Journal de Théorie des Nombres
de Bordeaux ***8*** *(1996), 31–45*

Langage de Łukasiewicz et diagonales de séries formelles

par Isabelle FAGNOT

RÉSUMÉ. Dans un corps fini, toute série formelle algébrique en une indéterminée est la diagonale d'une fraction rationnelle en deux indéterminées (Furstenberg 67). Dans cet article, nous donnons une nouvelle preuve de ce résultat, par des méthodes purement combinatoires.

ABSTRACT. In a finite field, every algebraic formal series in one variable is the diagonal of a two-variable rational fraction (Furstenberg 67). In this paper, a new proof of this result is given by combinatorial methods.

Introduction

Furstenberg [Fu] a démontré que,
a) dans un corps K de caractéristique non nulle, toute diagonale d'une série formelle rationnelle en n indéterminées est algébrique sur $K(X)$;
b) réciproquement, dans un corps fini, une série algébrique, en une seule variable, est la diagonale d'une fraction rationnelle en deux variables.

Ce théorème a été étendu, par des méthodes algébriques, au cas de certains corps infinis [De], [DL], [Ha], [SW], (cf. [All2] pour un panorama détaillé). En particulier, Deligne [De], puis Sharif et Woodcock [SW] montrent que la première partie du théorème de Furstenberg reste vraie si on suppose la série algébrique.

Christol, Kamae, Mendès France et Rauzy (voir [CKMR] et [All1]) ont mis en évidence le lien entre l'algébricité des séries formelles en une indéterminée dans un corps fini et les q-automates. A savoir :
Soit q premier. La série formelle $\sum a_i X^i$ dans $\mathbb{F}_q[[X]]$ est algébrique si et seulement si la suite $(a_i)_{i\in\mathbb{N}}$ est q-automatique.
Salon [Sa1] , [Sa2] généralise ce théorème au cas des séries à plusieurs indéterminées et du même coup, redémontre de manière élémentaire le résultat de Deligne dans le cas d'un corps fini. Par ailleurs, Fliess [Fl] a utilisé les séries formelles en variables non commutatives pour démontrer

Manuscrit reçu le 4 octobre 1993.

une variante du cas a) à savoir que dans un corps quelconque, une fraction rationnelle en deux indéterminées a une diagonale algébrique.

Le but de cet article est de donner une preuve combinatoire de la deuxième partie du théorème de Furstenberg :

THÉORÈME.*Soit K un corps fini et soit φ une série formelle algébrique sur $K(X)$. Alors, il existe une fraction rationnelle H en deux variables telle que $\varphi = diag(H)$.*

Pour ce faire, nous utilisons, comme Fliess, les séries non commutatives. Plus précisément, nous commençons par établir quelques relations entre des langages algébriques liés au langage de Łukasiewicz. Puis, dans la deuxième partie, nous montrons comment les appliquer aux séries algébriques commutatives, et nous en déduisons le résultat énoncé.

Première partie : Langage de Łukasiewicz généralisé.

1. Définitions et notations : Nous utilisons la terminologie de Lothaire [Lo].
Soit A un ensemble fini que l'on appellera *alphabet.* On appellera mot sur A tout n-uplet $w = (x_1, \dots, x_n)$, $x_i \in A$. On écrira aussi $x_1 \cdots x_n$ pour $(x_1, \dots, x_n)$, le 0-uplet () étant noté 1. On notera A^* l'ensemble des mots sur A, muni de la loi interne de *concaténation* ' $\cdot$' définie par :

$$(x_1 \cdots x_n) \cdot (y_1 \cdots y_m) = x_1 \cdots x_n y_1 \cdots y_m.$$

1 est l'élément neutre pour cette loi :

$$1 \cdot w = w \cdot 1 = w \quad \forall w \in A^*.$$

On notera également $A^+ = A^* - \{1\}$.

On appellera *langage* un sous-ensemble de A^*. Le produit de concaténation de deux langages M et N sera alors défini par :

$$M \cdot N = \{u \cdot v | u \in M \text{ et } v \in N\}.$$

Il sera aussi noté MN.

Soit K un corps. Une série formelle F sur K est une application

$$\begin{array}{rcl} A^* & \rightarrow & K \\ w & \mapsto & (F, w). \end{array}$$

On écrira aussi $F = \sum_{w \in A^*} (F, w) \cdot w$. On notera $K\langle\langle A \rangle\rangle$ l'ensemble de ces séries formelles.

Dans le souci d'alléger les notations, on ne distinguera pas un langage M, de sa série caractéristique $\mathbb{1}_M = \sum_{w \in M} w$, toutes les égalités données ici respectant les multiplicités.
Par ailleurs, soient deux langages M et N. On notera $M \equiv N$, si les images commutatives des séries caractéristiques des deux langages sont égales. Le *langage miroir* $\tilde{M}$ d'un langage M est

$$\tilde{M} = \{w \in A^* \mid w = x_1 \ldots x_n \text{ tel que } x_n \ldots x_1 \in M\}.$$

Soient deux séries formelles de $K\langle\langle A \rangle\rangle$, F et G. On définit le *produit de Hadamard* de F et G par :

$$F \odot G = \sum_{w \in A^*} (F, w)(G, w) \cdot w.$$

Soit l'alphabet $A = \{a_{-1}, a_1, \ldots, a_n\}$.
Sur cet alphabet, on définit le *langage* dit *de Łukasiewicz* (voir par exemple [Sch]) par l'équation :

$$L = a_{-1} + a_1 L^2 + \cdots + a_n L^{n+1}.$$

C'est un langage algébrique. Ce langage peut aussi se définir de manière combinatoire. Pour cela, on introduit un morphisme h de A^* dans le groupe additif $\mathbb{Z}$, défini par $h(a_i) = i$.
On a alors pour L, la définition équivalente :

$$L = \{w \in A^* \mid h(w) = -1 \text{ et } (w = w_1 w_2,\ w_2 \neq 1 \Rightarrow h(w_1) \geq 0)\}.$$

On peut généraliser cette dernière égalité : quel que soit $p > 0$ on a

$$(1)\quad L^p = \{w \in A^* \mid h(w) = -p \text{ et } (w = w_1 w_2, w_2 \neq 1 \Rightarrow h(w_1) > -p)\}.$$

(Voir [Sch] pour une démonstration et la figure 1 pour une représentation).
Pour les dessins, on représentera chaque a_i par le "vecteur" $\binom{1}{i}$.

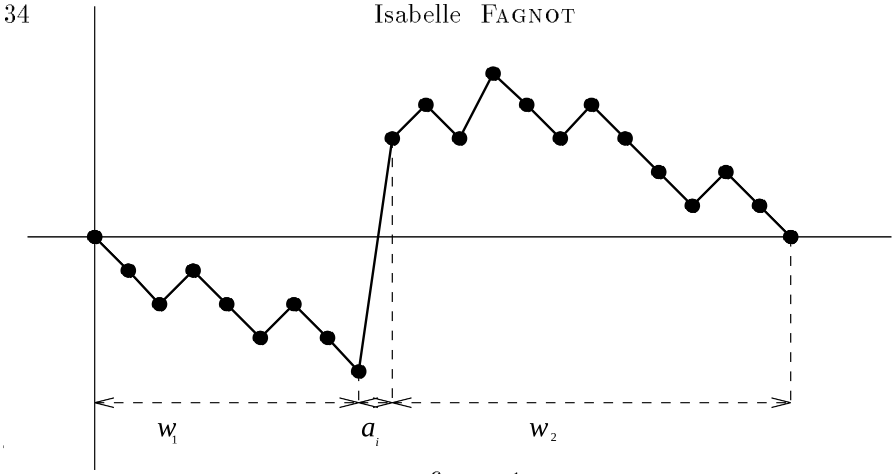


figure 1

En nous inspirant de [La], nous définissons également des langages D_p, pour $p \geq 0$, par :

$$D_p = h^{-1}(-p) = \{w \in A^* \mid h(w) = -p\}.$$

On notera également $D = D_0$.

Le langage C suivant joue un rôle central dans la suite :

$$C = \{w \in A^+ \quad \mid h(w) = 0 \text{ et } (w = w_1 w_2 \text{ et } h(w_1) = 0) \Rightarrow (w_1 = 1 \text{ ou } w_2 = 1)\}.$$

Les mots de C correspondent en quelque sorte aux "facteurs premiers" de ceux de D.

2. Premières relations : On se convaincra aisément de la validité des relations suivantes :

$$D_p = L^p \cdot D \qquad (p \geq 0); \tag{2}$$

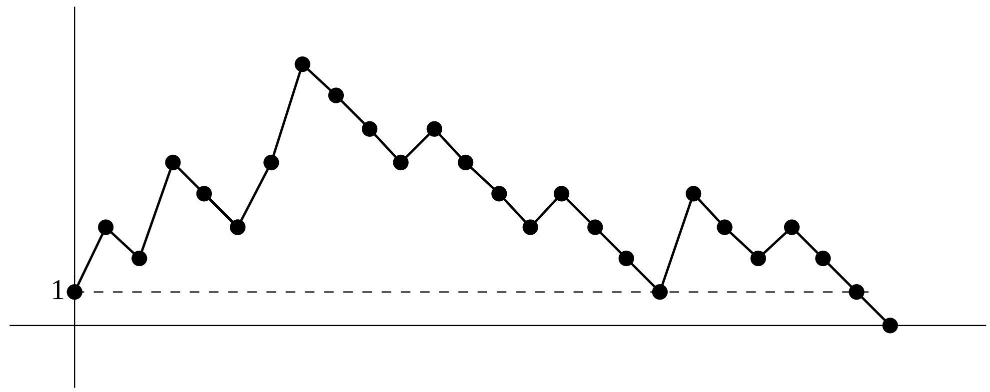
$$D = 1 + D \cdot C = \frac{1}{1-C}. \tag{3}$$

La relation suivante est fondamentale pour la suite :

Proposition 1. *On a :*

$$C = \sum_{i=1}^{n} \sum_{j+k=i} \tilde{L}^j a_i L^k$$

Démonstration. Soit w un mot de C. Soit w_1 le plus grand préfixe, différent de w, tel que $h(w_1) \leq 0$. Comme $w \neq w_1$, on peut décomposer w de la façon suivante : $w = w_1 a_i w_2$, avec $w_2 \in A^*$.



Posons $j = -h(w_1)$ et $k = -h(w_2)$. Par maximalité de w_1, $i \geq j$ ($i = j$ correspond au cas où $w_2 = 1$). D'où, $k = i - j \geq 0$.

On a donc $w_1 \in D_j$ et $w_2 \in D_k$. En fait, $w_1 \in \widetilde{L^j} = \tilde{L}^j$ et $w_2 \in L^k$.

Démontrons le pour w_2 (le cas de w_1 étant symétrique) :
D'après (2), il existe w' et w'' tels que : $w_2 = w' \cdot w''$ avec $w' \in L^k$ et $w'' \in D$
Ce qui donne : $w = w_1 a_i w' \cdot w''$ avec $h(w'') = 0$. Par définition de C, ceci implique que $w'' = 1$ et par là même que w_2 appartient à L^k.

On a donc :

$$C \subset \sum_{i=1}^{n} \sum_{j+k=i} \tilde{L}^j a_i L^k.$$

Démontrons l'inclusion réciproque : soit $w = w_1 a_i w_2$, avec $w_1 \in \tilde{L}^j$, $w_2 \in L^k$ et $j + k = i > 0$. Alors, bien sûr, w appartient à $h^{-1}(0)$.
En outre, si $w = w'w''$ avec $h(w') = 0$ alors $w' = 1$ ou $w'' = 1$.
En effet, si par exemple, $w' = w_1 a_i w_2'$ alors $w_2 = w_2' w''$ avec $h(w_2') = -k$.
Si $k > 0$, par (1) $w'' = 1$. Si $k = 0$, $L^0 = 1$ donc $w'' = 1$.
Le cas $w'' = w_1'' a_i w_2$ est symétrique du cas précédent.
Les deux points ci-dessus démontrent que w appartient à C.
En conséquence,

$$C = \sum_{i=1}^{n} \sum_{j+k=i} \tilde{L}^j a_i L^k$$

c. q. f. d.

Dans la deuxième partie nous allons avoir besoin du résultat suivant :

COROLLAIRE 2. *L'égalité suivante est vérifiée :*

$$L \equiv D_1 \odot \left[(1 - \sum_{i=1}^{n} (i+1) a_i) A^* \right]$$

et plus généralement, pour tout $j \geq 0$

$$L^j \equiv D_j \odot \left[(1 - \sum_{i=1}^{n} (i+1) a_i) A^* \right].$$

Démonstration. Par les équations (2) et (3), on a

$$D_j = L^j \cdot D = L^j (1 + DC).$$

Il en découle

$$L^j = D_j - L^j DC.$$

On remplace C par l'expression fournie dans la proposition 1 :

$$L^j = D_j - L^j D \sum_{i=1}^{n} \sum_{j+k=i} \tilde{L}^j a_i L^k.$$

On passe maintenant en variables commutatives

$$\begin{aligned} L^j &\equiv D_j - L^j D(\sum_{i=1}^{n} (i+1) a_i L^i) \equiv D_j - \sum_{i=1}^{n} (i+1) a_i L^{i+j} D \\ L^j &\equiv D_j - \sum_{i=1}^{n} (i+1) a_i D_{i+j}. \end{aligned}$$

Par ailleurs, en variables non commutatives, on a :

$$a_i D_{i+j} = a_i \sum_{h(w)=-(i+j)} w = \sum_{h(a_i w)=-j} a_i w = D_j \odot (a_i A^*).$$

D'où :

$$D_j - \sum_{i=1}^{n} (i+1) a_i D_{i+j} = D_j \odot \left[(1 - \sum_{i=1}^{n} (i+1) a_i) A^* \right]$$

En remplaçant dans (4), on obtient :

$$L^j \equiv D_j \odot \left[(1 - \sum_{i=1}^{n} (i+1) a_i) A^* \right]$$

c. q. f. d.

Deuxième partie : Application aux diagonales de séries rationnelles.

Dans cette partie, nous allons démontrer que dans un corps fini toute série algébrique en une variable est la diagonale d'une série rationnelle en deux variables.

Notations. Soit K un corps, on notera: $K\langle\langle X_1,\dots,X_n\rangle\rangle$ l'anneau des séries formelles en variables non commutatives, $K[[X_1,\dots,X_n]]$ l'anneau des séries formelles en variables commutatives, $K(X_1,\dots,X_n)$ le corps des fractions rationnelles en variables commutatives.

Soit φ une série formelle sur $K[[X_1,\dots X_n]]$,

$$\varphi = \sum a_{i_1,\dots,i_n} X_1^{i_1}\cdots X_n^{i_n}.$$

On définit la *diagonale* de φ par :

$$\mathrm{diag}(\varphi) = \sum a_{i,\dots,i} X^i.$$

Le lemme technique qui suit a pour fonction de montrer que l'on peut se ramener à de bonnes conditions initiales.

LEMME 3 ([Fu]). *Soit K un corps fini, de cardinal q. Soit φ une série formelle algébrique de $K[[X,Y]]$. Alors il existe un entier m, des polynômes $A_0, A_1,\dots,A_m$, avec $A_0(0)\neq 0$, et deux autres polynômes B et C, tels qu'en posant $\psi = C+\varphi$, on a $\psi(0)=0$ et ψ vérifie l'équation :*

$$A_0\psi = A_1\psi^q + \cdots + A_m\psi^{q^m} + B.$$

Preuve. Nous reproduisons, pour la commodité du lecteur, la preuve de [Fu].

– On définit sur $K[[X]]$ les opérateurs S_r, pour $0\le r\le q-1$:

$$\begin{array}{rcl} K[[X]] & \to & K[[X]] \\ f=\sum a_u X^u & \mapsto & S_r(f)=\sum a_{qu+r}X^u. \end{array}$$

(les S_r sont appelés opérateurs de sections mahlériennes dans [Du]). On a les relations suivantes :

$$\text{(4)} \qquad f = \sum_{r=0}^{q-1} X^r S_r(f)(X^q);$$

$$\text{(5)} \qquad S_r(f\cdot g^q) = S_r(f)\cdot g.$$

– Comme φ est algébrique, il existe des polynômes $A_0, A_1, \dots A_m$, non tous nuls, tels que
$$\sum_{i=0}^{m} A_i \varphi^{q^i} = 0.$$
On peut supposer $A_0 \neq 0$. En effet, soit l le plus petit entier tel que φ vérifie une équation du type :
$$\sum_{i=l}^{m} A_i \varphi^{q^i} = 0 \quad \text{avec} \quad A_l \neq 0.$$
Si $l > 0$, on applique (5)
$$\forall r \quad S_r(\sum_{i=l}^{m} A_i \varphi^{q^i}) = \sum_{i=l}^{m} S_r(A_i) \varphi^{q^{i-1}} = 0.$$
Or, par (4), $A_l \neq 0$ implique qu'il existe un r tel que $S_r(A_l) \neq 0$. L'équation
$$\sum_{i=l}^{m} S_r(A_i) \varphi^{q^{i-1}} = 0$$
contredit donc la minimalité de l.

– φ vérifie donc une équation de la forme :
$$A_0 \varphi = A_1 \varphi^q + \cdots + A_m \varphi^{q^m} + B,$$
avec $A_0 \neq 0$.
On peut supposer $A_0(0) \neq 0$, en effet :
Supposons $A_0 = X^r A_0'$, $r > 0$ avec $A_0'(0) \neq 0$. Soit s tel que $sq > r$ et ψ tel que $\varphi = X^s \psi + C$ où C est un polynôme. L'équation devient alors :
$$X^r A_0' X^s \psi = A_1 X^{sq} \psi^q + \cdots + A_m X^{sq^m} \psi^{sq^m} + B',$$
où B' est un polynôme. On peut diviser cette équation par X^r, et remplacer A_0 par A_0' et φ par ψ pour obtenir le résultat souhaité.

– Si $\psi(0) \neq 0$, alors on peut remplacer ψ par $\psi - \psi(0)$ sans changer la forme de l'équation.

c.q.f.d.

DÉFINITION. On définit la *valuation* v de l'anneau des séries formelles $K[[X,Y]]$ sur $\mathbb{N} \cup \{+\infty\}$ par :
$$v(\varphi) = \begin{cases} \min_{u,v}\{s = u + v \mid a_{u,v} \neq 0\} & \text{si } \varphi \neq 0, \\ +\infty & \text{sinon.} \end{cases}$$

où $\varphi = \sum a_{u,v} X^u Y^v$.

Ce lemme justifie la construction à venir.

LEMME 4. *Soient $B = \{b_1, \ldots, b_n\}$ un alphabet, $B_1, \ldots, B_n$ des séries formelles de $K[[X,Y]]$, telles que $v(B_i) > 0$.*
Soit le morphisme α défini par :

$$\begin{array}{rcl} \alpha : B^* & \to & K[[X,Y]] \\ b_i & \mapsto & b_i\alpha = B_i. \end{array}$$

Alors, on peut étendre ce morphisme en un morphisme de $K\langle\langle B\rangle\rangle$ dans $K[[X,Y]]$.

Preuve. On rappelle qu'une famille de séries formelles $(F_i)_{i\in I}$, $F_i(X,Y) = \sum a^i_{u,v} X^u Y^v$, est dite *localement finie* si :

$$\forall u, v \quad \mathrm{Card}\Big(\{i \mid a^i_{u,v} \neq 0\}\Big) < +\infty.$$

Il en découle que, si $(F_i)_{i\in I}$ est localement finie, cette famille est sommable.

Soit $w \in B^*$, $\mid w \mid = l$, $w = b_{i_1}, \ldots, b_{i_l}$.

$$v(w\alpha) = \sum_{j=1}^{l} v(b_{i_j}\alpha) \geq l.$$

De cette inégalité, il ressort que pour toute série formelle, $F = \sum (F,w)\cdot w$ de $K\langle\langle B\rangle\rangle$, la famille $((F,w)\cdot w\alpha)_{w\in B^*}$ est localement finie, et par là même sommable.

On peut donc prolonger le morphisme α par

$$F\alpha = \sum_{w\in B^*} (F,w)\cdot w\alpha.$$

D'où le résultat.

c. q. f. d.

Nous aurons encore besoin d'un lemme technique :

LEMME 5. *Soit le morphisme α défini par :*

$$\begin{array}{rcl} \alpha : A^* & \to & K[[X,Y]] \\ a_i & \mapsto & B_i(XY)Y^i, \end{array}$$

où les B_i sont des séries rationnelles de $K(X)$ telles que $v(B_i) \geq 0$ et $B_{-1}(0) = 0$. Soit $F = \sum_{w \in A^*}(F, w) \cdot w$ une série formelle de $K\langle\langle A\rangle\rangle$. Alors pour tout $j \geq 0$,

$$Y^j(D_j \odot F)\alpha = diag(Y^j \cdot F\alpha)$$

Preuve. Soit $w = a_{j_0} \dots a_{j_p}$ un mot de A^*. Alors

$$D_j \odot w = \begin{cases} w & \text{si } h(w) = -j, \\ 0 & \text{sinon.} \end{cases} \tag{6}$$

Donc,

$$Y^j(D_j \odot w)\alpha = \begin{cases} Y^j \cdot w\alpha & \text{si } h(w) = -j, \\ 0 & \text{sinon.} \end{cases}$$

$$Y^j(D_j \odot w)\alpha = \begin{cases} Y^j \cdot Y^{j_0} B_{j_0} \cdots Y^{j_p} B_{j_p} = B_{j_0} \cdots B_{j_p} & \text{si } h(w) = -j, \\ 0 & \text{sinon.} \end{cases}$$

Par ailleurs :

$$\begin{aligned} \mathrm{diag}(Y^j \cdot w\alpha) &= \mathrm{diag}\left(Y^j \cdot Y^{j_0} B_{j_0} \cdots Y^{j_p} B_{j_p}\right) \\ &= \mathrm{diag}\left(Y^{j+j_0+\cdots+j_p} B_{j_0} \cdots B_{j_p}\right) \end{aligned}$$

Donc,

$$\mathrm{diag}(Y^j \cdot w\alpha) = \begin{cases} B_{j_0} \cdots B_{j_p} & \text{si } j_0 + \cdots + j_p = h(w) = -j, \\ 0 & \text{sinon.} \end{cases}$$

D'où :

$$Y^j(D_j \odot w)\alpha = \mathrm{diag}(Y^j \cdot w\alpha) \quad \forall w \in A^*$$

Alors d'après le lemme 4, on peut conclure par linéarité

$$\begin{aligned} Y^j(D_j \odot F)\alpha &= \sum_{w \in A^*} (F, w) \cdot Y^j(D_j \odot w)\alpha \\ &= \sum_{w \in A^*} (F, w) \cdot \mathrm{diag}(Y^j \cdot w\alpha) \\ &= \mathrm{diag}\left(Y^j \cdot F\alpha\right). \end{aligned}$$

c. q. f. d.

Le résultat énoncé en introduction découle immédiatement de la proposition ci-dessous. La formule donnée ici est exactement la même que celle donnée par Furstenberg [Fu], mais ici elle découle de la "traduction" en variables commutatives de la formule donnée dans le corollaire 2, c'est ceci qui rend la preuve combinatoire.

PROPOSITION 6. *Soient K un corps quelconque, et φ une série formelle algébrique appartenant à $K[[X]]$.*
Soit P un polynôme, appartenant à $K[X,Y]$, tel que $P(X,\varphi(X)) = 0$.
On suppose de plus que :

$$\varphi(0) = 0$$
$$\frac{\partial P}{\partial Y}(0,0) \neq 0.$$

Alors

$$\varphi = diag\left(\frac{Y^2 \frac{\partial P}{\partial Y}(XY,Y)}{P(XY,Y)}\right).$$

Et, plus généralement, pour tout $j \geq 0$:

$$\varphi^j = diag\left(\frac{Y^{j+1} \frac{\partial P}{\partial Y}(XY,Y)}{P(XY,Y)}\right).$$

Démonstration.

– On peut écrire P sous la forme :

$$P(X,Y) = -P_0(X) + P_1(X)Y - P_2(X)Y^2 - \cdots P_{n+1}(X)Y^{n+1}.$$

Les hypothèses de l'énoncé impliquent alors :

$$P_0(0) = 0 \quad (\text{car } \varphi(0) = 0)$$
$$P_1(0) \neq \quad 0.$$

Et φ vérifie alors l'équation :

$$P_1\varphi = P_0 + P_2\varphi^2 + \cdots + P_{n+1}\varphi^{n+1}.$$

Ce qui peut se transformer en :

$$\varphi = R_{-1} + R_1\varphi^2 + \cdots + R_n\varphi^{n+1}, \tag{7}$$

avec $R_i = \frac{P_{i+1}}{P_1}$
(Ceci ne pose pas de problème dans la mesure où P_1 est inversible.)

– Soit le morphisme α défini par :

$$\begin{aligned} \alpha : A^* &\to K[[X,Y]] \\ a_i &\mapsto R_i(XY)Y^i. \end{aligned}$$

(On peut remarquer que le "déficit" ou "l'excédent" de $a_i\alpha$ en Y est égal à la hauteur, $h(a_i)$, de a_i).

– Alors, d'une part :

$$\varphi = Y \cdot L\alpha. \tag{8}$$

En effet, remarquons tout d'abord que les conditions imposées sur P et sur φ garantissent l'existence et l'unicité de la solution de $P(X, \varphi(X)) = 0$. (Si $\varphi(X) = \sum c_n X^n$, on va pouvoir trouver des relations de récurrence de la forme $c_n = f_n(c_0, \ldots, c_{n-1})$).
Or,

$$L\alpha = \frac{R_{-1}(XY)}{Y} + Y R_1(XY)(L\alpha)^2 + \cdots + Y^n R_n(XY)(L\alpha)^{n+1}.$$

Il en résulte

$$YL\alpha = R_{-1}(XY) + R_1(XY)(YL\alpha)^2 + \cdots + R_n(XY)(YL\alpha)^{n+1}.$$

Ce qui correspond bien à l'équation vérifiée par φ.

– D'autre part, dans le corollaire 2, on avait démontré :

$$\begin{aligned} L^j &\equiv D_j \odot \left[(1 - \sum_{i=1}^{n} (i+1)a_i)A^* \right] \\ &\equiv D_j \odot \left[\frac{(1 - \sum_{i=1}^{n}(i+1)a_i)}{1 - a_{-1} - a_1 - \cdots - a_n} \right] \end{aligned}$$

on applique α et on multiplie par Y^j :

$$Y^j \cdot L^j\alpha \equiv Y^j \left(D_j \odot \left[\frac{(1 - \sum_{i=1}^{n}(i+1)a_i)}{1 - a_{-1} - a_1 - \cdots - a_n} \right] \right) \alpha$$

en utilisant la formule (8) et le lemme 5, on obtient :

$$\begin{aligned} \varphi^j &= \operatorname{diag} \left(Y^j \frac{1 - \sum_{i=1}^{n}(i+1)Y^i R_i(XY)}{1 - \frac{R_{-1}(XY)}{Y} - R_1(XY)Y - \cdots - R_n(XY)Y^n} \right) \\ &= \operatorname{diag} \left(Y^j \frac{1 - \sum_{i=1}^{n}(i+1)Y^i \frac{P_{i+1}(XY)}{P_1(XY)}}{1 - \frac{1}{Y}\frac{P_0(XY)}{P_1(XY)} - Y\frac{P_2(XY)}{P_1(XY)} - \cdots - Y^n \frac{P_{n+1}(XY)}{P_1(XY)}} \right) \end{aligned}$$

en multipliant nominateur et dénominateur par $YP_1(XY)$, on obtient :

$$\varphi^j = \mathrm{diag}\left(\frac{Y^{j+1}\frac{\partial P}{\partial Y}(XY,Y)}{P(XY,Y)}\right).$$

c. q. f. d.

Corollaire 7. *Pour toute fraction rationnelle $H \in K(X,Y)$, telle que $v(H) \geq 0$, on a :*

$$H(X,\varphi(X)) = diag\left(\frac{YH(XY,Y)\frac{\partial P}{\partial Y}(XY,Y)}{P(XY,Y)}\right).$$

Et, en particulier :

$$\frac{1}{1-\varphi} = diag\left(\frac{Y}{1-Y}\frac{\frac{\partial P}{\partial Y}(XY,Y)}{P(XY,Y)}\right).$$

Démonstration. On peut écrire H sous la forme :

$$H(X,Y) = \sum_{i\geq 0} H_i(X)Y^i.$$

Alors :

$$\begin{aligned} H(X,\varphi(X)) &= \sum_{i\geq 0} H_i(X)\varphi^i(X) \\ &= \sum_{i\geq 0} H_i(X)\mathrm{diag}\left(\frac{Y^{i+1}\frac{\partial P}{\partial Y}(XY,Y)}{P(XY,Y)}\right) \\ &= \mathrm{diag}\left(\frac{\sum_{i\geq 0} H_i(XY)Y^{i+1}\frac{\partial P}{\partial Y}(XY,Y)}{P(XY,Y)}\right) \\ &= \mathrm{diag}\left(\frac{YH(XY)\frac{\partial P}{\partial Y}(XY,Y)}{P(XY,Y)}\right). \end{aligned}$$

c. q. f. d.

Nous pouvons maintenant énoncer le résultat donné en introduction :

Théorème 8. *Soit K un corps fini, φ une série formelle algébrique sur $K(X)$. Alors, il existe une fraction rationnelle H en deux variables telle que $\varphi = diag(H)$, de plus cette fonction est calculable.*

Démonstration. En effet, par le lemme 3, on peut calculer C et ψ tel que $\varphi = C + \psi$, ψ vérifiant les conditions de la proposition 6. D'où

$$\psi = \operatorname{diag}\left(\frac{Y^2\frac{\partial P}{\partial Y}(XY,Y)}{P(XY,Y)}\right)$$

pour un certain polynôme P. Et donc,

$$\psi = \operatorname{diag}\left(C(XY) + \frac{Y^2\frac{\partial P}{\partial Y}(XY,Y)}{P(XY,Y)}\right).$$

$H = C(XY) + \frac{Y^2\frac{\partial P}{\partial Y}(XY,Y)}{P(XY,Y)}$ convient donc.
c. q. f. d.

Exemple. La suite de Thue-Morse, $(u_n)_{n\in N}$, peut être définie de diverses façons (cf. [Lo]).
Par exemple, $u_n \equiv d_2(n) \pmod 2$, avec $d_2(n)$ représentant le nombre de 1 dans l'écriture binaire de n
Si on pose $F(X) = \sum u_n X^n$, alors F vérifie l'équation

$$(1+X)^3F^2 + (1+X)^2F + X = 0.$$

De la proposition 5, on déduit :

$$F = \operatorname{diag}\left(\frac{Y}{1 + Y(1+XY) + \frac{X}{(1+XY)^2}}\right).$$

(cf. [All1]).
Nota : On peut vérifier que l'on a également

$$F = \operatorname{diag}\left(\frac{X}{1 + X + Y + X^3Y}\right).$$

Je tiens à remercier J. Berstel pour ses précieux conseils.

Bibliographie

[All1] J.-P. Allouche, *Automates finis en théorie des nombres*, Expositiones Mathematicae, **5** (1987), 239–266.

[All2] J.-P. Allouche, *Note sur un article de Sharif et Woodcock*, Séminaire de Théorie des Nombres de Bordeaux, **1** (1989) 163–187.

[Du] P. Dumas, *Récurrences mahlériennes, suites automatiques, études asymptotiques*, Thèse Bordeaux I (1983).

[CKMR] G. Christol, T. Kamae, M. Mendès France et G. Rauzy, *Suites algébriques, automates et substitutions*, Bulletin de la Société mathématique de France, **108** (1980), 401–419.

[De] P. Deligne, *Intégration sur un cycle évanescent*, Inventiones Mathemeticae, **76** (1984), 129–143.

[DL] J. Denef et L. Lipshitz,*Algebraic power series and diagonals*, Journal of Number Theory, **26** (1987), 46–67.

[Ei] S. Eilenberg, *Automata, Languages and Machines,* vol. A London, New York, Academic Press (1974).

[Fl] M. Fliess, *Sur certaines familles de séries formelles,* Thèse, Paris VII (1972).

[Fu] H. Furstenberg, *Algebraic functions over finite fields*, Journal of Algebra, **7** (1967) 271–277.

[Ha] T. Harase, *Algebraic elements in formal power series rings*, Israel Journal of Mathematics, **63 3** (1988), 281–288.

[La] J. Labelle, *Langages de Dyck généralisés*, Prépublication.

[Lo] Lothaire, *Combinatorics on words,* Addison-Wesley Publishing Company (1983).

[Sa1] O. Salon, *Suites automatiques à multi-indices*, Séminaire de Théorie des Nombres de Bordeaux, exposé n^{o}4 (1986–1987), 4.01–4.36. (Avec un appendice de J. Shallit).

[Sa2] O. Salon, *Suites automatiques à multi-indices et algébricité*, Comptes-Rendus de l'Académie des Sciences de Paris, t. 305, série I, p. 501–504, 1987.

[Sch] M. P. Schützenberger, *Le théorème de Lagrange selon G. N. Raney*, Séminaires IRIA, Rocquencourt (1971) 199–205.

[SW] H. Sharif et C. F. Woodcock, *Algebraic functions over a field of positive characteristic and Hadamard products*, Journal of the London Mathematical Society, (2) **37** (1988), 395–403.

Isabelle Fagnot
LITP Université Paris 6
2, place Jussieu
75252 Paris Cedex 05.
e-mail: fagnot@litp.ibp.fr

Isabelle FAGNOT
LITP Université Paris 6
2, place Jussieu
75252 Paris Cedex 05
e-mail: fagnotlitp.ibp.fr