Clôture algébrique du corps $\mathbb{F}_q(t)$ et automates finis

Oleksandr Aksenov, Thibaut Kirchner
Encadrés par François Loeser

7 février 2008

Table des matières

1 Introduction

Dans cet exposé, on s'intéresse à la description explicite de la clôture algébrique d'un corps $\mathbb{F}_q(t)$ où q est une puissance d'un nombre premier p. On cherchera d'abord les éléments algébriques sur $\mathbb{F}_q(t)$ dans le corps $\mathbb{F}_q((t))$ des séries de Laurent formelles avec les coefficients dans $\mathbb{F}_q$ (théorème de Christol), ce qui donne une réponse explicite en termes de langages reconnaissables par un automate fini. Ensuite, comme le corps $\mathbb{F}_q((t))$ n'est pas algébriquement clos, on sera amené à travailler dans le corps des séries de Hahn, qui l'est, et dans lequel on obtiendra une caractérisation semblable des éléments algébriques sur $\mathbb{F}_q(t)$.

2 Théorème de Christol

Ici nous allons caractériser les séries de Laurent formelles à coefficients dans $\mathbb{F}_q$ qui sont algébriques sur $\mathbb{F}_q(t)$. Notons qu'en fait il suffit de travailler avec des séries entières.

Nous allons caractériser ces séries par leur lien avec les deux notions suivantes.

Définition 2.1. Un ensemble A d'entiers naturels sera appelé *q-reconnaissable* si l'ensemble des écritures de ses éléments en base q forme un langage rationnel (rappelons que le sens d'écriture des entiers n'a pas d'importance, et que la q-reconnaissabilité équivaut à la p-reconnaissabilité). Une suite $(a_n) \in \mathbb{F}_q$ sera appelée *q-reconnaissable* si pour tout $b \in \mathbb{F}_q$ l'ensemble $\{n \in \mathbb{N} : a_n = b\}$ est q-reconnaissable.

Définition 2.2. D'autre part, on appellera la *diagonale* d'une fraction rationnelle

$$\frac{P(x_1, x_2, \ldots, x_n)}{Q(x_1, x_2, \ldots, x_n)} = \sum_{k_1,k_2,\ldots,k_n} a_{k_1,k_2,\ldots,k_n} x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$$

la série formelle

$$\Delta \frac{P}{Q} = \sum_k a_{k,k,\ldots,k} t^k.$$

Nous montrerons que ces trois notions sont en fait équivalentes.

Le cas le plus facile à analyser est celui des séries avec les coefficients dans $\{0, 1\}$. En effet, une telle série est algébrique sur $\mathbb{F}_q(t)$ si et seulement si elle l'est sur $\mathbb{F}_p(t)$. La démonstration que nous donnons ici reprend des preuves de différentes propriétés données dans les articles [2] et [3]. En particulier, l'équivalence algébrique $\Leftrightarrow$ diagonale d'une fonction rationnelle à deux variables est prouvée dans [3], de façon plus technique. Par contre, le lien avec les ensemble p-reconnaissables a été remarqué pour la première fois par G. Christol.

Théorème 2.1 (Christol)**.** *Une série $f(x) = \sum_{n \in A} x^n \in \mathbb{F}_p[[x]]$ avec A un ensemble p-reconnaissable est algébrique sur $\mathbb{F}_p(t)$.*

Démonstration. Nous utiliserons l'écriture des entiers dans le sens inverse (c'est-à-dire, le chiffre de poids faible est lu en premier par l'automate) et noterons A_p l'ensemble des écritures des éléments de A. On notera pour tous $n, h \in \mathbb{N}$ tels que $n < p^h$:

$$f_{n,h}(x) = \sum_{m, mp^h+n \in A} x^m$$

la série qui correspond au langage $u^{-1}A_p$ où u est l'écriture inverse de l'entier n en h chiffres en base p. A est p-reconnaissable si et seulement s'il n'existe qu'un nombre fini de diffèrents $f_{n,h}$.

Notons N le nombre de $f_{n,h}$ différents, et posons

$$g = P_0(x)f(x) + P_1(x)f(x^p) + \cdots + P_{2N}(x)f(x^{p^{2N}})$$

avec P_i des polynômes de $\mathbb{F}_p[x]$ de degré strictement inférieur à p^{2N}. Définissons à partir de g les séries g_j par la relation

$$g = \sum_{j=0}^{p^{2N}-1} x^j g_j(x^{p^{2N}}).$$

Les g_j sont alors des combinaisons linéaires (à coefficients dans $\mathbb{F}_p$) des $f_{n,h}$ et des $xf_{n,h}$. Elles ont donc p^{2N} valeurs possibles, d'où il y a au maximum $(p^{2N})^{p^{2N}}$ valeurs possibles de g. Or il y a $(p^{p^{2N}})^{2N+1}$

écritures différentes de g. Il existe donc deux écritures différentes qui prennent la même valeur, et on obtient par soustraction une suite de polynômes P_i non tous nuls telle que

$$P_0 f + P_1 f^p + \cdots + P_{2N} f^{p^{2N}} = 0.$$

f est donc algébrique. □

La propriété suivante est valable dans un cas plus général.

Théorème 2.2 (Furstenberg)**.** *Soit $f(x) \in \mathbb{F}_q[[x]]$ une série $\mathbb{F}_q(t)$-algébrique. Alors elle est la diagonale d'une fraction rationnelle.*

Démonstration. Notons d'abord que les séries $f, f^p, f^{p^2}, \ldots$ sont linéairement liées sur $\mathbb{F}_q(t)$, donc il existe entre elles une relation de la forme

$$A'_0(x) f^{p^l}(x) = A'_1(x) f^{p^{l+1}}(x) + \cdots + A'_n(x) f^{p^{l+n}}(x)$$

avec $A'_0 \neq 0$. Montrons qu'on peut obtenir une relation du même type avec $l = 0$.

Supposons en effet, que $l > 0$. Alors, toutes les puissances de f dans cette expression sont fonctions de x^p. Soit $i < p$ un entier tel que dans A_0 apparaît au moins un terme d'exposant congru à i modulo p. En ne gardant dans les A'_j que ces termes-là, on obtient encore une égalité, qu'on peut diviser par x^i. On obtient alors une égalité de la forme

$$A''_0(x^p) f^{p^l}(x) = A''_1(x^p) f^{p^{l+1}}(x) + \cdots + A''_n(x^p) f^{p^{l+n}}(x)$$

avec $A_j \in \mathbb{F}_q[[x]]$ et $A_0 \neq 0$. Comme l'automorphisme de Frobenius est bijectif dans $\mathbb{F}_q$, on peut passer à son image réciproque dans l'égalité ci-dessus, ce qui donne une égalité de la même forme mais avec $(l-1)$ à la place de l.

En itérant la procédure précédente, on obtient donc une égalité de la forme

$$A_0(x) f(x) = A_1(x) f^p(x) + \cdots + A_n(x) f^{p^n}(x).$$

Montrons maintenant qu'on peut exprimer f sous forme $f(x) = R(x) + x^h \phi(x)$ avec R un polynôme et obtenir une relation

$$B_0(x)\phi(x) = B_1(x)\phi^p(x) + \cdots + B_n(x)\phi^{p^n}(x) + B(x)$$

avec, de plus, $B_0(0) \neq 0$.

En effet, si x^r $(r > 0)$ divise $A_0(x)$, posons $f(x) = f(0) + x\phi(x)$. On a alors :

$$A_0(x)x\phi(x) = A_1(x)x^p\phi^p(x) + \cdots + A_n(x)x^{p^n}\phi^{p^n}(x) + B'(x)$$

avec B' un polynôme. En posant $s = \min(p, r+1)$, on voit que chaque terme $A_k(x)x^{p^k}$ est multiple de x^s, d'où B' en est aussi un. En divisant par x^s, on obtient une égalité de même type mais le nouveau A_0 n'est plus multiple de x^r. En itérant cette procédure, on arrive à une égalité de type cherché. On en déduit une égalité de type suivant :

$$B_0(x)(\phi(x) - \phi(0)) = B_1(x)(\phi(x) - \phi(0))^p + \cdots + B_n(x)(\phi(x) - \phi(0))^{p^n} + C(x)$$

qui donne un polynôme $P \in \mathbb{F}_p[x, y]$ tel que $P(x, \phi(x) - \phi(0)) = 0$ et $\frac{\partial P}{\partial y} = B_0(0) \neq 0$. Nous allons noter par la suite $\psi(x) = \phi(x) - \phi(0)$.

Le polynôme P se factorise sous la forme $P(x, y) = (y - \psi(x))Q(x, y)$ avec $Q \in \mathbb{F}_q((x))[y]$. La dérivation logarithmique de cette égalité donne

$$\frac{1}{P}\frac{\partial P}{\partial y}(x, y) = \frac{1}{y - \psi(x)} + \frac{1}{Q}\frac{\partial Q}{\partial y}(x, y).$$

En multipliant par y^2 et en remplaçant x par xy, on obtient :

$$\frac{y^2}{P(xy, y)}\frac{\partial P}{\partial y}(xy, y) = \frac{y^2}{y - \psi(xy)} + \frac{y^2}{Q(xy, y)}\frac{\partial Q}{\partial y}(xy, y).$$

En passant aux diagonales, on obtient :

$$\Delta\left(\frac{y^2}{y-\psi(x,y)}\right)=\Delta\left(\frac{y}{1-\frac{\psi(xy)}{y}}\right)=\Delta\left(\sum_{n=0}^{\infty}y^{-n+1}\psi(xy)^n\right)=\Delta(\psi(xy))=\psi$$

et $\Delta(\frac{y^2}{Q(xy,y)}\frac{\partial Q}{\partial y}(xy,y))=0$ car $\frac{1}{Q(X,y)}\in\mathbb{F}_q((X))[[y]]$, d'où $\frac{\frac{\partial Q}{\partial y}(X,y)}{Q(X,y)}\in\mathbb{F}_q((X))[[y]]$. En remplaçant X par xy et en multipliant par y^2, on obtient donc une série de Laurent formelle de diagonale nulle.

Par conséquent,

$$\psi=\Delta\left(\frac{y^2}{P(xy,y)}\frac{\partial P}{\partial y}(xy,y)\right),$$

c'est-à-dire, ψ est la diagonale d'une fraction rationnelle. On en déduit facilement que f est aussi la diagonale d'une fraction rationnelle.

□

La propriété suivante montre l'équivalence des trois notions dans le cas d'une série avec les coefficients dans $\{0,1\}$ et le corps de base $\mathbb{F}_p$.

Théorème 2.3 (Christol)**.** *Soit $f(x)=\sum_{n\in A}x^n\in\mathbb{F}_p[[x]]$ une série qui est diagonale d'une fraction rationnelle. Alors, elle est p-reconnaissable.*

Démonstration. Soient $P(x_1,x_2,\ldots,x_m)$ et $Q(x_1,x_2,\ldots,x_m)$ deux polynômes tels que $f(t)=\Delta\frac{P}{Q}=\sum_m a_{m,m}t^m$. Pour tous $n,h\in\mathbb{N}$ tels que $n<p^h$ on peut réécrire

$$\frac{P(x_1,x_2,\ldots,x_m)}{Q(x_1,x_2,\ldots,x_m)}=\frac{P(x_1,x_2,\ldots,x_m)Q^{p^h-1}(x_1,x_2,\ldots,x_m)}{Q(x_1^{p^h},x_2^{p^h},\ldots,x_m^{p^h})},$$

d'où la série $f_{n,h}$ s'obtient comme $f_{n,h}(t)=\Delta\frac{R_{n,h}(X_1,X_2,\ldots,X_m)}{Q(X_1,X_2,\ldots,X_m)}$ où
$R_{n,h}(X_1,X_2,\ldots,X_m)$ est la série obtenue à partir du numérateur de cette fraction par la transformation linéaire suivante monôme par monôme :

$$\begin{array}{rcl} x_1^n x_1^{k_1p^h}x_2^n x_2^{k_2p^h}\ldots x_m^n x_m^{k_np^h} & \mapsto & X_1^{k_1}X_2^{k_2}\ldots X_m^{k_m} \\ \text{tout autre monôme} & \mapsto & 0 \end{array}.$$

Le degré d de chaque monôme de $R_{n,h}$ vérifie alors l'inégalité

$$mn+dp^h\leq deg(P)+(p^h-1)deg(Q),$$

d'où $d\leq\max(deg(P),deg(Q))$.

Il existe donc un nombre fini de $f_{n,h}$ différents, d'où A est p-reconnaissable.

□

Considérons à présent une série $f(x)=\sum_n a_nx^n\in\mathbb{F}_q[[x]]$. Si pour tout $b\in\mathbb{F}_q$ la série $f_b=\sum_{n,a_n=b}x^n$ est algébrique sur $\mathbb{F}_q(x)$, f l'est aussi. Réciproquement, si la série f est algébrique, alors elle est la diagonale d'une fonction rationnelle. On en déduit que chaque série f_b est diagonale d'une fonction rationnelle à l'aide du lemme suivant :

Proposition 2.4. *Le produit (terme à terme) de deux diagonales de fonctions rationnelles est aussi la diagonale d'une fonction rationnelle.*

Démonstration. Soient deux séries $\phi(x)=\sum_k a_kx^k=\Delta(R(x_1,x_2,\ldots,x_k))$ et $\psi(x)=\sum_k b_kx^k=\Delta(S(y_1,y_2,\ldots,y_m))$ avec R et S deux fonctions rationnelles. Alors, la fonction rationnelle

$$H(x_1,\ldots,x_n,y_1,\ldots,y_m)=R(x_1,x_2,\ldots,x_k)S(y_1,y_2,\ldots,y_m)$$

a pour diagonale $\theta(t)=\sum_k a_kb_kt^k$. □

Comme pour chaque $b\in\mathbb{F}_q$, on a $(f_b)_n=1-(a_n-b)^{q-1}$, grâce au lemme précédent, toutes ces suites sont diagonales de fonctions rationnelles. Donc, elles sont algébriques.

3 Introduction du corps $\mathbb{F}_q((t^{\mathbb{Q}}))$

Afin de décrire plus précisément la clôture algébrique de $\mathbb{F}_q(t)$, nous allons nous intéresser à sa fermeture algébrique dans un corps encore plus grand que $\mathbb{F}_q((t))$, à savoir $\mathbb{F}_q((t^{\mathbb{Q}}))$. Il s'agit de généraliser les séries de Laurent avec des exposants rationnels. Nous allons donc présenter $K((t^{\mathbb{Q}}))$ pour un corps K fixé pour toute cette section. Une construction encore plus générale (en remplaçant $\mathbb{Q}$ par un groupe totalement ordonné) pourra être trouvée dans [6] ou [5] .

L'essentiel des démonstrations de cette section peuvent être faites sans utiliser l'axiome du choix. Cependant, lorsque l'utilisation de celui-ci permet de simplifier la preuve, on ne s'en privera pas. On utilisera notamment la caractérisation des ensembles bien ordonnés comme étant les ensembles où toute suite décroissante stationne, qui utilise l'axiome du choix.

On rappelle que toute partie d'un ensemble bien ordonné est bien ordonnée (par l'ordre induit), propriété que l'on utilisera sans même la mentionner.

Définition 3.1 (Support)**.** Soit $f : \mathbb{Q} \to K$. On appellera *support de* f et on notera $Supp(f)$ l'ensemble $\{i \in \mathbb{Q}, f(i) \neq 0\}$.

Définition 3.2 (Série de Hahn)**.** Pour $f : \mathbb{Q} \to K$, on dira qu'il s'agit d'une *série de Hahn* (à coefficients dans K, à exposants dans $\mathbb{Q}$) lorsque $Supp(f)$ est bien ordonné. On la notera $x = \sum_{i\in\mathbb{Q}} f(i)t^i$ pour la considérer en tant que série de Hahn d'indéterminée t. On pourra aussi la noter $x(t)$ pour rappeler que l'indéterminée est t.

On note $K((t^{\mathbb{Q}}))$ l'ensemble des séries de Hahn à coefficients dans K et à exposants dans $\mathbb{Q}$.

Il s'agit bien d'une généralisation de la notion de série de Laurent, celles-ci étant les séries de Hahn à support dans $\mathbb{Z}$. On remarque que les parties bien ordonnées de $\mathbb{Z}$ sont précisément les parties minorées de $\mathbb{Z}$.

Comme on pourra le constater par la suite, la condition "bien ordonné" est essentielle pour définir la multiplication.

On munit $K((t^{\mathbb{Q}}))$ d'une structure de K-espace vectoriel par l'addition coefficient par coefficient, et la multiplication scalaire coefficient par coefficient.

La seule chose à prouver pour vérifier que c'est bien défini est que l'union de deux parties bien ordonnées de $\mathbb{Q}$ est bien ordonnée, ce qui est immédiat. La multiplication et l'inversibilité des éléments non nuls sont les points délicats de cette construction, et nécessitent quelques lemmes.

Notation 3.3. Pour $A, B \subset \mathbb{Q}$, on pose $A + B = \{a + b, (a, b) \in A \times B\}$.

Lemme 3.1. *Soient A, B deux parties bien ordonnées de $\mathbb{Q}$. Alors, pour $i \in \mathbb{Q}$, il n'existe qu'un nombre fini de $(a, b) \in A \times B$ tels que $i = a + b$. De plus, $A + B$ est bien ordonné.*

Démonstration. On rappelle que, de toute suite à valeurs réelles, on peut extraire une sous-suite monotone.

Soit $(i_n) \in (A + B)^{\mathbb{N}}$ décroissante. Pour $n \in \mathbb{N}$, on choisit $(a_n, b_n) \in A \times B$ tel que $i_n = a_n + b_n$. Quitte à extraire deux fois, on peut supposer (a_n) et (b_n) monotones. Leur somme est décroissante, donc l'une d'entre elles est décroissante, donc stationnaire. Donc l'autre est décroissante à partir d'un certain rang, donc stationnaire aussi. Puis (i_n) est également stationnaire.

On obtient le deuxième point de manière directe, et le premier en appliquant ce qui précède à une suite constante. □

On peut maintenant définir la multiplication :

Définition 3.4. Soient $x = \sum_{i\in\mathbb{Q}} x_i t^i$ et $y = \sum_{i\in\mathbb{Q}} y_i t^i$ deux éléments de $K((t^{\mathbb{Q}}))$.

On définit le produit de x et y par

$$xy = \sum_{i\in\mathbb{Q}} \left(\sum_{a+b=i} x_a y_b \right) t^i.$$

La première partie du lemme prouve que la somme interne est à support fini, la deuxième partie prouve que la somme externe est à support bien ordonné, et assure ainsi que le produit de deux éléments de $K((t^{\mathbb{Q}}))$ est bien défini et dans $K((t^{\mathbb{Q}}))$.

On prouve de la même manière que dans le cas de $K((t))$ que, muni de ces lois, $K((t^{\mathbb{Q}}))$ est une K-algèbre (associative, commutative et unitaire). Avant de passer à l'inversibilité des éléments non nuls, on a besoin d'introduire des notations et lemmes supplémentaires :

Définition 3.5 (Valuation)**.** Soit $x \in K((t^{\mathbb{Q}})) \setminus \{0\}$.

On appelle *valuation de* x, et on note $Val(x)$ le rationnel $\min Supp(x)$. On pose de plus $Val(0) = +\infty$.

Propriété 3.2. *Soient* $x, y \in K((t^{\mathbb{Q}}))$.

On a $Val(xy) = Val(x) + Val(y)$.

La preuve est la même que pour les polynômes, les séries entières ou les séries de Laurent.

Lemme 3.3. *Soit* (A_n) *une suite de parties bien ordonnées de* $\mathbb{Q}$*, telles que* $\min A_n \xrightarrow[n\infty]{} +\infty$.

Pour $i \in \mathbb{Q}$*, on n'a qu'un nombre fini de* $n \in \mathbb{N}$ *tels que* $i \in A_n$*. De plus,* $A = \bigcup_{n\in\mathbb{N}} A_n$ *est bien ordonné.*

Démonstration. La première partie du lemme est évidente, montrons la deuxième.

On choisit $\varphi : A \to \mathbb{N}$ telle que $\forall i \in A, i \in A_{\varphi(i)}$. Soit $(i_n) \in A^{\mathbb{N}}$ décroissante.

Soit $k_0 \in \mathbb{N}$ tel que $\forall k \geq k_0, \min A_k > i_0$.

On a, pour tout $n \in \mathbb{N}$, $\varphi(i_n) < k_0$. La suite $(\varphi(i_n))$ est à valeurs dans un ensemble fini ; quitte à en extraire une sous-suite, on peut la supposer constante, de valeur $k \in \mathbb{N}$. Ainsi, (i_n) est une suite décroissante dans A_k bien ordonné, donc stationnaire.

D'où A est bien ordonné. □

Définition 3.6. Soit $(x_n) = \left(\sum_{i\in\mathbb{Q}} a_{n,i}t^i\right) \in K((t^{\mathbb{Q}}))^{\mathbb{N}}$.

On dira que la série $\sum_{n\in\mathbb{N}} x_n$ *converge* lorsque $Val(x_n) \xrightarrow[n\infty]{} +\infty$.

Dans ce cas, on posera $\sum_{n=0}^{+\infty} x_n = \sum_{i\in\mathbb{Q}} \left(\sum_{n\in\mathbb{N}} a_{n,i}\right) t^i$.

D'après le lemme qui précède, la somme interne est à support fini, et la somme externe à support bien ordonné. Ainsi, $\sum_{n=0}^{+\infty} x_n$ est bien défini et dans $K((t^Q))$.

Lemme 3.4. *Soit* $x \in K((t^{\mathbb{Q}}))$*, tel que* $Val(x) > 0$.

Alors la série $\sum_{n\in\mathbb{N}} x^n$ *est convergente et* $1 - x$ *est inversible, d'inverse* $\sum_{n=0}^{+\infty} x^n$.

Démonstration. On a $Val(x^n) = n\,Val(x) \xrightarrow[n\infty]{} +\infty$, donc la série converge.

On en déduit que $(1-x)\sum_{k=0}^{+\infty} x^k = 1$, d'où le résultat. □

On peut maintenant passer à l'inversibilité dans le cas général :

Propriété 3.5. $K((t^{\mathbb{Q}}))$ *est un corps.*

Démonstration. Soit $x \in K((t^{\mathbb{Q}})) \setminus \{0\}$.

On pose $i = Val(x)$. On a $a \in K \setminus \{0\}$ et $y \in K((t^{\mathbb{Q}}))$ tels que $x = at^i(1-y)$ et $Val(y) > 0$. Alors, a est inversible car K est un corps, t^i est inversible, d'inverse t^{-i}, et $1 - y$ est inversible d'après le lemme.

Il vient que x est inversible. □

Pour finir cette section, on mentionnera le théorème suivant :

Théorème 3.6. *Si* K *est algébriquement clos, alors* $K((t^{\mathbb{Q}}))$ *est algébriquement clos.*

Ce théorème étant difficile, on ne le montrera pas. On n'aura pas non plus besoin de l'admettre, car il ne servira pas dans l'étude qui suit.

Par contre, il en justifie l'intérêt, car il assure qu'en étudiant la fermeture algébrique de $\mathbb{F}_q(t)$ dans $\mathbb{F}_q((t^{\mathbb{Q}}))$, on obtient quasiment la clôture algébrique de $\mathbb{F}_q(t)$.

4 Le théorème de Kedlaya

On dispose maintenant de quasiment tous les outils nécessaires pour énoncer la généralisation de Kedlaya du théorème de Christol. Il reste à définir ce qu'est une série de Hahn quasi-automatique.

Définition 4.1 (Ensemble q-(quasi-)automatique)**.** Soit I une partie de $\mathbb{Q}$.

On dit qu'elle est *q-automatique* lorsque $I \subset \mathbb{Z}[\frac{1}{p}] \cap \mathbb{Q}_+$ et que l'ensemble des écritures en base q des éléments de I est un langage rationnel.

On dit qu'elle est *q-quasi-automatique* lorsqu'il existe $a \in \mathbb{N}^*$, $b \in \mathbb{Q}$ tels que $aI+b$ soit q-automatique.

Les rationnels de $\mathbb{Z}[\frac{1}{p}]$, appelés rationnels p-adiques, sont ceux qui ont un développement fini en base p (ou q, c'est équivalent). L'écriture dont il est question est donc un mot sur l'alphabet $\Omega_q = \{0, \dots, q-1, .\}$. Le sens de l'écriture n'ayant aucune importance, on choisira par la suite de placer les chiffres de poids fort à gauche.

Comme les chiffres de l'écriture en base q s'obtiennent par regroupement k par k de ceux de l'écriture en base p (où $k \in \mathbb{N}^*$ tel que $p^k = q$), il est équivalent pour une partie I de $\mathbb{Q}$ d'être p-(quasi-)automatique et q-(quasi-)automatique.

Définition 4.2 (Série de Hahn quasi-automatique)**.** Soit $x = \sum_{i \in \mathbb{Q}} x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$.

On dit que x est *quasi-automatique* lorsque, pour tout $a \in \mathbb{F}_q^*$, $\{i \in \mathbb{Q}, x_i = a\}$ est q-quasi-automatique.

Théorème 4.1 (Kedlaya, [5])**.** *Soit $x \in \mathbb{F}_q((t^{\mathbb{Q}}))$.*

Alors x est algébrique sur $\mathbb{F}_q(t)$ si et seulement si x est quasi-automatique.

Le reste de l'exposé sera consacré à la démonstration de ce théorème. On commencera par quelques lemmes sur les automates, puis on donnera une preuve complète du sens facile (automatique $\Rightarrow$ algébrique, comme pour le théorème de Christol). Quant au sens difficile (algébrique $\Rightarrow$ automatique), on en donnera une preuve presque complète dans la dernière section. Il ne s'agit pas d'une généralisation de la preuve du théorème de Christol ; en fait, elle utilise le théorème.

5 Quelques résultats "automatiques"

Lemme 5.1. *Soit A et B deux alphabets disjoints, et $\Omega = A \cup B$. Soit L un langage rationnel non vide sur Ω, contenu dans A^*BA^*. Soit $\mathcal{A} = (Q, \Delta, i, F)$ un automate déterministe reconnaissant L, où tous les états sont accessibles.*

Alors on peut partitionner Q en Q_0, Q_1, P tels que $i \in Q_0$, $F \subset Q_1$ et

$$\Delta \subset (Q_0 \times A \times Q_0) \cup (Q_0 \times B \times Q_1) \cup (Q_1 \times A \times Q_1) \cup (Q \times \Omega \times P).$$

En particulier, on pourra appliquer le lemme avec $A_q = \{0, \dots, q-1\}$, $B = \{.\}$, $\Omega_q = A_q \cup B$ et L un langage rationnel sur Ω_q ne contenant que des écritures de rationnels p-adiques (on parlera de langages de nombres).

Démonstration. Soit Q_0 l'ensemble des états accessibles (à partir de i) en ne suivant que des transitions étiquetées par des lettres de A, et co-accessibles. Soit Q_1 l'ensemble des états co-accessibles (à partir de F) en ne suivant que des transitions étiquetées par des lettres de A. Soit P l'ensemble des états qui ne sont pas co-accessibles.

On a clairement $i \in Q_0$ (car $L \neq \emptyset$) et $F \subset Q_1$.

Pour montrer que Q_0, Q_1, P forment une partition de Q, il suffit de montrer que Q_0, Q_1 forment une partition de $Q \setminus P$. Supposons que l'on ait $q \in Q_0 \cap Q_1$. Alors q est bi-accessible en ne suivant que des transitions étiquetées par des lettres de A, donc on a un mot de A^* dans L, ce qui contredit l'inclusion $L \subset A^*BA^*$.

Supposons que l'on ait q co-accessible qui ne soit ni dans Q_0 ni dans Q_1. Alors q est accessible, mais à condition d'emprunter une transition étiquetée par une lettre de B. De même, q est co-accessible, mais à condition d'emprunter une transition étiquetée par une lettre de B. On en déduit l'existence d'un mot de L contenant au moins deux lettres de B, ce qui contredit l'inclusion $L \subset A^*BA^*$.

On a

$$\begin{aligned}\Delta =&(\Delta \cap (Q \times \Omega \times P))\\ &\cup(\Delta \cap (P \times \Omega \times (Q_0 \cup Q_1)))\\ &\cup(\Delta \cap (Q_0 \times \Omega \times Q_0))\\ &\cup(\Delta \cap (Q_0 \times \Omega \times Q_1))\\ &\cup(\Delta \cap (Q_1 \times \Omega \times Q_1))\\ &\cup(\Delta \cap (Q_1 \times \Omega \times Q_0)).\end{aligned}$$

On a $\Delta \cap (P \times \Omega \times (Q_0 \cup Q_1)) = \emptyset$ car les états de $Q_0 \cup Q_1$ sont co-accessibles, ce que ne sont pas les états de P. $\Delta \cap (Q_0 \times \Omega \times Q_0) \subset (Q_0 \times A \times Q_0)$ et $\Delta \cap (Q_1 \times \Omega \times Q_1) \subset (Q_1 \times A \times Q_1)$, car sinon on a un mot dans L contenant au moins deux lettres de B. Pour la même raison, $\Delta \cap (Q_1 \times \Omega \times Q_0) = \emptyset$. Enfin, $\Delta \cap (Q_0 \times \Omega \times Q_1) \subset (Q_0 \times B \times Q_1)$ sinon on a un mot de L ne contenant aucune lettre de B. □

Définition 5.1 (fonction q-automatique)**.** Soit O un ensemble fini, $f : \mathbb{Z}[\frac{1}{p}] \to O$. Pour $x \in O$, on pose $A_x = \{i \in \mathbb{Z}[\frac{1}{p}], f(i) = x\}$.

On dit que f est *q-automatique* lorsque les A_x sont des parties q-automatiques de $\mathbb{Q}$.

Lemme 5.2. *Soit V un ensemble fini contenant 0, $f : \mathbb{Z}[\frac{1}{p}] \to V$. On suppose que l'on a $M, c \in \mathbb{N}, N \in \mathbb{N}^*$, tels que :*

- *pour tout x dont la somme des chiffres de son écriture en base q dépasse c, $f(x) = 0$,*
- *pour tout $x = x_0.x_1 \dots x_n$, et pour tout $1 \leq j \leq n$, on a*

$$f(x_0.x_1 \dots x_j \underbrace{0 \dots 0}_{M \text{ zéros}} x_{j+1} \dots x_n) = f(x_0.x_1 \dots x_j \underbrace{0 \dots 0}_{M+N \text{ zéros}} x_{j+1} \dots x_n),$$

où l'on a identifié un rationnel p-adique et son écriture en base q.

Alors f est q-automatique.

Démonstration. Pour $y \in V$, on pose $A_y = \{i \in \mathbb{Z}[\frac{1}{p}], f(i) = y\}$, et B_y l'ensemble des écritures en base q des éléments de A_y. On montre l'existence d'une relation d'équivalence $\sim$ sur Ω_q^* telle que :

- $\sim$ passe au contexte à droite $(\forall x, y \in \Omega_q^*, (x \sim y) \Rightarrow (\forall z \in \Omega_q^*, xz \sim yz))$,
- $\Omega_q^*/\sim$ est un ensemble fini
- les A_y soient des unions de classes d'équivalence de $\sim$.

Le théorème de Nérode permet alors de conclure que les B_y sont rationnels, donc les A_y sont q-automatiques. Finalement, f est automatique. □

Définition 5.2 (Transducteurs)**.** Soit A et B deux alphabets, Q un ensemble fini, $\delta : Q \times A \to Q \times B^*$, $i \in Q$, $f : Q \to B$ On dira que $\mathcal{T} = (Q, i, \delta, f)$ forme un *transducteur (rationnel, déterministe, complet, d'alphabet d'entrée A, d'alphabet de sortie B, de fonction de transition δ).*

On appellera *fonction de transition étendue aux mots*, et on notera encore δ l'application de $Q \times A^*$ vers $Q \times B^*$ qui prolonge la fonction de transition et telle que

$$\forall q, q' \in Q, \forall a, a' \in A^*, \forall b, b' \in B^*, (\delta(q, a) = (q', b) \text{ et } \delta(q', a') = (q'', b')) \Rightarrow \delta(q, aa') = (q'', bb')$$

On définit ensuite la *transduction (rationnelle, déterministe)* $F : A^* \to B^*$ associée à $\mathcal{T}$ par

$$F : \begin{array}{ccc} A^* & \to & B^* \\ a & \mapsto & bf(q) \end{array} \quad \text{où } \delta(i, a) = (q, b)$$

On admettra le théorème suivant, démontré par exemple dans [1] :

Théorème 5.3. *L'image par une transduction rationnelle d'un langage rationnel est un langage rationnel.*

6 Une série quasi-automatique est algébrique

Les deux premiers lemmes sont purement algébriques.

Lemme 6.1. *Soit $K \to L$ une extension de corps de caractéristique p, $\sigma : L \to L$ l'endomorphisme de Frobenius, et soit $x \in L$.*

Alors x est algébrique sur K si et seulement s'il existe $P \in K[X] \setminus \{0\}$ tel que $P(\sigma)(x) = 0$.

Démonstration. Si x est algébrique sur K, on a $K' = K(x)$ de dimension finie sur K. La famille infinie $(sigma^k(x))_{k\in\mathbb{N}}$ est donc liée, on a donc une combinaison linéaire non triviale qui l'annule, ce qui correspond à un polynôme de σ annulant x.

Rêciproquement, si on a $P \in K[X] \setminus \{0\}$ tel que $P(\sigma)(x) = 0$, alors $P(\sigma)$ est un polyôme sur K, non nul, et qui annule x. Donc x algébrique sur K. □

Lemme 6.2. *Soit $K \to L$ une extension de corps de caractéristique p, et σ l'endomorphisme de Frobenius de L. Soient $A, B \in M_n(K)$, avec au moins l'une des deux matrices inversibles, $w \in K^n$. On suppose en outre que l'on a $v \in L^n$ tel que $Av^\sigma + Bv = w$, où l'on a noté v^σ l'application de σ á chaque composante de v. Alors les composantes de v sont algébriques sur K.*

Démonstration. On traite séparément le cas où A est inversible et celui où B est inversible.

- Premier cas : A est inversible.
  Alors $v^\sigma = A^{-1}w - A^{-1}Bv$.
  De même, pour $i > 0$, on peut écrire $v^{\sigma^i} = w_i + A_i v$, avec $w_i \in K^n, A_i \in M_n(K)$. La famille des (w_i, A_i) est liée (sur K) dès que l'on considère plus de $n^2 + n + 1$ termes, donc celle des $w_i + A_i v$ aussi. Il vient que l'on a $P \in K[X]$ tel que $P(\sigma)(v) = 0$.
  Finalement, les composantes de v sont algébriques sur K.
- Deuxième cas : B est inversible.
  On peut, quitte à agrandir L, supposer que L est clos par racine p-ième. Alors σ est bijectif. On pose ensuite $K' = \{x \in L, \exists i \in \mathbb{N}, \sigma^i(x)(= x^{p^i}) \in K\}$. K' est un sous-corps de L, algébrique sur K, sur lequel σ induit un automorphisme.
  On a $v = B^{-1}w + B^{-1}Av^\sigma$. On en déduit, pour $i \in \mathbb{N}$, l'existence de $A_i \in M_n(K'), w_i \in K'^n$ tels que $v^{\sigma^{-i}} = w_i + A_i v$. On conclut, de même que précédemment, que les composantes de v sont algébriques sur K', donc sur K.

□

On se donne $x \in \mathbb{F}_q((t^{\mathbb{Q}}))$ quasi-automatique pour le reste de la démonstration.

De même que pour le théorème de Christol, on va se ramener, à l'aide de deux nouveaux lemmes, au cas où x est de la forme $x = \sum_{i\in I} t^i$ avec I partie bien ordonnée et q-automatique de $\mathbb{Q}$, où l'on saura conclure.

Lemme 6.3. *On pose $x = \sum_{i\in\mathbb{Q}} x_i t^i$. Pour $u \in \mathbb{F}_q^*$, posons $I_u = \{i \in \mathbb{Q}, x_i = u\}$, et $x_u = \sum_{i\in I_u} t^i$. Si x est quasi-automatique, alors les I_u sont q-quasi-automatiques. Si les x_u sont algébriques (sur $\mathbb{F}_q(t)$), alors x l'est aussi.*

Démonstration. Pour le premier point, c'est la définition d'être quasi-automatique. Pour le second, il suffit d'écrire $x = \sum_{u\in\mathbb{F}_q^*} ux_u$, et de rappeler que la fermeture algébrique de $\mathbb{F}_q(t)$ dans $\mathbb{F}_q((t^{\mathbb{Q}}))$ est un surcorps de $\mathbb{F}_q(t)$, en particulier un $\mathbb{F}_q$-espace vectoriel. □

Lemme 6.4. *Soit $y = \sum_{i\in I} t^i$, avec $I \subset \mathbb{Q}$ bien ordonnée. Soient $a \in \mathbb{N}^*$ et $b \in \mathbb{Q}$, $J = aI + b$. Soit enfin $z = \sum_{j\in J} t^j$.*

Alors y est algébrique (sur $\mathbb{F}_p(t)$ ou sur $\mathbb{F}_q(t)$, c'est équivalent) si et seulement si z l'est.

Démonstration. On va travailler d'une part sur les translations, d'autre part sur les applications linéaires. Les transformations affines envisagées dans ce lemme se décomposant toutes en composées de telles transformations, le lemme en découlera.

- Premier cas : $a = 1$, b quelconque.
  Dans ce cas, $z = yt^b$. t^b étant algébrique, il vient l'équivalence souhaitée.
- Deuxième cas : a quelconque, $b = 0$.
  Soit $\tau : \begin{matrix} \mathbb{F}_p((t^{\mathbb{Q}})) & \to & \mathbb{F}_p((t^{\mathbb{Q}})) \\ x(t) & \mapsto & x(t^a) \end{matrix}$. τ est un automorphisme de corps de $\mathbb{F}_p((t^{\mathbb{Q}}))$, et on a $z = \tau(y)$.
  Ainsi, si $P \in \mathbb{F}_p(t)[X]$ annule y alors P^τ annule z (où τ agit sur P coefficient par coefficient). Or, τ laisse stable $\mathbb{F}_p(t)$, donc $P^\tau \in \mathbb{F}_p(t)[X]$, et z algébrique. Réciproquement, si $P \in \mathbb{F}_p(t)[X]$ annule z, alors $P^{\tau^{-1}}$ annule y. On a $\tau^{-1}\langle F_p(t)\rangle = \mathbb{F}_p(t^{\frac{1}{a}})$, donc $P^{\tau^{-1}} \in \mathbb{F}_p(t^{\frac{1}{a}})[X]$. Il vient que y algébrique sur $\mathbb{F}_p(t^{\frac{1}{a}})$, qui est lui-même algébrique sur $\mathbb{F}_p(t)$.

□

Dans le cas où $a = p$, la preuve se simplifie en remarquant qu'alors $z = y^p$ L'équivalence recherchée est alors immédiate.

Lemme 6.5. *Soit I partie bien ordonnée et p-automatique de $\mathbb{Q}$, et $y = \sum_{i \in I} t^i$.*

Alors y algébrique (sur $\mathbb{F}_p(t)$ ou $\mathbb{F}_q(t)$, c'est équivalent).

Démonstration. Soit L le langage sur $\Omega = \{0, \ldots, p-1, .\}$ formé par l'ensemble des écritures en base p des éléments de I. I est p-automatique, donc L est rationnel.

Soit $\mathcal{A} = (Q, \Delta, i, F)$ automate déterministe complet le reconnaissant, dont tous les états sont accessibles. On pose $\delta : Q \times \Omega \to Q$ sa fonction de transition, étendue aux mots. Comme L est un langage de nombres (ses mots contiennent une et une seule fois le symbole .), on peut décomposer Q en Q_0, Q_1, P comme dans le premier lemme.

Pour $q \in Q_0$, on pose T_q l'ensemble des $n \in \mathbb{N}$ dont l'écriture s (sans le point final) est telle que $\delta(i, s) = q$, et $U_q = \{(q', d) \in Q_0 \times A_q, \delta(q', d) = q\}$. Puis $f(q) = \sum_{j \in T_q} t^j$.

On a alors :

$$T_q = \bigcup_{(q',d) \in U_q} pT_{q'} + d \qquad \text{si } q \neq i$$

$$T_q = \bigcup_{(q',d) \in U_q} pT_{q'} + d \cup \{0\} \qquad \text{si } q = i$$

Dans tous les cas, ces unions sont disjointes.

On en déduit que :

$$f(q) = \sum_{(q',d) \in U_q} t^d f(q')^p \qquad \text{si } q \neq i$$

$$f(q) = \sum_{(q',d) \in U_q} t^d f(q')^p + 1 \qquad \text{si } q = i$$

(On rappelle qu'en caractéristique p l'élévation à la puissance p est un endomorphisme de corps).

Par le deuxième lemme "algébrique", il vient que les $f(q)$ $(q \in Q_0)$ sont tous algébriques sur $\mathbb{F}_p(t)$.

On définit de manière similaire, pour $q \in Q_1$, T_q l'ensemble des $i \in \mathbb{Z}[\frac{1}{p}] \cap [0, 1[$ dont l'écriture s (sans le point initial) est telle que $\delta(q, s) \in F$, puis $f(q) = \sum_{j \in T_q} t^j$.

On a alors des relations analogues entre les T_q $(q \in Q_1)$, d'où l'on déduit les relations :

$$f(q) = \sum_{d=0}^{p-1} t^d f(\delta(q, d))^p \qquad \text{si } q \notin F$$

$$f(q) = \sum_{d=0}^{p-1} t^d f(\delta(q, d))^p + 1 \qquad \text{si } q \in F$$

Le deuxième lemme "algébrique" permet à nouveau de conclure que les $f(q)$ $(q \in Q_1)$ sont algébriques.

On pose maintenant $J = \{(q, q') \in Q_0 \times Q_1, (q, ., q') \in \Delta\}$.

Alors $y = \sum_{(q,q') \in J} f(q) f(q')$, qui est donc algébrique.

□

Le théorème est conséquence immédiate des trois lemmes précédents.

7 Une série algébrique est quasi-automatique

Ici nous allons montrer qu'une série $x \in \mathbb{F}_q((t^{\mathbb{Q}}))$ algébrique sur $\mathbb{F}_q(t)$ est nécessairement p-quasi-automatique. Pour cela, nous allons utiliser la caractérisation des séries algébriques sur $\mathbb{F}_q((t))$, puis le théorème de Christol.

Pour énoncer cette caractérisation, nous allons utiliser la notation suivante.

Notation 7.1. Pour $c \in \mathbb{N}$, notons

$$T_c = \{n - b_1 p - b_2 p^2 - \cdots \mid n \in \mathbb{N}, b_i \in \{0, \ldots, p-1\}, \sum_i b_i \leq c\}.$$

La caractérisation des séries algébriques sur $\mathbb{F}_q((t))$ s'énonce alors comme suit :

Proposition 7.1. *Pour tout $x = \sum_i x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$, x est algébrique sur $\mathbb{F}_q((t))$ si et seulement s'il existe $a, b, c, M, N \in \mathbb{N}$ tels que*

(a) $\{i \in \mathbb{Q} \mid x_{\frac{i-b}{a}} \neq 0\} \subset T_c$.

(b) toute suite de la forme

$$c_n := x_{(m-b-b_1 p^{-1} - \cdots - b_{j-1} p^{-j+1} - p^{-n}(b_j p^{-j} + \ldots))/a} = x_{(m-b.b_1 \ldots b_{j-1} \underbrace{0 \ldots 0}_{n \text{ zéros}} b_j \ldots)/a}$$

avec $j \in \mathbb{N}$, $m \in \mathbb{N}^*$ et $b_i \in \{0, \ldots p-1\}$ une suite telle que $\sum b_i \leq c$, devient N-périodique à partir du rang M.

Cela implique de plus que pour tout triplet (a, b, c) vérifiant (a), il existe des entiers M et N qui vérifient (b).

Pour la démonstration de cette propriété, nous vous renvoyons vers [4]. Remarquons que pour une série x algébrique sur $\mathbb{F}_q((t))$, on peut toujours trouver a, b, c, M et N qui vérifient les conditions du critère et tels que $\{i \in \mathbb{Q} \mid x_{\frac{i-b}{a}} \neq 0\} \subset \mathbb{Q}_+^*$.

Utilisons cette caractérisation pour traiter un cas particulier, complémentaire en quelque sorte au cas du théorème de Christol.

Lemme 7.2. *Soit $x = \sum_i x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ une série à support dans $]0, 1] \cap T_c$ avec $c \in \mathbb{N}$, qui est algébrique sur $\mathbb{F}_q((t))$. Alors, x est p-automatique.*

Démonstration. La partie (a) du critère s'applique ici avec $a = 1$, $b = 0$ et la valeur de c fournie dans l'énoncé. Donc, chaque suite (c_n) de la forme

$$c_n = x_{1 - b_1 p^{-1} - \ldots - b_{j-1} p^{-j+1} - p^{-n}(b_j p^{-j} + \ldots)}$$

avec $b_i \in \{0, \ldots, p-1\}$ telle que $\sum b_i \leq c$, devient N-périodique à partir d'un rang fixe M.

Considérons la relation d'équivalence suivante sur $T_c \cap [0, 1[$. On pose $x \sim y$ si on peut passer de l'écriture de x en base p à celle de y en itérant l'opération suivante : on remplace une suite de $M + vN$ zéros consécutifs par une suite de $M + wN$ zéros consécutifs (v et w peuvent être des entiers naturels quelconques). La partie (b) du critère affirme alors exactement que $i \sim j$ implique $x_{1-i} = x_{1-j}$ pour tous $i, j \in T_c \cap]0, 1]$. On a alors un ensemble fini de classes d'équivalence. Donc, la fonction $f : \mathbb{Z}[\frac{1}{p}] \to \mathbb{F}_q$ définie par $f(i) = x_{1-i}$ est p-automatique. Donc, x est aussi p-automatique (car il existe un transducteur qui effectue la transformation $i \mapsto 1 - i$). □

Comme x est p-automatique, x est aussi algébrique sur $\mathbb{F}_q(t)$. D'autre part, on voit qu'une fois les entiers c, M et N sont fixés, x est déterminé par un nombre fini de ses coefficients. On peut obtient donc $x \in V(q, c, M, N)$, et les ensembles $V(q, c, M, N)$ sont finis.

Le lemme suivant donne un exemple de l'argument de "découpage d'une série de Hahn suivant la partie entière" qu'on utilisera aussi dans la démonstration principale.

Lemme 7.3. *Soient $x_1, \ldots, x_m \in \mathbb{F}_q((t^{\mathbb{Q}}))$ des séries à supports inclus dans $]0, 1]$, linéairement liées sur $\mathbb{F}_q((t))$. Alors, elles sont linéairement liées sur $\mathbb{F}_q$.*

Démonstration. Comme $x_1, \ldots, x_m$ sont linéairement liés, on obtient une relation entre eux de la forme $c_1 x_1 + \cdots + c_m x_m = 0$ avec $c_i \in \mathbb{F}_q[[t]]$. Écrivons $c_i = \sum_{j=0}^{\infty} c_{i,j} t^j$ avec $c_{i,j} \in \mathbb{F}_q$. On obtient alors une égalité

$$\sum_{j=0}^{\infty} \left(\sum_{i=1}^{m} c_{i,j} x_i t^j \right).$$

Or, le support de chaque terme entre parenthèses est inclus dans $]j, j+1]$, et ces supports sont deux-à-deux disjoints. Donc, tous ces termes doivent être nuls c'est-à-dire $\sum_{i=1}^{m} c_{i,j} x_i = 0$ pour tout $j \in \mathbb{N}$. Les coefficients $c_{i,j}$ n'étant pas tous nuls, on obtient une relation linéaire entre les x_i avec des coefficients dans $\mathbb{F}_q$. □

Montrons maintenant le théorème principal.

Théorème 7.4. *Soit $x = \sum x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ une série de Hahn algébrique sur $\mathbb{F}_q(t)$. Alors, x est p-quasi-automatique.*

Démonstration. Soient a, b, c, M, N des entiers du critère d'algébricité sur $\mathbb{F}_q((t))$, et tels que la série $y = \sum_i x_{(i-b)/a} t^i = \sum_i y_i t^i$ soit à support dans $\mathbb{Z}[\frac{1}{p}] \cap \mathbb{Q}^+$. Alors, y est aussi algébrique sur $\mathbb{F}_q(t)$ d'après le lemme 6.4, et $Supp(y) \subset T_c$. D'après le lemme 6.1, la série $(y - y_0)$ est racine d'un polynôme de la forme $P(z) = \sum_{i=0}^{m} c_i z^{q^i}$. On suppose que $c_m \neq 0$ et que, si on note l le plus petit indice tel que $c_l \neq 0$, on obtient $c_l = 1$.

Notons $V = V(q, c, M, N)$. C'est un $\mathbb{F}_q$-espace vectoriel de dimension finie, et on note $v_1, \ldots, v_r$ une de ses bases. D'après le lemme précédent, c'est aussi une famille libre sur $\mathbb{F}_q((t))$.

En décomposant la série $(y - y_0)$ suivant la partie entière supérieure des exposants (rappelons que $Supp(y - y_0) \subset T_c \cap \mathbb{Q}_+^*$), on obtient $y - y_0 = \sum_{j=0}^{\infty} v_j t^j$ avec $Supp(v_j) \subset]0, 1]$. On a alors $v_j \in V$. Donc, y est une combinaison linéaire d'éléments de V à coefficients dans $\mathbb{F}_q[[t]]$. De même pour les séries $(y - y_0)^{q^i}$, qu'on développera donc sous la forme $(y - y_0)^{q^i} = \sum_{j=1}^{r} a_{i,j} v_j$ avec $a_{i,j} \in \mathbb{F}_q[[t]]$. Nous allons montrer que les $a_{i,j}$ sont algébriques sur $\mathbb{F}_q(t)$ pour chaque $i \in \{l, \ldots, m-1\}$.

Notons pour chaque $j \in \{1, \ldots, r\}$:

$$v_j^q = \sum_{h=1}^{r} b_{j,h} v_h$$

avec $b_{j,h} \in \mathbb{F}_q[t]$. On obtient alors pour tout $i \in \{l+1, \ldots, m\}$, $j \in \{1, \ldots, r\}$:

$$a_{i,j} = \sum_{h=1}^{r} b_{h,j} a_{i-1,h}^q.$$

Ensuite, l'égalité $P(y - y_0) = 0$ s'exprime sous la forme

$$(y - y_0)^{q^l} = -c_{l+1} \left((y - y_0)^{q^l} \right)^q - \ldots - c_m \left((y - y_0)^{q^{m-1}} \right)^q,$$

d'où

$$\begin{aligned} \sum_{j=1}^{r} a_{l,j} v_j &= \sum_{i=l}^{m-1} -c_{i+1} \left(\sum_{h=1}^{r} a_{i,h} v_h \right)^q \\ &= \sum_{i=l}^{m-1} -c_{i+1} \sum_{h=1}^{r} \sum_{j=1}^{r} a_{i,h}^q b_{h,j} v_j. \end{aligned}$$

En réécrivant cette égalité coordonnée par coordonnée (car les v_j sont linéairement indépendants sur $\mathbb{F}_q((t))$), on obtient des équations de la forme

$$a_{l,j} = \sum_{i=l}^{m-1} \sum_{h=1}^{r} d_{i,h,j} a_{g,h}^q$$

avec $d_{i,h,j} \in \mathbb{F}_q(t)$.

Ces égalités forment un système d'équations auquel on peut appliquer le lemme 6.1 (avec $v = (a_{i,j})_{\substack{i = l, \ldots, m-1, \\ j = 1, \ldots, r}}$, $w = 0$, $B = -Id$). Donc, les $a_{i,j}$ sont algébriques.

D'après le théorème de Christol, les $a_{i,j}$ sont automatiques. Montrons que $(y - y_0)^{q^l}$ est aussi une série p-automatique. Décomposons-la sous la forme

$$(y - y_0)^{q^l} = \sum_{j=1}^{r} a_{l,j} v_j = \sum_{k=0}^{\infty} w_k t^k$$

avec $Supp(w_k) \subset]0, 1]$. On a alors $w_k = \sum_{j=1}^{r} a_{l,j(k)} v_j \in V$, où $a_{l,j(k)}$ est le coefficient d'indice k de la série $a_{l,j}$. La fonction $\mathbb{N} \to V, k \mapsto w_k$. est donc automatique (pour calculer w_k il suffit de calculer simultanément tous les $a_{l,j(k)}$). Les coefficients de $(y - y_0)^{q^l}$ sont alors calculés par un automate fini qui commence par lire la partie entière k de l'indice donné i (jusqu'au symbole ".") puis calcule le coefficient de w_k à partir de la partie fractionnaire de i.

Comme $(y - y_0)^{q^l}$ est p-automatique, $(y - y_0)$ est p-quasi-automatique. On en déduit que y et x le sont aussi. □

8 Conclusion

Il reste toujours le problème d'approche algorithmique. La démonstration de l'implication automatique $\Rightarrow$ algébrique donnée ici est constructive, mais celle de la proposition 7.1 (donnée dans [4]) ne l'est pas. Une preuve constructive de l'implication algébrique $\Rightarrow$ automatique est toutefois possible, mais beaucoup plus complexe. Elle est donnée dans [5].

Références

[1] J. Berstel. *Transductions and Context-Free Languages.* B.G. Teubner, 1979.

[2] Gilles Christol. Ensembles presque périodiques k-reconnaissables. *Theoretical Computer Science*, 9 :141–145, 1979.

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

[4] Kiran S. Kedlaya. The algebraic closure of the power series field in positive characteristic, 1998.

[5] Kiran S. Kedlaya. Finite automata and algebraic extensions of function fields, 2004.

[6] D.S. Passman. *The Algebraic Structure of Group Rings.* Wiley, 1977.