Série N et Z-rationnelles

Sary Drappeau

19 décembre 2007

1 Séries rationnelles

On pourra consulter [1] pour tout ce qui concerne les notions introduites.

Le livre de Salomaa et Soittola [2] fait plus de choses en lien avec les automates pondérés finis.

1.1 Définitions

On veut d'une certaine manière généraliser la notion de langage. Étant donné un alphabet A, on peut voir un langage L sur A comme une application de A^* dans le monoïde booléen $\mathbb{B}$ (défini par $1+1=1$). On attribue 1 aux mots de L et 0 aux autres :

$$L = \sum_{w \in L} w$$

On peut étendre ce concept à partir de la notion de série formelle. Il nous faut d'abord quelques définition.

Définition 1. Un *semi-anneau* K est un ensemble muni de deux lois $+$ et $\cdot$ telles que :

- $(K, +)$ est un monoïde commutatif d'élément neutre 0
- $(K, \cdot)$ est un monoïde d'élément neutre 1
- $\cdot$ est distributive par rapport à $+$
- $\forall x \in K, 0x = x0 = 0$

On définit de même manière que pour les anneaux classiques les notions de *semi-anneau commutatif*, *sous-semi-anneau*, et *morphisme de semi-anneau*

On se fixe un alphabet A et un semi-anneau K. K sera toujours considéré commutatif.

Définition 2. Une *série formelle* S est une fonction $S : A^* \longmapsto K$

L'image par S d'un mot w, notée (S, w), est appellée *coefficient* de w dans S.

On appelle *support* de S le langage

$$\mathrm{supp}(S) = \{w \in A^* \mid (S, w) \neq 0\}$$

L'ensemble des séries formelles sur K est noté $K\langle\langle A\rangle\rangle$. On y définit une structure de semi-module par les relations naturelles suivantes :

$$(S+T,w) = (S,w) + (T,w)$$

$$(ST,w) = \sum_{xy=w} (S,x)(T,y)$$

et par la multiplication externe : pour $a \in K$,

$$(kS,w) = k(S,w)$$

Un *polynôme* P est une série à support fini. Son *degré* est l'entier $\max\{|w|, w \in \text{supp}(P)\}$. Leur ensemble est noté $K\langle A\rangle$.

On injecte de façon naturelle A^* et K dans $K\langle\langle A\rangle\rangle$.

Dans le cas où A est réduit à un élément x, on obtient les séries formelles usuelles $K[[x]]$, et les polynômes $K[x]$.

Définition 3. On munit $K\langle\langle A\rangle\rangle = K^{A^*}$ de la topologie produit, ce qui en fait un semi-anneau topologique.

On définit pour une série S vérifiant $(S,1) = 0$ (série *quasi-inversible*) l'opération *étoile* : $S \mapsto S^*$ par

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

La *clôture rationnelle* d'une partie E de $K\langle\langle A\rangle\rangle$ est la plus petite partie contenant E, stable par addition, multiplication, multiplication externe, et par l'opération étoile.

Une série est dite *rationnelle* si elle est dans la clôture rationnelle de $K\langle A\rangle$.

L'ensemble des séries rationnelles est noté $K^{\text{RAT}}\langle\langle A\rangle\rangle$.

On a alors l'analogue du lemme d'Arden :

Lemme 4. *Si A et B sont deux série formelles, avec B quasi-inversible, alors l'unique solution du système $S = A + SB$ (resp. $S = A + BS$) est la série $S = AB^*$ (resp. $S = B^*A$).*

Démonstration. Comme B est quasi-inversible, on a :

$$lim_{n\to\infty} B^n = 0$$

$$lim_{n\to\infty} \sum_{k=0}^{n} B^k = B^*$$

Il suffit alors d'itérer la relation et de passer à la limite. □

Dans le cas des langages on avait fait le lien entre langage rationnel, langage reconnu par un automate et langage reconnu par un morphisme de monoïde. On peut procéder de manière similaire pour les séries formelles.

On donne d'abord les définitions utiles, puis on fera le lien entre elles.

Définition 5. Une série formelle S est dite *reconnaissable* s'il existe $n \geq 1$, un morphisme de monoïdes $\mu : A^* \longmapsto (\mathcal{M}_n(K), \cdot)$, un vecteur ligne λ et un vecteur colonne γ, à coefficients dans K, tels que pour tout w dans A^* :

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

(λ, μ, γ) est appellée *représentation* de S.
L'ensemble des séries reconnaissables est noté $K^{\mathrm{REC}}\langle\langle A \rangle\rangle$.

Définition 6. Un *automate pondéré fini* à poids dans K est un quadruplet $\mathcal{A} = (Q, I, E, F)$ où :
- Q est *l'ensemble des états* : c'est un ensemble fini
- I et F sont des applications de Q dans K
- E est une application de $Q \times A \times Q$ dans K

La *série reconnue* par $\mathcal{A}$ est la série définie par :

$$(S, w) = \sum_{\substack{w=a_1 \dots a_n \\ (q_0 \dots q_n)}} I(q_0)E(q_0, a_1, q_1) \dots E(q_{n-1}, a_n, a_n)F(q_n)$$

Où la somme est prise sur chaque mot w et sur chaque $(q_0, \dots, q_n)$ de Q^{n+1}.

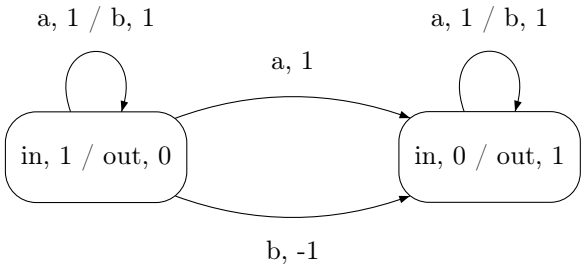
Proposition 7. *Une série formelle S est reconnue par un automate pondéré fini si et seulement si elle est reconnaissable.*

Démonstration. La manière dont ces deux classes d'objets sont définies suffit à montrer l'équivalence des deux définitions. On peut en effet faire correspondre :
- λ et I par : $\lambda_p = I(p)$
- γ et F par : $\gamma_p = F(p)$
- μ et E par : $E(p, a, q) = (\mu(a))_{p,q}$ et

$$\mu(a_1 \dots a_n)_{p,q} = \sum_{q_1, \cdots, q_{n-1}} E(p, a_1, q_1)E(q_1, a_2, q_2) \cdots E(q_{n-1}, a_n, q)$$

□

Par exemple, l'automate suivant :



reconnait la série dans $\mathbb{Z}\langle\langle a, b\rangle\rangle$:

$$S = \sum_w (|w|_a - |w|_b)w$$

Cette série admet la représentation (λ, μ, γ) avec :

$$\lambda = \begin{pmatrix}1 & 0\end{pmatrix} \quad \mu(a) = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \quad \mu(b) = \begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix} \quad \gamma = \begin{pmatrix}0\\ 1\end{pmatrix}$$

On voudrait bien montrer l'équivalence entre série rationnelle et série reconnaissable. On va préalablement montrer un résultat très utile qui caractérise les série reconnaissable par des notions d'algèbre générale.

Définition 8. Si $x \in A^*$ et $S \in K\langle\langle A\rangle\rangle$, alors on pose :

$$x^{-1}S = \sum_{w \in A^*} (S, xw)w$$

On dit qu'un sous-module M du monoïde additif K est *stable* si pour tout $x \in A^*$ et $S \in M$ on a $x^{-1}S \in M$.

On caractérise ensuite les langages reconnaissables : c'est le point central.

Proposition 9. *Une série formelle S de $K\langle\langle A\rangle\rangle$ est reconnaissable si et seulement si il existe un K-sous-module de $K\langle\langle A\rangle\rangle$ généré par une partie finie (*de type fini*), qui contient S.*

Démonstration. Supposons que S est reconnaissable : soit (λ, μ, γ) une représentation de S en dimension n. Alors on va pouvoir décomposer S suivant ses composantes. On définit $(S_i)_{i=0\dots n}$, des éléments de $K\langle\langle A\rangle\rangle$ par :

$$(S_i, w) = (\mu(w)\gamma)_i$$

On note M le sous-module sur K engendré par les S_i. Alors :

$$(S, w) = \sum_i \lambda_i(\mu(w)\gamma)_i = \sum_i \lambda_i(S_i, w)$$

Ce qui montre $S \in M$. Il reste à montrer la stabilité au sens introduit ci-haut.

Soit $x \in A^*$:

$$(x^{-1}S_i, w) = (S_i, xw) = (\mu(x)\mu(w)\gamma)_i = \sum_j \mu(x)_{i,j}(S_j, w) \in M$$

On en déduit, avec le fait que $x^{-1}(S + T) = x^{-1}S + x^{-1}T$, qu'on a bien la stabilité.

Réciproquement, soit M un sous-module engendré par $S_1, \dots S_n$ qui contient S. On pose plus précisément $S = \sum_i \lambda_i S_i$

Pose alors, pour tout x dans A^*, $\mu(x)$ la matrice $n \times n$ définie comme suit :

$$x^{-1}S_i = \sum_j \mu(x)_{i,j} S_j$$

Cette définition est inspirée du sens direct. On vérifie alors facilement que μ est un morphisme de monoïdes $(A^*, \cdot) \mapsto (\mathcal{M}_n, \cdot)$.

En posant ensuite γ le vecteur ligne tel que $\gamma_i = (S_i, 1)$ on obtient

$$(S_i, w) = (w^{-1}S_i, 1) = \sum_j \mu(w)_{i,j}\gamma_j = (\mu(w)\gamma)_i$$

D'où :

$$(S, w) = \sum_i \lambda_i (S_i, w) = \sum_i \lambda_i (\mu(w)\gamma)_i = \lambda\mu(w)\gamma$$

□

1.2 Le théorème de Schützenberger

On va d'abord énoncer un résultat sur les matrices à coefficients dans $K\langle\langle A\rangle\rangle$.

Lemme 10. *Si m est une matrice à coefficients dans $K\langle\langle A\rangle\rangle$, alors on peut définir $m^* = \sum_{k\geq 0} m^k$*

Dans ce cas, tous les coefficients de m^* sont dans la clôture rationnelle de m (dans $\mathcal{M}_n\langle\langle A\rangle\rangle$)

Démonstration. L'existence de m^* est vérifiée par le même argument que pour les séries formelles, en munissant $\mathcal{M}_n(K)\langle\langle A\rangle\rangle$ de la topologie produit.

On procède alors par récurrence. Le cas $n = 1$ est évident. Pour $n \geq 2$ on réduit la dimension en découpant m et m^* comme suit :

$$m^* = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \quad m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

De la relation $m^* = 1 + mm^*$ on déduit :

$$\begin{aligned} \alpha &= 1 + a\alpha + b\gamma & \beta &= a\beta + b\delta \\ \gamma &= c\alpha + d\gamma & \delta &= 1 + c\beta + d\delta \end{aligned}$$

On peut donc résoudre en utilisant Arden :

$$\begin{aligned} \alpha &= (a + bd^*c)^* & \delta &= (ca^*b + d)^* \\ \beta &= a^*b(ca^*b + d)^* & \gamma &= d^*c(a + bd^*c)^* \end{aligned}$$

D'après l'hypothèse de récurrence, a^* et d^* sont dans la clôture rationnelle des coefficients de a et d, donc de m. On en déduit le résultat. □

Théorème 11 (Schützenberger, 1961)**.** *Une série formelle de $K\langle\langle A\rangle\rangle$ est rationnelle si et seulement si elle est reconnaissable.*

Démonstration. Pour le sens direct, on montre que $K^{\mathrm{REC}}\langle\langle A\rangle\rangle$ contient les polynômes et est stable par les opérations rationnelles.

Soit P un polynôme. On veut stabiliser le sous-module engendré par P. On pose donc $M = \{w^{-1}P, w \in A^*\}$. C'est un ensemble fini car si w est de longueur supérieure au degré de P, alors $w^{-1}P = 0$. Le sous-module qu'il génère est donc de type fini, et stable. Comme $P = 1^{-1}P \in M$, on en déduit que P est reconnaissable.

On se fixe alors S et T deux séries, contenues dans deux sous-modules stables de type fini. $P = MT + N$ est un sous-module de types finis. Il est stable à cause de la relation suivante :

$$\forall a \in A, a^{-1}(ST) = (S, 1)(a^{-1}T) + (a^{-1}S)T$$

Comme P contient ST, on en déduit que ST est reconnaissable.

Ensuite, on suppose S quasi-inversible et on prend $Q = K + MS^*$. C'est un sous-module de type fini, qui contient $1 + SS^* = S^*$. Il est stable par le même argument que dans le cas du produit. Donc S^* est reconnaissable.

Le cas de la somme a déjà été vu : cela conclut le sens direct.

Réciproquement, on suppose que S est reconnaissable. Soit (λ, μ, γ) une représentation en dimension n. On considère le polynôme à coefficients dans $\mathcal{M}_n(K)$:

$$m = \sum_{a \in A} \mu(a)a$$

On peut également voir cet objet comme une matrice à coefficients dans $K\langle A\rangle$. Les deux conceptions sont équivalentes (la somme des matrices est la matrice des sommes).

m est quasi-inversible comme chacun de ses coefficients. On a par récurrence :

$$m^k = \sum_{w \in A^k} \mu(w)w$$

et donc

$$m^* = \sum_{w \in A^*} \mu(w)w$$

Les coefficients de m^* sont, d'après le lemme, dans $K^{\mathrm{RAT}}\langle\langle A\rangle\rangle$. Or on a :

$$S = \sum_{i,j} \lambda_i m^*_{i,j} \gamma_j$$

S est donc rationnelle.

□

2 Le cas de $\mathbb{N}$ et $\mathbb{Z}$

2.1 Caractérisation des langages rationnels

Au prix d'un travail supplémentaire, on peut obtenir le théorème de Kleene à partir de celui de Schützenberger. Je ne présente pas ici la démonstration. Le

lecteur curieux pourra se référer à [1].

La proposition suivante donne la caractérisation du support des séries $\mathbb{N}$-rationnelles.

Proposition 12. *Si L est un langage, on peut lui associer sa* série caractéristique $\underline{L} = \sum_{w \in L} w$

L est un langage rationnel sur A si et seulement si L est le support d'une série rationnelle de $\mathbb{N}\langle\langle A \rangle\rangle$

Démonstration. Si L est reconnu par un automate fini (Q, I, Δ, F), alors on peut faire reconnaitre $\underline{L}$ par un automate pondéré fini (Q, I', E, F') où :

$$I'(p) = \begin{cases} 1 & \text{si } p \in I \\ 0 & \text{sinon} \end{cases} \quad F'(p) = \begin{cases} 1 & \text{si } p \in F \\ 0 & \text{sinon} \end{cases} \quad E(p,a,q) = \begin{cases} 1 & \text{si } (p,a,q) \in \Delta \\ 0 & \text{sinon} \end{cases}$$

Réciproquement, à un automate pondéré $\mathcal{A}_1$ on peut associer un automate fini $\mathcal{A}_2$ qui reconnait son support. Les états initiaux, finaux, et les transitions sont définis exactement de la même façon que pour le sens direct. □

On a alors un résultat intéressant sur un type particulier de séries.

Définition 13. Pour un langage L, on appelle *fonction génératrice* de L la série formelle $\sum_{n \geq 0} |L \cap A^n| X^n$ de $\mathbb{N}\langle\langle X \rangle\rangle$

Proposition 14. *Une série $S = \sum_{n \geq 0} \alpha_n X^n$ de $\mathbb{N}\langle\langle X \rangle\rangle$ est la fonction génératrice d'un langage rationnel si et seulement si elle est $\mathbb{N}$-rationnelle et a pour terme constant $(S, 1) = 0$ ou 1.*

Démonstration. Soit L un langage rationnel. Dans une expression de L, on remplace toutes les occurences des lettres par l'indéterminée X, et on peut interprèter le résultat comme une série rationnelle S à coefficients dans $\mathbb{N}$. On a alors $(S, X^n) = |L \cap A^n|$: chaque fois qu'un mot est dans L, il contribue pour 1 à la valeur du coefficient X^n, où n est sa longueur. La fonction génératrice de L ainsi obtenue est donc bien rationnelle.

Dans l'autre sens, on procède à la transformation inverse. Soit S une série rationnelle à coefficients entiers, alors on prend une expression rationnelle de polynômes qui la définit. On y remplace alors n par $1 + \ldots + 1$, et X^d par $x_{d,1} x_{d,2} \ldots x_{d,d}$ où les $(x_{i,j})_{i \geq j}$ sont des indéterminées. Cela ne pose pas de problème dans la mesure où le mot vide a comme coefficient 0 ou 1, et où un nombre fini de monômes apparaissent dans l'expression. La série sur $\mathbb{N}$ ainsi obtenue est ainsi rationnelle à coefficient 0 ou 1, son support est donc un langage rationnel, et S est précisément la fonction génératrice de ce langage. □

2.2 Et sur les anneaux plus grands ?

Les propriétés vraies pour $K = \mathbb{N}$ ne le sont en général pas pour des semi-anneaux plus gros.

Exemple 15. La série

$$S = \sum_w (|w|_a - |w|_b)w$$

dans $\mathbb{Z}\langle\langle A\rangle\rangle$ est rationnelle, mais son support ne l'est pas.

On peut alors donner des exemples de séries $\mathbb{Z}$-rationnelles mais pas $\mathbb{N}$-rationnelles.

Définition 16. Le *produit d'Hadamard* de deux séries formelles S et T est la série définie par $(S \odot T, w) = (S, w)(T, w)$.

Proposition 17. *Le produit d'Hadamard de deux séries rationnelles est rationnel.*

La démonstration est automatique en utilisant la caractérisation par les sous-monoïdes stables de type fini.

On en déduit en particulier :

Exemple 18. On suppose $A = \{a, b\}$. La série :

$$S = \sum_w (|w|_a - |w|_b)^2 w$$

est dans $\mathbb{Z}^{\mathrm{REC}}\langle\langle A\rangle\rangle$ mais pas dans $\mathbb{N}^{\mathrm{REC}}\langle\langle A\rangle\rangle$

On a en fait :

Proposition 19.

$$\mathbb{Q}_+^{RAT}\langle\langle A\rangle\rangle = \mathbb{N}^{RAT}\langle\langle A\rangle\rangle$$

C'est une proposition que je ne démontrerai pas. Le lecteur patient pourra consulter [1].

Pour terminer, on examine la relation entre $\mathbb{R}$ et $\mathbb{Q}$.

Exemple 20. On suppose $A = \{a, b\}$, et on note $\phi = (1 + \sqrt{5})/2$. La série :

$$S = \sum_w (\phi^{2(|w|_a - |w|_b)} + \phi^{-2(|w|_a - |w|_b)})w$$

est à coefficients dans $\mathbb{N}$. Elle est $\mathbb{R}_+$-rationnelle mais pas $\mathbb{Q}_+$-rationnelle.

Démonstration. On a par récurrence : $\forall n \in \mathbb{N}, \phi^{2n} + \phi^{-2n} \in \mathbb{N}$

Donc S est bien à coefficients dans $\mathbb{Q}_+$.

On peut écrire dans $\mathbb{R}$: $S = (\phi^2 a + \phi^{-2} b)^* + (\phi^{-2} a + \phi^2 b)^*$. S est donc $\mathbb{R}_+$-rationnelle.

Supposons que S soit $\mathbb{Q}_+$-rationnelle. Alors d'après la proposition précédente, S est $\mathbb{N}$-rationnelle. D'après un théorème démontré (difficilement) dans [1], $S^{-1}(k) = \{w \mid (S, w) = k)\}$ est alors un langage rationnel pour tout k dans K. En particulier $S^{-1}(2) = \{w \mid |w|_a = |w|_b\}$ est rationnel, ce qui est absurde. □

La question de savoir si toute série $\mathbb{R}$-rationnelle est $\mathbb{Q}$-rationnelle est par ailleurs toujours ouverte...

Références

[1] J. Berstel and C. Reutenauer. Rational series and their languages. Nouvelle version, non encore publiée.

[2] A. Salomaa and M. Soittola. *Automata, theoretic aspects of formal power series*. Springer-Verlag, 1998.