Introduction au domaine de recherche

Équations polynômiales sur le corps $\mathbb{F}_q(t)$ et automates finis

Christophe Rose

encadré par Federico Pellarin

Introduction

Soit K un corps, et $K(t)$ son corps des fractions rationnelles en une indéterminée. Nous cherchons à caractériser les racines des polynômes non nuls de $K(t)[X]$, où X est une inconnue indépendante de t. Ces racines sont contenues dans une clôture algébrique de $K(t)$, qu'on définira par la suite.

Commençons par remarquer que cette clôture algébrique contient des séries formelles dont les exposants peuvent tendre vers $+\infty$. Pour $K = \mathbb{R}$, la série de Laurent

$$\sum_{n=0}^{+\infty} \frac{\frac{1}{2} \cdot \frac{-1}{2} \cdots (\frac{3}{2} - n)}{n!} t^n \in \mathbb{R}((t))$$

a pour carré $1 + t$.

La clôture algébrique contient également les racines des polynômes $X^i - t^j$ pour $i, j \in \mathbb{Z}$, $j \neq 0$, donc des éléments de la forme t^r avec $r \in \mathbb{Q}$.

Le corps des séries de Puiseux $K((t^{1/\infty})) = \bigcup_{n \geq 1} K((t^{1/n}))$ est l'ensemble des séries de Laurent en $t^{1/n}$ pour un certain entier n.

Un théorème de Puiseux [Ser79, Chapitre 2.4] dit que si K est algébriquement clos et de caractéristique 0, alors $K((t^{1/\infty}))$ est algébriquement clos.

Ce résultat est faux si K est de caractéristique $p > 0$: le polynôme $X^p - X - 1/t$ n'a pas de solutions dans $\overline{\mathbb{F}_p}((t^{1/\infty}))$. Il faut alors se placer dans un corps encore plus grand, le corps des séries de Hahn noté $K((t^{\mathbb{Q}}))$, que nous définirons plus tard. Il est constitué de séries formelles $\sum_{i \in \mathbb{Q}} x_i t^i$, où les x_i sont dans K. On peut montrer [Ked01, Proposition 1] que si K est algébriquement clos, alors $K((t^{\mathbb{Q}}))$ l'est aussi.

Le théorème de Kedlaya, qui est l'objet de cette présentation, dit qu'une série de Hahn de $\mathbb{F}_q((t^{\mathbb{Q}}))$ est algébrique sur $\mathbb{F}_q(t)$ si et seulement si elle est *p-quasi-automatique*, c'est-à-dire que ses coefficients sont « engendrés » d'une certaine manière par un *automate fini*.

Kedlaya a donné une preuve constructive de son théorème, qui permet à partir d'un polynôme de $\mathbb{F}_q(t)[X]$, de calculer explicitement ses racines dans $\overline{\mathbb{F}_q}((t^{\mathbb{Q}}))$.

Les deux premières sections introduisent le concept de série de Hahn et d'automates finis. Après avoir énoncé les théorèmes principaux, nous décrirons un algorithme pour calculer les racines des polynômes de $\mathbb{F}_q(t)[X]$.

1 Séries de Hahn et algébricité

On commence par quelques rappels d'algèbre.

Définition. Soit L/K une extension de corps. On dit qu'un élément x de L est *algébrique sur* K s'il existe un polynôme P de $K[X]$, non nul, tel que $P(x) = 0$.

Proposition 1.1. *Soit L/K une extension de corps et x un élément de L. Alors x est algébrique sur L si et seulement si $K[x]$ est un K-espace vectoriel de dimension finie.*

Proposition 1.2. *Soit L/K une extension de corps. Si x et y sont deux éléments de L qui sont algébriques sur K, alors leur somme $x + y$ et leur produit xy sont des éléments de L algébriques sur K.*

Si x est un élément non nul du corps L algébrique sur K, alors son inverse $1/x$ est un élément de L algébrique sur K.

Nous allons généraliser les séries formelles en les écrivant sous la forme $\sum_{i\in\mathbb{Q}} x_i t^i$ avec les $x_i \in K$. Pour définir la valuation, l'addition et la multiplication sur ces séries de Hahn, nous aurons besoin d'imposer des conditions sur ces séries. Des définitions et des preuves détaillées sont disponibles dans [Pas77, Chapitre 13].

Définition. Soit K un corps. On appelle *série de Hahn* sur le corps K (ou *série de Hahn-Mal'cev-Neumann*) une série formelle $\sum_{i\in\mathbb{Q}} f(i)t^i$ où f est une fonction de $\mathbb{Q}$ vers K dont le *support* $\mathrm{Supp}(f) = \{i \in \mathbb{Q} | f(i) \neq 0\}$ est *bien ordonné*, c'est-à-dire tel que tout sous-ensemble non vide possède un minimum. On note $K((t^{\mathbb{Q}}))$ l'ensemble des séries de Hahn sur K.

Proposition 1.3. *L'ensemble $K((t^{\mathbb{Q}}))$ est un corps valué pour les valuation, addition et multiplication suivantes, qui sont bien définies.*

Si $x = \sum x_i t^i \in K((t^{\mathbb{Q}}))$, on définit sa valuation comme le minimum de son support si x est non nul, et $+\infty$ si $x = 0$.

Si $x = \sum x_i t^i$ et $y = \sum y_i t^i$ sont deux séries de Hahn, on définit la somme et le produit de x et de y de la manière suivante : $x + y = \sum_{i\in\mathbb{Q}}(x_i + y_i)t^i$ et $xy = \sum_{k\in\mathbb{Q}} \left(\sum_{i+j=k} x_i y_j\right) t^k$.

Les éléments neutres de l'addition et de la multiplication sont respectivement les séries de Hahn $0_K t^0$ et $1_K t^0$.

Proposition 1.4. *Si K est un corps et t une indéterminée, alors on a les inclusions de corps suivantes. $K(t) \subset K((t)) \subset K((t^{1/\infty})) = \bigcup_{n\in\mathbb{N}^*} K((t^{1/n})) \subset K((t^{\mathbb{Q}}))$.*

Dans toute la suite, nous étudierons les séries de Hahn de $\mathbb{F}_q((t^{\mathbb{Q}}))$, où $q = p^e$, p étant un nombre premier et $e > 0$ un entier. Il y a exactement un corps à q éléments à isomorphisme près.

La proposition suivante est facile à démontrer.

Proposition 1.5. *Soit $a > 0$ et b deux rationnels, et $x = \sum_{i\in\mathbb{Q}} f(i)t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$. Considérons la série $x' = \sum_{i\in\mathbb{Q}} f(i)t^{ai+b} = \sum_{i\in\mathbb{Q}} f((i-b)/a)t^i$. Alors x' est une série de Hahn.*

De plus, x est algébrique sur $\mathbb{F}_q(t)$ si et seulement si x' est algébrique sur $\mathbb{F}_q(t)$.

Le fait d'appliquer une transformation affine sur les exposants des termes d'une série de Hahn s'appelle la *décimation*. Étant donnée une série de Puiseux, on peut lui appliquer la décimation pour obtenir une série entière.

2 Automates finis et combinatoire des mots

Les automates finis sont des machines formelles qui lisent des suites finies de lettres (les *mots*) et qui renvoient une valeur dans un ensemble fini, généralement $\{0, 1\}$. Ils sont d'usage commun en informatique. Entre autres, ils sont très efficaces pour rechercher une chaîne de caractères dans une autre.

Définition. On se donne un ensemble A fini et non vide, qu'on appelle l'*alphabet*. Ses éléments sont appelés les *lettres*. Pour i un entier naturel, on écrit les éléments du produit cartésien A^i par juxtaposition : ainsi (a, b, b) s'écrit plus simplement abb. On appelle ces éléments les *mots* de *longueur* i. Il n'y a qu'un seul mot de longueur 0, qu'on note ε.

Définition. On note $A^* = \bigcup_{i\in\mathbb{N}} A^i$ l'ensemble des mots sur l'alphabet A. On dit également que A^* est l'*étoile* de A, ou le *monoïde libre* sur l'alphabet A. Si $u = u_1 \dots u_m$ et $v = v_1 \dots v_n$ sont deux mots, le *concaténé* de u et de v est le mot $uv = u_1 \dots u_m v_1 \dots v_n$ obtenu par juxtaposition des lettres.

Ainsi, $\varepsilon u = u\varepsilon = u$ pour tout mot $u \in A^*$.

Définition. On appelle *langage* (sur l'alphabet A) un sous-ensemble quelconque de A^*.

Comme décrit précédemment, on peut voir une série de Hahn dans $\mathbb{F}_q((t^{\mathbb{Q}}))$ comme une fonction $f : \mathbb{Q} \to \mathbb{F}_q$ qui vérifie certaines propriétés. Mais comme $\mathbb{F}_q$ est fini, on peut la voir également comme une partition de $\mathbb{Q}$ en ensembles $(E_\alpha)_{\alpha\in\mathbb{F}_q}$ où $E_\alpha = \{i \in \mathbb{Q} | f(i) = \alpha\}$.

Remarque. Les E_α sont bien ordonnés sauf pour $\alpha = 0$.

Nous aurons besoin de coder les éléments des ensembles $E_\alpha \subset \mathbb{Q}$ pour les faire lire par des automates finis. Pour cela, nous utilisons les écritures des rationnels dans une certaine base b.

Définition. Fixons b un entier naturel supérieur ou égal à 2, qu'on appelle la *base*. On note $S_b = \mathbb{Q}^+ \cap \mathbb{Z}[1/b]$ l'ensemble des nombres rationnels positifs qui ont un nombre fini de chiffres après la virgule lorsqu'ils sont écrits en base b.

Définition. Soit $A_b = \{"0"; \dots; "b-1"; ","\}$ un alphabet à $b+1$ lettres, et Σ_b le langage sur A_b des mots de A_b^* qui ne contiennent qu'une seule virgule, et qui ne commencent ni ne se terminent par 0.

On voit facilement que l'ensemble des écritures des éléments de S_b est contenu dans le langage Σ_b, quitte à prendre la convention que 0 s'écrit ",", que les nombres entiers se terminent par une virgule et que les éléments strictement plus petits que 1 commencent par une virgule.

Inversement, à un élément de Σ_b de la forme "u, v", on lui associe sa *valeur* : $\sum_{i=1}^{m} u_i b^{m-i} + \sum_{i=1}^{n} v_i b^{-i}$, qui est un élément de S_b.

Définition. Un *automate (fini déterministe complet) à sortie* est un 6-uplet $(Q, A, i, \delta, \Delta, \tau)$ où :
- Q est un ensemble fini (l'ensemble des *états*) ;
- A est un ensemble fini (*l'alphabet d'entrée*) ;
- i est un élément de Q (*l'état initial*) ;
- δ est une fonction de $Q \times A$ dans Q (*la fonction de transition*) ;
- Δ est un ensemble fini (*l'ensemble de sortie*) ;

– τ est une fonction de Q dans Δ (*la fonction de sortie*).

Généralement, on dessine aussi une flèche non étiquetée qui rentre dans l'état i et des flèches qui sortent de chaque état q de Q, ces flèches étant étiquetées par $\tau(q)$.

Comme exemple, voici le graphe de transition de l'automate $(\{q_0, q_1\}, \{0,1\}, q_0, \{(q_0,0,q_0),(q_0,1,q_1),(q_1,0,q_1),(q_1,1,q_0)\}), \{0,1\}, \tau)$, où $\tau(q_0) = 0$ et $\tau(q_1) = 1$.

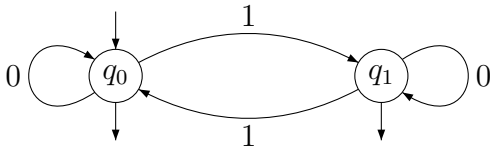

FIG. 1 – Exemple d'automate (automate de Thue-Morse)

Définition. On étend la fonction $\delta : Q \times A \to Q$ à la fonction $\delta^* : Q \times A^* \to Q$ défini de la façon suivante : si u est un mot de longueur n, alors $\delta^*(q_0, u) = q_n$ si et seulement s'il existe des états $q_1, \ldots, q_{n-1}$ tels que $q_0 \xrightarrow{u_1} q_1 \xrightarrow{u_2} \ldots \xrightarrow{u_{n-1}} q_{n-1} \xrightarrow{u_n} q_n$. On écrit alors $q_0 \xrightarrow{u} q_n$.

Définition. On associe à cet automate la fonction $f : A^* \to \Delta$ qui à un mot u associe $\tau(q)$ où q est l'état tel que $i \xrightarrow{u} q$. Deux automates sont dits *équivalents* s'ils ont la même fonction associée.

Exemple. La fonction associée à l'automate de Thue-Morse associe à un mot contenant un nombre pair de 1 la valeur 0, et à un mot contenant un nombre impair de 1 la valeur 1.

Il existe un algorithme simple, dont l'implémentation est rapide et nécessite peu de mémoire, pour calculer la valeur prise en un certain mot $u \in A^*$ par la fonction f associée à un automate fini déterministe complet à sortie.

On part de l'état initial, puis on lit successivement de gauche à droite chaque lettre du mot. À chaque lettre a lue, on passe de l'état q à l'état $\delta(q, a)$. On se retrouve après avoir lu toutes les lettres dans un certain état q'. On connaît alors $f(u) = \tau(q')$.

Définition. Soient A et Δ des ensembles finis. Une fonction $f : A^* \to \Delta$ est dite *automatique* s'il existe un automate à sortie $(Q, A, i, \delta, \Delta, \tau)$ associé à cette fonction.

Définition. Un langage L sur l'alphabet A est dit *rationnel* (ou *régulier*) si sa fonction caractéristique dans A^* est une fonction automatique.

Définition. Une fonction $f : S_b \to \Delta$ (où Δ est un ensemble fini) est dite *b-automatique* s'il existe un automate à sortie qui à l'écriture d'un élément $x \in S_b$ en base b renvoie $f(x)$. Une suite $(a_i)_{i\in\mathbb{N}}$ est dite *b-automatique* s'il existe un automate à sortie qui à l'écriture d'un entier i en base b renvoie a_i.

Définition. Un sous-ensemble S de $\mathbb{Q}$ est dit *b-rationnel* (ou *b-régulier*) s'il est inclus dans S_b et si sa fonction caractéristique dans S_b est b-automatique.

La proposition suivante est montrée dans le [AS03, Chapitre 4.3] et dans le [Sak03, Chapitre 4].

Proposition 2.1. *Soit S un sous-ensemble de S_b, et r et s deux entiers naturels avec $r > 0$ tels que $rS + s$ est inclus dans S_b. Alors S est b-rationnel si et seulement si $rS + s$ est b-rationnel.*

3 Théorèmes principaux

Nous allons maintenant étudier les séries de Hahn à la lumière des automates finis.

Définition. Soit $x = \sum_{i\in\mathbb{N}} x_i t^i$ une série entière dans $\mathbb{F}_q[[t]]$. Elle est dite *p-automatique* si la suite $(x_i)_{i\in\mathbb{N}}$ est p-automatique.

Définition. Soit $x = \sum_{i\in\mathbb{Q}} f(i)t^i = \sum_{i\in\mathbb{Q}} x_i t^i$ une série de Hahn dans $\mathbb{F}_q((t^{\mathbb{Q}}))$. Elle est dite *p-quasi-automatique* si les deux assertions suivantes sont vérifiées :

1. Il existe $a > 0$ et b deux entiers tels que $f((i-b)/a)$ a son support inclus dans S_p, c'est-à-dire qu'il est formé de rationnels positifs qui s'écrivent avec un nombre fini de chiffres après la virgule en base p.
2. Pour des entiers $a > 0$ et b qui vérifient l'assertion précédente, la fonction $f((i-b)/a)$ est p-automatique.

Si une série de Hahn p-quasi-automatique a son support inclus dans S_p (c'est-à-dire que la première assertion est vérifiée pour $a = 1$ et $b = 0$), alors on dit qu'elle est *p-automatique*.

Remarque. Par la proposition 2.1, si la deuxième assertion est vérifiée pour certains $a > 0$ et b entiers, elle l'est pour tous entiers $a > 0$ et b qui vérifient la première assertion.

Proposition 3.1. *Si on regarde $x \in \mathbb{F}_q(t)$ comme un élément de $\mathbb{F}_q((t^{\mathbb{Q}}))$, alors x est une série p-quasi-automatique.*

Proposition 3.2. *Si $x, y \in \mathbb{F}_q((t^{\mathbb{Q}}))$ sont deux séries p-quasi-automatiques, alors leur somme et leur produit sont également des séries de Hahn p-quasi-automatiques. Si de plus, x est non nul, son inverse est une série de Hahn p-quasi-automatique.*

Remarque. Cette proposition est une conséquence de la proposition 1.2 et du théorème de Kedlaya que nous allons bientôt énoncer. Cependant, il existe une preuve directe pour la somme et le produit, qui n'utilise que la théorie de automates.

Nous pouvons maintenant énoncer les deux théorèmes principaux, démontrés respectivement dans les articles [CKMR80] et [Ked05, Chapitre 5].

Théorème 3.3 (Christol). *Une série entière $x \in \mathbb{F}_q[[t]]$ est p-automatique si et seulement si elle est algébrique sur le corps $\mathbb{F}_q(t)$.*

Théorème 3.4 (Kedlaya). *Une série de Hahn $x \in \mathbb{F}_q((t^{\mathbb{Q}}))$ est p-quasi-automatique si et seulement si elle est algébrique sur le corps $\mathbb{F}_q(t)$.*

On peut remarquer que le théorème de Kedlaya est une généralisation du théorème de Christol.

Corollaire 3.5. *Une série de Hahn $x = \sum_{i\in\mathbb{Q}} f(i)t^i$ est algébrique sur $\mathbb{F}_q(t)$ si et seulement si pour chaque $\alpha \in \mathbb{F}_q \setminus \{0\}$, la série de Hahn $\sum_{i\in f^{-1}(\{\alpha\})} t^i$ est algébrique.*

Avant de continuer, on peut se poser le problème inverse. À partir d'un automate M, on cherche à savoir s'il correspond à une série de Hahn x. Dans l'affirmative, on peut chercher une équation polynômiale sur $\mathbb{F}_q(t)$ vérifiée par x.

À partir d'un automate fini déterministe complet à sortie de fonction associée $f : {A_b}^* \to \mathbb{F}_q$, on peut en construire un qui renvoie la même valeur pour les éléments de Σ_b, et qui renvoie une valeur qui n'appartient pas à $\mathbb{F}_q$ pour les autres éléments de ${A_b}^*$.

On peut ensuite regarder si tous les $E_\alpha = \{i \in S_b | f(i) = \alpha\}$ pour $\alpha \in \mathbb{F}_q \setminus \{0\}$ sont bien ordonnés, ce qui se montre facilement à l'aide de la théorie des graphes.

Exemple. Soit l'automate de sortie suivant, où la fonction de sortie vaut 0 aux états q_0, q_1 et q_2 et 1 à l'état q_3. Il correspond à l'expression $t^{0,c} + t^{0,abc} + t^{0,ababc} + \ldots$. Si $a > c$, alors les exposants forment une suite strictement croissante, et l'expression est une série de Hahn. Si $a < c$, alors les exposants forment une suite strictement décroissante, et l'expression n'est pas une série de Hahn.

La preuve du sens automatique $\implies$ algébrique du théorème de Kedlaya, est constructive et permet de calculer rapidement un polynôme de $\mathbb{F}_q(t)[X]$ qui annule x.

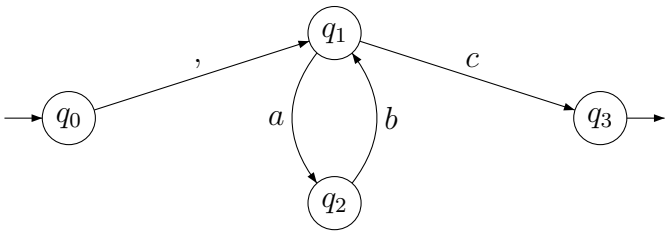

FIG. 2 – Exemple d'automate à sortie

4 Racines des polynômes de $\mathbb{F}_q(t)[X]$

Pour démontrer constructivement le sens algébrique $\Longrightarrow$ automatique du théorème de Kedlaya, nous devons montrer pourquoi l'ensemble des séries p-quasi-automatiques est stable par extraction de racines.

Lemme 4.1. *Pour toute série de Hahn p-quasi-automatique $x = \sum x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ à support dans $]-\infty; 0[$, il existe une série de Hahn $y \in \mathbb{F}_q((t^{\mathbb{Q}}))$ telle que $y^p - y = x$.*

Cette série est définie par $y = x^{1/p} + x^{1/p^2} + \ldots$.

Une difficulté apparaît pour les séries de Hahn dont les exposants tendent vers $+\infty$. Nous faisons abstraction de cette difficulté en utilisant les complétés.

Définition. Pour $q \neq 1$ une puissance de p, on note $R_q \subset \mathbb{F}_q((t^{\mathbb{Q}}))$ le complété pour la valuation v de l'anneau des séries p-quasi-automatiques.

Lemme 4.2. *Pour tout $a, b \in R_q$ avec $a \neq 0$, il existe q' une puissance de q telle que l'équation $z^p - az = b$ possède p racines dans $R_{q'}$.*

Lemme 4.3. *Pour tout $a_0, \ldots, a_{n-1}, b \in R_q$ avec a_0 non nul, il existe q' une puissance de q telle que l'équation $z^{p^n} - a_{n-1}z^{p^{n-1}} - \ldots - a_0 z = b$ possède p^n racines dans $R_{q'}$.*

Ce lemme est une amélioration du lemme précédent. Le principe est de voir le polynôme $X^{p^n} - a_{n-1}X^{p^{n-1}} - \ldots - a_0 X$ comme un opérateur additif, puis de décomposer cet opérateur en éléments de la forme $X^p - aX$, où $a \in R_{q'}$ pour une certaine puissance q' de q.

Lemme 4.4. *Soit $R = \bigcup_{e \in \mathbb{N}^*} R_{q^e}$ l'union des anneaux R_{q^e} pour les puissances de q. Alors tout polynôme non nul à coefficients dans R se scinde dans R.*

Kedlaya montre dans [Ked05, Chapitre 7] comment on conclut la preuve constructive. Si l'approximation y de la racine est assez bonne, on peut définir

x comme un polynôme en y sur $\mathbb{F}_q((t))$, où les coefficients sont algébriques. De cette manière, grâce au théorème de Christol, on peut voir que x est p-quasi-automatique.

À partir de cette preuve, on peut en déduire un algorithme pour trouver les racines du polynôme $P \in \mathbb{F}_q(t)[X]$, en les décrivant à l'aide d'automates. Les étapes de l'algorithme sont les suivantes.

- On commence, en considérant les X, X^p, X^{p^2}... modulo P, par trouver un polynôme $Q = X^{p^n} + \ldots + a_0 X$ qui est multiple de P.
- On regarde Q comme un opérateur additif et on le décompose en opérateurs du type $X^p - aX$.
- Il suffit alors de résoudre des équations du type $z^p - az = b$ à coefficients dans R_q, dans l'un des complétés des corps $\mathbb{F}_{q'}((t^{\mathbb{Q}}))$.
- On peut calculer les racines avec une précision arbitraire. Si x est une racine dont on connaît une bonne approximation y et un automate qui calcule y, alors on peut exprimer x comme un polynôme en y sur le corps $\mathbb{F}_{q'}((t))$.
- On trouve alors un automate qui calcule x.
- Après avoir trouvé toutes les racines x de Q, on calcule tous les $P(x)$ pour connaître les racines de P.

Références

[AS03] Jean-Paul Allouche and Jeffrey O. Shallit. *Automatic Sequences : Theory, Applications, Generalizations.* Cambridge University Press, 2003.

[CKMR80] G. Christol, T. Kamae, M. Mendès France, and G. Rauzy. Suites algébriques, automates et substitutions. *Bulletin de la Société Mathématique de France*, 108 :401–419, 1980.

[Ked01] Kiran S. Kedlaya. Power series and p-adic algebraic closures. *Journal of Number Theory*, 89 :324–339, 2001.

[Ked05] Kiran S. Kedlaya. Finite automata and algebraic extensions of function fields. arXiv :math/0410375v2 [math.AC].

[Pas77] Donald S. Passman. *The Algebraic Structure of Group Rings.* Wiley, 1977.

[Sak03] Jacques Sakarovitch. *Éléments de théorie des automates.* Vuibert, 2003.

[Ser79] Jean-Pierre Serre. *Local Fields.* Springer-Verlag, 1979.