Theoretical Computer Science 9 (1979) 141–145

NOTE

ENSEMBLES PRESQUE PERIODIQUES k-RECONNAISSABLES

Gilles CHRISTOL
Université Paris 6, Paris, France

Communicated by Maurice NIVAT
Received May 1978

Abstract. We characterize the automata which recognize almost periodic sets of written in k basis integral numbers.

Cet article a été inspiré par les résultats de [1]. Nous reprenons, pour tout ce qui concerne les automates et les ensembles k-reconnaissables, les définitions de [3, en particulier chapitre V].

Le lien de ce qui suit avec [1] est donné par le théorème suivant:

Théorème 1. *Soit p un nombre premier, et soit $\mathbf{F}_p$ le corps à p éléments. Un ensemble A d'entiers* ($\geqslant 0$) *est p-reconnaissable si et seulement si la série $f(x) = \sum_{n\in A} x^n$ de $\mathbf{F}_p[[x]]$ est algébrique sur $\mathbf{F}_p(x)$ (c'est à dire: il existe un polynôme P de $\mathbf{F}_p[x, y]$ non nul tel que $P(x, f(x)) = 0$).*

On pourra extraire une démonstration de ce résultat de [2] où un théorème analogue est établi dans le cas d'un corps p-adique. Comme cette démonstration se simplifie notablement dans le cas qui nous intéresse, nous en donnons un résumé.

Nous utiliserons, *pour ce théorème*, "l'interprétation inverse". C'est à dire que l'automate "lit" le nombre $n = n_0 + n_1p + \cdots + n_hp^h$ $(0 \leqslant n_i < p)$ dans l'ordre $n_0, \ldots, n_h$.

Posons, pour $0 \leqslant n < p^h$:

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

et définissons l'opérateur U_i $(0 \leqslant i < p)$ sur les $f_{n,h}$ par:

$$U_i f_{n,h} = f_{n+ip^h,h+1}$$

Il est facile de vérifier que A est p-reconnaissable si et seulement si l'ensemble des $f_{n,h}$ (différents) est fini. Dans ce cas A est reconnu par l'automate $\mathfrak{A}$ défini par les données suivantes: les états sont les $f_{n,h}$, l'état initial est $f=f_{0,0}$, les transitions sont les U_i et les états finaux sont les $f_{n,h}$ tels que $f_{n,h}(0)=1$.

Soit N le nombre d'états de $\mathfrak{A}$, posons:

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

où les P_i sont des polynômes de $\mathbf{F}_p[x]$ de degré strictement inférieur à p^{2N}. Nous définissons les g_j de manière unique par la relation:

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

Un calcul simple montre que les g_j sont des combinaisons linéaires, à coefficients dans $\mathbf{F}_p$, des $f_{n,h}$ et des $xf_{n,h}$. Il en résulte que les g_j ne peuvent prendre que p^{2N} valeurs différentes, donc que g ne peut prendre que $(p^{2N})^{p^{2N}}$ valeurs différentes. Comme il y a $(p^{p^{2N}})^{2N+1}$ manières différentes d'écrire g, deux g différents prennent la même valeur. Par soustraction on obtient un g, non identiquement nul, qui prend la valeur 0. Comme $f(x^p)=f^p(x)$, on a trouvé des polynômes P_i, *non tous nuls*, tels que:

$$P_0f+P_1f^p+\cdots+P_{2N}f^{p^{2N}}=0,$$

f est donc algébrique.

Réciproquement, si f est algébrique, on sait [4] que f est la diagonale d'une fraction rationnelle. C'est à dire qu'il existe deux polynômes P et Q dans $\mathbf{F}_p[x,y]$ tels que:

$$\frac{P(x,y)}{Q(x,y)}=\sum_{r,s} a_{r,s}x^ry^s \quad \text{et} \quad f(x)=\Delta\frac{P}{Q}=\sum_m a_{m,m}x^m$$

Les termes de f intervenant dans $f_{n,h}$ étant ceux qui sont de degré congru à n modulo p^h, en écrivant:

$$\frac{P(x,y)}{Q(x,y)}=\frac{P(x,y)Q^{p^h-1}(x,y)}{Q(x^{p^h},x^{p^h})}$$

nous obtenons:

$$f_{n,h}=\Delta\frac{R_{n,h}}{Q}$$

où $R_{n,h}(x^{p^h},y^{p^h})$ est le polynôme obtenu en ne conservant dans $P(x,y)Q^{p^h-1}(x,y)$ que les termes dont les degrés en x et en y sont congrus à n modulo p^h. Les $R_{n,h}$, étant de degré inférieur au maximum des degrés de P et de Q, sont en nombre fini. Il en est donc de même des $f_{n,h}$. La remarque faite au début de la démonstration montre que A est p-reconnaissable.

Définition [1]. Un ensemble A d'entiers est dit *presque périodique* si et seulement si pour tout n il existe N tel que pour tout m il existe $M<N$ tel que, pour tout $s\in[0,n]$, $(m+M+s)\in A$ si et seulement si $s\in A$.

k sera un nombre entier non nécessairement premier ($k \geq 2$)

Théorème 2. *Un ensemble d'entiers A, k-reconnaissable, est presque périodique si et seulement si il existe r tel que l'automate $\mathfrak{A}_r$ (minimal complet) qui reconnait A dans la base k^r (pour l'interprétation standard) ait son état initial récurrent.*

Preuve. Notons $\sum_r$ l'alphabet $(0, 1, \ldots, k^r - 1)$ et e l'état initial de $\mathfrak{A}_r$. Pour $u \in \sum_r^*$, $u = u_1 \cdots u_n$ (avec $u_i \in \sum_r$, c'est à dire $u \in \sum_r^n$), nous posons $n = l(u)$ et

$$\nu(u) = \sum_{i=1}^{n} u_i k^{r(n-i)}.$$

Supposons e récurrent. Pour tout $u \in \sum_r^*$ il existe alors $u' \in \sum_r^*$ tel que $euu' = e$. Lorsque u parcourt $\sum_r^*$, eu parcourt l'ensemble fini des états de $\mathfrak{A}_r$. Il suffit donc de considérer un nombre fini de u'. Soit α le maximum des $l(u')$ correspondants. Comme $\mathfrak{A}_r$ est minimal complet $e0 = e$. Quitte à rajouter des 0 à droite, on peut donc choisir les u' de telle sorte que pour tout u on trouve $l(u') = \alpha$.

Etant donné n nous choisissons β de telle sorte que $n < k^{r\beta}$. Pour tout m il existe L tel que

$$m \leq Lk^{r(\alpha+\beta)} < (L+1)k^{r(\alpha+\beta)} < m + 2k^{r(\alpha+\beta)}.$$

Soit u tel que $\nu(u) = L$, nous avons vu qu'il existe u' tel que $l(u') = \alpha$ et tel que $euu' = e$. Pour tout w on a donc $euu'w = ew$. Pour $l(w) = \beta$ il vient:

$$\nu(w) \in A \Leftrightarrow \nu(w) + \nu(u')k^{r\beta} + Lk^{r(\alpha+\beta)} \in A.$$

Comme $\nu(\sum_r^\beta) = [0, k^{r\beta} - 1] \supset [0, n]$ la condition suffisante est démontrée avec: $N = 2k^{r(\alpha+\beta)}$, $M = Lk^{r(\alpha+\beta)} + \nu(u')k^{r\beta} - m$ (comme $\nu(u') < k^{r\alpha}$ on a bien $M < N$).

Pour démontrer que la condition est nécessaire, nous utilisons Théorème 6 de [1]:

Si A est presque périodique, pour tout α, il existe β tel que, pour tout m il existe $M < k^\beta$ tel que pour tout $s < k^\alpha$ on ait:

$$mk^{\alpha+\beta} + Mk^\alpha + s \in A \Leftrightarrow s \in A.$$

Nous traduisons cette condition dans l'automate $\mathfrak{A}$ de A. En notant T l'ensemble des états finaux de $\mathfrak{A}$ et avec $m = k^{\gamma-\beta}\nu(u)$, $M = \nu(v)$ et $s = \nu(w)$, il vient: pour tout α il existe β tel que, pour tout $\gamma \geq \beta$ et tout $u \in \Sigma^*$ ($\Sigma = (0, 1, \ldots, k-1)$), il existe $v \in \Sigma^*$ tel que $l(v) = \gamma$ et, pour tout $w \in \Sigma^\alpha$, $euvw \in T \Leftrightarrow ew \in T$.

Soit q un état de $\mathfrak{A}$, nous posons:

$$E(q) = \{\alpha;\ \forall w \in \Sigma^\alpha,\ qw \in T \Leftrightarrow ew \in T\}.$$

Si A est presque périodique, nous obtenons la propriété:

(P): Pour tout α et tout $u \in \Sigma^*$, il existe β tel que, pour tout $\gamma \geq \beta$, il existe v tel que $l(v) = \gamma$ et $\alpha \in E(euv)$.

Le nombre des états de $\mathfrak{A}$ étant fini, il existe $v \in \Sigma^\gamma$ tel que $E(euv)$ soit infini.

Notons O_r le mot formé de r fois la lettre O, et choisissons r de telle sorte que, pour tout état q de $\mathfrak{A}$, on ait $qO_rO_r = qO_r$ (ceci est possible car il n'y a qu'un nombre fini d'états). Si $\alpha \in E(q)$, $\alpha \geqslant r$, pour tout $w \in \Sigma^{\alpha - r}$ on a $qO_rw \in T \Leftrightarrow eO_rw = ew \in T$, c'est à dire $\alpha - r \in E(qO_r)$. En particulier, si $E(q)$ est infini $E(qO_r) = E(qO_rO_r)$ est aussi infini et contient alors une progression arithmétique de raison r. Autrement dit, il existe d tel que, pour tout état q de $\mathfrak{A}$, si $\alpha \in E(qO_r)$ et $\alpha > d$ alors $\alpha + \lambda r \in E(qO_r)$ pour tout $\lambda \geqslant 0$.

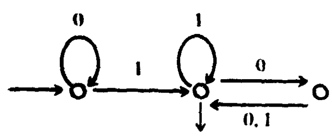
Si A est presque périodique, la propriété (P) montre que, pour tout u et tout $\alpha > d + 1$, il existe (au moins) un γ et un $v \in \Sigma^{r\gamma}$ tel que $r\alpha \in E(euv)$ donc tel que $r(\alpha - 1) \in E(euvO_r)$. En conclusion, pour tout $u \in \Sigma^*$, il existe $v \in \Sigma^{r\gamma}$ tel que, pour tout $\lambda \geqslant 0$, $(\alpha + \lambda)r \in E(euvO_r)$.

L'automate $\mathfrak{A}_r$, qui reconnait A dans la base k^r, a donc la propriété suivante: pour tout état q il existe $v \in \Sigma_r^\gamma$ tel que, pour tout $w \in \Sigma_r^\alpha\Sigma_r^*$, on ait $qvOw \in T \Leftrightarrow ew \in T$. En particulier, pour tout $w \in \Sigma_r^*$, on a $qvO_\alpha w \in T \Leftrightarrow eO_\alpha w = ew \in T$. Autrement dit, $\mathfrak{A}_r$ étant supposé minimal, qvO_α est l'état initial de $\mathfrak{A}_r$, ce qui achève la démonstration.

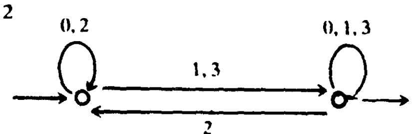
Exemples. (1) L'état initial peut être récurrent dans $\mathfrak{A}_r$ mais pas dans $\mathfrak{A}$ comme le montre l'exemple suivant:

$$k = 2, \qquad A = \nu(\Sigma^*1(00)^*) = \{n = m4^h, m \text{ impair}\}$$

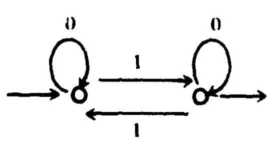
$\mathfrak{A}$



$\mathfrak{A}_2$



(2) La fonction 'somme des chiffres' en base 2 (ou suite de Morse Hedlund) est reconnue par l'automate:



ce qui montre immédiatement que cette suite est presque périodique.

Questions de densité.

La densité de A est définie, si elle existe, par:

$$d(A) = \lim_{N \to \infty} \frac{1}{N} \# \Big\{ A \cap [0, N] \Big\}.$$

Alors qu'en général si A est k-reconnaissable, $d(A)$ n'existe qu'en moyenne de Césaro, si A est k-reconnaissable presque périodique, $d(A)$ existe (on vérifie ce résultat trés facilement en remarquant que, puisque l'état initial de $\mathfrak{A}_r$ est récurrent, la chaine de Markov associée à $\mathfrak{A}_r$ est ergodique).

Il serait intéressant de caractériser parmi les ensembles k-reconnaissables ceux qui sont presque périodiques à l'aide d'une condition de densité. L'existence d'une densité ne suffit pas comme le montre l'exemple $A = \{2n\} \backslash \{2^m\}$: A étant 2-reconnaissable mais pas presque périodique a cependant une densité égale à 1/2.

Bibliographie

[1] L. E. Baum, N. P. Herzberg, S. J. Lomonaco, Jr. and M. M. Sweet, Field of Almost Periodic Sequences, *J. Combinatorial Theory Ser. A* **22** (1977) 169–180.

[2] G. Christol, Limites uniformes p-adiques de fonctions algébriques, Thèse Sciences Math., Paris (1977).

[3] Eilenberg *Automata, Languages and Machines* Vol. A (Academic Press, New York, 1974).

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