Université de Marne-La-Vallée

Thèse de Doctorat

Spécialité : Informatique Fondamentale

présentée par

Frédérique Bassino

pour l'obtention du titre de

Docteur de l'Université de Marne-La-Vallée

sur le sujet

Séries rationnelles et distributions de longueurs

Soutenue le 22 Novembre 1996 devant le jury composé de :

Jean-Paul Allouche
Jean Berstel
Véronique Bruyère
Michel Fliess
Dominique Perrin

Remerciements

Je tiens à remercier

- Dominique Perrin, qui a dirigé cette thèse, pour ses encouragements, son enthousiasme, enfin pour tout ce qu'il m'a appris.
- Véronique Bruyère pour son accueil si chaleureux à Mons, pour ses remarques pertinentes, ses conseils et pour le temps et le soin qu'elle a mis à s'acquitter de son lourd travail de rapporteur,
- Jean Berstel d'avoir accepté la tâche longue et délicate de rapporteur,
- Jean-Paul Allouche et Michel Fliess de m'avoir fait l'honneur de participer au jury,
- Maxime Crochemore de m'avoir accueillie durant ces trois années à l'Institut Gaspard Monge,
- Mike Boyle pour l'intérêt qu'il a manifesté pour ce travail, pour son accueil à l'Université du Maryland à College Park, pour les discussions enrichissantes que nous avons eues,
- Doug Lind de m'avoir permis de travailler durant l'été 95 à l'Université de Washington à Seattle,
- Marie-Pierre Béal et Olivier Carton pour leurs conseils,
- Line Fonfrède pour sa gentillesse et son efficacité à régler toutes les questions pratiques,
- Enfin, tous ceux qui contribuent à faire régner la bonne humeur au sein de l'Institut Gaspard Monge.

Résumé

Ce travail porte sur les séries à coefficients entiers positifs, sur les séries $\mathbb{N}$-rationnelles et est centré autour de deux types de questions : le problème de la hauteur d'étoile et l'étude des propriétés des distributions de longueurs des codes.

On étudie le problème de la hauteur d'étoile de séries rationnelles particulières : les séries $\mathbb{N}$-rationnelles en une variable. On caractérise de différentes façons les séries $\mathbb{N}$-rationnelles qui sont de hauteur d'étoile 1, et on donne un critère permettant de décider de la hauteur d'étoile d'une classe importante de séries $\mathbb{N}$-rationnelles en une variable.

L'étude de la hauteur d'étoile des séries $\mathbb{N}$-rationnelles en une variable repose sur l'utilisation des propriétés de leurs représentations par des matrices. On établit, en particulier, à partir d'un résultat d'Handelman, une caractérisation du rayon spectral d'une matrice compagnon irréductible à coefficients entiers positifs.

On étudie, ensuite, les distributions de longueurs des codes circulaires et des codes préfixes. On prouve trois nouveaux résultats concernant les codes circulaires. On généralise, dans plusieurs directions, la caractérisation des distributions de longueurs des codes circulaires établie dans le cas d'un alphabet fini par Schützenberger. D'une part, on remplace l'alphabet fini par un alphabet quelconque dont les éléments ont des poids, ce qui permet d'étendre le résultat à deux distributions de longueurs. D'autre part, on restreint les conditions, ce qui permet d'établir la décidabilité dans le cas d'une distribution finie. On donne une nouvelle formulation de cette caractérisation. Ce résultat, établi par des méthodes combinatoires, met en évidence la décidabilité dans le cas d'une distribution finie. On établit une condition nécessaire et suffisante pour qu'une suite d'entiers positifs soit la distribution de longueur d'un code circulaire maximal sur un alphabet fini.

Enfin, on met en évidence les liens entre les séries génératrices des codes préfixes rationnels et une classe de séries $\mathbb{N}$-rationnelles : les DOL-séries. On donne une condition suffisante pour qu'une suite $\mathbb{N}$-rationnelle soit la distribution de longueurs d'un code rationnel préfixe maximal sur un alphabet à k lettres.

Abstract

This work concerns rational series having nonnegative integral coefficients and is centered on two kinds of questions : the star-height problem and the study of the properties of length distributions of codes.

We study the star-height problem in the case of rational series of a particular kind : $\mathbb{N}$-rational series in one variable. We characterize in various ways $\mathbb{N}$-rational series having star-height 1. We also give a criterion for deciding the star-height of an important class of $\mathbb{N}$-rational series in one variable.

Basically, the study of the star-height of the $\mathbb{N}$-rational series in one variable makes use of the properties of their representations by matrices. We establish in particular, from a result of Handelman, a characterisation of the spectral radius of an irreducible companion matrix having nonnegative integral entries.

Next, we study length distributions of circular codes and of prefix codes. We prove three new results about circular codes. We generalize in several directions the characterization of length distributions of circular codes established, by Schützenberger, in the case of a finite alphabet. On the one hand, we replace the finite alphabet by an arbitrary alphabet whose elements are weighted ; this allows us to extend the result to two length distributions. On the other hand, we restrict the conditions which allows us to establish the decidability in the case of a finite sequence. We give a new formulation of this characterization. This result established by combinatorial methods underscores the decidability in the case of a finite distribution. We establish a necessary and sufficient condition for a sequence of nonnegative integers to be the length distribution of a maximal circular code over a finite alphabet.

Finally, we emphasize the links between the generating series of rational prefix codes and a class of $\mathbb{N}$-rational series : the DOL-series. We give a sufficient condition for an $\mathbb{N}$-rational sequence to be the length distribution of a maximal rational prefix code over a k-letter alphabet.

Table des matières

Introduction

Cette thèse s'inscrit dans le cadre général de la théorie des automates, de la combinatoire et de la dynamique symbolique. Les séries formelles, qui constituent l'objet central de ce travail, se trouvent à la confluence de plusieurs branches des mathématiques et de l'informatique. Les séries en indéterminées non-commutatives furent introduites, en 1961, par M.P. Schützenberger ([Sch61] et [CS63]). Ces séries généralisent simultanément les notions essentielles de séries, en mathématiques, et de langages, en informatique.

Elles interviennent, en particulier, en combinatoire algébrique et en combinatoire énumérative et constituent à ce titre un outil important en combinatoire des graphes ([Cor75]). Elles ont de nombreuses applications : en automatisme, les séries formelles en variables non-commutatives permettent de décrire le comportement des systèmes ([Fli81]) ; l'analyse d'algorithmes conduit aussi à l'étude de séries formelles ([FS83], [BR82]). Par ailleurs, ces séries peuvent aussi être vues comme des langages avec multiplicité et apparaissent ainsi naturellement en théorie du codage.

Les thèmes développés dans cette thèse se rattachent également à la dynamique symbolique qui est, à l'origine, une méthode pour étudier des systèmes dynamiques plus généraux. Depuis lors, les idées et techniques développées dans ce domaine ont trouvé de nombreuses applications en théorie de l'information aussi bien qu'en algèbre linéaire. Elles sont utilisées ici d'une part, pour obtenir des propriétés matricielles qui interviennent dans l'étude du problème de la hauteur d'étoile et, d'autre part, pour étudier les distributions de longueurs des codes préfixes.

Ce travail porte plus particulièrement sur les séries à coefficients entiers positifs, sur les séries $\mathbb{N}$-rationnelles et est centré autour de deux types de questions : le problème de la hauteur d'étoile et l'étude des propriétés des distributions de longueurs des codes.

Hauteur d'étoile

Un langage rationnel peut être vu comme les étiquettes des chemins dans un automate. Sa hauteur d'étoile est une mesure de la complexité en boucles d'automates associés au langage.

La notion de hauteur d'étoile d'une expression rationnelle exprimée au moyen de l'union, de la concaténation et de l'étoile, a été introduite par Eggan ([Egg63]). La hauteur d'étoile d'un langage formel est le nombre minimal d'étoiles superposées dans une expression décrivant ce langage. La difficulté de ce problème vient du fait que, dans le

cas général, il existe une infinité d'expressions asssociées à un langage donné. La hauteur d'étoile d'un langage rationnel n'est pas bornée mais elle est décidable : Hashiguchi ([Has89]) a établi l'existence d'un algorithme pour la déterminer.

Par la suite, la notion de hauteur d'étoile a été étendue aux séries en plusieurs variables non-commutatives (langages rationnels avec multiplicité). La généralisation des résultats connus pour les langages reste un problème ouvert. Récemment, Reutenauer ([Reu96]) a montré que pour les séries à coefficients dans un corps, la hauteur d'étoile n'est pas bornée.

Dans cette thèse, on a étudié le problème de la hauteur d'étoile de séries rationnelles particulières : les séries $\mathbb{N}$-rationnelles en une variable. On sait, d'après un résultat de Soittola ([Soi76]), que ces séries sont de hauteur d'étoile inférieure ou égale à 2. On s'est attaché plus particulièrement à la caractérisation des séries de hauteur d'étoile 1 et à la décidabilité de la hauteur d'étoile.

On a obtenu différentes caractérisations des séries $\mathbb{N}$-rationnelles qui sont de hauteur d'étoile 1 (Proposition 11 p.78), ainsi qu'un critère permettant de décider de la hauteur d'étoile d'une classe importante de séries $\mathbb{N}$-rationnelles en une variable (Théorème 17 p.78).

L'étude de la hauteur d'étoile des séries $\mathbb{N}$-rationnelles en une variable repose sur l'étude de leurs représentations par des matrices et utilise, pour cette raison, des résultats de théorie des automates et d'algèbre linéaire (propriétés spectrales des matrices à coefficients positifs, en particulier le théorème de Perron-Frobenius). On établit, en particulier, à partir d'un résultat d'Handelman ([Han92]), une caractérisation du rayon spectral d'une matrice compagnon irréductible à coefficients entiers positifs (Théorème 10 p.59).

Distribution de longueurs des codes

Le notion de codage évoque un procédé de transformation d'un objet associé à un procédé inverse, appelé le décodage, qui permet de restituer l'objet initial.

Les débuts de la théorie du codage et de la théorie de l'information datent des travaux de Shannon de 1948 ([Sha48]). La théorie des codes s'est ultérieurement développée dans deux directions indépendantes. La première est l'étude des codes de longueur constante dans l'optique de la détection et de la correction d'erreurs. L'autre direction, initiée par Schützenberger en 1955 ([Sch56]), a conduit au développement de la théorie des codes de longueur variable. Cette théorie est maintenant une branche de l'informatique théorique, qui a des liens importants avec les langages formels, la combinatoire sur les mots, la théorie des automates, la théorie des semigroupes et la dynamique symbolique ([BP85]). Son objet est l'étude des propriétés de factorisations de mots en suites finies de mots appartenant à un ensemble donné. Un ensemble de mots utilisés pour remplacer les lettres d'un message est un code si le décodage du message obtenu est unique.

La distribution de longueurs d'un code est la suite d'entiers qui indique la répartition des mots du code en fonction de leur longueur. Les suites ainsi définies permettent d'obtenir des conditions nécessaires pour qu'un code ait certaines propriétés, en particulier

celles de finitude, de maximalité et de rationalité. Ainsi, quand le code est rationnel, sa distribution de longueurs est une suite $\mathbb{N}$-rationnelle.

On peut également s'intéresser au problème inverse, à savoir : étant donné une série à coefficients entiers positifs, à quelles conditions peut-on construire un code ayant une propriété spécifique et cette série comme série génératrice ? C'est à ce type de problèmes que l'on s'est intéressé dans le cas des codes circulaires et des codes préfixes.

Les codes circulaires sont ceux pour lesquels tout message lu sur un cercle n'a qu'un seul décodage. Ils ont été introduits par Golomb et Gordon ([GG65]) en raison de leur forte propriété de synchronisation. Ils jouent aussi un rôle important pour leurs applications à la correction d'erreurs, à l'analyse de séquences biologique ([AM95]), ainsi qu'en combinatoire ([Sta86] Section 4.7).

On prouve trois nouveaux résultats concernant ces codes :

- On généralise (Théorème 23 p.116), dans plusieurs directions, la caractérisation des distributions de longueurs des codes circulaires établie dans le cas d'un alphabet fini par Schützenberger. D'une part, on remplace l'alphabet fini par un alphabet quelconque (pas nécessairement fini) dont les éléments ont des poids, ce qui permet d'étendre le résultat à deux distributions de longueurs. D'autre part, on restreint les conditions, ce qui permet d'établir la décidabilité dans le cas d'une distribution finie.

- On donne une nouvelle formulation de cette caractérisation (Théorème 24 p.121). Ce résultat, établi par des méthodes combinatoires, donne un algorithme de décision dans le cas d'une distribution finie.

- On établit une condition nécessaire et suffisante pour qu'une suite d'entiers positifs soit la distribution de longueur d'un code circulaire maximal sur un alphabet fini (Théorème 25 p.134).

Les codes préfixes ont été définis par Morse comme les codes dont aucun mot n'est le début d'un autre. Ils peuvent être vus comme des codes à décodage instantané, tout message étant immédiatement décodable au cours de sa lecture de gauche à droite. Un code préfixe peut être représenté par un arbre, dans lequel le nombre de fils d'un nœud est au plus égal à la taille de l'alphabet sur lequel est construit le code. Les feuilles correspondent alors aux mots du code.

On cherche à caractériser les suites à coefficients entiers qui sont distributions de longueurs d'un code préfixe rationnel sur un alphabet à k lettres ou de manière équivalente les séries génératrices des arbres rationnels dans lesquels chaque nœud a au plus k fils. On présente une réponse partielle à ce problème ; plus précisément, on donne, en utilisant un résultat de Perrin ([Per89]) sur les arbres rationnels, une condition suffisante pour qu'une série $\mathbb{N}$-rationnelle soit la distribution de longueur d'un code maximal sur un alphabet à k lettres (Théorème 27 p.150). On met également en évidence les liens entre les codes préfixes et une classe de séries $\mathbb{N}$-rationnelles : les DOL-séries.

Cette thèse est organisée de la manière suivante. Les deux premiers chapitres sont une introduction d'une part aux séries rationnelles, vues comme une extension de la notion de langages, d'autre part aux séries $\mathbb{N}$-rationnelles en lien avec les matrices positives utilisées pour les représenter.

La première partie est consacrée au problème de la hauteur d'étoile. On étudie, pour commencer, le rayon spectral des matrices compagnon à coefficients entiers positifs (Chapitre 1). Dans le Chapitre 2, après avoir récapitulé les résultats connus pour les langages rationnels, on étudie ensuite en détail la hauteur d'étoile des séries $\mathbb{N}$-rationnelles en une variable.

L'étude des distributions de longueurs des codes circulaires et des codes préfixes fait l'objet de la deuxième partie. Après une rapide présentation des codes, on présente une étude combinatoire des séries génératrices des codes circulaires (Chapitre 2). Le dernier chapitre (Chapitre 3) est consacré aux codes préfixes.

Chapitre 1

Des langages aux séries formelles

Ce chapitre est consacré au rappel de définitions et résultats concernant les langages et les séries formelles. Il présente les liens entre ces deux types d'objets en insistant essentiellement sur les notions de reconnaissabilitité et de rationalité, qui coïncident quand les générateurs ne commutent pas. Pour plus de détails, on pourra consulter [Eil74], [Per90], [SS78] et [BR88].

1.1 Langages

On rappelle qu'un *monoïde* est un ensemble muni d'une opération binaire associative, notée multiplicativement, et d'un élément neutre. Le produit de deux éléments a et b est noté $a.b$.

Soit A un ensemble fini ou non, appelé *alphabet*; ses éléments sont des *lettres*. Un *mot* w sur l'alphabet A est une suite finie d'éléments de A

$$w = (a_1, a_2, \ldots, a_n), \qquad \text{avec} \quad a_i \in A \quad \text{pour} \quad 1 \leq i \leq n.$$

L'ensemble de tous les mots sur l'alphabet A est noté A^* et est muni de l'opération associative définie par la concaténation de deux suites

$$(a_1, a_2, \ldots, a_n).(b_1, b_2, \ldots, b_m) = (a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m).$$

L'associativité de cette opération permet d'écrire

$$w = a_1 a_2 \cdots a_n$$

au lieu de $w = (a_1, a_2, \ldots, a_n)$, en identifiant chaque élément a de l'alphabet A à la suite (a). La suite vide, élément neutre pour la concaténation, est appelée *mot vide*, elle est notée 1. L'ensemble A^* des mots sur l'alphabet A est ainsi muni d'une structure de monoïde et est appelé *monoïde libre* sur A. Les parties de A^* sont les *langages (formels)* sur l'alphabet A.

1.1.1 Rationalité

On définit sur l'ensemble des parties du monoïde libre A^* les *opérations rationnelles* suivantes :

- l'union $X \cup Y$, également notée $X + Y$,
- le produit $XY = \{xy \mid x \in X, y \in Y\}$,
- l'étoile $X^* = \{x_1 x_2 \cdots x_n \mid \forall n \geq 0, \text{ avec } \quad x_i \in X \quad \text{pour} \quad 1 \leq i \leq n\}$.

Les parties rationnelles de A^*, appelées *langages rationnels* sur l'alphabet A sont alors les ensembles obtenus à partir des parties finies de A^* par une suite finie d'opérations rationnelles définies précédemment. De façon équivalente, l'ensemble des langages rationnels sur A est la plus petite famille de sous-ensembles de A^* contenant les parties finies du monoïde libre A^* et stable pour les trois opérations rationnelles.

Exemple 1 Soit $A = \{a, b\}$. L'ensemble de tous les mots de A^* qui se terminent par la lettre a est un langage rationnel, il est obtenu en faisant le produit de l'étoile de A et de l'ensemble réduit à la lettre a.

On définit les *expressions rationnelles* abstraites comme les termes de l'algèbre libre sur l'ensemble $A \cup \{0, 1\}$ muni des symboles fonctionnels $+, ., *$. Il existe alors une application, notée $e \to |e|$ de cette algèbre de termes sur l'algèbre des langages rationnels sur l'alphabet A définie inductivement de la manière suivante :

$$|0| = \emptyset, \quad |1| = \{1\}, \quad \forall a \in A \quad |a| = \{a\}$$

$$|e + e'| = |e| + |e'|, \quad |e.e'| = |e||e'|,$$

$$|e^*| = |e|^*.$$

On suppose, de plus, que l'application $e \to |e|$ satisfait les axiomes rendant l'opération $+$ idempotente et commutative, le produit associatif et distributif par rapport à $+$ et vérifie également les règles usuelles pour 0 et 1 :

$$\begin{array}{ll} |e + e'| = |e' + e| & |e + e| = |e| \\ |e.(e' + e'')| = |e.e' + e.e''| & |(e' + e'').e| = |e'.e + e''.e| \\ |e.(e'.e'')| = |(e.e').e''| & |0 + e| = |e + 0| = |e| \\ |1.e| = |e.1| = |e| & |0.e| = |e.0| = |0| \end{array}$$

Ces hypothèses sont cohérentes avec la définition de l'application $e \to |e|$.

Par souci de lisibilité, en l'absence d'ambiguïté, on notera e l'ensemble $|e|$ et on préférera l'écriture ee' à $e.e'$.

Ces expressions sont utilisées pour représenter les langages rationnels.

Exemple 2 Soit $A = \{a, b\}$. L'ensemble X de tous les mots de A^* qui se terminent par la lettre a, peut être représenté par l'expression rationnelle

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

Cependant, plusieurs expressions rationnelles distinctes peuvent décrire un même langage rationnel. Ainsi l'ensemble des mots qui s'écrivent sur l'alphabet $A = \{a, b\}$ peut être décrit par les expressions $(a + b)^*$ et $(a^*b)^*a^*$.

De façon plus générale, quelles que soient les expressions e et f, les interprétations des expressions rationnelles associées à $(e + f)^*$ et $(e^*f)^*e^*$ sont égales, cette relation est appelée une *identité* et est alors notée

$$(e + f)^* \equiv (e^*f)^*e^*.$$

Il existe, en particulier, des identités, à l'image de celle qui vient d'être décrite, reliant l'étoile aux autres opérations rationnelles. Cette propriété est la source du problème de la hauteur d'étoile qui sera explicité dans ce qui suit.

Exemple 3 Identités mettant en relation des expressions rationnelles dont la hauteur d'étoile diffère
Pour toutes expressions e et f, les deux membres des identités

$$(e + f)^* \equiv (e^*f)^*e^*,$$

$$1 + (e + f)^*f \equiv (e^*f)^*.$$

représentent les mêmes langages.

D'après un résultat dû à Redko et Salomaa (cf. [Con71]), tout système complet d'identités sur un alphabet à deux lettres est infini. Des résultats plus récents sur les identités sont présentés dans [Kro91a], [Kro91b] et [Kro92].

1.1.2 Reconnaissabilité

On rappelle quelques définitions relatives aux automates, pour plus de détails on pourra se reporter à [Eil74] ou [Per90].

Soit A un alphabet. Un *automate* sur l'alphabet A est un quadruplet

$$\mathcal{A} = (Q, I, F, E)$$

constitué d'un ensemble Q d'*états*, de deux sous-ensembles I et F de Q appelés respectivement ensembles des états *initiaux* et *finaux*, et d'un ensemble

$$E \subset Q \times A \times Q$$

dont les éléments sont des *transitions*. Une transition $f = (p, a, q)$ est également notée

$$f : p \xrightarrow{a} q.$$

La lettre a est l'*étiquette* de la transition. L'automate est *fini* quand l'ensemble Q de ses états est de cardinal fini.

L'automate est *déterministe* s'il ne possède qu'un seul état initial et si, pour tout état p de Q et toute lettre a de A, il existe au plus un état q de Q tel que

$$f : p \xrightarrow{a} q \in E.$$

L'ensemble des états initiaux d'un automate déterministe n'ayant qu'un seul élément, il sera souvent noté i au lieu de I. Un automate déterministe est dit *complet* si pour tout état p de Q et toute lettre a de A, il existe au moins un état q de Q tel que

$$f : p \xrightarrow{a} q.$$

Quand l'automate est déterministe, ses transitions définissent une fonction partielle, appelée *fonction de transition* de $Q \times A$ dans Q, qui, à tout couple (p, a) avec $p \in Q$ et $a \in A$, associe $p.a$ défini par

$$p.a = \begin{cases} q & \text{si} \quad (p, a, q) \in \mathcal{F} \\ \text{non défini,} & \text{sinon.} \end{cases}$$

Cette fonction est étendue aux mots de A^* en posant

$$\forall p \in Q, \quad p.1 = p \qquad \text{et} \qquad \forall w \in A^*, a \in A \quad p.wa = (p.w).a.$$

Deux transitions de $\mathcal{A}$, (p, a_i, q) et (p', a_j, q'), sont dites consécutives dans $\mathcal{A}$ si $q = p'$. Un *chemin* dans l'automate $\mathcal{A}$ est une suite finie

$$c = c_1 c_2 \cdots c_n$$

de transitions consécutives

$$c_i = (q_i, a_i, q_{i+1}), \quad 0 \leq i \leq n - 1.$$

L'entier n est la *longueur* du chemin c, les états q_1 et q_{n+1} respectivement son *origine* et sa *fin*. On écrit

$$c : q_0 \xrightarrow{w} q_n,$$

où $w = a_1 a_2 \cdots a_n$, *étiquette* du chemin, est le résultat de la concaténation des étiquettes des transitions qui constituent le chemin c. Par convention, il existe, pour tout état $q \in Q$, un chemin de longueur nulle d'extrémités q étiqueté par le mot vide de A^*. On appelle *cycle* un chemin allant d'un état à lui-même et passant au plus une fois par les autres états de l'automate et *boucle* un cycle de longueur 1.

Un chemin $c : i \to t$ est *réussi* si $i \in I$ et $t \in T$. L'ensemble *reconnu* par l'automate $\mathcal{A}$, noté $\mathcal{L}(\mathcal{A})$ est l'ensemble des étiquettes des chemins réussis. Deux automates qui reconnaissent le même langage sont dits *équivalents*. Un langage $X \subset A^*$ est dit *reconnaissable* s'il existe un automate fini $\mathcal{A}$ tel que $X = \mathcal{L}(\mathcal{A})$.

Un état p est dit *accessible* s'il existe dans l'automate un chemin allant d'un état initial à l'état p, il est dit coaccessible s'il existe un chemin allant de p à un état final. Un automate est *émondé* si tous ses états sont simultanément accessibles et coaccessibles. Si P est l'ensemble des états accessibles et coaccessibles d'un automate $\mathcal{A} = (Q, I, F, E)$, alors l'automate émondé $\mathcal{A}' = (P \cap Q, P \cap I, P \cap F, E')$, où

$$E' = E \cap ((P \cap Q) \times A \times (P \cap Q))$$

est équivalent à $\mathcal{A}$.

Remarque 1 La définition d'un langage reconnaissable n'implique pas un choix privilégié du sens de lecture. En effet, un ensemble X est reconnaissable si et seulement si l'ensemble $\tilde{X}$ obtenu en retournant les mots de X est reconnaissable.

Exemple 4 Dans l'exemple suivant (Figure 1.1), l'alphabet est $A = \{a, b\}$, l'état initial est noté par un flèche entrante et l'état final par un double cercle. On adoptera désormais cette convention.

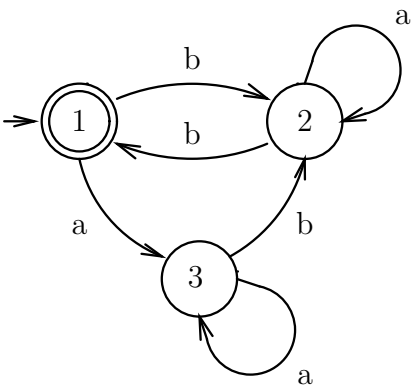


FIG. 1.1 – *Automate* $\mathcal{A}$, $\mathcal{L}(\mathcal{A}) = ((a^*b)^2)^*$

Automate minimal et monoïde syntactique

On définit maintenant, pour un langage X donné de A^*, un automate déterministe particulier $\mathcal{A}(X) = (Q, i, F, E)$ associé à ce langage.

Les états de $\mathcal{A}(X)$ sont les ensembles non vides

$$w^{-1}X = \{x \in A^* \mid wx \in X\} \qquad \text{pour} \quad w \in A^*,$$

l'état initial i est $X = 1^{-1}X$ et les états finaux sont ceux qui contiennent le mot vide. La fonction partielle de transition est définie pour un état $Y = w^{-1}X$ et une lettre a de A par

$$Y.a = a^{-1}Y \qquad \text{si} \quad a^{-1}Y \neq \emptyset.$$

Dans ces conditions, le langage reconnu par $\mathcal{A}(X)$ est X et l'automate $\mathcal{A}$ est appelé l'*automate minimal* (pour la lecture de gauche à droite), car le nombre d'états de $\mathcal{A}$ est minimal parmi les automates déterministes qui reconnaissent X .

On peut définir de manière analogue l'automate minimal à droite (*i.e.*, pour la lecture de droite à gauche) associé au langage X, en considérant les ensembles

$$Xw^{-1} \qquad \text{pour} \quad w \in A^*.$$

Un langage est reconnaissable, quand son automate minimal (à droite ou à gauche) est fini.

Exemple 4 (suite) L'automate minimal (pour la lecture de gauche à droite) du langage $((a^*b)^2)^*$ est celui de la Figure 1.1.

Exemple 5 Soit $A = \{a, b\}$ et X l'ensemble des mots de A^* qui se terminent par ab. Alors X est décrit par l'expression rationnelle $(a+b)^*ab$. Son automate minimal (pour la lecture de gauche à droite) est celui de la Figure 1.2.

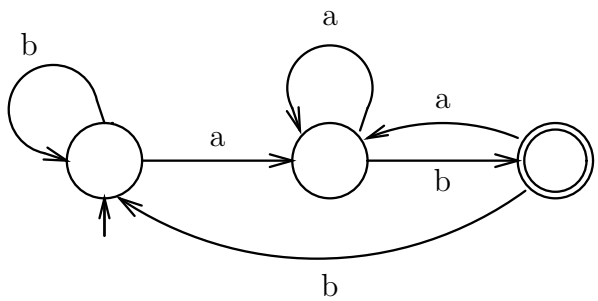


FIG. 1.2 – *Automate minimal à gauche de* $(a + b)^*ab$

La comparaison avec l'automate minimal (pour la lecture de droite à gauche) donné par la Figure 1.3 montre que les deux automates minimaux peuvent être sensiblement différents.

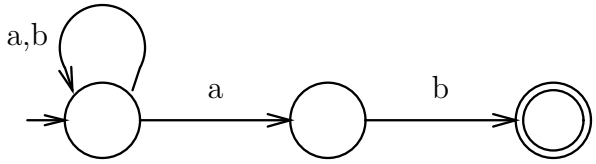


FIG. 1.3 – *Automate minimal à droite de* $(a+b)^*ab$

A tout automate déterministe, on peut associer un monoïde de la manière suivante. Soit $\mathcal{A} = (Q, i, F, E)$ un automate déterministe et soit Γ le monoïde des fonctions partielles de Q dans Q, la loi de composition étant définie (en notant les fonctions à droite : $q\gamma$ au lieu de $\gamma(q)$) par

$$\forall q \in Q, \quad \forall \gamma_1, \gamma_2 \in \Gamma, \qquad q(\gamma_1\gamma_2) = (q\gamma_1)\gamma_2.$$

Soit ϕ la fonction qui à tout mot w de A^* associe la fonction partielle $\phi(w)$ de Q dans Q définie par

$$q\phi(w) = q.w$$

Alors ϕ est un morphisme de A^* dans le monoïde des fonctions partielles de Q. Le sous-monoïde $\phi(A^*)$ est appelé le *monoïde des transitions* de l'automate $\mathcal{A}$.

On introduit la notion de monoïde syntactique d'un langage. Il est isomorphe au monoïde des transitions de l'automate minimal (Proposition 1) et sa structure reflète de nombreuses propriétés du langage. Soit $X \subset A^*$, on définit l'ensemble C_X des contextes d'un mot w de A^* selon X, en posant

$$C_X(w) = \{(u, v) \in A^* \times A^* \mid uwv \in X\}.$$

La *congruence syntactique* σ_X de X est alors la relation d'équivalence sur A^* définie par

$$w \equiv w' \qquad \Leftrightarrow \qquad C_X(w) = C_X(w'),$$

autrement dit, deux mots sont équivalents s'ils ont mêmes contextes dans X. Comme une congruence ést une relation d'équivalence compatible avec la structure de monoïde, le monoïde quotient de A^* par σ_X est appelé le *monoïde syntactique* de X.

Proposition 1 *Soit $X \subset A^*$. Le monoïde syntactique de X est isomorphe au monoïde des transitions de l'automate minimal de X.*

Ce résultat permet d'établir des propriétés du monoïde syntactique sans le calculer explicitement. En particulier, en remarquant que le complémentaire de X dans A^* est reconnu par l'automate obtenu à partir de l'automate minimal de X en changeant l'ensemble

des états finaux T en son complémentaire dans Q, on obtient que le complémentaire d'un langage reconnaissable X est reconnaissable et a le même monoïde syntactique que X.

Enfin, on énonce le théorème fondamental montrant le lien entre les langages rationnels et les langages reconnaissables.

Théorème 1 (Kleene) *Soit A un alphabet fini. Un ensemble $X \subset A^*$ est reconnaissable si, et seulement si, il est rationnel.*

La preuve originale de ce résultat se trouve dans l'article [Kle56]. Ce théorème peut également être vu comme la conséquence d'un théorème de Schützenberger (Théorème 2 p.17) sur les séries.

1.2 Séries formelles

Dans ce qui suit, on définit les séries formelles ainsi que les notions de reconnaissabilité et de rationalité associées. Le terme "formel" indique que l'on s'intéresse surtout aux diverses opérations définies sur les séries plutôt qu'à leur sommation. A la différence des séries étudiées en combinatoire, les variables ne commutent pas. Dans les deux approches, l'ensemble des séries est considéré comme une structure algébrique. Dans le cas de séries en une seule variable, les points de vue se confondent.

1.2.1 Séries : applications dans un demi-anneau

On rappelle qu'un *demi-anneau* K est un ensemble muni de deux lois de composition interne, la somme et le produit, notées + et . vérifiant les propriétés suivantes :

- $(K, +)$ est un monoïde commutatif dont l'élément neutre est noté 0.
- $(K, .)$ est un monoïde dont l'élément neutre est noté 1.
- Le produit est distributif par rapport à l'addition.
- $\forall z \in K, \quad 0.z = z.0 = 0.$

Soient A un alphabet et A^* le monoïde libre engendré par A. On définit une *série* s sur l'alphabet A à coefficients dans un demi-anneau K comme une application

$$\begin{array}{rl} s : & A^* \to K \\ & w \to \langle s, w \rangle, \end{array}$$

où l'image $\langle s, w \rangle$ d'un mot w est appelé le *coefficient* de w dans la série s. La série s est notée comme une somme formelle

$$s = \sum_{w \in A^*} \langle s, w \rangle w.$$

L'ensemble des séries formelles sur A à coefficients dans K est noté $K\langle\langle A \rangle\rangle$ et muni d'une structure de demi-anneau. La somme de deux séries s et s' de $K\langle\langle A \rangle\rangle$ est définie

par

$$s + s' = \sum_{w \in A^*} (\langle s, w \rangle + \langle s', w \rangle) w.$$

et le produit (de Cauchy) par

$$ss' = \sum_{w \in A^*} (\sum_{w_1 w_2 = w} \langle s, w_1 \rangle \langle s', w_2 \rangle) w.$$

Remarque 2 On peut également définir les séries sur un monoïde M quelconque au lieu de faire le choix d'un monoïde libre, cependant la définition du produit pose alors quelques difficultés si un mot admet un nombre infini de factorisations.

Dans le cas où l'alphabet A est réduit à un singleton et où K est le demi-anneau $\mathbb{N}$ des entiers naturels, on obtient les séries à coefficients entiers positifs en une variable.

Support d'une série

On définit le *support* d'une série s comme l'ensemble des mots ayant un coefficient non nul dans s

$$\mathrm{supp}(s) = \{w \in A^* \mid \langle s, w \rangle \neq 0\}.$$

Le sous-ensemble des séries ayant un support fini est noté $K\langle A \rangle$ et ses éléments sont appelés les *polynômes*. Le support d'une série s appartenant à $K\langle\langle A \rangle\rangle$ est un langage sur l'alphabet A.

Réciproquement, un langage $X \subset A^*$ où A est un alphabet peut être vu comme une application à valeurs dans l'anneau des booléens ou dans $\mathbb{N}$

$$\begin{array}{rccl} X : & A^* \to & \mathbb{B} = \{0, 1\} \\ & x \to & \begin{cases} 1 & \text{si } x \in X \\ 0 & \text{sinon.} \end{cases} \end{array}$$

On obtient ainsi la *série caractéristique* $\underline{X}$ du langage X donnée par

$$\underline{X} = \sum_{x \in A^*} X(x) x.$$

1.2.2 Séries rationnelles

Soient A un alphabet et K un demi-anneau. On appelle expression rationnelle sur un alphabet A avec multiplicité dans K toutes les expressions écrites sur $A \cup \{1\}$ à coefficients dans K à l'aide des opérateurs rationnels $+, ., *$. La *multiplicité* $\langle E, x \rangle$ d'un mot x relativement à une expression rationnelle E est alors le coefficient avec lequel ce mot apparaît dans l'expression.

De manière plus formelle, la multiplicité peut être définie par les règles récursives suivantes :

$$\forall k \in K, \quad \forall x \in A^*, \qquad \langle kx, x\rangle = k,$$
$$\langle E + F, x\rangle = \langle E, x\rangle + \langle F, x\rangle,$$
$$\langle E.F, x\rangle = \sum_{uv=x} \langle E, u\rangle\langle F, v\rangle,$$
$$\langle E^*, x\rangle = \sum_{n\geq 0} \sum_{x=u_1\ldots u_n} \langle E, u_1\rangle\langle E, u_2\rangle \ldots \langle E, u_n\rangle,$$

avec les règles, pour $a, b \in A$,

$$\langle a, b\rangle = 0 \qquad \text{si} \quad a \neq b \quad \text{et} \quad 1 \quad \text{dans le cas contraire,}$$
$$\langle 1, x\rangle = 0 \qquad \text{si} \quad x \neq 1 \quad \text{et} \quad 1 \quad \text{sinon,}$$

et, enfin, pour tout mot x, $\langle 0, x\rangle = 0$.

La notion de multiplicité permet de considérer, les séries K-rationnelles comme des langages rationnels avec multiplicité dans un demi-anneau K. Ainsi, comme pour les langages, si K est un demi-anneau, une série est dite *K-rationnelle* si et seulement si elle peut être obtenue à partir de polynômes à coefficients dans K à l'aide des trois opérations rationnelle suivantes :

- la somme,
- le produit
- l'opération unaire *étoile* définie, quand $P(0) = 0$, par $P^\star = \sum_{n\geq 0} P^n$.

Dans ces conditions, les langages rationnels sont les séries rationnelles à coefficients dans le demi-anneau de Boole.

Exemple 6 Soient $K = \mathbb{Z}$, x une lettre de l'alphabet A et s la série définie par

$$s = \sum_{w\in A^*} |w|_x w.$$

Comme la série caractéristique de A^* et le produit de séries rationnelles sont rationnels, il en de même de la série $\underline{A}^*\underline{x}\ \underline{A}^*$. Or,

$$\langle \underline{A}^*\underline{x}\ \underline{A}^*, w\rangle = \sum_{uxt=w} 1 = |w|_x.$$

On en déduit que la série

$$s = \sum_{w\in A^*} |w|_x w$$

est rationnelle.

Une autre propriété relie langages et séries : les langages rationnels sont exactement les supports des séries $\mathbb{N}$-rationnelles. Ce résultat est encore vrai quand le demi-anneau K est fini mais ne l'est pas de façon générale ; en particulier, il existe des séries $\mathbb{Z}$-rationnelles dont le support n'est pas un langage rationnel (cf Exemple 13 p.36).

1.2.3 Séries reconnaissables

On introduit maintenant la notion d'automate avec multiplicité. Un automate sur A avec multiplicité dans K

$$\mathcal{A} = (Q, I, T, M)$$

est défini de la manière suivante. L'ensemble Q est l'ensemble fini des états de l'automate et I, T, M sont des matrices indexées par Q de tailles respectives $1 \times n$, $n \times 1$ et $n \times 1$ si n est le cardinal de Q. Les coefficients de I et T sont des scalaires de K. Ceux de M sont soit nuls, soit des polynômes de degré 1. De plus, si

$$M_{pq} = \sum_{i=1}^{n} k_i a_i \qquad \text{avec} \quad k_i \in K, a_i \in A \quad \text{pour} \quad 1 \leq i \leq n,$$

alors il existe dans l'automate $\mathcal{A}$ une transition de l'état p à l'état q ayant pour étiquette ce polynôme.

Si c est le chemin

$$p \overset{k_1 a_1}{\to} q_1 \to \ldots \to q_{n-1} \overset{k_n a_n}{\to} q,$$

alors son étiquette est kw, où k est le produit des coefficients k_i et où w est obtenu par concaténation des lettres a_i, sa longueur est la même que celle du mot w. Par suite, le langage avec multiplicité $\mathcal{L}(\mathcal{A})$, reconnu par l'automate, est décrit par

$$\mathcal{L}(\mathcal{A}) = IM^*T \quad \text{avec} \quad M^* = \sum_{i \geq 0} M^i.$$

Une série formelle s appartenant à $K\langle\langle A \rangle\rangle$ est dite *reconnaissable* s'il existe un automate $\mathcal{A} = (Q, I, T, M)$ sur A, avec multiplicité dans K, tel que

$$\mathcal{L}(\mathcal{A}) = s.$$

Le triplet (I, M, T) est appelé une *représentation linéaire* de la série s.

De manière équivalente, une série s est dite reconnaissable s'il existe un entier $n \geq 1$, un morphisme de monoïdes

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

($K^{n \times n}$ muni de sa structure multiplicative) et deux vecteurs $l \in K^{1 \times n}$ et $c \in K^{n \times 1}$ tels que, pour tout mot w,

$$\langle s, w \rangle = l\mu(w)c.$$

Le triplet (l, μ, c) est alors une représentation linéaire de la série s et n est sa *dimension*.

Exemple 7 La série de Fibonacci

Soit $A = \{z\}$ et soit, pour tout entier n, a_n la multiplicité de z^n, c'est-à-dire le nombre de chemins réussis de longueur n dans l'automate suivant (Figure 1.4).

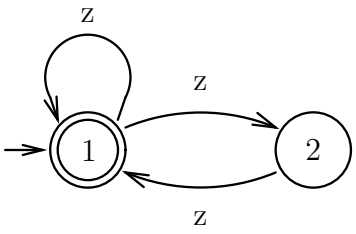


FIG. 1.4 – *Nombre de chemins de longueur n : le $n^{ième}$ nombre de Fibonacci*

On a alors

$$a_0 = 1 \quad \text{et} \quad a_1 = 1.$$

De plus, pour tout entier n supérieur à 2, tout chemin réussi w s'écrit

$$\begin{aligned} 1 &\xrightarrow{w'} 1 \xrightarrow{z} 2 \xrightarrow{z} 1 \quad & w' = z^{n-2} \\ 1 &\xrightarrow{w''} 1 \xrightarrow{z} 1 & w'' = z^{n-1}. \end{aligned}$$

On en déduit que

$$a_n = a_{n-2} + a_{n-1},$$

l'entier a_n est égal au $n$ième nombre de Fibonacci. Le langage avec multiplicité $\mathcal{L}$ reconnu par l'automate est alors décrit par la série

$$\mathcal{L} = \sum_{n \geq 0} a_n z^n = (z + z^2)^*.$$

Remarque 3 Dans le cas de séries en une seule variable, on supprimera désormais la lettre dans les étiquettes des transitions et seules apparaîtront les multiplicités.

Représentation linéaire minimale

Quand K est un anneau commutatif, Reutenauer ([Reu80]) a introduit une notion analogue à celle de monoïde syntactique d'un langage : l'*algèbre syntactique* d'une série. La notion de congruence est remplacée par celle d'idéal, l'*idéal syntactique* $\mathcal{I}_s$ d'une série $s \in K\langle\langle X \rangle\rangle$, considérée comme une application linéaire sur l'espace des polynômes, étant

le plus grand idéal bilatère de $K\langle X\rangle$ contenant le noyau de la série s. L'algèbre syntactique de s est alors le quotient de l'algèbre libre $K\langle X\rangle$ par $\mathcal{I}_s$. Dans ces conditions, une série est reconnaissable si, et seulement si, son algèbre syntactique est de dimension finie. La notion d'idéal syntactique unilatère remplace celle d'automate minimal : l'idéal syntactique droit, par exemple, de s étant

$$\mathcal{I}_s^d = \{P \in K\langle X\rangle \mid s \circ P = 0\}$$

où l'opération $\circ$ est définie $s \circ u = u^{-1}s$ pour tout mot $u \in X^*$ et étendue par linéarité à $K\langle X\rangle$.

Quand K est un corps, la *représentation minimale* d'une série s est une représentaion linéaire de taille minimale parmi toutes les représentations de s. D'après un résultat de Schützenberger, deux représentations minimales d'une même série sont similaires, autrement dit, les représentations minimales d'une série sont sur une même orbite pour l'action du groupe $Gl_n(K)$ sur $K^{n\times n}$ (où n est la dimension d'une représentation minimale de s). Quand une série est reconnaissable, la dimension d'une représentation minimale est égale à la codimension de ses idéaux syntactiques ([CP71] et [Fli74]).

Le théorème fondamental

Le théorème de Kleene ([Kle56]) qui établit l'équivalence entre rationalité et reconnaissabilité pour les langages (séries à coefficients dans le demi-anneau des booléens) peut être étendu aux séries formelles en plusieurs variables non-commutatives à coefficients dans des demi-anneaux quelconques ([Sch61]). Il s'énonce alors de la manière suivante.

Théorème 2 (Schützenberger) *Une série formelle en plusieurs variables non-commutatives est K-rationnelle si, et seulement si, elle est reconnaissable par un automate avec multiplicité dans K.*

Chapitre 2

Séries $\mathbb{N}$-rationnelles en une variable

Ce chapitre constitue une introduction aux séries $\mathbb{N}$-rationnelles en une variable qui sont des séries formelles particulières que l'on peut définir de plusieurs manières équivalentes. L'une de ces définitions est la suivante : ce sont les langages rationnels avec multiplicité sur un alphabet réduit à une unique lettre. Le coefficient d'ordre n est alors le nombre de chemins de longueur n d'un graphe orienté G, plus précisément, du graphe orienté des états d'un automate reconnaissant la série.

Dans ce qui suit, on présente différents types de caractérisations, analytique et algébrique, des séries $\mathbb{N}$-rationnelles en une variable.

Les raisonnements ultérieurs reposent essentiellement sur l'utilisation des propriétés de leurs représentations linéaires, et, plus généralement, sur l'exploitation des résultats connus sur les matrices à coefficients positifs (on pourra consulter sur ce sujet [Gan59] tome 2, [Min88], [BP79] et [LM95]).

L'étude des propriétés de ces matrices a débuté avec le théorème de Perron publié en 1907 ([Per07]), bientôt étendu par Frobenius ([Fro12]), et maintenant connu sous le nom du théorème de Perron-Frobenius (Théorème 5 p.22). Ce résultat donne en particulier une propriété fondamentale du spectre de telles matrices : elles ont pour rayon spectral une de leurs valeurs propres. Depuis, plusieurs tentatives ont été faites pour établir une réciproque à ce théorème par une caractérisation des applications linéaires pouvant être représentées par une matrice positive. Une possibilité consiste à étudier les conditions pour qu'un n-uplet soit le spectre d'une telle matrice (cf. [BP79], [BH91] et [LM95]). Une autre direction réside dans l'étude des conditions pour qu'une suite de nombres positifs soit l'image, par une forme linéaire positive fixée, de l'orbite d'un vecteur par l'action d'une matrice positive. De telles suites ne sont autres que les suites rationnelles positives. Un théorème de Soittola (Théorème 8 p.30) résout le problème qui vient d'être évoqué et donne une caractérisation des suites rationnelles positives vérifiant une relation de récurrence linéaire.

Ce dernier résultat, établi à l'aide d'autres techniques par Katayama, Okamoto et Enomoto ([KOE78]), constitue également une caractérisation analytique de ces séries par les pôles de leurs fonctions génératrices.

Dans la première section de ce chapitre, on rappelle les propriétés des matrices positives dont on aura besoin ultérieurement. On introduit également les matrices à coefficients polynomiaux qui permettent de représenter les graphes étiquetés de manière plus concise et dont le spectre est, aux valeurs propres nulles près, celui de la matrice adjacente du graphe.

La deuxième partie (Section 2.2 p.28) est consacrée aux séries $\mathbb{N}$-rationnelles en une variable et à leur caractérisation par le théorème de Soittola (Théorème 8 p.30).

2.1 Matrices positives

Dans ce qui suit, on donne une présentation de résultats connus sur les matrices carrées positives, *i.e.* les matrices carrées à coefficients positifs ou nuls (cf. [Gan59] tome 2, [Min88] ou [BP79]). Les propriétés des matrices à coefficients entiers positifs constituent un outil important pour l'étude des séries $\mathbb{N}$-rationnelles à partir de leurs représentations linéaires.

2.1.1 Matrices à coefficients positifs

Une matrice carrée est dite *positive*, respectivement *strictement positive*, si ses coefficients sont positifs ou nuls, respectivement strictement positifs.

On note $M \geq 0$, respectivement $M > 0$, une matrice positive, respectivement strictement positive. Ces deux relations d'ordre partiel sur les matrices de taille quelconque fixée sont des comparaisons, coefficient par coefficient ; ainsi deux matrices M et M' vérifient

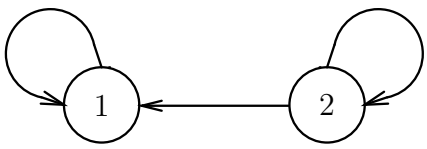
$$M \geq M' \qquad \Leftrightarrow \qquad \forall i, j \quad m_{ij} \geq m'_{ij}$$

et

$$M > M' \qquad \Leftrightarrow \qquad \forall i, j \quad m_{ij} > m'_{ij}.$$

Le *graphe orienté* G_M, associé à une matrice M de taille n, est constitué de n sommets, notés $1, 2, \ldots, n$, et d'arcs de i à j étiquetés m_{ij} si et seulement si $m_{ij} \neq 0$.

Exemple 8 La matrice M_R conduit ainsi au graphe suivant (Figure 2.1)



Matrice associée

$$M_R = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

FIG. 2.1 – *Matrice réductible*

On rappelle que le *polynôme caractéristique* d'une matrice M est le polynôme

$$\chi_M(x) = \det(xId - M),$$

où Id est la matrice identité. Ses racines sont appelées les *valeurs propres* de la matrice M. L'ensemble de toutes les valeurs propres d'une matrice constitue son *spectre* et le module maximal des éléments du spectre est son *rayon spectral*. Enfin, un *vecteur propre* de M associé à une valeur propre λ est un vecteur non nul v tel que $Mv = \lambda v$.

Propriétés générales

On commence par énoncer le principal résultat concernant les matrices positives connu sous le nom du théorème de Perron-Frobenius.

Théorème 3 (Perron-Frobenius) *Soit M une matrice positive. Alors M a une valeur propre réelle positive λ, supérieure aux modules de toutes les autres valeurs propres de M. La valeur propre λ est donc rayon spectral de la matrice. De plus, à cette valeur propre correspond un vecteur propre positif.*

Dans ce qui suit, On précise, sous des hypothèses supplémentaires, les propriétés du spectre des matrices positives (Théorème 5 p.22).

Une permutation peut être vue comme une opération qui consiste à réordonner simultanément les indices des lignes et des colonnes d'une matrice (ou les sommets du graphe associé). Elle est représentée par une matrice carrée dont tous les coefficients sont nuls à l'exception d'un coefficient dans chaque ligne et chaque colonne qui est égal à 1. On note $P^t = (p^t_{ij})$ la transposée d'une matrice $P = (p_{ij})$, définie par

$$\forall i, j \quad p^t_{ij} = p_{ji}.$$

Si P est une permutation, alors $P^{-1} = P^t$.

On rappelle que la relation de *congruence* sur les matrices carrées est définie de la façon suivante : deux matrices M et N sont dites *congruentes* s'il existe une matrice de permutation P, *i.e.*, $P^{-1} = P^t$ telle que $PMP^t = N$.

Une matrice carrée positive M est dite *réductible* si elle est congrue à une matrice triangulaire par blocs, *i.e.* , s'il existe une permutation P qui la rende triangulaire par blocs, soit

$$PMP^t = \begin{pmatrix} M_{11} & 0 \\ M_{21} & M_{22} \end{pmatrix},$$

où M_{11} et M_{22} sont des matrices carrées. Dans la cas contraire, la matrice M est dite *irréductible*.

Théorème 4 *Si $M = (m_{ij})_{1\leq i,j\leq n}$ est une matrice positive ayant pour rayon spectral λ, alors λ appartient à l'intervalle déterminé par les valeurs extrêmes des sommes des coefficients des lignes de la matrice M, soit*

$$\min_j \sum_{i=1}^{n} m_{ij} \leq \lambda \leq \max_j \sum_{i=1}^{n} m_{ij}.$$

De plus, si M est irréductible, alors l'égalité est atteinte d'un côté quelconque de l'inégalité si, et seulement si, les sommes de chacune des lignes de la matrice M sont égales.

La preuve est donnée, par exemple, dans [Min88] (Théorème 1.1 p.24).

Matrices irréductibles

Dans le cas de matrices irréductibles, on peut préciser l'énoncé du théorème de Perron-Frobenius de la manière suivante.

Théorème 5 (Perron-Frobenius) *Si la matrice M est irréductible alors son rayon spectral λ_M est une valeur propre simple de M, les autres valeurs propres de M de module λ_M sont également simples ; de plus, la matrice M a un vecteur propre strictement positif x correspondant à la valeur propre λ_M et tout vecteur propre positif de M, associé à λ_M, est un multiple de x.*

- *Si une matrice irréductible M a p valeurs propres de module $\lambda_M = r$,*

  $$\lambda_0 = re^{i\theta_0}, \lambda_1 = re^{i\theta_1}, \ldots, \lambda_{p-1} = re^{i\theta_{p-1}} \quad \text{où} \quad 0 = \theta_0 < \theta_1 < \ldots < \theta_{p-1} < 2\pi,$$

  alors ces nombres sont les p racines distinctes de l'équation $z^p - r^p = 0$.

- *Plus généralement, le spectre $S = \{\lambda_0, \lambda_1, \ldots, \lambda_{n-1}\}$ de M est stable par la rotation d'angle $2\pi/p$ du plan complexe.*

Le nombre p de valeurs propres de M de module λ_M est appelé *période* de M. Si p est strictement supérieur à 1, M est *périodique* de période p. Si $p = 1$, la matrice M est *primitive*.

Comme l'unique vecteur propre positif, à un coefficient multiplicatif près, d'une matrice irréductible M correspond au rayon spectral λ de M, le rayon spectral s'interprète comme un min max ou comme max min, *i.e.*,

$$\lambda = \max_{x>0} \left\{ \min_{x_i>0} \frac{(Mx)_i}{x_i} \right\} = \min_{x>0} \left\{ \max_{x_i>0} \frac{(Mx)_i}{x_i} \right\}.$$

Remarque 4 Si la matrice M est strictement positive, alors son rayon spectral λ_M est une valeur propre simple, strictement supérieure aux modules des autres valeurs propres de la matrice M.

On donne maintenant une caractérisation simple de l'irréductibilité.

Théorème 6 *Une matrice positive $M = (m_{ij})$ est irréductible si, et seulement si,*

$$\forall (i,j), \quad \exists n \geq 0 \quad \textit{tel que} \quad (M^n)_{ij} > 0.$$

Elle est primitive si, et seulement si,

$$\exists n \geq 0 \quad \textit{tel que} \quad \forall (i,j) \quad (M^n)_{ij} > 0.$$

Remarque 5 Soit m le degré du polynôme minimal de M. Si la matrice M est irréductible, alors, pour tout couple (i,j), l'entier n satisfaisant $(M^n)_{ij} > 0$ peut être choisi tel que
- $n \leq m$ si $i = j$
- et $n < m$ si $i \neq j$.

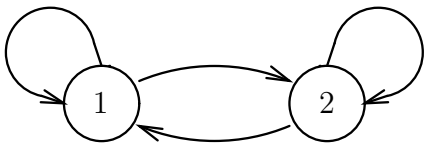
Ce résultat est dû à Gantmacher ([Gan59]).

Ces caractérisations des matrices irréductibles et primitives s'interprètent en termes de graphes de la façon suivante.

On rappelle préalablement qu'un graphe orienté G est *fortement connexe* si pour tout couple (i,j) de sommets de G, il existe un chemin (ou une suite d'arcs) de i à j. Comme $(M^n)_{ij} > 0$ si, et seulement si, il existe une suite de n arcs de i à j, une matrice M est irréductible si, et seulement si, le graphe associé G_M est fortement connexe.

Exemple 9 Les graphes des Figures 2.2 et 2.3 (p.24) étant fortement connexes, les matrices associées, respectivement M_P et M_I, sont irréductibles.

En revanche, comme il n'existe aucun chemin de l'état 1 à l'état 2 dans le graphe de la Figure 2.1 (p.20), la matrice M_R est réductible.



Matrice associée

$$M_P = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

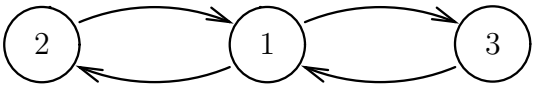
FIG. 2.2 – *Matrice primitive*

Proposition 2 *Si M est irréductible, sa période est égale au pgcd des longueurs des cycles de son graphe associé.*

Comme, de plus, une matrice positive a un coefficient strictement positif dans sa diagonale principale si, et seulement si, son graphe associé contient au moins une boucle, *i.e.*, un cycle de longueur 1, on obtient le résultat suivant.

Corollaire 1 *Une matrice irréductible dont la trace est strictement positive est primitive.*

Exemple 10 La matrice M_P (Figure 2.2 p.23) est primitive, alors que la matrice M_I (Figure 2.3) est irréductible de période 2.



Matrice associée

$$M_I = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

FIG. 2.3 – *Matrice irréductible*

Soit M une matrice non nulle et irréductible de période p. On dit que deux états i et j sont périodiquement équivalents s'il existe, dans le graphe associé à M, un chemin de i à j dont la longueur est divisible par p. La relation ainsi définie sur les états de la matrice M est une relation d'équivalence qui induit une partition des états de M en *classes périodiques*.

Proposition 3 *Soit M une matrice irréductible non nulle de période p. Alors il existe exactement p classes périodiques, qui peuvent être ordonnées en $D_1, D_2, \dots D_p$ telles que chaque transition du graphe associé à M va de D_i à D_{i+1} (ou à D_1 si $i = p$).*

La matrice M est alors congrue à

$$PMP^t = \begin{pmatrix} 0 & M_{12} & 0 & \dots & 0 \\ 0 & 0 & M_{23} & \dots & 0 \\ \vdots & & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & M_{p-1p} \\ M_{p1} & 0 & 0 & \dots & 0 \end{pmatrix}$$

où les blocs nuls de la diagonale sonts des matrices carrées et les matrices $M_{12}, \dots, M_{p1}$ sont rectangulaires et indexées, respectivement, sur $D_1 \times D_2, \dots, D_p \times D_1$.

Par suite, la matrice M^p peut être mise sous forme diagonale par blocs où chacun des blocs diagonaux est une matrice primitive représentant les chemins dont les extrémités sont contenus dans une même classe périodique. Soit

$$PM^pP^t = \begin{pmatrix} M_1 & 0 & \dots & 0 \\ 0 & M_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & M_p \end{pmatrix}$$

où les matrices

$$M_i = M_{i(i+1)}M_{(i+1)(i+2)}\dots M_{(i-1)i} \qquad (\text{avec} \quad M_{j(j+1)} = M_{p1} \quad \text{quand } j = p)$$

sont primitives de rayon spectral λ^p, si λ est le rayon spectral de M.

La période d'une matrice M est liée aux coefficients de son polynôme caractéristique.

Proposition 4 *Soit M une matrice irréductible ayant pour polynôme caractéristique*

$$\chi_M(z) = z^n + a_1 z^{n_1} + \dots + a_k z^{n_k},$$

où les coefficients a_i sont non nuls et où $n > n_1 > \dots > n_k$. Alors la période p de la matrice M est le plus grand commun diviseur des différences $n-n_1, n_1-n_2, \dots, n_{k-1}-n_k$.

La valeur propre maximale d'une matrice irréductible joue un rôle important dans le comportement des coefficients de la matrice ; quand la matrice est primitive, elle détermine complètement leur comportement asymptotique.

Théorème 7 *Soit M une matrice primitive ayant pour valeur propre maximale λ. Soient v, w les vecteurs propres droit et gauche associés, i.e., les vecteurs v et w strictement positifs normalisés tels que $Mv = \lambda v$, $wM = w\lambda$ et $w.v = 1$. Alors, pour tous i et j,*

$$(M^n)_{ij} = (v_i w_j + \rho_{ij}(n))\lambda^n,$$

où $\rho_{ij}(n) \to 0$ quand $n \to \infty$.

La preuve de ce résultat est exposée, par exemple, dans [LM95] (Théorème 4.5.12 p.130).

Matrices réductibles

D'une façon générale, les propriétés des matrices irréductibles ne sont pas conservées dans le cas de matrices réductibles. Cependant, comme toute matrice positive M peut être représentée comme la limite d'une suite de matrices M_i strictement positives et, par suite, irréductibles : $M = \lim_{i\to\infty} M_i$, certains résultats établis pour les matrices irréductibles peuvent être étendus sous une forme plus faible aux matrices positives quelconques par passage à la limite.

Si M est une matrice positive réductible, alors il existe une permutation P qui la rend triangulaire par blocs, soit

$$PMP^t = \begin{pmatrix} M_{11} & 0 \\ M_{21} & M_{22} \end{pmatrix},$$

où M_{11} et M_{22} sont des matrices carrées. Si la matrice M_{11} ou M_{22} est elle-même réductible, elle peut, de manière analogue, être mise sous une forme triangulaire par blocs. Ainsi, par une suite de permutations, on obtient le résultat suivant.

Proposition 5 *Si M est une matrice positive réductible, elle s'écrit, à une permutation près, sous la forme suivante :*

$$PMP^t = \begin{pmatrix} M_{11} & 0 & \dots & 0 \\ M_{21} & M_{22} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ M_{s1} & M_{s2} & & M_{ss} \end{pmatrix},$$

où chacun des blocs diagonaux M_{ii} est une matrice irréductible ou réduite à un unique coefficient nul. Une matrice irréducticle sous forme triangulaire est réduite à un bloc unique.

Le rayon spectral λ d'une matrice réductible M est alors le maximum des rayons spectraux des blocs diagonaux de son écriture sous forme triangulaire

$$\lambda = \max_{1 \leq i \leq s} \{\lambda_i \mid \lambda_i \quad \textit{rayon spectral de} \quad M_{ii}\}.$$

On peut remarquer que les blocs diagonaux de l'écriture sous forme triangulaire d'une matrice positive M quelconque sont les matrices correspondant aux composantes fortement connexes du graphe G_M associé à la matrice M. Les blocs M_{ij} avec $i > j$, situés sous la diagonale principale, décrivent, quant à eux, les transitions entre les différentes composantes fortement connexes.

2.1.2 Matrices à coefficients polynomiaux

On sait qu'une matrice de taille n à coefficients dans $\mathbb{N}$ peut être considérée comme la donnée d'un graphe orienté à n sommets par sa matrice adjacente.

Cependant, on peut également représenter un graphe orienté en utilisant des matrices à coefficients dans $z\mathbb{N}[z]$ (*i.e.*, ensemble des polynômes à coefficients dans $\mathbb{N}$ en une variable n'ayant pas de terme constant non nul). On obtient ainsi une représentation plus concise du graphe, tout en préservant l'usage d'arguments matriciels et algébriques. Pour une synthèse sur ces matrices, on pourra se reporter à [Boy94].

Soit M une matrice de taille n à coefficients dans $z\mathbb{N}[z]$. On construit, à partir de la matrice M, un graphe orienté de la manière suivante. L'ensemble des sommets du graphe contient un ensemble de n sommets (soit, $1, 2, \dots, n$) qui indexent les lignes et

les colonnes de la matrice M. Si $M_{ij} = \sum_k a_k z^k$, on construit a_k chemins de longueur k allant du sommet i au sommet j, de sorte que chaque sommet interne de ces chemins (un chemin de longueur k a $k-1$ sommets internes) n'ait qu'une transition entrante et une transition sortante et soit distinct des sommets distingués $1, 2, \ldots, n$. Ce procédé produit un graphe qui a beaucoup plus de n sommets (d'où la concision de la représentation). La matrice adjacente du graphe est alors une matrice à coefficients dans $\{0, 1\}$.

Une autre manière de représenter le coefficient $a_k z^k$ consiste à construire un unique chemin de longueur n, dont les sommets internes vérifient les conditions précédentes, mais dont toutes les transitions, sauf une, sont étiquetées par 1, la dernière ayant, quant à elle, pour étiquette a_k. La matrice, adjacente du graphe étiqueté ainsi obtenu, est alors une matrice à coefficients entiers positifs ou nuls. Cette transformation sera préférée à la précédente, la majorité des considérations présentées dans ce qui suit ayant trait à des matrices intégrales (*i.e.*, à coefficients dans $\mathbb{N}$).

Exemple 11 La matrice

$$M = \begin{pmatrix} 0 & z^2 \\ 2z^3 & 3z + z^3 \end{pmatrix}$$

conduit, par le deuxième procédé décrit, au graphe orienté suivant (Figure 2.4).

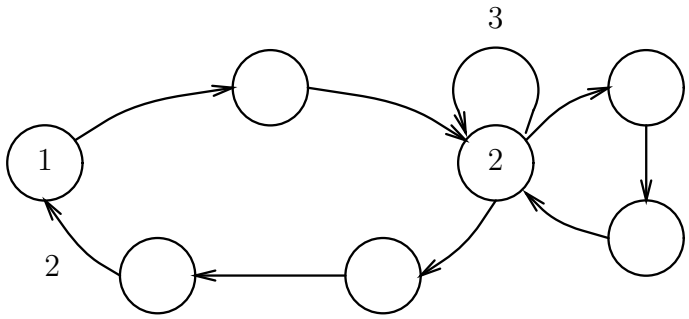


FIG. 2.4 – *Graphe associé à la matrice polynomiale M*

On appelle "*rome*" d'un graphe orienté G tout ensemble de sommets de G tel que tout chemin suffisamment long du graphe passe par au moins un sommet du "rome". Par exemple, l'ensemble constitué des sommets 1 et 2 constitue un "rome" du graphe de la Figure 2.4. L'ensemble ne contenant que le sommet 2 en est un également, c'est d'ailleurs, dans ce cas précis, le plus petit "rome" du graphe. On peut remarquer qu'il existe toujours un plus petit "rome", mais ce dernier n'est pas nécessairement unique.

Etant donné un "rome" dans un graphe orienté, on peut inverser la procédure de transformation qui vient d'être décrite et obtenir une représentation matricielle M à coefficients dans $z\mathbb{N}[z]$, où M est de taille n si le "rome" a pour cardinal n. Si N est une matrice à coefficients dans $\mathbb{N}$, adjacente d'un graphe orienté, alors zN est une matrice

à coefficients polynomiaux qui représente le graphe dans la nouvelle formalisation. Cette matrice peut être obtenue en fixant comme "rome" l'ensemble de tous les sommets du graphe.

Les matrices à coefficients polynomiaux ont une propriété importante : aux valeurs propres nulles près, leurs spectres sont les mêmes que ceux des matrices à coefficients dans $\mathbb{N}$ correspondantes.

En effet, soit $\chi_N(z)$ le polynôme caractéristique d'une matrice N de taille n à coefficients dans $\mathbb{N}$, alors le polynôme $\det(I - zN)$ est le polynôme réciproque de $\chi_N(z)$, soit

$$\det(I - zN) = z^n \chi_N(z^{-1}).$$

De plus, toutes les représentations polynomiales d'un graphe donné ont le même polynôme caractéristique, comme le montre la propriété suivante.

Propriété 1 *Si N et M sont, respectivement, des matrices à coefficients dans $\mathbb{N}$ et dans $z\mathbb{N}[z]$, et si M et N sont des représentations d'un même graphe orienté G, alors*

$$\det(I - zN) = \det(I - M).$$

2.2 Séries $\mathbb{N}$-rationnelles en une variable

Les séries $\mathbb{N}$-rationnelles en une variable peuvent être définies comme les langages rationnels avec multiplicité sur un alphabet réduit à une unique lettre. Le coefficient d'ordre n est alors le nombre de chemins de longueur n du graphe (orienté) des états de l'automate associé.

D'après le théorème de Soittola (Théorème 8 p.30), ces séries sont caractérisées par le pôle de plus petit module de leur fonction génératrice. La preuve de ce résultat permet également de donner une borne pour la hauteur d'étoile (cf. Section 2.3 p.76).

2.2.1 Définitions et résultats complémentaires

Une suite $r = (r_n)_{n\geq 0}$ d'éléments d'un demi-anneau K est dite *K-rationnelle* si sa série génératrice est K-rationnelle, c'est-à-dire, s'il existe un triplet (l, M, c), avec

$$l \in K^{1\times n}, M \in K^{n\times n}, c \in K^{n\times 1} \quad \text{et} \quad n \geq 1,$$

tels que

$$\forall k \geq 0 \qquad r_k = lM^k c.$$

La matrice M est la matrice adjacente du graphe des états d'un automate reconnaissant la série.

Quand K *est un corps*, une suite est K-rationnelle si, et seulement si, elle satisfait une relation de récurrence linéaire

$$r_n = \sum_{i=1}^{k} q_i r_{n-i} \quad (n \geq k).$$

L'unique polynôme unitaire

$$Q(z) = z^k - \sum_{i=1}^{k} q_i z^{k-i},$$

où k est choisi minimal, est appelé le *polynôme minimal* de la suite r sur K et ses racines sont appelées les *racines* de r. Si (l, M, c) est une représentation minimale de la série r (*i.e.*, M est de taille minimale), alors le polynôme caractéristique de M est le polynôme minimal de la série (à un coefficient scalaire près, le polynôme minimal de la série étant, par définition, unitaire).

De manière équivalente, la suite r est K-rationnelle si, et seulement si, sa fonction génératrice

$$f_r(z) = \sum_{n \geq 0} r_n z^n$$

peut s'écrire sous la forme

$$f_r(z) = \frac{P(z)}{Q(z)}$$

où $P, Q \in K[z]$ et $Q(0) = 1$. Si P et Q sont premiers entre eux, le polynôme minimal de r est alors le *polynôme réciproque* $\overline{Q}$ de Q,

$$\overline{Q}(z) = z^{degQ} Q(1/z).$$

Quand K est un corps, cette définition d'une série K-rationnelle coïncide avec la précédente (cf. Section 1.2.2) décrivant ces séries comme la clôture rationnelle des polynômes à coefficients dans K.

Un polynôme Q a une *racine dominante* s'il a une racine réelle positive α telle que $\alpha > |\beta|$ pour toute racine β ($\beta \neq \alpha$) de Q. On dit que la suite r a une racine dominante si son polynôme minimal en a une.

Proposition 6 *Si* $\mathbb{K}$ *est un sous-corps de* $\mathbb{C}$ *et* r *une série* $\mathbb{K}$*-rationnelle qui n'est pas un polynôme, alors pour tout* n *suffisamment grand*

$$r_n = \sum_{i=1}^{k} P_i(n) \alpha_i^n$$

où les α_i *sont les inverses des pôles distincts de la série génératrice* $f_r(z)$ *et les* P_i *des polynômes à coefficients algébriques sur* $\mathbb{K}$*, de degré égal à la multiplicité du pôle* $1/\alpha_i$ *diminuée de* 1.

Ce résultat est obtenu par une étude du développement en série entière des termes de la décomposition en éléments simples de la fonction génératrice de la série. L'unique polynôme ainsi obtenu s'appelle le *polynôme exponentiel* de la série (pour une étude plus détaillée de ce sujet, on pourra se reporter, par exemple, à [BR88] Chapitre IV).

On dit qu'une suite r est un *emboîtement* des suites $(s_i)_{0\leq i\leq p-1}$ si, pour $0 \leq i \leq p-1$ et pour tout entier naturel n, on a $r_{pn+i} = s_{i,n}$. Pour les fonctions génératrices, cela s'écrit

$$f_r(z) = \sum_{i=0}^{p-1} z^i f_{s_i}(z^p).$$

Exemple 12 La suite r dont la fonction génératrice est $f_r(z) = \frac{1}{1-z^2}$ est un emboîtement des suites dont les termes sont respectivement les termes pairs et impairs de r, soit

$$f_{s_0}(z) = \frac{1}{1-z} \quad \text{et} \quad f_{s_1}(z) = 0.$$

La notion d'emboîtement est assez naturelle, elle permet de se ramener au cas de séries ayant un seul pôle sur leur cercle de convergence et d'éviter ainsi les comportements asymptotiques oscillatoires des coefficients d'une série.

2.2.2 Théorème de Soittola

Berstel a montré ([Ber71] qu'une série $\mathbb{K}_+$-rationnelle, où $\mathbb{K}$ est un sous-corps de $\mathbb{R}$ et $\mathbb{K}_+ = \mathbb{K} \cap \mathbb{R}_+$, s'écrit comme un emboîtement de séries $\mathbb{K}$-rationnelles ayant une racine dominante. Soittola ([Soi76]), puis Katayama, Okamoto et Enomoto ([KOE78]) ont transformé cette propriété en caractérisation par des méthodes différentes.

On donne une nouvelle preuve du sens direct de ce théorème basée sur l'utilisation des propriétés des représentations linéaires des séries considérées. La deuxième partie de la démonstration que l'on présente ici est due à Perrin ([Per92]), elle suit la même trame que celle de Soittola mais préfère les manipulations de matrices à celles d'expressions rationnelles, l'interprétation de ce théorème en terme d'automates s'en déduit d'autant plus aisément. Grâce à une de leurs propriétés, on obtient une borne pour la hauteur d'étoile des séries $\mathbb{N}$-rationnelles.

Théorème 8 (Soittola) *Soit $\mathbb{K}$ un sous-corps de $\mathbb{R}$. Une série $r = \sum_{n\geq 0} r_n z^n$ à termes positifs qui n'est pas un polynôme est $\mathbb{K}_+$-rationnelle si et seulement si c'est un emboîtement de séries $\mathbb{K}$-rationnelles ayant une racine dominante.*

Démonstration : Si $r = \sum_{k\geq 0} r_k z^k$ est une série $\mathbb{K}_+$-rationnelle, alors elle admet une représentation linéaire (l, M, c), où $n \in \mathbb{N}^*, l \in \mathbb{K}_+^{1\times n}, M \in \mathbb{K}_+^{n\times n}$ et $c \in \mathbb{K}_+^{n\times 1}$, telle que

$$\forall k \geq 0 \qquad r_k = lM^k c.$$

A une permutation près, on peut supposer la matrice M triangulaire par blocs, d'après la Proposition 5 (p.26). Son rayon spectral est alors égal au maximum des rayons spectraux λ_i des matrices irréductibles M_i qui sont les blocs diagonaux. D'après le théorème de Perron-Frobenius (Théorème 5 p.22), pour chacune de ces matrices, λ_i est valeur propre simple de M_i et s'il existe p_i autres valeurs propres de M_i de module λ_i, elles sont simples et racines du polynôme $z^{p_i} - \lambda_i^{p_i} = 0$. On en déduit que $M_i^{p_i}$ a pour rayon spectral $\lambda_i^{p_i}$ qui est valeur propre (multiple si $p_i \neq 1$), strictement supérieure aux modules des autres valeurs propres de M_i.

Soit p le ppcm des entiers (p_i), la matrice M^p a alors son rayon spectral λ pour valeur propre, strictement supérieure au module de toutes les autres valeurs propres de M^p différentes de λ. De plus, la matrice M^p a pour blocs diagonaux des matrices primitives. Les séries $r_i = \sum_{n\geq 0} r_{np+i} z^n$ sont alors $\mathbb{K}$-rationnelles à coefficients positifs puisque

$$\forall n \geq 0, \quad r_{i,n} = (lM^i)(M^p)^n c.$$

Le taux de croissance de chaque série r_i est alors de l'ordre du maximum ρ_i des rayons spectraux des blocs diagonaux de M^p qui apparaissent dans la repésentation de r_i après émondage (suppression des composantes fortement connexes qui ne sont pas accessibles et coaccessibles) de l'automate associé.

Comme, de plus, les racines de chacune des séries r_i sont des valeurs propres de M^P et que les séries r_i étant $\mathbb{Q}_+$-rationnelles, leurs taux peuvent être déterminés par leurs polynômes exponentiels (Proposition 6 p.29), on en déduit, par identification, que ρ_i, étant strictement supérieur aux autres racines de r_i, est racine dominante.

Une série $\mathbb{N}$-rationnelle est donc un emboîtement de séries $\mathbb{Z}$-rationnelles ayant une racine dominante.

Réciproquement, comme la notion d'emboîtement correspond à une sommation finie couplée à un changement de variable, il conserve la $\mathbb{K}_+$-rationalité. Il suffit donc de montrer qu'une série, $r = \sum_{n\geq 0} r_n z^n$, $\mathbb{K}$-rationnelle à termes positifs, qui a une racine dominante λ, est $\mathbb{K}_+$-rationnelle, pour établir le résultat annoncé.

L'idée de la preuve peut être exprimée de la façon suivante : on construit une représentation linéaire de la série , à coefficients dans $\mathbb{K}_+$ et triangulaire par blocs (le nombre de blocs étant égal à la multiplicité de la racine dominante λ). Cette représentation existe si la série est $\mathbb{K}_+$-rationnelle puisque toute matrice à coefficients positifs s'écrit sous cette forme à une permutation près. On peut interpréter cette méthode comme la construction d'un automate reconnaissant la série, construction dans laquelle on procède composante connexe par composante connexe.

Soit $Q(z)$ le polynôme minimal de la série r sur $\mathbb{K}$ et soit m l'ordre de multiplicité de λ dans le polynôme Q. On factorise alors Q sous la forme

$$Q(z) = P(z)S(z),$$

où λ est racine simple de P et $S(z) = 1$ si λ est également racine simple de Q, dans le cas contraire S a pour racine dominante λ avec la multiplicité $m - 1$.

On raisonne par induction sur l'ordre de multiplicité m de la racine λ et on suppose que le résultat vrai pour une suite $\mathbb{K}$-rationnelle ayant un polynôme minimal dont la racine dominante a pour ordre de multiplicité $m-1$ (la preuve établit également la validité du résultat pour $m=1$).

Avant d'aller plus avant dans la mise en œuvre de la méthode précédemment décrite et sans perdre en généralité, on opère sur la série des transformations qui conservent la rationnalité.

L'addition et la multiplication par un polynôme à coefficients positifs conservant la $\mathbb{K}_+$-rationalité, la série r est $\mathbb{K}_+$-rationnelle si et seulement si la série

$$s_k(z) = \sum_{n\geq 0} r_{n+k} z^n$$

l'est également, pour k quelconque. On peut donc décaler la série d'un nombre fini arbitraire de rangs et il suffit alors de prouver que la série obtenue après décalage est $\mathbb{K}_+$-rationnelle.

De plus, pour tout nombre $b \in \mathbb{K}_+$, la série $\sum_{n\geq 0} r_n z^n$ est $\mathbb{K}_+$-rationnelle si, et seulement si, la série $\sum_{n\geq 0}(r_n/b^n)z^n$ l'est également. Cette transformation a pour effet, sur le polynôme minimal de changer, la variable z en bz.

Ces remarques étant faites, on transforme maintenant la série de la façon suivante : on la "déboîte" et on en extrait la série $\sum_{n\geq 0}(r_{np})z^n$ que l'on substitue dans l'étude qui suit à la série initiale, de telle sorte que pour $\epsilon > 0$ arbitrairement petit fixé, il existe un réel $b \in \mathbb{K}_+$ tel que les racines $\lambda, \lambda_1, \ldots, \lambda_{k-1}$ du nouveau polynôme P vérifient

$$\frac{\lambda}{b} > \frac{1}{\epsilon}, \qquad \frac{\lambda_i}{b} < \epsilon \quad (1 \leq i \leq k-1).$$

Comme le décalage d'indice conserve la rationalité, on peut faire un raisonnement analogue pour chacune des séries $\sum_{n\geq 0}(r_{np+i})z^n$ $(0 \leq i \leq p-1)$. De plus ϵ étant fixé,

$$M = \frac{\lambda}{\max_{1\leq i\leq p-1} \lambda_i} > 1,$$

on peut alors choisir p tel que $1/\epsilon^2 < M^p$ et tel qu'il existe $b \in \mathbb{K}_+$ vérifiant

$$\max_{1\leq i\leq p-1} \frac{\lambda_i^p}{\epsilon} < b < \lambda^p \epsilon.$$

Dans ces conditions, les racines de la série $\sum_{n\geq 0}(r_{np})z^n$ vérifient les inégalités souhaitées.

On change alors la variable z en bz et les racines du polynôme P satisfont alors

$$\lambda > \frac{1}{\epsilon}, \qquad \lambda_i < \epsilon \quad (1 \leq i \leq k-1).$$

On peut maintenant écrire le polynôme P sous la forme :

$$\begin{aligned} P(z) &= z^k - p_1 z^{k-1} - \cdots - p_k \\ &= (z^{k-1} - P_1 z^{k-2} - \cdots - P_{k-1})(z-1) - P_k, \end{aligned}$$

où $P_1, P_2, \ldots, P_k$ sont positifs et

$$\frac{p_1}{\lambda} + \frac{2p_2}{\lambda^2} + \cdots + \frac{kp_k}{\lambda^k} > 0. \tag{2.1}$$

En effet, en posant $P_0 = -1$, on a, pour $1 \leq i \leq k$,

$$p_i = P_i - P_{i-1},$$

et par suite

$$P_i = p_1 + p_2 + \cdots + p_i - 1.$$

De l'expression des coefficients d'un polynôme en fonction de ses racines, soit, avec $\lambda_0 = \lambda$, pour $1 \leq i \leq k$

$$p_i = (-1)^{i+1} \sum_{n_1 < n_2 < \ldots < n_i} \lambda_{n_1} \lambda_{n_2} \ldots \lambda_{n_i},$$

on déduit que

$$P_i = \lambda(1 - \sum \lambda_n + \sum \lambda_n \lambda_m - \cdots) + \Lambda(\lambda_1, \ldots, \lambda_{k-1}) - 1,$$

où Λ est un polynôme symétrique en $\lambda_1, \ldots, \lambda_{k-1}$. On obtient donc l'égalité

$$P_i = \lambda(1 - O(\epsilon)) + O(\epsilon) - 1,$$

dont on tire que tous les P_i sont strictement positifs quand ϵ est choisi suffisamment petit. L'inégalité (2.1) est alors satisfaite puisque le terme dominant du membre gauche est p_1/λ.

Soit maintenant, $R = \sum_{n \geq k} R_n z^n$ la série dont le terme général est défini par

$$R_n = r_n - p_1 r_{n-1} - \cdots - p_k r_{n-k}.$$

Si λ est racine simple de r, $R_n = 0$ pour tout $n \geq k$ puisque P est alors le polynôme minimal de la série r. Dans la cas contraire, soit $\overline{P}(z) = 1 - p_1 z - \cdots - p_k z^k$ le polynôme réciproque de P. On a

$$f_R(z) = f_r(z)\overline{P}(z) - T(z),$$

où T est un polynôme de degré au plus $k - 1$.

Comme la série r est $\mathbb{N}$-rationnelle, d'après la Proposition 6 (p.29), pour tout n suffisamment grand,

$$r_n = \sum_{0 \leq i \leq p} A_i(n) \alpha_i^n \quad \forall n \geq n_0,$$

où les α_i sont les inverses des pôles distincts de la fonction génératrice $f_r(z)$ de r et chaque A_i un polynôme de degré égal à la multiplicité du pôle $1/\alpha_i$ diminuée de 1. Soit a_0 le coefficient dominant du polynôme A_0, on a alors

$$r_n \sim_{n \to \infty} a_0 n^{m-1} \lambda^n.$$

Comme $r_n \geq 0$ et que r n'est pas un polynôme, $a_0 > 0$. On utilise alors la formule suivante :

$$\begin{aligned}(*) \qquad & n^j\alpha_i^n - q_1(n-1)^j\alpha_i^{n-1} - \cdots - q_q(n-q)^j\alpha_i^{n-q} \\ = \; & n^j\alpha_i^n(1 - \sum_{k=1}^{q}\frac{q_k}{\alpha_i^k}) + jn^{j-1}\alpha_i^n\sum_{k=1}^{q}\frac{kq_k}{\alpha_i^k} + B(n)\alpha_i^n,\end{aligned}$$

où B est un polynôme de degré $j-2$. On en déduit que, pour tout n suffisamment grand,

$$R_n = \sum_{0\leq i\leq p} B_i(n)\alpha_i^n.$$

Comme $1/\lambda$ est racine du polynôme $\overline{P}$, le polynôme B_0 est de degré $m-2$ et son coefficient dominant est alors, d'après $(*)$,

$$a_0(m-1)\lambda^n\sum_{i=1}^{k}\frac{ip_i}{\lambda^i}.$$

Comme, d'après (2.1), $\sum_{i=1}^{k}(ip_i/\lambda^i) > 0$, et que

$$R_n \sim_{n\to\infty} a_0(m-1)\lambda^n\sum_{i=1}^{k}\frac{ip_i}{\lambda^i}n^{m-2},$$

on en déduit que pour tout n suffisamment grand, R_n est positif.

A un décalage près des indices, la série R est alors $\mathbb{K}_+$-rationnelle d'après l'hypothèse d'induction ; par suite, il existe une représentation linéaire (L, M, C) de R à coefficients dans $\mathbb{K}_+$ telle que

$$\forall n > 0, \qquad R_{n+k} = LM^nC.$$

Enfin, le triplet (l, N, c) défini par

$$l = \left(\begin{array}{c} L \\ \hline s_{k-1} \\ \vdots \\ s_1 \\ r_0 \end{array}\right)^t, \quad N = \left(\begin{array}{c|cccccc} M & C & 0 & \dots & \dots & 0 \\ \hline 0 & P_1 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \vdots & 0 & \ddots & 0 \\ \vdots & P_{k-1} & \vdots & \vdots & \ddots & 1 \\ 0 & P_k & 0 & \dots & 0 & 1 \end{array}\right) \quad \text{et} \quad c = \left(\begin{array}{c} 0 \\ \vdots \\ 0 \\ 1 \end{array}\right),$$

où $s_n = r_n - r_{n-1}$.

Comme $\lim_{n\to\infty} r_{n-1}/r_n = 1/\lambda$, on peut supposer, quitte à décaler les indices d'un nombre approprié de rangs, que les nombres $s_{k-1}, \dots, s_1$ sont positifs.

On vérifie alors, par récurrence sur n, que, pour tout $n \geq 0$,

$$lN^n = (LM^n | s_{n+k-1}, \ldots, s_{n+1}, r_n). \tag{2.2}$$

Cette égalité est, par définition de l, vérifiée pour $n = 0$. De plus, on a

$$lN^{n+1} = (LM^{n+1} | * s_{n+k-1}, \ldots, s_{n+2}, r_{n+1}),$$

où la valeur du coefficient $*$ est

$$\begin{aligned} * &= LM^nC + P_1 s_{n+k-1} + \cdots + P_{k-1} s_{n+1} + P_k r_n \\ &= R_{n+k} - r_{n+k-1} + p_1 r_{n+k-1} + p_2 r_{n+k-2} + \cdots + g_k r_n \\ &= r_{n+k} - r_{n+k-1} = s_{n+k} \end{aligned}$$

On a ainsi établi par induction l'égalité (2.2). On en déduit que

$$r_n = lN^n c \quad \forall n \geq 0,$$

ce qui montre que la série r est $\mathbb{K}_+$-rationnelle et conclut la preuve du théorème de Soittola. □

En utilisant le théorème de Soittola, on obtient la caractérisation suivante des séries $\mathbb{N}$-rationnelles.

Proposition 7 *Une série $\mathbb{Z}$-rationnelle à coefficients positifs est $\mathbb{N}$-rationnelle si, et seulement si, c'est un emboîtement de séries $\mathbb{Z}$-rationnelles ayant une racine dominante.*

Démonstration : On rappelle que si K et L sont deux demi-anneaux tels que $K \subset L$, alors L est une *extension de Fatou* de K si toute série L-rationnelle à coefficients dans K est K-rationnelle.

D'après un résultat dû à Fliess ([Fli75]), $\mathbb{Q}_+$ est une extension de Fatou de $\mathbb{N}$, autrement dit, toute série $\mathbb{Q}_+$-rationnelle à coefficients entiers est $\mathbb{N}$-rationnelle. En utilisant le théorème de Soittola, on obtient alors qu'une série à coefficients entiers positifs est $\mathbb{N}$-rationnelle si et seulement si elle s'écrit comme emboîtement de séries $\mathbb{Q}$-rationnelles ayant une racine dominante. Mais, comme le lemme de Fatou ([Fat04]) stipule qu'une fraction rationnelle irréductible

$$\frac{P(z)}{Q(z)} \in \mathbb{Q}(z) \quad \text{telle que } Q(0) = 1$$

dont les coefficients du développement en série entière sont entiers est le quotient de deux polynômes à coefficients entiers, on en déduit qu'une série $\mathbb{Q}$-rationnelle à coefficients entiers est en fait $\mathbb{Z}$-rationnelle. On en conclut qu'une série à coefficients entiers positifs est $\mathbb{N}$-rationnelle si et seulement si c'est un emboîtement de séries $\mathbb{Z}$-rationnelles ayant une racine dominante. □

Exemple 13 Série $\mathbb{Z}$-rationnelle à coefficients positifs qui n'est pas $\mathbb{N}$-rationnelle.

Soit

$$s = \sum_{w \in (a+b)^*} (|w|_a - |w|_b)^2 w.$$

Cette série est $\mathbb{Z}$-rationnelle (comme carré d'Hadamard d'une série $\mathbb{Z}$-rationnelle) et à coefficients dans $\mathbb{N}$, mais elle n'est pas $\mathbb{N}$-rationnelle, sinon son support et son complémentaire seraient des langages rationnels, ce qui n'est pas le cas. En effet, le support de s est le langage des mots de $\{a, b\}^*$ dont le nombre d'occurrences de la lettre a n'est pas égal à celui de la lettre b, son complémentaire est, par suite, le langage de Dick

$$D = \{w \in \{a, b\}^* \mid |w|_a = |w|_b\},$$

qui n'est pas rationnel (cf. [BP85] par exemple).

Berstel et Mignotte ([BM75]) ont établi la calculabilité du nombre de séries à emboîter pour qu'aucune des racines des séries intervenant dans l'emboîtement ne soit de la forme $\rho\theta$ où ρ est un réel positif et θ une racine de l'unité différente de 1.

Puis Soittola ([Soi76]) a montré qu'il est possible de décider si une série $\mathbb{Z}$-rationnelle est $\mathbb{N}$-rationnelle.

Première partie

Hauteur d'étoile

Introduction

La notion de hauteur d'étoile d'un langage rationnel a été introduite par Eggan ([Egg63]) et a ensuite été étendue aux séries en plusieurs variables par Schützenberger. Le problème de sa calculabilité effective a été soulevé depuis le début de la théorie des automates. Ce qui suit s'attache à présenter la notion de hauteur d'étoile du point de vue algébrique, ainsi que son interprétation en terme d'automates.

La hauteur d'étoile d'un langage rationnel est le minimum des hauteurs d'étoile des expressions rationnelles qui le décrivent. Dans le cas d'un langage rationnel infini, il peut exister une infinité d'expressions rationnelles qui le représentent.

D'après un résultat dû à Eggan, la notion de hauteur d'étoile s'interprète en termes d'automates : soit $r(\mathcal{A})$ le nombre maximal de cycles imbriqués dans un automate $\mathcal{A}$, la hauteur d'étoile d'un langage donné est alors égale au minimum des entiers $r(\mathcal{A})$ quand $\mathcal{A}$ parcourt l'ensemble des automates reconnaissant ce langage. En ce sens, la hauteur d'étoile peut être considérée comme une mesure de la complexité en cycles du langage.

Mais, comme la hauteur d'étoile n'est pas une propriété syntactique, l'étude de l'automate minimal du langage ne donne qu'une borne supérieure pour la hauteur d'étoile du langage associé. McNaughton([McN67]) a cependant montré que celle-ci est donnée par l'automate minimal dans certains cas où le monoïde syntactique du langage est un groupe.

Dans le cas des langages formels, on sait que la hauteur d'étoile n'est pas bornée ([Egg63]) mais qu'elle est décidable : Hashiguchi a établi l'existence d'un algorithme pour la déterminer (la démonstration est présentée dans [Has89]).

En revanche, on ne dispose que de peu de résultats concernant les séries formelles. La notion de hauteur d'étoile s'interprète également en termes d'automates, de manière analogue au cas des langages, en considérant cette fois des automates avec multiplicité. Reutenauer a récemment prouvé ([Reu96]) que, si $\mathbb{K}$ est un corps, il existe, pour tout entier n, des séries $\mathbb{K}$-rationnelles en variables non-commutatives de hauteur d'étoile n. De plus, il existe alors une représentation minimale dont le nombre de cycles imbriqués est égal à la hauteur d'étoile de la série $\mathbb{K}$-rationnelle.

On étudie ici le cas des séries $\mathbb{N}$-rationnelles en une variable. On peut montrer que la hauteur d'étoile est, dans ce cas, inférieure à 2, d'après le théorème de Soittola. On donne une caractérisation des séries de hauteur d'étoile 1, dont on déduit une propriété de leurs racines positives. A la différence du théorème de Soittola, elle concerne toutes les racines positives de la série.

On établit enfin le résultat suivant (Théorème 17 p.78) : pour qu'une série $\mathbb{N}$-rationnelle soit de hauteur 1, il faut que toutes ses racines réelles positives soient des nombres d'Handelman ; de plus, cette condition est suffisante pour décider la hauteur d'étoile d'une série $\mathbb{N}$-rationnelle ayant une racine dominante.

Le chapitre 1 est consacré à la caractérisation des rayons spectraux des matrices compagnons irréductibles intégrales, qui sont les matrices grâce auxquelles on peut représenter tout automate dont les chemins fermés passent par un même état. On y donne une preuve complète d'un théorème d'Handelman (Théorème 9 p.56) qui traite de ce problème dans le cas primitif. En utilisant ce résultat, on caractérise (Théorème 10 p.59) ces rayons spectraux dans le cas irréductible. Ce dernier théorème joue un rôle central dans l'étude de la hauteur d'étoile des séries $\mathbb{N}$-rationnelles en une variable.

Le chapitre 2 porte sur le problème de la hauteur d'étoile. Après avoir récapitulé les résultats connus pour les langages rationnels, on présente les analogies entre séries et langages concernant cette question. On étudie ensuite en détail la hauteur d'étoile des séries $\mathbb{N}$-rationnelles en une variable. On établit en particulier un critère de décidabilité pour les séries ayant une racine dominante.

Les nouveaux résultats présentés dans cette partie (cf théorème 10 p.59 et section 2.3 p.76) ont fait l'objet d'une communication à STACS 96 ([Bas96]). L'article ([Bas97]) en donne un exposé plus complet.

Chapitre 1

Matrices compagnons irréductibles intégrales

Introduction

Ce chapitre est consacré à l'étude des matrices compagnons irréductibles intégrales. Ces matrices ont la propriété suivante : tout automate en pétales, *i.e.* automate dont tous les cycles passent par un même état, est équivalent à un automate dont le graphe est associé à une telle matrice. Dans la perspective de l'étude de la hauteur d'étoile des séries $\mathbb{N}$-rationnelles en une variable, on étudie le spectre de ces matrices et plus particulièrement leur rayon spectral. Dans le cas de matrices primitives, Handelman a montré ([Han92]) que ce sont exactement les entiers algébriques réels positifs λ dont tous les conjugués algébriques sont de module strictement inférieur à λ et dont aucun n'est un réel positif. A partir de ce résultat, on établit une caractérisation (Théorème 10 p.59) des rayons spectraux des matrices irréductibles, en d'autres termes, des entiers algébriques qui sont supérieurs au module de leurs conjugués et qui sont racines positives d'un polynôme de la forme :

$$x^k - \sum P_{k-i}x^i \qquad \text{où} \quad \forall i, P_i \in \mathbb{N}. \tag{1.1}$$

On prouve que ce sont exactement les entiers algébriques réels positifs dont une puissance entière est strictement supérieure aux modules de ses conjugués et n'a pas de conjugué algébrique réel positif.

Ces théorèmes ont un autre intérêt en théorie des automates. En effet, les polynômes définis par (1.1) correspondent aux ensembles de la forme $X^\star$ où X est un ensemble fini. La racine positive λ du polynôme est un paramètre important du langage formel $X^\star$: $\log \lambda$ est l'entropie de $X^\star$.

On expose ici une preuve complète du théorème d' Handelman (Théorème 9 p.56) en y apportant des compléments concernant, en particulier, les relations avec les polynômes log-concaves. On traite, dans un premier temps, le cas des polynômes ayant un changement de signe (Section 1.2 p.44). On présente ensuite les principales propriétés des polynômes

log-concaves (Section 1.3 p.48). La Section 1.4 (p.56) est consacrée au théorème d'Handelman, illustrée par quelques exemples (Section 1.5). On établit, dans la dernière section, une caractérisation du rayon spectral des matrices compagnons irréductibles intégrales (Théorème 10 p.59).

Ces théorèmes permettent, à partir d'un entier algébrique vérifiant des conditions adéquates, la construction d'un polynôme de la forme (1.1), mais la démonstration ne donne aucune indication sur les bornes éventuelles du degré de ce polynôme.

1.1 Préliminaires

Un *entier algébrique* est un nombre complexe λ racine d'un polynôme unitaire à coefficients entiers.

On appelle *nombre de Perron* tout nombre réel qui est un entier algébrique supérieur ou égal à 1 et strictement plus grand que les modules de ses conjugués algébriques.

D'après le théorème de Perron-Frobenius, une matrice irréductible M a une valeur propre simple λ positive et supérieure au module des autres valeurs propres. S'il existe p valeurs propres de module λ alors, d'après la Proposition 3 p.24, ce sont exactement les racines de l'équation $z^p - \lambda^p = 0$ et λ^p est rayon spectral de chacun des blocs diagonaux primitifs de M^p. On en déduit que λ^p est strictement supérieur à ses conjugués algébriques.

Si, de plus, la matrice est intégrale, alors λ, et *a fortiori* λ^p, sont des entiers algébriques et $\lambda \geq 1$, car le produit de λ et de ses conjugués algébriques est un entier ; λ^p est, par suite, un nombre de Perron et λ la racine $p$ième positive d'un nombre de Perron. Réciproquement, Lind a prouvé (se reporter à [Lin84]) que si λ est la $p$ième racine positive d' un nombre de Perron alors il existe une matrice irréductible intégrale dont le rayon spectral est λ. Il ne donne cependant pas de borne pour la taille de la matrice construite, Boyle ([Boy94]) a montré que si λ est de degré n, alors il existe une matrice de taille n à coefficients dans $z\mathbb{N}[z]$ ayant λ pour rayon spectral et dont le graphe associé est irréductible.

La *matrice compagnon* d'un polynôme unitaire P

$$P(x) = x^k - \sum_{j=0}^{k-1} P_{k-j} x^j$$

est la matrice carrée

$$C = \begin{pmatrix} P_1 & 1 & 0 & \dots & 0 \\ \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & 0 & \ddots & 0 \\ P_{k-1} & \vdots & \vdots & \ddots & 1 \\ P_k & 0 & 0 & \dots & 0 \end{pmatrix}$$

Le problème auquel on s'intéresse est le suivant : quels sont les entiers algébriques λ qui sont rayons spectraux d'une matrice compagnon irréductible intégrale (Figure 1.1) ?

Matrice compagnon

$$\begin{pmatrix} P_1 & 1 & 0 & \dots & 0 \\ \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & 0 & \ddots & 0 \\ P_{k-1} & \vdots & \vdots & \ddots & 1 \\ P_k & 0 & 0 & \dots & 0 \end{pmatrix}$$

Matrice à coefficients polynomiaux

$$\left(\sum_{i=1}^{k} P_i x^i \right)$$

Automate (en pétales) associé à un nombre d'Handelman

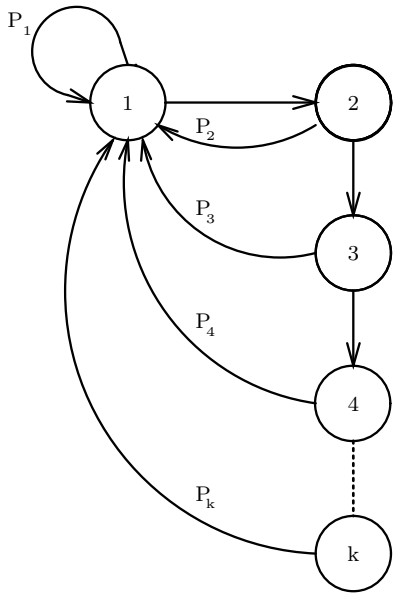


FIG. 1.1 – *Représentations associées aux nombres d'Handelman*

Le problème posé revient, en fait, à déterminer les racines *p*ièmes positives de nombres de Perron λ qui vérifient une équation de la forme

$$x^k = \sum P_{k-i} x^i$$

où les P_i sont des entiers naturels, la matrice étant positive, et P_k est strictement positif puisque la matrice est irréductible. On peut noter que, comme P_i est le nombre de chemins de longueur i dans le graphe associé à la matrice, la période de la matrice est égale au pgcd des indices i tels que P_i soit non nul ; la matrice est donc primitive si, et seulement si, ce pgcd est égal à 1.

De façon équivalente, cette condition sur l'entier algébrique λ peut aussi s'énoncer de la manière suivante : λ doit être la racine *p*ième positive d'un nombre de Perron et ne pas avoir de conjugué algébrique réel positif.

En effet, la fonction $\sum P_i x^i$ étant strictement croissante sur $\mathbb{R}_+$ ($P_k \neq 0$), le polynôme réciproque de P

$$\overline{P}(x) = 1 - \sum P_i x^i$$

a une unique racine positive $1/\lambda$.

Handelman a démontré que cette condition est suffisante quand λ est lui-même un nombre de Perron (Théorème 9 p.56). Pour cela, il montre qu'il est possible de construire, à partir de tout nombre de Perron λ qui n'a pas de conjugué algébrique réel positif, une matrice compagnon primitive intégrale de rayon spectral λ (Figure 1.2).

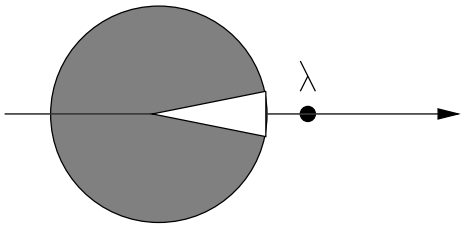


FIG. 1.2 – *Rayon spectral d'une matrice compagnon primitive*

On montre ensuite (Théorème 10 p.59) qu'une condition nécessaire et suffisante pour que λ, racine $p$ième positive d'un nombre de Perron, soit rayon spectral d'une matrice compagnon irréductible intégrale est que λ^p n'ait pas de conjugué algébrique réel positif. On appelle *nombre d'Handelman* les entiers algébriques réels positifs ainsi définis.

1.2 Cas des polynômes ayant un changement de signe

Un polynôme P à coefficients réels *a exactement un changement de signe* si la suite de ses coefficients non nuls a exactement un changement de signe.

Soit λ un nombre de Perron qui n'a pas de conjugué algébrique réel positif. Dans cette section, on construit une matrice compagnon primitive intégrale (de rayon spectal λ) à partir d'un polynôme ayant exactement un changement de signe et qui a pour racine λ (Lemme 2 p.46). On verra par la suite qu'il est toujours possible de se ramener à ce cas de figure.

On commence par établir un résultat de calcul matriciel (Lemme 1 p.44 et [Han81]) dont on aura besoin dans la construction qui est faite au Lemme 2 (p.46).

Soit A une matrice carrée à coefficients réels. On dit que A satisfait *la propriété de Perron faible* si A a une valeur propre simple r telle que, pour toute autre valeur propre $r' \in \mathbb{C}$ de A, on ait $r > |r'|$.

Le nombre réel r est appelée *valeur propre de Perron faible.*

Lemme 1 *Soit A une matrice carrée d'ordre n à coefficients réels. Alors A a une puissance entière dont tous les coefficients sont strictement positifs si, et seulement si,*

1. *A vérifie la propriété de Perron faible ;*
2. *Les vecteurs propres gauche et droit correspondant à la valeur propre de Perron faible peuvent être choisis strictement positifs.*

Démonstration : Si A ou une de ses puissances entières est à coefficients strictement positifs, le théorème de Perron-Frobenius (Théorème 5 p.22) et le Théorème 6 (p.23) conduisent à *1* et à *2*.

Réciproquement, on suppose vérifiées les conditions *1* et *2*. Soit r la valeur propre de Perron faible et soient v, w les vecteurs propres, respectivement gauche et droit, strictement positifs correspondant à la valeur propre r.

On pose $B = r^{-1}A$. Alors B a 1 pour valeur propre simple et toutes ses autres valeurs propres sont de module strictement inférieur à 1. La matrice B est semblable à la matrice

$$B' = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & J_1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & J_k \end{pmatrix}$$

d'après la décomposition de Jordan et

$$\lim_{m\to\infty} J_i^m = 0.$$

On obtient alors

$$\lim_{m\to\infty} B'^m = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & 0 \end{pmatrix} = B_0$$

et B_0 est une projection.

Par suite,

$$\lim_{m\to\infty} B^m = P$$

où P est une projection.

On va montrer que tous les coefficients de P sont strictement positifs. Comme v est une matrice-ligne et w une matrice-colonne, toutes deux strictement positives, vw est un scalaire strictement positif et wv une $n \times n$ matrice à coefficients strictement positifs, tout comme

$$Q = (vw)^{-1}wv.$$

La matrice Q ainsi définie est une projection, car $Q^2 = Q$.

Comme v et w sont les vecteurs propres respectivement gauche et droit de la matrice B associés à la valeur propre 1, $wvB^m = wv$; d'où par continuité $QP = Q$ et de façon similaire $Q = PQ$. On a donc

$$\ker P \subset \ker Q \quad \text{et} \quad \operatorname{Im} Q \subset \operatorname{Im} P.$$

Comme, de plus, les matrices P et Q sont de rang 1, on en déduit que $P = Q$. La matrice P est donc à coefficients strictement positifs.

Puisque la suite $(B^m)_{m\geq 1}$ converge vers une matrice à coefficients strictement positifs, toutes les puissances entières suffisamment grandes de B sont à coefficients strictement positifs et il en est de même pour la matrice A, ce qui achève la preuve du lemme. □

On peut maintenant prouver le résultat suivant :

Lemme 2 *Soit P un polynôme unitaire de degré n à coefficients entiers ayant exactement un changement de signe et tel que $P(0) \neq 0$. On suppose de plus que P a une seule racine réelle positive λ, que λ est racine simple et est supérieure au module des autres racines du polynôme P.*

Alors il existe un entier naturel N, $N \geq n$ et des entiers strictement positifs T_i tels que

$$\lambda^N = \sum_{i=0}^{n-1} P_{n-i}\lambda^i$$

et P divise, dans $\mathbb{Z}[x]$, le polynôme

$$x^N - \sum_{i=0}^{n-1} P_{n-i}x^i$$

Démonstration : Soit $P(x) = x^n - \sum_{i=0}^{n-1} p_{n-i}x^i$. Soit $(e_i)_{1\leq i\leq n}$ la base canonique de $\mathbb{Z}^n$ et soit C la matrice compagnon du polynôme P dans cette base. Alors

$$Ce_1 = \sum_{i=1}^{n} p_i e_i \quad \text{et} \qquad Ce_i = e_{i-1} \qquad \text{pour} \quad 2 \leq i \leq n-1.$$

On pose $v = Ce_n$. Le vecteur propre gauche de C pour la valeur propre λ est le vecteur

$$W = (\lambda^{n-1}, \lambda^{n-2}, \ldots, \lambda, 1)$$

(Ceci est vrai pour toute matrice compagnon et toute valeur propre).

Le vecteur propre droit pour la valeur propre λ est le vecteur colonne

$$V = (V_i)_{1\leq i\leq n}$$

où

$$\sum_{i=0}^{n-1} V_{i+1}x^i = \frac{P(x)}{(x-\lambda)}$$

et les V_i sont strictement positifs. En effet,

$$\forall 1 \leq i \leq n-1, \qquad V_i = \lambda^{n-i} - p_1\lambda^{n-i-1} - \cdots - p_{n-i-1}\lambda - t_{n-i} \quad \text{et} \quad V_n = 1.$$

Le polynôme P ayant exactement un changement de signe, il existe un entier naturel k, $0 \leq k \leq n-2$ tel que :

$$\begin{cases} p_{n-l} \leq 0 \text{ pour } l \geq k \\ p_{n-l} \geq 0 \text{ pour } l < k. \end{cases}$$

Si $i \geq k, V_i > 0$ de façon évidente. On suppose $i < k$. Alors,

$$\lambda^i V_i - P(\lambda) = \sum_{j=0}^{i} p_{n-j}\lambda^j > 0,$$

puisque $P(0) = p_n > 0$ et $p_{n-j} \geq 0$ pour $j < k$. Par conséquent, les vecteurs W et V sont strictement positifs.

Comme la matrice C vérifie la propriété de Perron faible, toutes les puissances suffisamment grandes de C sont à coefficients strictement positifs, d'après le Lemme 1. Il existe donc un entier naturel M tel que :

$$\text{pour } m \geq M, \quad C^{m+1}e_1 = \textstyle\sum_{i=1}^{n} P_i e_i$$

où les P_i sont des entiers strictement positifs. Alors, comme $Ce_i = e_{i-1}$

$$C^{m+n}e_1 = \sum_{i=0}^{n-1} P_{n-i}C^i e_1.$$

En appliquant le vecteur propre gauche W, on obtient :

$$(\lambda^{m+n} - \sum_{i=0}^{n-1} P_{n-i}\lambda^i)We_1 = 0.$$

Comme $We_1 \neq 0$, on en déduit que $\lambda^{m+n} = \sum_{i=0}^{n-1} P_{n-i}\lambda^i$.

De plus, pour $1 \leq j \leq n$,

$$C^{m+n}e_j = C^{m+n+j-1}e_1 = C^{n-j}\sum_{i=1}^{n} P_i e_i = \sum_{i=0}^{n-1} P_i C^{n-i}e_j.$$

On en déduit que la matrice C est racine du polynôme $x^{m+n} - \sum_{i=0}^{n-1} P_{n-i}x^i$.

Le polynôme P étant le polynôme minimal de C, car C est la matrice compagnon de P dans la base (e_i), et C étant racine du polynôme

$$x^{m+n} - \sum_{i=0}^{n-1} P_{n-i}x^i,$$

on en déduit que le polynôme P divise ce polynôme (dans $\mathbb{Z}[x]$), ce qui achève la preuve du Lemme 2. □

On a ainsi montré qu'à partir d'un polynôme qui a exactement un changement de signe et qui a pour racine un nombre de Perron λ n'ayant pas de conjugué algébrique réel positif, on peut construire une matrice compagnon primitive intégrale ayant pour rayon spectral λ.

1.3 Polynômes log-concaves

Les résultats qui suivent seront utilisés pour se ramener d'un polynôme P à coefficients entiers, ayant une seule racine réelle positive simple et supérieure aux modules des autres racines de P, à un polynôme vérifiant les hypothèses du Lemme 2 (p.46), c'est à dire ayant, de plus, exactement un changement de signe.

Remarque 6 En 1883, Poincaré (se reporter à [Poi83]) a démontré que si un polynôme P à coefficients réels a exactement n racines réelles positives, alors il existe un polynôme Q tel que le produit PQ ait exactement n changements de signes.

Dans le cas présent, on cherche à construire, pour $n = 1$, un polynôme unitaire Q à coefficients entiers ayant la même propriété et dont les racines ont un module strictement inférieur à celui module de la racine réelle positive du polynôme P.

Un polynôme P à coefficients réels (a_i) est *fortement unimodal* ou *log-concave* si

- tous ses coefficients sont positifs
- si $i < j < k$ et $a_i a_k \neq 0$ alors $a_j \neq 0$
- $\forall i, a_i^2 \geq a_{i-1} a_{i+1}$.

De nombreux résultats et exemples relatifs à la log-concavité sont donnés dans l'article de R.P. Stanley ([Sta89]).

Le résultat qui suit établit un lien entre les polynômes ayant un changement de signe et les polynômes log-concaves.

Lemme 3 *Si Q est un polynôme fortement unimodal à coefficients réels et si λ est un réel positif, alors le polynôme $(x - \lambda)Q$ a exactement un changement de signe.*

Démonstration : On peut écrire le polynôme Q sous la forme

$$Q = \sum_{i=n}^{m} a_i x^i.$$

On pose

$$r_i = \frac{a_{i-1}}{a_i} \qquad \text{pour} \quad n \leq i \leq m+1,$$

alors

$$\begin{cases} r_{m+1} = \infty \\ r_n = 0. \end{cases}$$

Comme le polynôme Q est log-concave, on a $r_{i+1} \geq r_i$ pour tout entier i. Alors il existe un entier I tel que $r_{I+1} \geq \lambda \geq r_I$.

Dans ces conditions, le coefficient de x^j dans le polynôme $(x-\lambda)Q$ est

$$\begin{cases} \text{positif pour } j > I \\ \text{négatif pour } j \leq I. \end{cases}$$

On a ainsi démontré que le polynôme $(x-\lambda)Q$ a exactement un changement de signe. □

Remarque 7 Le résultat correspondant pour deux réels positifs n'est pas valable. Il suffit pour s'en rendre compte de considérer le polynôme suivant :

$$(x-1)^2(x^2+1,9x+3) = x^4 - 3,9x^3 + 0,2x^2 - 4,1x + 3$$

qui a quatre changements de signe et non deux.

En revanche, la multiplication par des termes de la forme $(x+a)$, où $a > 0$, n'augmente pas le nombre de changements de signe.

Dans la suite, on considère un polynôme unitaire P à coefficients entiers ayant une seule racine réelle positive λ. On suppose de plus que λ est racine simple et strictement supérieure aux modules des autres racines de P.

On pose alors $Q(x) = P(x)/(x-\lambda)$. C'est un polynôme dont les coefficients sont réels, mais pas nécessairement entiers, et qui n'a pas de racine réelle positive. On va montrer que, pour tout entier M suffisamment grand, le polynôme

$$(1+x)^M Q$$

est log-concave (Proposition 8 p.56) ; dans ces conditions, le polynôme

$$(1+x)^M P$$

vérifie les hypothèses du Lemme 2 (p.46), ce qui permet d'achever la preuve (Théorème 9 p.56).

Pour prouver ce résultat, on utilise la propriété suivante :

Propriété 2 *Le produit de polynômes log-concaves est log-concave.*

Démonstration : Soient A et B deux polynômes log-concaves de degrés respectifs m et n. On pose

$$A(x) = \sum_{i=0}^{m} a_i x^i$$

et

$$B(x) = \sum_{i=0}^{n} b_i x^i.$$

On considère les deux matrices d'ordre $m+n$ suivantes, associées respectivement aux polynômes A et B,

$$\begin{pmatrix} a_0 & a_1 & \dots & a_{m+n} \\ 0 & \ddots & \ddots & \vdots \\ \vdots & 0 & \ddots & a_1 \\ 0 & \dots & 0 & a_0 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} b_0 & b_1 & \dots & b_{m+n} \\ 0 & \ddots & \ddots & \vdots \\ \vdots & 0 & \ddots & b_1 \\ 0 & \dots & 0 & b_0 \end{pmatrix}$$

avec la convention :

$$\begin{cases} a_i = 0 & \text{si } i > m \\ b_i = 0 & \text{si } i > n. \end{cases}$$

On peut noter que les relations sur les coefficients qui caractérisent les polynômes log-concaves correspondent à des mineurs d'ordre 2 des matrices ainsi associées aux polynômes.

Soit C la matrice produit AB. D'après la formule de Cauchy-Binet,

$$C\begin{pmatrix} i_1 & \dots & i_p \\ j_1 & \dots & j_p \end{pmatrix} = \sum_{1 \le k_1 < \dots < k_p \le m+n} A\begin{pmatrix} i_1 & \dots & i_p \\ k_1 & \dots & k_p \end{pmatrix} B\begin{pmatrix} k_1 & \dots & k_p \\ j_1 & \dots & j_p \end{pmatrix}$$

où M étant une matrice,

$$M\begin{pmatrix} l_1 & \dots & l_p \\ c_1 & \dots & c_p \end{pmatrix}$$

désigne le mineur d'ordre p de la matrice M formé des lignes $l_1, \dots, l_p$ et des colonnes $c_1, \dots, c_p$.

De plus, si $(d_0, \dots, d_p)$ est une suite log-concave de réels, alors

$$d_i d_j \ge d_{i-r} d_{j+r} \qquad \text{si } i \le j \text{ et } r \ge 0.$$

On utilise pour montrer ce résultat une double récurrence.

Pour $r = 0$, ce résultat est évident. Pour $r = 1$, on pose $j = i + p$. Pour $p = 0$, on obtient l'inégalité caractéristique des suites log-concaves. Pour $p = 1$, comme

$$d_i^2 \ge d_{i-1} d_{i+1} \text{ et } d_{i+1}^2 \ge d_i d_{i+2},$$

on a $d_i d_{i+2} \ge d_{i-1} d_{i+2}$. On suppose l'inégalité vérifiée au rang $p-2$, on va démontrer qu'alors elle est vraie au rang p. En effet,

$$d_i^2 d_{i+p}^2 \ge d_{i-1} d_{i+1} d_{i+p-1} d_{i+p+1}.$$

D'après l'hypothèse de récurrence,

$$d_{i+1} d_{i+p-1} \ge d_i d_{i+p}.$$

Donc $d_i d_{i+p} \ge d_{i-1} d_{i+p+1}$. L'inégalité est donc vraie pour $r = 1$.

On suppose $d_i d_j \geq d_{i-r} d_{i+r}$. D'après ce qui précède $d_i d_j \geq d_{i-1} d_{i+1}$ et, par hypothèse de récurrence, $d_{i-r-1} d_{j+r+1}$. On a ainsi prouvé le résultat annoncé.

Les matrices A et B étant associées à des polynômes log-concaves, on en déduit que tous les mineurs d'ordre 2 de ces matrices sont positifs. D'après l'expression donnée précédemment des mineurs de C en fonction de ceux de A et de B, tous les mineurs d'ordre 2 de C sont également positifs.

On en conclut que le polynôme AB est log-concave. □

Cette propriété permet ainsi de ramener le problème à la transformation de polynômes quadratiques, n'ayant pas de racine réelle, en polynômes log-concaves. (Les polynômes auxquels on s'intéresse ici n'ont en effet pas de racine réelle positive et les facteurs de la forme $(x + a)$ où $a > 0$ sont log-concaves).

Certains de ces polynômes sont déjà log-concaves. Plus exactement, les polynômes de la forme :

$$x^2 - 2xr \cos \alpha + r^2$$

sont log-concaves si, et seulement si, l'argument des racines est compris entre $2\pi/3$ et $4\pi/3$.

Pour établir le résultat (Lemme 5 p.53) de transformation de polynômes quadratiques en polynômes log-concaves, on prouve d'abord le lemme suivant :

Lemme 4 *Soient P et f deux polynômes non constants à coefficients réels. On suppose de plus que le polynôme $P(P(x) = \sum a_i x^i)$ n'est pas un monôme, que ses coefficients sont positifs et vérifient*

$$\textit{si } a_i \neq 0 \textit{ et } a_j \neq 0 \textit{ alors pour } i \leq k \leq j \ , \ a_k \neq 0.$$

Alors si $f(x)$ est strictement positif pour tout réel x strictement positif, il existe un entier positif N tel que $P^N f$ soit un polynôme à coefficients positifs

Démonstration : Il suffit de démontrer le résultat annoncé pour les polynômes P de la forme : $P(x) = a + bx$ avec $a, b > 1$. En effet, tout polynôme $P(x) = \sum a_i x^i$ vérifiant

– $\forall i$, $a_i \in \mathbb{R}_+$

– si $a_i \neq 0$ et $a_j \neq 0$ alors pour $i \leq k \leq j$, $a_k \neq 0$

peut s'écrire $P(x) = \frac{1}{M} \sum x^i (a_i + b_i x)$ où a_i, b_i sont des réels supérieurs à 1 et M un réel strictement positif.

En multipliant par une puissance convenablement choisie de x, on peut supposer que f est un polynôme et que $f(0)$ est non nul. On pose alors $\deg f = d$.

Soit S la limite du système inductif $(M_i, f_i^j)_{i,j \geq 0}$ où

$$\begin{cases} \forall i \in \mathbb{N}, & M_i & = \mathbb{R}[x] \\ \text{si} \quad i \leq j, & f_i^j : & M_i \longrightarrow M_j \\ & & Q \longrightarrow P^{j-i} Q \end{cases}$$

Dans ces conditions, $S = \mathbb{R}[x][P^{-1}]$.

L'anneau $\mathbb{R}[x]$ est un anneau partiellement ordonné ayant pour cône positif $\mathbb{R}_+[x]$. On définit sur S un ordre de la façon suivante :

$$\forall a \in \mathbb{R}[x], aP^{-k} \geq 0 \qquad \Leftrightarrow \qquad \exists n \in \mathbb{N} \quad \text{tel que} \quad aP^n \in \mathbb{R}_+[x].$$

Muni de cet ordre, S est un anneau partiellement ordonné. On peut remarquer que cet ordre ne coïncide pas avec l'ordre défini précédemment sur $\mathbb{R}[x]$, mais l'inclusion de $\mathbb{R}[x]$ dans S préserve l'ordre.

On définit maintenant la notion d'idéal d'un groupe partiellement ordonné G pour poursuivre la preuve. On dit qu'un sous-groupe H est un *idéal d'ordre* ("order-ideal") de G si, en posant $H^+ = H \cap G$, on a $H = H^+ - H^+$ et si $0 \leq g \leq h$, h étant un élément de H, alors g appartient à H. D'autre part, un élément u de G est une *unité d'ordre* ("order-unit") pour G si u est positif et si pour tout g appartenant à G, il existe un entier naturel N tel que $g \leq Nu$.

Soit R le plus petit idéal de S contenant 1 (1 est, dans ce cas, une unité d'ordre pour R), alors

$$R = \{s \in S \mid \exists N \in \mathbb{N}, -N \leq s \leq N\} = \mathbb{R}[x^w P]_{w \in J}$$

où $J = \{w \in \mathbb{Z} \mid x^w \leq P\}$, *i.e.*, J est l'ensemble des entiers w tels que x^w est un monôme qui apparaît dans P. De plus, le cône positif R^+ de R est engendré additivement et multiplicativement par $\{x^w P^{-1} \mid w \in J\}$. La preuve de ces résultats est donnée dans [Han85] (Théorème I.4).

Pour démontrer qu'il existe un entier naturel N tel que $P^N f$ soit à coefficients positifs, il suffit de prouver qu'il existe un entier d tel que fP^{-d} appartienne à R^+, car alors fP^{-d} appartiendra à S^+ et on en déduira que le polynôme fP^N, pour un certain entier N, est à coefficients positifs.

On introduit des notions qui interviennent dans la suite de la démonstration. On appelle *état* d'un groupe partiellement ordonné G tout homomorphisme, défini sur G, qui préserve l'ordre et qui est à valeurs dans $\mathbb{R}$. Un état ϕ est *normalisé* à u, une unité d'ordre fixée, si, de plus, $\phi(u) = 1$. Dans l'ensemble des états normalisés de G, un état ϕ est un *état pur* si, et seulement si, ϕ_1 et ϕ_2 étant des états normalisés,

$$\phi = \frac{\phi_1 + \phi_2}{2} \quad \Rightarrow \quad \phi = \phi_1 = \phi_2.$$

On peut maintenant énoncer les deux résultats suivants :

1. Dans un groupe partiellement ordonné possédant une unité d'ordre, un élément est positif si son image par tout état pur est strictement positive.

2. Dans un groupe partiellement ordonné ayant 1 pour unité d'ordre, tous les états sont multiplicatifs.

Dans le cas présent,

$$R = \mathbb{R}[(a+bx)^{-1}; x(a+bx)^{-1}]$$

et a pour cône positif $\{\sum X^i Y^j\}$ où

$$X = (a+bx)^{-1} \qquad \text{et} \qquad Y = x(a+bx)^{-1}.$$

On a alors $aX + bY = 1$. De plus, comme $S = R[P]$, les états purs de S sont exactement les extensions multiplicatives des états purs de R qui associent à P^{-1} une valeur non nulle (cf.[Han85] Théorème I.3). On en déduit que si α est un état pur de R qui n'est pas la restriction d'un état multiplicatif de S, $\alpha(P^{-1}) = 0$ et, par suite, $X \in \ker\alpha \cap R^+$. On en déduit que $R/\ker\alpha$ est isomorphe à $\mathbb{R}[1/b]$. Il existe donc au plus un tel état pur et celui-ci est donné par

$$X \longrightarrow 0 \qquad Y \longrightarrow \frac{1}{b}.$$

On obtient alors que $\alpha(Q) = \lim_{t\to\infty} Q(t)$ (comme α est multiplicatif, d'après (2), il suffit de vérifier que cela est vrai pour X et Y, ce qui est immédiat).

Par hypothèse, $f(\mathbb{R}_+) \subset \mathbb{R}_+^*$ et f est bornée inférieurement et supérieurement par un multiple de P^d (puisque $\deg f = d$), par conséquent, fP^{-d} appartient à R . De plus,

$$\alpha(fP^{-d}) = \lim_{t\to\infty} fP^{-d}(t) = \frac{f^{(d)}(0)}{d!b}$$

et comme $\deg f = d$, $f^{(d)}(0) > 0$ (car $f(\mathbb{R}_+) \subset \mathbb{R}_+^\star$). Par suite, fP^{-d} a une image strictement positive par tout état pur de R (les autres états purs sont les évaluations en un point de $\mathbb{R}_+$), ce qui prouve, d'après (1) que fP^{-d} appartient à R^+.

On obtient ainsi le résultat cherché : pour un certain entier naturel N, le polynôme $P^N f$ est à coefficients positifs. □

On peut maintenant démontrer l'énoncé suivant qui permet, à partir d'un polynôme quadratique n'ayant pas de racine réelle, d'obtenir un polynôme fortement unimodal.

Lemme 5 *Soient d et e deux réels tels que $d^2 < 4e$ et soit f le polynôme*

$$f(x) = x^2 - dx + e,$$

alors il existe un entier naturel N tel que $(1+x)^N f$ soit un polynôme log-concave.

Remarque 8 Il est équivalent de considérer le polynôme

$$x - d + ex^{-1}$$

On le fait ici pour des raisons de commodité dans les calculs.

Démonstration : La condition sur les coefficients du polynôme assure que

$$\forall x > 0 \qquad f(x) > 0.$$

On déduit du Lemme 4 (p.51) qu'il existe un entier n_0 tel que si $n \geq n_0$ le polynôme $(1+x)^n f$ est à coefficients strictement positifs.

On note alors P_n le polynôme $(1+x)^n$ et

$$P_n(x) = \sum_{i=0}^{n} C_n^i x^i = \sum_{i=0}^{n} a_i x^i.$$

On note (Q, x^k) le coefficient de x^k dans le polynôme Q. Alors, pour tout entier positif $k, 1 \leq k \leq n-1$, on a

$$(P_n f, x^k) = (a_{k-1} - a_k d + a_{k+1} e) = a_k(\frac{k}{n-k+1} - d + e\frac{n-k}{k+1})$$

et $a_k^2/a_{k+1}a_{k-1} = (1+1/k)(1+1/(n-k))$. On pose alors $t = k/n$ et on définit la fonction $G_n(t)$ sur l'intervalle $[0,1]$ par :

$$G_n(t) = \frac{tn}{n(1-t)+1} - d + e\frac{n(1-t)}{nt+1}.$$

On montre, pour commencer, que, pour tout entier n suffisamment grand, pour tout réel $\delta \geq 2/n$ et tout t de l'intervalle $[\delta, 1-\delta]$,

$$G_n^2(t)(1+\frac{1}{k})(1+\frac{1}{(n-k)}) > G_n(t+\frac{1}{n})G_n(t-\frac{1}{n}).$$

Cette inégalité est équivalente, pour tout n suffisamment grand et pour tout entier k tel que $\delta n \leq k \leq (1-\delta)n$, à

$$(P_n f, x^k)^2 > (P_n f, x^{k+1})(P_n f, x^{k-1}),$$

ce qui démontre alors la log-concavité des coefficients du polynôme $P_n f$ pour $2 \leq k \leq n-2$. On vérifie ensuite la validité de cette inégalité pour $k=0$, $k=1$, $k=n-1$ et $k=n$.

Dans un premier temps, on suppose le réel δ fixé et $2/n \leq \delta \leq t$ et $t \leq 1-\delta$. (On peut faire croître n autant que l'on veut car si $n' \geq n$, $P_{n'} f$ est aussi à coefficients positifs).

On calcule alors $G_n(t-1/n) - G_n(t)$. On a

$$\begin{aligned} G_n(t-\frac{1}{n}) - G_n(t) &= \frac{tn-1}{n(1-t)+2} - \frac{tn}{n(1-t)+1} \\ &\quad + e(\frac{n(1-t)+1}{nt} - \frac{n(1-t)}{nt+1}) \\ &= -\frac{n+1}{(n(1-t)+2)(n(1-t)+1)} + e\frac{n+1}{nt(nt+1)} \\ &= \frac{1}{n}(-\frac{1}{(1-t)^2} + \frac{e}{t^2}) + O(\frac{1}{n^2}). \end{aligned}$$

Le terme en O vient du fait que t est borné : $2/n \leq \delta \leq t \leq 1-\delta$. On en déduit

$$G_n(t-\frac{1}{n}) = G_n(t) + \frac{1}{n}(-\frac{1}{(1-t)^2} + \frac{e}{t^2}) + O(\frac{1}{n^2})$$

et, en remplaçant t par $t+1/n$ dans l'égalité précédente, on obtient :

$$G_n(t+\frac{1}{n}) = G_n(t) + \frac{1}{n}(\frac{1}{(1-t)^2} - \frac{e}{t^2}) + O(\frac{1}{n^2}).$$

Par conséquent,

$$G_n(t+\frac{1}{n})G_n(t-\frac{1}{n}) = G_n^2(t) + O(\frac{1}{n^2}).$$

En effet, les termes en $G_n(t)/n$ s'annulent et les termes en $G_n(t)O(1/n^2)$ sont eux-mêmes $O(1/n^2)$ car les fonctions G_n sont uniformément bornées sur l'intervalle $[\delta, 1-\delta]$:

$$0 \leq G_n(t) \leq \frac{1-\delta}{\delta}(1+e) - d.$$

De plus, les fonctions G_n convergent uniformément en n sur l'intervalle $[\delta, 1-\delta]$ vers $t/(1-t) - d + e(1-t)/t$, donc, pour tout n suffisamment grand, G_n est bornée inférieurement par un réel strictement positif sur l'intervalle $[\delta, 1-\delta]$ ($x - d + ex^{-1} > 0$ pour $x > 0$).

On a alors, pour tout n suffisamment grand,

$$G_n^2(t)(1+\frac{1}{tn})(1+\frac{1}{n(1-t)}) > G_n^2(t)(1+\frac{1}{nt}) > G_n^2(t) + O(\frac{1}{n^2})$$

car $0 < 1/nt < 1/n\delta$ et $1/n$ est infiniment plus grand que $1/n^2$.

On a donc montré que, pour $\delta \leq t \leq 1-\delta$,

$$G_n^2(t)(1+\frac{1}{nt})(1+\frac{1}{n(1-t)}) > G_n(t-\frac{1}{n})G_n(t+\frac{1}{n}),$$

c'est à dire pour tout entier k tel que $2 \leq k \leq n-2$, on a

$$(P_n f, x^k)^2 > (P_n f, x^{k+1})(P_n f, x^{k-1}).$$

Il reste à prouver cette inégalité quand k prend les valeurs 0, 1, $n-1$ et n. Or,

$$(P_n f, 1)^2 - (P_n f, x^{-1})(P_n f, x) \sim_\infty \tfrac{e^2 n^2}{2},$$

$$(P_n f, x)^2 - (P_n f, x^1)(P_n f, x^2) \sim_\infty \tfrac{e^2 n^4}{12},$$

$$(P_n f, x^{n-1})^2 - (P_n f, x^{n-2})(P_n f, x^n) \sim_\infty \tfrac{n^4}{12},$$

$$(P_n f, x^n)^2 - (P_n f, x^{n-1})(P_n f, x^{n+1}) \sim_\infty \tfrac{n^2}{2}.$$

Pour tout n suffisamment grand, ces grandeurs sont donc strictement positives, ce qui démontre la log-concavité des coefficients de $P_n f$ dans le cas où $k = 0, k = 1, k = n-1$ et $k = n$.

On a donc établi que le polynôme $P_n f$ est log-concave pour tout n suffisamment grand, ce qui achève la preuve du Lemme 5. □

On peut maintenant établir le résultat de transformation de polynômes n'ayant pas de racine réelle positive en polynômes log-concaves.

Proposition 8 *Si f est un polynôme à coefficients réels n'ayant pas de racine réelle positive à valeurs positives sur $\mathbb{R}_+$ alors il existe un entier naturel N tel que le polynôme $(1+x)^N f$ soit log-concave.*

Démonstration : On factorise le polynôme f en un produit de polynômes linéaires et quadratiques. Les polynômes linéaires ne peuvent provenir que des racines réelles négatives. On applique alors le Lemme 5 (p.53) aux polynômes quadratiques et on utilise le fait que le produit de polynômes log-concaves est log-concave (Propriété 2 p.49) pour conclure. □

On a ainsi prouvé qu'on peut, à partir d'un polynôme n'ayant pas de racine réelle et qui est à valeurs positives sur $\mathbb{R}_+$, se ramener à un polynôme log-concave. Ceci permet de transformer les polynômes auxquels on s'intéresse en polynômes ayant un changement de signe.

1.4 Théorème d'Handelman

Avec les résultats des sections précédentes, on peut maintenant prouver le théorème d'Handelman.

Théorème 9 (Handelman) *Soit P un polynôme unitaire de degré n à coefficients entiers et tel que $P(0) \neq 0$. On suppose que P a une seule racine réelle positive λ, que λ est racine simple et strictement supérieure aux modules des autres racines de P. On a alors*

1. *Pour tout entier N suffisamment grand, le polynôme*

$$(1+x)^N P$$

   a exactement un changement de signe.

2. *Pour tout entier M suffisamment grand, il existe des entiers strictement positifs T_i tels que*

$$\lambda^{N+M+n} = \sum_{i=0}^{N+n-1} T_i \lambda^i.$$

3. La matrice compagnon du polynôme

$$C = x^{N+M+n} - \sum_{i=0}^{N+n-1} T_i x^i$$

est primitive, a pour rayon spectral λ et P divise le polynôme C dans $\mathbb{Z}[x]$.

Remarque 9 Si $\lambda = 1$, nécessairement $P = (x-1)$. Il n'y a alors aucune transformation à opérer et le résultat est obtenu directement.

Démonstration : Soit $Q = P/(x-\lambda)$. Pour tout entier naturel N suffisamment grand le polynôme $(1+x)^N Q$ est fortement unimodal d'après la Proposition 8 (p.56). De plus, d'après le Lemme 3 (p.48), le polynôme

$$(x-\lambda)(x+1)^N Q = (x+1)^N P$$

a alors exactement un changement de signe, ce qui prouve *1.*

On obtient *2* en appliquant le Lemme 3 (p.48) au polynôme $(x+1)^N P$.

Enfin, la matrice compagnon du polynôme C est primitive, a λ pour rayon spectral par construction et P divise le polynôme C dans $\mathbb{Z}[x]$, d'après le Lemme 3 (p.48). □

On peut ainsi construire des matrices compagnons primitives intégrales de rayon spectral donné λ. Pour cela, λ doit être un nombre de Perron qui n'a pas de conjugué algébrique réel positif (cf. Figure 1.2 p.44).

1.5 Quelques exemples

On considère un nombre de Perron n'ayant pas de réel positif pour conjugué algébrique. Soit P son polynôme minimal ; P est un polynôme de degré n à coefficients entiers ayant une seule racine réelle positive qui est simple et supérieure aux modules des autres racines de P.

Dans un premier temps, on détermine le plus petit entier N tel que le polynôme

$$(1+x)^N P$$

ait un changement de signe. Soit C la matrice compagnon du polynôme $(1+x)^N P$. On calcule alors le plus petit entier M tel que C^{M+1} soit à coefficients strictement positifs. L'entier $M+1$ est inférieur ou égal au carré du degré du polynôme $(1+x)^N P$. La matrice cherchée est la matrice compagnon du polynôme unitaire de degré $n+N+M-1$ dont les coefficients sont déterminés par les éléments de la dernière colonne de la matrice C^{M+1}.

1.5.1 Nombres de Perron de degré 2

Dans le cas où le nombre de Perron que l'on considère est un entier algébrique λ de degré 2, son polynôme minimal est de la forme :

$$P(x) = x^2 - ax - b$$

où a et b sont des entiers naturels. En effet, soit λ' l'autre racine du polynôme P, $\lambda' \in \mathbb{R}_-^\star$ et $|\lambda'| < |\lambda|$, alors $a = \lambda + \lambda'$ et $b = -\lambda\lambda'$ sont strictement positifs. Le polynôme P a exactement un changement de signe, sa matrice compagnon est la matrice

$$C = \begin{pmatrix} 0 & b \\ 1 & a \end{pmatrix}$$

dont le carré :

$$C^2 = \begin{pmatrix} b & ab \\ a & (b + a^2) \end{pmatrix}$$

a ses coefficients strictement positifs. La matrice que l'on obtient dans ce cas est la matrice compagnon du polynôme

$$T(x) = x^3 - (a^2 + b)x - ab$$

Le résultat est immédiat.

1.5.2 Nombres de Perron de degré supérieur à 2

L'algorithme de construction d'une matrice compagnon primitive intégrale est beaucoup plus intéressant quand on considère un nombre de Perron de degré strictement supérieur à deux. Ce problème peut nécessiter, dès le degré 3, un grand nombre de calculs comme le montrent les exemples qui suivent. La question reste ouverte de l'existence d'une borne pour la dimension de la matrice construite. Ce problème se ramène en fait à la question suivante : les valeurs que prend l'entier N tel que $(1+x)^N P$ ait un changement de signe sont-elles bornées ?

Exemple 14 Soit P le polynôme

$$P(x) = x^3 - 3x^2 + 3x - 4.$$

Le polynôme $(1 + x)P = x^4 - 2x^3 - x - 4$ a alors un changement de signe. La matrice compagnon du polynôme $(1 + x)P$ élevée à la puissance 5 est à coefficients strictement positifs et la matrice obtenue est la matrice compagnon du polynôme

$$T(x) = x^8 - 60x^3 - 25x^2 - 60x - 96.$$

Exemple 15 Soit P le polynôme

$$P(x) = x^3 - 6x^2 + 12x - 13.$$

Le polynôme $(1+x)^5 P$ a alors un changement de signe. La matrice compagnon du polynôme $(1+x)^5 P$ élevée à la puissance 9 est alors à coefficients strictement positifs et la matrice obtenue est la matrice compagnon d'un polynôme de degré 16.

Exemple 16 Soit P le polynôme

$$P(x) = x^5 - 5x^4 + 10x^3 - 10x^2 + 5x - 4.$$

Le polynôme $(1+x)^{12} P$ a alors un changement de signe. La matrice compagnon du polynôme $(1+x)^{12} P$ élevée à la puissance 43 est alors à coefficients strictement positifs et la matrice obtenue est la matrice compagnon d'un polynôme de degré 59.

1.6 Matrices compagnons irréductibles intégrales

On établit à partir du résultat d'Handelman une caractérisation des rayons spectraux des matrices compagnons irréductibles intégrales. On en donne également une interprétation en termes d'automates. Les nombres ainsi déterminés jouent un rôle central dans l'étude de la hauteur d'étoile des séries $\mathbb{N}$-rationnelles que l'on étudie dans le prochain chapitre (Section 2.3 p.76).

Théorème 10 *Soit λ un nombre réel strictement positif, λ est racine d'un polynôme de la forme : $x^n - \sum a_i x^i$ où les a_i sont des entiers naturels et a_0 non nul si, et seulement si, λ vérifie les conditions suivantes*

$$\exists k \text{ tel que } \begin{cases} \lambda^k \text{ soit un nombre de Perron} \\ \lambda^k \text{ n'a pas de conjugué algébrique réel positif.} \end{cases}$$

On appellera dorénavant *nombres d'Handelman* les nombres réels positifs vérifiant les conditions du Théorème 10.

Démonstration : Soit $P(x)$ le polynôme $x^n - \sum_{i=0}^{n-1} P_i x^i$ où les P_i sont des entiers naturels et P_0 non nul. Le polynôme P a une unique racine réelle positive λ qui n'a donc pas de conjugué algébrique réel positif. De plus, les conjugués λ_j de λ sont racines du polynôme P et ont donc un module inférieur à λ, en cas d'égalité λ_j s'écrivant $\lambda\theta$ où θ est une racine de l'unité. Soit k l'ordre commun de ces racines de l'unité, alors λ^k est un

nombre de Perron et k est la période de la matrice compagnon du polynôme P. De plus, si

$$P(x) = x^n - \sum_{n_1>\cdots>n_j} P_{n_i} x^{n_i} - P_0,$$

où $(P_{n_1}, P_{n_2}, \ldots, P_{n_j})$ est la sous-suite des nombres strictement positifs extraite de la suite $(P_i)_{1\leq i\leq n-1}$, l'indice k est alors le plus grand commun diviseur des différences

$$n - n_1, n_1 - n_2, \ldots, n_j - 0,$$

d'après la Proposition 4 (p.25). Par suite, tous les exposants non nuls qui apparaissent dans le polynôme P sont des multiples de k et l'on peut effectuer le changement de variable $y = x^k$. On obtient alors le polynôme $y^{n/k} - \sum_{i=0}^{n-1} P_i y^{i/k}$, on en déduit que λ^k n'a pas de conjugué algébrique réel positif. L'unique racine réelle positive du polynôme P est donc un nombre d'Handelman.

Réciproquement, soit λ un nombre d'Handelman. Soit P le polynôme minimal de λ^k, P est un polynôme unitaire de degré n à coefficients entiers tel que $P(0) \neq 0$ puisque $\lambda^k \neq 0$. Comme λ^k est un nombre de Perron qui n'a pas de conjugué algébrique réel positif, d'après le théorème d'Handelman (p.56), il existe un polynôme

$$C_0(x) = x^m - \sum_{i=0}^{m-1} p_i x^i$$

où les p_i sont des entiers naturels, tel que la matrice compagnon du polynôme C_0 soit primitive.

Le polynôme C défini par

$$C(x) = C_0(x^k)$$

est alors le polynôme cherché, ce qui achève la démonstration du théorème. □

Corollaire 2 *Soit M une matrice intégrale non nulle et irréductible dont le rayon spectral λ est un nombre d'Handelman et soit P son polynôme caractéristique. Alors il existe, dans l'idéal $P\mathbb{Z}[x]$, un polynôme*

$$C(x) = x^n - \sum P_i x^i, \qquad P_i \in \mathbb{N}, \quad C(0) \neq 0$$

dont la matrice compagnon est irréductible et a pour rayon spectral λ.

Démonstration : Soit P le polynôme caractéristique de la matrice M et soit k la période de la matrice M. L'entier k est alors le plus grand commun diviseur de toutes les différences entre deux exposants qui apparaissent consécutivement dans le polynôme P. Par suite, tous les exposants non nuls du polynôme P sont divisibles par k, ce qui permet d'effectuer le changement de variable $y = x^k$ dans le polynôme P. Le polynôme ainsi obtenu vérifie alors les conditions du théorème d'Handelman (p.56) dont l'application conduit au résultat

annoncé. Il suffit pour obtenir la matrice cherchée de faire le changement de variable réciproque. □

Les nombres d'Handelman sont exactement les nombres qui peuvent être rayons spectraux de matrices compagnons irréductibles intégrales (Figure 1.1).

Les matrices associées étant irréductibles, les automates sont donc de graphe fortement connexe. De plus, les automates associés possèdent une propriété remarquable : tous les cycles passent par un même état et tout automate en pétales étiqueté sur un alphabet réduit à une lettre et avec multiplicité dans $\mathbb{N}$ est équivalent à un tel automate. C'est à cette spécificité que l'on s'intéressera dans la suite.

Les *automates en pétales* sont exactement les automates finis dont tous les cycles passent par un même sommet, ce sont donc les automates de rang cyclique 1.

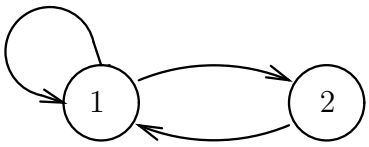


FIG. 1.3 – *Automate en pétales.*

Si $\mathcal{A}$ est un automate en pétales dont tous les cycles passent par le sommet 1, alors $\mathcal{A}$ est équivalent à un automate dont l'unique composante fortement connexe du graphe des états est de la forme suivante (Figure 1.4). Pour tout i, l'entier P_i est égal au nombre de cycles de longueur i ayant pour extrémités l'état 1 dans l'automate initial $\mathcal{A}$.

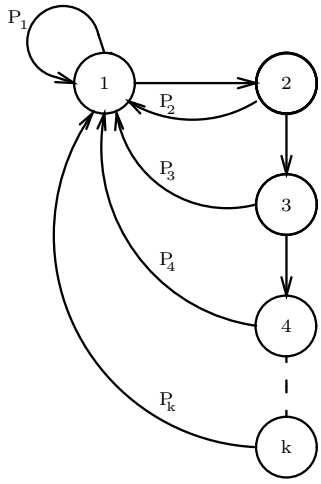


FIG. 1.4 – *Automate (en pétales) associé à un nombre d'Handelman*

Chapitre 2

Hauteur d'étoile

Introduction

En 1963, Eggan a introduit la notion de hauteur d'étoile (cf. [Egg63]) des expressions rationnelles définies à l'aide des opérateurs de l'union, de la concaténation et de l'étoile. Cette hauteur est égale au nombre d'étoiles superposées dans l'expression considérée.

Par définition, la hauteur d'étoile d'un langage rationnel est égale au plus petit nombre d'étoiles superposées dans une expression rationnelle qui le représente. Cependant, il peut exister une infinité d'expressions rationnelles qui décrivent un même langage rationnel.

La notion de hauteur d'étoile peut être interprétée en termes d'automates : la hauteur d'étoile d'un langage rationnel est égale au nombre minimal de cycles imbriqués dans un automate qui reconnaît ce langage. En ce sens, la hauteur d'étoile est une mesure de la complexité en cycles du langage. Mais, la hauteur d'étoile n'étant pas une propriété syntactique, elle ne peut être calculée à partir de l'automate minimal.

Eggan a montré, dans l'article précédemment cité, que, pour tout entier naturel k, il existe un langage rationnel de hauteur d'étoile k et a soulevé le problème de la calculabilité de la hauteur d'étoile. En 1966, Dejean et Schützenberger (cf. [DS66]) ont prouvé que, pour tout entier naturel k, il existe des langages rationnels de hauteur d'étoile exactement k sur un alphabet à deux lettres. En 1967, McNaughton (cf. [McN67]) a donné un algorithme pour déterminer la hauteur d'étoile d'un langage rationnel dont le monoïde syntactique est un groupe. Enfin, Hashigushi a trouvé en 1982 un algorithme permettant de décider si un langage rationnel est de hauteur d'étoile 1 ([Has82]), et en 1989 un algorithme permettant de décider la hauteur d'étoile dans le cas général (cf. [Has89] et [Has88]).

On a vu précédemment que les séries $\mathbb{N}$-rationnelles en une variable peuvent être définies comme des langages rationnels avec multiplicité sur un alphabet réduit à une unique lettre et que le coefficient d'ordre n est alors le nombre de chemins de longueur n dans graphe orienté G (le graphe orienté des états de l'automate associé). Soit $h(G)$ le nombre maximum de cycles nécessairement imbriqués du graphe G. La hauteur d'étoile s'interprète alors comme le minimum parmi les entiers $h(G)$ quand G décrit l'ensemble des graphes représentant une même série. Ainsi, les séries de hauteur nulle sont associées

aux graphes acycliques et se réduisent aux polynômes.

Une conséquence du théorème de Soittola (Théorème 8 p.30) est qu'une série $\mathbb{N}$-rationnelle en une variable est au plus de hauteur d'étoile 2. Ce résultat a été obtenu indépendamment par Katayama, Okamoto et Enomoto ([KOE78]) par des méthodes différentes.

Dans ce qui suit, on établit une propriété des séries de hauteur 1 qui se révèle être suffisante pour décider la hauteur d'étoile d'une classe importante de séries. A la différence du théorème de Soittola, la condition que l'on donne ne porte pas uniquement sur la plus grande racine réelle positive de la série, mais sur l'ensemble de ses racines réelles positives.

La hauteur d'étoile des séries en une variable est liée à diverses notions, en particulier à celle de représentation par une matrice à coefficients polynomiaux. Toute série de la classe à laquelle on s'intéresse plus spécialement dans ce qui suit (série $\mathbb{N}$-rationnelle ayant une racine dominante) peut être représentée par une matrice à coefficients polynomiaux dans $z\mathbb{N}[z]$, triangulaire par blocs et dont les blocs diagonaux sont carrés de dimension 2. On donne également une caractérisation des séries de hauteur d'étoile 1 à l'aide de leur représentation par des matrices à coefficients polynomiaux (pour une présentation générale des matrices à coefficients polynomiaux on se reportera à la synthèse de Boyle [Boy94]).

La première partie de chapitre récapitule les résultats connus pour les langages rationnels. La suivante présente le problème de la hauteur d'étoile des séries rationnelles en plusieurs variables non-commutatives par analogie avec le cas des langages. La section 2.3 (p.76) est entièrement consacrée à l'étude du problème de la hauteur d'étoile des séries $\mathbb{N}$-rationnelles en une variable.

2.1 Langages rationnels

On définit la hauteur d'étoile d'un langage rationnel, on introduit la notion de rang cyclique d'un automate ainsi que son analogue en termes matriciels. Muni de ces notions, on donne une interprétation de la hauteur d'étoile au moyen des automates ; enfin, on récapitule les résultats connus.

2.1.1 Définitions

On définit la *hauteur d'étoile* d'une expression rationnelle comme le nombre maximal d'étoiles "superposées" dans l'expression. Formellement, elle est définie, sur l'ensemble

des expressions rationnelles non nulles, comme une fonction à valeurs dans $\mathbb{N}$ par

$$h(1) = 0,$$

$$h(a) = 0 \quad \text{si} \quad a \in A,$$

$$h(X + Y) = h(XY) = \max\{h(X), h(Y)\},$$

$$h(X^*) = h(X) + 1.$$

Exemple 17 Identités mettant en relation des expressions rationnelles dont la hauteur d'étoile diffère (cf. Exemple 3).

Si, dans les identités,

$$(e + f)^* \equiv (e^* f)^* e^*,$$
$$1 + (e + f)^* f \equiv (e^* f)^*,$$

les expressions e et f sont instanciées par des lettres d'un alphabet donné, les membres gauches associés à l'instanciation de ces identités sont alors de hauteur d'étoile 1, alors que les membres droits sont de hauteur d'étoile 2. Ainsi, les deux expressions rationnelles apparaissant dans l'instanciation d'une identité n'ont pas nécessairement la même hauteur d'étoile.

La *hauteur d'étoile* d'un langage rationnel est, par définition, égale au minimum des hauteurs d'étoile des expressions rationnelles décrivant ce langage.

Exemples 18 L'ensemble des mots sur l'alphabet $\{a, b\}$ qui se terminent par la lettre a, représenté, entre autres, par les expressions rationnelles $(a+b)^*a$ et $(a^*b)^*a$, est de hauteur d'étoile 1.

Les langages rationnels de hauteur d'étoile nulle sont exactement les langages finis.

2.1.2 Lien avec les automates

Ce paragraphe présente une interprétation de la hauteur d'étoile en termes d'automates.

On met en évidence dans ce qui suit le lien entre la notion de hauteur d'étoile d'un langage rationnel et celle de complexité en cycles du graphe des états des automates reconnaissant le langage. Les résultats présentés ici sont dus à Eggan ([Egg63]).

L'objet de ce qui suit est le suivant : on introduit la notion de rang cyclique d'un automate et on montre que la hauteur d'étoile d'un langage rationnel est égale au minimum des rangs cycliques des automates reconnaissant ce langage.

On définit récursivement le *rang* d'une composante fortement connexe de la façon suivante :

- Une composante fortement connexe est de rang 0 si elle est réduite à un seul sommet et si le seul chemin qu'elle contient est le chemin associé au mot vide.
- Une composante fortement connexe est de rang 1 s'il existe un sommet par lequel passent tous les cycles de la composante fortement connexe.
- Une composante fortement connexe est de rang k s'il existe un sommet tel que le graphe obtenu en supprimant ce sommet et les transitions ayant pour extrémité ce sommet contient un cycle de rang $k-1$ (et éventuellement d'autres cycles de rangs inférieurs) et si le graphe obtenu, à partir du cycle initial, en supprimant tout autre sommet, contient un cycle de rang supérieur ou égal à $k-1$.

On définit la notion de *rang cyclique* d'un automate de la façon suivante : si le graphe des états de l'automate est acyclique, ce rang est nul, sinon il est égal au maximum des rangs de ses composantes fortement connexes.

Exemple 19 Automates en pétales

Les automates en pétales étant exactement les automates finis dont tous les cycles passent par un même sommet, ce sont donc les automates de rang cyclique 1. Les deux

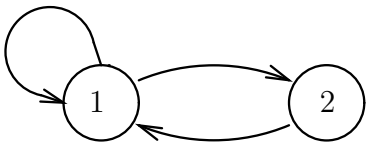


FIG. 2.1 – *Automate de rang cyclique* 1.

cycles de l'automate de la Figure 2.1 passent par l'état 1 : l'automate est de rang 1.

Exemple 20 Automate de rang cyclique 2 (Figure 2.2).

Du fait des propriétés de symétrie du graphe, tous les états jouent le même rôle. De plus, en supprimant l'un quelconque des états de l'automate, on obtient un automate en pétales (cf. Exemple 19). L'automate est donc de rang 2.

La preuve du résultat suivant est donnée dans [Egg63].

Théorème 11 (Eggan) *La hauteur d'étoile d'un langage rationnel est égal au minimum des rangs cycliques des automates finis reconnaissant ce langage.*

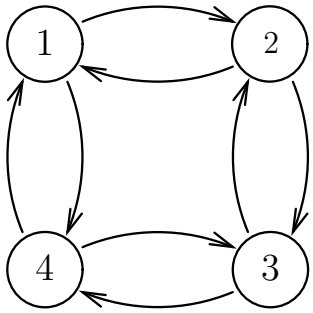


FIG. 2.2 – *Automate de rang cyclique* 2

En ce sens, la hauteur d'étoile peut être interprétée comme une mesure de la complexité en cycles du langage.

Démonstration : Le minimum r des rangs cycliques des automates reconnaissant un langage rationnel L est inférieur à sa hauteur d'étoile. En effet, soit E une expression rationnelle représentant le langage L, en utilisant les méthodes usuelles pour construire un automate à partir d'une expression rationnelle, on crée une composante fortement connexe quand opère une étoile et on augmente éventuellement le rang d'une composante fortement connexe d'une unité si l'étoile opère sur une expression contenant déjà cet opérateur. La hauteur d'étoile de l'expression E est donc supérieure à r. Comme, par définition, la hauteur d'étoile d'un langage rationnel est égale au minimum des hauteurs d'étoile des expressions rationnelles décrivant ce langage, elle est supérieure au minimum des rangs cycliques des automates finis reconnaissant ce langage.

Il reste à établir l'inégalité $r \geq h(L)$. On va prouver (Lemme 6 p.67) que si i et f sont deux états d'un automate de rang cyclique k, il existe une expression rationnelle de hauteur d'étoile au plus k qui décrit l'ensemble des étiquettes des chemins allant de l'état i à l'état f. Comme le langage L est reconnu par un automate de rang cyclique r, il existe une expression rationnelle de hauteur d'étoile au plus r qui décrit L . Cette expression est obtenue par union finie des étiquettes des chemins allant de i à f quand i et f décrivent respectivement l'ensemble des états initiaux et finaux de l'automate, ce qui montre que $h(L) \leq r$. □

Lemme 6 *Si i et f sont deux états d'un automate $\mathcal{A}$ de rang cyclique k, il existe une expression rationnelle de hauteur au plus k qui décrit l'ensemble des étiquettes des chemins allant de l'état i à l'état f.*

Démonstration : On établit la preuve de ce lemme par induction sur le rang cyclique k de l'automate $\mathcal{A}$.

Si $k = 0$, l'automate $\mathcal{A}$ est acyclique, il n'existe alors qu'un nombre fini de chemins allant de l'état i à l'état f, dont les étiquettes sont décrites par une expression rationnelle de hauteur d'étoile nulle.

On suppose maintenant que, dans un automate de rang cyclique $k' \leq k$, l'ensemble des étiquettes des chemins entre deux états peut être décrit par une expression rationnelle de hauteur d'étoile au plus k'.

Soit $\mathcal{A}$ un automate de rang cyclique $k+1$.

Cas d'une composante fortement connexe : L'automate $\mathcal{A}$ est réduit à une seule composante fortement connexe.

Si l'automate $\mathcal{A}$ n'a qu'un seul état s, alors les chemins de cette composante fortement connexe sont décrits par le mot vide si le seul chemin de l'automate est le chemin vide et par l'expression rationnelle de hauteur d'etoile 1 : e_{ss}^*, si e_{ss} est l'étiquette de la boucle sur l'état s.

Soit s un état (de l'automate $\mathcal{A}$) tel que l'automate obtenu en supprimant s et toutes les transitions d'extrémité s soit de rang cyclique k.

Soient

$$P = \{p \mid \quad \text{il existe une transition dans } \mathcal{A} \text{ allant de } p \text{ à } s\}$$

et

$$Q = \{q \mid \quad \text{il existe une transition dans } \mathcal{A} \text{ allant de } s \text{ à } q\}.$$

On note $e_{vv'}$ l'étiquette de la transition allant de v à v' et respectivement $L_{vv'}$ et $L^s_{vv'}$ l'ensemble des étiquettes des chemins de v à v' dans $\mathcal{A}$ et dans $\mathcal{A} - \{s\}$. On a alors

$$L_{ss} = \left(e_{ss} + \sum_{q\in Q}\sum_{p\in P} e_{sq} L^s_{qp} e_{ps} \right)^* .$$

D'après l'hypothèse d'induction, pour tous i et j, L^s_{qp} est de hauteur d'étoile au plus k et L_{ss} est, par suite, de hauteur d'étoile au plus $k+1$.

Si $v \neq s$,

$$L_{vv} = L^s_{vv} + \left(\sum_{p\in P}\sum_{q\in Q} L^s_{vp} e_{ps} L_{ss} e_{sq} L^s_{qv} \right),$$

$$L_{vs} = \sum_{p\in P} L^s_{vp} e_{ps} L_{ss},$$

$$L_{sv} = \sum_{q\in Q} L_{ss} e_{sq} L^s_{qv}.$$

Chacun de ces langages est de hauteur d'étoile inférieure à $k+1$.

Si, de plus, $v' \neq s$,

$$L_{vv'} = L^s_{vv'} + \left(\sum_{p\in P}\sum_{q\in Q} L^s_{vp} e_{ps} L_{ss} e_{sq} L^s_{qv'} \right),$$

d'où $h(L_{vv'}) \leq k+1$. On a donc établi le résultat annoncé dans le cas où l'automate est réduit à une seule composante fortement connexe.

Cas général : $\mathcal{A}$ est un automate de rang cyclique $k+1$.

Toutes les composantes fortement connexes de $\mathcal{A}$ sont alors de rang inférieur à $k+1$.

Si v est dans une composante connexe réduite à un singleton, $L_{vv} = e_{vv}^*$. Sinon L_{vv} est un langage de hauteur au plus $k+1$ d'après ce qui précède.

Si $v \neq v'$ et si v et v' sont dans la même composante fortement connexe, on est également ramené au cas précédent, le langage $L_{vv'}$ est de hauteur d'étoile au plus $k+1$. Dans le cas contraire (*i.e.*, il existe un chemin de v à v' mais v et v' sont dans deux composantes connexes distinctes du graphe des états), soient $C_1, C_2, \ldots, C_t$ les composantes par lesquelles passent les chemins de la composante fortement connexe de v à celle de v'. Toute étiquette d'un chemin de v à v' est alors de la forme

$$xw_1e_1w_2 \ldots w_te_tw_{t+1}y$$

où x (resp. y) désigne l'étiquette d'un chemin dans la composante contenant v (resp. v') ayant v comme origine (resp. v' comme fin), w_1 est l'étiquette d'un chemin de la composante connexe contenant v à C_1, w_{t+1} celle d'un chemin de C_t à la composante connexe contenant v' et w_j $(2 \leq j \leq u)$ celle d'un chemin de C_{j-1} à C_j, enfin e_j est l'étiquette d'un chemin dans C_j. Toute étiquette d'un chemin de v à v' est un élément de l'ensemble

$$Xw_1L_1w_2 \ldots w_tL_tw_{t+1}Y.$$

Comme il n'existe qu'un nombre fini de chemins entre deux composantes connexes, on en déduit que $L_{vv'}$ est une union finie de langages de hauteur d'étoile au plus $k+1$.

On a ainsi établi que l'ensemble des étiquettes des chemins entre deux états d'un automate de rang cyclique k peut être décrit par une expression rationnelle de hauteur d'étoile au plus k. □

La hauteur d'étoile n'est pas une propriété syntactique, il est facile de s'en convaincre en considérant un langage fini sur un alphabet à deux lettres : sa hauteur d'étoile est nulle mais celle de son complémentaire ne l'est pas alors qu'ils ont le même monoïde syntactique.

Une des conséquences de cette remarque est la suivante : l'automate minimal du langage ne donne qu'une borne supérieure de la hauteur d'étoile du langage (on rappelle que le monoïde de transition est isomorphe au monoïde syntactique). De plus, selon le sens de lecture du mot, le rang cyclique de l'automate minimal associé peut être différent.

Exemple 21 On considère l'alphabet $A = \{a, b\}$ et X l'ensemble des mots de A^* qui se terminent par ab. Alors X n'est pas fini et est décrit par l'expression rationnelle $(a+b)^*ab$, il est donc de hauteur d'étoile 1.

L'automate minimal (Figure 2.3 p.70), associé à une lecture de gauche à droite, est de rang cyclique 2.

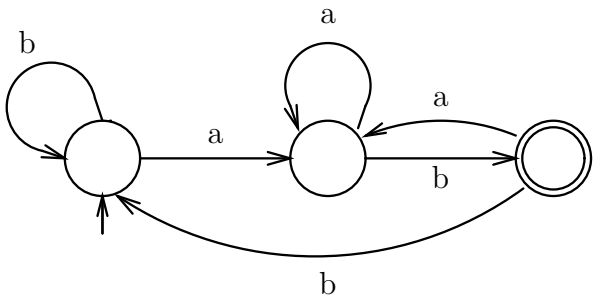


FIG. 2.3 – *Automate minimal de rang cyclique* 2

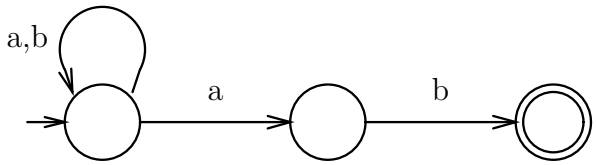


FIG. 2.4 – *Automate minimal de rang cyclique* 1

L'automate minimal (Figure 2.4), associé à une lecture de droite à gauche, est lui de rang cyclique 1.

Le résultat suivant, dû à McNaughton ([McN67] Théorème 9), montre cependant que, dans certains cas, la hauteur d'étoile du langage peut être déterminée en utilisant son automate minimal.

Théorème 12 (McNaughton) *Soit X un langage rationnel. Si le monoïde syntactique de X est un groupe et si l'automate minimal de X a un seul état final, alors la hauteur d'étoile du langage X est égale au rang cyclique de cet automate.*

Exemple 22 Soit $A = \{a, b\}$ et soit $X = (a^* + ba^*b)^*$. On construit l'automate minimal de X (Figure 2.5). Comme le monoïde syntactique de X est isomorphe au monoïde des

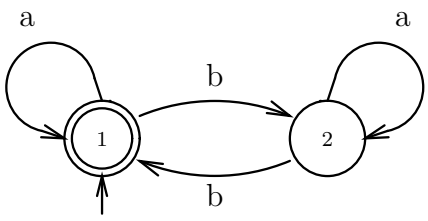


FIG. 2.5 – *Automate minimal de* $X = (a^* + ba^*b)^*$

transitions de l'automate minimal, et que la lecture d'une lettre est une permutation des états de l'automate, le monoïde syntactique est un groupe. On en déduit que la hauteur d'étoile de X est égale au rang cyclique de son automate minimal, c'est-à-dire 2.

2.1.3 Problème des bornes

Dans cette section, on montre que la hauteur d'étoile d'un langage rationnel n'est pas bornée et que ce résultat est déjà vrai si l'alphabet est réduit à deux lettres (sur un alphabet à une lettre, la hauteur d'un langage est 0 ou 1). Le résultat suivant est dû à Eggan ([Egg63]).

Théorème 13 (Eggan) *La hauteur d'étoile des langages rationnels n'est pas bornée.*

Démonstration : On considère, pour tout entier n, un langage rationnel sur un alphabet à n lettres dont l'automate minimal n'a qu'un seul état final et tel que la lecture de chacune des n lettres est une permutation des états de l'automate. Alors, d'après le théorème de McNaughton, ce langage est de hauteur d'étoile n. □

Le théorème précédent a été amélioré et précisé par Dejean et Schützenberger ([DS66]) de la façon suivante.

Théorème 14 (Dejean-Schützenberger) *Pour tout entier naturel n, il existe des langages rationnels de hauteur d'étoile exactement n sur un alphabet à deux lettres.*

Démonstration : Soit $A = \{a, b\}$ l'alphabet utilisé dans ce qui suit. Pour tout entier naturel non nul n, on définit le langage $X_n(a, b)$ comme l'ensemble des mots du monoïde libre A^* dont le nombre d'occurrences de la lettre a est congru modulo 2^n au nombre d'occurrences de la lettre b, soit

$$X_n(a, b) = \{x \in A^* \mid |x|_a \equiv |x|_b \bmod 2^n\}.$$

Chacun des langages X_n est de hauteur d'étoile exactement n.

Pour $n = 1$, on obtient l'ensemble des mots de longueur paire sur l'alphabet A. Comme $X_1(a, b)$ est infini, sa hauteur d'étoile est strictement positive, elle est en fait égale à 1 puisque ce langage peut être décrit par une expression rationnelle de hauteur d'étoile 1 :

$$X_1(a, b) = (a + b)^{2*},$$

ou par un automate de rang cyclique 1 (Figure 2.6 p.72).

Pour $n = 2$, on construit l'automate minimal (Figure 2.7 p.72) de X_2 :

$$X_2(a, b) = \{x \in A^* \mid |x|_a \equiv |x|_b \bmod 4\}.$$

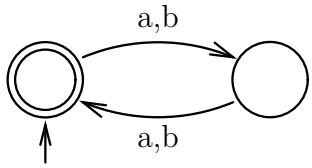


FIG. 2.6 – *Automate reconnaissant* $X_1(a,b) = (a+b)^{2*}$

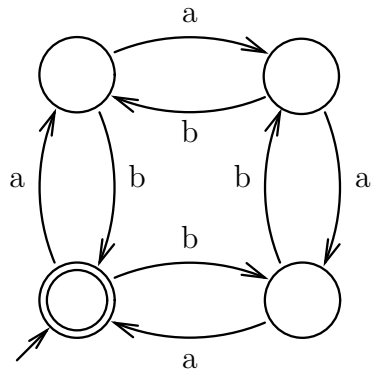


FIG. 2.7 – *Automate reconnaissant* $X_2(a,b) = \{x \in A^* \mid |x|_a \equiv |x|_b \bmod 4\}$

Comme la lecture d'un a ou d'un b correspond à une permutation des états de l'automate, on en déduit que le monoïde syntactique de X_2 est un groupe. L'automate ayant de plus un seul état final, d'après le théorème de McNaughton, la hauteur d'étoile de X_2 est égale au rang cyclique de son automate minimal c'est-à dire 2 (on supprime par exemple l'état 3 puis l'état 1). On aurait pu établir que X_1 est de hauteur d'étoile 1 de la même manière.

On va maintenant traiter de manière analogue le cas général. Soit

$$X_n(a,b) = \{x \in A^* \mid |x|_a \equiv |x|_b \bmod 2^n\}.$$

L'automate minimal de X_n (Figure 2.8) a 2^n états, soit $\{1, 2, \ldots, 2^n\}$. L'état 1 est l'état initial et l'unique état final. La fonction de transition est la suivante

$$i.a = \begin{cases} 1 & \text{si} \quad i = 2^n \\ i+1 & \text{sinon} \end{cases}$$

et

$$i.b = \begin{cases} 2^n & \text{si} \quad i = 1 \\ i-1 & \text{sinon} \end{cases}$$

Comme la lecture d'un a ou d'un b est une permutation de l'ensemble des états et que le monoïde des transitions de l'automate minimal est isomorphe au monoïde syntactique

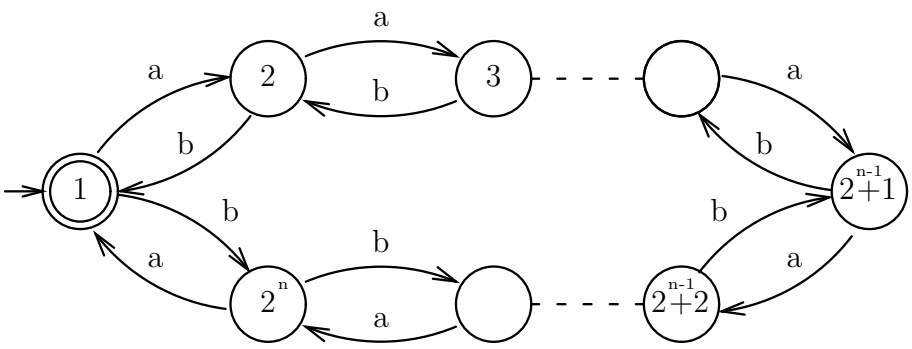


FIG. 2.8 – *Automate reconnaissant* $X_n(a,b) = \{x \in A^* \mid |x|_a \equiv |x|_b \bmod 2^n\}$

du même langage, on en déduit que celui de X_n est un groupe. Comme, de plus, l'automate minimal de X_n a un seul état final, on en déduit d'après le théorème de McNaughton que la hauteur d'étoile de X_n est égale au rang cyclique de son automate minimal.

Du fait des propriétés de symétrie de l'automate considéré (Figure 2.8), il n'est pas difficile de montrer que ce dernier est de rang cyclique n. En supprimant l'état $2^{n-1}+1$, on peut représenter de manière "linéaire" l'automate. Pour obtenir un graphe acyclique en minimisant le nombre d'états à éliminer, on procède par dichotomie : on supprime l'état médian (l'état 1 à la première étape), on obtient deux composantes fortement connexes qui sont de même rang cyclique, on itère le procédé, par exemple en choisissant systématiquement la composante comportant les états de plus petits indices. On supprime alors les états $2^{n-2}+1, 2^{n-3}+1, \ldots, 3$, soit $n-2$ états. On aura donc supprimé au total n états, ce qui prouve bien que l'automate est de rang cyclique n. □

2.1.4 Décidabilité

Le problème de la hauteur d'étoile est très lié à celui de la propriété de la puissance finie. En effet, l'étoile d'un ensemble possédant cette propriété s'exprime sous une forme polynomiale dont l'unique variable est l'ensemble lui-même, *i.e.*, l'étoile peut-être remplacée par des sommes et des produits ; en particulier X et X^* ont alors la même hauteur d'étoile.

Simon ([Sim78]) et Hashiguchi ([Has79]) ont établi indépendamment que l'on peut décider si un ensemble rationnel donné possède la propriété de puissance finie. La preuve de Simon réduit ce problème à celui de la finitude de monoïdes de matrices à coefficients dans le semi-anneau tropical (pour une synthèse sur le semi-anneau tropical on pourra consulter [Pin95]). Une généralisation de cette méthode a permis à Hashiguchi de donner un algorithme pour décider si un langage rationnel est de hauteur d'étoile 1 ([Has82]). La calculabilité de la hauteur d'étoile dans le cas général a également été établie par Hashiguchi en 1989 ([Has89] et [Has88]).

Théorème 15 (Hashiguchi) *La hauteur d'étoile d'un langage rationnel est décidable.*

2.2 Analogies entre les langages et les séries

Dans cette section, on présente les analogies entre langages et séries rationnels. On définit la notion de hauteur d'étoile pour les séries et on en donne une interprétation en termes d'automates avec multiplicité. On énonce enfin un résultat (Théorème 16 p.75), dû à Reutenauer, à savoir que, quand $\mathbb{K}$ est un corps, il existe des séries $\mathbb{K}$-rationnelles de hauteur d'étoile arbitraire et que la hauteur d'étoile d'une série est donnée par l'une de ses représentations minimales.

On définit la hauteur d'étoile d'une série K-rationnelle comme le minimum des hauteurs d'étoile des expressions rationnelles avec multiplicité décrivant cette série.

De façon plus formelle, on peut donner une définition algébrique, équivalente à la précédente, de la hauteur d'étoile d'une série rationnelle S. Soit $(R_i)_{0\leq i\leq n}$ une suite croissante (pour l'inclusion) d'ensembles tels que

- leur réunion est l'ensemble de toutes les séries rationnelles ;
- l'ensemble des polynômes est R_0 ;
- chaque R_i est stable pour l'addition et la multiplication ;
- si $S \in R_i$ est propre, *i.e.*, $S(0) = 0$, alors $S^\star \in R_{i+1}$.

Le plus petit entier n tel que $S \in R_n$ est alors la *hauteur d'étoile* de la série S.

Le résultat suivant donne une interprétation en termes d'automates avec multiplicité de la hauteur d'étoile d'une série K-rationnelle ($\in K\langle\langle A\rangle\rangle$). La preuve de ce résultat découle directement de celle donnée par Eggan (Théorème 11 p.66) pour les langages rationnels à condition de considérer cette fois des automates avec multiplicité.

Proposition 9 *La hauteur d'étoile d'une série K-rationnelle en plusieurs variables non-commutatives est égale au minimum des rangs cycliques des automates (finis), avec multiplicité dans K, reconnaissant la série.*

En ce sens, la hauteur d'étoile peut être interprétée comme une mesure de la complexité en cycles de la série.

Exemple 23 Les séries de hauteur nulle sont exactement celles qui se réduisent à des polynômes, ce sont celles qui sont reconnues par des automates acycliques.

Exemple 24 La série de Fibonacci, qui est reconnue par l'automate de la Figure 2.9 et peut être représentée par l'expression rationnelle de hauteur d'étoile 1

$$(z + z^2)^* = \frac{1}{1 - (z + z^2)},$$

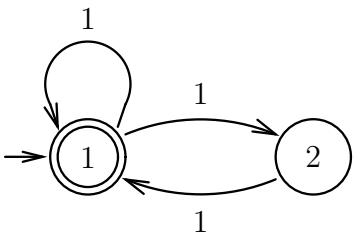


FIG. 2.9 – *Automate reconnaissant la série de Fibonacci*

est de hauteur d'étoile 1.

Exemple 25 Les termes d'indice pair de la série de Fibonacci
La série des termes pairs de la série de Fibonacci peut être représentée par un automate

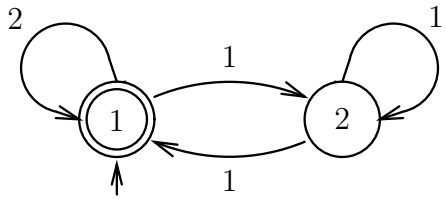


FIG. 2.10 – *Automate des termes d'indice pair de la série de Fibonacci*

de rang cyclique 2 (Figure 2.10) et décrite par l'expression rationnelle $(2z + z^2z^*)^*$. Elle est donc de hauteur au plus 2, en fait exactement 2 comme on le verra dans ce qui suit (Exemple 26 p.81).

Récemment, Reutenauer a démontré ([Reu96]) que, si $\mathbb{K}$ est un corps, la hauteur d'étoile des séries $\mathbb{K}$-rationnelles n'est pas bornée et surtout qu'elle peut être obtenue à partir de l'une de ses représentations minimales. L'énoncé du théorème suivant précise ces résultats.

Théorème 16 *Si $\mathbb{K}$ est un corps, alors pour tout entier n, il existe des séries $\mathbb{K}$-rationnelles de hauteur d'étoile n. Si une série $\mathbb{K}$-rationnelle s est de hauteur d'étoile n alors il existe une représentation minimale de s dont le graphe associé est de rang cyclique n.*

2.3 Séries $\mathbb{N}$-rationnelles en une variable

On étudie maintenant en détail le cas d'une famille particulière de séries rationnelles : *les séries* $\mathbb{N}$*-rationnelles en une variable*. On montre qu'une des conséquence du théorème de Soittola (Théorème 8 p.30) est que la hauteur d'étoile d'une série $\mathbb{N}$-rationnelle est de hauteur d'étoile au plus 2.

La caractérisation par des critères adéquats de celles qui sont de hauteur d'étoile 1 permettrait donc de décider, dans le cas général, de la hauteur d'étoile d'une série $\mathbb{N}$-rationnelle en une variable. C'est le problème que l'on s'est attaché à résoudre et le résultat obtenu (cf. Théorème 17, p.78) donne une condition nécessaire pour qu'une série $\mathbb{N}$-rationnelle en une variable soit de hauteur d'étoile 1 et permet de décider de la hauteur d'étoile de certaines de ces séries.

En utilisant la caractérisation du rayon spectral des matrices compagnons irréductibles intégrales (Théorème 10 p.59), on donne une caractérisation des séries de hauteur d'étoile 1, on en déduit une propriété de leurs racines positives. A la différence du théorème de Soittola, elle concerne toutes les racines positives de la série.

On établit enfin le résultat suivant (Théorème 17 p.78) : le fait d'avoir pour racines réelles positives exclusivement des nombres d'Handelman est une condition nécessaire pour qu'une série $\mathbb{N}$-rationnelle soit de hauteur 1 et suffisante pour décider la hauteur d'étoile d'une série $\mathbb{N}$-rationnelle ayant de plus une racine dominante. La démonstration établie par induction utilise la représentation linéaire d'une série rationnelle et la caractérisation de ses racines réelles positives.

On clôt le chapitre sur le problème de la décidabilité de la hauteur d'étoile des séries $\mathbb{N}$-rationnelles en une variable.

2.3.1 Conséquence du théorème de Soittola

Une conséquence importante du théorème de Soittola concerne la complexité de séries rationnelles. Les séries $\mathbb{Z}$-rationnelles, étant $\mathbb{Q}$-rationnelles, s'écrivent sous la forme

$$\frac{P(z)}{1-Q(z)}$$

où P et Q sont à coefficients entiers d'après la lemme de Fatou (cf. p.35) ; ces séries sont de hauteur d'étoile 0 ou 1. La preuve du théorème de Soittola montre que la hauteur d'étoile d'une série $\mathbb{N}$-rationnelle est au plus égale à 2. Ce résultat a été établi indépendamment par Katayama, Okamoto et Enomoto ([KOE78]).

Corollaire 3 *Une série* $\mathbb{N}$*-rationnelle est de hauteur d'étoile au plus* 2*.*

Démonstration : Une série $\mathbb{Z}$-rationnelle à coefficients positifs ayant une racine dominante peut être représentée par un automate de rang cyclique 2. En effet, d'après les preuves du théorème de Soittola et de la Proposition 7 (p.35), on peut construire un automate dont chaque composante fortement connexe du graphe des états est de rang 2. La

matrice

$$P = \begin{pmatrix} P_1 & 1 & 0 & \dots & 0 \\ \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ P_{k-1} & \vdots & & 0 & 1 \\ P_k & 0 & \dots & 0 & 1 \end{pmatrix}$$

peut être représentée par l'automate de la Figure 2.11 qui est de bien de rang 2.

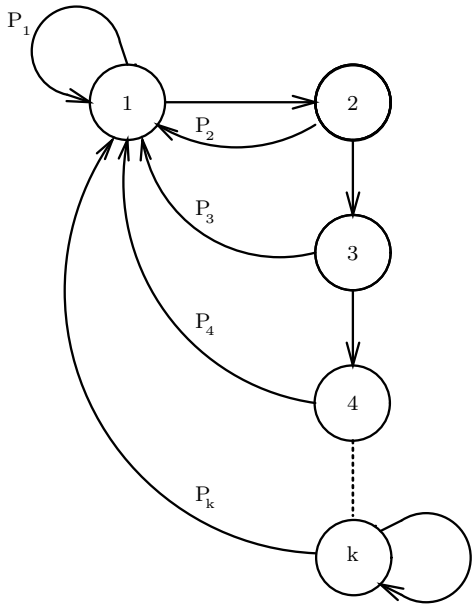


FIG. 2.11 – *Composante connexe d'un automate reconnaissant une série* $\mathbb{N}$*-rationnelle qui a une racine dominante*

On peut également noter que la matrice à coefficients polynomiaux

$$P_P = \begin{pmatrix} \sum_{i=1}^{k-1} P_i z^i & z^{k-1} \\ P_k z & z \end{pmatrix}$$

associée à cet automate est également de taille 2.

De la stabilité de la hauteur d'étoile d'une série par sommation et par emboîtement, on déduit qu'une série $\mathbb{N}$-rationnelle en une variable est au plus de hauteur d'étoile 2.

On montre dans ce qui suit qu'il existe des séries de hauteur d'étoile exactement 2 et l'Exemple 26 (p.81) en est une illustration. □

Remarque 10 La hauteur d'étoile d'une série obtenue par emboîtement est au plus égale au maximum des hauteurs d'étoile des séries intervenant dans l'emboîtement. En revanche,

une série intervenant dans l'emboîtement peut avoir une hauteur d'étoile strictement supérieure à celle de la série résultante (Exemple 27 p.82).

2.3.2 Séries de hauteur d'étoile 1

Sachant que les séries $\mathbb{N}$-rationnelles sont de hauteur d'étoile au plus 2, que les polynômes sont exactement les séries de hauteur d'étoile nulle, on est conduit à étudier les séries de hauteur d'étoile 1. Dans ce qui suit, on en établit plusieurs caractérisations dont on déduit une propriété analytique des séries de hauteur 1 qui, sous une condition appropriée, donne un critère pour décider de la hauteur d'étoile de certaines séries.

Principal théorème

Le résultat suivant donne une condition nécessaire pour qu'une série $\mathbb{N}$-rationnelle soit de hauteur d'étoile 1 et permet de décider sa hauteur d'étoile dans le cas où elle a de plus une racine dominante.

Théorème 17 *Soit r une série $\mathbb{N}$-rationnelle. Si r est de hauteur d'étoile 1, alors ses racines réelles positives sont des nombres d'Handelman.*

Si, de plus, la série r a une racine dominante, cette condition suffit à caractériser les séries de hauteur d'étoile 1.

Les nombres réels positifs vérifiant les conditions du Théorème 17 sont les *nombres d'Handelman* (cf. Théorème 10 p.59).

La preuve du Théorème 17 permet également d'établir le résultat suivant (on pourra se reporter à la Remarque 13 p.85).

Proposition 10 *Si r est une série $\mathbb{N}$-rationnelle n'ayant qu'une seule racine réelle positive λ, alors la série r est de hauteur d'étoile 1 si et seulement si λ est un nombre d'Handelman.*

Pour déterminer la hauteur d'étoile d'une série $\mathbb{N}$-rationnelle, on s'intéresse aux racines réelles positives de son polynôme minimal. Dans la preuve du Théorème 17, on utilise le Théorème 10 (p.59) qui donne une caractérisation des racines positives des polynômes de la forme : $z^n - \sum a_i z^i$ où les a_i sont des entiers naturels et a_0 non nul.

Preuve du théorème (sens direct)

On donne pour commencer plusieurs caractérisations équivalentes des séries de hauteur d'étoile 1, dont on déduit que la condition est nécessaire.

Proposition 11 *Soit $r = \sum_{n\geq 0} r_n z^n$ une série $\mathbb{N}$-rationnelle, alors r est de hauteur d'étoile 1 si et seulement si l'une des trois conditions suivantes est satisfaite*

1. *la série r s'écrit sous la forme*

$$\sum_{i\in I} \frac{P_i}{\prod_{j\in J_i}(1-Q_{i_j})} \qquad \forall i,j \quad P_i \in \mathbb{N}[z], \quad Q_{i_j} \in z\mathbb{N}[z], \tag{2.1}$$

   où I, J sont des ensembles de cardinal fini et où l'un au moins des polynômes Q_{i_j} est non nul.

2. *la série r admet une représentation linéaire (l, M, c) avec, n étant un entier supérieur à 1, $l \in \mathbb{N}^{1\times n}, M \in \mathbb{N}^{n\times n}$ et $c \in \mathbb{N}^{n\times 1}$, telle que*
   - $\forall k \geq 0 \qquad r_k = lM^k c$,
   - *La matrice M soit triangulaire par blocs et ses blocs diagonaux soient des matrices compagnons irréductibles.*

3. *la série r admet une représentation linéaire polynomiale, i.e. (l, M, c) avec, n étant un entier supérieur à 1, $l \in \mathbb{N}[z]^{1\times n}, M \in z\mathbb{N}[z]^{n\times n}$ et $c \in \mathbb{N}[z]^{n\times 1}$, telle que*
   - $r = \sum_{k=0}^{\infty} lM^k c$,
   - *La matrice M soit triangulaire.*

Démonstration : Les séries définies de l'une des trois manières précédentes sont de hauteur d'étoile 1.

Dans le premier cas, elles sont données par une expression rationnelle de hauteur d'étoile 1 :

$$\sum_{i\in I} P_i \prod_{j\in J_i} Q_{i_j}^*.$$

Dans les autres cas, l'automate associé à la matrice M est de rang cyclique 1, chacune des composantes fortement connexes de son graphe étant de rang 1.

Il reste à établir la réciproque.

r est de hauteur d'étoile 1 $\Rightarrow$ 1 : On montre que les séries de hauteur d'étoile 1 peuvent être mises sous la forme (2.1).

Soient R_0 l'ensemble des polynômes à coefficients dans $\mathbb{N}$ et R_1' l'ensemble des séries $\mathbb{N}$-rationnelles de hauteur d'étoile 1. L'ensemble des séries de la forme (2.1) est inclus dans R_1' et contient tout élément $P^\star$ où $P \in R_0$ et $P(0) = 0$.

De plus, cet ensemble est stable pour l'addition et le produit (de convolution), on en conclut que l'expression (2.1) caractérise les séries $\mathbb{N}$-rationnelles de hauteur d'étoile 1.

1 $\Rightarrow$ 3 : On prouve dans ce qui suit que toute série de la forme (2.1) admet une représentation polynomiale vérifiant la condition *3*. Si

$$r_i = \frac{P_i}{\prod_{j\in J_i}(1-Q_{i_j})},$$

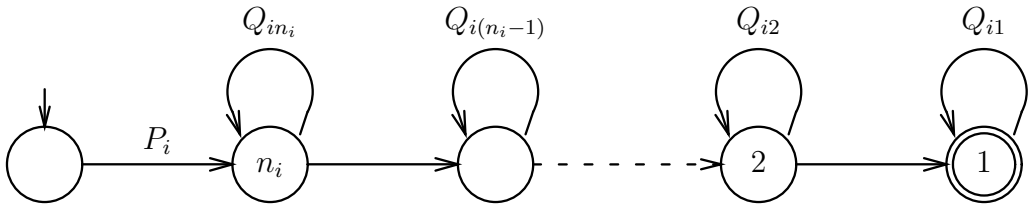


FIG. 2.12 – *La représentation polynomiale* (l_i, M_i, c_i)

la série $r_i z^{n_i}$ où $n_i = \text{Card } J_i$ admet la représentation polynomiale (l_i, M_i, c_i) (Figure 2.12) avec

$$l_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ P_i \end{pmatrix}^t, \quad M_i = \begin{pmatrix} Q_{i1} & 0 & \dots & \dots & 0 \\ z & Q_{i2} & \ddots & & \vdots \\ 0 & z & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \dots & 0 & z & Q_{in_i} \end{pmatrix} \quad \text{et} \quad c_i = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Par suite, si $r = \sum_{i=1}^{N} r_i$, alors la série rz^n, où $n = \max_{1 \le i \le N}\{n_i\}$, admet la représentation polynomiale (l, M, c) avec

$$l = \begin{pmatrix} l_1 z^{n-n_1} \\ l_2 z^{n-n_2} \\ \vdots \\ l_N z^{n-n_N} \end{pmatrix}^t, \quad M = \begin{pmatrix} M_1 & 0 & \dots & \dots & 0 \\ 0 & M_2 & \ddots & & \vdots \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 0 & M_N \end{pmatrix} \quad \text{et} \quad c = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_N \end{pmatrix}.$$

A un décalage près des indices, toute série qui s'écrit sous la forme (2.1) a donc une représentation polynomiale vérifiant les assertions *3*.

3 $\Rightarrow$ *2 :*

Pour la réciproque, on construit à partir de M_P un graphe orienté de la manière suivante. L'ensemble des sommets du graphe contient un ensemble de n sommets (soit, $1, 2, \dots, n$) qui indexent les lignes et les colonnes de M.

Si $M_{ij} = \sum_k a_k z^k$, il y a a_k chemins de longueur k allant du sommet i au sommet j (Figure 2.13). Tous les sommets intérieurs de ces chemins n'ont qu'une transition entrante et une transition sortante, ils sont de plus disjoints des sommets $1, 2, \dots, n$.

Les coefficients de l_P et c_P sont développés de la même manière et les sommets dont partent (resp. arrivent) les chemins correspondants aux coefficients polynomiaux de l_P (resp. c_P) sont alors les états initiaux (resp. finaux) du nouvel automate. On obtient la représentation linéaire cherchée en interprétant cet automate. □

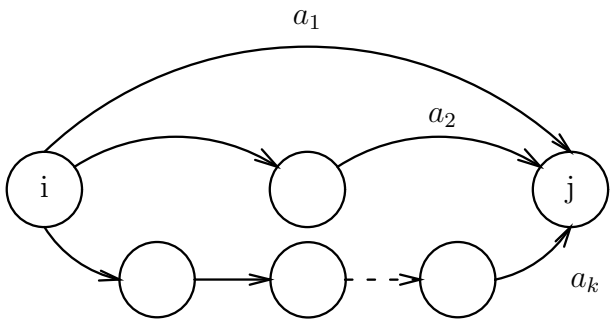


FIG. 2.13 – *Représentation du coefficient* $M_{ij} = \sum_k a_k z^k$

Remarque 11 Les représentations *2* et *3* sont équivalentes. Pour obtenir une représentation linéaire polynomiale (l_P, M_P, c_P) à partir d'un représentation (l, M, c) de la forme *2*, on procède de la façon suivante :

- On indexe la matrice M_P sur l'ensemble des sommets par lesquels passent tous les cycles de chaque bloc diagonal de M (on obtient un sommet par bloc puisque ces blocs sont des matrices compagnons irréductibles). Les coefficients M_{ij} de M_P sont alors des polynômes de la forme $\sum a_k z^k$ où a_k est le nombre de chemins de longueur k allant du sommet i au sommet j et ne passant par aucun autre sommet distingué du graphe.
- Les coefficients l_i du vecteur l_P sont également des polynômes $\sum a_k z^k$ où a_k est égal au nombre de chemins de longueur k allant d'un état initial (affecté du coefficient correspondant de l) de l'automate précédent à l'état i.
- De même les coefficients c_i de c_P sont définis par l'ensemble des chemins allant du sommet i aux états finaux (affectés de leur coefficient correspondant dans c) de l'automate précédent.

On déduit de la Proposition 11 que les racines réelles positives d'une série de hauteur d'étoile 1 sont, chacune, racine d'un des polynômes réciproques $\overline{(1 - Q_{i_j})}$ ou, ce qui est équivalent, rayon spectral d'une matrice compagnon irréductible intégrale. D'après le Théorème 10 (p.59), ce sont donc des nombres d'Handelman.

Exemple 26 Si une série ℕ-rationnelle r est de hauteur d'étoile 1, alors toutes ses racines réelles positives sont des nombres d'Handelman. On exhibe une série qui montre que la condition nécessaire du Théorème 17 (p.78) permet de justifier l'existence de série de hauteur d'étoile 2.

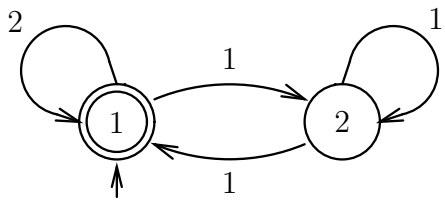


FIG. 2.14 – *Automate des termes d'indice pair de la série de Fibonacci*

La série constituée des termes pairs ou des termes impairs de la série de Fibonacci est reconnue par l'automate (Figure 2.14). L'expression rationnelle et la matrice associée à cet automate sont respectivement les suivantes

$$(2z + z^2z^*)^* \qquad \text{et} \qquad A \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

Le polynôme caractéristique s'écrit

$$g(z) = z^2 - 3z + 1,$$

il a deux racines conjuguées réelles positives :

$$\frac{3+\sqrt{5}}{2} \quad \text{et} \quad \frac{3-\sqrt{5}}{2}$$

La série n'est donc pas de hauteur d'étoile 1, elle est, par suite, de hauteur d'étoile 2.

Remarque 12 Pour la réciproque, on ne peut pas utiliser la caractérisation des séries $\mathbb{N}$-rationnelles par un emboîtement de séries $\mathbb{Z}$-rationnelles ayant une racine dominante. En effet, la hauteur d'étoile des séries intervenant dans l'emboîtement ne donne pas d'information sur la hauteur d'étoile de la série initiale. C'est ce qui conduit à supposer l'existence d'une racine dominante, ce qui écarte les cas où les coefficients de la série ont un comportement asymptotique oscillatoire. On se servira de cette hypothèse pour prouver que les séries auxiliaires introduites au cours de la démonstration sont $\mathbb{N}$-rationnelles.

Exemple 27 La série r, dont la fonction génératrice est

$$f_r(z) = \frac{1}{(1-9z^2)(1-z-z^2)},$$

est de hauteur d'étoile 1 et a deux racines de module maximal (3 et -3). En revanche, la série, ayant pour terme général les termes d'indices pairs de r et dont la fonction génératrice est

$$h(z) = \frac{1}{2}\left(f_r(z) + f_r(-z)\right) = \frac{1-z}{(1-9z)(1-3z+z^2)},$$

est de hauteur d'étoile 2, car elle possède deux racines réelles positives conjuguées

$$\frac{3+\sqrt{5}}{2} \quad \text{et} \quad \frac{3-\sqrt{5}}{2}.$$

Cet exemple montre que la hauteur d'étoile n'est pas conservée quand on "déboîte" la série.

Preuve de la réciproque

Réciproquement, soit r une série $\mathbb{N}$-rationnelle ayant une racine dominante. On suppose que ses racines réelles positives sont des nombres d'Handelman, c'est à dire qu'elles vérifient les conditions suivantes

$$\forall i, \quad \exists k_i \text{ tel que} \begin{cases} \lambda_i^{k_i} \text{ soit un nombre de Perron} \\ \lambda_i^{k_i} \text{ n'a pas de conjugué algébrique réel positif.} \end{cases}$$

Le but est d'établir qu'une telle série est de hauteur d'étoile 1.

Méthode : la preuve est faite par induction sur le nombre de racines réelles positives de la série. On utilise essentiellement la représentation linéaire des séries et la caractérisation du rayon spectral des matrices compagnons primitives intégrales (dont l'interprétation en termes d'automates conduit à des automates de rang cyclique 1).

Comme r est une série $\mathbb{N}$-rationnelle, elle a une représentation (l, M, c), où

$$l \in \mathbb{N}^{1\times p}, M \in \mathbb{N}^{p\times p} \quad \text{et} \quad c \in \mathbb{N}^{p\times 1},$$

telle que

$$\forall k \geq 0 \qquad r_k = lM^k c.$$

A une permutation près, on peut supposer que la matrice M est de la forme

$$\begin{pmatrix} M_{11} & 0 & \dots & 0 \\ M_{21} & M_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ M_{m1} & \dots & M_{mm-1} & M_{mm} \end{pmatrix}$$

où les matrices M_{ii} sont non nulles et irréductibles. Le polynôme caractéristique de la matrice M s'écrit alors sous forme du produit des M_i, polynômes caractéristiques des matrices M_{ii}. D'après le Corollaire 2 (p.60), on peut alors construire une matrice compagnon irréductible intégrale ayant même rayon spectral que M_{ii} et dont le polynôme caractéristique C_i appartient à l'idéal $M_i\mathbb{Z}[z]$. Si la matrice M_{ii} est primitive, alors la matrice ainsi construite est également primitive.

Dans ces conditions, la série génératrice $f_r(z)$ de la série r s'écrit :

$$f_r(z) = \frac{P(z)}{\prod_{i=1}^{m}(1-Q_i)(z)} \quad ,$$

où $P \in \mathbb{Z}[z]$ et $\forall i$, $1-Q_i$ est le polynôme réciproque de C_i, et par suite $Q_i \in \mathbb{N}[z]$.

On raisonne alors par récurrence sur le nombre m de racines réelles positives de la série r. Soient $\lambda_1, \lambda_2, \ldots, \lambda_m$ ces racines rangées par ordre croissant (une racine multiple étant présente dans cette suite autant de fois que son ordre de multiplicité). On pose

$$(1-Q_1)(z) = 1 - \sum_{j=1}^{q} q_j z^j,$$

et on définit la suite $(s_n)_{n\geq q}$ par :

$$s_n = r_n - \sum_{j=1}^{q} q_j r_{n-j} \qquad (\forall n \geq q).$$

Si $m = 1$, alors $s_n = 0$ pour $n \geq h = \max(\deg P + 1, q)$ et

$$r_{n+h} = lM^n c \qquad \forall n \geq 0,$$

où

$$l = \begin{pmatrix} r_{h+q-1} \\ \vdots \\ r_{h+1} \\ r_h \end{pmatrix}^t, \quad M = \begin{pmatrix} q_1 & 1 & 0 & \ldots & 0 \\ \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & 0 & \ddots & 0 \\ q_{q-1} & \vdots & \vdots & \ddots & 1 \\ q_q & 0 & 0 & \ldots & 0 \end{pmatrix} \quad \text{et} \quad c = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

Deux arguments de nature différente peuvent être invoqués pour établir que la série r est de hauteur d'étoile 1. Le premier, analytique, est le suivant. De la représentation linéaire de la série r, on tire l'égalité

$$\sum_{n\geq h} r_n z^n = \frac{1}{1-Q(z)}(P(z) - (1-Q(z)) \sum_{n=0}^{h-1} r_n z^n),$$

où $(1-Q)$ est le polynôme réciproque du polynôme caractéristique de la matrice M. L'expression $(P(z) - (1-Q(z)) \sum_{n=0}^{h-1} r_n z^n)$ est alors nécessairement de degré supérieur ou égal à h, les seuls termes qui ne s'annulent pas proviennent donc du produit $Q(z) \sum_{n=0}^{h-1} r_n z^n$. On en déduit que le numérateur de la fraction rationnelle précédente est un polynôme à coefficients positifs. L'autre argument tient à la représentation d'une série $\mathbb{N}$-rationnelle par un automate : dans ce cas précis, l'automate obtenu est un automate en pétales, il est donc de rang cyclique 1. En conclusion, la série r est de hauteur d'étoile 1.

Remarque 13 Dans le cas d'une série n'ayant qu'une racine réelle positive, l'hypothèse de l'existence d'une racine dominante n'est pas nécessaire pour conclure, ce qui justifie l'énoncé de la Proposition 10 (p.78).

On suppose maintenant le résultat vrai pour une série $\mathbb{N}$-rationnelle qui a une racine dominante et pour racines réelles positives exactement $(m-1)$ nombres d'Handelman.

On va démontrer que la série s vérifie l'hypothèse de récurrence énoncée ci-dessus, on pourra alors prouver le résultat annoncé.

On prouve, dans un premier temps, qu'il existe un entier naturel h tel que

$$\forall n \geq h \qquad s_n \geq 0.$$

Comme la série r est $\mathbb{N}$-rationnelle, d'après la Proposition 6 (p.29), pour tout entier n suffisamment grand,

$$r_n = \sum_{0 \leq i \leq p} A_i(n)\alpha_i^n \quad \forall n \geq n_0,$$

où les α_i sont les inverses des pôles distincts de la fonction génératrice $f_r(z)$ de r et chaque A_i un polynôme de degré égal à la multiplicité du pôle $1/\alpha_i$ diminuée de 1.

On utilise alors la formule :

$$\begin{aligned}(*) \qquad & n^j\alpha_i^n - q_1(n-1)^j\alpha_i^{n-1} - \cdots - q_q(n-q)^j\alpha_i^{n-q} \\ = \; & n^j\alpha_i^n(1 - \sum_{k=1}^{q}\frac{q_k}{\alpha_i^k}) + jn^{j-1}\alpha_i^n\sum_{k=1}^{q}\frac{kq_k}{\alpha_i^k} + B(n)\alpha_i^n,\end{aligned}$$

où B est un polynôme de degré $j-2$.

Comme $(r_n)_{n\geq n_0}$ est combinaison linéaire de séries de la forme

$$\sum_{n\geq n_0} n^j\alpha_i^n z^n,$$

la série $\sum_{n\geq n_0+q} s_n z^n$ est combinaison linéaire de séries de la forme

$$\sum_{n\geq n_0+q} \left[n^j\alpha_i^n - q_1(n-1)^j\alpha_i^{n-1} - \cdots - q_q(n-q)^j\alpha_i^{n-q}\right] z^n.$$

On en déduit que

$$\forall n \geq n_0 + q, \quad s_n = \sum_{0\leq i\leq p} B_i(n)\alpha_i^n.$$

On pose $\alpha_0 = \lambda_m$. Comme λ_m est racine dominante de la série r,

$$\forall i \in \{1, 2, \ldots, p\}, \quad \lambda_m > |\alpha_i|.$$

Soient β l'ordre de multiplicité de λ_m dans le polynôme $\overline{1-Q}$ et a_0 le coefficient dominant du polynôme A_0, on a alors

$$r_n \sim_{n\to\infty} a_0 n^{\beta-1}\lambda_m^n.$$

Comme $r_n \geq 0$ et que r n'est pas un polynôme, $a_0 > 0$. On peut maintenant calculer l'équivalent de s_n quand n tend vers l'infini.

Si $\lambda_1 \neq \lambda_m$, le coefficient dominant de B_0 est, d'après $(*)$ (p.85),

$$a_0\lambda_m^n(1-\sum_{i=1}^{q}\frac{q_i}{\lambda_m^i}) = a_0\lambda_m^n(1-Q_1)(1/\lambda_m).$$

Or, $(1-Q_1)(1/\lambda_m) > 0$ car ce polynôme a pour seule racine réelle positive $1/\lambda_1$ et $1/\lambda_1 > 1/\lambda_m$. Comme

$$s_n \sim_{n\to\infty} a_0\lambda_m^n(1-Q_1)(1/\lambda_m)n^{\beta-1},$$

on en déduit que pour tout n suffisamment grand, $n \geq h$, $s_n \geq 0$.

Si $\lambda_1 = \lambda_m$, $\beta = m$, comme $1/\lambda_1$ est racine du polynôme $(1-Q_1)$, le polynôme B_0 est de degré $m-2$ et son coefficient dominant est alors, d'après $(*)$ (p.85),

$$a_0(m-1)\lambda_m^n\sum_{i=1}^{q}\frac{iq_i}{\lambda_m^i} > 0.$$

Comme

$$s_n \sim_{n\to\infty} a_0(m-1)\lambda_m^n\sum_{i=1}^{q}\frac{iq_i}{\lambda_m^i}n^{m-2},$$

on en déduit que pour tout n suffisamment grand, $n \geq h$, $s_n \geq 0$.

On a donc démontré que la suite $(s_n)_{n\geq h}$ est à coefficients positifs. De plus, la fonction génératrice de la série s s'écrit

$$f_s(z) = f_r(z)(1-Q_1)(z) - W(z),$$

où W est un polynôme de degré $(q-1)$, la série s est donc $\mathbb{Z}$-rationnelle et a pour racine dominante λ_m. Comme, de plus, la série s a pour seules racines réelles positives $(m-1)$ nombres d'Handelman, d'après l'hypothèse de récurrence, la série s est $\mathbb{N}$-rationnelle de hauteur d'étoile 1. Il existe donc une représentation linéaire (l_s, M_s, c_s), où les coefficients des matrices l_s, M_s et c_s sont des entiers naturels, telle que

$$s_{n+h} = l_s {M_s}^n c_s \quad \forall n \geq 0$$

et que la matrice M_s soit associée à un automate de rang cyclique 1 (automate qui, privé d'un de ses états ainsi que des transitions ayant pour extrémité cet état, devient acyclique).

On considère alors le triplet (L, N, C) défini par

$$L = \left(\begin{array}{c} \dfrac{l_s}{r_{h+q}} \\ \vdots \\ r_{h+1} \\ r_h \end{array}\right)^t, \quad N = \left(\begin{array}{c|cccc} M_s & c_s & 0 & \dots & 0 \\ \hline 0 & q_1 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \vdots & 0 & \ddots & 0 \\ \vdots & q_{q-1} & \vdots & \vdots & \ddots & 1 \\ 0 & q_q & 0 & 0 & \dots & 0 \end{array}\right) \quad \text{et} \quad C = \left(\begin{array}{c} 0 \\ \vdots \\ 0 \\ 1 \end{array}\right).$$

On vérifie par récurrence sur n que, pour tout $n \geq 0$,

$$LN^n = (l_s {M_s}^n | r_{n+h+q}, \dots, r_{n+h})$$

et on déduit que

$$r_{n+h} = LN^nC \quad \forall n \geq 0.$$

On a ainsi démontré que la série r est de hauteur d'étoile 1, ce qui achève la preuve du théorème.

2.3.3 Décidabilité

La décidabilité de la hauteur d'étoile dans le cas des séries $\mathbb{N}$-rationnelles ayant une racine dominante vient de la possibilité de calculer, pour chaque racine réelle positive λ, l'entier k maximal tel que λ^k vérifie les conditions du Théorème 17 (p.78). La méthode est analogue à celle utilisée pour décider la $\mathbb{N}$-rationalité d'une série $\mathbb{Z}$-rationnelle (se reporter à [Soi76]).

On construit le polynôme à coefficients entiers

$$T(x) = \prod_{i,j} (\beta_i x - \beta_j)$$

où β_i décrit l'ensemble des racines de module λ. On détermine ensuite l'entier n_T tel que

$$\forall n > n_T, \qquad \phi(n) > \deg(T)$$

où ϕ est l'indicateur d'Euler et on factorise le polynôme T en un produit de polynômes cyclotomiques d'ordre inférieur à n_T. L'entier k est alors le p.p.c.m. des ordres des polynômes cyclotomiques intervenant dans la factorisation de T.

Conclusion

◦ Le Théorème 17 et la Proposition 10 (p.78) permettent de décider la hauteur d'étoile de séries $\mathbb{N}$-rationnelles ayant une seule racine positive, ayant une racine dominante ou dont l'écriture sous forme d'emboîtement de séries $\mathbb{Z}$-rationnelles ne fait pas apparaître

de nouvelle racine positive. C'est le cas, par exemple, pour une série ayant une racine périodique multiple mais unique

$$f_r(z) = \frac{1}{(1-z^n)^q}.$$

On peut conjecturer que le fait d'avoir pour racines réelles positives exclusivement des nombres d'Handelman suffit à caractériser les séries $\mathbb{N}$-rationnelles de hauteur d'étoile 1.

◦ Le problème de la hauteur d'étoile des séries $\mathbb{N}$-rationnelles en plusieurs variables commutatives demeure ouvert. On peut se demander par exemple si, dans le cas de deux variables commutatives, la hauteur est encore bornée.

Deuxième partie

Distributions de longueurs de codes

Introduction

Le codage évoque un procédé de transformation d'un objet associé à un procédé inverse, appelé le décodage, qui permet de restituer l'objet initial.

Les débuts de la théorie du codage et de la théorie de l'information datent des travaux pionniers de Shannon de 1948 ([Sha48]). La théorie des codes s'est ultérieurement développée dans deux directions indépendantes. La première est l'étude des codes de longueur constante dans l'optique de la détection et de la correction d'erreurs. L'autre direction, initiée par Schützenberger en 1955 ([Sch56]), a conduit au développement de la théorie des codes de longueurs variables. Cette théorie est maintenant une branche de l'informatique théorique, qui a des liens importants avec les langages formels, la combinatoire sur les mots, la théorie des automates, la théorie des semigroupes et la dynamique symbolique.

Son objet est l'étude des propriétés des factorisations de mots en suites finies de mots appartenant à un ensemble donné. Plus précisément, on suppose donnés un *alphabet source* B et un *alphabet de canal* A. On cherche à coder des messages v écrits sur B en messages w sur l'alphabet A. Les lettres de B sont alors mises en correspondance avec les mots d'un code X sur l'alphabet A. Chaque lettre du message source v est remplacée par le mot qui lui est associé dans X. De plus, le codage doit être fait de telle sorte que le décodage du mot obtenu $w \in X^*$ ne conduise à aucune *ambiguïté*, quant au texte original.

La distribution de longueurs d'un code est la suite dont le terme d'ordre n correspond au nombre de mots de longueur n du code. Les suites ainsi définies permettent d'obtenir des conditions nécessaires pour qu'un code ait certaines propriétés, en particulier celles de finitude, de maximalité et de rationalité. Ainsi, quand le code est rationnel, la série dont les coefficients constituent la distribution de longueurs du code est alors $\mathbb{N}$-rationnelle.

On peut également s'intéresser au problème inverse, à savoir : étant donné une série à coefficients entiers positifs, à quelles conditions peut-on construire un code ayant une propriété spécifique et cette série pour série génératrice ?

Dans cette partie, on s'est intéressé aux distribution de longueurs des codes circulaires, d'une part et à celles des codes rationnels préfixes.

Dans le premier chapitre de cette partie, on rappelle des résultats connus sur les codes et les distributions qui seront utilisés dans ce qui suit. On pourra consulter [BP85] pour les preuves et pour une présentation plus générale du sujet.

Les codes circulaires sont ceux pour lesquels tout message lu sur un cercle a au plus un décodage. Ils ont été introduits en raison de leurs propriétés de synchronisation qui leur fait jouer un rôle important dans la corrections d'erreurs. Il interviennent aussi bien dans

des applications (analyses de séquences biologiques [GG65], [GGW58]) qu'en combinatoire ([Sta86] Section 4.7).

Le Chapitre 2 (p.103) est consacré aux distributions de longueurs des codes circulaires. On prouve trois nouveaux résultats : on étend la caractérisation des distributions de longueurs, on en donne une nouvelle formulation et on établit une condition nécessaire et suffisante pour qu'une suite d'entiers positifs soit la distribution de longueurs d'un code circulaire maximal sur un alphabet fini.

Les codes préfixes ont été définis par Morse comme les codes dont aucun mot n'est le début d'un autre. Ils peuvent être vus comme des codes à décodage instantané, tout message étant immédiatement décodable au cours de sa lecture de gauche à droite.

Dans le Chapitre 3 (p.139), on étudie les distributions de longueurs des codes préfixes rationnels. On présente leurs liens avec une classe particulière de séries $\mathbb{N}$-rationnelles : les DOL-séries. On donne, en utilisant la technique d'éclatement des états empruntée à la dynamique symbolique, une condition suffisante pour qu'une suite soit la distribution de longueurs d'un code préfixe maximal sur un alphabet dont le nombre de lettres est fixé.

Chapitre 1

Codes

Introduction

Ce chapitre est consacré au rappel de définitions et résultats classiques de la théorie des codes. Il se limite aux notions qui interviendront dans les chapitres suivants, en particulier celles relatives aux codes circulaires et aux codes préfixes. Pour une présentation plus générale de ce sujet et pour les preuves que l'on ne mentionne pas, on pourra se reporter à [BP85].

1.1 Codes

On suppose donnés un *alphabet source* B et un *alphabet de canal* A. On cherche à coder des messages v écrits sur B en messages w sur l'alphabet A. Les lettres de B sont alors mises en correspondance avec les mots d'un code X sur l'alphabet A. Chaque lettre du message source v est remplacée par le mot qui lui est associé dans X. De plus, le codage doit être fait de telle sorte que le décodage du mot obtenu $w \in X^*$ ne conduise à aucune *ambiguïté*, quant au texte original.

De manière plus formelle, un sous-ensemble X du monoïde libre $A^\star$ est un *code* sur A si, et seulement si,

$$\forall n, m \geq 1 \qquad \text{et} \qquad x_1, \ldots, x_n, x'_1, \ldots, x'_m \in X$$
$$x_1 x_2 \cdots x_n = x'_1 x'_2 \cdots x'_m \quad \Rightarrow \quad n = m \quad \text{et} \quad x_i = x'_i \quad \text{pour} \quad i = 1, \ldots, n.$$

En d'autres termes, un ensemble X est un code si tout mot w de X^+ a une unique factorisation en mots de X. Une telle décomposition d'un mot w de X^+ en une suite finie d'éléments, $x_1 x_2 \cdots x_n$, de X est appelée une *X-factorisation*. Les termes, x_i, de la suite sont des *facteurs* du mot w.

Proposition 12 *Si un partie $X \subset A^*$ est un code, alors tout morphisme $\phi : B^* \to A^*$ qui induit une bijection d'un alphabet B sur X est injectif. Réciproquement, s'il existe un morphisme injectif $\phi : B^* \to A^*$ tel que $X = \phi(B)$, alors X est un code.*

Les mots de X codent alors les lettres de B. L'injectivité du morphisme ϕ assure que le texte codé pourra être décodé de manière unique pour obtenir le texte original.

Un morphisme

$$\phi : B^* \to A^*$$

qui est injectif et tel que $X = \phi(B)$ est appelé un *morphisme codant* pour X. Pour tout code $X \subset A^*$, on obtient un morphisme codant à chaque fois que l'on étend une bijection d'un ensemble B dans X en un morphisme de B^* dans A^*.

Exemple 28 Le code de Morse X_M est un code sur l'alphabet $\{., \wedge, -\}$ dont les mots sont mis en correspondance avec les lettres $a, b, \ldots, z$. Le symbole $\wedge$ n'apparaît qu'à la fin des mots de X_M, ce qui assure que X_M est un code.

a	$.-\wedge$	j	$.---\wedge$	s	$...\wedge$
b	$-...\wedge$	k	$-.-\wedge$	t	$-\wedge$
c	$-.-.\wedge$	l	$.-..\wedge$	u	$..-\wedge$
d	$-..\wedge$	m	$--\wedge$	v	$...-\wedge$
e	$.\wedge$	n	$-.\wedge$	w	$.--\wedge$
f	$..-.\wedge$	o	$---\wedge$	x	$-..-\wedge$
g	$--.\wedge$	p	$.--.\wedge$	y	$-.--\wedge$
h	$....\wedge$	q	$--.-\wedge$	z	$--..\wedge$
i	$..\wedge$	r	$.-.\wedge$		

On peut noter que les mots du code de Morse sont de longueurs variables.

Exemple 29 Le code ASCII X_A sur l'alphabet binaire $\{0, 1\}$ constitue un autre exemple de code. A la différence du code de Morse, tous les mots sont, dans ce cas, de même longueur égale à 7.

Par définition, un sous-monoïde M de A^* est *libre* s'il existe un isomorphisme

$$\phi : B^* \to M$$

d'un monoïde libre B^* dans M. Les codes sur l'alphabet A peuvent alors être caractérisés de la façon suivante (cf. [BP85] Proposition 2.2 p.43).

Proposition 13 *Si M est un sous-monoïde libre de A^*, alors son système minimal de générateurs est un code. Réciproquement, si $X \subset A^*$ est un code, alors le sous-monoïde X^* de A^* est libre et X est son système minimal de générateurs.*

La *longueur* $|w|$ d'un mot $w = a_1 a_2 \dots a_n$, où les a_i sont des lettres, est égal au nombre n de lettres qui apparaissent dans w. On peut maintenant définir la série génératrice f_X d'un code $X \in A^*$ comme la série formelle, en une seule variable, dont le $n$ième coefficient est égal au nombre de mots de longueur n du code, soit

$$f_X(z) = \sum_{i \geq 1} \alpha_i z^i = \sum_{i \geq 1} \mathrm{Card}(X \cap A^i) z^i.$$

La suite $\alpha = (\alpha_i)_{i \geq 1}$, ainsi définie, est appelée la *distribution de longueurs* du code X.

Le résultat suivant ([McM56]) donne une condition nécessaire pour qu'une suite d'entiers positifs soit la distribution de longueurs d'un code sur un alphabet fini.

Théorème 18 (Inégalité de Kraft-McMillan) *Soit X un code sur un alphabet à k lettres, alors*

$$\sum_{x \in X} k^{-|x|} \leq 1$$

ou, de façon équivalente,

$$\sum_{n \geq 0} \alpha_n k^{-n} \leq 1 \qquad \textit{avec} \quad \alpha_n = \textit{Card}\ (X \cap A^n).$$

En d'autres termes, si un ensemble a un nombre trop important de mots de petite longueur, il ne peut pas être un code.

L'énoncé complet du théorème de Kraft-McMillan comprend une réciproque que l'on mentionne ultérieurement (se reporter à la Proposition 29 p.144).

Soient X un code et $f_X = \sum_{i \geq 0} \alpha_i z^i$ sa série génératrice. La série génératrice $f_{X^*}(z)$ du monoïde libre $X^* = \sum_{i \geq 1} X^i$, engendré par X, est, par définition,

$$f_{X^*} = \sum_{i \geq 0} f_{X^i}(z),$$

où $f_{X^i}(z)$ est la série génératrice de X^i, et, comme X est un code, $f_{X^i}(z) = (f_X(z))^i$. On obtient ainsi

$$f_{X^*}(z) = \sum_{i \geq 1} (f_X(z))^i = \frac{1}{1 - f_X(z)} = \frac{1}{1 - \sum_{i \geq 1} \alpha_i z^i}. \tag{1.1}$$

Par suite, le rayon de convergence ρ de la série $f_{X^*}(z)$ est égal à la plus petite valeur positive pour laquelle $f_X(z)$ vaut 1. En effet, $f_X(z) = \sum_{i \geq 1} \alpha_i z^i$ est une fonction continue et strictement croissante sur $\mathbb{R}^+$ et $f_X(0) = 0$, il existe donc un réel positif ρ tel que $f_X(\rho) = 1$. De plus, si $f_X(z_0) = f_X(\rho) = 1$, alors

$$\sum_{i \geq 1} \alpha_i |z_0|^i \geq |\sum_{i \geq 1} \alpha_i z_0^i| = 1 = \sum_{i \geq 1} \alpha_i \rho^i.$$

Par suite, $|z_0| \geq \rho$.

Les distributions de longueurs permettent d'obtenir des conditions nécessaires pour qu'un code ait certaines propriétés, en particulier celles de finitude, de maximalité et de rationalité.

On peut également s'intéresser au problème inverse, à savoir : étant donné une série s à coefficients entiers positifs, à quelles conditions peut-on construire un code ayant une propriété spécifique et dont la série génératrice est s ?

L'exemple le plus simple est celui de la finitude : si un code X est fini, sa distribution de longueurs est une suite finie. Réciproquement, si un polynôme $P(z)$ à coefficient entiers positifs vérifie l'inégalité de Kraft-McMillan, *i.e.*,

$$\exists k \in \mathbb{N}^*, \qquad \text{tel que} \qquad P(1/k) \leq 1,$$

alors on peut construire un code fini sur un alphabet à k lettres dont $P(z)$ est la série génératrice.

On s'intéressera à ce type de problèmes dans ce qui suit.

1.2 Maximalité et complétude

De nombreux problèmes ayant trait à l'optimisation du processus de codage sont liées aux propriétés extrêmes des codes, telles que celles de maximalité et de complétude. Les principaux résultats de cette section sont dus à Schützenberger ([Sch56]). Pour une synthèse des résultats sur ce sujet, on pourra se reporter à [BL96].

Un code X est dit *maximal* sur l'alphabet A s'il n'est pas inclus dans un autre code sur le même alphabet, *i.e.*,

$$(\quad \text{si} \quad X \subset X' \quad \text{et} \quad X' \quad \text{code} \quad) \qquad \Rightarrow \qquad X = X'.$$

Proposition 14 *Soit X un code maximal fini sur l'alphabet A. Alors, pour toute partie non vide B de A, le code $X \cap B^*$ est un code maximal sur le nouvel alphabet B. En particulier, pour toute lettre a de A, il existe un entier positif tel que le mot a^n appartienne au code X.*

La preuve de cette proposition est donnée dans [BP85] (Proposition 5.9 p.67).

Un code est dit *complet* si, et seulement si, tout mot de A^* est facteur d'un mot de X^* : pour tout mot w de A^*,

$$A^* w A^* \cap X^* \neq \emptyset.$$

En d'autres termes, si on note $F(L)$ l'ensemble des facteurs du langage $L \subset A^*$, *i.e.*, l'ensemble des mots de A^* qui apparaissent dans la factorisation d'un mot de L, alors un code $X \subset A^*$ est complet si, et seulement si,

$$F(X^*) = A^*.$$

Ainsi, tout mot de A^* apparaît alors comme fragment d'un message codé. En ce sens, un code complet utilise toute la capacité du canal de transmission.

Exemple 30 Le code de Morse X_M n'est pas un code complet. En effet, le mot $\wedge\wedge$, par exemple, n'est facteur d'aucun mot de X_M^*.

Sur l'alphabet $A = \{a, b\}$, le code $X = b^*a$ est complet.

Un code complet est dit *dense* si $F(X) = A^*$, il est dit *coupant* dans le cas contraire.

On rappelle qu'une *mesure de Bernoulli* sur A^*, $\pi : A^* \to \mathbb{R}_+$, est un morphisme à valeurs dans le monoïde multiplicatif $\mathbb{R}_+$ des réels positifs et tel que

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

Une mesure est dite *positive* si pour tout $a \in A$, $\pi(a) > 0$.

Exemple 31 Distribution de Bernoulli uniforme
Soit A un ensemble non vide. On pose

$$\forall a \in A, \qquad \pi(a) = \frac{1}{\mathrm{Card}(A)}.$$

L'application π définit alors une distribution de Bernoulli positive sur A^* appelée la distribution *uniforme*.

Le résultat suivant, dont la preuve est donnée dans [BP85] (Théorème 5.10 p.68), met en évidence les liens entre les notions de maximalité et de complétude. Il permet également de caractériser les distributions de longueurs de codes ayant ces propriétés.

Théorème 19 *Si X est un code coupant, alors les conditions suivantes sont équivalentes*

1. *X est complet.*
2. *X est maximal.*
3. *Il existe une distribution de Bernoulli positive π telle que $\pi(X) = 1$.*
4. *Pour toute distribution de Bernoulli positive π, $\pi(X) = 1$.*

Ainsi, si A est un alphabet fini à k lettres et si π est la distribution de Bernoulli uniforme sur A, l'égalité avec 1 dans l'inégalité de Kraft-McMillan (Théorème 18 p.95) :

$$\sum_{n \geq 0} \alpha_n k^{-n} = 1$$

caractérise les distributions de longueurs des codes coupants maximaux sur l'alphabet A.

Méthode de complétion

On donne maintenant la méthode générale de complétion des codes, en particulier des codes rationnels, due à Ehrenfeucht et Rozenberg (cf. [ER85]). On rappelle, pour commencer, la définition d'un mot sans bord ainsi que des propriétés liées à cette notion.

Un mot w de A^+ est dit *sans bord* si aucun facteur propre gauche non vide de w n'est également un facteur droit. En d'autres termes, le mot w est sans bord si, et seulement si,

$$w \in uA^+ \cap A^+u \qquad \Rightarrow \qquad u = 1.$$

Si w est sans bord, alors

$$wA^* \cap A^*w = wA^*w \cup w.$$

Soit A un alphabet ayant au moins deux lettres ; alors pour tout mot u de A^+, il existe un mot v de A^* tel que uv soit sans bord. En effet, soit a la première lettre de u et soit $b \in A \setminus \{a\}$, alors le mot $w = uab^{|u|}$ est sans bord.

Théorème 20 *Soient X un code et $y \in A^*$ un mot sans bord tel que*

$$X^* \cap A^*yA^* = \emptyset$$

(i.e., y n'est facteur d'aucun mot de X^*) et soit $U = A^* \setminus X^* \setminus A^*yA^*$. Alors

$$Y = X \cup y(Uy)^*$$

est un code complet.

De plus, si X est rationnel, Y est également rationnel.

1.3 Rationalité

Soient A un alphabet et $\mathcal{A} = (Q, 1, F, E)$ un automate ayant un unique état initial, noté 1, et dont les transitions sont étiquetées sur l'alphabet A.

On note $X_{\mathcal{A}} \subset A^*$ l'ensemble des étiquettes des chemins *de premier retour*, c'est-à-dire des chemins allant de l'état 1 à lui-même et ne passant à aucun autre moment par cet état distingué (cf. Exemple 32).

On introduit maintenant la notion d'automate non-ambigu qui généralise celle, introduite précédemment, d'automate déterministe. Un automate $\mathcal{A}$, sur l'alphabet A, est dit *non-ambigu* si pour tout couple (p, q) d'états de l'automate et pour tout mot w de A^*, il existe au plus, dans $\mathcal{A}$, un chemin de p à q d'étiquette w.

Exemple 32 Soit $A = \{a, b\}$. On considère l'automate $\mathcal{A}$ sur l'alphabet dont le graphe est donné par la Figure 1.1 et dont l'unique état initial est l'état 1. Alors l'automate $\mathcal{A}$ est non-ambigu et l'ensemble ses chemins de premier retour est

$$X_{\mathcal{A}} = \{aa, ba, baa, bba, bb\}.$$

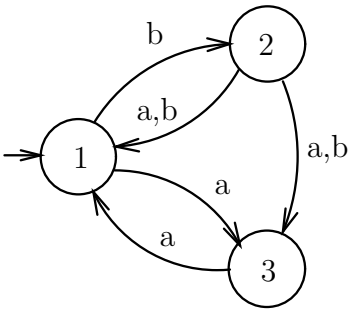


FIG. 1.1 – *Automate $\mathcal{A}$ non ambigu, $X_{\mathcal{A}} = \{aa, ba, baa, bba, bb\}$*

De plus, d'après la Proposition 15, $X_{\mathcal{A}}$ est donc un code sur l'alphabet A.

Proposition 15 *Un ensemble rationnel X est un code si, et seulement si, il existe un automate non-ambigu $\mathcal{A}$ dont X constitue l'ensemble des étiquettes des chemins de premier retour, soit*

$$X = X_{\mathcal{A}}.$$

Quand le code est rationnel, sa distribution de longueurs est une suite $\mathbb{N}$-rationnelle ([CS63]). Sa série génératrice est reconnue par tout automate obtenu, à partir d'un automate reconnaissant le code, en remplaçant chaque lettre étiquetant une transition par l'entier 1.

Les automates non-ambigus permettent également une caractérisation des codes finis.

Proposition 16 *Un code rationnel $X \subset A^*$ est fini si, et seulement si, il existe un automate non-ambigu $\mathcal{A} = (Q, 1, F, E)$ étiqueté sur A, tel que $X = X_{\mathcal{A}}$, dont tous cycles passent par l'état distingué* 1.

Exemple 33 Dans l'automate de la Figure 1.1, tous les cycles passent par l'état 1 et le code $X_{\mathcal{A}}$ est fini.

Enfin, la complétude d'un code $X = X_{\mathcal{A}}$ peut également être traduite en termes d'automates de la manière suivante : tout mot $w \in A^*$ est l'étiquette d'un chemin dans l'automate $\mathcal{A}$, ce qui permet de caractériser les codes rationnels complets.

On peut noter que tout code rationnel est coupant et, par suite, que les notions de maximalité et de complétude coincident dans le cas de codes rationnels.

1.4 Délai de décodage

Pouvoir commencer le déchiffrage d'un message codé sans attendre la réception de la totalité du message peut être intéressant ; c'est ce qui conduit à étudier les codes permettant une telle opération : les codes à délai de décodage borné.

Un langage $X \subset A^+$ est dit *à délai de décodage borné*, s'il existe un entier positif d tel que

$$\forall x, x' \in X, \quad \forall y \in X^d, \forall u \in A^*, \qquad xyu \in x'X^* \quad \Rightarrow \quad x = x'. \tag{1.2}$$

Le plus petit entier d vérifiant (1.2) est alors appelé le *délai de décodage* de X. En d'autres termes, d mesure le nombre de facteurs à identifier, dans la lecture du mot, entre le moment où est identifié un possible facteur d'une X-factorisation et le moment où l'on a la confirmation que ce facteur est celui de la factorisation du mot. L'intérêt de cette notion est mis en évidence par le résultat suivant (cf.[BP85] Proposition 8.1 p128).

Proposition 17 *Tout langage $X \subset A^+$ à délai de décodage borné est un code.*

Les codes ayant un délai de décodage nul sont appelés codes *préfixes* ou codes *instantanés*. Dans ce cas, aucun mot du code ne peut être préfixe d'un autre. Cette propriété est la caractérisation utilisée par Morse pour les définir.

Exemple 34 Le code de Morse (cf. Exemple 28) et le code ASCII sont des codes préfixes. Le code $X = \{a, aab\}$ n'est pas préfixe et a pour délai de décodage 2.

Exemple 35 Le code $X = \{a, ab, bb\}$ n'a pas de délai de décodage borné, puisque, pour tout entier positif n, le mot ab^n ne peut être décodé qu'après sa lecture complète.

Ce dernier exemple constitue un code préfixe si la lecture est effectuée de droite à gauche. De tels codes sont dits *suffixes*. Un code qui est à la fois préfixe et suffixe est dit *bipréfixe*.

1.5 Synchronisation

Une autre exemple intéressant de famille de codes est celle des codes uniformément synchronisants, introduite par Golomb et Gordon ([GG65]). On dit qu'un code X sur un alphabet A est *uniformément synchronisant* s'il existe un entier positif s tel que

$$uxyv \in X^*, \quad \text{avec} \quad x, y \in X^s, u, v \in A^* \quad \Rightarrow \quad ux, yv \in X^*. \tag{1.3}$$

Le plus petit entier s vérifiant (1.3) est alors appelé le *délai de synchronisation* du code.

Dans la pratique, la présence dans le message codé $uxyv$ de la paire synchronisante xy force le décodage à passer entre x et y. De cette manière, une erreur intervenant avant x n'affecte pas le décodage de yv, sa propagation est donc limitée.

Exemple 36 Le code de Morse X_M a pour délai de synchronisation 1, puisque la fin de chaque mot est marquée par le symbole blanc $\wedge$.

Exemple 37 Le code bipréfixe $X + ab^*c \cup \{b\}$ n'a pas de délai de synchronisation borné : en effet, pour tout entier positif n, $b^n \in X^n$ et $ab^nc \in X$.

On peut noter que le délai de synchronisation s d'un code est supérieur à son délai de décodage. En effet,

$$\forall y \in X, x \in X^s, v \in A^*, \qquad yxv \in X^* \quad \Rightarrow \quad xv \in X^*,$$

ce qui montre que le délai de décodage de X est au plus s.

Exemple 38 Codes "comma-free" ([GGW58])
Un code $X \subset A^+$ est dit *comma-free* si X est bipréfixe et a 1 pour délai de synchronisation. De manière équivalente, X est comma-free si

$$\forall x \in X^+, \forall u, v \in A^*, \qquad uxv \in X^* \Rightarrow \quad u, v \in X^*.$$

Ces codes sont particulièrement intéressants parce qu'ils permettent un décodage facile : dans un mot de X^*, dès qu'un facteur est identifié comme un mot de X, il correspond à une X-factorisation.

De manière plus générale, un code coupant est dit *synchronisant* s'il existe des mots x et y de X^* tels que pour $u, v \in A^*$

$$uxyv \in X^* \quad \Rightarrow \quad ux, yv \in X^*.$$

Proposition 18 *Soit X un code coupant, alors X est complet et synchronisant si, et seulement si,*

$$\exists x, y \in X^*, \quad \textit{tels que} \quad xA^*y \subset X^*.$$

La preuve de ce résultat est présentée dans [BP85] (Proposition 6.5 p.240).

Exemple 39 Codes circulaires (voir Chapitre 2 p.103)
Les codes circulaires sont ceux qui définissent au plus une factorisation des mots écrits sur un cercle. Les codes comma-free sont des codes circulaires.

Proposition 19 *Tout code circulaire coupant est synchronisant*

Pour la preuve, on pourra se reporter à [BP85] (Corollaire 1.3 p.325).

1.6 Composition

On introduit maintenant l'opération de composition qui permet, à partir de codes simples, d'en construire de plus compliqués.

Soient $Z \subset A^*$ et $Y \subset B^*$ deux codes tels que B soit l'alphabet sur lequel est écrit Y ($B = \text{alph}(Y)$), alors les codes Y et Z sont dits *composables* s'il existe une bijection de B sur Z. Si ϕ est une telle bijection, alors Y et Z sont composables par ϕ et ϕ induit un morphisme de B^* dans A^* qui est injectif puisque Z est un code.

L'ensemble $X = \phi(Y) \subset Z^* \subset A^*$ est obtenu par composition de Y et Z au moyen de ϕ et est noté

$$X = Y \circ_\phi Z \qquad \text{ou} \qquad X = Y \circ Z.$$

Comme l'application ϕ est injective, X et Y sont en bijection ; de plus les mots de X sont obtenus en remplaçant dans les mots de Y chaque lettre de B par son image par ϕ.

Le résultat suivant met en évidence l'intérêt de l'opération de composition (pour la preuve, on se reportera à [BP85] Propositions 6.1 p.71 et 6.3 p.73).

Proposition 20 *Si Y et Z sont deux codes composables alors $X = Y \circ Z$ est un code. Si, de plus,*

- les codes Y et Z sont circulaires, X est circulaire,

- les codes Y et Z sont préfixes, X est préfixe,

- les codes Y et Z sont coupants, X est coupant.

Chapitre 2

Codes circulaires

Introduction

On étudie ici une famille particulière de codes appelés codes circulaires. Leur spécificité tient au fait qu'ils définissent une unique factorisation des mots écrits sur un cercle.

Ils ont été introduits par Golomb et Gordon ([GG65]) en raison de leur forte propriété de synchronisation. Ainsi, tout code circulaire coupant est synchronisant et tout code uniformément synchronisant est circulaire. Pour cette raison, ils jouent un rôle important dans la correction d'erreurs.

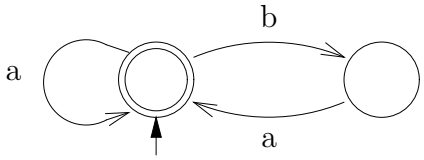
Un type particulier de codes circulaires, les codes comma-free, ont été l'objet de nombreuses investigations ([GGW58]). Quand ils ont été définis, on pensait que le code biologique en était un (hypothèse de Crick, [CGO57]). En effet, les 20 acides aminés apparaissant dans les protéines sont codés par des mots de trois lettres sur l'alphabet des quatre bases A, C, G et T. Or, dans un code circulaire, le nombre maximal de mots de 3 lettres sur un alphabet à 4 lettres est précisément 20. Plus tard, il est apparu que le code biologique n'etait même pas un code au sens où on l'entend ici, plusieurs triplets de bases pouvant coder le même acide aminé. Plus récemment, par une étude statistique de la répartition des trinucléotides dans les gènes codant les protéines, D. Arquès et C. Michel ([AM95], [AM96] et [AFM96]) ont identifié un ensemble de codons constituant un code circulaire.

Les codes circulaires apparaissent dans de multiples problèmes de combinatoire des mots. Par exemple, pour calculer le nombre de mots circulaires sur l'alphabet $A = \{a, b\}$ ne comportant pas deux occurrences consécutives de la lettre b, on peut utiliser le codage

$$\begin{array}{ll} \alpha : & A^* \to B^* = \{a, ba\}^* \\ & a \to a \\ & b \to ba \end{array}$$

représenté par l'automate ou la matrice M de la Figure 2.1 (p.104).

Le coefficient f_n d'ordre n de la série génératrice du monoïde libre engendré par le



$$M = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

FIG. 2.1 – *Codage* α

code circulaire $\{a, ba\}$

$$\sum_{n\geq 0} f_n z^n = \frac{1}{1 - z - z^2} = \det(I - Mz)^{-1}$$

est alors égal au nombre de mots circulaires de A^* de longueur n ($n \geq 2$) n'ayant pas bb comme facteur. D'autres exemples de problèmes combinatoires résolus à l'aide des codes circulaires sont présentés dans [Sta86] (Section 4.7).

Enfin, les codes circulaires sont liés aux problèmes de factorisation du monoïde libre, tous les facteurs intervenant dans une telle factorisation sont circulaires ([Sch59], [Sch65a], [Vie74], [Vie78], [Kro87], [DT88]).

Dans ce qui suit, on prouve quatre nouveaux résultats. On décrit, en fonction de différents paramètres, la série génératrice de l'étoile d'un code circulaire. On généralise, dans plusieurs directions, la caractérisation des distributions de longueurs des codes circulaires établie dans le cas d'un alphabet fini par Schützenberger ([Sch65b]). D'une part, on remplace l'alphabet fini par un alphabet quelconque dont les éléments ont des poids, ce qui permet d'étendre le résultat à deux distributions de longueurs. D'autre part, on restreint les conditions, ce qui permet d'établir la décidabilité dans le cas d'une distribution finie. On donne une nouvelle formulation de cette caractérisation qui met en évidence la décidabilité dans le cas d'une suite finie. Enfin, on établit une condition nécessaire et suffisante pour qu'une suite d'entiers positifs soit la distribution de longueur d'un code circulaire maximal sur un alphabet fini. Les preuves présentées utilisent essentiellement des arguments combinatoires.

La première partie de ce chapitre est consacrée au rappel de définitions et résultats relatifs aux codes circulaires et à leurs distributions de longueurs (cf.[BP85]). On introduit également la notion d'alphabet pondéré, qui n'est autre qu'un ensemble de symboles auxquels sont associés des poids entiers. Shannon ([Sha48]) fut l'un des premiers à s'intéresser aux alphabets dont les lettres ont des coûts quelconques, ces derniers représentent dans ce cas la durée des symboles de transmission. Ces alphabets furent utilisés par la suite en théorie de l'information afin de généraliser la notion d'entropie qu'il avait proposée ([Csi69], [Kra62]). Ils apparaissent dans de nombreux articles ayant trait aux arbres ou, ce qui est équivalent, aux codes préfixes optimaux relativement à des fonctions de coût ([Huf52], [Kar61], [CG74], [Lon76], [Cot80]). Selon les applications, les coûts sont des paramètres liés à l'amplitude, la durée ou l'énergie d'un signal.

Dans la deuxième partie (p.107), on donne différentes manières de calculer la distribution de longueurs du monoïde engendré par un code circulaire.

Dans la partie suivante (p.115), on étend la caractérisation des distributions de longueurs des codes circulaires établie par Schützenberger ([Sch65b]) au cas de codes sur un alphabet pondéré (Théorème 23 p.116).

On en donne, au cours de la Section 2.4 (p.120), une nouvelle formulation, qui fait l'objet du Théorème 24 (p.121), mettant ainsi en évidence une propriété de ces distributions.

Enfin, la Section 2.5 est consacrée aux codes maximaux et complets. On y définit une mesure de Bernoulli uniforme sur un alphabet pondéré, on donne une preuve directe de l'inégalité de Kraft-McMillan et une condition nécessaire et suffisante pour qu'une série à coefficients entiers positifs soit la distribution de longueurs d'un code circulaire maximal (Théorème 25 p.134). On vérifie finalement que la méthode de complétion des codes donnée par Ehrenfeucht et Rozenberg (Théorème 20 p.98) s'applique également aux codes circulaires.

2.1 Préliminaires

Alphabet pondéré

On définit maintenant un *alphabet pondéré* comme un couple (A, λ) formé d'un alphabet A et d'une application $\lambda : A \to \mathbb{N}$. Celle-ci peut être interprétée comme un coût aussi bien que comme une distance ou une longueur. On étend la fonction λ aux mots de A^* de la façon suivante

$$\begin{array}{rccl} \lambda : & A^* & \to & \mathbb{N} \\ & x & \to & \lambda(x) = \sum_{a \in A} \lambda(a)|x|_a \end{array}$$

où $|x|_a$ désigne le nombre d'occurrences de la lettre a dans le mot x. L'entier $\lambda(x)$ est alors appelé la *longueur* du mot x de (A^*, λ) .

Un alphabet ordinaire A peut être vu comme un alphabet pondéré pour lequel la fonction λ vaut identiquement 1 sur A.

Les définitions et résultats établis sur un alphabet ordinaire pour lesquels la notion de longueur n'intervient pas restent inchangés sur un alphabet pondéré.

Code circulaire

Un sous-ensemble X du semigroupe A^+ est un *code circulaire* si, pour tous entiers $n, m \geq 1$ et $x_1, x_2, \ldots, x_n \in X$, $y_1, y_2, \ldots, y_m \in X$ et $p \in A^\star$ et $s \in A^+$, les égalités

$$sx_2x_3 \cdots x_np = y_1y_2 \cdots y_m \quad \text{et} \quad x_1 = ps$$

impliquent

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

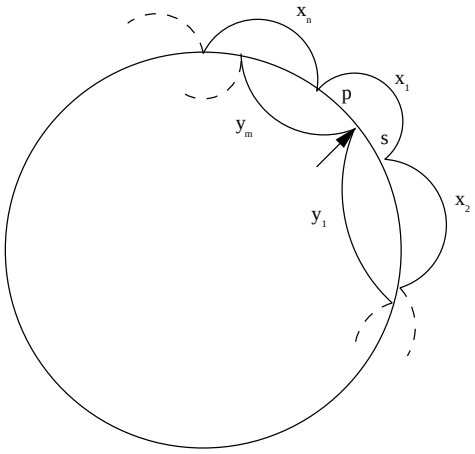


FIG. 2.2 – *Deux factorisations circulaires*

En d'autres termes, tout mot de X^+ écrit sur un cercle (Figure 2.2) admet une unique décomposition.

Un code circulaire est un code et toute partie d'un code circulaire est encore un code circulaire.

Conjugaison

Dans ce qui suit, on introduit la notion de conjugaison dans un monoïde dont on présente également certaines propriétés. Cette relation d'équivalence permet de caractériser les codes circulaires.

Deux mots x et y de A^* sont *conjugués* s'il existe des mots u et v tels que $x = uv$ et $y = vu$. Plus précisément, deux mots x et y sont alors conjugués s'il existe une permutation circulaire $\gamma : A^* \to A^*$ définie par

$$\gamma(1) = 1 \quad \text{et} \quad \gamma(av) = (va) \qquad (\text{où} \quad a \in A \quad \text{et} \quad v \in A^*)$$

et un entier positif n tels que $x = \gamma^n(y)$. Les classes de cette relation d'équivalence sont appelée les *classes de conjugaison.*

Un mot $x \in A^*$ est *primitif* s'il n'est puissance d'aucun autre mot : x est primitif si, et seulement si,

$$(x = y^n \quad \text{et} \quad n \geq 0) \quad \Rightarrow \quad x = y.$$

Le mot vide n'est pas primitif.

Remarque 14 Un code circulaire X ne peut contenir deux mots conjugués distincts. De plus, tout mot de X est primitif.

Soit X un code. Deux mots w et w' de X^* sont dits *X-conjugués* s'il existe $x, y \in X^*$ tels que $w = xy$ et $w' = yx$. On appelle *classes de X-conjugaison* les classes de cette relation d'équivalence. Un mot $x \in X^*$ est dit *X-primitif* si

$$(x = y^n \quad \text{et} \quad y \in X^*) \quad \Rightarrow \quad n = 1.$$

Remarque 15 La relation de conjugaison peut être vue comme celle de la A-conjugaison et la notion de primitivité comme celle de A-primitivité.

Deux mots de X^* qui sont X-conjugués sont conjugués. De même, un mot de X^* qui est primitif est également X-primitif.

Quand X est un code circulaire, deux mots de X^* sont X-conjugués si, et seulement si, ils sont conjugués. De même, un mot de X^* est primitif si, et seulement si, il est également X-primitif.

On peut maintenant donner une caractérisations des codes circulaires basée sur la notion de conjugaison (cf. [BP85] Proposition 1.1 p.323).

Proposition 21 *Soit $X \subset A^+$ un code, X est un code circulaire si, et seulement si, X^* est* très pur*, i.e.,*

$$\forall u, v \in A^*, \quad uv, vu \in M \qquad \Rightarrow \qquad u, v \in M.$$

Exemple 40 Soient $A = \{a, b\}$ et $X = a^*b$, alors $X^* = A^*b \cup \{1\}$. Par suite, si uv et vu sont dans X^*, chacun des mots u et v est le mot vide ou se termine par un b, il appartient donc à X^*. On en déduit que X^* est très pur, et que X est un code circulaire.

Soient $A = \{a_i \mid i \geq 0\}$ et $X = \{a_i a_{i+1} \mid i \geq 0\}$. On peut vérifier sans difficulté que X est encore un code circulaire.

Soient $A = \{a, b, c, d\}$ et $X = \{ab, cd, bc, da\}$, les mots $abcd$ et $bcda$ sont dans X^*, alors que ni a, ni bcd ne sont des mots du code ; par suite, X n'est pas circulaire.

2.2 Monoïde libre très pur

Soient (A, λ) un alphabet pondéré et X une partie de A^+. Pour tout entier strictement positif n, on note A_n l'ensemble des mots de longueur n de A^*, soit

$$A_n = \{x \in A^* \mid \lambda(x) = n\}$$

et α_n le nombre de mots de longueur n de X^*, soit

$$\alpha_n = \text{Card}\{x \in X \mid \lambda(x) = n\} = \text{Card}\,(X \cap A_n)\,.$$

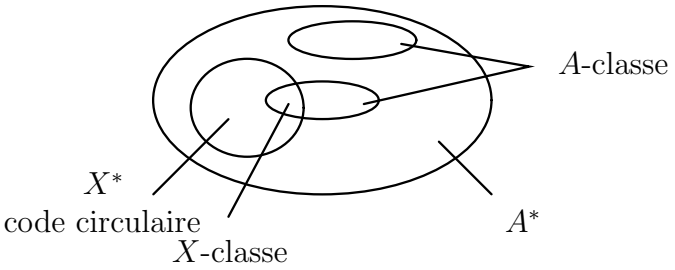


FIG. 2.3 – *Classes de conjugaison*

Si A est un alphabet ordinaire, l'entier $\alpha_n = (X \cap A^n)$ est alors le nombre de mots de n lettres.

De manière générale, la suite $\alpha = (\alpha_n)_{n\geq 1}$ est appelée la *distribution de longueurs* de X.

Etant donné un code X sur un alphabet pondéré (A, λ), on désigne par $L_n(X)$ le nombre de classes de X-conjugaison de mots X-primitifs dans $X^* \cap A_n$.

Proposition 22 *Soit A un alphabet pondéré et soit $X \subset A^+$ un code circulaire sur A. Alors, pour tout entier $n \geq 1$,*

$$L_n(X) \quad \leq \quad L_n(A). \tag{2.1}$$

et l'égalité est atteinte si, et seulement si, toute classe de conjugaison de mots primitifs de A_n a une intersection non vide avec X^*.

Démonstration : Ce résultat est une extension d'un résultat connu dans le cas des codes circulaires sur un alphabet ordinaire (cf. [BP85] Proposition 3.2 p.338).

Soient $\mathcal{X}$ l'ensemble des classes de conjugaison de mots X-primitifs de $X^* \cap A_n$ et $\mathcal{A}$ l'ensemble des classes de conjugaison (ou de A-conjugaison) de mots primitifs de A_n. Par définition,

$$L_n(X) = \mathrm{Card}(\mathcal{X}) \quad \text{et} \quad L_n(A) = \mathrm{Card}(\mathcal{A}).$$

Soit C une classe de $\mathcal{X}$. Comme les mots de C sont X-conjugués, ils sont conjugués ; comme le code X est circulaire et que les mots de C sont X-primitifs, ils sont également primitifs. Ainsi toute classe de $\mathcal{X}$ est une partie d'une classe de $\mathcal{A}$ (Figure 2.3). On définit alors la fonction suivante

$$\begin{array}{rccc} \psi : & \mathcal{X} & \longrightarrow & \mathcal{A} \\ & C & \longrightarrow & C' \supset C. \end{array}$$

Cette fonction est injective puisque, le code X étant circulaire, deux mots de X^* qui sont X-conjugués sont également conjugués, ce qui prouve l'inégalité (2.1). De plus, la fonction ψ est surjective si, et seulement si, toute classe de $\mathcal{A}$ contient une classe de $\mathcal{X}$, ce qui établit le résultat annoncé. □

D'après un résultat dû à Golomb et Gordon ([GG65]), le nombre de classes de conjugaison de mots primitifs de longueur n d'un code circulaire X sur un alphabet à k lettres ne dépend que de la distribution de longueurs du code. Cette propriété est encore vraie quand X est un code circulaire sur un alphabet pondéré quelconque.

Pour établir ce résultat, on calcule $L_n(X)$ à partir de la distribution de longueurs α de X.

On note $\alpha_n^{(i)}$ le nombre de mots de X^i de longueur n. Comme X est un code, $\underline{X^i} = (\underline{X})^i$ et $\alpha_n^{(i)}$ est le coefficient d'ordre n de la série $(\sum_{j\geq 1} \alpha_j z^j)^i$. On pose également

$$\forall n \geq 1, \qquad s_n(\alpha) = \sum_{i=1}^{n} \frac{n}{i} \alpha_n^{(i)},$$

et

$$\forall n \geq 1, \qquad l_n(\alpha) = \frac{1}{n} \sum_{d/n} \mu(\frac{n}{d}) s_d(\alpha),$$

où μ désigne la fonction de Möbius

$$\mu : \mathbb{N}^\star \to \mathbb{N}$$

définie par :

$$\mu(1) = 1$$

$$\mu(n) = \begin{cases} (-1)^i & \text{si } n \text{ est le produit de } i \text{ nombres premiers distincts,} \\ 0 & \text{dans le cas contraire.} \end{cases}$$

Proposition 23 *Soit $X \subset A^+$ un code et soit α sa distribution de longueurs. Le nombre $L_n(X)$ de classes de X-conjugaison de mots X-primitifs dans $X^* \cap A_n$ est donné par*

$$\forall n \geq 1, \qquad L_n(X) = l_n(\alpha).$$

Démonstration : On pose

$$\forall n \geq 1, \quad S_n(X) = \sum_{d/n} d L_d(X).$$

On va établir l'égalité $S_n(X) = s_n(\alpha)$.

On aura alors $s_n(\alpha) = \sum_{d/n} d L_d(X)$, dont on déduira, en utilisant la formule d'inversion de Möbius,

$$L_n(X) = \frac{1}{n} \sum_{d/n} \mu(\frac{n}{d}) s_d(\alpha).$$

Le membre de droite de cette égalité étant, par définition, égal à $l_n(\alpha)$, on aura montré l'égalité $L_n(X) = l_n(\alpha)$. Par suite, le nombre de classes de mots X-primitifs de X ne dépend que de la distribution de longueurs du code.

Par définition de $\alpha_n^{(i)}$ et de $s_n(\alpha)$, on a

$$s_n(\alpha) = \sum_{i=1}^{n} \frac{n}{i} \text{ Card}(X^i \cap A_n).$$

On prouve, dans ce qui suit, que

$$S_n(X) = \sum_{i=1}^{n} \frac{n}{i} \text{ Card}(X^i \cap A_n).$$

Pour tout mot de X^*, on note $||x||$ le nombre de termes de la X-factorisation de x et $\hat{X}$ l'ensemble des mots X-primitifs de X^*. On a alors

$$\sum_{i=1}^{n} \frac{n}{i} \text{ Card}(X^i \cap A_n) = \sum_{w \in X^* \cap A_n} \frac{\lambda(w)}{||w||}.$$

Comme tout mot w de $X^* \cap A_n$ est la puissance d'un unique mot x de $\hat{X}$ et réciproquement, on obtient

$$\sum_{i=1}^{n} \frac{n}{i} \text{ Card}(X^i \cap A_n) = \sum_{d/n} \sum_{x \in \hat{X} \cap A_d} \frac{\lambda(x^{n/d})}{||x^{n/d}||} = \sum_{d/n} \sum_{x \in \hat{X} \cap A_d} \frac{d}{||x||}.$$

De plus, le nombre de classes de conjugaison de mots X-primitifs de $X^* \cap A_d$ est donné par

$$L_d(X) = \sum_{x \in \hat{X} \cap A_d} \frac{1}{||x||},$$

puisque la classe de X-conjugaison d'un mot x de $\hat{X}$ contient exactement $||x||$ éléments. Par conséquent,

$$\sum_{i=1}^{n} \frac{n}{i} \text{ Card}(X^i \cap A_n) = \sum_{d/n} dL_d(X) = S_n(X).$$

On en conclut que $S_n(X) = s_n(\alpha)$, ce qui achève la preuve de la Proposition 23. □

La preuve de la Proposition 23 permet également d'établir le résultat suivant.

Proposition 24 *Soit X un code circulaire, de distribution de longueurs $\alpha = (\alpha_n)_{n \geq 1}$, défini sur un alphabet pondéré (A, λ). Le nombre de mots de A_n dont un conjugué a une X-factorisation est égal à $s_n(\alpha)$.*

Démonstration : On donne une autre preuve de cette proposition en raisonnant sur un code fini, les mots de longueurs strictement supérieures à n ne jouant aucun rôle.

On considère un automate non-ambigu $\mathcal{A} = (Q, 1, 1)$, étiqueté sur l'alphabet pondéré A, reconnaissant X^*. Soit T la matrice à coefficients polynomiaux (sur ce sujet, on pourra se reporter à la Section 2.1.2 p.26) définie par

$$T_{pq} \in z\mathbb{N}[z] \qquad \text{et} \qquad T_{pq} = \sum_{p \xrightarrow{a} q} z^{\lambda(a)}.$$

Comme X est un code circulaire fini, d'après un résultat connu (cf., par exemple, [Béa93] Propositions 4.5 et 4.6 p.128), la série génératrice de X^*, $f_{X^*} = 1/(1 - f_X)$ s'écrit sous la forme suivante

$$\frac{1}{1 - f_X(z)} \;=\; \frac{1}{\det(I - T)}. \tag{2.2}$$

Les membres de l'égalité (2.2) s'écrivent, d'une part,

$$\begin{aligned}
\log\left(\frac{1}{1 - f_X(z)}\right) &= -\sum_{n\geq 1} \frac{f_X(z)^n}{n} \\
&= -\sum_{n\geq 1}\sum_{i\geq 1} \frac{\alpha_i^{(n)}}{n} z^i \quad \text{si } f_X(z) = \textstyle\sum_{n\geq 1} \alpha_n z^n \\
&= -\sum_{i\geq 1} \frac{s_i(\alpha)}{i} z^i \quad \text{par définition de } s_i(\alpha)\,;
\end{aligned}$$

et, d'autre part,

$$\begin{aligned}
\log\left(\frac{1}{\det(I - T)}\right) &= -\mathrm{Tr}(\log(I - T)) \\
&= -\mathrm{Tr}(\sum_{i\geq 1} \frac{T^i}{i}).
\end{aligned}$$

De plus, pour tout entier positif n, on a

$$\mathrm{Tr}(\sum_{i=1}^{n} T^i) = \sum_{i=1}^{n} t_i z^i + R(z)$$

où R est soit le polynôme nul, soit un polynôme formé de monômes de degré supérieur à $n + 1$.

Comme le code X est fini, tous les cycles de l'automate $\mathcal{A}$ passent par l'état 1, et comme X est circulaire, toutes les étiquettes des cycles de l'automate sont distinctes. Par suite, t_n est le nombre de mots de longueur n dont un conjugué admet une X-factorisation. Ainsi

$$\mathrm{Tr}(\sum_{i\geq 1} \frac{T^i}{i}) = \sum_{i\geq 1} \frac{t_i z^i}{i}.$$

En utilisant l'égalité (2.2), on en déduit que $t_i = s_i(\alpha)$, ce qui conclut la preuve. □

Distribution de longueurs d'un monoïde libre très pur

Dans ce qui suit, on décrit, en fonction de différents paramètres, la série génératrice d'un monoïde libre très pur : monoïde engendré par un code circulaire.

Théorème 21 *Soit X un code circulaire sur un alphabet pondéré et soit*

$$f_X(z) = \sum_{n\geq 1} \alpha_n z^n$$

sa série génératrice. Dans ces conditions, la série génératrice $f_{X^*}(z) = 1 + \sum_{n\geq 1} f_n(\alpha) z^n$ du monoïde très pur X^* engendré par X peut être décrite par les différents membres de l'égalité suivante

$$f_{X^*}(z) = \frac{1}{1 - f_X(z)} = \exp\left(\sum_{n\geq 1} \frac{s_n(\alpha)}{n} z^n\right) = \frac{1}{\prod_{n\geq 1}(1 - z^n)^{l_n(\alpha)}} = \frac{1}{\prod_{n\geq 1}(1 - a_n(\alpha) z^n)}$$

où - $s_n(\alpha)$ est le nombre de mots de longueur n dont un conjugué appartient à X^*,
- $l_n(\alpha)$ est le nombre de classes de conjugaison de mots X-primitifs de $X^* \cap A_n$ et
- $(a_n(\alpha))_{n\geq 1}$ est la distribution de longueurs d'un alphabet pondéré A' engendrant un monoïde commutatif (i.e., dont tous les éléments commutent) ayant pour série génératrice $f_{X^*}(z)$.

Démonstration : L'expression $f_{X^*}(z) = 1/(1 - f_X(z))$ découle simplement du fait que X est un code (cf. (1.1) p.95). On montre ensuite, au cours du Lemme 7, que

$$\frac{1}{1 - f_X(z)} = \exp\left(\sum_{n\geq 1} \frac{s_n(\alpha)}{n} z^n\right),$$

l'interprétation de $s_n(\alpha)$ est directement tirée de la Proposition 24 (p.110). Enfin, les égalités

$$\frac{1}{1 - f_X(z)} = \frac{1}{\prod_{n\geq 1}(1 - z^n)^{l_n(\alpha)}} \qquad \text{et} \qquad \frac{1}{1 - f_X(z)} = \frac{1}{\prod_{n\geq 1}(1 - a_n(\alpha) z^n)}$$

sont établies dans le Lemme 8 et le Lemme 9 respectivement. □

Lemme 7 *Soit X un code circulaire sur un alphabet pondéré A. Si $\alpha = (\alpha_n)_{n\geq 1}$ est la distribution de longueurs du code X, on a alors*

$$\frac{1}{1 - f_X(z)} = \exp\left(\sum_{n\geq 1} \frac{s_n(\alpha)}{n} z^n\right). \tag{2.3}$$

Démonstration : De la définition de $s_n(\alpha) : \forall n \geq 1,\ s_n(\alpha) = \sum_{i=1}^{n} \frac{n}{i}\alpha_n^{(i)}$, on déduit que

$$\sum_{n\geq 1} \frac{s_n}{n} z^n \quad = \quad \sum_{i\geq 1} \frac{1}{i} f_{X^i}(z), \tag{2.4}$$

où la distribution de longueurs de X^i, $f_{X^i}(z)$, vérifie $f_{X^i}(z) = (f_X)^i(z)$, puisque X est un code. Comme

$$\sum_{i\geq 1} \frac{1}{i} f_{X^i}(z) = \log\left(\frac{1}{1 - f_X(z)}\right),$$

on obtient (2.3), en prenant l'exponentielle de chacun des membres de l'égalité (2.4). □

D'après la formule de Moreau (cf. [Luc91] p.501-503), encore appelée formule de Witt (cf. [Lot83] p.79 et p.84), si A est un alphabet (au sens usuel) à k lettres, alors

$$\frac{1}{1 - kz} = \frac{1}{\prod_{n\geq 1}(1 - z^n)^{l_n(k)}},$$

où $l_n(k)$ est le nombre de classes de conjugaison de mots primitifs de longueur n dans A^*. Ce résultat peut être généralisé à un alphabet pondéré quelconque A de la manière suivante.

Lemme 8 *Soit X un code circulaire sur un alphabet pondéré A. Si $\alpha = (\alpha_n)_{n\geq 1}$ est la distribution de longueurs du code X, on a alors*

$$\frac{1}{1 - f_X(z)} = \frac{1}{\prod_{n\geq 1}(1 - z^n)^{l_n(\alpha)}}.$$

Démonstration : Des définitions de $s_n(\alpha)$ et de $l_n(\alpha)$

$$\forall n \geq 1 \qquad s_n(\alpha) = \sum_{i=1}^{n} \frac{n}{i}\alpha_n^{(i)} \quad \text{et} \quad s_n(\alpha) = \sum_{d/n} d l_d(\alpha),$$

on tire

$$\sum_{i\geq 1} \frac{1}{i} f_{X^i}(z) = \sum_{n\geq 1} \sum_{d/n} d l_d(\alpha) \frac{z^n}{n}, \tag{2.5}$$

Le dernier membre de l'égalité peut être réécrit de la façon suivante

$$\sum_{n\geq 1} \sum_{d/n} d l_d(\alpha) \frac{z^n}{n} = \sum_{d\geq 1} l_d(\alpha) \sum_{q\geq 1} \frac{z^{qd}}{q} = \sum_{d\geq 1} l_d(\alpha) \log\left(\frac{1}{1 - z^d}\right).$$

On obtient alors le résultat annoncé en prenant l'exponentielle de chacun des termes de l'égalité (2.5). □

Lemme 9 *Soient X un code sur un alphabet pondéré A et $f_X(z) = \sum_{n\geq 1} \alpha_n z^n$ sa série génératrice. On a alors*

$$f_{X^*}(z) = \frac{1}{1 - f_X(z)} = \frac{1}{\prod_{n\geq 1}(1 - a_n(\alpha)z^n)},$$

où $(a_n(\alpha))_{n\geq 1}$ est la distribution de longueurs d'un alphabet pondéré A' engendrant un monoïde commutatif dont la série génératrice est $f_{X^*}(z)$.

Démonstration : On pose

$$f_{X^*}(z) = 1 + \sum_{n\geq 1} f_n(\alpha) z^n.$$

Les coefficients $(a_n(\alpha))_{n\geq 1}$ tels que

$$f_{X^*}(z) = \frac{1}{\prod_{n\geq 1}(1 - a_n(\alpha)z^n)},$$

vérifient alors les équations

$$\begin{aligned}
&f_1(\alpha) = a_1(\alpha)\\
&f_2(\alpha) = a_2(\alpha) + a_1^2(\alpha)\\
&f_3(\alpha) = a_3(\alpha) + a_2(\alpha)a_1(\alpha) + a_1^3(\alpha)\\
&\vdots\\
&f_n(\alpha) = \textstyle\sum_{\mathcal{P}(n)} \prod_{i_1\leq\ldots\leq i_k} a_{i_1}(\alpha)\ldots a_{i_k}(\alpha)
\end{aligned}$$

où la somme est effectuée sur l'ensemble $\mathcal{P}(n)$ des partitions de l'entier n.

Ce système peut être réécrit de la manière suivante

$$\begin{aligned}
&a_1(\alpha) = f_1(\alpha)\\
&a_2(\alpha) = f_2(\alpha) - a_1^2(\alpha)\\
&a_3(\alpha) = f_3(\alpha) - a_2(\alpha)a_1(\alpha) - a_1^3(\alpha)\\
&\vdots\\
&a_n(\alpha) = \textstyle\sum_{\mathcal{P}'(n)} \prod_{i_1\leq\ldots\leq i_k} a_{i_1}(\alpha)\ldots a_{i_k}(\alpha)
\end{aligned}$$

où la somme est effectuée sur l'ensemble

$$\mathcal{P}'(n) = \mathcal{P}(n) \setminus \{(n)\}$$

des partitions de l'entier n ayant au moins deux éléments.

Les $(a_n(\alpha))_{n\geq 1}$ s'expriment alors en fonction des $(\alpha_n)_{n\geq 1}$:

$$\forall n \in \mathbb{N}^*, \qquad a_n(\alpha) = \alpha_n + \sum_{\mathcal{P}''(n)} \prod_{i_1\leq\ldots\leq i_k} \alpha_{i_1}\ldots\alpha_{i_k},$$

où la somme est effectuée sur l'ensemble $\mathcal{P}''(n)$ des partitions de l'entier n faisant intervenir au moins deux entiers distincts. Ainsi

$$a_1(\alpha) = \alpha_1, \qquad a_2(\alpha) = \alpha_2, \qquad a_3(\alpha) = \alpha_3 + \alpha_2\alpha_1$$
$$a_4(\alpha) = \alpha_4 + \alpha_3\alpha_1 + \alpha_2\alpha_1^2.$$
$$a_5(\alpha) = \alpha_5 + \alpha_4\alpha_1 + \alpha_3\alpha_2 + \alpha_3\alpha_1^2 + \alpha_2^2\alpha_1 + \alpha_2\alpha_1^3.$$

L'entier $a_1(\alpha)$ est le nombre de lettres de longueur 1 d'un alphabet pondéré engendrant un monoïde commutatif ayant $f_1(\alpha)$ mots de longueur 1. L'entier $a_2(\alpha)$ est le nombre de mots de longueur 2 qui ne peuvent être écrits avec les $a_1(\alpha)$ lettres de longueur 1. L'expression de de $a_3(\alpha)$ en fonction des α_n met en évidence le fait que les lettres commutent (cf. le facteur $\alpha_2\alpha_1$).

Plus généralement, on peut montrer, par induction sur n, que la suite $(a_i(\alpha))_{1\leq i\leq n}$ est la distribution de longueurs d'un alphabet pondéré engendrant un monoïde commutatif dont la distribution de longueurs coïncide jusqu'au rang n (inclus) avec celle du monoïde libre X^*. □

2.3 Extension d'un théorème de Schützenberger

Les distributions de longueurs $(\alpha_n)_{n\geq 1}$ des codes sur un alphabet à k lettres sont caractérisées par l'inégalité de Kraft-McMillan : $\sum_{n\geq 1} \alpha_n k^{-n} \leq 1$ (cf. Théorème 18 p.95). Schützenberger ([Sch65b]) a identifié par des conditions plus fortes celles de ces suites qui sont distributions de longueurs d'un code circulaire.

Dans ce qui suit, on étend cette caractérisation. Cette généralisation porte sur deux points. D'une part, on remplace l'alphabet fini par un alphabet pondéré quelconque, ce qui permet également d'étendre le résultat au cas de deux distributions de longueurs (Corollaire 5) ; d'autre part, on réduit l'ensemble des valeurs pour lesquelles les inégalités considérées doivent être vérifiées, ce qui permet d'établir la décidabilité dans le cas d'une distribution de longueurs finie (Corollaire 4).

On rappelle l'énoncé du résultat de Schützenberger ([Sch65b]).

Théorème 22 (Schützenberger) *Une suite d'entiers positifs $(\alpha_n)_{n\geq 1}$ est la distribution de longueurs d'un code circulaire sur un alphabet à k lettres si, et seulement si, elle vérifie*

$$\forall n \geq 1 \qquad l_n(\alpha) \leq l_n(k)$$

où $l_n(k)$ est le nombre de classes de conjuguaison des mots primitifs de longueur n sur un alphabet à k lettres.

L'idée est de substituer, dans l'énoncé du théorème de Schützenberger, à l'alphabet à k lettres un alphabet pondéré. L'analogie provient du fait que les propriétés de la relation de conjugaison sont conservées ; on étend ainsi sans difficulté la preuve initiale.

De plus, on réduit l'ensemble des valeurs pour lesquelles les inégalités sur les classes de mots primitifs doivent être vérifiées.

Théorème 23 *Soit (A, λ) un alphabet pondéré et soit $\alpha = (\alpha_n)_{n\geq 1}$ sa distribution de longueurs. Une suite d'entiers positifs $\beta = (\beta_n)_{n\geq 1}$ est alors la distribution de longueurs d'un code circulaire $Y \subset A^+$ si, et seulement si,*

$$\forall n \geq 1 \quad \textit{tel que} \quad \beta_n \neq 0 \qquad l_n(\beta) \leq l_n(\alpha)$$

On peut tout de suite noter le corollaire suivant qui montre que, lorsque la distribution de longueurs β est une suite finie, on peut décider si les inégalités ci-dessus sont satisfaites.

Corollaire 4 *Une suite finie $\beta = (\beta_i)_{1\leq i\leq m}$ d'entiers positifs est la distribution de longueurs d'un code circulaire sur l'alphabet (A, λ) de distribution de longueurs $\alpha = (\alpha_n)_{n\geq 1}$ si, et seulement si,*

$$\forall n \leq m \quad \textit{tel que} \quad \beta_n \neq 0 \qquad l_n(\beta) \leq l_n(\alpha).$$

On peut donc décider si une suite finie est la distribution de longueurs d'un code circulaire construit sur un alphabet pondéré donné.

Remarque 16 Le fait de ne vérifier les inégalités sur les classes de mots primitifs que jusqu'au rang m dans le cas d'une suite $\beta = (\beta)_{1\leq i\leq m}$ n'a rien d'évident *a priori*. En effet, le plus petit mot circulaire ayant plus d'une factorisation sur un code qui n'est pas circulaire peut être plus long que les mots du code. Par exemple, si $Y = \{ab, cd, bc, da\}$, le mot circulaire ambigu le plus court, $abcd$, est de longueur 4.

Les inégalités $l_n(\beta) \leq l_n(\alpha)$, pour tout entier strictement positif n, se déduisent du fait que $Y^* \subset A^*$ et que les relations de conjugaison et de Y-conjugaison ainsi que les notions de mot primitif et Y-primitif coïncident sur Y^* car le code est circulaire. Ce résultat est donné dans la Proposition 22 (p.108).

La construction d'un code circulaire à partir de la série β est basée sur l'utilisation des suites de Hall. On étend aux alphabets pondérés cette notion et des résultats, qui lui sont liés, connus dans le cas des alphabets ordinaires.

Soit (A, λ) un alphabet pondéré. On dit qu'une suite finie ou infinie est une *suite de Hall* sur A si elle peut être obtenue inductivement de la façon suivante :

- Soit $X_1 = A$. On définit x_1 comme un mot arbitraire pris parmi les mots les plus courts (λ minimal) de A.
- Si x_i et X_i sont définis, on pose $X_{i+1} = x_i^*(X_i \setminus x_i)$ et x_{i+1} est un élément arbitraire de X_{i+1} vérifiant $\lambda(x_{i+1}) \geq \lambda(x_i)$.

La suite $(X_i)_{i\geq 1}$ est la *suite de codes associés* à $(x_i)_{i\geq 1}$.

Chacun des codes X_i est circulaire. En effet, $X_1 = A$ est circulaire. De plus, pour tout entier i, $X_{i+1} = H \circ X_i$ où H est un code circulaire de la forme $x^*(X \setminus x)$. Comme, d'après la Proposition 20 (p.102), le composé de codes circulaires est circulaire, on en déduit par induction que, pour tout i, X_i est circulaire.

Lemme 10 *Soit $(x_i)_{i\geq 1}$ une suite de Hall sur un alphabet pondéré A et soit $(X_i)_{i\geq 1}$ la suite de codes associés. Pour tout $n > \lambda(x_i)$,*

$$l_n(X_{i+1}) = l_n(A).$$

Démonstration : On va montrer que le nombre de classes de conjugaison de mots primitifs de longueur n ($n > \lambda(x_i)$) dans A^* et celui des classes de mots primitifs de X_{i+1} de même longueur sont égaux. Soient $l_n(A)$ et $l_n(X_{i+1})$ respectivement ces deux nombres.

Comme $X_{i+1} \subset A^*$ et que X_{i+1} est un code circulaire,

$$\forall n \geq 1, \qquad l_n(X_{i+1}) \leq l_n(A).$$

De plus, pour tout $i \geq 1$, tout mot primitif w de A^+ de longueur supérieure à celle de x_i a un conjugué dans X_{i+1}^*.

En effet, en posant $x_0 = 1$ (le mot vide), l'assertion précédente pour $i = 0$ signifie que tout mot primitif de A^+ appartient à A^*.

Soit $i \geq 1$ et soit $w \in A^+$ un mot primitif de longueur supérieure à celle de x_i. Comme $\lambda(x_i) \geq \lambda(x_{i-1})$, $\lambda(w) > \lambda(x_{i-1})$. D'après l'hypothèse d'induction, il existe un conjugué w' de w dans X_i^*. Le mot w' n'appartient pas à x_i^* puisque w' est primitif et que sa longueur est strictement supérieure à celle de x_i. Il se factorise donc sous la forme

$$w' = uxv \qquad \text{où} \quad u, v \in X_i^* \quad \text{et} \quad x \in (X_i \setminus x_i).$$

Son conjugué $w'' = vux$ appartient alors à $X_i^*(X_i \setminus x_i) \subset X_{i+1}^*$. Le mot w a donc un conjugué dans X_{i+1}^*, ce qui prouve l'égalité

$$\forall n > \lambda(x_i), \qquad l_n(X_{i+1}) = l_n(A).$$

et achève la preuve du lemme. □

Démonstration : (du Théorème 23)

Dans ce qui suit, on construit une suite de Hall sur un alphabet pondéré (A, λ) telle qu'il existe une suite extraite de la suite de codes associés ayant comme propriété que le $i$ème code a, jusqu'au $i$ème rang compris, la distribution de longueurs β (le $i$ème code a β_j mots de longueur j pour tout entier j inférieur ou égal à i).

Dans ces conditions, Y apparaît comme la limite de cette nouvelle suite ou peut être défini par ses mots de longueur i qui coïncident avec les mots de longueur i du $i$ème code de la suite.

Pour ce faire, on pose

$$\forall n, m \geq 1, \quad \epsilon_n = l_n(\alpha) - l_n(\beta)$$

$$\text{et} \qquad \sigma_m = \sum_{n=1}^{m} \epsilon_n.$$

On définit par induction, en partant de la suite (de Hall) vide, une suite de Hall $(x_i)_{i\geq 1}$ sur l'alphabet pondéré (A, λ).

On suppose qu'une suite de Hall sur A: $(x_1, x_2, \ldots, x_{\sigma_{m+1}})$ de mots de longueur au plus m est déjà construite de sorte que la distribution de longueurs γ de $Y_m = X_{\sigma_m+1}$ satisfasse

$$\gamma_n = \beta_n \qquad 1 \leq n \leq m.$$

On a alors

$$\gamma_{m+1} - \beta_{m+1} = l_{m+1}(\gamma) - l_{m+1}(\beta).$$

En effet,

$$l_{m+1}(\gamma) = \frac{1}{m+1} \sum_{d/(m+1)} \mu(\frac{m+1}{d}) \sum_{i=1}^{d} \frac{d}{i} \gamma_d^{(i)} \qquad \text{où} \quad \gamma_d^{(i)} = \text{Card}\{y \in Y_m^i \mid \lambda(y) = d\}.$$

Comme

$$\gamma_d^{(i)} = \sum_{m_1+m_2+\cdots+m_i=d} \gamma_{m_1}\gamma_{m_2}\ldots\gamma_{m_i},$$

les indices m_j sont inférieurs à m sauf si $d = m+1$ et $i = 1$. On a donc l'égalité de tous les monômes $\gamma_{m_1}\gamma_{m_2}\ldots\gamma_{m_i} = \beta_{m_1}\beta_{m_2}\ldots\beta_{m_i}$ sauf pour $d = m+1$ et $i = 1$. Par conséquent,

$$l_{m+1}(\gamma) - l_{m+1}(\beta) = \gamma_{m+1} - \beta_{m+1}.$$

D'après le Lemme 10 (p.117), on a aussi l'égalité $l_{m+1}(\gamma) = l_{m+1}(A)$ car x_{σ_m} est un mot de longueur au plus m ($l_{m+1}(\gamma) = l_{m+1}(Y_m) = l_{m+1}(A) = l_{m+1}(\alpha)$). On obtient finalement,

$$\gamma_{m+1} - \beta_{m+1} = l_{m+1}(\alpha) - l_{m+1}(\beta) = \epsilon_{m+1}.$$

Le code Y_m contient, par suite, au moins ϵ_{m+1} mots de longueur $m+1$.

On prolonge la suite de Hall déjà construite en choisissant, dans Y_m, ϵ_{m+1} mots de longueur $m+1$ notés

$$x_{\sigma_m+1}, x_{\sigma_m+2}, \ldots, x_{\sigma_{m+1}}.$$

La distribution de longueurs δ du code associé $Y_{m+1} = X_{1+\sigma_{m+1}}$ vérifie alors

$$\delta_n = \beta_n \qquad \text{pour} \quad 1 \leq n \leq m+1.$$

En effet, comme la suite des longueurs des mots de la suite $(x_i)_{1\leq i\leq \sigma_{m+1}}$ est croissante, les codes X_i et X_{i+1} coïncident sur tous les mots d'une longueur inférieure à celle de x_i.

Les codes $X_{1+\sigma_m}, \ldots, X_{1+\sigma_{m+1}}$ possèdent donc les mêmes mots de longueur au plus m (ou coïncident sur l'ensemble des mots de longueur inférieure à n), d'où $\delta_n = \gamma_n = \beta_n$ pour $1 \leq n \leq m$.

De plus, $\delta_{m+1} = \beta_{m+1}$ puisque dans le processus de construction du code Y_{m+1}, on a supprimé ϵ_{m+1} mots de longueur $m+1$ au code Y_m, d'où

$$\delta_{m+1} = \gamma_{m+1} - \epsilon_{m+1} = \beta_{m+1}.$$

On a donc construit une suite de codes circulaires $(Y_i)_{i\geq 1}$ telle que Y_i et Y_{i+1} coïncident sur l'ensemble des mots de longueur au plus i et telle que Y_i ait β_i mots de longueur i.

On définit alors Y par ses mots de longueur i comme suit

$$\{x \in Y \mid \lambda(x) = i\} = \{y \in Y_i \mid \lambda(y) = i\}.$$

Ce code sur A (*i.e.*, $Y \subset A^+$) est circulaire et a pour distribution de longueurs β. □

Remarque 17 Si $\beta_{m+1} = 0$ et si $l_n(\alpha) \geq l_n(\beta)$ pour $1 \leq n \leq m$, on a alors nécessairement l'inégalité $l_{m+1}(\alpha) \geq l_{m+1}(\beta)$, ce qui justifie la réduction de l'intervalle pour lequel les inégalités sur les classes de mots primitifs doivent être vérifiées et assure la décidabilité dans le cas où la suite β est finie.

Remarque 18 Cette preuve ne permet pas d'établir la rationalité de Y dans le cas où on suppose que la suite β est $\mathbb{N}$-rationnelle.

Exemple 41 Soient $k = 3$ et $A = \{a, b, c\}$.

Si $\beta_1 = 1$, $\beta_2 = 1$, $\beta_3 = 7$, $\beta_4 = 10$ et $\beta_i = 0$ pour $i \geq 5$, alors $\epsilon_1 = l_1(3) - l_1(\beta) = 2$, en supprimant a puis b, on obtient le code

$$Y_1 = \{c, \mid ab, ac, bc \mid, a^2b, a^2c, bab, bac, b^2c, a^3, a^3c, ba^2b, ba^2c, b^3c, \ldots\}.$$

Comme $\epsilon_2 = 2$, en supprimant ab puis ac, on obtient le code

$$\begin{aligned} Y_2 \;=\; & \{c, bc, \mid a^2b, a^2c, bab, bac, b^2c, abc, acc \mid, a^3b, a^3c, \\ & ba^2b, ba^2c, b^2ab, b^2ac, b^3c, abac, abbc, acbc, \ldots\} \end{aligned}$$

Enfin, comme $\epsilon_3 = 0$ et $\epsilon_4 = 0$, $Y_2 = Y_3 = Y_4$. On obtient le code circulaire Y de distribution de longueurs $(1, 1, 7, 10)$ suivant

$$\begin{aligned} Y = Y_4 \cap A^4 \;=\; & \{c, bc, a^2b, a^2c, bab, bac, b^2c, abc, acc, \mid a^3b, a^3c, \\ & ba^2b, ba^2c, b^2ab, b^2ac, b^3c, abac, abbc, acbc\} \end{aligned}$$

Le résultat suivant se déduit du Théorème 23 par morphisme codant.

Corollaire 5 *Soit X un code circulaire sur l'alphabet (ordinaire) A et soit $\alpha = (\alpha_n)_{n\geq 1}$ sa distribution de longueurs. Une suite d'entiers positifs $\beta = (\beta_n)_{n\geq 1}$ est alors la distribution de longueurs d'un code circulaire $Y \subset X^+$ si, et seulement si,*

$$\forall n \geq 1 \quad \textit{tel que} \quad \beta_n \neq 0 \qquad l_n(\beta) \leq l_n(\alpha)$$

Démonstration : Comme X est un code, il existe un morphisme codant $\phi : B^* \to A^*$ pour X qui induit une bijection d'un alphabet B sur X. On définit sur B la fonction λ de la façon suivante

$$\forall x \in B, \quad \lambda(x) = |\phi(x)|,$$

où $|\phi(x)|$ représente la longueur de $\phi(x)$ au sens usuel, *i.e.*, le nombre d'occurrences de lettres de A dans $\phi(x)$. On obtient ainsi un alphabet pondéré dont la distribution de longueurs coïncide avec celle de X définie sur A.

Par suite, d'après le Théorème 23 (p.116), on peut construire un code circulaire Z sur B^* ayant β pour distribution de longueur. Comme X et Z sont composables par ϕ et que X et Z sont eux-mêmes circulaires, d'après la Proposition 20 (p.102), $Y = Z \circ X = \phi(Z)$ est un code circulaire sur A^* et par suite sur X^* car $Y^* \subset X^*$ et que ces deux codes sont circulaires.

Enfin, par conséquence directe de la définition de λ, Y a β pour distribution de longueurs sur l'alphabet A. □

2.4 Une nouvelle formulation des inégalités

Dans cette partie, on montre que les distributions de longueurs $(\beta_n)_{n\geq 1}$ des codes circulaires sur un alphabet pondéré de distribution de longueurs $(\alpha_n)_{n\geq 1}$ peuvent être caractérisées par des inégalité portant directement sur les β_n. Ce résultat met en évidence le fait que si un code circulaire est fini, les inégalités sur les nombres de classes de mots primitifs sont nécessairement vérifiées à partir du rang strictement supérieur au plus long mot du code.

2.4.1 Résultats

On déduit de la construction précédente (Section 2.3 p.115) une expression à coefficients positifs de $\beta_i + \epsilon_i$ en fonction des $(\alpha_j)_{j\leq i}, (\beta_j)_{j<i}$ et $(\epsilon_j)_{j<i}$, où $\epsilon_i = l_i(\alpha) - l_i(\beta)$.

Proposition 25 *Soit A un alphabet pondéré ayant pour distribution de longueurs $\alpha = (\alpha_i)_{i\geq 1}$ et soit $\beta = (\beta_i)_{i\geq 1}$ la distribution de longueurs d'un code circulaire sur A. Alors, pour tout entier positif n, la somme $\epsilon_n + \beta_n$ est un polynôme à coefficients entiers positif en les variables $(\beta_i)_{i<n}$, $(\epsilon_i)_{i<n}$ (où $\epsilon_i = l_i(\alpha) - l_i(\beta)$) et $(\alpha_i)_{i\leq n}$.*

Le théorème suivant est alors une conséquence directe de la Proposition 25 et du précédent théorème de caractérisation des distributions de longueurs d'un code circulaire (Théorème 23 p.116).

Théorème 24 *Soit (A, λ) un alphabet pondéré ayant pour distribution de longueurs $\alpha = (\alpha_i)_{i\geq 1}$ et soit $\beta = (\beta_i)_{i\geq 1}$ une suite d'entiers positifs. Alors, il existe une suite $(P_n)_{n\geq 1}$ de polynômes à coefficients entiers positif en les variables $(\beta_i)_{i<n}$, $(\epsilon_i)_{i<n}$ (où $\epsilon_i = l_i(\alpha) - l_i(\beta)$) et $(\alpha_i)_{i\leq n}$. telle que les conditions suivantes soient équivalentes*

1. *la suite $\beta = (\beta_i)_{i\geq 1}$ est la distribution de longueurs d'un code circulaire sur A.*
2. $\forall n \geq 1, \qquad \beta_n \leq P_n$.

Démonstration : Si β est la distribution de longueurs d'un code circulaire, alors, d'après la Proposition 25, pour tout entier n strictement positif, il existe des polynômes vérifiant les conditions du Théorème 24 tels que

$$\epsilon_n + \beta_n = P_n.$$

Comme le code est circulaire, d'après le Théorème 23 (p.116), ϵ_n est positif. Par suite,

$$\forall n \geq 1, \qquad \beta_n \leq P_n.$$

Réciproquement, si

$$\forall n \geq 1, \qquad \beta_n \leq P_n,$$

alors $\epsilon_n = P_n - \beta_n$ est positif. En appliquant le Théorème 23 (p.116), on peut construire un code circulaire de distribution de longueurs β. □

On donne maintenant, dans la Section 2.4.2 une méthode directe pour calculer les polynômes P_n à l'aide de laquelle on explicite P_n pour les petites valeurs de n. On prouve ensuite (Section 2.4.3 p.125) de manière combinatoire la Proposition 25 (p.120).

2.4.2 Calcul direct des premiers polynômes

Codes auxiliaires

On rappelle la manière dont on a construit une suite de codes circulaires préfixes $(Y_i)_{i\geq 0}$ à partir d'un alphabet pondéré (A, λ), suite dont la limite est un code circulaire de distribution de longueurs $\beta = (\beta_n)_{n\geq 1}$ dans la preuve du Théorème 23 (p.116).

Construction Pour obtenir le code Y circulaire de distribution de longueurs $(\beta_n)_{n\geq 1}$ du Théorème 23 (p.116), on construit une suite de codes circulaires préfixes $(Y_i)_{i\geq 0}$ à partir de l'alphabet pondéré (A, λ) de sistribution de longueurs $(\alpha_n)_{n\geq 1}$. Le code circulaire que l'on obtient finalement coïncide, pour tout entier i, sur l'ensemble des mots de longueur inférieure ou égale à i, avec Y_i.

La construction des codes $(Y_i)_{i\geq 0}$ est la suivante $Y_0 = A$. Pour tout entier strictement positif i, si $f_i(z) = \sum_{j\geq 1} y_{i,j} z^j$ est la distribution de longueurs du code Y_i, le code Y_{i+1} est obtenu en supprimant successivement

$$\epsilon_i = y_{i-1,i} - \beta_i = l_i(\alpha) - l_i(\beta)$$

mots de longueur i au code $Y_{i-1} : x_{i,1}, x_{i,2}, \ldots, x_{i,\epsilon_i}$ et en construisant les codes auxiliaires

$$X_{i,1} = x^*_{i,1}(Y_{i-1} \setminus x_{i,1}),$$

$$X_{i,2} = x^*_{i,2}(X_{i,1} \setminus x_{i,2}),$$

$$\cdots$$

$$Y_i = X_{i,\epsilon_i} = x^*_{i,\epsilon_i}(X_{i,\epsilon_i - 1} \setminus x_{i,\epsilon_i}).$$

Si $\lambda(x)$ est la longueur du mot x et si f_X est la fonction génératrice du code X, alors la fonction génératrice $f_{X'}$ du code $X' = x^*(X \setminus x)$ s'exprime en fonction de celle de X

$$f_{X'}(z) = \frac{1}{1 - z^{\lambda(x)}}(f_X(z) - z^{\lambda(x)}).$$

Par conséquent, la suite des fonctions génératrices des codes $(Y_i)_{i\geq 0}$ vérifie la relation de récurrence suivante, obtenue par applications successives de la formule précédente,

$$f_0(z) = f_A(z) = \sum_{n\geq 1} \alpha_n z^n,$$

$$\forall i \in \mathbb{N}^*, \quad f_i(z) = \frac{1}{(1 - z^i)^{\epsilon_i}}(f_{i-1}(z) - z^i \sum_{j=0}^{\epsilon_i - 1}(1 - z^i)^j),$$

soit

$$f_i(z) = 1 + \frac{f_{i-1}(z) - 1}{(1 - z^i)^{\epsilon_i}}.$$

Ces fonctions génératrices s'écrivent finalement

$$\forall i \in \mathbb{N}, \quad f_i(z) = 1 + \frac{f_A(z) - 1}{\prod_{j=0}^{i}(1 - z^j)^{\epsilon_j}},$$

avec la convention $\epsilon_0 = 0$.

La distribution de longueurs du code circulaire Y est donc donnée par l'expression

$$f_Y(z) = \sum_{i\geq 1} \beta_i z^i = 1 + \frac{f_A - 1}{\prod_{j\geq 0}(1 - z^j)^{\epsilon_j}} \quad \text{où} \quad \epsilon_j = l_j(\alpha) - l_j(\beta).$$

En posant

$$\sum_{n\geq 0} E_n z^n = \frac{1}{\prod_{j\geq 0}(1 - z^j)^{\epsilon_j}}, \qquad \forall n \in \mathbb{N}, \quad E_n \geq 0.$$

et en supposant que l'alphabet a pour distribution de longueurs $\alpha = (\alpha_n)_{n\geq 1}$, on obtient la relation

$$\forall n > 0, \quad \beta_n = \sum_{p=1}^{n} \alpha_p E_{n-p} - E_n \quad \text{avec} \quad E_0 = 1. \tag{2.6}$$

On a

$$\begin{aligned} \sum_{n\geq 0} E_n z^n &= \prod_{j\geq 0} (1-z^j)^{-\epsilon_j} = \prod_j \sum_{k_j \geq 0} P_{k_j} z^{jk_j} \\ &= \sum_{n\geq 0} \Big(\sum_{\Sigma j_l k_{j_l} = n} \prod_l P_{k_{j_l}} \Big) z^n, \end{aligned}$$

où

$$\forall k_j \in \mathbb{N}, \qquad P_{k_j} = \binom{\epsilon_j + k_j - 1}{k_j}.$$

Le calcul des E_i donne

$$E_1 = \epsilon_1,$$

$$E_2 = \binom{\epsilon_1 + 1}{2} + \epsilon_2,$$

$$E_3 = \binom{\epsilon_1 + 2}{3} + \epsilon_1\epsilon_2 + \epsilon_3,$$

$$E_4 = \binom{\epsilon_1 + 3}{4} + \binom{\epsilon_1 + 1}{2}\epsilon_2 + \epsilon_1\epsilon_3 + \binom{\epsilon_2 + 1}{2} + \epsilon_4$$

$$E_5 = \binom{\epsilon_1 + 4}{5} + \binom{\epsilon_1 + 2}{3}\epsilon_2 + \binom{\epsilon_1 + 1}{2}\epsilon_3 + \epsilon_1\binom{\epsilon_2 + 1}{2} + \epsilon_1\epsilon_4 + \epsilon_2\epsilon_3 + \epsilon_5$$

$$E_6 = \binom{\epsilon_1 + 5}{6} + \binom{\epsilon_1 + 3}{4}\epsilon_2 + \binom{\epsilon_1 + 2}{3}\epsilon_3 + \binom{\epsilon_1 + 1}{2}\binom{\epsilon_2 + 1}{2} + \binom{\epsilon_1 + 1}{2}\epsilon_4$$
$$+\epsilon_1\epsilon_2\epsilon_3 + \epsilon_1\epsilon_5 + \binom{\epsilon_2 + 2}{3} + \epsilon_2\epsilon_4 + \binom{\epsilon_3 + 1}{2} + \epsilon_6.$$

Cas d'un alphabet ordinaire à k lettres

Dans ce cas, la relation (2.6) (p.123) qui donne le nombre de mots de longueur n du code circulaire construit, s'écrit

$$\forall n > 0, \quad \beta_n = kE_{n-1} - E_n \qquad \text{et} \qquad E_0 = 1.$$

On obtient, pour les premièress valeurs de i, les polynômes $P_i (= \beta_i + \epsilon_i)$ suivants

$$P_1 = \beta_1 + \epsilon_1 = kE_0 - E_1 + \epsilon_1 = k.$$

$$P_2 = \epsilon_1 \left(k - \frac{\epsilon_1 + 1}{2} \right) = \beta_1 \epsilon_1 + \binom{\epsilon_1}{2}.$$

$$P_3 = \binom{\epsilon_1 + 1}{2} \left(k - \frac{\epsilon_1 + 2}{3} \right) + \beta_1 \epsilon_2 = \left(\binom{\epsilon_1 + 1}{2} + \epsilon_2 \right) \beta_1 + 2 \binom{\epsilon_1 + 1}{3}.$$

$$P_4 = \left(\binom{\epsilon_1 + 2}{3} + \epsilon_3 \right) \beta_1 + \epsilon_2 \beta_2 + 3 \binom{\epsilon_1 + 2}{4} + \binom{\epsilon_2}{2}.$$

$$P_5 = \left(\binom{\epsilon_1 + 3}{4} + \epsilon_2 \binom{\epsilon_1 + 1}{2} + \binom{\epsilon_2 + 1}{2} + \epsilon_4 \right) \beta_1 + \epsilon_3 \beta_2 + 4 \binom{\epsilon_1 + 3}{5} + 2\epsilon_2 \binom{\epsilon_1 + 1}{3}.$$

et

$$P_6 = \left(\binom{\epsilon_1 + 4}{5} + \epsilon_2 \binom{\epsilon_1 + 2}{3} + \epsilon_5 \right) \beta_1 + \left(\binom{\epsilon_2 + 1}{2} + \epsilon_4 \right) \beta_2 + \epsilon_3 \beta_3 + 5 \binom{\epsilon_1 + 4}{6}$$
$$+ 3\epsilon_2 \binom{\epsilon_1 + 2}{4} + 2 \binom{\epsilon_2 + 1}{3} + \binom{\epsilon_3}{2}.$$

...

Cas d'un alphabet pondéré quelconque

Quand l'alphabet est pondéré, la relation (2.6) (p.123) s'écrit

$$\forall n > 0, \quad \beta_n = \sum_{p=1}^{n} \alpha_p E_{n-p} - E_n \quad \text{avec} \quad E_0 = 1,$$

où $(\alpha_n)_{n \geq 1}$ est la distribution de longueurs de l'alphabet pondéré (A, λ).

Le calcul direct des sommes $\beta_i + \epsilon_i$ donne alors, pour les petites valeurs de i, les polynômes suivants

$$P_1 = \beta_1 + \epsilon_1 = \alpha_1 E_0 - E_1 + \epsilon_1 = \alpha_1,$$

$$P_2 = \epsilon_1 \left(\beta_1 + \frac{(\epsilon_1 - 1)}{2} \right) + \alpha_2 = \epsilon_1 \beta_1 + \binom{\epsilon_1}{2} + \alpha_2,$$

$$P_3 = \left(\binom{\epsilon_1 + 1}{2} + \epsilon_2 \right) \beta_1 + 2 \binom{\epsilon_1 + 1}{3} + \epsilon_1 \alpha_2 + \alpha_3.$$

et

$$P_4 = \left(\binom{\epsilon_1 + 2}{3} + \epsilon_3 \right) \beta_1 + \epsilon_2 \beta_2 + 3 \binom{\epsilon_1 + 2}{4} + \binom{\epsilon_2}{2} + \binom{\epsilon_1 + 1}{2} \alpha_2 + \epsilon_1 \alpha_3 + \alpha_4.$$

...

2.4.3 Preuve combinatoire

On donne maintenant une preuve combinatoire de la Proposition 25 (p.120) dans le cas d'un alphabet ordinaire puis dans le cas d'un alphabet pondéré. Par construction (p.121), le nombre de mots de longueur n du code Y_{n-1} est égal à $\beta_n + \epsilon_n$. En étudiant la manière dont ces mots sont engendrés, on donne une autre expression de cette somme qui correspond au polynôme P_n cherché.

Cas d'un alphabet ordinaire à k lettres

Pour compter le nombre de mots de longueur n du code Y_{n-1}, on en distingue deux types distincts :

- les produits de mots qui ont été supprimés à une étape de la construction :

$$w = w_p w_{p-1} \cdots w_1$$

où les w_i $(1 \leq i \leq p)$ sont des mots qui ont été supprimés précédemment

- et de tels mots concaténés avec un mot qui appartient lui-même au code Y_{n-1} :

$$w = w_p w_{p-1} \cdots w_1 w_0, \qquad w_0 \in Y_{n-1}$$

où les w_i $(1 \leq i \leq p)$ sont des mots qui ont été supprimés.

L'ordre dans lequel les mots ont été supprimés induit un ordre total sur l'ensemble de ces mots (le premier mot supprimé étant le plus petit) et conditionne la structure des concaténations, la construction étant, de plus, faite au moyen de transformations mettant en jeu des mots de longueur croissante. Par suite, les produits, préfixes d'un mot du code ou eux-mêmes éléments du code, se décomposent en une suite décroissante (pour cet ordre) de mots qui ont été supprimés :

$$\forall i, \qquad |w_{i+1}| \geq |w_i|.$$

Cependant, quand le produit appartient lui-même au code, le dernier terme est strictement plus grand que celui qui le précède : c'est-à-dire si $w = w_p w_{p-1} \cdots w_1$ alors $|w_1| = |w_2|$ et w_1 a été supprimé après w_2.

Plus précisément, les mots de longueur n de la forme $w = w_p w_{p-1} \cdots w_1$, où les w_i $(1 \leq i \leq p)$, sont des mots qui ont été supprimés précédemment (et sont, par conséquent, de longueur strictement inférieure à n) vérifient les conditions suivantes sur les longueurs :

- soit $|w_{i+1}| = |w_i|$,
- soit $|w_{i+1}| > |w_i|$ et $|w_{i+1}| < |w_i w_{i-1} \dots w_1|$.
  En effet, dans le cas contraire (*i.e.* si $|w_{i+1}| \geq |w_i w_{i-1} \dots w_1|$), $w_i w_{i-1} \dots w_1$ est lui-même, soit un mot du code et w est alors un mot de l'autre type que l'on a distingué, soit un mot que l'on supprime, w fait alors partie des mots précédemment décrits.

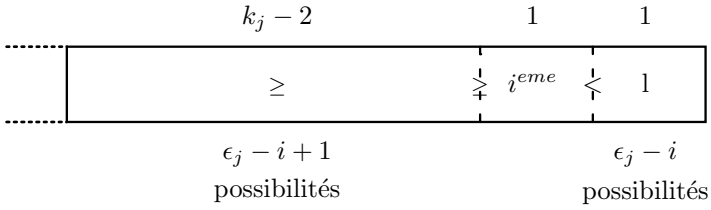


FIG. 2.4 – *Suffixes formés à partir des ϵ_j mots supprimés de longueur j*

On calcule d'abord le nombre de produits de k_j éléments de même longueur qui peuvent apparaître dans un tel mot. On peut noter que les éléments intervenant dans un tel produit peuvent être répétés, mais leur ordre est déterminé de manière unique.

Si le facteur associé n'est pas en position de suffixe (*i.e.*, $|w_1| \neq j$), ce nombre est égal au nombre de combinaisons avec répétitions de k_j éléments pris parmi les ϵ_j éléments supprimés de longueur j soit $\binom{\epsilon_j+k_j-1}{k_j} = P_{k_j}$.

Quand ce produit est en position de suffixe (*i.e.*, $|w_1| = j$), k_j est nécessairement supérieur ou égal à 2 et le dernier élément du produit est strictement plus grand (pour l'ordre de suppression) que le précédent (Figure 2.4)

Soit i le rang de l'avant dernier élément du produit, alors le nombre de préfixes associés de longueur $k_j - 2$ est égal au nombre de combinaisons avec répétition de $k_j - 2$ éléments pris parmi $\epsilon_j - i + 1$, soit $\binom{\epsilon_j+k_j-i-2}{k_j-2}$ et le nombre de valeurs que peut prendre la dernière lettre est égal à $\epsilon_j - i$. Le nombre de produits de k_j éléments de même longueur en position suffixe est donc égal à

$$T_{k_j} = \sum_{i=1}^{\epsilon_j-1} \binom{\epsilon_j + k_j - i - 2}{k_j - 2} (\epsilon_j - i) = (k_j - 1) \sum_{i=1}^{\epsilon_j-1} \binom{\epsilon_j + k_j - i - 2}{k_j - 1} = (k_j - 1) \binom{\epsilon_j + k_j - 2}{k_j}.$$

Par suite, le nombre de mots de longueur n de Y_{n-1} obtenus par concaténation de mots supprimés est

$$R_n = \sum_{\mathcal{P}} \prod_{j_1<j_2<\ldots<j_p} P_{k_{j_p}} \ldots P_{k_{j_2}} T_{k_{j_1}} \quad \text{avec} \quad \begin{cases} T_{k_j} = (k_j - 1)\binom{\epsilon_j+k_j-2}{k_j} & \text{et} \quad k_j > 1 \\ P_{k_j} = \binom{\epsilon_j+k_j-1}{k_j} \end{cases}$$

où la somme est prise sur l'ensemble $\mathcal{P}$ des p-uplets vérifiant les deux conditions suivantes (la deuxième condition exprimant la croissance des longueurs des facteurs) :

$$\sum_l j_l k_{j_l} = n \qquad \text{et} \qquad \forall k, \quad j_k < \sum_{l=1}^{k-1} j_l k_{j_l}.$$

Les autres mots de longueur n du code Y_{n-1} sont de la forme $w = w_p w_{p-1} \cdots w_1 w_0$ où les w_i $(1 \leq i \leq p)$ sont des mots qui ont été supprimés et où w_0 est un mot du code Y_{n-1}

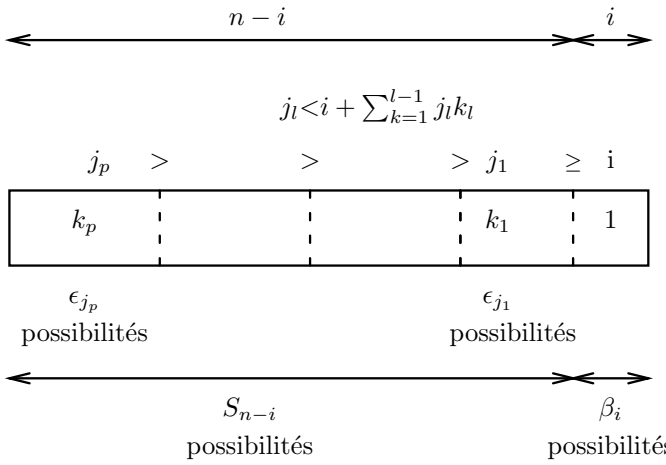


FIG. 2.5 – *Mots formés à partir des mots supprimés et d'un mot du code*

qui a été engendré avant la suppression du mot w_1. Les w_i vérifient alors les conditions suivantes sur les longueurs (Figure 2.5) :

- $\forall i \geq 0, \quad |w_{i+1}| \geq |w_i|$,
- $\forall i \geq 1, \quad |w_{i+1}| < |w_i w_{i-1} \dots w_1 w_0|$.
  En effet, si $|w_{i+1}| \geq |w_i w_{i-1} \dots w_1 w_0|$, alors $w_i w_{i-1} \dots w_1 w_0$ est lui-même, soit un mot du code et w peut alors être factorisé sous une autre forme plus courte, soit un mot que l'on supprime et w est alors un mot du type précédent.

Soit S_{n-i} le nombre de produits $w_p w_{p-1} \cdots w_1$ de longueur $n-i$ pouvant être concaténés avec un mot w_0 de Y_{n-1} de longueur i, alors

$$S_{n-i} = \sum_{\mathcal{S}} \prod_{i \leq j_1 < j_2 < \dots < j_p} P_{k_{j_p}} \dots P_{k_{j_2}} P_{k_{j_1}} \quad \text{avec} \quad P_{k_j} = \binom{\epsilon_j + k_j - 1}{k_j},$$

(les P_{k_j} représentent le nombre de combinaisons avec répétitions de k_j éléments pris dans un ensemble de cardinal ϵ_j) où la somme est prise sur l'ensemble $\mathcal{S}$ des p-uplets vérifiant les conditions suivantes (la condition sur j_k exprimant les relations entre les longueurs des facteurs)

$$\sum_l j_l k_{j_l} = n - i, \qquad i \leq j_1 \quad \text{et} \qquad \forall k \geq 2, \quad j_k < i + \sum_{l=1}^{k-1} j_l k_{j_l}.$$

Le nombre de mots de longueur n, $\beta_n + \epsilon_n$, du code Y_{n-1} est finalement donné par

$$\beta_1 + \epsilon_1 = k,$$

$$\boxed{\forall n \geq 2, \qquad \beta_n + \epsilon_n = \textstyle\sum_{i=1}^{\lfloor n/2 \rfloor} S_{n-i}\beta_i + R_n,}$$

où $\lfloor x \rfloor = \max\{n/n \leq x, n \in \mathbb{N}\}$.

Exemple 41 (suite cf p.119) Soient $k = 3$ et $A = \{a, b, c\}$. On a

$$Y_1 = \{c, \mid \underline{ab}, ac, bc \mid, a^2b, a^2c, bab, bac, b^2c, a^3, a^3c, ba^2b, ba^2c, b^3c, \ldots\}$$

et

$$\beta_2 + \epsilon_2 = P_{1_1}\beta_1 + T_2 = \binom{\epsilon_1}{1}\beta_1 + \binom{\epsilon_1}{2} = 3.$$

$$\begin{aligned} Y_2 \;=\; & \{c, bc, \mid \underline{a^2b}, a^2c, \underline{bab}, bac, b^2c, abc, acc \mid, a^3b, a^3c, \\ & ba^2b, ba^2c, b^2ab, b^2ac, b^3c, abac, abbc, acbc, \ldots\} \end{aligned}$$

et

$$\beta_3 + \epsilon_3 = (P_{2_1} + P_{1_2})\beta_1 + T_{3_1} = \left(\binom{\epsilon_1 + 1}{2} + \epsilon_2\right)\beta_1 + 2\binom{\epsilon_1 + 1}{3} = 7.$$

$$\begin{aligned} Y_3 = Y_2 \;=\; & \{c, bc, a^2b, a^2c, bab, bac, b^2c, abc, acc, \mid \underline{a^3b}, a^3c, \\ & \underline{ba^2b}, ba^2c, \underline{b^2ab}, b^2ac, b^3c, \underline{abac}, abbc, acbc \mid, \ldots\} \end{aligned}$$

et

$$\beta_4+\epsilon_4 = (P_{3_1}+P_{1_3})\beta_1+P_{1_2}\beta_2+T_{4_1}+T_{2_2} = \left(\binom{\epsilon_1 + 2}{3} + \epsilon_3\right)\beta_1+\epsilon_2\beta_2+3\binom{\epsilon_1 + 2}{4}+\binom{\epsilon_2}{2}.$$

Les produits de mots supprimés (soulignés) sont

- pour $n = 2$: ab,
- pour $n = 3$: a^2b, bab,
- pour $n = 4$: $a^3b, ba^2b, b^2ab, abac$.

Les autres mots se décomposent en produits de mots supprimés et d'un mot appartenant au code, ce dernier est alors en position suffixe (par exemple, pour $n = 4$, $b.a^2.c, a^3.c, b^2.a.c, ab.ac$).

Cas d'un alphabet pondéré

Soit $(\alpha_n)_{n\geq 1}$ la distribution de longueurs de l'alphabet pondéré (A, λ).

Le nombre de mots de longueur n du code Y_{n-1} est comme précédemment égal à $\beta_n+\epsilon_n$. Leur description est identique à la précédente à ceci près que l'alphabet étant pondéré, il contient des mots de longueur supérieure à 1, ce qui amène à distinguer un troisième type de mots. En effet, les mots de longueur n du code Y_{n-1} peuvent, dans ce cas, être de la forme $w_pw_{p-1}\cdots w_1w_0$ où les w_i $(1 \leq i \leq p)$ sont des mots qui ont été supprimés et où w_0 appartient à l'alphabet. De plus, les α_i mots de longueur i de l'alphabet étant comptés parmi les ϵ_i mots que l'on supprime ou les β_i qui font partie du code, les longueurs des facteurs vérifient (Figure 2.6)

– $\forall i \geq 1, \quad \lambda(w_{i+1}) \geq \lambda(w_i)$,

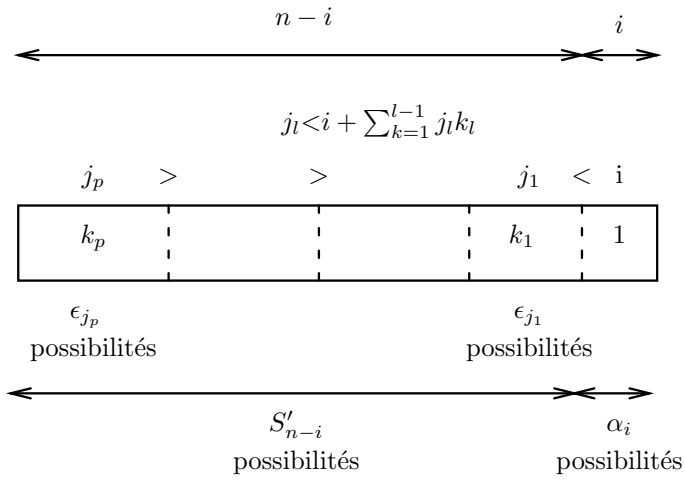


FIG. 2.6 – *Mots formés à partir des mots supprimés et d'un mot de l'alphabet*

– $\forall i \geq 0, \quad \lambda(w_{i+1}) < \lambda(w_i w_{i-1} \dots w_1 w_0)$.
En effet, si $\lambda(w_{i+1}) \geq \lambda(w_i w_{i-1} \dots w_1 w_0)$, $w_i w_{i-1} \dots w_1 w_0$ est lui-même, soit un mot du code, soit un mot que l'on supprime et, w est alors un mot d'un des deux types étudiés précédemment.

En utilisant le calcul fait pour les préfixes des mots du codes dont le nombre est donné par le coefficient S_{n-i} et en tenant compte des relations sur les longueurs des facteurs, on obtient

$$S'_{n-i} = \sum_{\mathcal{S}'} \prod_{j_1<j_2<\dots<j_p} P_{k_{j_p}} \dots P_{k_{j_2}} P_{k_{j_1}} \quad \text{avec} \quad P_{k_j} = \binom{\epsilon_j + k_j - 1}{k_j} \quad \text{et} \quad S'_0 = 1,$$

où la somme est prise sur l'ensemble $\mathcal{S}'$ des p-uplets tels que

$$\sum_j j_l k_{j_l} = n - i, \qquad i > j_1 \quad \text{et} \qquad \forall k \geq 2, \quad j_k < i + \sum_{l=1}^{k-1} j_l k_{j_l}.$$

Finalement, la somme $\beta_n + \epsilon_n$, égale au nombre de mots de longueur n du code Y_{n-1}, s'écrit

$$\beta_1 + \epsilon_1 = \alpha_1,$$

$$\boxed{\forall n \geq 2, \qquad \beta_n + \epsilon_n = \sum_{i=1}^{\lfloor n/2 \rfloor} S_{n-i}\beta_i + R_n + \sum_{i=\lceil n/2 \rceil}^{n} S'_{n-i}\alpha_i.}$$

où $\lfloor x \rfloor = \max\{n \mid n \leq x, n \in \mathbb{N}\}$ et $\lceil x \rceil = \min\{n \mid n \geq x, n \in \mathbb{N}\}$.

2.5 Mesure et propriétés

On définit une mesure de Bernoulli sur un alphabet pondéré fini, ce qui permet de donner une condition nécessaire pour qu'une suite d'entiers naturels soit la distribution de longueurs d'un code. On donne alors une preuve directe du fait que les inégalités sur le nombre de classes de mots primitifs qui caractérisent les codes circulaires implique cette condition, qui est une extension de l'inégalité de Kraft-McMillan.

On établit ensuite une condition nécessaire et suffisante pour qu'une suite d'entiers positifs soit la distribution de longueurs d'un code circulaire maximal sur un alphabet (au sens usuel) fini. On vérifie enfin que la méthode donnée par Ehrenfeucht et Rozenberg (Théorème 20 p.98) pour compléter un code conserve la propriété qui caractérise les codes circulaires.

2.5.1 Mesure sur un alphabet pondéré fini

Soit (A, λ) un alphabet pondéré fini et soit k le nombre réel positif défini par

$$\sum_{a \in A} k^{-\lambda(a)} = 1,$$

alors l'application π qui à $a \in A$ associe $k^{-\lambda(a)}$ est une mesure de Bernoulli positive sur A, uniforme relativement à la longueur λ.

Remarque 19 Le nombre réel k est défini par l'egalité

$$\sum_{a \in A} k^{-\lambda(a)} = \sum_{n=1}^{\Lambda} \alpha_n k^{-n} = 1,$$

où $\alpha_n = \text{Card } \{a \in A \mid \lambda(a) = n\}$ et $\Lambda = max_{a \in A}(\lambda(a))$. On en déduit que k est l'unique solution de l'équation

$$z^{\Lambda} - \sum_{n=0}^{\Lambda-1} \alpha_{\Lambda-n} z^n = 0.$$

Ce réel est donc un nombre d'Handelman, *i.e.*, un nombre dont une puissance entière est un nombre de Perron (entier algébrique strictement supérieur aux modules de ses conjugués) qui n'a pas de conjugué algébrique réel positif. La preuve de ce résultat est donnée par le Théorème 9 (p.56) quand k est lui-même un nombre de Perron et par le Théorème 10 (p. 59) quand k est la racine $n$ième d'un nombre de Perron.

2.5.2 L'inégalité de Kraft-McMillan

La distribution de longueurs d'un code sur un alphabet fini vérifie nécessairement l'inégalité de Kraft-McMillan (Théorème 18 p.95). On étend ce résultat aux codes définis

sur un alphabet pondéré fini (A, λ) et on donne une preuve directe du fait que les inégalités sur les classes de mots primitifs impliquent l'inégalité de Kraft-McMillan.

L'inégalité de Kraft-McMillan s'étend aux alphabets pondérés sous la forme suivante.

Proposition 26 *Soit Y un code sur un alphabet pondéré fini (A, λ) et soit k le nombre réel positif défini par $\sum_{a\in A} k^{-\lambda(a)} = 1$, alors*

$$\sum_{y\in Y} k^{-\lambda(y)} \leq 1$$

ou de façon équivalente

$$\sum_{n\geq 1} \beta_n k^{-n} \leq 1 \qquad \beta_n = Card\,\{y \in Y \mid \lambda(y) = n\}.$$

On donne maintenant deux preuves directes du fait que les inégalités qui caractérisent un code circulaire impliquent l'inégalité de la Proposition 26.

De la relation (2.6) (p.123) et de la définition de k, soit

$$\forall n > 0, \quad \beta_n = \sum_{p=1}^{\Lambda} \alpha_p E_{n-p} - E_n \quad \text{avec} \quad E_0 = 1 \quad \text{et} \quad \sum_{n=1}^{\Lambda} \alpha_n k^{-n} = 1,$$

on déduit

$$\forall n \geq \Lambda, \quad \sum_{i=1}^{n} \beta_i k^{-i} = 1 - \sum_{i=n+1-\Lambda}^{n-1} \frac{E_i}{k^i} \Big(\sum_{j=n+1-i}^{\Lambda} \frac{\alpha_j}{k^j} \Big) - \frac{E_n}{k^n} \leq 1,$$

car

$$\sum_{n\geq 0} E_n z^n = \frac{1}{\prod_{j\geq 0}(1 - z^j)^{\epsilon_j}}, \qquad \Rightarrow \quad \forall n \in \mathbb{N}, \quad E_n \geq 0.$$

La distribution de longueurs $(\beta_i)_{i\geq 0}$ vérifie donc l'inégalité de Kraft-McMillan.

Un raisonnement élémentaire sur le rayon de convergence de la série $1/(1 - \sum_{i\geq 1} \beta_i z^i)$ conduit également au résultat. En effet, en sommant sur l'ensemble des diviseurs d de n les inégalités $dl_d(\beta) \leq dl_d(\alpha)$, comme $s_n = \sum_{d/n} dl_d$, on obtient

$$\forall n \geq 1 \qquad s_n(\beta) \leq s_n(\alpha).$$

De plus, en notant respectivement $\beta_n^{(*)}, \beta_n^{(i)}$ le nombre de mots de longueur n de Y^* et Y^i, on a

$$\begin{aligned} \beta_n^{(*)} &= \sum_{i=1}^{n} \beta_n^{(i)} \\ &\leq \sum_{i=1}^{n} \frac{n}{i} \beta_n^{(i)} = s_n(\beta). \end{aligned}$$

En utilisant la Proposition 24 (p.110), on en déduit que le rayon de convergence de la série génératrice de Y^*,

$$f_{Y^*}(z) = \frac{1}{1 - f_Y(z)} = \frac{1}{1 - \sum_{i\geq 1} \beta_i z^i},$$

est supérieur ou égal à celui de

$$f_{A^*}(z) = \sum_{n\geq 0} s_n(\alpha) z^n = \frac{1}{1 - \sum_{i=1}^{\Lambda} \alpha_i z^i},$$

soit $1/k$, d'où $f_Y(1/k) \leq 1$.

2.5.3 Maximalité et complétude

Dans ce paragraphe, on établit une caractérisation des distributions de longueurs des codes circulaires maximaux sur un alphabet fini A qui n'est pas pondéré. On vérifie également que la méthode générale de complétion d'un code permet de compléter un code circulaire.

On peut remarquer pour commencer que tout code circulaire maximal sur l'alphabet A est nécessairement infini, sauf si $X = A$. En effet, si le code X est fini, alors, d'après la Proposition 14 (p.96), pour toute lettre $a \in A$ il existe un entier $n \geq 1$ tel que $a^n \in X$, comme X est circulaire, $n = 1$ et par conséquent $X = A$.

On rappelle une caractérisation des codes circulaires maximaux ([BP85] Théorème 1.8 p.328).

Proposition 27 *Soit X un code circulaire coupant, alors les trois conditions suivantes sont équivalentes*

1. *X est complet.*
2. *X est un code maximal.*
3. *X est maximal comme code circulaire.*

Exemple 42 L'automate $(Q, 1, 1)$ (Figure 2.7) reconnaît le sous-monoïde X^* engendré par le code circulaire maximal

$$X = (b^2 b^* a)^* \{a, ba\}.$$

Sa série génératrice est

$$f_X(z) = \frac{z - z^3}{1 - z - z^3}, \quad \text{et} \quad f_X(\frac{1}{2}) = 1.$$

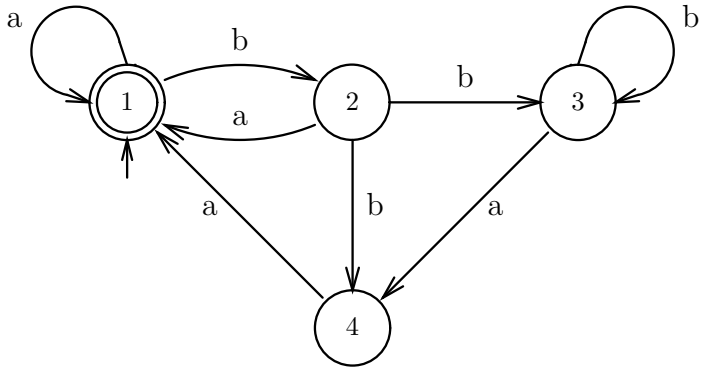


FIG. 2.7 – *Automate reconnaissant X^* où $X = (b^2b^*a)^*\{a, ba\}$ est circulaire maximal*

Caractérisation des codes maximaux

On donne ici une caractérisation des distributions de longueurs des codes circulaires maximaux sur un alphabet fini à k lettres. Ce critère porte sur le comportement asymptotique du nombre de classes de mots primitifs.

On rappelle celui du nombre de classes de mots primitifs de A^*, quand A est un alphabet à k lettres.

Propriété 3 *Soit $l_n(k)$ le nombre de classes de mots primitifs de longueur n sur un alphabet (au sens usuel) à k lettres, alors*

$$\lim_{n\to\infty} \frac{nl_n(k)}{k^n} = 1.$$

Démonstration : On a

$$nl_n(k) = \sum_{d/n} \mu(\frac{n}{d})k^d,$$

soit

$$\frac{nl_n(k)}{k^n} = 1 + \sum_{d/n, d\neq n} \mu(\frac{n}{d})k^{d-n}.$$

Comme $k^{d-n} \leq k^{-n/2}$, la valeur absolue de la somme qui apparaît dans le membre droit est majorée par $nk^{-n/2}$, on en déduit que $\sum_{d/n} \mu(\frac{n}{d})k^{d-n}$ tend vers 0 quand n tend vers l'infini. □

On établit maintenant une propriété concernant le comportement asymptotique du nombre de classes de mots primitifs d'un code circulaire sur un alphabet fini.

Propriété 4 *Soit X un code circulaire de distribution de longueurs $(\alpha_n)_{n\geq 1}$, alors les trois limites suivantes sont égales*

$$\limsup_{n\to\infty} \frac{s_n(\alpha)}{k^n} = \limsup_{n\to\infty} \frac{nl_n(\alpha)}{k^n} = \limsup_{n\to\infty} \frac{l_n(\alpha)}{l_n(k)} = \delta_X.$$

Leur valeur commune δ_X est appelée la *densité circulaire* du code X sur l'alphabet A.

Démonstration : Comme $s_n(\alpha) = \sum_{d/n} dl_d(\alpha)$ et que

$$\forall d/n, \quad d \neq n, \qquad dl_d(\alpha) \leq \frac{n}{2} k^{n/2}$$

on a

$$\limsup_{n\to\infty} \frac{nl_n(\alpha)}{k^n} \leq \limsup_{n\to\infty} \frac{s_n(\alpha)}{k^n} \leq \limsup_{n\to\infty} (\frac{nl_n(\alpha)}{k^n} + \frac{n^2}{4} k^{-n/2}) = \limsup_{n\to\infty} \frac{nl_n(\alpha)}{k^n},$$

soit, en utilisant également la propriété 3 (p.133)

$$\limsup_{n\to\infty} \frac{s_n(\alpha)}{k^n} = \limsup_{n\to\infty} \frac{nl_n(\alpha)}{k^n} = \limsup_{n\to\infty} \frac{l_n(\alpha)}{l_n(k)},$$

ce qui prouve la propriété annoncée. □

La proposition suivante dit qu' un code circulaire X est maximal dans A^* si, et seulement si, les comportements asymptotiques du nombre de classes de mots primitifs de X^* et de A^* sont du même ordre.

Théorème 25 *Soit X un code circulaire coupant de distribution de longueurs $(\alpha_n)_{n\geq 1}$, alors le code X est maximal sur A où A est un alphabet à k lettres si, et seulement si, sa densité circulaire δ_X dans A^* est strictement positive.*

Démonstration : On va établir

$$\delta_X = \limsup_{n\to\infty} \frac{s_n(\alpha)}{k^n} > 0.$$

Si le code coupant X est maximal, d'après le Théorème 27 (p.132), il est alors complet. Comme il est coupant et circulaire, il est également synchronisant (Proposition 19 p.101). Le code étant coupant, complet et synchronisant, on en déduit, en utilisant la Proposition 18 (p.101), qu'il existe donc deux mots x et y de X^* tels que

$$xA^*y \subset X^*.$$

On appelle l la somme des longueurs des mots x et y, soit $l = |x| + |y|$. On a alors

$$\forall n > 0, \quad xA^n y \subset \left(X^* \cap A^{n+l}\right),$$

d'où

$$s_{n+l}(\alpha) \geq k^n.$$

On en déduit que

$$\forall n > 0, \quad \frac{s_{n+l}(\alpha)}{k^{n+l}} \geq \frac{1}{k^l}.$$

Par suite, si le code est maximal

$$\exists l \in \mathbb{N}^* \qquad \limsup_{n\to\infty} \frac{s_n(\alpha)}{k^n} > \frac{1}{k^l} > 0.$$

D'autre part, d'après le Théorème 27 (p.132), si le code X n'est pas maximal, il n'est pas complet. Par suite, il existe un mot y de A^* de longueur n_0 qui n'est facteur d'aucun mot de X^*. Soit w un mot de longueur $n \geq n_0$ dont un conjugué appartient à X^*, alors y n'est pas un facteur de w. En effet, si y était facteur d'un mot $w = uv$ ayant un conjugué $t = vu$ dans X^*, alors y serait facteur de $t^2 = vuvu$. On en déduit que le plus long préfixe de longueur multiple de n_0 d'un mot de longueur n dont un conjugué appartient à X^* peut être codé sur $A^{n_0} \setminus \{y\}$. On a alors

$$\exists n_0 = |y|, \quad \text{tel que} \quad \forall n \geq n_0 \qquad s_n \leq (k^{n_0} - 1)^{\lfloor n/n_0 \rfloor} k^{(n \bmod n_0)},$$

où $\lfloor x \rfloor = \max\{n \mid n \leq x, n \in \mathbb{N}\}$. On obtient finalement

$$\limsup_{n\to\infty} \frac{s_n(\alpha)}{k^n} \leq \lim_{n\to\infty} (1 - \frac{1}{k^{n_0}})^{\lfloor n/n_0 \rfloor} = 0.$$

Par conséquent, si

$$\limsup_{n\to\infty} \frac{s_n(\alpha)}{k^n} > 0,$$

alors le code peut être construit maximal, ce qui montre que cette dernière condition est nécessaire et suffisante et conclut la preuve du Théorème 25 □

Méthode de complétion

On rappelle pour commencer une propriété connue des codes circulaires (pour la démonstration, on pourra se reporter à [BP85] Proposition 1.7 p.327)

Lemme 11 *Si un code circulaire X n'est pas complet, alors il existe un mot y sans bord de A^* qui n'est pas un facteur de X^* et tel que $X \cup \{y\}$ soit un code circulaire.*

On montre, dans ce qui suit, que la méthode générale (Théorème 20 p.98) de complétion des codes permet également de compléter un code circulaire en conservant cette propriété.

Proposition 28 *Soient X un code circulaire et $y \in A^*$ un mot sans bord tel que*

$$X^* \cap A^* y A^* = \emptyset$$

et soit $U = A^* \setminus X^* \setminus A^* y A^*$ alors $Y = X \cup y(Uy)^*$ est un code circulaire complet.

Démonstration : Soit V l'ensemble des mots de A^* dont y n'est pas facteur :

$$V = A^* \setminus A^* y A^*.$$

Par hypothèse, X^* est une partie de V et $U = V \setminus X^*$.

On peut remarquer pour commencer que l'ensemble $Z = Vy$ est un code préfixe. En effet, si l'on suppose $vy < v'y'$ où v et v' sont deux mots de V. Comme y est sans bord, vy est nécessairement un facteur gauche de de v'. Alors v' appartient à A^*yA^*, ce qui contredit l'hypothèse $v' \in V$. L'ensemble Z est donc préfixe.

On va maintenant montrer que Y est un code circulaire. On suppose le contraire ; pour cela, soient x_i $(1 \leq i \leq n)$ et y_i $(1 \leq i \leq m)$ des mots de Y et soient $p \in A^*$ et $s \in A^+$ tels que

$$sx_2x_3 \dots x_n p = y_1 y_2 \dots y_m,$$

$$x_1 = ps.$$

Si tous les x_i $(1 \leq i \leq n)$ sont dans X, il en est de même des y_i puisque Y n'est facteur d'aucun mot de X^*. Comme, de plus, X est circulaire cela implique que

$$n = m, \qquad p = 1 \qquad x_i = y_i \quad (1 \leq i \leq n). \tag{2.7}$$

On suppose maintenant qu'un des x_i n'appartient pas à X. Soit t le plus petit indice tel que $x_t \in Y \setminus X$.

$\circ$ On traite pour commencer le cas où $t \neq 1$.

Comme $y \notin F(X^*)$, $x_t \notin F(X^*)$. Par suite l'un des y_i est un élément de $y(Uy)^*$, soit q le plus petit indice tel que $y_q \in y(Uy)^*$. Alors

$$sx_2x_3 \dots x_{t-1}y, \qquad y_1y_2 \dots y_{q-1}y \in Z,$$

et $sx_2x_3 \dots x_{t-1} = y_1y_2 \dots y_{q-1}$ puisque Z est préfixe. On pose

$$x_t = yu_1y \dots yu_ky,$$

$$y_q = yv_1y \dots yv_ly,$$

où les u_i $(1 \leq i \leq l)$ et les v_i $(1 \leq i \leq l)$ sont des éléments de U.

On suppose $x_t < y_q$; comme Z est préfixe, Z^* est unitaire à droite , *i.e.*,

$$u, uv \in Z^* \Rightarrow v \in Z^*.$$

Comme $U \subset V$, il s'en suit que chaque u_iy et chaque v_iy est un élément de Z et que $u_i = v_i$ $(1 \leq i \leq k)$. Soit $t = v_{k+1}y \dots yv_l$, on a

$$x_{t+1} \dots x_n p = t y_{q+1} \dots y_m.$$

Comme le mot y est un facteur de t, il apparaît aussi dans $x_{t+1}\dots x_np$. Comme $x_1 = ps \in X$ et que y est sans bord, l'un des $x_{t+1},\dots,x_n$ appartient à $y(Uy)^*$, soit x_r l'élément correspondant d'indice minimal. Alors $x_{t+1}\dots x_{r-1}y \in Z$ et $v_{k_+1}y \in Z$ sont les facteurs gauches d'un même mot. Comme Z est un code préfixe, $v_{k+1} = x_{t+1}\dots x_{r-1}$. Par suite $v_{k+1} \in X^*$ ce qui contredit l'hypothèse $v_{k+1} \in U$.

On suppose maintenant $x_t > y_q$; on obtient de façon analogue que $u_i = v_i$ $(1 \le i \le l)$. Soit $t = u_{l+1}y\dots u_k$, on a

$$tx_{t+1}\dots x_np = y_{q+1}\dots y_m,$$

dont on déduit également que nécessairement $u_{l+1} = y_{q+1}\dots y_{r-1}$ et la contradiction entre $u_{l+1} \in X^*$ et l'hypothèse $u_{l+1} \in U$.

Par suite, $k = l$ et $x_t = y_q$, ce qui conduit à l'égalité

$$sx_2\dots\dots x_{t-1}x_{t+1}\dots x_np = y_1\dots y_{q-1}y_{q+1}\dots y_m,$$

on obtient alors (2.7) par induction sur la longueur des mots.

∘ On traite finalement le cas où $x_1 \in y(Uy)^*$.

Comme

$$x_1x_2\dots x_np = py_1y_2\dots y_m,$$

le mot p est facteur droit (et facteur gauche) d'un mot de Y^*.

Si $|p| < y$, alors p est préfixe de y et suffixe de $y_1y_2\dots y_m$. Le mot s a y pour suffixe et est préfixe de $y_1y_2\dots y_m$. Par suite, comme y est sans bord, le mot $ps \in X^*$, ce qui contredit l'hypothèse $x_1 \in y(Uy)^*$.

Si $|p| > y$, $p = yu_1y\dots yu_k$ et $s = u'_ky\dots y$ où les u_i et $u_ku'_k$ sont dans U.

Un autre cas de figure possible est celui où s est un suffixe de y, on le traite de manière analogue au au cas $|p| < y$.

Comme $u_ku'_k \notin X^*$, l'un des y_i appartient à $y(Uy)^*$, soit j le plus petit indice correspondant, comme y est sans bord et que $y \notin F(X^*)$, on a $u'_k = y_1\dots y_{j-1}$, c'est-à dire $u'_k \in X^*$; de plus, comme yu_k est un suffixe de $y_1y_2\dots y_m$, que y est est sans bord et n'est pas facteur de u_k, on en déduit que $u_k \in X^*$. On aboutit alors à une contradiction puisque $u_ku'_k \notin X^*$.. On en conclut que $p = 1$ et comme Y est un code, on obtient (2.7).

Il reste à montrer que le code Y est complet. Soit $w \in A^*$. On pose

$$w = v_1y\dots yv_n, \quad \text{où} \quad n \ge 1 \quad \text{et} \quad v_i \in A^* \setminus A^*yA^*.$$

Alors $ywy \in Y^*$. Soit $(v_{i_1}, v_{i_2}, \dots, v_{i_k})$ la sous-suite formée des v_i appartenant à X^*. Alors

$$ywy = (yv_1y\dots yv_{i_{i-1}}y)v_{i_1}(yv_{1+1}y\dots yv_{i_2-1}y)\dots v_{i_k}(yv_{i_k+1}y\dots yv_{i_n}y) \in Y^*,$$

chaque mot entre parenthèses étant un mot de Y. Le code Y est donc circulaire et complet.□

Problème ouvert

La caractérisation des distributions de longueurs des codes circulaires rationnels demeure un problème ouvert. On peut de demander si la caractérisation des codes circulaires s'étend aux codes rationnels sous l'hypothèse supplémentaire que la série est $\mathbb{N}$-rationnelle :

Soit $f(z) = \sum_{n\geq 1} \alpha_n z^n$ une série $\mathbb{N}$-rationnelle dont les coefficients vérifient les inégalités

$$\forall n \geq 1 \qquad l_n(\alpha) \leq l_n(k),$$

existe-il alors un code rationnel circulaire sur un alphabet à k lettres dont f est la série génératrice ?

Chapitre 3

Codes préfixes rationnels

Introduction

Les codes préfixes sont une famille de codes, introduite par Morse. Ces codes sont caractérisés par la propriété suivante : aucun mot du code n'est le début d'un autre. Vérifier qu'un code est préfixe est alors immédiat. De tels codes présentent l'avantage de permettre un décodage instantané.

Par ailleurs, beaucoup de problèmes intéressants de la théorie des codes peuvent être étudiés dans le cadre particulier des codes préfixes. Ceux-ci constituent, en un certain sens, des "modèles" de codes : il est souvent plus facile d'étudier les codes préfixes que des codes généraux et les raisonnements sont souvent encore valides dans le cas général.

Un code préfixe peut être représenté par un arbre, dans lequel le nombre de fils d'un nœud est au plus égal à la taille de l'alphabet sur lequel est construit le code. Les feuilles correspondent alors aux mots du code. Les codes préfixes complets $X \subset A^*$ sont ceux qui ont pour représentation un arbre complet, c'est-à-dire dont les nœuds ont, soit autant de fils que l'alphabet a d'éléments, soit aucun fils. La représentation graphique est ainsi plus lisible qu'une simple énumération des mots du code.

On sait, d'après le théorème de Kraft-McMillan (Proposition 29 p.144), qu'à partir de toute suite $(\alpha_n)_{n\geq 1}$ à coefficients entiers positifs telle que

$$\exists k \in \mathbb{N}^* \qquad \sum_{n\geq 1} \alpha_n k^{-n} \leq 1,$$

on peut construire un code préfixe sur un alphabet à k lettres ayant, pour tout entier n, α_n mots de longueur n.

On cherche à caractériser lesquelles parmi ces suites à coefficients entiers sont distributions de longueurs d'un code préfixe rationnel sur un alphabet à k lettres. Une condition nécessaire évidente est que la suite $(\alpha)_{n\geq 1}$ soit $\mathbb{N}$-rationnelle. Mais est-ce suffisant ?

D'une manière générale, si $\alpha = \sum_{n\geq 1} \alpha_n z^n$ est une série $\mathbb{N}$-rationnelle vérifiant l'inégalité de Kraft-McMillan :

$$\exists k \in \mathbb{N}^*, \qquad \text{tel que} \quad \alpha(\frac{1}{k}) \leq 1,$$

on peut construire un code préfixe rationnel ayant, pour tout n, α_n mots de longueur n. L'alphabet sur lequel est écrit le code a alors éventuellement plus de k lettres. La difficulté réside dans le fait d'obtenir un code préfixe qui soit rationnel et écrit sur alphabet à k lettres.

On présente une réponse partielle à cette question : on donne, en utilisant un résultat de Perrin ([Per89]) sur les arbres rationnels, une condition suffisante pour qu'une série $\mathbb{N}$-rationnelle soit la distribution de longueurs d'un code complet sur un alphabet à k lettres.

Dans la première partie de ce chapitre, on donne le mode de représentation d'un code préfixe sous forme d'arbre.

On met en évidence, dans la deuxième partie, les liens entre les codes préfixes et une classe de séries $\mathbb{N}$-rationnelles liée à des systèmes de réécriture particuliers : les DOL-séries. On montre que l'on peut construire un arbre rationnel à partir de toute série $\mathbb{N}$-rationnelle vérifiant l'inégalité de Kraft-McMillan.

La dernière partie est consacrée à la construction, sous une hypothèse appropriée, de codes préfixes rationnels et maximaux sur un alphabet à k lettres.

Dans l'ensemble, ce chapitre regroupe des résultats déjà connus. Son but est essentiellement de préciser les données du problème et les cas de figure que l'on sait traiter.

3.1 Représentation littérale

Ensembles préfixes et préfixiels

On dit qu'un mot v est *préfixe* d'un mot u s'il existe un mot w de A^* tel que $u = vw$. La relation "être préfixe" est une relation d'ordre partiel sur A^*, appelée *ordre préfixiel* et notée $\leq$.

Si l'alphabet est un ensemble totalement ordonné, on peut définir une relation d'ordre total sur les mots de A^*, appelé *ordre lexicographique* et noté $\leq_{lex}$. On a alors

$$u \leq_{lex} v \quad \text{si} \quad \begin{cases} u \leq v \\ \text{ou} \quad u = xau', v = xbv' \quad \text{avec} \quad x, u', v' \in A^* \quad \text{et} \quad a <_{lex} b. \end{cases}$$

Une partie X de $A^\star$ est *préfixe* si $X \cap XA^+ = \emptyset$, *i.e.* si elle est formée d'éléments deux à deux incomparables pour l'ordre préfixiel :

$$\forall x, x' \in X, \quad x \leq x' \quad \Rightarrow \quad x = x'$$

Si X contient le mot vide 1 alors $X = \{1\}$. Dans les autres cas, X est un code.

Exemple 43 Le code de Morse (cf. Exemple 28 p.94) et le code ASCII sont des codes préfixes.

Exemple 44

Soient A un alphabet et X un langage sur A.

- L'ensemble des éléments de X qui sont minimaux pour l'ordre préfixe, $X \setminus XA^+$, est un code préfixe.

- De même, l'ensemble des éléments de X qui sont maximaux pour l'ordre préfixe

$$X \setminus XA^- = XA \setminus X(A^+)^{-1} \qquad \text{en notant} \quad XA^- = X(A^+)^{-1}$$

est préfixe.

De manière duale, une partie de A^* est dite *préfixielle* si elle contient les préfixes de tous ses éléments.

Exemple 45 Si X est un code préfixe sur l'alphabet A, alors l'ensemble des mots de A^* qui n'ont aucun préfixe dans X, $A^* \setminus XA^+$ est préfixiel.

Soit A un alphabet fini. On peut définir une bijection entre les ensembles préfixes et les ensembles préfixiels de A^* en associant à chaque ensemble préfixe P, l'ensemble préfixiel, $A^* \setminus PA^*$, formé des mots de A^* n'ayant aucun préfixe dans P. Réciproquement, on associe à chaque ensemble préfixiel P', l'ensemble préfixe formé des éléments minimaux, pour l'ordre préfixiel, de A^* qui ne sont pas préfixes d'un mot de P'.

Ces deux notions sont étroitement liées à la notion d'arbre.

Arbres

Un *arbre* T est un triplet (N, r, p) où N est un ensemble non vide, dont les éléments sont appelés les *nœuds* de l'arbre, r est un élément distingué de N appelé la *racine* de l'arbre et p une fonction

$$p : N \setminus \{r\} \longrightarrow N$$

qui, à un nœud n distinct de la racine, associe un unique nœud appelé son *père* et telle que, pour chaque nœud n de N, il existe un entier positif k, appelé la *hauteur* du nœud n, tel que

$$p^k(n) = r.$$

On dira qu'un nœud n est *interne* s'il existe au moins un nœud n' tel que $p(n') = n$, dans le cas contraire on dira que n est une *feuille*.

Le vocabulaire utilisé pour qualifier les relations entre les nœuds est emprunté à celui de la langue courante désignant les liens de parenté. On dit ainsi que n est le fils de $p(n)$ et que n est un *descendant* de n' s'il existe un entier positif k tel que $n' = p^k(n)$.

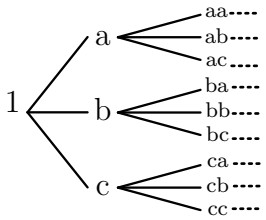


FIG. 3.1 – *L'arbre associé à* $\{a, b, c\}^*$

Si n est un nœud de l'arbre T, l'application p induit une application

$$p_n : N_n \setminus \{n\} \longrightarrow N_n,$$

où N_n désigne l'ensemble des descendants de n. Le triplet (N_n, n, p_n) est alors le sous-arbre de T issu de n.

Dans un arbre, on appelle *branche* ou chemin d'un nœud n_1 à un nœud n_k toute suite $(n_1, n_2, \ldots, n_k)$ de nœuds telle que, pour tout i compris entre 1 et $k-1$, n_i est le père de n_{i+1}. De manière analogue, on appelle *branche infinie* ou *chemin infini* d'origine n_1 toute suite infinie $(n_1, n_2, \ldots)$ de nœuds telle que, pour tout $i \geq 1$, n_i est le père de n_{i+1}.

Le nombre de fils d'un nœud est l'*arité* de ce nœud. L'*arité* d'un arbre est égale au maximum des arités de ses nœuds.

On dira qu'un arbre *fini* d'arité fixée k est *complet* si tous ses nœuds internes ont exactement k fils. On dira qu'un arbre *infini* est *complet* si tous ses nœuds internes ont exactement k fils et si, de plus, à partir de tout nœud, il existe une branche finie menant à une feuille.

Représentation littérale

On associe à l'ensemble A^* des mots écrits sur l'alphabet A un arbre infini étiqueté de la manière suivante. L'alphabet est totalement ordonné et les mots de même longueur sont classés selon l'ordre lexicographique. Chaque nœud de l'arbre est étiqueté par un mot distinct de A^*, la racine étant étiquetée par le mot vide. L'ensemble des fils d'un nœud est muni d'une relation d'ordre totale, les fils sont alors représentés verticalement selon cet ordre. Les mots de longueur n sont exactement les étiquettes des nœuds de hauteur n de l'arbre. Si u est un préfixe de v, alors il existe chemin fini du nœud n_u étiqueté par v au nœud n_v étiqueté par v. L'arbre ainsi obtenu est appelé la *représentation littérale* de A^*.

Exemple 46 Le monoïde libre A^* où $A = \{a, b, c\}$
L'ensemble $\{a, b, c\}^*$ des mots écrits avec les lettres a, b et c a pour représentation littérale l'arbre suivant (Figure 3.1).

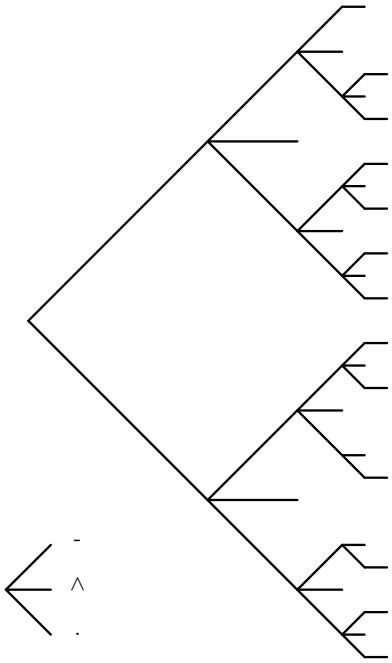


FIG. 3.2 – *Représentation littérale du code de Morse*

A un langage donné X sur l'alphabet A, on associe alors un sous-arbre de la représentation littérale de A^* en ne conservant que les nœuds qui correspondent à des mots de X, ainsi que tous les nœuds qui apparaissent dans les chemins menant de la racine à ces nœuds. L'arbre ainsi obtenu est la *représentation littérale* du langage X.

Un code X est alors préfixe si, et seulement si, dans sa représentation littérale, les mots du code sont exactement les feuilles de l'arbre.

Exemple 47 Le code de Morse (cf. Exemple 28 p.94) a pour représentation littérale l'arbre ternaire de la Figure 3.2. Le code étant préfixe, ses éléments sont les feuilles de cet arbre.

Dans ce mode de représentation, un langage $P \subset A^*$ est alors préfixiel si tous les nœuds de l'arbre correspondent à des mots de P.

Si $X \subset A^*$ est un code préfixe, la partie préfixielle P, formée des mots n'ayant pas de préfixe dans X,

$$P = A^* \setminus XA^+$$

est représentée par l'arbre obtenu à partir de la représentation littérale de A^* en coupant toutes les branches ayant comme origine un mot de X. Les codes préfixes sur un alphabet fini sont en bijection avec les parties préfixielles ainsi décrites.

Codes préfixes rationnels

Un arbre est *rationnel* s'il ne possède qu'un nombre fini de sous-arbres non isomorphes.
Soit $T = (N, r, p)$ un arbre, on appelle série génératrice de T la série formelle

$$s(T) = \sum_{k\geq 0} s_k z^k \qquad \text{où} \quad \forall k \geq 0, \quad s_k = \text{Card } \left(p^{-k}(r)\right)$$

est le nombre de nœuds de hauteur k dans T. Si T est un arbre rationnel, la série $s(T)$ est alors $\mathbb{N}$-rationnelle.

Un code rationnel X est préfixe si, et seulement si, l'automate $\mathcal{A} = (Q, 1, F, E)$ non-ambigu dont X constitue l'ensemble des étiquettes des chemins de premier retour, *i.e*, $X = X_{\mathcal{A}}$, peut être choisi déterministe.

Le code rationnel est préfixe et complet si, et seulement si, l'automate $\mathcal{A} = (Q, 1, F, E)$ peut être choisi déterministe et complet :

$$\forall p \in Q, \quad \forall a \in A, \quad \exists! q \in Q \qquad \text{tel que} \quad (p, a, q) \in E.$$

Si le code est rationnel, sa représentation littérale est un arbre rationnel. Il est rationnel et complet s'il en est de même de sa représentation littérale.

Un langage rationnel est préfixiel s'il est reconnu par un automate dont tous les états sont finaux.

Si X est un code rationnel sur un alphabet A à k lettres, sa série génératrice n'est autre que celle de sa représentation littérale. Sa distribution de longueurs α est alors une suite $\mathbb{N}$-rationnelle et $\alpha(1/k) \leq 1$, d'après l'inégalité de Kraft-McMillan (Théorème 18 p.95).

Problème

On cherche à établir la réciproque.
Soit $\alpha(z) = \sum_{n\geq 0} \alpha_n z^n$ une série $\mathbb{N}$-rationnelle telle que $\alpha(1/k) \leq 1$.

- Existe-t-il un code rationnel préfixe X sur un alphabet à k lettres dont la série génératrice est α ? De manière équivalente, existe-t-il un arbre rationnel d'arité au plus k ayant α_n feuilles à la hauteur n ?

- Si $\alpha(1/k) = 1$, le code peut-il être construit maximal ? En d'autres termes, l'arbre peut-il être choisi complet ?

Le résultat suivant constitue la deuxième partie du théorème de Kraft-McMillan ([McM56]). Il montre que l'on peut construire un code préfixe sur un alphabet à k lettres. Il permet également d'écarter dans l'étude qui suit les séries réduites à des polynômes, la rationalité ne posant aucun problème dans ce cas.

Proposition 29 *Soit α une suite d'entiers positifs telle que*

$$\sum_{n\geq 0} \alpha_n k^{-n} \leq 1.$$

Alors, il existe un code préfixe X sur un alphabet à k lettres ayant pour distribution de longueurs $(\alpha_n)_{n\in\mathbb{N}^*}$.

Démonstration : Soit A un alphabet à k lettres. On définit par induction une suite de codes $(X_n)_{n\geq 1}$ telle que, pour tout n, X_n est une partie de A^n de cardinal α_n et telle que l'union de tous les ensembles X_n soit un code préfixe.

On choisit arbitrairement α_1 lettres de A pour constituer X_1, ce qui est possible puisque $\alpha_1 \leq k$. On suppose ensuite les $n-1$ premiers codes X_i construits et on pose

$$Y_n = \bigcup_{i=1}^{n-1} X_i.$$

Le nombre de préfixes "libres" de longueur n est alors

$$\mathrm{Card}((A^* \setminus Y_n A^*) \cap A^n) = k^n - \sum_{i=1}^{n-1} \alpha_i k^{n-i} = k^n \left(1 - \sum_{i=1}^{n-1} \alpha_i k^{-i}\right).$$

Comme, par hypothèse, $\sum_{i=1}^{n} \alpha_i k^{-i} \leq 1$, on en déduit que

$$(1 - \sum_{i=1}^{n-1} \alpha_i k^{-i}) \geq \alpha_n k^{-n}.$$

Par suite, le nombre de préfixes libres de longueur n dans A^* est supérieur à α_n. Il suffit maintenant d'en choisir α_n pour constituer X_n et l'ensemble $X_n \cup Y_n$ ainsi obtenu est préfixe. □

On utilise maintenant la bijection qui met en correspondance tout code préfixe sur un alphabet A à k lettres avec le langage dont les mots n'ont aucun préfixe dans ce code.

Si X est un code préfixe de distribution de longueurs $(\alpha_n)_{n\geq 1}$, la partie préfixielle formée des mots n'ayant pas de préfixe dans X a alors pour série génératrice

$$\beta(z) = \frac{1 - \alpha(z)}{1 - kz},$$

où α est la série $\sum_{n\geq 1} \alpha_n z^n$. Le problème présenté ci-dessus peut alors être reformulé sous la forme suivante :

– Existe-t-il un arbre rationnel d'arité au plus k dont la série des nœuds internes est β ? En d'autres termes, existe-t-il un automate reconnaissant la série β ayant un seul état initial, tous ses états finaux et chacun à l'origine d'au plus k transitions ?

3.2 Fonctions de croissance des DOL-systèmes

Les L-systèmes ont été introduits par Lindenmayer ([Lin68]) dans le cadre de préoccupations biologiques. Ce sont des systèmes de réecriture parallèle : à chaque étape de ce processus les lettres du mot considéré sont réécrites simultanément. Pour une présentaion générale de ce sujet, on pourra se reporter à [RS80].

Les DOL-systèmes sont des L-systèmes déterministes qui peuvent être définis comme la donnée d'un alphabet A, d'un mot w de A^* et d'un endomorphisme h de A^*. Le langage engendré par un tel système est alors la suite des mots $(h^n(w))_{n\geq 0}$.

DOL-séries

La *fonction de croissance* d'un DOL-système est la suite des longueurs des mots du langage engendré. La série associée est alors une *DOL-série* (cf. [Sal90],[SS78]).

Ces séries peuvent également être définies de manière intrinsèque : une série $\mathbb{N}$-rationnelle en une variable r est appelée une *DOL-série* s'il existe une représentation linéaire (l, M, c) de r à coefficients dans $\mathbb{N}$, telle que

$$\forall n \geq 0 \qquad r_n = lM^n c,$$

où c est un vecteur colonne ne comportant que des 1. La suite des coefficients $(r_n)_{n\geq 0}$ de r est appelée une *DOL-suite*.

Ces suites sont caractérisées par le théorème suivant, dont la preuve est donnée dans [SS78] p.104 (Corollaire 7.8).

Théorème 26 (Soittola) *Si $(r_n)_{n\geq 0}$ est une suite $\mathbb{N}$-rationnelle telle que*
- $\forall n \in \mathbb{N}, \quad r_n \neq 0$
- il existe une constante k telle que, pour tout n, $r_{n+1}/r_n \leq k$
alors $(r_n)_{n\geq 0}$ est une DOL-suite.

A l'aide de ce résultat, on établit que la série "préfixielle" $\beta = (1-\alpha)/(1-kz)$ associée à la série α est une DOL-série ; comme, de plus, $\beta_0 = 1$, on en déduit que l'on peut construire un arbre rationnel dont le nombre de nœuds internes à distance n de la racine est β_n.

Proposition 30 *Soit $\alpha(z) = \sum_{n\geq 1} \alpha_n z^n$ une série $\mathbb{N}$-rationnelle, telle que*

$$\exists k \in \mathbb{N}^*, \qquad \alpha(\frac{1}{k}) \leq 1.$$

Alors la série $\beta(z) = \sum_{n\geq 0} \beta_n z^n = (1-\alpha(z))/(1-kz)$ est
- une DOL-série et $\beta_0 = 1$,
- la série génératrice des nœuds internes d'un arbre rationnel,
- reconnue par un automate ayant un seul état initial et dont tous les états sont finaux.

Démonstration : On suppose désormais $k \geq 2$.

Soit $\alpha(z) = \sum_{n\geq 1} \alpha_n z^n$ une série $\mathbb{N}$-rationnelle qui n'est pas un polynôme et telle que

$$\alpha(1/k) \leq 1.$$

On définit la série associée β correspondant aux nœuds internes de l'arbre par

$$\beta(z) = \sum_{n\geq 0} \beta_n z^n = \frac{1-\alpha(z)}{1-kz}.$$

La suite $(\beta_n)_{n\geq 0}$ vérifie alors

$$\beta_0 = 1$$

et

$$\forall n \geq 1, \quad \beta_n = k\beta_{n-1} - \alpha_n.$$

La série β est $\mathbb{N}$-rationnelle.

En effet, soit

$$\alpha(z) = \frac{P(z)}{Q(z)}$$

la fonction génératrice de la série α où P et Q sont des polynômes à coefficients entiers qui sont premiers entre eux. Alors la série génératrice de la série β est donnée par

$$\beta(z) = \frac{Q(z) - P(z)}{(1-kz)Q(z)}.$$

On en déduit que β est $\mathbb{Z}$-rationnelle.

De plus,

$$\forall n \in \mathbb{N}, \quad \beta_n \geq 0,$$

car

$$\sum_{n\geq 0} \beta_n z^n = (1 - \sum_{n\geq 1} \alpha_n z^n) \sum_{n\geq 0} k^n z^n = \sum_{n\geq 0} (k^n - \sum_{1\leq p\leq n} \alpha_p k^{n-p}) z^n,$$

soit

$$\beta_n = k^n (1 - \sum \alpha_p k^{-p}) \geq 0,$$

car $\alpha(1/k) \leq 1$.

Enfin si $\alpha(1/k) < 1$, la série β a pour racine dominante k et pour rayon de convergence $1/k$.

Dans le cas contraire, comme $\alpha(1/k) = 1$, le polynôme $Q(z) - P(z)$ est divisible par $(1-kz)$ et les racines de la série β sont celles de la série α. Par suite, la série β a le même rayon de convergence ρ ($\rho > 1/k$) que la série α.

Dans les deux cas, la série β est donc $\mathbb{N}$-rationnelle.

Puisque la série α n'est pas un polynôme et que $\alpha(1/k) \leq 1$, les coefficients de la série β sont tous strictement positifs.

Comme, de plus,

$$\beta_0 = 1 \qquad \text{et} \qquad \forall n \geq 1, \quad \beta_n \leq k\beta_{n-1},$$

on en déduit, d'après le Théorème 26 (p.146), que la série β est une DOL-série.

Par suite, la série β admet une représentation linéaire (l, M, c) à coefficients dans $\mathbb{N}$, telle que

$$\forall n \geq 0 \qquad r_n = lM^n c,$$

où c est un vecteur colonne ne comportant que des 1. Comme $\beta_0 = 1$, le vecteur-ligne l ne contient qu'un seul coefficient non nul égal à 1. L'automate fini associé à cette représentation linéaire a un seul état initial et tous ses états finaux. Son interprétaion conduit à un arbre rationnel dont l'arité est égale au maximum des sommes des lignes de la matrice M. □

PDOL-séries

Les PDOL-séries sont des DOL-séries pariculières que l'on peut définir de façon suivante. Une série r est une *PDOL-série*, s'il existe une représentation linéaire (l, M, c) de r à coefficients dans $\mathbb{N}$, telle que

$$\forall n \geq 0 \qquad r_n = lM^n c,$$

où c est un vecteur colonne ne comportant que des 1 et M une matrice dont aucune ligne n'est entièrement nulle.

On rappelle une caractérisation de ces séries ([SS78] Théorème 7.5 p.102) : une série $\mathbb{N}$-rationnelle r en une variable est une PDOL-série non nulle si, et seulement si, $r(0) > 0$ et la série $\sum_{n\geq 0}(r_{n+1} - r_n)z^n$ est $\mathbb{N}$-rationnelle.

Proposition 31 *Soit $\alpha(z) = \sum_{n\geq 1} \alpha_n z^n$ une série $\mathbb{N}$-rationnelle, telle que*

$$\exists k \in \mathbb{N}^*, \qquad \alpha(\frac{1}{k}) < 1.$$

Alors la série

$$\beta(z) = \sum_{n\geq 0} \beta_n z^n = \frac{1 - \alpha(z)}{1 - kz}$$

est

- une PDOL-série et $\beta_0 = 1$,

- la série génératrice d'un arbre rationnel dont tout nœud a au moins un fils.

Démonstration : D'après l'étude qui vient d'être faite, comme $\alpha(1/k) < 1$, la série β est une DOL-série et a pour racine dominante (et simple) k. Par suite, elle admet une représentation linéaire (l, M, c) où $l \in \mathbb{N}^{1\times m}$, $M \in \mathbb{N}^{m\times m}$ et $c \in 1^{m\times 1}$, telle que

$$\forall n \geq 0 \qquad \beta_n = lM^n c$$

et où la matrice M a pour rayon spectral k.

Comme, de plus, $\beta_0 = 1$ et que, pour tout entier n, $\beta_{n+1} \leq k\beta_n$, on obtient

$$\beta_n \sim_\infty bk^n,$$

où b est un entier algébrique positif inférieur ou égal à 1.

On montre maintenant que la série $\sum_{n\geq 0}(\beta_{n+1} - \beta_n)z^n$ est $\mathbb{N}$-rationnelle. On a

$$\beta_{n+1} - \beta_n = (k-1)\beta_n - \alpha_n.$$

Comme la série α a pour rayon de convergence $1/\lambda$, que β a pour rayon de convergence $1/k$ et que $k > \lambda$, asymptotiquement,

$$\beta_{n+1} - \beta_n \sim_\infty (k-1)bk^n \geq 0.$$

Les coefficients de la série $\sum_{n\geq 0}(\beta_{n+1} - \beta_n)z^n$ sont donc positifs. De plus,

$$\sum_{n\geq 0}(\beta_{n+1} - \beta_n)z^n = \sum_{n\geq 0}((k-1)\beta_n - \alpha_n) = \frac{k(z-1)\alpha(z) + k - 1}{1 - kz},$$

la série est, par suite, $\mathbb{Z}$-rationnelle et a pour racine dominante k puisque $\alpha(1/k) < 1$. On a ainsi montré que la série $\sum_{n\geq 0}(\beta_{n+1} - \beta_n)z^n$ est $\mathbb{N}$-rationnelle. Comme, par définition, $\beta_0 = 1$, on en conclut que β est une PDOL-série.

La série β étant une PDOL-série, il existe une représentation linéaire (l, M, c) de β, où c est un vecteur colonne dont toutes les composantes sont égales à 1 et M est une matrice dont aucune ligne n'est nulle. L'interprétation en termes d'arbres de ce résultat permet alors de conclure la preuve. □

Remarque 20 On peut remarquer également que si α n'est pas un polynôme, la matrice M d'une représentation linéaire de β est nécessairement réductible. En effet, l'inégalité, valide après un éventuel décalage,

$$Mc \leq kc$$

où le vecteur-colonne c a toutes ses composantes égales à 1, implique que

$$\forall j \quad \sum_{i=1}^{n} m_{ij} \leq k.$$

Comme, d'après le Théorème 4 (p.21),

$$\min_j \sum_{i=1}^{n} m_{ij} \leq k \leq \max_j \sum_{i=1}^{n} m_{ij},$$

et que M est irréductible, l'égalité ne peut être atteinte à gauche ou à droite que si toutes les lignes de la matrice M ont même somme. On en déduit, dans ce cas, que $\forall j, \quad \sum_{i=1}^{n} m_{ij} = k$. Ce cas de figure correspond à des arbres dont tous les nœuds internes, à partir d'une certaine hauteur, ont exactement k fils. Le code préfixe alors associé est nécessairement fini.

3.3 Arbres rationnels k-aires

D'après la Proposition 30 (p.146), on peut construire un arbre rationnel dont la série génératrice des nœuds internes est

$$\beta(z) = \frac{(1-\alpha(z))}{(1-kz)}.$$

On cherche maintenant à construire un arbre rationnel ayant les mêmes propriétés mais dont l'arité soit bornée par k.

Si le rayon de convergence de la série β est strictement supérieur à $1/k$ et que la matrice de sa représentation linéaire peut être choisie primitive, on construit un code préfixe sur un alphabet à k lettres tel que la série génératrice des mots n'ayant pas de préfixe dans ce code soit β.

Théorème 27 *Soit $\alpha(a) = \sum_{n\geq 1} \alpha_n z^n$ une série $\mathbb{N}$-rationnelle telle que*

- *$\exists k \in \mathbb{N}^*$, tel que $\alpha(1/k) = 1$*

- *La série*

$$\beta(z) = \frac{1-\alpha(z)}{1-kz}$$

a une représentation linéaire (l, M, c) à coefficients entiers positifs où la matrice M est primitive et $c = (1, \ldots, 1)^t$.

Dans ces conditions, on peut construire un code rationnel préfixe et complet sur un alphabet à k lettres ayant $(\alpha_n)_{n\geq 1}$ comme distribution de longueurs.

Construction

Soit

$$\beta(z) = \sum_n \beta_n z^n$$

la série $\mathbb{N}$-rationnelle définie par

$$\beta(z) = \frac{(1-\alpha(z))}{1-kz}.$$

Dans ce qui suit, on montre que β est la série génératrice des nœuds internes d'un arbre d'arité au plus k. Par définition même de β, la série α est alors la série génératrice des feuilles de l'arbre complété T, ce qui prouve que α est la série génératrice d'un code rationnel préfixe et complet sur un alphabet à k lettres : code dont T est la représentation littérale. La construction que l'on donne repose essentiellement sur un résultat (Proposition 32 p.152) établi par Perrin ([Per89]).

Soit (l, M, c) une représentation linéaire de β à coefficients dans $\mathbb{N}$, telle que

$$\forall n \geq 0 \qquad \beta_n = lM^n c,$$

où M est une matrice primitive de rayon spectral $\lambda < k$ et c est un vecteur colonne ne comportant que des 1. En utilisant le Théorème 7 (p.25), on obtient, pour tous i et j,

$$\frac{(M^{n+1})_{ij}}{k^{n+1}} - \frac{(M^n)_{ij}}{k^n} = \left(\frac{\lambda}{k}\right)^n \left(\left(\frac{\lambda}{k} - 1\right) v_i w_j + \left(\frac{\lambda}{k}\rho_{ij}(n+1) - \rho_{ij}(n)\right)\right).$$

Comme $\rho_{ij}(n) \to 0$ quand $n \to \infty$ et que $\lambda < k$, on en déduit que, pour tout entier n suffisamment grand,

$$\frac{M^{n+1}}{k^{n+1}} - \frac{M^n}{k^n} < 0.$$

On a alors l'inégalité

$$\forall n \geq n_0, \qquad M^{n+1}c < kM^n c.$$

On effectue le décalage d'indices suivant

$$\forall n \geq 0, \quad \beta_{n+n_0} = lM^n C \quad \text{où} \quad C = M^{n_0} c.$$

On donne dans ce qui suit une construction des β_{n_0} branches de l'arbre ayant pour origine un nœud de hauteur n_0, la partie de l'arbre constituée des chemins de la racine aux nœuds de hauteur n_0 pouvant être construite à la main.

Comme la matrice M est primitive, toutes les composantes de C sont strictement positives. On peut, de plus, choisir K minimal, *i.e.*, $K - 1 < \lambda \leq K$, puisque la série α est de toute façon obtenue en complétant l'arbre obtenu de sorte que tous les nœuds internes aient k fils. Dans ces conditions, on a

$$(K-1)C \leq MC \leq KC.$$

Il reste à montrer que l'on peut remplacer le triplet (l, M, C) par un triplet (l', M', C') tel que la matrice M' ait la somme des coefficients de chacune de ses lignes majorée par K et le vecteur colonne C' ait toutes ses composantes égales à 1. Quitte à augmenter la taille de la matrice M, on peut la supposer à coefficients dans $\{0, 1\}$.

La construction de cette nouvelle représentation linéaire est due à Perrin ([Per89]) et utilise essentiellement la technique d'éclatement d'états ([ACH83] et [Mar85]).

Proposition 32 *Soit M une matrice irréductible de taille m à coefficients dans $\{0,1\}$. Soient K un entier positif et $C \in \mathbb{N}^{m\times 1}$ un vecteur colonne, tels que*

$$(K-1)C \leq MC \leq KC.$$

Alors il existe deux matrices $R \in \mathbb{N}^{l\times m}$ et $S \in \mathbb{N}^{m\times l}$ telles que

1. *$M = SR$*
2. *$C = SC'$ où $C' \in \mathbb{N}^{l\times 1}$ a toutes ses composantes égales entre elles.*
3. *la matrice $M' = RS$ satisfait l'inégalité*

$$M'C' \leq KC'$$

4. *S est inversible à droite.*

Remarque 21 On a supprimé par rapport à l'énoncé l'initial l'hypothèse de primitivité de la matrice M qui n'est pas nécessaire pour établir ce résultat.

La preuve de cette proposition nécessite le lemme suivant.

Lemme 12 *Soient $k_1, k_2, \ldots, k_n$ des entiers strictement positifs. Alors, il existe une partie I de $\{1,2,\ldots,n\}$ telle $\sum_{i\in I} k_i$ soit divisible par n.*

Démonstration : On considère les n sommes partielles $k_1, k_1+k_2, \ldots, k_1+k_2+\ldots+k_n$. Deux cas peuvent se produire :

- soit ces sommes sont toutes distinctes modulo n, l'une d'elles est alors nécessairement congrue à 0 modulo n,
- soit deux d'entre elles sont congrues modulo n. Dans ce cas, il existe des entiers n_1 et n_2 tels que

$$1 \leq n_1 < n_2 \leq n, \qquad \sum_{i=1}^{n_1} k_i \equiv \sum_{i=1}^{n_2} k_i \bmod n.$$

Par suite,

$$\sum_{n_1}^{n_2} k_i \equiv 0 \bmod n,$$

ce qui prouve le résultat annoncé. □

Démonstration : (de la Proposition 32) La méthode consiste à itérer la transformation suivante de la matrice M. On choisit une ligne i de la matrice M telle que C_i soit maximal

et que, pour au moins un indice j, on ait $M_{ij} = 1$ et $C_j < C_i$, ce qui est possible car la matrice est irréductible. Soit J l'ensemble des indices j, tels que $M_{ij} = 1$. Comme

$$(K-1)C_i \leq \sum_{j\in J} C_j.$$

Alors Card$J \geq K$.

On distingue alors deux cas qui découlent du Lemme 12.

<u>1^{er} *cas*</u>

$$\exists J' \subset J \quad \text{et} \quad J' \neq J \quad \text{tel que} \quad \sum_{j\in J'} C_j \equiv 0 \bmod K.$$

On définit alors les matrices $R \in \mathbb{N}^{l\times m}$ et $S \in \mathbb{N}^{m\times l}$, où $l = m+1$ par

$$S = \left(\begin{array}{ccc|c} & & & O^{(i-1)\times(l-i)} \\ & Id_i & & \\ \hline -- & -- & -- & -- \quad -- \quad -- \\ \hline & & & Id_{l-i} \\ & O^{(m-i)\times i} & & \end{array}\right) \quad \text{et} \quad R = \left(\begin{array}{c} M_1 \\ \vdots \\ M_{i-1} \\ R_i \\ R_{i+1} \\ M_{i+1} \\ \vdots \\ M_m \end{array}\right)$$

où M_j est la $j$ième ligne de la matrice M,

$$R_{ij} = \left\{\begin{array}{ll} 1 & \text{pour} \quad j \in J' \\ 0 & \text{sinon} \end{array}\right. \qquad \text{et} \qquad R_{(i+1)j} = \left\{\begin{array}{ll} 1 & \text{pour} \quad j \in J \setminus J' \\ 0 & \text{sinon} \end{array}\right.$$

Par suite, la $i$ème ligne de la matrice M satisfait l'égalité $M_i = R_i + R_{i+1}$ de sorte que $M = SR$. On définit $C' \in \mathbb{N}^{l\times 1}$ tel que $C = SC'$ en posant

$$C'_i = \frac{1}{K}\sum_{j\in J'} C_j, \qquad C'_{i+1} = C_i - C'_i.$$

On a alors l'inégalité

$$M'C' \leq KC'.$$

<u>$2^{ème}$ *cas*</u> L'autre cas de figure est celui où Card $J = K$ et $\sum_{j\in J} C_j \equiv 0 \bmod K$.

Comme $\sum_{j\in J} C_j < KC_i$ et que les membres de l'inégalité sont multiples de K, on obtient

$$\sum_{j\in J} C_j \leq K(C_i - 1). \tag{3.1}$$

On se ramène alors au cas précédent en introduisant une partition (J', J'') de J, la seule modification est le calcul de C'_{i+1} qui est alors égal à la partie entière par excès

de $\sum_{j\in J'} C_j/K$. D'après (3.1), C'_{i+1} est strictement positif et le vecteur C' ainsi défini vérifie l'inégalité

$$M'C' \leq KC'.$$

Cette transformation est itérée jusqu'à ce que le vecteur C' ait toutes ses composantes égales. Par construction, la somme de celles-ci est invariante par la transformation que l'on vient de décrire, ce qui assure que le résultat annoncé sera obtenu au bout d'un nombre fini d'éclatements d'états. Enfin, les transformations successives se composent sans difficulté. Si

$$M = SR, \quad C = SC', M' = RS = S'R', \quad C' = S'C'',$$

on obtient, en notant S^{-1} l'inverse à droite de S

$$M = SR = SM'S^{-1} = (SS')R'S^{-1} \qquad \text{et} \qquad C = (SS')C'',$$

ce qui conclut la preuve de la Proposition 32. □

On obtient alors une nouvelle représentation (L', M', C') où $L' = lS$. Si

$$C' = c_0(1, \ldots, 1)^t, \quad \text{où} \quad c_0 \in \mathbb{N}^*,$$

on construit une nouvelle représentation dont le vecteur colonne a toutes ses composantes égales à 1 en remplaçant le vecteur-ligne L' par le vecteur-ligne c_0L'. La somme des composantes c_0L' est alors β_{n_0}.

On a ainsi construit une représentation linéaire de la série β dont l'interprétation montre que β est la série génératrice des nœuds internes d'un arbre rationnel d'arité au plus k. La série α est, par suite, la série génératrice des feuilles de l'arbre complet associé. En d'autre termes, la série α est la série génératrice d'un code rationnel préfixe et complet sur un alphabet à k lettres.

La construction d'un arbre rationnel même dans le cas irréductible reste un problème entièrement ouvert. De plus, aucun résultat n'est connu dans le cas des codes préfixes rationnels qui ne sont pas maximaux.

Bibliographie

[ACH83] R. L. Adler, D. Coppersmith, and M. Hassner. Algorithms for sliding block codes. *I.E.E.E. Trans. Inform. Theory*, IT-29:5–22, 1983.

[AFM96] D. Arquès, Jean-Paul Fallot, and Christian Michel. An evolutionnary model of a complementary circular code. *J. of Theoret. Biology*, 1996. sous presse.

[AM95] D. Arquès and Christian Michel. A possible code in the genetic code. In E. W. Mayr and C. Puech, editors, *STACS 95*, volume 900 of *Lect. Notes in Comput. Sci.*, pages 640–651. Springer, 1995.

[AM96] D. Arquès and Christian Michel. A complementary circular code in the protein coding genes. *J. of Theoret. Biology*, 182:45–58, 1996.

[Bas96] F. Bassino. Star-height of an $\mathbb{N}$-rational series. In C. Puech and R. Reischuk, editors, *STACS 96*, volume 1046 of *Lect. Notes in Comput. Sci.*, pages 125–135. Springer, 1996.

[Bas97] F. Bassino. Nonnegative companion matrices and star-height of $\mathbb{N}$-rational series. *Theoret. Comput. Sci.*, 1997. (à paraître).

[Béa93] M.-P. Béal. *Codage symbolique*. Masson, 1993.

[Ber71] J. Berstel. Sur les pôles et le quotient d'Hadamard des séries $\mathbb{N}$-rationnelles. *C. R. A. S. Paris, Série A*, pages 1079–1081, 1971.

[BH91] M. Boyle and D. Handelman. The spectra of nonnegative matrices via symbolic dynamics. *Annals of Math.*, 133:249–316, 1991.

[BL96] V. Bruyère and M. Latteux. Variable-length maximal codes. In F. Meyer auf der Heide and B. Monien, editors, *ICALP 96*, volume 1099 of *Lect. Notes in Comput. Sci.*, pages 24–47. Springer, 1996.

[BM75] J. Berstel and M. Mignotte. Deux propriétés décidables des suites récurrentes linéaires. *Séminaire d'Informatique, Univ. Louis Pasteur, Strasbourg*, 1975.

[Boy94] M. Boyle. Symbolic dynamics and matrices. In R. Brualdi S. Friedland and V. Klee, editors, *Combinatorial and Graph-Theoretic Problems in Linear Algebra*, volume 50 of *IMA Volumes in Mathematics and Its Applications*. Springer-Verlag, 1994.

[BP79] A. Berman and R. Plemmons. *Nonnegative matrices in mathematical sciences*. Academic Press, 1979.

[BP85] J. Berstel and D. Perrin. *Theory of codes*. Pure and Applied Mathematics. Academic Press, Inc., 1985.

[BR82] J. Berstel and C. Reutenauer. Recognizable formal power series on trees. *Theoret. Comput. Sci.*, 18:115–148, 1982.

[BR88] J. Berstel and C. Reutenauer. *Rational series and their languages*. Springer-Verlag, Berlin, 1988.

[CG74] L. Carter and J. Gill. Conjectures on uniquely decipherable codes. *IEEE Trans. on Inform. Theory*, 20:394–396, 1974.

[CGO57] H.C. Crick, J.S. Griffith, and L.E. Orgel. Codes without commas. In *Nat. Acad. Sci.*, volume 43, pages 416–421, 1957.

[Con71] J. H. Conway. *Regular algebra and finite machine*. Chapman and Hall, London, 1971.

[Cor75] R. Cori. *Un code pour les graphes planaires et ses applications*, volume 27 of *Astérisque*. Société Mathématique de France, Paris, 1975.

[Cot80] N. Cot. *Combinatoire des arbres t-aires dont les branches ont des coûts positifs quelconques*. Thèse d'Etat, Paris VI, 1980.

[CP71] J. W. Carlyle and A. Paz. Realizations by stochastic finite automaton. *J. Comput. System Sci.*, 5:26–40, 1971.

[CS63] N. Chomsky and M.P. Schützenberger. The algebraic theory of context-free languages. In P. Braffort and D. Hirschberg, editors, *Computer programming and formal systems*, pages 118–161. North-Holland, 1963.

[Csi69] I. Csiszar. Simple proofs of some theorems on noiseless channels. *Inform. and Control*, 14:185–198, 1969.

[DS66] F. Dejean and M. P. Schützenberger. On a question of Eggan. *Inform. and Control*, 9:23–25, 1966.

[DT88] G. Duchamp and J.-Y. Thibon. Bisections reconnaissables. *RAIRO Inform. Theor. Appl.*, 22:113–128, 1988.

[Egg63] L. C. Eggan. Transition graphs and star height of regular events. *Michigan Math. J.*, 10:385–397, 1963.

[Eil74] S. Eilenberg. *Automata, Languages and Machines*, volume A. Academic Press, New-York, 1974.

[ER85] A. Ehrenfeucht and G. Rozenberg. Each regular code is included in a regular maximal code. *RAIRO Inform. Theor. Appl.*, 20:89–96, 1985.

[Fat04] P. Fatou. Sur les séries entières à coefficients entiers. *C. R. A. S. Paris, Groupe A*, 138:342–344, 1904.

[Fli74] M. Fliess. Matrices de Hankel. *J. Math. Pures Appl.*, 53:197–222, 1974. erratum 54(1965).

[Fli75] M. Fliess. Séries rationnelles positives et processus stochastiques. *Annales Institut H. Poincaré, Sect. B*, 11(2):1–21, 1975.

[Fli81] M. Fliess. Fonctionnelles causales non linéaires et indéterminées non commutatives. *Bull. Soc. Math. France*, 109:3–40, 1981.

[Fro12] G. Frobenius. Über matrizen aus nicht negativen elementen. *Sitz. der Preuss. Akad der Wiss., Berlin*, pages 456–477, 1912.

[FS83] P. Flajolet and J.M. Steyaert. Patterns and pattern-matching in trees : an analysis. *Inform. and Control*, 58:19–58, 1983.

[Gan59] F.R. Gantmacher. *The theory of matrices*. Chelsea, New-York, 1959.

[GG65] S. W. Golomb and B. Gordon. Codes with bounded synchronisation delay. *Inform. and Control*, 8:355–372, 1965.

[GGW58] S. W. Golomb, B. Gordon, and L. R. Welch. Comma-free codes. *Canadian J. Math.*, 10:202–209, 1958.

[Han81] D.E. Handelman. Positive matrices and dimension groups affiliated to $\mathbb{C}^\star$-algebras and topological Markov chains. *J.Operator Theory*, 6:55–74, 1981.

[Han85] D.E. Handelman. Positive polynomials and product type action of compact groups. *Memoirs of the A.M.S.*, 54(320), 1985.

[Han92] D.E. Handelman. Spectral radii of primitive integral companion matrices and log-concave polynomials. In Peter Walters, editor, *Symbolic Dynamic and its Applications*, volume 135 of *Contempory Mathematics*, pages 231–238. A.M.S., 1992.

[Has79] K. Hashiguchi. A decision procedure for the order of regular events. *Theoret.Comput.Sci*, 8:69–72, 1979.

[Has82] K. Hashiguchi. Regular languages of star height one. *Inform. and Control*, 53:199–210, 1982.

[Has88] K. Hashiguchi. Algorithms for determining relative star height and star height. *Inform. and Computation*, 78:124–169, 1988.

[Has89] K. Hashiguchi. Relative star-height, star-height and finite automata with distance functions. In J.-E. Pin, editor, *Formal properties of finite automata and applications*, volume 386 of *Lect. Notes in Comput. Sci.*, pages 74–88. Springer, 1989.

[Huf52] D. A. Huffman. A method for the construction of minimal redundancy codes. *Proc. IRE*, 40:1098–1101, 1952.

[Kar61] R. M. Karp. Minimum-redundancy coding for the discret noiseless channels. *IRE Trans. Inform. Theory*, IT-17(1):27–38, 1961.

[Kle56] S. C. Kleene. Representation of events in nerve nets and finite automata. In C. Shannon and J. McCarthy, editors, *Automata Studies*, pages 3–41. Princeton Univ. Press, Princeton, NJ, 1956.

[KOE78] T. Katayama, M. Okamoto, and H. Enomoto. Characterization of the structure-generating functions of regular sets and DOL growth functions. *Inform. and Control*, 36:85–101, 1978.

[Kra62] R. M. Krause. Channels which transmit letters of unequal duration. *Inform. and Control*, 5:13–24, 1962.

[Kro87] D. Krob. Codes limités et factorisations finies du monoïde libre. *RAIRO Inform. Theor. Appl.*, 21:437–467, 1987.

[Kro91a] D. Krob. Complete systems of $\mathbb{B}$-rational identities. *Theoret. Comput. Sci.*, 89:207–343, 1991.

[Kro91b] D. Krob. Expressions k-rationnelles sur un anneau. In M.-P. Malliavin, editor, *Topics in invariant theory*, volume 1478 of *Lect. Notes in Math.*, pages 215–243. Springer-Verlag, 1991.

[Kro92] D. Krob. Differentiation of k-rational expressions. *Int. Journ. of Alg. and Comput.*, 2:57–87, 1992.

[Lin68] A. Lindenmayer. Mathematicals models for cellular interaction in development, i and ii. *J. Theor. Biol.*, 18:280–315, 1968.

[Lin84] D. Lind. The entropies of topological Markov shifts and a related class of algebraic integers. *Ergod. Th. and Dynam. Syst.*, 4:283–300, 1984.

[LM95] D. Lind and B. Marcus. *An introduction to symbolic dynamics and coding.* Cambridge, 1995.

[Lon76] G. Longo. A noiseless coding theorem for sources having utilities. *SIAM J. Appl. Math.*, 30(4), 1976.

[Lot83] M. Lothaire. *Combinatorics on Words*, volume 17 of *Encyclopedia of Mathematics and its Applications.* Addison-Wesley, 1983.

[Luc91] E. Lucas. *Théorie des nombres.* Gauthier-Villars, Paris, 1891.

[Mar85] B. Marcus. Sofic systems and encoding data. *I.E.E.E. Trans. Inform. Theory*, IT-31:366–377, 1985.

[McM56] B. McMillan. Two inequalities implied by unique decipherability. *IRE Trans Inform. Theory*, IT-2:115–116, 1956.

[McN67] R. McNaughton. The loop complexity of pure-group events. *Inform. and Control*, 11:167–176, 1967.

[Min88] H. Minc. *Nonnegative matrices.* Wiley Inter-Sciences, 1988.

[Per07] O. Perron. Zur theorie der matrizen. *Math. Ann.*, 64:248–263, 1907.

[Per89] D. Perrin. Arbres et séries rationnelles. *C. R. A. S. Paris, Série I*, 309:713–716, 1989.

[Per90] D. Perrin. Finite automata. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B, chapter 1, pages 1–57. North Holland, 1990.

[Per92] D. Perrin. On positive matrices. *Theoret.Comput.Sci*, 94:357–366, 1992.

[Pin95] J.-E. Pin. Tropical semiring. Technical Report 95/40, LITP, Sept 1995.

[Poi83] H. Poincaré. Sur les équations algébriques. *C. R. A. S. Paris*, 97:1418–1419, 1883.

[Reu80] C. Reutenauer. Séries formelles et algèbres syntactiques. *J. Algebra*, 66:448–483, 1980.

[Reu96] C. Reutenauer. Inversion height in free fields. *Selecta Mathematica, New Series*, 2(1):1–18, 1996.

[RS80] G. Rozenberg and A. Soittola. *The mathematical theory of L-systems.* Academic Press, 1980.

[Sal90] A. Salomaa. Formal languages and power series. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B, chapter 3, pages 104–132. North Holland, 1990.

[Sch56] M.P. Schützenberger. *Une théorie algébrique du codage.* Séminaire Dubreuil-Pisot, Institut H. Poincaré,Paris, 1955-1956. Exposé n^0 15.

[Sch59] M.P. Schützenberger. *Sur une propriété combinatoire des algèbres de Lie libres pouvant être utilisée dans un problème de mathématiques appliquées.* Séminaire Dubreuil-Pisot, Institut H. Poincaré,Paris, 1958-1959.

[Sch61] M.P. Schützenberger. On the definition of a family of automata. *Inform. and Contr.*, 4:245–270, 1961.

[Sch65a] M. P. Schützenberger. On a factorization of free monoids. *Proc. Amer. Math. Soc.*, 16:21–24, 1965.

[Sch65b] M. P. Schützenberger. Sur une question concernant certains sous-monoïdes libres. *C. R. A. S. Paris, Groupe 1*, 261:2419–2420, 1965.

[Sha48] C. Shannon. A mathematical theory of communication. *Bell Sys. Tech. J.*, 27:379–423,623–656, 1948.

[Sim78] I. Simon. Limited subsets of a free monoid. In *19th Annual IEEE Symposium on Foundation of Computer Science*, pages 143–150, 1978.

[Soi76] M. Soittola. Positive rational sequences. *Theoret.Comput.Sci*, 2:317–322, 1976.

[SS78] A. Salomaa and M. Soittola. *Automata-theoretic aspect of formal power series.* Springer-Verlag, Berlin, 1978.

[Sta86] R. P. Stanley. *Enumerative Combinatorics*, volume I. Wadsworth & Brooks/Cole, 1986.

[Sta89] R.P. Stanley. Log-concave and unimodal sequences in algebra, combinatorics and geometry. In *Graph theory and its applications: East and West*, number 576 in Annals of the New-York Academy of Sciences, pages 500–535. 1989.

[Vie74] G. Viennot. *Algèbres de Lie libres et monoïdes libres.* Thèse d'Etat, Université Paris VII, 1974.

[Vie78] G. Viennot. *Algèbres de Lie libres et monoïdes libres.* Number 691 in Lect. Notes in Math. Springer-Verlag, 1978.

Index

Table des figures