Suites automatiques

Xuedong Shang
École Normale Supérieure

26 Janvier 2012

Contents

Abstract

Nous donnons ici, dans ce petit rapport, un premier traitement, très bref, des suites engendrées par un automate, modèle le plus simple de machine. Une suite automatique n'est pas nécessairement très simple ou régulière (ultimement périodique par exemple) malgré le fait que cela soit dûe à un automate dont les états sont finis. La premère partie de ce rapport est consacrée à une première aperçu des suites automatiques avec quelques exemples connus. Puis nous traiterons quelques caractérisations de l'automaticité en cherchant les liens entre les automates et leurs suite engendrée associée. À la fin, nous donnerons certains résultats divers sur les suites automatiques.

1 Définitions et exemples

On va commencer par définir la k-automaticité et donner deux exemples de suites 2-automatiques. Ces suites présenteront des similarité dont les liens seront développés dans la partie suivante.

Les automates que l'on va utiliser sont déterministes et complets. L'ensemble des états sera noté Q et au lieu d'avoir certains états finaux on dispose d'une fonction de sortie τ qui à chaque état associe un valeur "de sortie".

Définition 1. Un automate fini est la donnée de $\{Q, \Sigma, \delta, i, \tau, \Gamma\}$ où Q est l'ensemble des états, $i \in Q$ est l'état initial, Σ est l'alphabet d'entrée, δ la fonction de transition de $Q \times \Sigma$ dans Q. Γ l'alphabet de sortie et τ la fonction de sortie de Q dans Γ.

On remarque que pour obtenir un automate usuel, il suffit de prendre $\Gamma = \{0, 1\}$ et de considérer q état final si et seulement si $\tau(q) = 1$. Dans la suite, on n'introduit plus l'alphabet de sortie Γ dans l'automate s'il n'y pas d'ambiguïté.

Définition 2. Soit k un entier ≥ 2. On dit qu'une suite $(u_n)_n$ est k-automatique s'il existe un automate $\mathcal{A} = \{Q, \Sigma, \delta, i, \tau\}$ tel que :

$$\forall n, \tau(\delta(i, \langle n \rangle_k)) = u_n$$

où $\langle n \rangle_k$ désigne l'écriture en base k de n **à partir du chiffre de poids faible**. Si on lit dans l'automate $\mathcal{A}$ la suite constituée des chiffres de n en base k à partir du chiffre de poids faible, on tombe sur un état dont la valeur de sortie est u_n. Il est tout à fait naturel de considérer que la fonction de sortie est à valeur dans le même ensemble que la suite et que les arêtes de l'automate sont étiqueées par $\{0, 1, \cdots, k-1\}$.

Remarque 3. Un tel automate est appelé k-automate, et on peut ainsi dire qu'une suite est k-automatique si elle est engendrée par un k-automate.

1.1 La suite de Thue-Morse

La suite de Thue-Morse (appelée souvent suite de Prouhet-Thue-Morse chez les francophones) fut décrite pour la première fois par le mathématicien français Eugène Prouhet en 1851. Il la utilisa pour donner une solution à un problème de théorie des nombres qui s'appelle le problème de Prouhet-Tarry-Escott. La suite fut redécouverte par le mathématicien norvégien Axel Thue dans un article publié en 1906 qui est l'article fondateur de la combinatoire des mots. Puis Marston Morse, en 1922, donna une nouvelle interprétation de la suite, dans le cadre de la géométrie différentielle.

Définition 4. On définit la suite de Thue-Morse, $(t_n)_n$ de la façon suivante :

$$\begin{gathered} t_0 = 0, \\ \forall n \geq 0, t_{2n} = t_n, \\ \forall n \geq 0, t_{2n+1} = 1 - t_n \end{gathered}$$

On donne ses premiers termes ci-dessous : 0110100110...

1

0 $q_0/0$ $q_1/1$ 0

1

Figure 1: L'automate de Thue-Morse.

On voit que, d'après la définition de t, t_n correspond à la somme des chiffres dans l'écriture en base 2 de n modulo 2. La suite de Thue-Morse est ainsi 2-automatique; elle est engendrée par l'automate suivant[1] :

Donnons une autre manière pour définir la suite de Thue-Morse. On considère le morphisme 2-uniforme[2] $\sigma : \{0,1\}^* \to \{0,1\}^*$ donné par :

$$\sigma(0) = 01$$
$$\sigma(1) = 10$$

La suite $(\sigma^n(0))_n$ converge simplement vers t. Il en résulte que t est point fixe de σ.

1.2 La suite de Rudin-Shapiro

La suite de Rudin-Shapiro, aussi appelée la suite de Golay-Rudin-Shapiro est une suite automatique nommée par Marcel Golay, Walter Rudin et Harold S.Shapiro, qui l'ont décourvert indépendemment.

Définition 5. On définit la suite de Rudin-Shapiro $(r_n)_n$ de la façon suivante :

$$r_0 = 0,$$
$$\forall n \geq 0, r_{2n} = r_n,$$
$$\forall n \geq 0, r_{4n+1} = r_n,$$
$$\forall n \geq 0, r_{4n+3} = 1 - r_{2n+1}.$$

Ses premiers termes sont les suivants : 000100100001...

Il s'agit encore d'une suite 2-automatique. Elle est engendrée par l'automate suivant :

1 1 0

0 $q_0/0$ $q_1/0$ $q_2/1$ $q_3/1$ 0

0 1 1

Figure 2: L'automate de Rudin-Shapiro.

Cette suite donne le nombre d'occurrences de "11" dans l'écriture de n en base 2, le tout modulo 2. On ne peut pas trouver comme pour la suite de Thue-Morse un morphisme

[1] q/n est la notation pour dire que la valeur de sortie $\tau(q)$ de l'état q est n.

[2] Un morphisme est dit k-uniforme si l'image de toute lettre est un mot de taille k.

2-uniforme dont la suite soit point fixe. Il faut d'abord "agrandir" l'alphabet. Définissons un morphisme σ sur l'alphabet $\{A, B, C, D\}$ par :

$$\begin{aligned} \sigma(A) &= AB \\ \sigma(B) &= AC \\ \sigma(C) &= DB \\ \sigma(D) &= DC \end{aligned}$$

La limite simple de $\sigma^n(A)$ est de la forme suivante :

$$ABACABDBABACDCAC\cdots$$

La suite de Rudin-Shapiro s'obtient alors en prenant l'image du point fixe pour σ par la projection $\pi : \{A, B, C, D\} \to \{0, 1\}$ définie par :

$$\begin{aligned} \pi(A) = \pi(B) = 0 \\ \pi(C) = \pi(D) = 1 \end{aligned}$$

2 Théorème de Cobham

2.1 Le q-noyau

Au niveau des ressemblances entre les deux suites, il est pertinent d'introduire certaines définitions.

Définition 6. Soit u une suite donnée et $k \in \mathbb{N}$. le q-noyau que l'on notera désormais $K_u^{(q)}$ (ou plus simplement K_u s'il n'y a pas d'ambiguïté) est :

$$K_u^{(q)} = \{(u(q^\alpha n + r))_n \mid \alpha \in \mathbb{N},\ 0 \leq r < \alpha\}$$

Le q-noyau nous intéresse lorsqu'il n'est pas "trop gros" et qu'il contraint les suites à coïncider avec leurs propres sous-suites extraites de pas q^k. Or il y a au plus un nombre dénombrable de telle suite, on s'intéresse alors au cas fini.

Lorsque le q-noyau est fini, il est facile de le calculer par machine. Il suffit de construire récursivement les ensembles X_k donnés par :

$$X_0 = \{(a_n)_{n\geq 0}\} et X_{k+1} = X_k \cup \{(b_{qn+r})_n | (b_n)_n \in X_k, r \in [0, q-1]\}.$$

S'il existe k tel que $X_k = X_{k+1}$ alors c'est la valeur du q-noyau, ce dernier est alors fini.

Proposition 7. *Le 2-noyau de la suite de Thue-Morse est fini.*

Proof. On a

$$X_1 = \{(t_{2n})_n, (t_{2n+1})_n\} = \{(t_n)_n, (1 - t_n)_n\}$$

Donc $K_t = \{(t_n)_n, (1 - t_n)_n\}$ dont le 2-noyau est fini. □

Proposition 8. *Le 2-noyau de la suite de Rudin-Shapiro est fini.*

Proof. On a

$$X_1 = \{(r_n)_n, (r_{2n+1})_n\}$$

Puis

$$X_2 = \{(r_n)_n, (r_{2n+1})_n, (r_{4n+3})_n\}$$

Ensuite

$$X_3 = \{(r_n)_n, (r_{2n+1})_n, (r_{4n+3})_n, (r_{8n+3})_n\}$$

Enfin

$$X_4 = \{(r_n)_n, (r_{2n+1})_n, (r_{4n+3})_n, (r_{8n+3})_n\} = X_3$$

D'où le 2-noyau $K_r = \{(r_n)_n, (r_{2n+1})_n, (r_{4n+3})_n, (r_{8n+3})_n\}$ est fini. □

2.2 Théorème de Cobham

Donnons maintenant un lien avec les morphismes q-uniformes.

Définition 9. Une suite u à valeur dans un alphabet Σ est dite *l'image d'un point fixe d'un point fixe d'un morphisme k-uniforme* $\sigma : \Sigma' \to \Sigma'$ s'il existe $w \in \Sigma'^{\mathbb{N}}$ point fixe de σ et π projection de Σ' dans Σ tels que $\forall n \in \mathbb{N}, u_n = \pi(w_n)$.

En écrivant le fait d'être un point fixe lettre à lettre on obtient la caractérisation suivante qui sera souvent utile.

Lemme 10. *Si σ est un morphisme q-uniforme d'un alphabet Σ dans lui même, alors w en est un point fixe si et seulement si :*

$$\forall n \in \mathbb{N}, \forall r \leq q, \sigma(w_n)_r = w_{qn+r}$$

Le lemme est facile à démontrer d'une façon très intuitive. Les deux suites t et r sont image de point fixe d'un morphisme 2-uniforme. On est à présent en mesure de donner une généralisation qui porte le nom de Cobham :

Proposition 11 (Cobham, 1972)**.** *Soient $q \in \mathbb{N}^*$ et $(u_n)_n$ une suite à valeurs dans $\{0, \cdots, q-1\}$, alors les trois assertions suivantes sont équivalentes :*

i) la suite $(u_n)_n$ est q-automatique

ii) le q-noyau K_u de u est fini

iii) la suite $(u_n)_n$ est image d'un point fixe d'un morphisme q-uniforme

Proof. $i) \Rightarrow ii)$. On dispose d'un k-automate $\mathcal{A} = \{Q, \Sigma, \delta, i, \tau\}$ qui engendre $(u_n)_n$. On rappelle que $u_n = \tau(\delta(q_0, \langle n \rangle_q))$. Or pour $i \geq 0, 0 \leq j < i$, $(q^i n + j)_q = j0 \dots 0 \langle n \rangle_q = w \langle n \rangle_q$ où l'on note $w = j0^{i-1}$. On a alors $u_{q^i n + j} = \tau(\delta(q_0, w\langle n \rangle_q)) = \tau(\delta(\delta(q_0, w), \langle n \rangle_q))$.

Comme il y a un nombre fini d'états, ainsi que $\delta(q_0, w)$ selon que i et j varient. Le q-noyau est alors bien fini.

$ii) \Rightarrow iii)$. Le q-noyau étant fini supposé de cardinal d, on peut alors écrire $K_u = \{(u_n^{(1)})_n, (u_n^{(2)})_n, \dots, (u_n^{(d)})_n\}$ avec $(u_n^{(1)})_n = (u_n)_n$. On définit une suite $(V_n)_n$ sur l'alphabet Σ^d par $\forall n \in \mathbb{N}$, $V_n = (u_n^{(1)}, u_n^{(2)}, \dots, u_n^{(d)})$. Pour $j \in [0, q-1]$, on dispose d'une application :

$$\sigma_j : \Sigma^d \to \Sigma^d \ telleque \ \forall n \in \mathbb{N}, V_{qn+j} = \sigma_j(V_n)$$

On considère le morphisme $\sigma : (\Sigma^d)^* \to (\Sigma^d)^*$ défini par :

$$\forall V \in \Sigma^d, \sigma(V) = \sigma_0(V)\sigma_1(V) \cdots \sigma_{q-1}(V).$$

Il est aisé à voir que le morphisme h est q-uniforme, et par le **lemme 10**, la suite $(V_n)_n$est point fixe de σ. $(u_n)_n$ est l'image de $(V_n)_n$ par la projection sur la première coordonnée.

$iii) \Rightarrow i)$. On pose $(v_n)_n = \sigma^\infty(v)^3$, c'est-à-dire le point fixe de σ où σ est un morphisme q-uniforme sur l'alphabet Σ' et posons aussi une application f telle que $\forall n, u_n = f(v_n)$.

Consiérons maintenant l'automate $\mathcal{A} = \{\Sigma', \Sigma, \delta, v, f\}$ où la fonction de transition δ est définie par : $\sigma(x) = \delta(x, 0)\delta(x, 1) \cdots \delta(x, q-1)$. On a alors $\forall n \in \mathbb{N}, u_n = f(\delta(v, \langle n \rangle_q))$. En effet, on montre par récurrence que :

$$\forall k, \sigma^k(v) = \delta(v, \langle 0 \rangle_q)\delta(v, \langle 1 \rangle_q) \cdots \delta(v, \langle q^k - 1 \rangle_q).$$

L'initialisation est claire. Pour l'héritage, on a :

$$\begin{aligned}
\sigma^{k+1}(v) &= \sigma(\delta(v, \langle 0 \rangle_q)\delta(v, \langle 1 \rangle_q) \cdots \delta(v, \langle q^k - 1 \rangle_q)) \\
&= \delta(\delta(v, \langle 0 \rangle_q), 0) \cdots \delta(\delta(v, \langle 0 \rangle_q), q-1) \cdots \delta(\delta(v, \langle q^k - 1 \rangle_q), 0) \cdots \delta(\delta(v, \langle q^k - 1 \rangle_q), q-1) \\
&= \delta(v, \langle 0 \rangle_q) \cdots \delta(v, \langle q-1 \rangle_q) \cdots \delta(v, \langle q^{k+1} - q \rangle_q) \cdots \delta(v, \langle q^{k+1} - q + (q-1) \rangle_q).
\end{aligned}$$

Donc $(u_n)_n$ est bien engendrée par le q-automate $\mathcal{A}$. □

3 Théorème de Christol

Nous présentons dans cette partie un résultat de Gilles Christol. Auparavant, les suites considérées sont q-automatiques, avec $q = p^n$ et p premier. Le théorème donne une caractérisation surprenante du fait d'être automatique en terme d'algébricité (voir [1]) de série sur le corps $\mathbb{F}_q(X)$.[4] Plus précisément, le théorème donne une équivalence entre l'algébricité d'une série formelle à coefficients dans un corps fini et la nature automatique de la suite des coefficients. On va, dans un premier temps, définir un opérateur qui porte le nom de Cartier.

[3] $\sigma^\infty(v)$ désigne le mot $vx\sigma(x)\sigma^2(x)\dots$ qui est un point fixe de σ si $\sigma(v) = vx$ avec x non vide.

[4] $\mathbb{F}_q$ désigne le corps fini à q éléments.

3.1 Opérateur de Cartier

Notons $\mathbb{F}_q[[X]]$ l'ensemble des séries formelles à coefficients dans $\mathbb{F}_q$. Soit u une suite à valeur dans $\mathbb{F}_q$, on note :

$$F(u) = F_u = \sum_{n=0}^{\infty} u_n X^n.$$

Pour éclaircir l'idée, regardons les deux exemples suivantes:

Exemple 12. On se place dans $\mathbb{F}_2$[5]. En utilisant la définition de la suite de Thue-Morse t, il vient :

$$\begin{aligned} F_t(X) &= \textstyle\sum_n t_n X^n &&= \textstyle\sum_n t_{2n} X^{2n} + \sum_n t_{2n+1} X^{2n+1} \\ & && = \textstyle\sum_n t_n X^{2n} + \sum_n X^{2n+1} + \sum_n t_n X^{2n+1} \\ & && = F(X^2) + \tfrac{X}{1+X^2} + XF(X^2) \\ & && = (1+X)F(X^2) + \tfrac{X}{1+X^2}. \end{aligned}$$

F est donc algébrique sur le corps $\mathbb{F}_2(X)$ des fractions rationnelles modulo 2. Elle est racine du polynôme P à coefficients dans $\mathbb{F}_2(X)$:

$$P(Y) = (1+X)Y^2 + Y + \frac{X}{1+X^2}.$$

Exemple 13. Par des calculs analogues, on obtient la relation suivante pour la suite de Rudin-Shapiro r :

$$(1+X)^5 F(X)^2 + (1+X)^4 F(X) + X^3 = 0.$$

Avant de continuer, il sera utile d'introduire une famille d'opérateurs sur les séries formelles qui portent le nom de l'opérateur de Cartier.

Définition 14 (Cartier)**.** Soit $r \in \{0, \cdots, q-1\}$. On définit l'opérateur Λ_r :

$$\Lambda_r : \sum_n a_n X^n \in \mathbb{F}_q[[X]] \mapsto \sum_n a_{qn+r} X^n.$$

Le lemme suivant se vérifie facilement.

Lemme 15. *Soit $r \in \{0, \cdots, q-1\}$ et $F, G \in \mathbb{F}_q[[X]]$. Alors :*

$$\Lambda_r(FG^q) = \Lambda_r(F)G.$$

Précisons maintenant ce que veut dire être algégrique sur $\mathbb{F}_q(X)$ pour une série formelle F.

Lemme 16. *Soit $F = \sum_n a_n X^n$ une série formelle à coefficients dans $\mathbb{F}_q$, alors F est algébrique si et seulement si on peut trouver des polynômes $B_0(X), B_1(X), \cdots, B_k(X)$, non tous nuls tels que :*

$$B_0 F + B_1 F^q + \cdots + B_k F^{q^k} = 0$$

On peut supposer en outre que $B_0 \neq 0$.

[5]On confond donc + et −, de plus, pour une série formelle F, $F(X^2) = F(X)^2$

Proof. Si F est algébrique sur $\mathbb{F}_q(X)$, la famille $(F^{q^k})_{k\geq 0}$ est liée, d'où une relation de combinaison linéaire non triviale de la forme de l'énoncé. Réciproquement une telle liaison implique l'algébricité de F. Il reste à montrer que B_0 n'est pas nul.

Prenons $k \in \mathbb{N}$ minimal tel que l'on ait une relation de liaison non triviale comme ci-dessus et montrons par l'absurde que $B_0 = 0$:

$$B_1 F^q + \cdots + B_k F^{q^k} = 0$$

Puis, en utilisant le lemme plus haut :

$$\Lambda_r(B_1 F^q + \cdots + B_k F^{q^k}) = \Lambda_r(B_1)F + \cdots + \Lambda_r(B_k)F^{q^{k-1}} = 0$$

Ce qui contredit alors la minimalité de k. □

3.2 Théorème de Christol

Théorème 17 (Christol, 1979)**.** [6] *Soit $p \geq 2$ un nombre premier et q une puissance de p. Une suite u à valeurs dans $\mathbb{F}_q$ est q-automatique si et seulement si la série formelle $F(u) = \sum_n u_n X^n$ est algébrique sur $\mathbb{F}_q(X)$.*

Proof. ($\Rightarrow$). Soit u une suite q-automatique. On se servira de l'équivalence prouvée par Cobham : le q-noyau K_u est fini. Posons alors $d = Card(K_u)$.

$$F(u) = \sum_{r=0}^{q-1} X^r \sum_n u_{qn+r} X^{nq}$$

Comme on a dans $\mathbb{F}_q$, $G(X^q) = G(X)^q$ où G est un polynôme

$$F(u) = \sum_{r=0}^{q-1} X^r (\sum_n u_{qn+r} X^n)^q$$

Ce qui montre que :

$$F(u) \in Vect_{v\in K_u}\langle F(v)^q \rangle$$

On peut ainsi répéter le processus de la même manière :

$$\forall k \leq d : F(u)^{q^k} \in Vect_{v\in K_u}\langle F(v)^{q^{k+1}} \rangle$$

Et donc par une récurrence simple, on obtient :

$$\forall k \leq d : F(u)^{q^k} \in Vect_{v\in K_u}\langle F(v)^{q^{d+1}} \rangle$$

Mais $Vect_{v\in K_u}\langle F(v)^{q^{d+1}} \rangle$ est de dimension au plus d, la famille $\{F(u), F(u)^q, \cdots, F(u)^{q^d}\}$ est liée. $F(u) = \sum_n u_n X^n$ est donc algébrique sur $\mathbb{F}_q(X)$.

[6] La version donnée ici est dûe à Christol, Kamae, Mendès et Rauzy. Dans sa version initiale, le théorème ne portait que sur $\mathbb{F}_2$

($\Leftarrow$). Réciproquement, si la série formelle $F(u)$ est algébrique sur $\mathbb{F}_q(X)$, d'après le **lemme 16**, on peut trouver des polyômes B_i avec B_0 non nul tels que :

$$\sum_{i=0}^{k} B_i(X)F_u(X)^{q^i} = 0$$

Posons $G_u = F_u/B_0$. Il vient $G_u = \sum_{i=0}^{k} C_i G_u^{q^i}$ où $\forall i \in \{1,\dots,k\}, C_i = -B_i B_0^{q^i-2}$. Posons ensuite $N = max\{deg(B_0), deg(C_1), \cdots, deg(C_k)\}$ et $\mathcal{H}$ l'ensemble défini par :

$$\mathcal{H} \quad = \{H \in \mathbb{F}_q[[X]] | H = \textstyle\sum_{i=0}^{k} D_i G_u^{q^i} et D_i \in \mathbb{F}_q[X], deg(D_i) \leq N\}.$$

$\mathcal{H}$ est un ensemble fini contenant F_u. Pour montrer que K_u est fini, il suffit de montrer que $\forall r < q$, $\mathcal{H}$ est stable par Λ_r. Soit alors H un élément de $\mathcal{H}$, on a :

$$\Lambda_r(H) = \Lambda_r(D_0 G_u + \sum_{i=1}^{k} D_i G_u^{q^i}) = \Lambda_r(\sum_{i=1}^{k}(D_0 G_u + D_i)G_u^{q^i}) = \sum_{i=1}^{k} \Lambda(D_0 C_i + D_i) G_u^{q^{i-1}}$$

Comme pour tout i, on a $deg(D_0 C_i + D_i) \leq deg(D_0 C_i + D_i)/q \leq 2N/q \leq N$, donc $\Lambda_r(H) \in \mathcal{H}$. □

4 Divers

Dans cette partie, nous donnons quelques autres résultats importants sur les suites automatiques. Cobham a démontré le résultat qui suit dont on trouvera une démonstration dans [2] :

Théorème 18. *Soit k et l deux entiers multiplicativement indépendants*[7] *et soit u une suite k et l-automatique, alors u est ultimement périodique.*

Corollaire 19. *Soit q_1 et q_2 multiplicativement indépendants et soit u une suite telle que F_u soit à la fois algébrique sur $\mathbb{F}_{q1}$ et $\mathbb{F}_{q2}$, alors u est ultimement périodique.*

Proof. En vertu du théorème précédent et celui de Christol. □

En particulier, les suites de Thue-Morse et de Rudin-Shapiro ne sont pas 3-automatiques.[8] Il est donc intéressant de comparer ce corollaire à la conjecture suivante.

Conjecture 20. *Soit $(u_n)_n \in \{0,1\}^{\mathbb{N}}$ telle que les deux nombres réels $\sum_{n\in N} \frac{u_n}{2^n}$ et $\sum_{n\in N} \frac{u_n}{3^n}$ sont algébriques sur $\mathbb{Q}$, alors ces deux nombres sont rationnels.*

Par ailleurs, on montre que si deux suites u et v à valeurs dans $\{0,\dots,q-1\}$ sont q-automatiques, leur produit uv l'est aussi. En appliquant le théorème de Christol, on a :

[7] $i.e\ k^\alpha = l^\beta \Rightarrow \alpha = \beta = 0$

[8] Par contraposée.

Corollaire 21. *Soient u et v à valeurs dans $\{0, \ldots, q-1\}$ telles que F_u et F_v sont algébriques sur $\mathbb{F}_q(X)$, alors le produit d'Hadamard*[9] *de F_u et F_v est aussi algébrique que l'on note F_{uv}.*

Le lien entre les automates et l'algébricité laisse entrevoir un champ de recherche en théorie des nombres et en algèbre.

References

[1] J-P.Allouche. Automates et algébricité. In *Journal de Théorie des Nombres de BORDEAUX*, volume 17, pages 1–11. Université Bordeaux 1, 2005.

[2] J-P.Allouche and J.Shallit. *Automatic sequences*, volume 1. Cambridge University Press, 2003.

[9] *i.e* produit composante par composante.