) Si $f(x)$ est $\mathbb{N}$-rationnelle, $\Delta \leq 0$.

(ii) Si $\Delta \leq 0$ et $c \leq a^3$, $f(x)$ est $\mathbb{N}$-rationnelle.

(2) Si $a^2 < 3b$,

(i) Si $b^3 < -a^3\,c$, $f(x)$ est $\mathbb{N}$-rationnelle si et seulement si $f_n \geq 0$, $\forall n \geq 0$.

(ii) Si $b^3 = -a^3\,c$, $f(x)$ est $\mathbb{N}$-rationnelle si et seulement si $2b = a^2$ ou $b = a^2$.

(iii) Si $b^3 > -a^3\,c$, $f(x)$ n'est jamais $\mathbb{N}$-rationnelle.

Remarque 4.13. Si $b = 0$, alors $a^2 \geq 3b$ et $\Delta = -\dfrac{4a^3}{27} + c \leq 0$. On retrouve la condition nécessaire et suffisante du théorème 4.3 pour $k = 3$.

Remarque 4.14. On retrouve le cas (1) lorsque toutes les racines de $p(x) = x^3 - ax^2 + bx + c$ sont réelles et le cas (2) si une seule racine est réelle. Cette dernière est dominante en (i), est égale au module de la racine complexe en (ii) et est strictement inférieure à ce module en (iii).

Exemple 4.15. Considérons la série suivante

$$\frac{1}{1 - 3x + 4x^2 - 3x^3} = \frac{1 + 3x + 4x^2 + 3x^3}{1 - x^2 - 2x^4 - 9x^6}.$$

Cette série, provenant de (Rinaldi, 1999), est $\mathbb{N}$-rationnelle par l'égalité. On a $3b > a^2$, $64 = b^3 < -c\,a^3 = 81$ et tous les coefficients sont positifs.

L'exemple suivant montre que la condition $c \leq a^3$ n'est pas nécessaire.

Exemple 4.16.

$$\begin{aligned} f(x) &= \frac{1}{1 - x + 5x^2 + 2x^3} \\ &= 1 + 6x^2 + (7AB + 30A)\,x^4 + 10AaBx^6 + 54A^2Bx^8 \\ &\quad + x\left(1 + 9x^2 + (45A + 25AB)\,x^4 + 13ABx^6 + 81A^2Bx^8\right), \end{aligned}$$

où

$$A = (5x^2)^*, \qquad B = (6x^2 + x^4 + 9Ax^6)^*.$$

On trouve $\Delta = -4,48 < 0$ et $2 = c > 1^3 = a^3$.

L'exemple suivant montre que la condition $\Delta \leq 0$ n'est pas suffisante.

Exemple 4.17. On prend $a = 1$, $b = -5$ et $c = 6$, on trouve $\Delta = -0,48 < 0$. Les racines du polynôme $x^3 - x^2 - 5x + 6$ étant 2, $1,3028$ et $-2,3028$, la série $(1 - x - 5x^2 + 6x^3)^{-1}$ n'est pas $\mathbb{N}$-rationnelle.

La démonstration du Théorème 4.12 nécessite les résultats suivants.

Définition 4.18. Un *entier algébrique* λ est une racine d'un polynôme unitaire à coefficients dans $\mathbb{Z}$.

Définition 4.19. Une extension finie K de $\mathbb{Q}$ est appelée un *corps de nombres algébriques*. Les entiers algébriques contenus dans K forment un anneau dénoté A_K. K peut s'écrire sous la forme $K = \mathbb{Q}(\lambda)$, où $\lambda \in A_K$. Le degré de λ sur K est le degré du polynôme minimal ayant λ comme racine.

Théorème 4.20 (Kronecker). *Soit λ un entier algébrique tel que λ et tous ses conjugués soient de module ≤ 1, alors λ est une racine de l'unité.*

Voir par exemple (Berstel et Reutenauer, 1984) Exercice V.2.1.

Proposition 4.21. *Soit*

$$f(x) = \frac{1}{1 - a\,x + b\,x^2 + c\,x^3} = \sum_{n=0}^{\infty} f_n\, x^n, \quad a,\, b,\, c \in \mathbb{N}.$$

Soit $p(x) = x^3 - a\,x^2 + b\,x + c$ le polynôme réciproque du dénominateur de $f(x)$. Si $p(x)$ a une racine dominante alors, pour tout $n \geq 0$, $f_n > 0$.

Démonstration. Dénotons par λ la racine dominante. Comme $p(0) = c \geq 0$ et que $p'(x) = 3\,x^2 - 2\,a\,x + b \geq 0$, si $x < 0$, alors $p(x)$ est croissant sur l'intervalle $]-\infty, 0[$. Donc $p(x)$ a une racine réelle négative. Comme $p(x)$ a une racine dominante, il s'ensuit du Lemme 4.11 que $p(x)$ a 3 racines réelles, une qui est négative et deux qui sont positives. Supposons par l'absurde que $\lambda \leq 1$. On a du Théorème de Kronecker que toutes les racines de $p(x)$ sont des racines de l'unité. Ainsi, 1 et -1 sont les deux seules racines réelles. On aurait $1 - a + b + c = 0$ et $-1 - a - b + c = 0$; la seule possibilité est $b = -1$; contradiction car $b \in \mathbb{N}$. Ainsi, on a $\lambda > 1$. Puisque λ est une racine de $p(x)$, on a

$$\lambda^3 - a\,\lambda^2 + b\,\lambda + c = 0 \Leftrightarrow \lambda^3 = a\,\lambda^2 - b\,\lambda - c \Leftrightarrow \lambda = a - \frac{b}{\lambda} - \frac{c}{\lambda^2}.$$

Définissons la propriété $P(i)$ comme suit :

$$P(n) : \frac{f_i}{f_{i-1}} > \lambda, \qquad i = 1, \ldots, n.$$

Démontrons cette propriété par récurrence.

(i) Vérifions que $P(1)$ est vraie. On a

$$\frac{f_1}{f_0} = \frac{a}{1} = a.$$

(ii) Supposons $P(n)$ vraie. Montrons $P(n+1)$ vraie ; i.e. $\frac{f_i}{f_{i-1}} > \lambda$, $i = 1, \ldots, n+1$.

Par hypothèse de récurrence, on a $\frac{f_i}{f_{i-1}} > \lambda$, $i = 1, \ldots, n$. Il reste à montrer que $\frac{f_{n+1}}{f_n} > \lambda$. On a $f_n > \lambda^{k-1} f_{n-k+1}$, $k \leq n$. On en déduit que

$$\begin{aligned} \frac{1}{\lambda} &> \frac{f_{n-1}}{f_n} \Leftrightarrow \frac{-b}{\lambda} < -b\,\frac{f_{n-1}}{f_n}, \\ \frac{1}{\lambda^2} &> \frac{f_{n-2}}{f_n} \Leftrightarrow \frac{-c}{\lambda^2} < -c\,\frac{f_{n-2}}{f_n}. \end{aligned}$$

Du numérateur et du dénominateur de $f(x)$, on en déduit que les coefficients f_n satisfont la récurrence :

$$f_n = a\,f_{n-1} - b\,f_{n-2} - c\,f_{n-3}, \quad f_n = 0,\ n < 0,\ f_0 = 1.$$

Ainsi, on obtient

$$\frac{f_{n+1}}{f_n} = \frac{a\,f_n - b\,f_{n-1} - c\,f_{n-2}}{f_n} = a - \frac{b\,f_{n-1}}{f_n} - \frac{c\,f_{n-2}}{f_n} > a - \frac{b}{\lambda} - \frac{c}{\lambda^2} = \lambda.$$

Ainsi, $P(n)$ est vraie pour tout $n \in \mathbb{N}^*$. Comme $f_n > \lambda^n f_0 > 1$, alors tous les coefficients f_n de $f(x)$ sont positifs.

Lemme 4.22. *Si une racine n^e de l'unité est racine d'un polynôme $P(x) \in \mathbb{Q}[x]$ avec* $\deg(P) = 2$, *alors* $n = 1, 2, 3, 4$ *ou* 6.

Démonstration. On doit avoir $\varphi(n) \leq 2$, où $\varphi(n)$ est la *fonction d'Euler*. Par (Lang, 2002) p.279, le polynôme minimal d'une racine primitive n^e est de degré $\varphi(n)$.

Si $n = p_1^{n_1} p_2^{n_2} \ldots$, alors $\varphi(n) = (p_1^{n_1} - p_1^{n_1-1})(p_2^{n_2} - p_2^{n_2-1})\ldots$. Comme pour $p \geq 5$, $m \geq 1$, on a $(p^m - p^{m-1}) = p^{m-1}(p-1) \geq 4$. Il s'ensuit que $n = 2^x 3^y$.

Si $y \geq 2$, $3^y - 3^{y-1} = 3^{y-1}(3-1) \geq 6$. Donc $y = 0$ ou 1. Si $x \geq 3$, $2^x - 2^{x-1} = 2^{x-1}(2-1) \geq 4$. On a donc $x = 0$, 1 ou 2. En combinant les x et y, on trouve $n = 1$, 2, 3, 4, 6 ou 12. Or $\varphi(12) = 4$. □

Démonstration du Théorème 4.12

Si $p(x)$ a trois racines réelles dénotées α, β et γ. On a

$$\begin{aligned} p(x) = x^3 - ax^2 + bx + c &= (x-\alpha)(x-\beta)(x-\gamma) \\ &= x^3 - (\alpha+\beta+\gamma)x^2 + (\alpha\beta + \alpha\gamma + \beta\gamma)x - \alpha\beta\gamma. \end{aligned}$$

En comparant les coefficients de part et d'autre, on obtient les relations

$$a = \alpha + \beta + \gamma, \tag{4.1}$$

$$b = \alpha\beta + \alpha\gamma + \beta\gamma, \tag{4.2}$$

$$c = -\alpha\beta\gamma. \tag{4.3}$$

Si $p(x)$ a une unique racine réelle dénotée γ,

$$\begin{aligned} p(x) = x^3 - ax^2 + bx + c &= (x-\alpha)(x-\overline{\alpha})(x-\gamma) \\ &= (x^2 - (\alpha+\overline{\alpha})x + |\alpha|^2)(x-\gamma) \\ &= (x^2 - 2\Re(\alpha)x + |\alpha|^2)(x-\gamma) \\ &= x^3 - (2\Re(\alpha)+\gamma)x^2 + (2\gamma\Re(\alpha) + |\alpha|^2)x - |\alpha|^2\gamma. \end{aligned}$$

Comparons les coefficients, on trouve

$$a = 2\Re(\alpha) + \gamma, \tag{4.4}$$

$$b = 2\gamma\Re(\alpha) + |\alpha|^2, \tag{4.5}$$

$$c = -|\alpha|^2\gamma. \tag{4.6}$$

(1) $a^2 \geq 3b$

(i) Supposons $f(x)$ $\mathbb{N}$-rationnelle. Soit ρ le module maximal des racines de $p(x) = x^3 - ax^2 + bx + c$. Du Théorème de Berstel, ρ est une racine de $p(x)$.

(1) $c \geq 0$. $p(x)$ a une racine réelle négative. Comme $\rho \in \mathbb{R}_+$ est une racine de $p(x)$, il s'ensuit que $p(x)$ a trois racines réelles. Par conséquent, $\Delta \leq 0$ du Lemme 4.11.

(2) $c < 0$ et $b < 0$. $f(x) = (1 - ax + bx^2 + cx^3)^{-1}$ est $\mathbb{N}$-rationnelle et

$$\Delta = \frac{-2a^3}{27} - \frac{2}{27}(a^2 - 3b)^{3/2} + \frac{ab}{3} + c \leq 0.$$

(3) $c < 0$ et $b \geq 0$. Supposons par l'absurde que $\Delta > 0$. Du Lemme 4.11, $p(x)$ a une seule racine réelle positive $\gamma = \rho$. Le graphique de $p(x)$ se comportant comme suit.

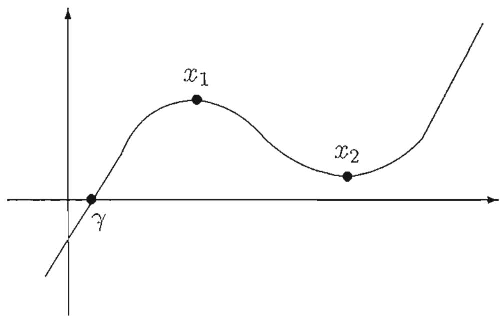


Figure 4.4 Graphique de $p(x) = x^3 - a\,x^2 + bx + c$, où $a^2 \geq 3b$ et $c \geq 0$.

On remarque que

$$\gamma < x_1 = \frac{a - \sqrt{a^2 - 3b}}{3} < \frac{a}{3}.$$

De l'équation (4.4),

$$\begin{aligned} a &= 2\Re(\alpha) + \gamma \\ \Rightarrow a &< 2\Re(\alpha) + \frac{a}{3} \\ \Leftrightarrow \frac{2a}{3} &< 2\,\Re(\alpha) \\ \Leftrightarrow \frac{a}{3} &< \Re(\alpha). \end{aligned}$$

Ainsi on a $\gamma < \frac{a}{3} < \Re(\alpha) < |\alpha|$. On a contradiction car $\gamma = |\alpha| = \rho$; donc $\Delta \leq 0$.

(ii) Supposons $\Delta \leq 0$ et $c \leq a^3$. Considérons les 4 cas suivants.

(1) $b \geq 0$ et $c > 0$. Comme $\Delta \leq 0$, on a du Lemme 4.11 que $p(x)$ a trois racines réelles, une négative et deux positives. Posons $\alpha < 0$ et $\gamma > \beta > 0$.

Supposons par l'absurde que $-\alpha \geq \gamma$. De (4.2), on a

$$\begin{aligned} b &= \alpha\beta + \alpha\gamma + \beta\gamma \\ &= \alpha(\beta + \gamma) + \beta\gamma \\ &= \alpha\,(a - \alpha) + \beta\,\gamma \\ &= \alpha\,a - \alpha^2 + \beta\,\gamma. \end{aligned}$$

Comme $-\alpha \geq \gamma$ et $-\alpha > \beta$, $\alpha^2 > \beta\,\gamma \Leftrightarrow -\alpha^2 + \beta\,\gamma < 0$. Comme $\alpha\,a < 0$, on aurait $b = \alpha\,a - \alpha^2 + \beta\,\gamma < 0$. Contradiction car $b \geq 0$ par hypothèse. Ainsi γ est une racine dominante. De la Proposition 4.21, tous les termes de la série $(1 - a\,x + b\,x^2 + c\,x^3)^{-1}$ sont positifs. Finalement, comme $f(x) = (1 - a\,x + b\,x^2 + c\,x^3)^{-1}$ est $\mathbb{Z}$-rationnelle, alors $f(x)$ est $\mathbb{N}$-rationnelle par le Théorème de Soittola.

(2) $b < 0$ et $c > 0$. Comme $\Delta \leq 0$, on a du Lemme 4.11 que $p(x)$ a trois racines réelles, une négative et deux positives. Posons $\alpha < 0$ et $\gamma > \beta > 0$.

Supposons par l'absurde que $-\alpha > \gamma$.

$$\begin{aligned} 0 &\geq \alpha + \gamma \\ \Leftrightarrow \beta &\geq \alpha + \gamma + \beta \\ \Leftrightarrow \beta &\geq a \\ \Leftrightarrow c &= -\alpha\beta\gamma > \beta^3 > a^3. \end{aligned}$$

On a une contradiction car $c \leq a^3$ par hypothèse. Il s'ensuit que $\gamma \geq -\alpha$. Si $\gamma > -\alpha$, on a une une racine dominante. Supposons $\gamma \leq 1$, du Théorème de Kronecker, on aurait $\alpha = -1$ et $\beta = \gamma = 1$. Contradiction car $\gamma > \alpha$. Ainsi, $\gamma > 1$. Il reste à vérifier la non négativité de chaque coefficient de la série $f(x) = \sum_{n=0}^{\infty} f_n x^n$.

$$\begin{aligned}
f_0 &= 1, \\
f_1 &= a > 0, \\
f_2 &= a^2 - b > 0, \\
f_3 &= a^3 - 2ab - c = (a^3 - c) - 2ab \geq 0, \\
&\vdots
\end{aligned}$$

Du Corollaire 1.17, on a pour un n suffisamment grand que $\frac{f_{n+1}}{f_n} \sim \gamma > 1$. Il s'ensuit que pour tout $n \geq 0$, $f_n \geq 0$. Comme $f(x)$ est une série $\mathbb{Z}$-rationnelle, elle est $\mathbb{N}$-rationnelle par le théorème de Soittola.

Si $\gamma = -\alpha$, $a = \alpha + \beta + \gamma = \beta$. Il s'ensuit que a est une racine de $p(x)$. On trouve donc $p(a) = ab + c = 0$, d'où $c = -ab$.

$$f(x) = \frac{1}{1 - ax + bx^2 + cx^3} = \frac{1}{1 - ax + bx^2 - abx^3} = \frac{1}{(1 - ax)(1 + bx^2)} = (ax)^* \, (-bx^2)^*.$$

Cette série est $\mathbb{N}$-rationnelle car $b < 0$ par hypothèse.

(3) $b < 0$ et $c < 0$. $f = (1 - ax + bx^2 + cx^3)^{-1}$ est $\mathbb{N}$-rationnelle.

(4) $b \geq 0$ et $c < 0$. Comme $\Delta \leq 0$, on a du Lemme 4.11 que $p(x)$ a trois racines réelles positives. Ainsi, γ est une racine dominante. Supposons $\gamma \leq 1$, du Théorème de Kronecker, on aurait $\alpha = i$ et $\alpha = -i$. On trouve

$$p(x) = (x - i)(x + i)(x - 1) = x^3 - x^2 + x - 1.$$

Il s'ensuit que $a^2 - 3b = 1 - 3 = -2 < 0$. On a une contradiction ; ainsi, $\gamma > 1$. Il reste à vérifier la non négativité de chaque coefficient. On a

$$\begin{aligned}
f_1 &= a > 0, \\
f_2 &= a^2 - b \geq 3b - b = 2b \geq 0 \\
f_3 &= a^3 - 2ab - c = (\alpha + \beta + \gamma)^3 - 2(\alpha + \beta + \gamma)(\alpha\beta + \alpha\gamma + \beta\gamma) + \alpha\beta\gamma \\
&= \alpha^2\beta + \alpha^2\gamma + \alpha\beta^2 + \beta^2\gamma + \alpha\gamma^2 + \beta\gamma^2 + \alpha^3 + \beta^3 + \gamma^3 + \alpha\beta\gamma > 0, \\
&\vdots
\end{aligned}$$

Pour un n suffisamment grand, on a $\frac{f_n}{f_{n-1}} \sim \gamma > 1$. Donc, tous les coefficients de $f(x)$ sont non négatifs. Comme $f(x)$ est $\mathbb{Z}$-rationnelle, elle est $\mathbb{N}$-rationnelle par le Théorème de Soittola.

(2) $a^2 < 3b$

Si $b < 0$, la condition $3b > a^2$ n'est jamais satisfaite.

Si $b \geq 0$ et $c > 0$. On a $b^3 > -ca^3$. Soit ρ le module maximal des racines de $p(x)$. Du Lemme 4.10, $p(x)$ a une seule racine réelle qui est négative. Ainsi, ρ n'est pas une racine de $p(x)$, par conséquent, $f(x)$ n'est pas $\mathbb{N}$-rationnelle.

Si $b \geq 0$ et $c < 0$, on considère les trois cas suivants.

(i) $b^3 < -a^3 c$.

$\Rightarrow$) Supposons $f(x)$ $\mathbb{N}$-rationnelle, tous les coefficients f_n sont non négatifs.

$\Leftarrow$) Supposons que tous les coefficients soient non négatifs. Comme $b^3 < -c\,a^3$,

$$\begin{aligned} \frac{b^3}{a^3} &< -c \\ \Leftrightarrow \frac{b^3}{a^3} - a\frac{b^2}{a^2} + b\frac{b}{a} + c &< 0 \\ \Leftrightarrow p\left(\frac{b}{a}\right) &< 0 \\ \Leftrightarrow \frac{b}{a} &< \gamma \\ \Leftrightarrow b &< \gamma\, a. \end{aligned}$$

Par l'équation (4.5), on trouve

$$b = 2\gamma\Re(\alpha) + |\alpha|^2 = \gamma(a-\gamma) + |\alpha|^2 = \gamma a - \gamma^2 + |\alpha|^2.$$

Par conséquent,

$$\gamma a - \gamma^2 + |\alpha|^2 < \gamma a \Leftrightarrow |\alpha|^2 < \gamma^2.$$

Il s'ensuit que γ est une racine dominante. Comme f est une série $\mathbb{Z}$-rationnelle à coefficients non négatifs, f est $\mathbb{N}$-rationnelle par le Théorème de Soittola.

(ii) $b^3 = -a^3 c$.

$\Rightarrow$) Supposons $f(x)$ $\mathbb{N}$-rationnelle. On a

$$\begin{aligned} \frac{b^3}{a^3} &= -c \Leftrightarrow \frac{b^3}{a^3} - a\frac{b^2}{a^2} + b\frac{b}{a} + c = 0 \\ \Leftrightarrow p\left(\frac{b}{a}\right) &= 0 \Leftrightarrow \frac{b}{a} = \gamma. \end{aligned}$$

On trouve que b est un multiple (positif) de a. En effet, supposons par l'absurde que b n'est pas un multiple de a, $\frac{b}{a}$ est une fraction irréductible. Ainsi, $-c = \frac{b^3}{a^3}$ est aussi une fraction irréductible car b^3 et a^3 ont exactement les mêmes facteurs que b et a respectivement. Contradiction car $-c$ est un entier. Écrivons $b = ma$. Le Lemme 4.10 nous assurant l'unicité de la racine réelle, il s'ensuit que $m = \gamma$. On trouve alors $b = ma$ et $c = -m^3$.

Par hypothèse, $a^2 < 3b$, du Lemme 4.10, on a $\alpha \notin \mathbb{R}$ et $\gamma > 0$. Puisque

$$\begin{aligned} b &= 2\gamma\Re(\alpha) + |\alpha|^2 = \gamma(a-\gamma) + |\alpha|^2 = \gamma a - \gamma^2 + |\alpha|^2 \\ \Leftrightarrow ma &= ma - m^2 + |\alpha|^2 \\ \Leftrightarrow m^2 &= |\alpha|^2 \\ \Leftrightarrow m &= \alpha. \end{aligned}$$

La série étant $\mathbb{N}$-rationnelle par hypothèse, on a du Théorème de Berstel que $\frac{\alpha}{\gamma}$ et $\frac{\alpha}{\gamma}$ sont des racines de 1.

Elles sont racines du polynôme à coefficients rationnels

$$H(x) = \left.\frac{x^3 - ax^2 + bx - c}{x - \gamma}\right|_{x \to \gamma x}.$$

Du Lemme 4.22, $\frac{\alpha}{\gamma}$ est une racine de l'unité avec $n = 1$, 2, 3, 4 ou 6. Comme $\alpha \notin \mathbb{R}$, $n = 3$, 4 ou 6. On a donc

$$\begin{aligned} H(x) &= x^2 + x + 1 = \Phi_3(x), \\ \text{ou} \quad & x^2 + 1 = \Phi_4(x), \\ \text{ou} \quad & x^2 - x + 1 = \Phi_6(x). \end{aligned}$$

Il s'ensuit que

$$x^3 - ax^2 + bx + c = \gamma^2 (x - \gamma) H\left(\frac{x}{\gamma}\right).$$

Si $H(x) = \Phi_3(x)$, on a

$$\begin{aligned} x^3 - ax^2 + bx + c &= \gamma^2 (x - \gamma) \left(\frac{x^2}{\gamma^2} + \frac{x}{\gamma} + 1\right) \\ &= \gamma^2 \left(\frac{x^3}{\gamma^2} - \gamma^3\right) \\ &= x^3 - \gamma^3. \end{aligned}$$

On trouve $a = 0$ et $b = 0$, ce qui contredit l'hypothèse $a^2 < 3b$.

Si $H(x) = \Phi_4(x)$, on a

$$\begin{aligned} x^3 - ax^2 + bx + c &= \gamma^2 (x - \gamma) \left(\frac{x^2}{\gamma^2} + 1\right) \\ &= \gamma^2 \left(\frac{x^3}{\gamma^2} - \frac{x^2}{\gamma} + x - \gamma\right) \\ &= x^3 - \gamma x^2 + \gamma^2 x - \gamma^3. \end{aligned}$$

On trouve $a = \gamma$ et $b = \gamma^2 = a^2$.

Si $H(x) = \Phi_6(x)$, on a

$$\begin{aligned} x^3 - ax^2 + bx + c &= \gamma^2 (x - \gamma) \left(\frac{x^2}{\gamma^2} - \frac{x}{\gamma} + 1\right) \\ &= \gamma^2 \left(\frac{x^3}{\gamma^2} - 2\,\frac{x^2}{\gamma} + 2x - \gamma\right) \\ &= x^3 - 2\gamma x^2 + 2\gamma^2 x - \gamma^3. \end{aligned}$$

On trouve $a = 2\gamma$ et $b = 2\gamma^2 = \frac{a^2}{2}$.

$\Leftarrow$) Supposons $b = a^2$ ou $2b = a^2$. Si $b = a^2$ alors $b^3 = a^6 = -a^3 c \Rightarrow -a^3 = c$.

$$\begin{aligned} f &= \frac{1}{1 - ax + bx^2 + cx^3} = \frac{1}{1 - ax + a^2x^2 - a^3x^3} = \frac{1}{(1 - ax)(1 + a^2x^2)} \\ &= \frac{1 + ax}{(1 + ax)(1 - ax)(1 + a^2x^2)} = \frac{1 + ax}{(1 - a^2x^2)(1 + a^2x^2)} = \frac{1 + ax}{1 - a^4x^4} = (1 + ax)(a^4x^4)^*. \end{aligned}$$

Si $2b = a^2$, alors $2ma = a^2 \Rightarrow 2m = a$. On trouve

$$\begin{aligned} f &= \frac{1}{1 - ax + bx^2 + cx^3} = \frac{1}{1 - 2mx + 2m^2x^2 - m^3x^3} = \frac{1}{(1-mx)(1-mx+m^2x^2)} \\ &= \frac{1+mx}{(1-m^2x^2)(1-mx+2m^2x^2)} = \frac{(1+mx)(1+mx+m^2x^2)}{(1-m^2x^2)(1+mx+m^2x^2)(1-mx+2m^2x^2)} \\ &= \frac{(1+mx)(1+mx+m^2x^2)}{(1-m^6x^6)} = (1+mx)(1+mx+m^2x^2)(1-m^6x^6)^*. \end{aligned}$$

Dans les 2 cas, $f(x)$ est $\mathbb{N}$-rationnelle.

(iii) Si $b^3 > -a^3c$, soit γ est la racine réelle de $p(x)$, alors

$$\begin{aligned} \frac{b^3}{a^3} + c &> 0 \Leftrightarrow \frac{b^3}{a^3} - a\frac{b^2}{a^2} + b\frac{b}{a} + c > 0 \\ \Leftrightarrow p\left(\frac{b}{a}\right) &> 0 \Rightarrow \frac{b}{a} > \gamma \Leftrightarrow b > \gamma a. \end{aligned}$$

Par l'équation (4.5), on trouve

$$b = 2\gamma\Re(\alpha) + |\alpha|^2 = \gamma(a-\gamma) + |\alpha|^2 = \gamma a - \gamma^2 + |\alpha|^2.$$

Par conséquent,

$$\gamma a - \gamma^2 + |\alpha|^2 > \gamma a \Leftrightarrow |\alpha|^2 > \gamma^2.$$

Ainsi, $p(x)$ n'a pas de racine dominante, ce qui implique que $f(x)$ n'est pas $\mathbb{N}$-rationnelle.

□

Conjecture 4.23. *Soit* $f = \dfrac{1}{1 - ax + bx^2 - cx^3} = \sum_{n=0}^{\infty} f_n x^n$, $a = 2, 3, 4$, $b, c \in \mathbb{N}$ *et* $a^2 < 3b$. *Alors* $f(x)$ *est* $\mathbb{N}$*-rationnelle si et seulement si* $b^3 \leq c\,a^3$ *et* $f_3 = a^3 - 2ab + c \geq 0$.

L'implication directe se démontre de la même façon que la condition nécessaire du Théorème 4.12.

Cette conjecture a été énoncée à la suite de simulations faites à l'aide du paquetage *RLangGFun*.

CHAPITRE V

FONCTION ZÊTA D'UN AUTOMATE

La fonction zêta d'un automate fini $\mathcal{A}$ est la série génératrice $\exp\left\{\sum_{n=1}^{\infty} a_n \frac{z^n}{n}\right\}$, où a_n est le nombre de chemins bi-infinis dans $\mathcal{A}$ ayant la période n. On va montrer que a_n est égal à la somme des rangs stables des mots w de longueur n. Par ailleurs, on montrera plusieurs propriétés de cette série telle la $\mathbb{N}$-rationalité ou concernant l'apériodicité, la nil-simplicité et l'existence d'un zéro dans le monoïde des relations. Étant donné que ces résultats sont valides pour des automates non ambigus, ceux-ci s'appliqueront aux codes. En effet, on aura dans ce cas que a_n désigne le nombre de séquences bi-infinies des mots du code, dont l'évaluation est un mot bi-infini sur A de période n. Une fois de plus, les propriétés de la fonction zêta se refléteront aux codes : complétion de codes, codes purs, codes circulaires et codes bifixes.

5.1 Rang stable dans les automates finis non ambigus

Soit A un alphabet, un *automate* $\mathcal{A}$ sur A est composé d'un ensemble d'états Q, d'un sous-ensemble I de Q (*états initiaux*), d'un sous-ensemble T de Q (*états terminaux ou finaux*) et d'un ensemble d'arêtes $F \subset Q \times A \times Q$. L'automate est dénoté $\mathcal{A} = (Q, I, T)$ et un automate est fini si Q l'est.

Un *chemin* dans l'automate $\mathcal{A}$ est une séquence $c = (f_1, f_2, \ldots, f_n)$ d'arêtes consécutives $f_i = (q_i, a_i, q_{i+1})$. Le mot $w = a_1 \ldots a_n$ est *l'étiquette* du chemin c. L'état q_1 est *l'origine* de c et l'état q_{n+1}, la *fin* de c, on écrit $q_1 \xrightarrow{w} q_{n+1}$. Par convention il existe pour tout état $q \in Q$ un chemin de longueur 0 de q vers q. Son étiquette est le mot vide.

Un arête $f = (p,\, a,\, q)$ est aussi dénotée par $p \xrightarrow{a} q$, où $p,\, q \in Q$ sont deux états de $\mathcal{A}$.

Un *mot bi-infini* est un élément de $A^{\mathbb{Z}}$. De façon similaire, un *chemin bi-infini* est un élément de $F^{\mathbb{Z}}$, avec les conditions de compatibilité semblables à celles d'un chemin. Clairement, il existe une application μ de $F^{\mathbb{Z}}$ vers $A^{\mathbb{Z}}$; ainsi, on définit *l'étiquette* d'un chemin bi-infini p comme étant le mot bi-infini $\mu(p)$. Soit w un mot non vide, on dénote ${}^{\infty}w^{\infty}$ le mot bi-infini $\ldots ww \,\bullet\, wwww \ldots$, où le point désigne la position du 0.

À tout automate $\mathcal{A}$, on associe la série formelle $S_{\mathcal{A}} = \sum_{w \in A^*} (S_{\mathcal{A}},\, w)\, w$, où le coefficient $(S_{\mathcal{A}},\, w)$ du mot w, est le nombre de chemins bi-infinis dans $\mathcal{A}$ étiquetés $\ldots www \ldots$.

À tout automate $\mathcal{A} = (Q, I, T)$, on associe la fonction $\varphi_{\mathcal{A}} : A \rightarrow \mathbb{N}^{Q \times Q}$ définie par

$$\varphi_{\mathcal{A}}(a)_{p,q} = \begin{cases} 1 & \text{si } (p,\, a,\, q) \in F, \\ 0 & \text{sinon.} \end{cases}$$

Cette fonction s'étend en un morphisme $\varphi_{\mathcal{A}}$ de A^* vers le monoïde multiplicatif $\mathbb{N}^{Q \times Q}$ des matrices de dimension $Q \times Q$ à coefficients dans $\mathbb{N}$. Il est bien connu que pour tout mot w, le coefficient $\varphi_{\mathcal{A}}(w)_{p,q}$ est égal au nombre de chemins de p vers q étiquetés w.

On dit que l'automate $\mathcal{A} = (Q, I, T)$ sur A est *non ambigu* si, pour tous $p,\, q \in Q$ et $w \in A^*$, $\varphi_{\mathcal{A}}(w)_{p,q} \in \{0,\, 1\}^{Q \times Q}$. Autrement dit, il existe au plus un chemin d'étiquette w de p vers q. On identifie la matrice $\varphi_{\mathcal{A}}(w)$ et la relation sur Q qu'elle représente.

Soit $\mathcal{A}$ un automate non ambigu. On appelle le *rang* du mot w le plus petit entier r tel que $\varphi_{\mathcal{A}}(w) = cl$, où $c \in \mathbb{N}^{Q \times r}$ et $l \in \mathbb{N}^{r \times Q}$. On a que $rang(uvw) \leq rang(v)$ (voir (Berstel et Perrin, 1984), Section IV.4) ; en particulier, on a que pour tout $n \in \mathbb{N}$,

$$rang(w^{n+1}) \leq rang(w^n).$$

On définit le *rang stable* de w, dénoté $rgst(w)$: c'est le le rang de w^n pour un n

suffisamment grand ; autrement dit

$$rgst(w) = \lim_{n\to\infty} rang(w^n).$$

Soit $\mathcal{A}$ un automate non ambigu ; on dénote $T_{\mathcal{A}}$ la série formelle telle que le coefficient de w est le rang stable de w. Autrement dit,

$$T_{\mathcal{A}} = \sum_{w\in A^*} rgst(w)\, w.$$

Proposition 5.1. *Soit $\mathcal{A}$ un automate non ambigu. Le rang stable de w est égal au nombre de chemins bi-infinis dans $\mathcal{A}$ étiquetés ${}^{\infty}w^{\infty}$.*

Remarque 5.2. Un *automate déterministe* est un automate non ambigu. Dans ce cas, le rang de w, qui agit sur l'ensemble des états, est égal à la cardinalité de l'image de w. De plus, le rang stable de w est égal à la cardinalité des états finaux des chemins étiquetés w^N, où N est un entier suffisamment grand.

La démonstration de la proposition 5.1 nécessite les résultats suivants.

Soit m une relation entre P et Q. On dit que m est une *relation non ambiguë* si $m \in \{0, 1\}^{P\times Q}$. Un *monoïde de relations non ambiguës* sur Q est un sous-monoïde de $\mathbb{N}^{Q\times Q}$ tel que tous ses éléments sont non ambigus. Puisque c'est un sous-monoïde de $\mathbb{N}^{Q\times Q}$, il contient l'identité I_Q. Soient p et q deux états. Afin de simplifier l'écriture, on écrit pmq au lieu de (p, m, q). Par non ambiguïté, si on a $pmrnq$ et $pmsnq$, alors $r = s$.

Soit m une relation non ambiguë sur Q. Un *point fixe de m* est un élément (état) $q \in Q$ tel que qmq. On note $Fix(w)$ l'ensemble des points fixes de w ; i.e. l'ensemble des états q tels que $q \xrightarrow{w} q$. On dénote $tr(w) = |Fix(w)|$. Finalement, une relation m est *idempotente* si $m^2 = m$.

Proposition 5.3. *(voir (Berstel et Perrin, 1984), Prop. IV.3.3) Soit M un monoïde de relations non ambiguës sur Q. Soient $m \in M$ et $S = Fix(m)$. On a les équivalences suivantes.*

(i) m est une relation idempotente.

(ii) Pour tout $p, q \in Q$, *on a* pmq *si et seulement si il existe un* $s \in S$ *tel que* pms *et* smq.

(iii) On a

$$m = cl, \qquad lc = I_S,$$

où $c \in \{0, 1\}^{Q \times S}$ *et* $l \in \{0, 1\}^{S \times Q}$ *sont les restrictions de* m *à* $Q \times S$ *et* $S \times Q$ *respectivement.*

Si m *est une relation idempotente, on a en plus les formes matricielles*

$$c = \begin{bmatrix} I_S \\ c' \end{bmatrix}, \qquad l = \begin{bmatrix} I_S & l' \end{bmatrix}, \qquad m = \begin{bmatrix} I_s & l' \\ c' & c'l' \end{bmatrix},$$

où $c' \in \{0, 1\}^{(Q-S) \times S}$ *et* $l' \in \{0, 1\}^{S \times (Q-S)}$ *et* $l'c' = 0$.

Lemme 5.4. *Si* $\varphi_{\mathcal{A}}(w)$ *est une relation idempotente et si* $p \xrightarrow{w} q \xrightarrow{w} r$ *, alors* $q \in Fix(w)$.

Démonstration. Comme $\varphi_{\mathcal{A}}(w)$ est une relation idempotente, on a $p \xrightarrow{w} r$. Par la proposition 5.3, il existe $q' \in Fix(w)$ tel que $p \xrightarrow{w} q'$ et $q' \xrightarrow{w} r$. Par non ambiguïté, $q = q'$. Donc $q \in Fix(w)$. □

Lemme 5.5. *Soient* $p, q \in Fix(w)$ *et* $p \xrightarrow{w} q$ *; alors* $p = q$.

Démonstration. Soient $p, q \in Fix(w)$, on a $p \xrightarrow{w} p \xrightarrow{w} q$ et $p \xrightarrow{w} q \xrightarrow{w} q$. Puisque l'automate est non ambigu, le chemin étiqueté w^2 entre p et q est unique. Donc, $p = q$. □

Proposition 5.6. *(voir (Berstel et Perrin, 1984), Prop. IV.4.3) Soit* m *une relation non ambiguë idempotente, alors*

$$rang(m) = |Fix(m)|.$$

Démonstration de la proposition 5.1

Il existe un entier $n \geq 1$ tel que $\varphi_{\mathcal{A}}(w^n)$ est une relation idempotente. Ainsi, on peut supposer que $\varphi_{\mathcal{A}}(w)$ est elle-même une relation idempotente. En effet, il y a une bijection évidente entre les chemins étiquetés ${}^{\infty}w^{\infty}$ et les chemins étiquetés ${}^{\infty}(w^n)^{\infty}$. Soit $q \in Fix(w)$; alors on a le chemin bi-infini étiqueté ${}^{\infty}w^{\infty}$

$$\ldots\; q \xrightarrow{w} q \xrightarrow{w} q \xrightarrow{w} q \;\ldots.$$

Inversement, soit π un chemin bi-infini étiqueté ${}^{\infty}w^{\infty}$. Ce chemin se décompose comme

$$\ldots\; q_{-2} \xrightarrow{w} q_{-1} \xrightarrow{w} q_0 \xrightarrow{w} q_1 \xrightarrow{w} q_2 \;\ldots.$$

Du lemme 5.4, chaque état $q_i \in Fix(w)$. Du Lemme 5.1 les q_i sont tous égaux. Ainsi, pour chaque état $q \in Fix(w)$ il existe un et un seul chemin bi-infini étiqueté ${}^{\infty}w^{\infty}$ passant par q. Il s'ensuit que le nombre de tels chemins est $|Fix(w)|$.

Comme $\varphi_{\mathcal{A}}(w)$ est une relation idempotente, $rang(w) = rang(w^n)$, pour tout entier $n \geq 1$; donc, on a $rgst(w) = rang(w)$. De la Proposition 5.6, le rang de cette relation est le nombre de points fixes de $\varphi_{\mathcal{A}}(w)$. Par conséquent, le rang stable de w est égal au nombre de chemins bi-infinis étiquetés ${}^{\infty}w^{\infty}$.

$\square$

La démonstration montre aussi le résultat suivant

Proposition 5.7. *Soient $\mathcal{A}$ un automate, w un mot et $n \geq 1$ tel que $\varphi_{\mathcal{A}}(w^n)$ soit une relation idempotente. Alors $rgst(w) = |Fix(w^n)|$.*

5.2 Fonction zêta d'un automate

Soit $\mathcal{A}$ un automate. On définit la *fonction zêta de l'automate $\mathcal{A}$* : c'est la série formelle

$$\zeta(\mathcal{A}) = \exp\left\{\sum_{n=1}^{\infty} a_n \frac{z^n}{n}\right\}, \tag{5.1}$$

où a_n est la somme des rangs stables de tous les mots de longueur n.

Proposition 5.8. *$\zeta(\mathcal{A})$ est une série $\mathbb{N}$-rationnelle.*

La démonstration de cette proposition exige les définition et résultat suivants.

Définition 5.9. Un langage L est cyclique si pour tous mots u, v, w et tout entier $n \geq 1$, les conditions suivantes sont satisfaites :

$$\begin{aligned} uv \in L &\Leftrightarrow vu \in L; \\ w \in L &\Leftrightarrow w^n \in L. \end{aligned}$$

La *conjugaison* dans d'un monoïde libre est la relation d'équivalence $uv \sim vu$; une classe de conjugaison est appelée *mot circulaire*.

Théorème 5.10. *(Reutenauer, 1997) La fonction zêta d'un langage rationnel cyclique est $\mathbb{N}$-rationnelle.*

Démonstration de la proposition 5.8

Soit L_i le langage composé de tous les mots de rang stable i. On va montrer que L_i est un langage rationnel pour tout entier i. Notons M le monoïde fini $\varphi_{\mathcal{A}}(A^*)$ et P_i l'ensemble des relations dans M de rang stable i. On a $L_i = \varphi_{\mathcal{A}}^{-1}(P_i)$. Donc L_i est reconnaissable. Du Théorème de Kleene, L_i est rationnel.

Soient $u, v \in A^*$ des mots, et n un entier ; comme ${}^{\infty}(uv)^{\infty} = {}^{\infty}(vu)^{\infty}$, et ${}^{\infty}w^{\infty} = {}^{\infty}(w^n)^{\infty}$, pour $n \geq 1$, $rgst(uv) = rgst(vu)$ et $rgst(w) = rgst(w^n)$. Par conséquent, L_i est un langage cyclique. Soit $\zeta_i = \zeta(L_i)$ la fonction zêta du langage L_i, où

$$\zeta(L) = \exp\left\{\sum_{n=1}^{\infty} |L \cap A^n| \frac{z^n}{n}\right\},$$

pour un langage L. Du Théorème 5.10, ζ_i est une série $\mathbb{N}$-rationnelle.

Soit $L_n(i)$ le nombre de mots de longueur n dans L_i ; en calculant $\zeta(\mathcal{A})$, on obtient

$$\begin{aligned} \zeta(\mathcal{A}) &= \exp\left\{\sum_{n=1}^{\infty} a_n \frac{z^n}{n}\right\} = \exp\left\{\sum_{n=1}^{\infty}\left(\sum_{|w|=n} rgst(w)\right)\frac{z^n}{n}\right\} \\ &= \exp\left\{\sum_{n=1}^{\infty}\left(\sum_{i} L_n(i)\, i\right)\frac{z^n}{n}\right\} = \exp\left\{\sum_{i} i \sum_{n=1}^{\infty} L_n(i)\frac{z^n}{n}\right\} \\ &= \prod_i \left[\exp\left\{\sum_{n=1}^{\infty} L_n(i)\frac{z^n}{n}\right\}\right]^i \end{aligned}$$

$$\begin{aligned} &= \prod_i \left[\exp\left\{\sum_{n=1}^{\infty} |L_i \cap A^n| \frac{z^n}{n}\right\}\right]^i \\ &= \prod_i \zeta(L_i)^i = \prod_i \zeta_i^i. \end{aligned}$$

Il s'ensuit que $\zeta(\mathcal{A})$ est une série $\mathbb{N}$-rationnelle, puisque L_i est vide pour un i suffisamment grand, donc, le produit est fini.

□

Nous allons calculer sur un exemple la fonction ζ d'un automate. Nous avons besoin de quelques notions.

Soit $\mathcal{A}$ un automate, la *trace* de $\mathcal{A}$ est la série non commutative énumérant le nombre de points fixes de chaque mot :

$$tr(\mathcal{A}) = \sum_{w \in A^+} |Fix(w)|\, w.$$

Exemple 5.11. Considérons l'automate suivant

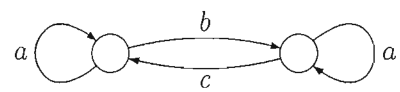


Figure 5.1 Un automate.

La trace de $\mathcal{A}$ est la série dont le coefficient de w est 2 si w est une puissance de a, 1 si w est un mélange de a et d'un mot de la forme $(bc)^i$ ou $(cb)^i$, $i \geq 1$ et 0 sinon.

Théorème 5.12. *(Berstel et Reutenauer, 1990) La série caractéristique d'un langage cyclique régulier est une combinaison linéaire sur $\mathbb{Z}$ de traces d'automates finis déterministes.*

Soit $\varphi : \mathbb{Z}\langle\langle A\rangle\rangle \to \mathbb{Z}[[A]]$ la transformation rendant commutatif le produit des lettres ; par exemple, $\varphi(2ab - ba) = ab$. Soit S une série non commutative, on a $S = \sum_{n=0}^{\infty} S_n$, où

S_n est la partie homogène de degré n de S. La *fonction zêta généralisée* de S est la série commutative

$$Z(S) = \exp\left\{\sum_{n=1}^{\infty} \frac{\varphi(S_n)}{n}\right\}.$$

Rappelons que $\underline{L}$ est la série caractéristique du langage L, définie par $\underline{L} = \sum_{w \in L} w$. De (Berstel et Reutenauer, 1990), on a que si L est un langage, $\zeta_L = \theta(Z(\underline{L}))$, où $\theta : \mathbb{Z}\langle\langle A \rangle\rangle \mapsto \mathbb{Z}[[z]]$ l'homomorphisme défini par $\theta(a) = z$, pour toute lettre $a \in A$.

Le *déterminant d'un automate* est le déterminant de la matrice $I - zM$, où I est la matrice identité de la taille appropriée et M, la matrice de l'automate. C'est une version en plusieurs variables du déterminant de (Perrin, 1976).

Proposition 5.13. *(Berstel et Reutenauer, 1990) La fonction zêta généralisée de la trace d'un automate fini est égale à l'inverse du déterminant de cet automate.*

Exemple 5.14. Considérons l'automate

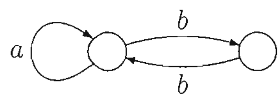


Figure 5.2 Un automate.

On a $S_{\mathcal{A}} = tr(\mathcal{A}) - tr(\mathcal{A}_1) + 2tr(\mathcal{A}_2)$, où $\mathcal{A}_1$ et $\mathcal{A}_2$ sont respectivement les automates

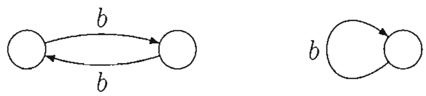


Figure 5.3 Les automates $\mathcal{A}_1$ et $\mathcal{A}_2$.

En effet, on le vérifie facilement avec le mot $w = b^n$, puisque ce mot est de rang stable 2. Considérons maintenant un autre mot w, si $rgst(w) = 1$, alors w est de la forme

$$w = b^{i_0}ab^{i_1}a \dots ab^{i_n}, \quad n \geq 1, \tag{5.2}$$

où $i_1, i_2, \dots, i_{n-1}$ et $i_0 + i_n$ sont pairs. Ce qui implique la formule pour $S_{\mathcal{A}}$. De cette formule, on trouve que

$$\zeta_{\mathcal{A}} = \frac{\det(1 - M_1 z)}{\det(1 - Mz)\ \det(1 - M_2 z)^2},$$

où M, M_1, M_2 sont les matrices adjacentes de $\mathcal{A}$, $\mathcal{A}_1$ et $\mathcal{A}_2$. respectivement. On trouve ainsi

$$\zeta_{\mathcal{A}} = \frac{1 - z^2}{(1 - z - z^2)(1 - z)^2} = \frac{1 + z}{(1 - z - z^2)(1 - z)}.$$

5.3 Apériodicité

Un monoïde est *apériodique* si ses sous-groupes sont tous triviaux (on note que les éléments identité du monoïde et d'un sous-groupe peuvent différer). Un monoïde fini M est apériodique si et seulement si pour tout $x \in M$, il existe un entier $n \geq 0$ tel que $x^n = x^{n+1}$. Un *automate est apériodique* si son monoïde des relations l'est.

Proposition 5.15. *Les trois conditions suivantes sont équivalentes pour un automate fini non ambigu :*

(1) $\mathcal{A}$ est un automate apériodique

(2) $S_{\mathcal{A}} = tr(\mathcal{A})$,

(3) $\zeta(\mathcal{A})$ est l'inverse du déterminant de $\mathcal{A}$.

La démonstration nécessite le résultat suivant.

Lemme 5.16. *Soit w un mot agissant sur les états d'un automate. Alors la trace de w ; (i.e. le nombre de points fixes de w) est supérieur ou égal au rang stable de w. On a égalité si et seulement si w est apériodique ; i.e. le sous-monoïde engendré par la relation induite par w est apériodique.*

Démonstration.

1. Chaque point fixe de w est également un point fixe de w^N, pour tout entier N. On peut choisir N de façon à ce que w^N soit idempotent. Par la Proposition 5.7, $rgst(w) = |Fix(w^N)|$.

2. Supposons que w soit apériodique. Alors $w^k = w^{k+1} = w^{k+2} = \ldots$ pour un entier k suffisamment grand. Puisque toutes les puissances de w^N sont idempotentes, on peut supposer en augmentant N que $w^N = w^{N+1}$. Soit q un point fixe de w^N. On a donc un chemin $\pi : q = q_0 \xrightarrow{w} q_1 \xrightarrow{w} q_2 \xrightarrow{w} \cdots \xrightarrow{w} q_{N-1} \xrightarrow{w} q_0$. On a cependant le chemin $\pi' : q_0 \xrightarrow{w^{N+1}} q_0$. Si π n'est pas un préfixe de π', on obtient deux chemins distincts π^{N+1} et π'^N étiquetés $w^{N(N+1)}$ ayant les mêmes états initial et final. Ce qui contredit la non ambiguïté. Donc, π est un préfixe de π'. Donc, il y a un chemin $q_0 \xrightarrow{w} q_0$. Par conséquent, q est un point fixe de w et on a l'égalité du lemme.

3. Inversement, supposons qu'on a l'égalité. Alors tout point fixe de w^N (N est l'entier de la partie 1.) est un point fixe de w. Soit $q_0 \xrightarrow{w} q_1 \xrightarrow{w} q_2 \xrightarrow{w} \cdots \xrightarrow{w} q_0$ un chemin fermé dans le graphe de la relation sur Q induite par w. Alors q_0 est un point fixe d'un certaine puissance de w, donc de w^N (puisque $w^N = w^{2N} = \ldots$). Donc q_0 est un point fixe de w. On a donc le chemin $q_0 \xrightarrow{w} q_0 \xrightarrow{w} \cdots \xrightarrow{w} q_0$. En comparant ce chemin au premier, on obtient par non ambiguïté que $q_0 = q_1 = q_2 = \ldots$. Ce qui montre qu'il n'y a aucun chemin fermé dans le graphe de w à l'exception de ceux qui sont des répétitions de boucles. Si on enlève ces boucles du graphe, on obtient un nouveau graphe sans chemin fermé ; donc, il existe un entier k tel qu'il n'existe aucun chemin de longueur k dans ce graphe. On va montrer que $w^k = w^{k+1}$. En effet, un chemin de longueur k ou $k+1$ dans le graphe de w a nécessairement une boucle. Donc, par répétition ou suppression de la boucle, on a que $p \xrightarrow{w^k} q$ est équivalent à $p \xrightarrow{w^{k+1}} q$. Donc w est apériodique.

Démonstration de la proposition 5.15

1) $\Rightarrow$ 2) On utilise directement le Lemme 5.16.

2) $\Rightarrow$ 3) on a $a_n = \sum_{|w|=n} rgst(w) = \sum_{|w|=n} |Fix(w)| = tr(M^n)$, où M est la matrice d'incidence de l'automate $\mathcal{A}$. Donc.

$$\zeta(\mathcal{A}) = \exp\left\{\sum_{n=1}^{\infty} a_n \frac{z^n}{n}\right\} = \exp\left\{\sum_{n=1}^{\infty} tr(M^n)\frac{z^n}{n}\right\}$$

$$= \exp\left\{tr\sum_{n=1}^{\infty}\frac{M^n z^n}{n}\right\} = \exp\left\{tr\ln\left(\frac{1}{1-zM}\right)\right\} = \det(1-zM)^{-1},$$

par la formule de Jacobi $\exp \circ\ tr \circ \ln = \det$.

$\neg 1) \Rightarrow \neg 3)$ Du Lemme 5.16, pour tout mot w, on a $|Fix(w)| < rgst(w)$. Également du Lemme 5.16, on a $a_n \geq tr(M^n)$ pour tout n, et pour au moins un n, on a l'inégalité stricte. Donc $\zeta(\mathcal{A}) = \exp\left\{\sum_{n=1}^{\infty} a_n \frac{z^n}{n}\right\} > \exp\left\{\sum_{n=1}^{\infty} tr(M^n)\frac{z^n}{n}\right\}$ et par les mêmes calculs faits ci-haut, on en déduit que $\zeta(\mathcal{A}) > \det((I-zM)^{-1})$.

□

5.4 Relation nulle

Rappelons que le *support* de la série $S = \sum_{w\in A^*} a_w w$, dénoté $Supp(S)$, est l'ensemble des mots dont le coefficient a_w est non nul, $Supp(S) = \{w \in A^* \mid a_w \neq 0\}$.

Proposition 5.17. *Les énoncés suivants sont équivalents.*

(1) La relation nulle est élément du monoïde des relations de l'automate $\mathcal{A}$.

(2) $Supp(S_{\mathcal{A}}) \neq A^*$.

(3) $\zeta_{\mathcal{A}}$ converge pour $z = \frac{1}{|A|}$, où $|A|$ est la cardinalité de l'alphabet A.

Démonstration. 1) $\Rightarrow$ 2) Supposons que la relation nulle est élément du monoïde des relations de l'automate $\mathcal{A}$. Alors, il existe un mot w qui induit la relation nulle. Donc, $rgst(w) = 0$ et $w \notin Supp(S_{\mathcal{A}})$.

2) $\Rightarrow$ 1) Supposons $Supp(S_{\mathcal{A}}) \neq A^*$. Alors il existe un mot w tel que $rgst(w) = 0$. Donc, pour un entier N suffisamment grand, on a $rang(w^N) = 0$. Par conséquent, w^N induit la relation nulle.

2) $\Rightarrow$ 3) Soient $L = Supp(S_{\mathcal{A}}) \neq A^*$ et $q = Card(A)$. Soit $w \in A^*$ un mot qui induit la relation nulle. Si $u \in L$, $u \in A^* \backslash A^*wA^*$; autrement, u est la relation nulle et $rgst(u) = 0$.

On a $L = \bigcup_{i=0}^{\ell-1} L_i$, où $\ell = |w|$, $L_i = L \cap A^i(A^\ell)^*$. On obtient donc $L_i \subseteq A^i(A^\ell \setminus w)^*$. Ainsi

$$\left|L_i \cap A^i A^{n\ell}\right| \leq q^i (q^\ell - 1)^n \leq q^{\ell-1}(q^\ell - 1)^{\frac{i+n\ell}{\ell}},$$

puisque $i \leq \ell - 1$. D'où, pour tout N

$$\left|L \cap A^N\right| \leq q^{\ell-1}\left((q^\ell - 1)^{\frac{1}{\ell}}\right)^N.$$

On a $\zeta_A = \exp\left\{\sum_{N=1}^{\infty} a_N \frac{z^N}{N}\right\}$, où $a_N = \sum_{|u|=N} rgst(u)$. Puisque le rang stable $rgst(u)$ est borné, il existe un entier D tel que pour tout u, $rgst(u) \leq D$. D'où

$$a_N = \sum_{\substack{|u|=N \\ u \in L}} rgst(u) \leq D\, q^{\ell-1}\left((q^\ell - 1)^{\frac{1}{\ell}}\right)^N.$$

D'où

$$\begin{aligned}
\zeta_A &\leq \exp\left\{D\, q^{\ell-1} \sum_{N=1}^{\infty} \left((q^\ell - 1)^{\frac{1}{\ell}}\right)^N \frac{z^N}{N}\right\} \\
&= \left(\exp\left\{\sum_{N=1}^{\infty} \left((q^\ell - 1)^{\frac{1}{\ell}}\right)^N \frac{z^N}{N}\right\}\right)^{Dq^{\ell-1}} \\
&= \left(\frac{1}{1 - (q^\ell - 1)^{\frac{1}{\ell}} z}\right)^{Dq^\ell - 1} \\
&= \left(\sum_{N=0}^{\infty} (q^\ell - 1)^{\frac{N}{\ell}} z^N\right)^{Dq^\ell - 1}.
\end{aligned}$$

Si on pose $z = q^{-1} = (Card(A))^{-1}$, la série entre parenthèses converge car

$$(q^\ell - 1)^{\frac{1}{\ell}} q^{-1} = \frac{(q^\ell - 1)^{\frac{1}{\ell}}}{q} < 1,$$

puisque $q^\ell - 1 < q^\ell$, donc $(q^\ell - 1)^{\frac{1}{\ell}} < q$.

$\neg 2) \Rightarrow \neg 3)$ Supposons $Supp(S_A) = A^*$. Pour tout mot w, $rgst(w) \geq 1$; d'où $a_n \geq |A|^n$. On obtient donc

$$\begin{aligned}
\zeta_A &\geq \exp\left\{\sum_{n=1}^{\infty} |A|^n \frac{z^n}{n}\right\} \\
&= \frac{1}{1 - |A| z}.
\end{aligned}$$

Donc ζ_A diverge pour $z = |A|^{-1}$. $\square$

5.5 Nil-simplicité

Soient M un monoïde fini et J son idéal minimal bilatéral. On dit que M est un *monoïde nil-simple* s'il existe un entier $n \geq 1$ tel que $(M \setminus 1)^n \subset J$. Autrement dit, si chaque élément $\neq 1$ du monoïde a une puissance dans l'idéal minimal. Comme $(M \setminus 1)^n$ est un idéal bilatéral et que J est minimal, il s'ensuit que $(M \setminus 1)^n = J$, on a alors $(M \setminus 1)^n = (M \setminus 1)^{n+1}$.

Proposition 5.18. *(voir (Berstel et Perrin, 1984), Prop. V.3.1) Les énoncés suivants sont équivalents*

(i) M est nil-simple,

(ii) Tous les idempotents de M sont dans l'idéal minimal J de M.

Le *rang minimal* de M est le minimum des rangs de M autre que la relation nulle, on le dénote $r(M)$.

Théorème 5.19. *(voir (Berstel et Perrin, 1984), Thm IV.4.11) Soit M le monoïde des relations non ambiguës sur Q de rang minimal fini ne contenant pas la relation nulle. L'ensemble des éléments de rang $r(M)$ est dans l'idéal minimal de M.*

Proposition 5.20. *Soit $\mathcal{A}$ un automate. Les énoncés suivants sont équivalents.*

(i) Le monoïde des relations de $\mathcal{A}$ est nil-simple.

(ii) $S_{\mathcal{A}} = d\,A^*$, pour un certain entier non-négatif d.

Démonstration. $(i) \Rightarrow (ii)$ Soit d le rang commun des éléments de l'idéal minimal du monoïde des relations M de $\mathcal{A}$. De la proposition 5.18, on a que si M est nil-simple, chaque élément de w est de rang stable d.

$(ii) \Rightarrow (i)$ Soit e un idempotent de l'idéal minimal de M. Du théorème 5.19, le rang de e est le rang minimal de M. De plus, ce rang est égal au rang stable de e. Puisque le rang stable est constant et est égal à d, on conclut que le rang minimal est d. Puisque tout élément w du monoïde a le rang stable $rgst(w) = d$, une certaine puissance de w

est de rang d. Donc, cette puissance appartient à l'idéal minimal de M par le théorème 5.19. □

5.6 Applications aux codes

Rappelons qu'un sous-ensemble X du monoïde libre A^* est un *code* si et seulement si $m, n \in \mathbb{N}^* = \mathbb{N} \setminus \{0\}$, $x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_n \in X$, la condition

$$x_1 x_2 \ldots x_m = y_1 y_2 \ldots y_n$$

implique

$$n = m, \quad \text{et} \quad x_i = y_i, \; 1 \leq i \leq n.$$

On note 1 le mot vide et X^* le sous-monoïde libre engendré par X.

L'ensemble reconnu par $\mathcal{A}$, dénoté par $L(\mathcal{A})$ est l'ensemble des étiquettes des chemins $c : i \to t$, où $i \in I$ et $t \in T$. On associe à l'automate $\mathcal{A} = (Q, I, T)$ la série formelle

$$|\mathcal{A}| = \sum_{w \in A^*} (|\mathcal{A}|, w)\, w,$$

où $(|\mathcal{A}|, w)$ est le nombre de chemins $c : i \to t$, où $i \in I$ et $t \in T$ d'étiquette w. Si $\mathcal{A}$, est un automate non ambigu, on identifie la série $|\mathcal{A}|$ associée à $\mathcal{A}$ avec l'ensemble $L(\mathcal{A})$ reconnu par $\mathcal{A}$.

Proposition 5.21. *((Berstel et Perrin, 1984), Prop. IV.1.4) Soit $X \subset A^*$ et $\mathcal{A}$ l'automate tel que $|\mathcal{A}| = \underline{X}$. Alors $|\mathcal{A}^*| = (\underline{X})^*$, où $\underline{X}$ est la série caractéristique de X.*

Il s'ensuit que X est un code si et seulement si $\mathcal{A}^*$ est non ambigu.

Soient X un code fini et $w \in A^+$ un mot non-vide. Une *X-factorisation* F de ${}^\infty w^\infty$ est un sous-ensemble F de $\mathbb{Z}$ tel que F contienne des entiers arbitrairement grands et arbitrairement petits et que pour deux entiers consécutifs i, j dans F, $x_i\, x_{i+1} \ldots x_{j-1} \in X$. Définissons la série formelle S_X par

$$S_X = \sum_{w \in A^*} (S_X, w)\, w,$$

où (S_X, w) est le nombre de X-factorisations du mot bi-infini ${}^{\infty}w^{\infty}$.

Rappelons que la série indicatrice $L_X = \sum_{w \in A^*} (L_X,\, w)\, w$ d'un code X, où $(L_X,\, w)$ est le nombre d'analyses du mot w ; i.e. le nombre de triplets $(u,\, m,\, v)$, tel que $w = vmu$ et

$$v \in A^* \setminus A^*X, \qquad m \in X^*, \qquad u \in A^* \setminus XA^*.$$

Le *degré de* X est le nombre $\max\{(L_X,\, w) \mid w \in A^*\}$.

Remarque 5.22. Dans (Vincent, 1985), Vincent considère déjà les X-factorisations des mots bi-infinis périodiques. Il montre que pour un mot donné, ces X-factorisations sont disjointes. De plus, le nombre minimal de X-factorisations est égal au degré de X.

Un *automate à pétales* $\mathcal{A} = (Q, (1,1), (1,1))$ de X est défini par

$$Q = \{(u,\, v) \in A^+ \times A^+ \mid uv \in X\} \cup \{(1,1)\}, \quad I = T = \{(1,1)\},$$

et quatre types d'arêtes

$$\begin{aligned}
(u,\, av) &\xrightarrow{\quad a \quad} (ua,\, v) && \text{for}\, uav \in X,\ u \neq 1 \text{ and } v \neq 1,\\
(1,\, 1) &\xrightarrow{\quad a \quad} (a,\, v) && \text{for}\, av \in X,\ v \neq 1,\\
(u,\, a) &\xrightarrow{\quad a \quad} (1,\, 1) && \text{for}\, ua \in X,\ u \neq 1,\\
(1,\, 1) &\xrightarrow{\quad a \quad} (1,\, 1) && \text{for}\, a \in X.
\end{aligned}$$

Autrement dit, chaque pétale est un cycle d'état initial $(1,\, 1)$ et a comme étiquette un mot de X. Il s'ensuit que le nombre de pétales est le nombre de mots de X.

Exemple 5.23. Considérons le code $X = \{a,\, ab,\, bb\}$. Son automate à pétales est

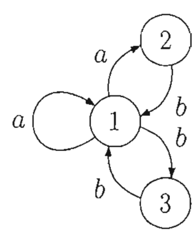


Figure 5.4 L'automate à pétales du code $X = \{a,\, ab,\, bb\}$.

Théorème 5.24. *(voir (Berstel et Perrin, 1984), Thm IV.2.1) Les énoncés suivants sont équivalents*

(i) X est un code.

(ii) L'automate à pétales est non ambigu.

Proposition 5.25. *Soit $\mathcal{A}$ l'automate à pétales de X, alors $S_{\mathcal{A}} = S_X$.*

Démonstration. Il y a une bijection entre les X-factorisations de ${}^{\infty}w^{\infty}$ et les chemins bi-infinis de $\mathcal{A}$ étiquetés ${}^{\infty}w^{\infty}$. □

Remarque 5.26. Il est possible de démontrer que le résultat précédent est aussi valide pour tout automate non ambigu connexe $\mathcal{A} = (Q, 1, 1)$ reconnaissant X^*.

Définition 5.27. Soit L un sous-ensemble de A^*. La *fermeture cyclique* de L est l'ensemble défini par

$$\{vu \mid u, v \in A^*, uv \in L\}.$$

Les mots uv et vu sont appelés des *conjugués*

Corollaire 5.28. *$Supp(S_X)$ est égal à la fermeture cyclique de X^*.*

Démonstration.

$\subseteq$) Soit $w \in Supp(S_X)$; alors il existe au moins une X-factorisation du mot bi-infini ${}^{\infty}w^{\infty}$. Soit $\mathcal{A}$ l'automate à pétales reconnaissant X^*. De la proposition 5.25, il existe un chemin bi-infini étiqueté ${}^{\infty}w^{\infty}$ dans $\mathcal{A}$. Soit Q l'ensemble des états de $\mathcal{A}$. Comme Q est fini, il existe un entier positif $n \in \mathbb{N}^*$ et $i \in Q$ tels que $i \xrightarrow{w^n} i$ est un chemin dans $\mathcal{A}$.

Soit 1 l'état initial et final de $\mathcal{A}$. Puisque $\mathcal{A}$ est un automate à pétales, le chemin étiqueté w^n passe nécessairement par 1. Soient $u, v \in A^*$ deux mots tels que $w^n = uv$ et $i \xrightarrow{u} 1 \xrightarrow{v} i$ pour n et i choisis plus haut. Alors, on a $1 \xrightarrow{v} i \xrightarrow{u} 1$. Donc, il existe un mot $w' = vu$ conjugué à w^n tel que $w' \in X^*$. Par conséquent, w appartient à la fermeture cyclique de X^*.

$\supseteq$) Supposons que w appartient à la fermeture cyclique de X^*. Alors il existe un entier positif $n \in \mathbb{N}^*$ et un mot w' tels que w' soit conjugué à w^n et $w' \in X^*$. Puisque ${}^\infty(w')^\infty = {}^\infty(w^n)^\infty = {}^\infty w^\infty$ et $(S_X, w') \neq 0$, $w \in Supp(S_X)$. $\square$

La fonction zêta $\zeta(X)$ d'un code fini X est défini comme la fonction zêta de son automate à pétales. Autrement dit, $\zeta(X) = \exp\left(\sum a_n \frac{z^n}{n}\right)$, où a_n est le nombre total de X-factorisations des mots bi-infinis ${}^\infty w^\infty$, tels que $|w| = n$. Le prochain corollaire est une conséquence directe des propositions 5.8 et 5.25.

Corollaire 5.29. *$\zeta(X)$ est une série $\mathbb{N}$-rationnelle.*

Un mot w est un *facteur* d'un mot x s'il existe des mots u, $v \in A^*$ tels que $x = uwv$. Un code est *complet* si tout mot $w \in A^*$ est un facteur d'un mot de X^*.

Corollaire 5.30. *Soit X un code fini. Les conditions suivantes sont équivalentes.*

(1) X est un code complet.

(2) $Supp(S_X) = A^*$.

(3) La fonction zêta de X diverge pour $z = \frac{1}{|A|}$, où $|A|$ est la cardinalité de l'alphabet A.

On a que X est complet si et seulement si la relation nulle n'est pas élément du monoïde des relations de son automate à pétales. Le corollaire découle alors directement de la proposition 5.17.

Rappelons que $\underline{X}$ est la série caractéristique de X, définie par $\underline{X} = \sum_{w \in X} w$. Soit $\theta : \mathbb{Z}\langle\langle A \rangle\rangle \mapsto \mathbb{Z}[[z]]$ l'homomorphisme défini par $\theta(a) = z$, pour toute lettre $a \in A$. Un sous-monoïde M de A^* est dit *pur* si pour tout $x \in A^*$ et $n \geq 1$, $x^n \in M \Rightarrow x \in M$.

Proposition 5.31. *Soit X un code fini. Les énoncés suivants sont équivalents.*

(1) X^* est un code pur.

(2) $\zeta_X = \frac{1}{1-\theta(\underline{X})}$.

Cette proposition provient de (Berstel et Perrin, 1984), Prop. VII.3.3, (Béal, 1993), Prop.9.6 et (Stanley, 1986) Prop. 4.7.11. La démonstration de cette proposition nécessite les résultats suivants.

Proposition 5.32. *(Restivo, 1973) Soit $X \subset A^+$ un code fini. X^* est pur si et seulement si le monoïde des relations $\varphi(A^*)$ ne contient pas de sous-groupe trivial.*

Proposition 5.33. *(voir (Berstel et Perrin, 1984), Prop. VIII.2.1)*

$$1 - \theta(\underline{X}) = \det(I - zM).$$

Démonstration de la Proposition 5.31

1) $\Rightarrow$ 2) Soit X^* un code pur. Par la proposition 5.32, le monoïde des relations de son automate à pétales est apériodique. De la proposition 5.15, on a $\zeta_X = (\det(I - zM))^{-1}$, où M est la matrice d'incidence de l'automate $\mathcal{A}$. De la proposition 5.33, $\zeta_X = \frac{1}{1-\theta(X)}$.

2) $\Rightarrow$ 1) De la proposition 5.33, $\zeta_X = (\det(I - zM))^{-1}$. Par la proposition 5.15, l'automate à pétales de X est apériodique. Par la proposition 5.32, X^* est pur.

□

Un code X est dit *circulaire* si pour tout n, $m \geq 1$ et $x_1, x_2, \ldots, x_n \in X$, $y_1, y_2, \ldots, y_m \in X$, $p \in A^*$ et $s \in A^+$, les égalités

$$sx_2x_3 \ldots x_np = y_1y_2 \ldots y_m, \qquad x_1 = ps,$$

impliquent $n = m$, $p = 1$ et $x_i = y_i$, $1 \leq i \leq n$. De façon équivalente, un code circulaire satisfait la condition suivante

$$uv \in X^*, \quad vu \in X^* \Rightarrow u, v \in X^*.$$

Proposition 5.34. *Soit X un code fini. Les énoncés suivants sont équivalents.*

(1) X est un code circulaire.

(2) $(S_X, w) \in \{0,1\}$ *pour tout mot* w.

Dans ce cas, S_X *est la fermeture sous la conjugaison de* $\underline{X^*}$.

La démonstration nécessite le résultat suivant.

Proposition 5.35. *(voir (Berstel et Perrin, 1984), Prop. VIII.1.2) Soit* X *un code et* φ *la représentation associée de l'automate à pétales de* X*. Les énoncés suivants sont équivalents.*

(1) X *est un code circulaire.*

(2) Pour tout $w \in A^+$*, la relation* $\varphi(w)$ *a au plus un point fixe.*

Démonstration de la Proposition 5.34

(1) $\Rightarrow$ (2) Soit X un code circulaire. Par la proposition 5.35, $(S_X, w) \in \{0, 1\}$.

(2) $\Rightarrow$ (1) Soit $\mathcal{A}$ l'automate à pétales de X. Alors, tout mot w a seulement un seul point fixe. En effet si w avait au moins 2 points fixes, son rang stable serait supérieur à 1. Par la proposition 5.35, X n'est pas circulaire.

$\square$

Rappelons qu'un code X est préfixe si $X \cap XA^+ = \phi$. Autrement dit, X est un code préfixe si aucun mot de X est un facteur gauche d'un autre mot de X. De façon similaire, un X est suffixe si $X \cap A^+X = \phi$. Un code est *bifixe* s'il est préfixe et suffixe.

Un code X est *maximal* si pour tout mot $w \notin X$, $X \cup \{w\}$ n'est pas un code.

Proposition 5.36. *Soit* X *un code maximal. Les énoncés suivants sont équivalents.*

(i) X *est bifixe.*

(ii) $S_X = d\,A^*$*, pour un certain entier* d.

Dans ce cas, on a $\zeta(X) = (1 - z|A|)^{-d}$*, où* $|A|$ *est la cardinalité de l'alphabet* A.

La démonstration exige le résultat suivant.

Théorème 5.37. *(voir (Berstel et Perrin, 1984), Thm V.3.3) Soient X un code fini maximal et $\mathcal{A}$ un automate non ambigu reconnaissant X^*. On a les équivalences suivantes.*

(i) X est un code bifixe.

(ii) Le semi-groupe $\varphi(A^+)$ est nil-simple.

Démonstration. C'est une conséquence directe de la Proposition 5.20 et du Théorème 5.37. □

5.7 Exemples

Définition 5.38. Un *morphisme de Bernoulli* sur A^* est un morphisme $\pi : A^* \to \mathbb{R}_+$ satisfaisant

$$\sum_{a \in A} \pi(a) = 1.$$

Un morphisme π est positif si $\pi(a) > 0$, pour tout $a \in A$.

La *distribution uniforme* π est un morphisme de Bernoulli défini par $\pi(a) = \frac{1}{|A|}$, où $|A|$ est la cardinalité de A.

Théorème 5.39. *(Schützenberger, voir (Berstel et Perrin, 1984) Thm I.5.11) Soit X un code mince et π un morphisme positif de Bernoulli. N'importe quelles deux des trois conditions suivantes impliquent la troisième.*

(i) X est un code.

(ii) $\pi(X) = 1$.

(iii) X est complet.

Exemple 5.40. Soit $X = \{aa, ab, b\}$. Posons $\pi(a) = s$ et $\pi(b) = t = 1 - s$. Puisque

$$\begin{aligned}\pi(X) &= s^2 + s(1-s) + (1-s)\\ &= s^2 + s - s^2 + 1 - s\\ &= 1,\end{aligned}$$

il s'ensuit du Théorème 5.39 que X est un code complet. Du corollaire 5.30, $Supp(S_X) = A^*$. Le sous-monoïde X^* est reconnu par l'automate suivant :

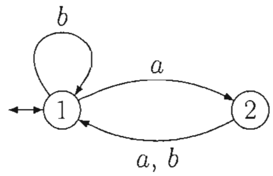


Figure 5.5 Automate complet reconnaissant le sous-monoïde $X^* = \{aa, ab, b\}^*$.

Cet automate étant déterministe, on utilise le fait que le rang stable de w est égal à la cardinalité des états finaux des chemins étiquetés w^n, pour un entier n suffisamment grand. Ainsi, on trouve que $rgst(a^+) = 2$ et $rgst(A^*ba^*) = 1$. De la remarque 5.26, $Supp(S_X) = Supp(S_A) = A^*$, par conséquent, $S_X = 2a^+ + A^*ba^*$.

Soit a_n le nombre total de X-factorisations des mots bi-infinis ${}^\infty w^\infty$, tels que $|w| = n$. De S_X, on a $a_n = 2^n + 1$ et

$$\begin{aligned}\zeta_X &= \exp\left\{\sum_{n=1}^{\infty} a_n \frac{z^n}{n}\right\} = \exp\left\{\sum_{n=1}^{\infty} (2^n+1)\frac{z^n}{n}\right\} = \exp\left\{\sum_{n=1}^{\infty} \frac{2^n z^n}{n}\right\} \exp\left\{\sum_{n=1}^{\infty} \frac{z^n}{n}\right\}\\ &= \exp\left\{\ln\left(\frac{1}{1-2z}\right)\right\} \exp\left\{\ln\left(\frac{1}{1-z}\right)\right\} = \frac{1}{(1-2z)(1-z)}.\end{aligned}$$

Exemple 5.41. Considérons le code $X = \{aa, ab, aab, abb, bb\}$. Une fois de plus, en posant $\pi(a) = s$ et $\pi(b) = t = 1 - s$, on trouve $\pi(X) = 1$. Il s'ensuit du Théorème 5.39 que X est un code complet ; et, du corollaire 5.30, $Supp(S_X) = A^*$. Le sous-monoïde X^* est reconnu par l'automate suivant

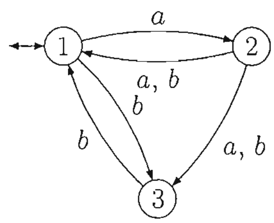


Figure 5.6 L'automate reconnaissant le sous-monoïde $X^* = \{aa,\, ab,\, aab,\, abb,\, bb\}^*$.

a et b induisent sur $\mathcal{A}$ les relations $a = \begin{pmatrix} 1 & 2 \\ 2 & 13 \end{pmatrix}$ et $b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 13 & 1 \end{pmatrix}$. Puisque $a^2 = \begin{pmatrix} 1 & 2 \\ 13 & 2 \end{pmatrix}$ et $b^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 13 & 3 \end{pmatrix}$ sont des relations idempotentes, on a $rgst(a^+) = rgst(b^+) = 2$. En écrivant les relations ab et ba sous une forme matricielle, on a

$$ab = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} [1,\, 0,\, 1], \quad ba = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} [0,\, 1,\, 0].$$

Par définition du rang d'une relation, un mot contenant a et b (ou ayant ab ou ba comme facteur) aurait un rang stable d'au plus 1. Puisque X est un code complet, du Corollaire 5.30, on a $Supp(S_X) = A^*$. Donc, pour tout mot w tel que $|w|_a \neq 0$, $|w|_b \neq 0$, son rang stable vaut 1. Par conséquent, on obtient

$$S_X = S_{\mathcal{A}} = 2a^+ + 2b^+ + \sum_{\substack{w \in A^* \\ |w|_a \neq 0,\, |w|_b \neq 0}} w.$$

Soit a_n le nombre de X-factorisations des mots bi-infinis ${}^{\infty}w^{\infty}$ tels que $|w| = n$. On obtient directement $a_n = 2^n + 2$ et

$$\begin{aligned} \zeta_X &= \exp\left\{\sum_{n=1}^{\infty} a_n \frac{z^n}{n}\right\} = \exp\left\{\sum_{n=1}^{\infty} (2^n + 2)\frac{z^n}{n}\right\} = \exp\left\{\sum_{n=1}^{\infty} \frac{2^n z^n}{n}\right\} \exp\left\{\sum_{n=1}^{\infty} \frac{z^n}{n}\right\}^2 \\ &= \exp\left\{\ln\left(\frac{1}{1-2z}\right)\right\} \exp\left\{\ln\left(\frac{1}{1-z}\right)\right\}^2 = \frac{1}{(1-2z)(1-z)^2}. \end{aligned}$$

5.8 Fonction zêta et systèmes dynamiques

La fonction zêta d'un système dynamique a été introduite par Smale et elle permet de compter les orbites périodiques. Elle constitue un invariant par isomorphisme de systèmes dynamiques. La rationalité de la fonction zêta d'un système sofique a été établie par A. Manning (Manning, 1971) ainsi que par J. Berstel et C. Reutenauer (Berstel et Reutenauer, 1990) où la démonstration est adaptée à la fonction zêta généralisée d'un langage cyclique.

Soient A un alphabet fini et $A^{\mathbb{Z}}$ l'ensemble des mots bi-infinis. Un *décalage* est une application $\sigma : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ définie par

$$\sigma((a_n)_{n\in\mathbb{Z}}) = (a_{n+1})_{n\in\mathbb{Z}}.$$

Un système dynamique (S, σ) est une partie S de $A^{\mathbb{Z}}$ qui est fermée et invariante sous σ, i.e. $\sigma(S) = S$.

Soient (S, σ) et (T, τ) deux systèmes dynamiques, *un homomorphisme ϕ de systèmes dynamiques* est une application continue $\phi : S \to T$ qui commute avec les décalages ; i.e., $\phi \circ \sigma = \tau \circ \phi$.

Mike Boyle (Boyle, 1989) associe à chaque homomorphisme de systèmes dynamiques une fonction zêta en plusieurs variables. On va vérifier que la fonction zêta de l'automate (équation (5.1)) est une spécialisation de celle de M. Boyle.

Soit $\mathcal{A}$ un automate non ambigu. On lui associe deux systèmes dynamiques (S, σ) et (T, τ), où S et T sont les ensembles des chemins bi-infinis dans $\mathcal{A}$ et des étiquettes (mots bi-infinis) de ces chemins respectivement, et où σ et τ sont les décalages définis par la translation $(a_n)_{n\in\mathbb{Z}} = (a_{n+1})_{n\in\mathbb{Z}}$. Définissons $\phi : S \to T$ par l'étiquetage d'un chemin bi-infini, on a $\phi \circ \sigma = \tau \circ \phi$.

Un morphisme ϕ de deux systèmes dynamiques est *fini* ("finite-to-one") (resp. *borné* ("bounded-to-one")) si pour tout $t \in T$, la cardinalité de $\phi^{-1}(t)$ est finie (resp. bornée).

Proposition 5.42. *(voir (Béal et Perrin, 1997), Prop. 16) Soit $\mathcal{A}$ un automate transitif.*

On a les équivalences suivantes.

(i) $\mathcal{A}$ est non ambigu.

(ii) Le morphisme qui envoie les chemins bi-infinis de $\mathcal{A}$ vers leurs étiquettes est fini.

Proposition 5.43. *(voir (Béal et Perrin, 1997), Prop. 17) Soit $f : S \to T$ une application finie réalisée par un transducteur sur n états. Le nombre de pré-images de tout élément de T est borné par n^2.*

Définition 5.44. Un mot bi-infini w est *périodique* de période k si k est le plus petit entier positif tel que $\sigma^k(w) = w$.

Soit $t \in T$ un mot périodique de période n, $\phi^{-1}(t)$ est fermé sous σ^n. Par définition de ϕ, chaque élément de $\phi^{-1}(t)$ est périodique. En effet, ϕ commute avec les décalages, $\phi \circ \sigma = \tau \circ \phi$, donc $\phi \circ \sigma^n = \tau^n \circ \phi$. Or

$$\phi(x) = y \Rightarrow \phi \circ \sigma^n(x) = \tau^n \circ \phi(x) = \tau^n(y) = y.$$

Donc le décalage σ^n induit une permutation sur l'ensemble fini $\phi^{-1}(t)$ et on dénote par $\lambda(t)$ le partage $\lambda_1, \ldots, \lambda_k$ où les longueurs des cycles de cette permutation sont $\lambda_1, \ldots \lambda_k$, avec les multiplicités.

Soit x_λ une variable, une pour chaque partage λ. Par les deux dernières Propositions, puisque $\mathcal{A}$ est non ambigu alors, ϕ est un morphisme borné. Puisque $\phi^{-1}(t)$ est de cardinalité bornée, on a un nombre fini de partages. Fixons λ et considérons tous les $t \in T$ de période n tels que $\lambda(t) = \lambda$. Dénotons par $N_n(\lambda)$ leurs cardinalités. Boyle définit la fonction zêta partielle de λ par

$$\zeta_\lambda(z) = \exp\left\{\sum_{n\geq 1} N_n(\lambda)\frac{z^n}{n}\right\},$$

et la fonction zêta de ϕ par

$$Z_\phi = \prod_\lambda \zeta_\lambda^{x_\lambda},$$

où on utilise les développements usuels des séries de la forme $(1 + a_1 z + a_2 z + \ldots)^x$.

Toujours par Boyle, les fonctions zêta de (S, σ) et (T, τ) sont obtenues de Z_ϕ par

$$\begin{aligned}\zeta_\tau(z) &= \prod_\lambda \zeta_\lambda(z), \\ \zeta_\sigma(z) &= \prod_\lambda (\zeta_\lambda(z))^{|Fix(\lambda)|}.\end{aligned}$$

Autrement dit, pour le système (T, τ), on envoie chaque x_λ sur 1 et pour le système (S, σ), on envoie x_λ sur le nombre de parts de λ égales à 1 ; i.e. le nombre de points fixes de σ^n agissant sur $\phi^{-1}(t)$.

Montrons que la spécialisation $x_\lambda \mapsto |\lambda| = \sum \lambda_i$ envoie Z_ϕ vers $\zeta_\mathcal{A}$. En effet, on a que $|\lambda|$ est le nombre de points fixes de $\phi^{-1}(t)$. Donc, $\sum_\lambda N_n(\lambda)\,|\lambda|$ égale le nombre d'éléments de T étant des étiquettes de période n dans T ; $\sum_\lambda N_n(\lambda)\,|\lambda| = a_n$, où a_n est la somme des rangs stables de tous les mots de longueur n.

Ainsi Z_ϕ se spécialise à

$$\prod_\lambda \zeta_\lambda^{|\lambda|} = \prod_\lambda \left(\exp\left\{ \sum_{n\geq 1} N_n(\lambda) \frac{z^n}{n} \right\} \right)^{|\lambda|}$$

$$= \exp\left\{ \sum_{n\geq 1} \sum_\lambda |\lambda|\, N_n(\lambda) \frac{z^n}{n} \right\} = \exp\left\{ \sum_{n\geq 1} a_n \frac{z^n}{n} \right\} = \zeta_\mathcal{A}.$$

Cette spécialisation de Z_ϕ peut être définie directement en termes de systèmes dynamiques via la formule

$$\exp\left\{ \sum_{n\geq 1} \sum_{\tau^n(t)=t} |\phi^{-1}(t)| \frac{z^n}{n} \right\}.$$

Cette fonction est $\mathbb{N}$-rationnelle par la Proposition 5.8.

Exemple 5.45. Reprenons l'automate de la section 5.2. Si $t = {}^\infty b^\infty$, alors la plus petite période de t est 1 et $\phi^{-1}(t)$ a 2 éléments. Si n est impair, σ^n agit transitivement sur $\phi^{-1}(t)$ et si n est pair, il y a deux orbites. Elles correspondent à $\lambda = 2$ et $\lambda = 11$. Ainsi, pour tout autre t, $\phi^{-1}(t)$ a 0 ou 1 élément, on a donc : $N_n(2) = 1$ si n est impair, 0 autrement ; $N_n(11) = 1$ si n est pair, 0 sinon. Choisissons t tel que $\phi^{-1}(t)$ a un élément. Ce correspond au cas où $t = {}^{\infty}w^{\infty}$, où w est de la forme (5.2). Donc $N_1(1)$ est le nombre de tels mots et ζ_1 est la fonction zêta de L, l'ensemble de ces mots.

La série caractéristique L de L est égale à $tr(\mathcal{A}) - tr(\mathcal{A}_1)$, avec les notations de la Section 5.2. Par les méthodes de (Berstel et Reutenauer, 1990), on

$$\begin{aligned}
\zeta_1 &= \frac{1-z^2}{1-z-z^2}, \\
\zeta_{11} &= \exp\left\{\sum_{n\geq 1} \frac{z^{2n}}{2n}\right\} = \exp\left\{\sum_{n\geq 1} \frac{z^{2n}}{n}\right\}^{\frac{1}{2}} = \exp\left\{\ln\left(\frac{1}{1-z^2}\right)\right\}^{\frac{1}{2}} = \left(\frac{1}{1-z^2}\right)^{\frac{1}{2}}, \\
\zeta_2 &= \exp\left\{\sum_{n\geq 0} \frac{z^{2n+1}}{2n+1}\right\} = \frac{\exp\left\{\sum_{n\geq 1} \frac{z^n}{n}\right\}}{\exp\left\{\sum_{n\geq 1} \frac{z^{2n}}{2n}\right\}} = \frac{(1-z^2)^{\frac{1}{2}}}{1-z} = \left(\frac{1+z}{1-z}\right)^{\frac{1}{2}}.
\end{aligned}$$

Ainsi, la fonction zêta de Boyle est

$$\begin{aligned}
Z_\phi &= \prod_{\lambda} \zeta_\lambda^{|\lambda|} = \frac{(1-z^2)^{x_1}(1+z)^{\frac{x_2}{2}}}{(1-z-z^2)^{x_1}(1-z^2)^{\frac{x_{11}}{2}}(1-z)^{\frac{x_2}{2}}} \\
&= \frac{(1-z)^{x_1}(1+z)^{x_1}(1+z)^{\frac{x_2}{2}}}{(1-z-z^2)^{x_1}(1-z)^{\frac{x_{11}}{2}}(1+z)^{\frac{x_{11}}{2}}(1-z)^{\frac{x_2}{2}}} \\
&= \frac{(1+z)^{\frac{x_2}{2}-\frac{x_{11}}{2}+x_1}}{(1-z-z^2)^{x_1}(1-z)^{\frac{x_{11}}{2}-x_1+\frac{x_2}{2}}}.
\end{aligned}$$

En spécialisant x_λ à $|\lambda|$, i.e. $x_1 \mapsto 1$, x_{11} et $x_2 \mapsto 2$, cette fonction se spécialise à

$$\frac{1+z}{(1-z-z^2)(1-z)}.$$

CHAPITRE VI

MATRICES GÉNÉRIQUES NON COMMUTATIVES STOCHASTIQUES

Dans ce chapitre, on étudie les matrices génériques stochastiques ; en particulier, on s'intéresse au vecteur propre à gauche associé à la valeur propre 1. Dans le cas commutatif, on montrera que ce vecteur propre de la matrice M est le vecteur ligne des mineurs principaux de la matrice $M - I_n$ (Proposition 6.7). La démonstration est purement algébrique. Dans le cas non-commutatif, on montrera que les éléments de ce vecteur sont les inverses des dérivations des codes reconnus par l'automate dont M est la matrice de cet automate (Théorème 6.12). La démonstration des parties (iv) et (v) du Théorème 6.12 est complètement différente que celle de (Lavallée et al., 2008).

La démonstration du cas non-commutatif nécessite des résultats provenant de la théorie des corps libres, des matrices génériques stochastiques et des corps libres stochastiques.

6.1 Corps libres

Soit $\mathbb{K}$ un corps. Si le groupe multiplicatif de $\mathbb{K}$ est commutatif, $\mathbb{K}$ est un corps commutatif. Lorsqu'il n'y a pas de commutativité, $\mathbb{K}$ est appelé *corps gauche* ou *anneau de division*. L'anneau des séries rationnelles à variables non commutatives $\mathbb{Q}^{rat}\langle\langle A\rangle\rangle$ n'est pas un corps gauche. Cependant, il existe des corps gauches contenant $\mathbb{Q}\langle A\rangle$; parmi ceux-ci, il y a le *corps libre*, dénoté $\mathcal{F}$. Le corps libre est un objet non commutatif dont l'analogue commutatif est le corps des fractions de l'anneau des polynômes commutatifs. On retrouve plusieurs constructions du corps libre, citons celle d'Amitsur (Amitsur, 1966), Bergman (Bergman, 1970), Malcolmson (Malcolmson, 1978), Cohn (Cohn, 1971) et (Cohn, 1995).

Définition 6.1. Une matrice carrée d'ordre n est *pleine* si elle ne peut pas être écrite comme un produit de matrices $n \times n-1$ par $n-1 \times n$. Une matrice qui n'est pas pleine est dite non pleine.

Les corps libres sont caractérisés par la propriété suivante due à Cohn : toute matrice M à coefficients dans $\mathbb{K}\langle X\rangle$ qui est pleine est inversible dans le corps libre ((Cohn, 1995), Théorème 4.5.8.).

Définition 6.2. Une matrice carrée d'ordre n est *creuse* s'il existe une sous-matrice de 0 de dimension $p \times q$ telle que $p+q \geq n+1$.

Exemple 6.3. La matrice $\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ est creuse puisqu'il y a un bloc de 0 de dimensions 2×2 et $4 > 3$.

Le résultat suivant est évident.

Proposition 6.4. *Une matrice creuse est non pleine.*

Proposition 6.5. *Soient $\lambda \in \mathcal{D}^{1\times n}$, $M \in \mathcal{D}^{n\times n}$ et $\gamma \in \mathcal{D}^{n\times 1}$, où $\mathcal{D}$ est un corps gauche. On suppose que M est inversible. Alors $\begin{bmatrix} M & \gamma \\ \lambda & 0 \end{bmatrix}$ est inversible si et seulement si $\lambda M^{-1}\gamma \neq 0$.*

Démonstration.

($\Leftarrow$) Supposons que $c = \lambda M^{-1}\gamma \neq 0$, alors l'inverse de $\begin{bmatrix} M & \gamma \\ \lambda & 0 \end{bmatrix}$ est

$$\begin{bmatrix} M^{-1} - M^{-1}\gamma c^{-1}\lambda M^{-1} & M^{-1}\gamma c^{-1} \\ c^{-1}\lambda M^{-1} & -c^{-1} \end{bmatrix}.$$

En effet, cette matrice est l'inverse à droite de M puisque

$$\begin{aligned}
&\begin{bmatrix} M & \gamma \\ \lambda & 0 \end{bmatrix} \begin{bmatrix} M^{-1} - M^{-1}\gamma c^{-1}\lambda M^{-1} & M^{-1}\gamma c^{-1} \\ c^{-1}\lambda M^{-1} & -c^{-1} \end{bmatrix} \\
= &\begin{bmatrix} M(M^{-1} - M^{-1}\gamma c^{-1}\lambda M^{-1}) + \gamma c^{-1}\lambda M^{-1} & M(M^{-1}\gamma c^{-1}) - \gamma c^{-1} \\ \lambda(M^{-1} - M^{-1}\gamma c^{-1}\lambda M^{-1}) & \lambda M^{-1}\gamma c^{-1} \end{bmatrix} \\
= &\begin{bmatrix} 1 - \gamma c^{-1}\lambda M^{-1} + \gamma c^{-1}\lambda M^{-1} & \gamma c^{-1} - \gamma c^{-1} \\ \lambda M^{-1} - \underbrace{\lambda M^{-1}\gamma}_{=c} c^{-1}\lambda M^{-1} & \underbrace{\lambda M^{-1}\gamma}_{=c} c^{-1} \end{bmatrix} \\
= &\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.
\end{aligned}$$

Cette matrice est également l'inverse à gauche de M car

$$\begin{aligned}
&\begin{bmatrix} M^{-1} - M^{-1}\gamma c^{-1}\lambda M^{-1} & M^{-1}\gamma c^{-1} \\ c^{-1}\lambda M^{-1} & -c^{-1} \end{bmatrix} \begin{bmatrix} M & \gamma \\ \lambda & 0 \end{bmatrix} \\
= &\begin{bmatrix} (M^{-1} - M^{-1}\gamma c^{-1}\lambda M^{-1})M + M^{-1}\gamma c^{-1}\lambda & (M^{-1} - M^{-1}\gamma c^{-1}\lambda M^{-1})\gamma \\ (c^{-1}\lambda M^{-1})M - c^{-1}\lambda & (c^{-1}\lambda M^{-1})\gamma \end{bmatrix} \\
= &\begin{bmatrix} 1 - M^{-1}\gamma c^{-1}\lambda + M^{-1}\gamma c^{-1}\lambda & M^{-1}\gamma - M^{-1}\gamma c^{-1} \underbrace{\lambda M^{-1}\gamma}_{=c} \\ c^{-1}\lambda - c^{-1}\lambda & c^{-1} \underbrace{\lambda M^{-1}\gamma}_{=c} \end{bmatrix} \\
= &\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.
\end{aligned}$$

($\Rightarrow$) Supposons que $\begin{bmatrix} M & \gamma \\ \lambda & 0 \end{bmatrix}$ soit inversible. Soit $\begin{bmatrix} M' & \gamma' \\ \lambda' & \alpha \end{bmatrix}$ son inverse. Alors on a

$$\begin{bmatrix} M & \gamma \\ \lambda & 0 \end{bmatrix} \begin{bmatrix} \gamma' \\ \alpha \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}.$$

Donc $M\gamma' + \gamma\alpha = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} = 0$ et $\lambda\gamma' = 1$. Il s'ensuit que

$$\begin{aligned} \gamma' &= -M^{-1}\gamma\alpha \\ \Rightarrow \lambda\gamma' &= -\lambda M^{-1}\gamma\alpha = 1 \\ \Rightarrow \lambda M^{-1}\gamma &\neq 0. \end{aligned}$$

On en déduit le résultat suivant.

Corollaire 6.6. *Soient λ, M et γ des matrices à coefficients dans $\mathbb{K}\langle A\rangle$ où M est pleine. Si $\begin{bmatrix} M & \gamma \\ \lambda & 0 \end{bmatrix}$ est non pleine (en particulier si $\begin{bmatrix} M & \gamma \\ \lambda & 0 \end{bmatrix}$ est équivalente par transformations élémentaires de lignes et de colonnes à une matrice creuse) alors $\lambda M^{-1}\gamma = 0$ dans le corps libre.*

6.2 Matrices génériques stochastiques

Soit M une matrice carrée ayant un vecteur propre à droite donné pour une certaine valeur propre donnée. On s'intéresse au vecteur propre à gauche de M pour cette même valeur propre. Puisqu'on peut toujours se ramener à une *matrice stochastique* (i.e. la somme des éléments de chaque ligne vaut 1), on va se ramener au vecteur propre à droite $(1, 1, \ldots, 1)^T$ associé à la valeur propre 1. En effet, supposons que la matrice carrée $M = (a_{ij})_{1\leq i,j\leq n}$ soit stochastique ; i.e. pour tout $i = 1, \ldots, n$, $\sum_{j=1}^{n} a_{i\,j} = 1$. On a

$$\begin{aligned} M \cdot {}^t(1, \ldots, 1) &= {}^t\left(\sum_{j=1}^{n} a_{1\,j}, \ldots, \sum_{j=1}^{n} a_{n\,j}\right) \\ &= {}^t(1, \ldots, 1) \\ &= I_n\, {}^t(1, \ldots, 1) \\ \Leftrightarrow (M - I_n) \cdot {}^t(1, \ldots, 1) &= {}^t(0, \ldots, 0), \end{aligned}$$

où I_n est la matrice identité d'ordre n. Dans le cas commutatif, on a le résultat suivant

Proposition 6.7. *Soient M une matrice stochastique et $N = M - I_n = (b_{ij})_{1 \leq i, j \leq n}$; i.e. pour tout $i = 1, \ldots, n$, $\sum_{j=1}^{n} b_{ij} = 0$. Le vecteur ligne des mineurs principaux N_i de N est un vecteur propre à gauche de N associé à 0.*

Démonstration. Par définition de N, $\det(N) = 0$. On va montrer que

$$(N_1, N_2, \ldots, N_n)\, N = 0.$$

Vérifions cette équation avec la 1^{re} colonne de N, on a

$$
\begin{aligned}
& N_1\, b_{11} + \ldots + N_n\, b_{n1} \\
= & \begin{vmatrix} b_{22} & b_{23} & \ldots & b_{2n} \\ b_{32} & b_{33} & \ldots & b_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n2} & b_{n3} & \ldots & b_{nn} \end{vmatrix} b_{11} + \ldots + \begin{vmatrix} b_{11} & b_{12} & \ldots & b_{1,n-1} \\ b_{21} & b_{22} & \ldots & b_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n-1,1} & b_{n-1,2} & \ldots & b_{n-1,n-1} \end{vmatrix} b_{n1} \\
= & \begin{vmatrix} b_{22} & b_{23} & \ldots & b_{2n} \\ b_{32} & b_{33} & \ldots & b_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n2} & b_{n3} & \ldots & b_{nn} \end{vmatrix} b_{11} + \ldots + \begin{vmatrix} -\sum_{j=2}^{n} b_{1j} & b_{12} & \ldots & b_{1,n-1} \\ -\sum_{j=2}^{n} b_{2j} & b_{22} & \ldots & b_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ -\sum_{j=2}^{n} b_{n-1,j} & b_{n-1,2} & \ldots & b_{n-1,n-1} \end{vmatrix} b_{n1} \\
= & \begin{vmatrix} b_{22} & b_{23} & \ldots & b_{2n} \\ b_{32} & b_{33} & \ldots & b_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n2} & b_{n3} & \ldots & b_{nn} \end{vmatrix} b_{11} + \ldots - \underbrace{\begin{vmatrix} b_{12} & b_{12} & \ldots & b_{1,n-1} \\ b_{22} & b_{22} & \ldots & b_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n-1,2} & b_{n-1,2} & \ldots & b_{n-1,n-1} \end{vmatrix}}_{=0} b_{n1} \\
& - \ldots - \underbrace{\begin{vmatrix} b_{1,n-1} & b_{12} & \ldots & b_{1,n-1} \\ b_{2,n-1} & b_{22} & \ldots & b_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n-1,n-1} & b_{n-1,2} & \ldots & b_{n-1,n-1} \end{vmatrix}}_{=0} b_{n1} - \begin{vmatrix} b_{1n} & b_{12} & \ldots & b_{1,n-1} \\ b_{2n} & b_{22} & \ldots & b_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n-1,n} & b_{n-1,2} & \ldots & b_{n-1,n-1} \end{vmatrix} b_{n1}
\end{aligned}
$$

$$
\begin{aligned}
&= \begin{vmatrix} b_{22} & b_{23} & \ldots & b_{2n} \\ b_{32} & b_{33} & \ldots & b_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n2} & b_{n3} & \ldots & b_{nn} \end{vmatrix} b_{11} - \ldots - \begin{vmatrix} b_{1n} & b_{12} & \ldots & b_{1,n-1} \\ b_{2n} & b_{22} & \ldots & b_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n-1,n} & b_{n-1,2} & \ldots & b_{n-1,n-1} \end{vmatrix} b_{n1} \\
&= \begin{vmatrix} b_{22} & b_{23} & \ldots & b_{2n} \\ b_{32} & b_{33} & \ldots & b_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n2} & b_{n3} & \ldots & b_{nn} \end{vmatrix} b_{11} - \ldots - (-1)^{n-2} \begin{vmatrix} b_{12} & b_{13} & \ldots & b_{1n} \\ b_{22} & b_{23} & \ldots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n-1,2} & b_{n-1,3} & \ldots & b_{n-1,n} \end{vmatrix} b_{n1} \\
&= \begin{vmatrix} b_{22} & b_{23} & \ldots & b_{2n} \\ b_{32} & b_{33} & \ldots & b_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n2} & b_{n3} & \ldots & b_{nn} \end{vmatrix} b_{11} - \ldots + (-1)^{n+1} \begin{vmatrix} b_{12} & b_{13} & \ldots & b_{1n} \\ b_{22} & b_{23} & \ldots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n-1,2} & b_{n-1,3} & \ldots & b_{n-1,n} \end{vmatrix} b_{n1} \\
&= \det(N) \\
&= 0.
\end{aligned}
$$

Ce résultat est bien connu en probabilités puisqu'il permet de calculer la probabilité limite d'un procédé de Markov fini, en remplaçant la matrice stochastique M par $M - I$. On peut calculer ces probabilités en utilisant le Théorème des arbres de chaînes de Markov (Markov chain trees theorem), voir (Broder, 1989), (Anantharam et Tsoucas, 1989) ou (Aldous, 1990), où ce calcul est donné en termes d'arbres générateurs.

On va énoncer une version non-commutative de ce résultat. Soit $M = (a_{ij})_{1 \leq i,j \leq n}$ une *matrice générique non commutative* ; i.e. les a_{ij} sont des variables non commutatives. On dénote $\mathcal{F}$ le corps libre correspondant. On associe à M la matrice S : c'est la même matrice sauf qu'on suppose que les a_{ij} sont soumis aux *relations stochastiques*

$$\forall i = 1, \ldots, n, \sum_{j=1}^{n} a_{ij} = 1. \tag{6.1}$$

Autrement dit, la somme de chaque ligne de S vaut 1 ; donc S est une matrice stochastique. On appelle S une *matrice générique non commutative stochastique*. L'algèbre sur $\mathbb{Q}$ engendrée par ces coefficients est une algèbre associative libre, puisqu'isomorphe à l'algèbre $\mathbb{Q}\langle a_{ij},\, i \neq j\rangle$. En effet, on peut éliminer les a_{ii} par les relations (6.1). On dénote cette algèbre $\mathbb{Q}\langle a_{ij}/(6.1)\rangle$, en référence aux relations (6.1). Ainsi, il y a un corps libre correspondant appelé *corps libre stochastique* dénoté $\mathcal{S}$.

6.3 Existence des éléments et identités dans le corps libre stochastique

On veut vérifier que certaines expressions rationnelles ont un sens dans le corps libre stochastique libre $\mathcal{S}$. Par exemple, soient a, b, c et d quatre variables non commutatives soumises aux relations stochastiques $a + b = 1$ et $c + d = 1$ et $(1 + bd^*)^{-1} = (1 + b(1 - d)^{-1})^{-1}$ une expression rationnelle. On veut montrer que cette expression existe dans $\mathcal{S}$.

On va démontrer l'existence de certaines spécialisations des variables, compatibles avec les relations stochastiques de $\mathcal{S}$ de façon à ce que les expressions rationnelles spécialisées ont un sens dans $\mathcal{S}$. Reprenons l'exemple précédent, posons $b = 0$, alors bd^* se spécialise à 0 et $1 + bd^*$ à 1. Ainsi, l'expression $(1 + bd^*)^{-1}$ est définie sous cette spécialisation.

Définition 6.8. Un *morphisme de Bernoulli* est un morphisme π de $\mathbb{Q}$-algèbres de l'algèbre associative libre $\mathbb{Q}\langle a_{ij}\rangle$ vers $\mathbb{R}$ tel que

(i) pour tout $i = 1, \ldots, n$, $\sum_{j=1}^{n} \pi(a_{ij}) = 1$;

(ii) $\pi(a_{ij}) > 0$, pour tout $i, j = 1, \ldots, n$.

Un tel morphisme induit naturellement un morphisme de $\mathbb{Q}$-algèbres de $\mathbb{Q}\langle a_{ij}/(6.1)\rangle$ vers $\mathbb{R}$.

Lemme 6.9. *Il existe un sous-anneau $\mathcal{S}_\pi$ du corps libre stochastique $\mathcal{S}$ tel que*

(i) $\mathcal{S}_\pi$ contient $\mathbb{Q}\langle a_{ij}/(6.1)\rangle$;

(ii) il existe un prolongement de π vers $\mathcal{S}_\pi$ (qu'on dénote π) ;

(iii) si $f \in \mathcal{S}_\pi$ and $\pi(f) \neq 0$, alors $f^{-1} \in \mathcal{S}_\pi$.

Démonstration. C'est une conséquence du fait que $\mathcal{S}$ est un corps libre, donc le corps universel des fractions $\mathbb{Q}\langle a_{ij}$ (6.1)$\rangle$. Ce qui implique qu'il existe une spécialisation $\mathcal{S} \rightarrow \mathbb{R}$ prolongeant $\pi : \mathbb{Q}\langle a_{ij}/(6.1)\rangle \rightarrow \mathbb{R}$, et le lemme s'ensuit. Voir (Cohn, 1971) 7.2 et Cor. 7.5.11.

Corollaire 6.10. *Soient π un morphisme de Bernoulli et $S = \sum_{w \in L} w$, où L est un langage rationnel du monoïde libre $\{a_{ij}\}^*$ tel que $\sum_{w \in L} \pi(w) < \infty$. Alors, pour toute expression rationnelle de S, cette expression est définie dans le corps libre stochastique $\mathcal{S}$.*

Démonstration. On le démontre par récurrence sur la taille de l'expression rationnelle de S. Comme π est un morphisme positif, pour chaque sous-expression et série correspondante S', $\pi(S')$ converge et est > 0. On applique par récurrence le lemme et on voit que pour chaque sous-expression, que l'élément correspondant est dans $\mathcal{S}_\pi$.

Lemme 6.11. *Soit S une série rationnelle dans $\mathbb{Q}\langle\langle a_{ij}\rangle\rangle$ ayant une expression rationnelle définie dans $\mathcal{S}$. Alors elle est définie dans $\mathcal{F}$. De plus, si $S = 0$ dans $\mathcal{F}$, alors $S = 0$ dans $\mathcal{S}$.*

Démonstration. Il existe une spécialisation $\mathcal{F} \rightarrow \mathcal{S}$, car $\mathcal{F}$ est le corps universel des fractions de $\mathbb{Q}\langle a_{ij}\rangle$, voir (Cohn, 1971), Chapitre 7. Donc, il existe un sous-anneau H de $\mathcal{F}$ et un morphisme surjectif de $\mathbb{Q}$-algèbres $\mathcal{S} : H \rightarrow \mathcal{S}$ tel que : $\forall f \in H$, $\mathcal{S}(H) \neq 0 \Rightarrow f^{-1} \in H$, et tel que H contienne $\mathbb{Q}\langle a_{ij}\rangle$.

On prouve donc par induction sur la taille de l'expression rationnelle que S existe dans $\mathcal{F}$ et que $\mathcal{S}(S)$ est un élément de $\mathcal{S}$ défini par l'expression rationnelle. Il s'ensuit que si $S = 0$ dans $\mathcal{F}$, alors $S = 0$ dans $\mathcal{S}$.

6.4 Chemins

Soit $M = (a_{ij})_{1 \leq i, j \leq n}$ une matrice générique non commutative. Soit $\mathcal{A}$ l'automate à n états ayant les flèches $i \xrightarrow{a_{ij}} j$, $i, j = 1, \ldots, n$. La matrice M est donc la *matrice de l'automate $\mathcal{A}$.*

Soit C_i l'ensemble des étiquettes de tous les chemins $i \to i$. Puisque que C_i est un langage reconnu par $\mathcal{A}$, sa série caractéristique C_i est une série reconnaissable ; du Théorème de Schützenberger, C_i est une série rationnelle. Il s'ensuit que cette série est un élément du corps libre $\mathcal{F}$.

Soit P_i la somme des chemins partant de i et ne repassant pas par i, alors P_i est l'ensemble des préfixes propres de C_i. Du même raisonnement que C_i, P_i est un élément de $\mathcal{F}$.

Soit w un mot, on définit la *dérivation* λ de w par $\lambda(w) = |w|\, w$. Du Théorème 7.5.17 de (Cohn, 2005), λ se prolonge de façon unique dans le corps libre $\mathcal{F}$, que nous noterons encore λ.

Cette fonction a les propriétés suivantes :

$$\begin{aligned}
\lambda(P\,Q) &= \lambda(P)\,Q + P\,\lambda(Q), \\
\lambda\,(P^*) &= P^*\lambda(P)\,P^*,
\end{aligned}$$

où P et Q sont deux expressions rationnelles non commutatives. Démontrons la première propriété ; soient u et v deux mots, on a

$$\begin{aligned}
\lambda(u\,v) &= |u\,v|\,u\,v \\
&= (|u| + |v|)\,u\,v \\
&= |u|\,u\,v + u\,|v|\,v \\
&= \lambda(u)\,v + u\,\lambda(v).
\end{aligned}$$

Démontrons la seconde propriété, on a

$$\begin{aligned}
\lambda\,(P^*) &= \sum_{n=0}^{\infty} \lambda\,(P^n) \\
&= \sum_{n=0}^{\infty} \left(\lambda(P)\,P^{n-1} + P\,\lambda(P)\,P^{n-2} + \ldots\right) \\
&= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} P^i\,\lambda(P)\,P^j
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=0}^{\infty} P^i \, \lambda(P) \sum_{j=0}^{\infty} P^j \\
&= P^* \, \lambda(P) \, P^*.
\end{aligned}
$$

Soit $\mathcal{A}$ un automate ayant n sommets et soit M la matrice de $\mathcal{A}$. Soient $C_1, C_2, \ldots, C_n$ les n langages reconnus par $\mathcal{A}$. Si $\mathcal{A}$ est non ambigu, les langages C_i sont des codes par la Proposition 5.21. Soient $\lambda_1 = \lambda(C_1)$, $\lambda_2 = \lambda(C_2), \ldots, \lambda_n = \lambda(C_n)$ les longueurs moyennes des codes $C_1, C_2, \ldots, C_n$ respectivement.

Théorème 6.12. *Soit $M = (a_{ij})_{1 \leq i, j \leq n}$ (matrice générique non commutative) la matrice de l'automate $\mathcal{A}$. Soient C_i et P_i les langages définis ci-haut.*

(i) Les P_i^{-1} sont définis dans le corps libre stochastique $\mathcal{S}$.

(ii) Les C_i sont définis dans $\mathcal{S}$ et sont égaux à 1.

(iii) $\lambda(C_i)$ est défini dans $\mathcal{S}$ et est égal à P_i.

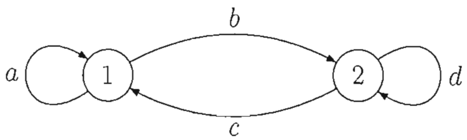
(iv) On a dans $\mathcal{S}$

$$(P_1^{-1}, \ldots, P_n^{-1}) \, M = (P_1^{-1}, \ldots, P_n^{-1}), \tag{6.2}$$

(v) On a dans $\mathcal{S}$

$$\sum_{i=1}^{n} P_i^{-1} = 1. \tag{6.3}$$

Exemple 6.13. Soit $\mathcal{A}$ l'automate



La matrice de $\mathcal{A}$ est $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Soit $S = M$ avec $a + b = 1$ et $c + d = 1$. On trouve

$$
\begin{aligned}
C_1 &= a + bd^*c, \qquad C_2 = d + ca^*b, \\
P_1 &= 1 + bd^*, \qquad P_2 = 1 + ca^*.
\end{aligned}
$$

Vérifions la condition (ii),

$$C_1 = a + bd^*c = (1 - b) + bd^*(1 - d) = 1 - b + b = 1.$$

De la même façon on trouve $C_2 = 1$.

Vérifions la condition (iii),

$$\begin{aligned}
\lambda(C_1) &= \lambda(a) + \lambda(bd^*c) \\
&= a + bd^*c + b\lambda(d^*)c + bd^*c = a + 2bd^*c + bd^*dd^*c \\
&= (1-b) + 2bd^*(1-d) + bd^*dd^*(1-d) \\
&= 1 - b + 2b + bd^*d = 1 + b + bd^*d = 1 + b(1+d^+) = 1 + bd^* = P_1.
\end{aligned}$$

De façon similaire, on trouve $\lambda(C_2) = P_2 = 1 + ca^*$. Vérifions la condition (iv), pour ce faire, on va montrer que le système suivant satisfait

$$(P_1^{-1}, P_2^{-1})\, M = (P_1^{-1}, P_2^{-1}).$$

De ce système, on a les 2 équations suivantes :

$$P_1^{-1}\, a + P_2^{-1}\,(1-d) = P_1^{-1}, \tag{6.4}$$

$$P_1^{-1}\,(1-a) + P_2^{-1}\, d = P_2^{-1}. \tag{6.5}$$

Vérifions l'équation (6.4),

$$\begin{aligned}
P_1^{-1}\, a + P_2^{-1}\,(1-d) &= P_1^{-1} \\
\Leftrightarrow P_2^{-1}\,(1-d) &= P_1^{-1}\,(1-a) \\
\Leftrightarrow d^*\, P_2 &= a^*\, P_1 \qquad (6.6) \\
\Leftrightarrow d^*\,(1+ca^*) &= a^*\,(1+bd^*) \\
\Leftrightarrow d^* + d^*(1-d)a^* &= a^* + a^*(1-a)d^* \\
\Leftrightarrow d^* + a^* &= a^* + d^*.
\end{aligned}$$

Ainsi, l'équation (6.4) est satisfaite. Vérifions maintenant l'équation (6.5), on a

$$\begin{aligned}
P_1^{-1}\,(1-a) + P_2^{-1}\, d &= P_2^{-1} \\
\Leftrightarrow P_1^{-1}\,(1-a) &= \lambda_2^{-1}\,(1-d) \\
\Leftrightarrow a^*\, P_1 &= d^*\, P_2.
\end{aligned}$$

Puisqu'on obtient encore l'équation (6.6), il s'ensuit que l'équation (6.5) est également satisfaite ; ainsi, le système l'est aussi.

Finalement, il reste à vérifier la condition (v).

$$\begin{aligned} P_1^{-1} + P_2^{-1} &= P_1^{-1} + P_1^{-1}(1-a)d^* \quad \text{par l'équation (6.6)} \\ &= P_1^{-1} + P_1^{-1}bd^* \\ &= P_1^{-1}(1+bd^*) = P_1^{-1}P_1 = 1. \end{aligned}$$

Démonstration du Théorème 6.12.

Soit $M = (a_{ij})_{1\leq i,\, j\leq n}$ la matrice de l'automate $\mathcal{A}$. Soit a_{ij} l'étiquette de l'arête joignant i à j. Considérons le monoïde libre $\{a_{ij}\}^*$. On peut identifier une somme infinie de chemins étiquetés avec leurs séries correspondantes dans $\mathbb{Q}\langle\langle a_{ij}\rangle\rangle$.

Soit P_{ij} l'ensemble des chemins de i vers j ne passant pas par i. On a $P_i = \sum P_{ij}$. On observe que chaque chemin de i vers j peut être décomposé comme la concaténation d'un chemin de i vers i (un élément de C_i^*) et d'un chemin de i vers j ne passant pas par i (élément de P_{ij}).

Comme $(M^*)_{ij}$ est la somme de tous les chemins de i vers j, on obtient l'identité dans $\mathbb{Q}\langle\langle a_{ij}\rangle\rangle : (M^*)_{ij} = C_i^*\, P_{ij}$.

On a $P_{ii} = 1$. Les P_{ij}, $i \neq j$ n'ont pas de termes constants ; d'où $(P_{ij}))_{1\leq i,j\leq n}$ est inversible dans $\mathbb{Q}\langle\langle a_{ij}\rangle\rangle$. On a

$$
\begin{aligned}
M^* &= \begin{bmatrix} C_1^* & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & C_n^* \end{bmatrix} \begin{bmatrix} P_{11} & \dots & \dots & P_{1n} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ P_{n1} & \dots & \dots & P_{nn} \end{bmatrix} \\
\Leftrightarrow \begin{bmatrix} 1-C_1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1-C_n \end{bmatrix} &= \begin{bmatrix} P_{11} & \dots & \dots & P_{1n} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ P_{n1} & \dots & \dots & P_{nn} \end{bmatrix} (1-M)
\end{aligned}
$$

$$
\begin{aligned}
\Leftrightarrow \begin{bmatrix} C_1-1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & C_n-1 \end{bmatrix} &= \begin{bmatrix} P_{11} & \dots & \dots & P_{1n} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ P_{n1} & \dots & \dots & P_{nn} \end{bmatrix} (M-1) \\
\Leftrightarrow (C_1-1, \dots, C_n-1) &= (P_{ij})_{1\leq i,j\leq n}\,(M-1)\,\gamma, \qquad (6.7)
\end{aligned}
$$

où $\gamma = {}^t(1,\dots,1)$. Cette dernière égalité est valide dans $\mathbb{Q}\langle\langle a_{ij}\rangle\rangle$ ainsi que dans sa sous-algèbre des séries rationnelles puisque les C_i et les P_{ij} sont des séries rationnelles. Donc, cette égalité est valide dans le corps libre $\mathcal{F}$.

Montrons que les C_i, P_{ij} et les $\lambda(C_i)$ sont bien définis dans le corps libre stochastique $\mathcal{S}$. Soit π un morphisme de Bernoulli. Soit $1 \leq i \leq n$, considérons l'ensemble E des chemins ne passant pas par i. Alors $\pi(E) < \infty$ puisque la matrice N, obtenu de M en enlevant la i^e ligne et la i^e colonne satisfait $\pi(N) < 1$. Il s'ensuit que $\pi(C_i)$ et $\pi(P_{ij})$ sont finis. Pour $\lambda(C_i)$, il est facile de voir par induction sur la taille de l'expression rationnelle de C_i que $\lambda(C_i)$ est défini dans $\mathcal{S}$ puisque C_i l'est. On a aussi $\pi(P_i) > 0$, donc P_i est non nul dans $\mathcal{S}$; d'où P_i^{-1} est un élément de $\mathcal{S}$. Ceci démontre (i).

Appliquons la dérivation λ de part et d'autre de l'équation (6.7), on a

$$\begin{aligned}
(\lambda(C_1-1),\, \ldots,\, \lambda(C_n-1)) &= (\lambda(P_{ij})_{1\leq i,j\leq n})\,(M-1)\,\gamma + (P_{ij})_{1\leq i,j\leq n}\,\lambda(M-1)\,\gamma \\
\Leftrightarrow (\lambda(C_1),\, \ldots,\, \lambda(C_n)) &= (\lambda(P_{ij})_{1\leq i,j\leq n})\,(M-1)\,\gamma + (P_{ij})_{1\leq i,j\leq n}\,M\,\gamma \\
&= (\lambda(P_{ij})_{1\leq i,j\leq n})\,(M\gamma-\gamma) + (P_{ij})_{1\leq i,j\leq n}\,M\,\gamma \\
&= (\lambda(P_{ij})_{1\leq i,j\leq n})\,(\gamma-\gamma) + (P_{ij})_{1\leq i,j\leq n}\,\gamma, \qquad \text{car } M\gamma=\gamma \text{ dans } \mathcal{S} \\
&= (P_{ij})_{1\leq i,j\leq n}\,\gamma \\
&= (P_1,\, \ldots,\, P_n).
\end{aligned}$$

Ce qui démontre (ii) et (iii).

Démontrons maintenant (iv). Soient $M=(a_{ij})_{1\leq i,j\leq n}$ la matrice de l'automate $\mathcal{A}$ et P_i, le langage reconnu par $\mathcal{A}$ auquel on enlève toutes les flèches arrivant à l'état i. On a

$$P_i = \sum_{j=1}^{n} L_{ij}, \quad i=1,\, \ldots,\, n,$$

où

$$L_{ij} = \begin{cases} 1, & \text{si } i=j, \\ \displaystyle\sum_{k=1}^{n} L_{ik}\,a_{kj} = a_{ij} + \sum_{\substack{k=1\\k\neq i}}^{n} L_{ik}\,a_{kj}, & \text{si } i\neq j. \end{cases}$$

Soit (S_i) le système composé des n équations définissant P_i, L_{i1}, ..., $L_{i,i-1}$, $L_{i,i+1}$, ..., L_{in}. Multiplions à gauche par P_i^{-1} chacune des équations de S_i , on obtient le système

$$(T_i) : \begin{cases} 1 = P_i^{-1} + \displaystyle\sum_{\substack{j=1\\j\neq i}}^{n} P_i^{-1}\,L_{ij}, \quad i=1,\ldots,n, \\ P_i^{-1}\,L_{ij} = P_i^{-1}\,a_{ij} + \displaystyle\sum_{\substack{k=1\\k\neq i}}^{n} P_i^{-1}\,L_{ik}\,a_{kj}. \end{cases}$$

Posons $Q_{ij} = P_i^{-1}\,L_{ij}$, le système (T_i) devient

$$(T_i) : \begin{cases} 1 = P_i^{-1} + \displaystyle\sum_{\substack{j=1\\j\neq i}}^{n} Q_{ij}, \quad i=1,\ldots,n, \\ Q_{ij} = P_i^{-1}\,a_{ij} + \displaystyle\sum_{\substack{k=1\\k\neq i}}^{n} Q_{ik}\,a_{kj}. \end{cases}$$

Réécrivons ce système sous la forme

$$
(U_i) : \begin{cases} 1 = P_i^{-1} + \displaystyle\sum_{\substack{j=1 \\ j \neq i}}^{n} Q_{ij}, \quad i = 1, \dots, n, \\[2ex] 0 = P_i^{-1}\, a_{ij} + Q_{ij}\,(a_{jj} - 1) + \displaystyle\sum_{\substack{k=1 \\ k \neq i,\, k \neq j}}^{n} Q_{ik}\, a_{kj}. \end{cases}
$$

On veut démontrer que

$$
\sum_{k=1}^{n} P_k^{-1}\, a_{k1} \equiv P_1^{-1}.
$$

Posons

$$
R = \sum_{k=1}^{n} P_k^{-1}\, a_{k1} - P_1^{-1}. \tag{6.8}
$$

On va montrer que $R = 0$. Tout d'abord, on réécrit la dernière équation comme

$$
R - P_1^{-1}\,(1 - a_{11}) - \sum_{k=2}^{n} P_k^{-1}\, a_{k1} = 0. \tag{6.9}
$$

Considérons le système des $n^2 + 1$ équations constitué de l'équation (6.9) et des n systèmes (U_1), ..., (U_n). On représente ce système sous la forme matricielle suivante

$$
(R, P_1^{-1}, Q_{12}, Q_{13}, \dots, Q_{1n},\, P_2^{-1}, Q_{21}, Q_{23}, \dots, Q_{2n}, \dots P_n^{-1}, Q_{n1}, \dots, Q_{n,n-1}) \cdot E = \lambda,
$$

$$
E = \left[\begin{array}{ccccccccc}
1 & 0 & 0 & \dots & 0 & & 0 & & \\
1 - a_{11} & & & & & 1 & & & \\
 & A_1 & 0 & & 0 & \vdots & & 0 & \\
0 & & & & & & & & \\
 & & & & & 1 & & & \\
-a_{21} & & & & & & 1 & & \\
 & 0 & A_2 & & 0 & 0 & \vdots & 0 & \\
0 & & & & & & & & \\
 & & & & & & 1 & & \\
\vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & & \\
-a_{n1} & & & & & & & & 1 \\
 & 0 & 0 & & A_n & & 0 & & \vdots \\
0 & & & & & & & & \\
 & & & & & & & & 1
\end{array}\right],
$$

$$A_m \;=\; \begin{bmatrix} a_{m1} & a_{m2} & \cdots & a_{m,\,m-1} & a_{m,\,m+1} & \cdots & a_{mn} \\ a_{11}-1 & a_{12} & \cdots & a_{1,\,m-1} & a_{1,\,m+1} & \cdots & a_{1n} \\ a_{21} & a_{22}-1 & \cdots & a_{2,\,m-1} & a_{2,\,m+1} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ a_{m-1,\,1} & a_{m-1,\,2} & \cdots & a_{m-1,\,m-1}-1 & a_{m-1,\,m+1} & \cdots & a_{m-1,\,n} \\ a_{m+1,\,1} & a_{m+1,\,2} & \cdots & a_{m+1,\,m-1} & a_{m+1,\,m+1}-1 & \cdots & a_{m+1,\,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ a_{n,\,1} & a_{n,\,2} & \cdots & a_{n,\,m-1} & a_{n,\,m+1} & \cdots & a_{nn}-1 \end{bmatrix},$$

où $m = 1, \ldots, n$ et $\lambda = (0, \ldots, 0, \underbrace{1, \ldots, 1}_{n\ fois})$. E est une matrice carrée d'ordre n^2+1.

On a $R = \lambda E^{-1}\gamma$, $\quad \gamma = {}^t(1, \underbrace{0, \ldots, 0}_{n^2\ fois})$ et $F = \begin{bmatrix} E & \gamma \\ \lambda & 0 \end{bmatrix}$. Cette dernière matrice est de dimension n^2+2. Par ailleurs, E est congrue modulo les relations stochastiques à

$$E \;\equiv\; \left[\begin{array}{cccccccc} 1 & 0 & 0 & \cdots & 0 & & 0 & \\ \begin{matrix} a_{12}+\ldots+a_{1n} \\ \\ 0 \end{matrix} & B_1 & 0 & & 0 & \begin{matrix}1\\ \vdots \\ 1\end{matrix} & 0 & \\ \begin{matrix} -a_{21} \\ \\ 0 \end{matrix} & 0 & B_2 & & 0 & 0 & \begin{matrix}1\\ \vdots \\ 1\end{matrix} & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & & \vdots & \\ \begin{matrix} -a_{n1} \\ \\ 0 \end{matrix} & 0 & 0 & & B_n & & 0 & \begin{matrix}1\\ \vdots \\ 1\end{matrix} \end{array}\right],$$

$$
B_m = \begin{bmatrix}
a_{m1} & a_{m2} & \cdots & a_{m,\,m-1} & a_{m,\,m+1} & \cdots & a_{mn} \\
-\sum\limits_{\substack{k=1\\k\neq 1}}^{n} a_{1k} & a_{12} & \cdots & a_{1,\,m-1} & a_{1,\,m+1} & \cdots & a_{1n} \\
a_{21} & -\sum\limits_{\substack{k=1\\k\neq 2}}^{n} a_{2k} & \cdots & a_{2,\,m-1} & a_{2,\,m+1} & \cdots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
a_{m-1,\,1} & a_{m-1,\,2} & \cdots & -\sum\limits_{\substack{k=1\\k\neq m-1}}^{n} a_{m-1,\,k} & a_{m-1,\,m+1} & \cdots & a_{m-1,\,n} \\
a_{m+1,\,1} & a_{m+1,\,2} & \cdots & a_{m+1,\,m-1} & -\sum\limits_{\substack{k=1\\k\neq m+1}}^{n} a_{m+1,\,k} & \cdots & a_{m+1,\,n} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
a_{n,\,1} & a_{n,\,2} & \cdots & a_{n,\,m-1} & a_{n,\,m+1} & \cdots & -\sum\limits_{\substack{k=1\\k\neq n}}^{n} a_{nk}
\end{bmatrix}.
$$

Afin de montrer que $R = 0$, on va montrer que la matrice F est creuse. On va effectuer des transformations élémentaires de lignes et de colonnes sur F de telle façon à ce qu'elle contienne une sous-matrice de 0 de dimensions $s \times t$ telles que $s + t \geq n^2 + 3$.

$$
F = \begin{bmatrix}
1 & 0 & 0 & \dots & 0 & & 0 & & 1 \\
a_{12} + \ldots + a_{1n} & & & & & 1 & & & \\
 & B_1 & 0 & & 0 & \vdots & 0 & & 0 \\
0 & & & & & & & & \\
 & & & & & 1 & & & \\
-a_{21} & & & & & & 1 & & \\
 & 0 & B_2 & & 0 & 0 & \vdots & 0 & 0 \\
0 & & & & & & & & \\
 & & & & & & 1 & & \\
\vdots & \vdots & \vdots & \ddots & \vdots & & \ddots & & \vdots \\
-a_{n1} & & & & & & & 1 & \\
 & 0 & 0 & & B_n & & 0 & \vdots & 0 \\
0 & & & & & & & & \\
 & & & & & & & 1 & \\
0 & 0 & 0 & \dots & 0 & 1 & \dots & 1 & 1
\end{bmatrix},
$$

Étape 1. On élimine la première ligne et la dernière colonne de F, on obtient ainsi la matrice carrée F_1 d'ordre n^2+1 $(s+t \geq n^2+2)$.

$$F_1 = \left[\begin{array}{cccccc}
\begin{array}{c} a_{12}+\ldots+a_{1n} \\ \boxed{0} \end{array} & \boxed{B_1} & \boxed{0} & \cdots & \boxed{0} & \begin{array}{c|c} 1 & \\ \vdots & 0 \\ 1 & \end{array} \\
\begin{array}{c} -a_{21} \\ \boxed{0} \end{array} & \boxed{0} & \boxed{B_2} & & \boxed{0} & \begin{array}{c|c|c} & 1 & \\ 0 & \vdots & 0 \\ & 1 & \end{array} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \ddots \\
\begin{array}{c} -a_{n1} \\ \boxed{0} \end{array} & \boxed{0} & \boxed{0} & & \boxed{B_n} & \begin{array}{c|c} & 1 \\ 0 & \vdots \\ & 1 \end{array} \\
\boxed{0} & \boxed{0} & \boxed{0} & \cdots & \boxed{0} & 1 \quad \ldots \quad 1
\end{array}\right],$$

Étape 2. On veut obtenir un bloc $n \times n$ de 0 dans le coin supérieur droit. Pour ce faire, on va procéder comme suit. Considérons la j^e ligne de F_1 (correspondant à la j^e ligne de B_1). Par la construction de B_1, le premier indice des éléments de la j^e ligne de ce bloc est j. Par la suite, on considère la ligne passant par le bloc B_2 dont le premier indice des éléments de cette ligne B_2 soit j. Une telle ligne existe par construction de B_2. On répète l'opération pour chaque ligne des blocs $B_3, \ldots, B_n$. On additionne chacune de ces lignes à la j^e ligne de F_1. Il s'ensuit que les n derniers éléments des j^e premières lignes sont tous des 1. Il reste à soustraire chacune des j premières lignes de F_1 par la dernière ligne de F_1. On obtient la matrice

$$F_2 = \left[\begin{array}{c|c|c|c|c||c|c|c}
a_{12}+\ldots+a_{1n} & & & & & 0 & & \\
\boxed{0} & B_1 & C_2 & \ldots & C_n & \vdots & 0 & \\
 & & & & & 0 & & \\
\hline
-a_{21} & & & & & & 1 & \\
\boxed{0} & 0 & B_2 & & 0 & 0 & \vdots & 0 \\
 & & & & & & 1 & \\
\hline
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \\
\hline
-a_{n1} & & & & & 0 & & 1 \\
\boxed{0} & 0 & 0 & & B_n & \vdots & 0 & \\
 & & & & & 0 & & 1 \\
0 & 0 & 0 & \ldots & 0 & 1 & \ldots & 1
\end{array}\right],$$

où

$$C_m = \begin{bmatrix}
-\sum\limits_{\substack{k=1\\k\neq 1}}^{n} a_{1k} & a_{12} & \cdots & a_{1,m-1} & a_{1,m+1} & \cdots & a_{1n} \\
a_{21} & -\sum\limits_{\substack{k=1\\k\neq 2}}^{n} a_{2k} & \cdots & a_{2,m-1} & a_{2,m+1} & \cdots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
a_{n,1} & a_{n,2} & \cdots & a_{n,,m-1} & a_{n,m+1} & \cdots & -\sum\limits_{\substack{k=1\\k\neq n}}^{n} a_{nk}
\end{bmatrix},$$

$m = 2, \ldots, n$. On réduit F_2 en supprimant la dernière ligne et la n^e colonne à partir de la droite. On obtient ainsi la matrice carrée F_3 d'ordre n^2, $(s + t \geq n + 1)$.

$$F_3 = \begin{bmatrix} a_{12}+\ldots+a_{1n} & & & & & \\ 0 & B_1 & C_2 & \ldots & C_n & 0 \\ -a_{21} & & & & & \\ 0 & 0 & B_2 & & 0 & \begin{matrix} 1 & \\ \vdots & 0 \\ 1 & \end{matrix} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \ddots \\ -a_{n1} & & & & & \\ 0 & 0 & 0 & & B_n & \begin{matrix} & 1 \\ 0 & \\ & 1 \end{matrix} \end{bmatrix},$$

Étape 3. Considérons les lignes L_i de F_3, où $i > n$ et $i \not\equiv 0 \mod n$. On veut que les $(n-1)$ derniers éléments de ces lignes soient tous 0. Soit $i = kn + m$, où $0 \leq m \leq n-1$, on va faire $L_i - L_{(k+1)n} = L_{kn+m} - L_{(k+1)n}$, on obtient la matrice

$$F_4 = \begin{bmatrix} a_{12}+\ldots+a_{1n} & & & & & \begin{matrix} 0 & \ldots & 0 \\ \vdots & & \vdots \\ 0 & \ldots & 0 \end{matrix} \\ 0 & B_1 & C_2 & \ldots & C_n & \\ -a_{21} & & & & & \begin{matrix} \vdots & & \vdots \\ 0 & & \vdots \\ 1 & & 0 \end{matrix} \\ 0 & 0 & D_2 & & 0 & \\ \vdots & \vdots & \vdots & \ddots & \vdots & \\ -a_{n1} & & & & & \begin{matrix} 0 & \ddots & \vdots \\ \vdots & & 0 \\ 0 & & 1 \end{matrix} \\ 0 & 0 & 0 & & D_n & \end{bmatrix},$$

où pour tout $m = 2, \ldots, n$,

$$D_m = (d_{ij}^m)_{1 \leq i,j \leq n}, \quad B_m = (b_{ij}^m), \quad d_{ij} = b_{ij}^m - b_{nj}^m.$$

En supprimant les $(n-1)$ lignes L_i où $i > n$ et $n \mid i$ et les $(n-1)$ dernières colonnes de F_4 on obtient matrice carrée F_5 d'ordre $n^2 - n + 1$, $(s + t \geq n^2 - n + 2)$.

$$F_5 \quad = \quad \left[\begin{array}{ccccc} \begin{array}{c} a_{12}+\ldots+a_{1n} \\ \boxed{0} \end{array} & \boxed{B_1} & \boxed{C_2} & \ldots & \boxed{C_n} \\ \begin{array}{c} -a_{21} \\ \boxed{0} \end{array} & \boxed{0} & \boxed{D'_2} & & \boxed{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \begin{array}{c} -a_{n1} \\ \boxed{0} \end{array} & \boxed{0} & \boxed{0} & & \boxed{D'_n} \end{array}\right],$$

où D'_m est la matrice obtenue de D_m en enlevant la dernière ligne.

Étape 4. Dénotons par C_m^1 la première colonne de la matrice C_m et d_m, la colonne de F_5 qui est le prolongement de C_m^1. On veut que C_m^1 devienne un vecteur nul, $m = 2, \ldots, n$. Pour ce faire, on fait $d_j + c_2 + c_3 + \ldots + c_n$, où c_i est la i^e colonne de F_3.

Finalement on veut que les n premiers éléments de la première colonne de F_5 soient tous 0 ; il suffit de faire $c_1 - c_2 - \ldots - c_n$. On obtient la matrice F_6 d'ordre $n^2 - n + 1$ $(s + t \geq n^2 - n + 2)$ suivante

$$F_6 \quad = \quad \left[\begin{array}{ccccc} \boxed{0} & \boxed{B_1} & \boxed{0 \mid C'_2} & \ldots & \boxed{0 \mid C'_n} \\ \begin{array}{c} -a_{21} \\ \boxed{0} \end{array} & \boxed{0} & \boxed{D'_2} & & \boxed{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \begin{array}{c} -a_{n1} \\ \boxed{0} \end{array} & \boxed{0} & \boxed{0} & & \boxed{D'_n} \end{array}\right],$$

où C'_m est la matrice obtenue de C_m en enlevant la première colonne.

Étape 5. On veut que toute matrice C'_m contienne uniquement des 0. À toute colonne non nulle q de C'_m, dénotée $(C'_m)^q$ correspond la colonne $d_q = {}^t((C'_m)^q, *, \ldots, *)$ de

F_6. Par construction de C_m (donc de C'_m), il existe une colonne b_q de F_6 telle que $b_q = {}^t((C'_m)^q, 0, \ldots, 0)$. Ainsi pour tout q, on fait $d_q - b_q$. On obtient la matrice F_7 d'ordre $n^2 - n + 1$ $(s + t \geq n^2 - n + 2)$.

$$F_7 = \left[\begin{array}{ccccc} 0 & B_1 & 0 & \cdots & 0 \\ \begin{array}{c} -a_{21} \\ 0 \end{array} & 0 & D'_2 & & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \begin{array}{c} -a_{n1} \\ 0 \end{array} & 0 & 0 & & D'_n \end{array}\right],$$

Étape 6. Permutons la première et la n^e colonne de F_7, on obtient la matrice F_8 d'ordre $n^2 - n + 1$ $(s + t \geq n^2 - n + 2)$.

$$F_8 = \left[\begin{array}{cccccc} B_1^n & B'_1 & & & 0 & \\ 0 & 0 & \begin{array}{c} -a_{21} \\ 0 \end{array} & D'_2 & & 0 \\ \vdots & \vdots & & \vdots & \ddots & \vdots \\ 0 & 0 & \begin{array}{c} -a_{n1} \\ 0 \end{array} & 0 & & D'_n \end{array}\right],$$

où B'_1 est le bloc obtenu de B_1 en enlevant la première colonne. On trouve une sous-matrice de 0 située dans le coin supérieur droit de dimensions $n \times (n-1)^2 + 1$ telles que

$$n + (n-1)^2 + 1 = n^2 - n + 2 \geq n^2 - n + 1 = \dim(F_8).$$

Il s'ensuit que F est une matrice creuse. Du Corollaire 6.6, $R = \lambda E^{-1}\gamma = \sum_{k=1}^{n} P_k^{-1} a_{k1} - P_1^{-1} = 0$. Ce qui démontre l'équation (6.2), d'où (iv).

Démontrons (v). Posons

$$R' = 1 - \sum_{k=1}^{n} P_k^{-1},$$

on va montrer

$$R' + \sum_{k=1}^{n} P_k^{-1} = 1.$$

On remplace la première colonne de la matrice E par le vecteur

$${}^t(1, 1, 0, \ldots, 0, 1, 0, \ldots, 0, \ldots, 1, 0, \ldots, 0)$$

et le premier élément de λ par 1. Dénotons E' et λ' ces deux matrices. Considérons la matrice $F' = \begin{bmatrix} E' & \gamma \\ \lambda' & 0 \end{bmatrix}$, on refait les étapes 1 à 6 à l'exception de la dernière de l'étape 4, concernant la 1^{re} colonne. On montre de la même façon que la matrice F' est creuse. Par conséquent, du Corollaire 6.7, $R' = 0$. Ce qui démontre l'équation (6.3).

$\square$

L'exemple suivant illustre la démonstration de l'élément (iv) du Théorème 6.12 pour une matrice générique stochastique d'ordre 3.

Exemple 6.14. Soit $M = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$ une matrice générique non commutative dont les variables sont soumises aux relations stochastiques $a_{i1}+a_{i2}+a_{i3} = 1$, $i = 1, 2, 3$. On lui associe l'automate

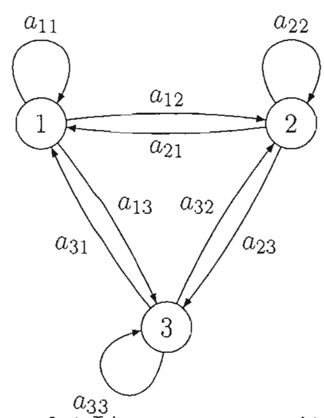


Figure 6.1 L'automate associé à M.

P_1 est le langage reconnu par l'automate

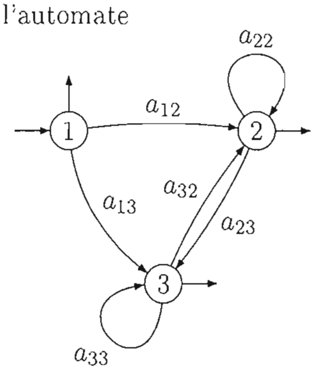


Figure 6.2 L'automate reconnaissant le langage P_1.

Soit L_{ij} l'ensemble des mots allant de i vers j, on a $P_1 = L_{11} + L_{12} + L_{13}$, où

$$\begin{aligned} L_{11} &= 1, \\ L_{12} &= a_{12} + L_{12}\,a_{22} + L_{13}\,a_{32}, \\ L_{13} &= a_{13} + L_{12}\,a_{23} + L_{13}\,a_{33}. \end{aligned}$$

On a le système

$$(S_1) : \begin{cases} P_1 & = 1 + L_{12} + L_{13}, \\ L_{12} & = a_{12} + L_{12}\,a_{22} + L_{13}\,a_{32}, \\ L_{13} & = a_{13} + L_{12}\,a_{23} + L_{13}\,a_{33}. \end{cases}$$

En multipliant à gauche chaque équation de S_1 par P_1^{-1}, on obtient le système

$$(T_1) : \begin{cases} 1 & = P_1^{-1} + P_1^{-1}L_{12} + P_1^{-1}L_{13}, \\ P_1^{-1}L_{12} & = P_1^{-1}\,a_{12} + P_1^{-1}L_{12}\,a_{22} + P_1^{-1}L_{13}\,a_{32}, \\ P_1^{-1}L_{13} & = P_1^{-1}\,a_{13} + P_1^{-1}L_{12}\,a_{23} + P_1^{-1}L_{13}\,a_{33}. \end{cases}$$

Posons $Q_{ij} = P_1^{-1}L_{ij}$, le système devient

$$T_1 : \begin{cases} 1 & = P_1^{-1} + Q_{12} + Q_{13}, \\ Q_{12} & = P_1^{-1}\,a_{12} + Q_{12}\,a_{22} + Q_{13}\,a_{32}, \\ Q_{13} & = P_1^{-1}\,a_{13} + Q_{12}\,a_{23} + Q_{13}\,a_{33}. \end{cases}$$

On réécrit ce système sous la forme

$$(U_1) : \begin{cases} 1 & = P_1^{-1} + Q_{12} + Q_{13}, \\ 0 & = P_1^{-1}\, a_{12} + Q_{12}\,(a_{22} - 1) + Q_{13}\, a_{32}, \\ 0 & = P_1^{-1}\, a_{13} + Q_{12}\, a_{23} + Q_{13}\,(a_{33} - 1). \end{cases}$$

En permutant les indices des équations de U_1 on obtient les systèmes

$$(U_2) \quad : \quad \begin{cases} 1 & = P_2^{-1} + Q_{21} + Q_{23}, \\ 0 & = P_2^{-1}\, a_{21} + Q_{21}\,(a_{11} - 1) + Q_{23}\, a_{31}, \\ 0 & = P_2^{-1}\, a_{23} + Q_{21}\, a_{13} + Q_{23}\,(a_{33} - 1), \end{cases}$$

$$(U_3) \quad : \quad \begin{cases} 1 & = P_3^{-1} + Q_{31} + Q_{32}, \\ 0 & = P_3^{-1}\, a_{31} + Q_{31}\,(a_{11} - 1) + Q_{32}\, a_{21}, \\ 0 & = P_3^{-1}\, a_{32} + Q_{31}\, a_{12} + Q_{32}\,(a_{22} - 1). \end{cases}$$

Pour montrer que $(P_1^{-1},\, P_2^{-1},\, P_3^{-1})\, M \;=\; (P_1^{-1},\, P_2^{-1},\, P_3^{-1})$, il suffit de montrer que $P_1^{-1}a_{11} + P_2^{-1}a_{21} + P_3^{-1}a_{31} = P_1^{-1}$. Posons

$$R = P_1^{-1}a_{11} + P_2^{-1}a_{21} + P_3^{-1}a_{31} - P_1^{-1},$$

alors

$$R + P_1^{-1}(1 - a_{11}) - P_2^{-1}a_{21} - P_3^{-1}a_{31} = 0.$$

Réécrivons le système constitué de la dernière équation et des systèmes (U_1), (U_2) et (U_3) sous la forme matricielle. On a

$$(R, P_1 - 1,\, Q_{12}, Q_{13}, P_2^{-1}, Q_{21}, Q_{23}, P_3^{-1}, Q_{31},\, Q_{32})\, E = \lambda$$

où

$$\lambda = (0,\, 0,\, 0,\, 0,\, 0,\, 0,\, 0,\, 1,\, 1,\, 1),$$

et

$$E = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1-a_{11} & a_{12} & a_{13} & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & a_{22}-1 & a_{23} & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & a_{32} & a_{33}-1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ -a_{21} & 0 & 0 & a_{21} & a_{23} & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & a_{11}-1 & a_{13} & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & a_{31} & a_{33}-1 & 0 & 0 & 0 & 1 & 0 \\ -a_{31} & 0 & 0 & 0 & 0 & a_{31} & a_{32} & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & a_{11}-1 & a_{12} & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & a_{21} & a_{22}-1 & 0 & 0 & 1 \end{bmatrix}.$$

On a $R = \lambda E^{-1}\gamma$, où $\gamma = {}^t(1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$ et que E est congrue (modulo les relations stochastiques) à

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ a_{12}+a_{13} & a_{12} & a_{13} & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & -a_{21}-a_{23} & a_{23} & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & a_{32} & -a_{31}-a_{32} & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ -a_{21} & 0 & 0 & a_{21} & a_{23} & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -a_{12}-a_{13} & a_{13} & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & a_{31} & -a_{31}-a_{32} & 0 & 0 & 0 & 1 & 0 \\ -a_{31} & 0 & 0 & 0 & 0 & a_{31} & a_{32} & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & -a_{12}-a_{13} & a_{12} & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & a_{21} & -a_{21}-a_{23} & 0 & 0 & 1 \end{bmatrix}.$$

Soit $F = \begin{bmatrix} E & \gamma \\ \lambda & 0 \end{bmatrix}$, on va montrer que F est creuse.

$$F = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ a_{12}+a_{13} & a_{12} & a_{13} & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -a_{21}-a_{23} & a_{23} & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & a_{32} & -a_{31}-a_{32} & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ -a_{21} & 0 & 0 & a_{21} & a_{23} & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -a_{12}-a_{13} & a_{13} & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & a_{31} & -a_{31}-a_{32} & 0 & 0 & 0 & 1 & 0 & 0 \\ -a_{31} & 0 & 0 & 0 & 0 & a_{31} & a_{32} & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -a_{12}-a_{13} & a_{12} & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & a_{21} & -a_{21}-a_{23} & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$$F_1 = \begin{bmatrix} a_{12}+a_{13} & a_{12} & a_{13} & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & -a_{21}-a_{23} & a_{23} & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & a_{32} & -a_{31}-a_{32} & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ -a_{21} & 0 & 0 & a_{21} & a_{23} & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -a_{12}-a_{13} & a_{13} & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & a_{31} & -a_{31}-a_{32} & 0 & 0 & 0 & 1 & 0 \\ -a_{31} & 0 & 0 & 0 & 0 & a_{31} & a_{32} & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & -a_{12}-a_{13} & a_{12} & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & a_{21} & -a_{21}-a_{23} & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$L_1 + L_5 + L_8 - L_{10}, \qquad L_2 + L_4 + L_9 - L_{10}, \qquad L_3 + L_6 + L_7 - L_{10},$$

$$F_2 = \begin{bmatrix} a_{12}+a_{13} & a_{12} & a_{13} & -a_{12}-a_{13} & a_{13} & -a_{12}-a_{13} & a_{12} & 0 & 0 & 0 \\ 0 & -a_{21}-a_{23} & a_{23} & a_{21} & a_{23} & a_{21} & -a_{21}-a_{23} & 0 & 0 & 0 \\ 0 & a_{32} & -a_{31}-a_{32} & a_{31} & -a_{31}-a_{32} & a_{31} & a_{32} & 0 & 0 & 0 \\ -a_{21} & 0 & 0 & a_{21} & a_{23} & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -a_{12}-a_{13} & a_{13} & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & a_{31} & -a_{31}-a_{32} & 0 & 0 & 0 & 1 & 0 \\ -a_{31} & 0 & 0 & 0 & 0 & a_{31} & a_{32} & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & -a_{12}-a_{13} & a_{12} & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & a_{21} & -a_{21}-a_{23} & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$F_3 = \begin{bmatrix} a_{12}+a_{13} & a_{12} & a_{13} & -a_{12}-a_{13} & a_{13} & -a_{12}-a_{13} & a_{12} & 0 & 0 \\ 0 & -a_{21}-a_{23} & a_{23} & a_{21} & a_{23} & a_{21} & -a_{21}-a_{23} & 0 & 0 \\ 0 & a_{32} & -a_{31}-a_{32} & a_{31} & -a_{31}-a_{32} & a_{31} & a_{32} & 0 & 0 \\ -a_{21} & 0 & 0 & a_{21} & a_{23} & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -a_{12}-a_{13} & a_{13} & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & a_{31} & -a_{31}-a_{32} & 0 & 0 & 1 & 0 \\ -a_{31} & 0 & 0 & 0 & 0 & a_{31} & a_{32} & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & -a_{12}-a_{13} & a_{12} & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & a_{21} & -a_{21}-a_{23} & 0 & 1 \end{bmatrix}$$

$$L_4 - L_6, \quad L_5 - L_6, \quad L_7 - L_9, \quad L_8 - L_9,$$

$$F_4 = \begin{bmatrix} a_{12}+a_{13} & a_{12} & a_{13} & -a_{12}-a_{13} & a_{13} & -a_{12}-a_{13} & a_{12} & 0 & 0 \\ 0 & -a_{21}-a_{23} & a_{23} & a_{21} & a_{23} & a_{21} & -a_{21}-a_{23} & 0 & 0 \\ 0 & a_{32} & -a_{31}-a_{32} & a_{31} & -a_{31}-a_{32} & a_{31} & a_{32} & 0 & 0 \\ -a_{21} & 0 & 0 & a_{21}-a_{31} & a_{23}+a_{31}+a_{32} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -a_{12}-a_{13}-a_{31} & a_{13}+a_{31}+a_{32} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a_{31} & -a_{31}-a_{32} & 0 & 0 & 1 & 0 \\ -a_{31} & 0 & 0 & 0 & 0 & a_{31}-a_{21} & a_{32}+a_{21}+a_{23} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -a_{12}-a_{13}-a_{21} & a_{12}+a_{21}+a_{23} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & a_{21} & -a_{21}-a_{23} & 0 & 1 \end{bmatrix}$$

$$F_5 = \begin{bmatrix} a_{12}+a_{13} & a_{12} & a_{13} & -a_{12}-a_{13} & a_{13} & -a_{12}-a_{13} & a_{12} \\ 0 & -a_{21}-a_{23} & a_{23} & a_{21} & a_{23} & a_{21} & -a_{21}-a_{23} \\ 0 & a_{32} & -a_{31}-a_{32} & a_{31} & -a_{31}-a_{32} & a_{31} & a_{32} \\ -a_{21} & 0 & 0 & a_{21}-a_{31} & a_{23}+a_{31}+a_{32} & 0 & 0 \\ 0 & 0 & 0 & -a_{12}-a_{13}-a_{31} & a_{13}+a_{31}+a_{32} & 0 & 0 \\ -a_{31} & 0 & 0 & 0 & 0 & a_{31}-a_{21} & a_{32}+a_{21}+a_{23} \\ 0 & 0 & 0 & 0 & 0 & -a_{12}-a_{13}-a_{21} & a_{12}+a_{21}+a_{23} \end{bmatrix}$$

$$C_1 - C_2 - C_3, \quad C_4 + C_2 + C_3, \quad C_6 + C_2 + C_3,$$

$$F_6 = \begin{bmatrix} 0 & a_{12} & a_{13} & 0 & a_{13} & 0 & a_{12} \\ 0 & -a_{21} - a_{23} & a_{23} & 0 & a_{23} & 0 & -a_{21} - a_{23} \\ 0 & a_{32} & -a_{31} - a_{32} & 0 & -a_{31} - a_{32} & 0 & a_{32} \\ -a_{21} & 0 & 0 & a_{21} - a_{31} & a_{23} + a_{31} + a_{32} & 0 & 0 \\ 0 & 0 & 0 & -a_{12} - a_{13} - a_{31} & a_{13} + a_{31} + a_{32} & 0 & 0 \\ -a_{31} & 0 & 0 & 0 & 0 & a_{31} - a_{21} & a_{32} + a_{21} + a_{23} \\ 0 & 0 & 0 & 0 & 0 & -a_{12} - a_{13} - a_{21} & a_{12} + a_{21} + a_{23} \end{bmatrix}$$

$$C_5 - C_3, \quad C_7 - C_2,$$

$$F_7 = \begin{bmatrix} 0 & a_{12} & a_{13} & 0 & 0 & 0 & 0 \\ 0 & -a_{21} - a_{23} & a_{23} & 0 & 0 & 0 & 0 \\ 0 & a_{32} & -a_{31} - a_{32} & 0 & 0 & 0 & 0 \\ -a_{21} & 0 & 0 & a_{21} - a_{31} & a_{23} + a_{31} + a_{32} & 0 & 0 \\ 0 & 0 & 0 & -a_{12} - a_{13} - a_{31} & a_{13} + a_{31} + a_{32} & 0 & 0 \\ -a_{31} & 0 & 0 & 0 & 0 & a_{31} - a_{21} & a_{32} + a_{21} + a_{23} \\ 0 & 0 & 0 & 0 & 0 & -a_{12} - a_{13} - a_{21} & a_{12} + a_{21} + a_{23} \end{bmatrix}$$

$$C_1 \leftrightarrow C_3$$

$$F_8 = \begin{bmatrix} a_{13} & a_{12} & 0 & 0 & 0 & 0 & 0 \\ a_{23} & -a_{21} - a_{23} & 0 & 0 & 0 & 0 & 0 \\ -a_{31} - a_{32} & a_{32} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -a_{21} & a_{21} - a_{31} & a_{23} + a_{31} + a_{32} & 0 & 0 \\ 0 & 0 & 0 & -a_{12} - a_{13} - a_{31} & a_{13} + a_{31} + a_{32} & 0 & 0 \\ 0 & 0 & -a_{31} & 0 & 0 & a_{31} - a_{21} & a_{32} + a_{21} + a_{23} \\ 0 & 0 & 0 & 0 & 0 & -a_{12} - a_{13} - a_{21} & a_{12} + a_{21} + a_{23} \end{bmatrix}$$

On a un bloc de zéros de dimensions 3×5 et $8 > 7$. Il s'ensuit que F est une matrice creuse. Du Corollaire 6.6, $R = P_1^{-1}a_{11} + P_2^{-1}a_{21} + P_3^{-1}a_{31} - P_1^{-1} = 0$.

CONCLUSION

Dans ce travail, nous avons étudié dans un premier temps différentes classes de séries rationnelles à coefficients non négatifs.

La première classe des séries rationnelles est l'ensemble des séries de la forme $(\det(1 - xM))^{-1}$, où M est une série à coefficients entiers non négatifs. Ce sont les séries génératrices des monoïdes partiellement commutatifs libres. Il s'ensuit que ces séries sont $\mathbb{N}$-rationnelles. On a montré que l'ensemble de ces séries coïncide avec l'ensemble des polynômes de cliques de graphes pondérés (Thm 2.4). L'inclusion d'un sens était déjà connu ; en effet, il suffit d'utiliser la théorie des monoïdes partiellement commutatifs libres où il est démontré que $\det(1 - xM)$ est égal au polynôme de cliques pondéré du graphe des circuits. Cette transformation n'étant pas surjective, on ne pouvait pas inverser le processus. La preuve de l'inclusion inverse était entièrement basée sur un résultat de (Kim, Ormes et Roush, 2000), établissant les conditions nécessaires et suffisantes afin qu'un ensemble de nombres complexes soit le spectre d'une matrice à coefficients entiers non négatifs. Ce résultat avait été conjecturé par Boyle et Handelman ((Boyle et Handelman, 1991)).

La seconde classe sont les séries de la forme $(\det(1-xM))^{-1}$, où M est une série à coefficients réel non négatifs. On a montré que l'ensemble de ces séries coïncide avec l'ensemble des l'ensemble des polynômes de cliques généralisés (Thm 3.3). Par construction, ces séries sont $\mathbb{R}_+$-rationnelles. Le polynôme de clique généralisé est une généralisation du polynôme de cliques étant donné que l'on pondère chaque sommet du graphe par un monôme de la forme αx^d, où α est un réel positif et d, un entier non négatif. La démonstration de ce théorème est exactement la même que celle du Théorème 2.4 à la différence qu'on utilise le théorème de Boyle et Handelman (Boyle et Handelman, 1991) au lieu de Kim, Ormes et Roush pour démontrer l'inclusion inverse. Ceux-ci ont toutefois établi les conditions nécessaires et suffisantes afin qu'un ensemble de nombres complexes soit le spectre d'une matrice à coefficients réels non négatifs.

Les troisième et quatrième classes des séries rationnelles étudiées sont les ensembles des séries de la forme $(1 - ax + bx^k)^{-1}$, où $a \in \mathbb{N}$, $b \in \mathbb{Z}$, $k \geq 2$ et de la forme $(1 - ax + bx^2 + cx^3)^{-1}$, où $a \in \mathbb{N}$ et b, $c \in \mathbb{Z}$. On a caractérisé ces deux ensembles de séries en établissant les conditions nécessaires et suffisantes nous permettant de décider de la $\mathbb{N}$-rationalité.

La cinquième classe des séries rationnelles est l'ensemble des fonctions zêta associées à des automates. En effet, soit $\mathcal{A}$ un automate, on définit sa fonction zêta la série $\exp\left\{\sum_{n=1}^{\infty} a_n \frac{z^n}{n}\right\}$, où a_n est le nombre de chemins bi-infinis dans $\mathcal{A}$ dont la période est n. On montre qu'une telle série est $\mathbb{N}$-rationnelle (Prop. 5.8). Par la suite on définit plusieurs propriétés de cette série concernant l'apériodicité et la divergence. Étant donné que le langage reconnu par un automate non ambigu est un code (Thm 5.24), on a défini la fonction zêta d'un code. On a montré que cette série est $\mathbb{N}$-rationnelle (Cor 5.29). On a démontré plusieurs propriétés de cette série lorsque X est un code complet, un code pur, un code circulaire ou un code bifixe. Finalement, on a montré que $\zeta(\mathcal{A})$ est une spécialisation de la fonction zêta Z_ϕ d'un morphisme de systèmes dynamiques définie dans (Boyle, 1989).

La seconde partie portait sur les matrices stochastiques : la somme des éléments de chaque ligne vaut 1. Il est connu dans la littérature que toute matrice stochastique a 1 comme valeur propre dont le vecteur propre à droite associé à 1 est ${}^t(1, \ldots, 1)$. On s'est s'intéressé au vecteur propre à gauche associé à 1. Soit M une telle matrice. Dans le cas commutatif, on a montré que ce vecteur est composé des mineurs principaux de $M - I_n$ (Prop 6.7). La preuve est purement algébrique.

Dans le cas non commutatif, on a montré que les éléments du vecteur propre à gauche sont les inverses des dérivations des codes reconnus par l'automate dont M est la matrice de cet automate. On dit que M est une matrice générique non commutative stochastique ;

i.e. ses éléments sont des variables non commutatives telles que la somme de chaque ligne vaut 1. La démonstration nécessite des résultats provenant de la théorie des corps libres (au sens de Cohn). En effet, on a plongé chaque expression rationnelle dans un corps libre, on a prouvé que cette évaluation est bien définie dans ce corps libre. Soit μ ce vecteur propre à gauche, l'équation $\mu M = \mu$ est vue comme un système d'équations où chacune d'entre elles a une représentation linéaire $\lambda E^{-1}\gamma$, où E est une certaine matrice générique non commutative stochastique et λ et γ sont des vecteurs ligne et colonne respectivement. On a démontré que la matrice $F = \begin{bmatrix} F & \gamma \\ \lambda & 0 \end{bmatrix}$ est une matrice creuse, elle est donc non pleine. Ce qui implique qu'elle n'est pas inversible dans le corps libre. Il s'ensuit que $\mu M - \mu = 0$ dans le corps libre.

ANNEXE A

NOTATIONS

1 : mot vide ou matrice identité,

a : lettre,

$[a]$: classe d'équivalence de a dans le monoïde $A^*/\sim_C$,

A : alphabet fini,

A^* : ensemble des mots finis,

$\mathcal{A} = (Q, I, T)$: automate,

$|\mathcal{A}| = \sum_{w \in A^*} (|\mathcal{A}|, w)\, w$, où $(|\mathcal{A}|, w)$ est le nombre de chemins $i \to t$ étiquetés w, $i \in I$ et $t \in T$,

α_n : nombre de mots de L de longueur n,

$A^*/\sim_C$: monoïde libre partiellement commutatif gradué,

b : lettre,

B : sous-ensemble commutatif de $A^*/\sim_C$,

c : circuit,

$|c|$: longueur du circuit c,

C : graphe simple non orienté,

$\overline{C}$: graphe complémentaire de C,

$\mathbb{C}$: ensemble des nombres complexes,

D : graphe orienté,

D_1 : sous-graphe de D,

$\mathcal{D}$: corps gauche,

d_s : degré du sommet s,

deg : degré d'un ensemble,

$disc(p(x))$: discriminant de $p(x)$,

$|E|$: cardinalité de l'ensemble E,

e_i : i^e fonction symétrique élémentaire,

$\mathcal{F}$: corps libre,

$F(x) = \sum_{n=1}^{\infty} f_n x^n$: série,

$Fix(w)$: ensemble des points fixes par w,

$\mathbb{K}$: demi-anneau,

$\mathbb{K}[x]$: ensemble des polynômes en la variable x à coefficients dans $\mathbb{K}$,

$\mathbb{K}[[x]]$: ensemble des séries en la variable x à coefficients dans $\mathbb{K}$,

$\mathbb{K}\langle A\rangle$: ensemble des polynômes non commutatifs en les variables de A à coefficients dans $\mathbb{K}$,

$\mathbb{K}\langle\langle A\rangle\rangle$: ensemble des séries non commutatives en les variables de A à coefficients dans $\mathbb{K}$,

λ : valeur propre,

$\lambda(w) = |w|w$: dérivation de w,

L : langage,

$\underline{L}$: série caractéristique du langage L,

l_i : élément de Lyndon,

L_i : i^e ligne d'une matrice,

m : mot,

$|m|$: longueur d'un mot

M : matrice,

μ : fonction de Möbius,

N : matrice,

p : état,

P_C : polynôme de cliques du graphe pondéré C,

$PG_C(x)$: polynôme de cliques généralisé de C,

$\phi(n)$: fonction d'Euler,

$\Phi_n(x)$: n^e polynôme cyclotomique,

p_n : n^e fonction symétrique somme de puissances,

ψ : spécialisation $a \mapsto \alpha_s\, x^{d_a}$,

q : état,

Q : ensemble des états d'un automate,

$\mathbb{Q}$: ensemble des nombres rationnels,

$\mathbb{R}$: ensemble des nombres réels,

$\mathbb{R}_+$: ensemble des nombres réels positifs,

$rgst(w)$: rang stable de w,

ρ : module maximum des racines,

s : sommet,

S : corps libre stochastique,

$S(p, q)$: matrice de Sylvester de p et q,

$S_{\mathcal{A}} = \sum_{w \in A^*} (S_{\mathcal{A}}, w)\, w$, où $(S_{\mathcal{A}}, w) =$ le nombre de chemins bi-infinis étiquetés ${}^{\infty}w^{\infty}$ dans $\mathcal{A}$,

$Supp(S)$: support de la série S,

$S_X = \sum_{w \in A^*} (S_X, w) w$: (S_X, w) est le nombre de X-factorisations de ${}^{\infty}w^{\infty}$,

$T_{\mathcal{A}} = \sum_{w \in A^*} rgst(w)\, w$,

$tr = |Fix(w)|$,

$tr(\mathcal{A}) = \sum_{w \in A^*} tr(w)\, w$,

$tr^n(\lambda_1, \ldots, \lambda_k) = \sum_{i=1}^{k} \lambda_i^n$,

$tr_n(\lambda_1, \ldots, \lambda_k) = \sum_{d\,|\,n}^{k} \mu\left(\frac{n}{d}\right) tr^n$,

u : mot,

v : mot,

$\varphi_{\mathcal{A}}(w)_{p,q}$: nombre de chemins de p vers q dans $\mathcal{A}$ étiquetés w,

w : mot,

${}^{\infty}w^{\infty}$: mot bi-infini $\ldots ww.www \ldots$, où le point désigne la position du 0,

x : élément de X,

X : code,

X^* : sous-monoïde libre de A^* engendré par X,

$X^+ = X^* \setminus \{1\}$,

$\zeta(\mathcal{A})$: fonction zêta de l'automate $\mathcal{A}$,

$Z(S)$: fonction zêta généralisée de la série non commutative S.

RÉFÉRENCES

Aldous, D.-J. 1990. « The randow walk construction of uniform spanning trees and uniform labelled trees », *SIAM J. Discrete Maths*, vol. 3, p. 450–465.

Amitsur, A. 1966. « Rational identities and applications to algebra and geometry », *J. Algebra*, vol. 3, p. 304–359.

Anantharam, V. et P. Tsoucas. 1989. « A proof of the Markov chain tree theorem », *Statistic and probability letters*, vol. 8, p. 189–192.

Béal, M.-P. 1993. *Codage symbolique.* Masson.

Béal, M.-P. et D. Perrin. 1997. *Symbolic Dynamics and finite automata, in Handbook of formal languages, G. Rozenberg, A. Salomaa eds.* T. 2. Springler Verlag.

Barcucci, E., A. D. Lungo, A. Frosini, et S. Rinaldi. 2001. « A technology for reverse-engineering a combinatorial problem from a rational generating function », *Advances in Applied Mathematics*, vol. 26, p. 129–153.

Bergman, G. 1970. « Skew field of noncommutative rational functions, after Amitsur. séminaire schützenberger-lentin-nivat », vol. 16.

Berstel, J. 1971. « Sur les pôles et le quotient de Hadamard de séries $\mathbb{N}$-rationnelles. », *R. Acad. Sci. Paris Sér. A-B*, vol. 272, p. A1079–A1081.

Berstel, J. et D. Perrin. 1984. *Theory of Codes.* Pure and Applied Mathematics. Academic Press.

Berstel, J. et C. Reutenauer. 1984. *Les séries rationnelles et leurs langages.* Masson.

———. 2008a. « Another proof of Soittola's theorem », *TCS*, vol. 393, p. 196–203.

———. 2008b. *Rational Series and Their Languages, http ://www-igm.univ-mlv.fr/~berstel/LivreSeries/LivreSeries08janvier2008.pdf.*

———. october 1990. « Zeta functions of formal languages », *Transactions of the American Mathematical Society*, vol. 321, no. 2, p. 533–546.

Bollobas, B. 1998. *Modern Graph theory.* T. 184. Graduate Texts in Mathematics, Springer.

Boyle, M. 1989. « A zeta function for homomorphisms of dynamical systems », *Journal of the London mathematical Society*, vol. 40, p. 355–368.

———. 1993. « Symbolic dynamics and matrices », *Institute for Mathematics and Its Applications*, vol. 50, p. 1–38.

———. 2005. *Notes on the Perron-Frobenius theory of nonnegative matrix, http ://www.math.umd.edu/~mmb/475/spec.pdf.*

Boyle, M. et D. Handelman. 1991. « The spectra of nonnegative matrices via symbolic dynamics », *The Annals of Mathematics*, vol. 133, no. 2, p. 249–316.

Broder, A. 1989. « Generating random spanning trees », *Proc 30th IEEE Symp. On Found. of Computer Science*, p. 442–447.

Cartier, P. et D. Foata. 1969. « Problèmes combinatoires de commutations et de réarrangement, lecture notes in maths », *Springler-Verlag*, vol. 85.

Cohn, P. 1971. *Free Rings and Their Relations*. Academic Press.

———. 1995. *Skew fields : theory of general division rings*. T. 57. Encyclopedia of Mathematics and its applications, Cambridge University Press.

———. 2005. *Free ideal rings and localization in general rings*. Cambridge.

Coste, M. 2001. *Élimination, Résultant et Discriminant, http ://www.dynamaths.com/docs/lecons/ developpement_algebre_374.pdf.*

Eilenberg, S. 1974. *Automata, languages and machines*. T. A. Academic Press.

Fisher, D. 1989. « The number of words of length n in a free semi-abelian monoid », *Amer. Math. Monthly*, vol. 96, p. 610–614.

Gessel, I. 2003. « Rational functions with nonnegative power series », *50th Seminaire Lotharingien de Combinatoire, page Domaine Saint-Jacques, available at http ://people.brandeis.edu/~gessel/homepage/papers/nonneg.pdf.*

Goldwurm, M. et M. Santini. 2000. « Clique polynomials have a unique root of smallest modulus », *Information Proceeding letters*, vol. 75, p. 127–132.

Goldwurm, M. et M. Saporiti. 1998. « Clique polynomials and trace monoids », *Rapporto Interno*, vol. 222-98, p. 1–12.

Hajialbolhassan, H. et M. Mehrabadi. 1998. « On clique polynomials », *Australian Journal of combinatorics*, vol. 18, p. 313–316.

Katayama, T., O., et H. Enomoto. 1978. « Characterization of the structure-generating functions of regular sets and the dol growth functions », *Inform. Control*, vol. 6, p. 85–101.

Kim, K., N. Ormes, et F. Roush. 2000. « The spectra of nonnegative integer matrices via formal power series », *AMS*, vol. 13, no. 4, p. 773–806.

Kleene, S. 1956. « Representation of events in nerve nets and finite automata », *Shannon, C. E., McCarthy, J., editors, Automata Studies, Annals of mathematics studies, Princeton University Press, Princeton, N. J.*, vol. 34, p. 3–41.

Koutschan, C. 2005. *Regular Langages and their generating functions : the inverse problem.* Diplomarbeit informatik, Friedrich-Alexander-Universität Erlangen-Nürnberg.

———. 2008. « Regular languages and their generating functions : The inverse problem », *Theoretical Computer Science*, vol. 391, no. 1-2, p. 65–74.

Krattenthaler, C. 2006. « The theory of heaps and the cartier foata monoid », *Appendix of Commutation and Rearrangements*, p. 63–73.

Lalonde, P. 1995. « Lyndon heaps : An analogue of Lyndon words in free partially commutative monoids », *Discrete Maths*, vol. 145, p. 171–189.

Lang, S. 2002. *Algebra, 3rd Ed.* T. 211. Graduate Texts in Mathematics, Springer-Verlag.

Lavallée, S., D. Perrin, C. Reutenauer, et V. Retakh. 2008. « Codes and noncommutative stochastic matrices », *À paraître.*

Leighton, F. et R. Rivest. 1983. « The markov chain tree theorem », *Technical report MIT/LCS/TM-249, MIT.*

Levit, V. et E. Mandrescu. 2005. « The independence polynomial of a graph - a survey », *Holon Academic Institute of Technology*, p. 1–22.

Macdonald, I. 1995. *Symmetric functions and Hall polynomials.* Oxford Mathematical Monographs, second edn, The Clarendon Press Oxford University Press, New York.

Malcolmson, P. 1978. « A prime matrix ideal yields a skew field », *J. London Math Soc*, vol. 18, p. 221–233.

Manning, A. 1971. « Axiom a diffeomorphisms have rational zeta function », *Bull. London Math Soc*, vol. 3, p. 215–220.

Marcus, B., R. Roth, et P. Siegel. 2001. *An Introduction to Coding for Constrained Systems, http ://vivaldi.ucsd.edu :8080/~psiegel/Book/Book_pdf/chapter3.pdf.*

Perrin, D. 1976. « The characteristic polynomial of a finite automaton », *In A. Mazurkevitch, editor, Proceedings of MFCS 76, Lecture Notes in Computer Science*, vol. 45, p. 453–457.

———. 1992. « On positive matrices », *Theoret. Comput. Sci*, vol. 94, no. 2, p. 357–366.

Restivo, A. 1973. « Codes and aperiodic languages », *Lecture Notes in Computer Science*, vol. 2, p. 175–181.

Reutenauer, C. 1997. « N-rationality of zeta functions », *Advances in Applied Mathematics*, vol. 18, p. 1–17.

Rinaldi, S. 1999. « e-mail à christophe reutenauer ».

Salomaa, A. et M. Soittola. 1978. *Automata-Theoretic Aspects of Formal Power Series*. Springer-Verlag.

Schützenberger, M. 1961. « On the definition of a family of automata », *Information and control*, vol. 4, p. 245–270.

Soittola, M. 1976. « Positive rational sequences. », *Theoret. Comput. Sci*, vol. 2, no. 3, p. 317–322.

Stanley, R. 1986. *Enumerative Combinatorics*. Wadsworth and Brooks/Cole.

Viennot, X. 1986. « Heaps of pieces. 1. basic definitions and combinatorial lemmas, lecture notes in maths », *Springler-Verlag*, vol. 1234, p. 321–350.

Vincent, M. 1985. « Construction de codes indécomposables », *RAIRO Informatique Théorique/Therical Informatics*, vol. 19, p. 165–178.

Index