Journal de Théorie des Nombres
de Bordeaux **8** *(1996), 205–214*

Représentation par automate de fonctions continues de tore

par F. BLANCHARD, B. HOST ET A. MAASS

RÉSUMÉ. Soient $A_p = \{0, ..., p-1\}$ et $Z \subseteq A_p^{\mathbb{N}} \times A_p^{\mathbb{N}}$ un sous-système. Z est une représentation en base p d'une fonction f du tore si pour tout point x du tore, ses développements en base p sont liés par le couplage Z aux développements en base p de $f(x)$. On prouve que si f est représentable en base p alors $f(x) = (ux + \frac{m}{p-1}) \bmod 1$, où $u \in \mathbb{Z}$ et $m \in A_p$. Réciproquement, toutes les fonctions de ce type sont représentables en base p par un transducteur. On montre finalement que les fonctions du tore qui peuvent être représentées par automate cellulaire sont exclusivement les multiplications par un diviseur d'une puissance de la base.

1. Introduction.

La représentation des fonctions continues de l'intervalle par des systèmes discrets simples, par exemple les automates cellulaires, les automates finis, les transducteurs, a fait l'objet de plusieurs travaux récents; voir par exemple [M], [BG] ou [BDT]. Les motivations viennent d'une part de l'informatique théorique, notamment du calcul arithmétique en ligne, et d'autre part de la théorie ergodique.

Soit p un entier positif, et notons $A_p = \{0, ..., p-1\}$. A chaque élément x du tore est associé l'ensemble de ses développements en base p, $T_p(x) \subseteq A_p^{\mathbb{N}}$. Tout le monde sait que $|T_p(x)| \leq 2$. Soit $Z \subseteq A_p^{\mathbb{N}} \times A_p^{\mathbb{N}}$ un couplage entre $A_p^{\mathbb{N}}$ et un sous-système $X_S \subseteq A_p^{\mathbb{N}}$. Z représente une fonction f du tore si pour chaque $\underline{x} \in T_p(x)$ les $\underline{y} \in A_p^{\mathbb{N}}$ tels que $(\underline{x}, \underline{y}) \in Z$ représentent le même élément $y = f(x)$ du tore. Un tel couplage est appellé une représentation en base p de f. La proposition 2.2 établit que les fonctions ayant une représentation en base p sont continues. Il faut remarquer qu'à toute fonction f du tore est associé un sous-ensemble Z de $A_p^{\mathbb{N}} \times A_p^{\mathbb{N}}$ qui la représente. Il suffit de prendre $Z = \{(\underline{x}, \underline{y}) \in A_p^{\mathbb{N}} \times A_p^{\mathbb{N}} \ / \ \underline{x}$ est un développement de x et $\underline{y}$ de $f(x)$ $\}$. Si f est continue, Z est fermé, mais pas nécessairement invariant par le décalage.

Manuscrit reçu le 25 novembre 1993

Dans cette article on s'intéresse en particulier aux couplages Z engendrés par automates cellulaires et transducteurs. Dans le premier cas Z est simplement le graphe d'une application.

La partie 2 est consacrée aux définitions et résultats préliminaires.

L'objet essentiel de la troisième partie est de démontrer que trois familles de fonctions sont identiques : l'une, les fonctions représentables, est définie en termes de couplages dynamiques; la seconde, les fonctions représentables par transducteur, est définie par automates; et la troisième se décrit de façon purement arithmétique : ce sont les fonctions $f(x) = (ux + \frac{m}{p-1})$ mod 1, où $u \in \mathbb{N}$ et $m \in A_p$.

On prouve dans le théorème 3.3 que lorsqu'une fonction du tore f a une représentation en base p, elle est de la forme $f(x) = (ux + \frac{m}{p-1})$ mod 1, où $u \in \mathbb{N}$ et $m \in A_p$; la démonstration repose essentiellement sur le fait peu connu que toute fonction continue du tore, commutant avec la multiplication par p, est de cette même forme. On applique ce résultat aux automates cellulaires et transducteurs. Il est établi dans [BDT], et rappelé ici, qu'on peut représenter par transducteurs toutes les fonctions $f(x) = (ux + \frac{m}{p-1})$ mod 1. Finalement, le corollaire 3.5 établit que les automates cellulaires ne peuvent représenter que les fonctions du type $f(x) = (ux)$ mod 1, où u est un entier qui divise une puissance positive de p.

Le résultat obtenu - il n'existe pas d'autres fonctions représentables que celles que nous savions déjà l'être au départ - est limitatif : on peut l'interpréter en allant jusqu'à dire que les seules fonctions "bien adaptées" à la représentation en base entière sont celles décrites plus haut. Par contre, on peut introduire une forme plus faible de la représentabilité, par exemple en exigeant que la fonction soit seulement définie par transducteur, surjective et continue en dehors des points p-adiques. On définit ainsi une classe bien plus vaste de fonctions, dont on ne sait que peu de choses; toutefois, comme elles sont toutes mesurables et préservent la mesure uniforme, il serait fort intéressant d'étudier la dynamique mesurée qu'elles définissent chacune sur le tore.

Nous remercions B. Weiss de nous avoir signalé la relation avec les résultats figurant dans [JR].

2. Définitions et Notations.

Soit A un alphabet fini. On appellera A_k l'alphabet $\{0, ..., k-1\}$. On note A^* l'ensemble des suites finies ou mots de A. Un *langage* est une partie quelconque de A^*. Dans cet article $\mathbb{N}$ représente l'ensemble des entiers positifs. $A^{\mathbb{N}}$ est l'ensemble des suites infinies $\underline{x} = (x_i)_{i\in\mathbb{N}}$ où $x_i \in A$. On munit $A^{\mathbb{N}}$ de la topologie produit et du décalage $\sigma : \sigma(\underline{x}) = (x_{i+1})_{i\in\mathbb{N}}$. Un *sous-système* $S \subseteq A^{\mathbb{N}}$ est un ensemble fermé et σ invariant. Le langage associé au sous-système S est $L(S) = \{w = w_0...w_n \in A^*/\exists\ \underline{x} \in S$ tel que $w = x_0...x_n\}$. Il est bien connu que S est complétement décrit par son langage. Un couplage entre deux sous-systèmes $X \subseteq A^{\mathbb{N}}$ et $Y \subseteq B^{\mathbb{N}}$ est un sous-système $Z \subseteq A^{\mathbb{N}} \times B^{\mathbb{N}}$ dont les projections sur les première et deuxième composantes sont X et Y respectivement.

Soit $p \in \mathbb{N}$. On note $\mathbb{T}$ le tore $\mathbb{R}/\mathbb{Z}$ et on pose $[\cdot]_p = (\cdot) \bmod p$. A chaque point $x \in \mathbb{T}$ on associe l'ensemble des développements en base p,

$$T_p(x) = \{\underline{x} = (x_i)_{i\in\mathbb{N}} \in A_p^{\mathbb{N}}\ /\ x = V_p(\underline{x})\}.$$

où $V_p(\underline{x}) = [\sum_{i\in\mathbb{N}} \frac{x_i}{p^i}]_1$ est la valuation de $\underline{x}$. T_p est 1-1 sauf pour les éléments p-adiques du tore, $x = \frac{k}{p^l}$ avec $l \in \mathbb{N}$, $k \in \{0, ..., p^l - 1\}$, pour lesquels $T_p(x) = \{\underline{x}_1 = x_1...x_l0^{\infty},\ \underline{x}_2 = x_1...x_{l-1}(x_l - 1)(p-1)^{\infty}\}$.

Définition 2.1. *Soit $f : \mathbb{T} \to \mathbb{T}$ une fonction du tore. On dira que f a une représentation en base $p \in \mathbb{N}$, s'il existe un sous-système $Z_f \subseteq A_p^{\mathbb{N}} \times A_p^{\mathbb{N}}$ tel que : (i) quels que soient $x \in \mathbb{T}$, $\underline{x} \in T_p(x)$, $\underline{y} \in A_p^{\mathbb{N}}$ avec $(\underline{x}, \underline{y}) \in Z_f$ alors $\underline{y} \in T_p(f(x))$ et (ii) si on note X_E et X_S les projections de Z_f sur les première et deuxième composantes respectivement, $X_E = A_p^{\mathbb{N}}$. La condition (ii) fait de Z_f un couplage entre $A_p^{\mathbb{N}}$ et X_S.*

Le fait d'être représentable en base p est une propriété forte. Un couplage qui représente une fonction doit coupler tous les développements (il y en a au plus deux) d'un point du tore avec des développements de son image. La proposition suivante met en valeur deux propriétés cruciales des fonctions représentables.

Proposition 2.2. *Si la fonction $f : \mathbb{T} \to \mathbb{T}$ est représentable en base $p \in \mathbb{N}$, elle est continue et commute avec la multiplication par p (mod 1).*

Preuve. La continuité découle directement de la compacité du sous-système Z_f qui représente f. En effet, fixons $x \in \mathbb{T}$. Soit $(x_n)_{n\in\mathbb{N}} \subseteq \mathbb{T}$ tel que $\lim_{n\to\infty} x_n = x$ et $\lim_{n\to\infty} f(x_n) = z \in \mathbb{T}$. Il est facile de voir qu'il existe $\underline{x}_{n_k} \in T_p(x_{n_k})$, $k \in \mathbb{N}$, telle que $\lim_{k\to\infty} \underline{x}_{n_k} = \underline{x} \in T_p(x)$. Pour simplifier on va oublier les n_k. Il découle de 2.1 (ii), qu'il existe $\underline{y}_n = (y_{i,n})_{i\in\mathbb{N}} \in X_S$, $n \in \mathbb{N}$, tel que $(\underline{x}_n, \underline{y}_n) \in Z_f$. En outre, via l'extraction d'une sous-suite, on peut supposer $\lim_{n\to\infty} \underline{y}_n = \underline{y} = (y_i)_{i\in\mathbb{N}}$. Comme Z_f est fermé $(\underline{x}, \underline{y}) \in Z_f$. Mais Z_f représente f, donc

$$\lim_{n\to\infty} f(x_n) = \lim_{n\to\infty} V_p(\underline{y}_n) = z = f(x) = V_p(\underline{y}).$$

En conséquence, si on se donne une suite $(x_n)_{n\in\mathbb{N}} \subseteq \mathbb{T}$ qui converge vers x, toute sous-suite $(f(x_{n_k}))_{k\in\mathbb{N}}$ converge vers $f(x)$, d'où la continuité de f.

La commutation avec $\times p$ (mod 1) résulte immédiatement de l'invariance de Z_f par $\sigma \times \sigma$.

On s'intéresse ici avant tout aux sous-systèmes Z_f engendrés par transducteurs et automates cellulaires. En général ils ne représentent pas une fonction.

DÉFINITION 2.3. *Un transducteur est un quadruplet* $\mathcal{T} = (A_E, A_S, G, \delta)$ *où* A_E *et* A_S *sont des alphabets finis d'entrée et sortie, respectivement;* G *est un graphe orienté fini, ayant* K *pour ensemble des arcs; et enfin* $\delta : K \to A_E \times A_S$ *est la fonction de transduction : un arc* $e \in K$ *est étiqueté* $(a_E, a_S) \in A_E \times A_S$ *si* $\delta(e) = (a_E, a_S)$. *Soient* $w_E = (w_1, ..., w_n) \in A_E^*$ *et* $w_S = (w'_1, ..., w'_n) \in A_S^*$. *On dira que* w_S *est une transduction de* w_E, *et on notera* $w_S \in \mathcal{T}(w_E)$, *s'il existe un chemin sur le graphe* G, $v = e_1, ..., e_n$, *tel que* $\delta(e_i) = (w_i, w'_i)$ *pour* $i = 1, ..., n$. *Le langage associé à* $\mathcal{T}$ *est* $L(\mathcal{T}) = \{(w_E, w_S) \in A_E^* \times A_S^* \ / \ w_S \in \mathcal{T}(w_E)\}$.

Au transducteur $\mathcal{T}$ on associe deux couplages. Le premier, qu'on lit de gauche à droite, $Z_g \subseteq (A_E \times A_S)^{\mathbb{N}}$ tel que $L(Z_g) = L(\mathcal{T})$, et le second, $Z_d \subseteq (A_E \times A_S)^{\mathbb{N}}$, qu'on lit de droite à gauche, tel que $L^r(Z_d) = \{w_n ... w_1 \in (A_E \times A_S)^* / w_1 ... w_n \in L(Z_d)\} = L(\mathcal{T})$. Les transducteurs agissant de droite à gauche ont déjà été utilisés dans [BDT], pour représenter la multiplication par un nombre entier en base p. Lorsqu'une fonction f du tore peut être représentée en base p par Z_g ou Z_d, on dit qu'elle est *transductorielle* (à droite ou à gauche respectivement).

Soit $x = \sum_{i=1}^{l} \frac{b_i}{p^i} \in \mathbb{T}$, $b_i \in A_p$. L'algorithme de multiplication par un entier, $k \in \mathbb{N}$, agit sur le mot $w = b_1 ... . b_l$, de droite à gauche, de la façon suivante : si $[kx]_1 = \sum_{i=1}^{l} \frac{b'_i}{p^i}$ alors $b'_i = [kb_i + c_{i+1}]_p \in A_p$, la retenue $c_i = \lfloor \frac{kb_i + c_{i+1}}{p} \rfloor$ et $c_{l+1} = 0$ ($\lfloor \cdot \rfloor$ est la partie entière inférieure). Un calcul simple montre que $c_i \in A_k$. Dans [BDT] on décrit un transducteur qui réalise la multiplication par k en base p suivant l'algorithme ci-dessus. Les états du transducteur correspondent aux retenues et un arc entre deux retenues c et b est étiqueté par $(a, v) \in A_p \times A_p$ si et seulement si $ka + c = bp + v$.

Soit $a \in A_p$, on note $l_{a,p} \in A_k$ et $f_{a,p} \in A_p$ les entiers tels que $ka = l_{a,p}p + f_{a,p}$. Lorsqu'il n'y a pas ambiguïté par rapport à la base on écrit simplement l_a et f_a.

Le lemme suivant précise certains propriétés de l'algorithme de la multiplication.

Lemme 2.4. *Soient $p,\ k \in \mathbb{N}$.*

(i) Soit $a \in A_{p^r}$, $r \in \mathbb{N}$. Alors il existe $(b_i)_{i=1}^{r} \subseteq A_p$ tel que $ka = l_{a,p^r}p^r + \sum_{i=1}^{r} b_i p^{r-i}$.

(ii) Si k divise p (k/p), quel que soit $a \in A_p$, $f_{a,p} + k - 1 \leq p - 1$.

(iii) Si $k < p$ et k ne divise aucun puissance de p alors il existe $a_0, ..., a_{T-1} \in A_p$ tels que pour tout $j \in A_T$, $f_{a_j,p} + l_{a_{[j+1]_T}} = p - 1$ et $l_{a_{[j+1]_T}} \in A_{k-1}$.

Preuve.

(i) C'est direct.

(ii) Supposons que k divise p, donc $p = qk$, $q \in \mathbb{N}$, et $A_p = \{iq + j \ / \ i \in A_k,\ j \in A_q\}$. Si $a = iq + j \in A_p$, $ka = ikq + kj = ip + jk$ et $f_a = jk$. Finalement, $f_a + k - 1 = jk + k - 1 \leq (q - 1)k + k - 1 = p - 1$, d'où le résultat.

(iii) Supposons que $k < p$ et k ne divise aucun puissance de p. Donc, $\frac{1}{k}$ n'est pas un p-adique du tore, et son développement en base $= p$ est ultimement périodique avec partie périodique non nulle. Notons $\underline{x} = (a_0....a_T)^\infty$ la partie périodique. Il est direct que $V_p(\underline{x}) \neq 0$. Soit $\underline{y}_n = (a_0....a_{T-1})^n 0^\infty$; $\underline{y}_n$ est le développement en base p d'un point y_n du tore. Choisissons n assez grand, de façon que la suite des retenues obtenue en appliquant l'algorithme de la division par k à $\underline{y}_n$ devient aussi périodique (à gauche). Notons r_i la retenue associé à a_i. Alors $ka_i + r_{[i+1]_T} = r_i p + s_i$. Comme $k\frac{1}{k} = 1$, $s_i = 0 \vee (p-1)$. Mais y_n converge, par la gauche, vers $V_p(\underline{x})$, donc, forcement, $s_i = p - 1$. En conséquence, $ka_i + r_{[i+1]_T} = r_i p + p - 1 = l_{a_i} = p + f_{a_i} + r_{[i+1]_T}$; comme $k < p$, $f_{a_i} + r_{[i+1]_T} = p - 1$ et $l_{a_i} = r_i \in A_k$, d'où la première affirmation de (iii).

Pour finir supposons que $r_i = k - 1$ pour un certain $i \in A_T$. Donc, $ka_i + r_{[i+1]_T} = (k-1)p + p - 1 = kp - 1$, d'où $a_i = p - 1$ et $r_{[i+1]_T} = k - 1$.

En itérant on déduit que $a_i = p-1$ et $r_i = k-1$ pour tout $i \in A_T$, ce qui est une contradiction. On a donc montré que $r_i \in A_{k-1}$ et par conséquent l'affirmation (iii).

Dans cet article, on ne considère que des automates cellulaires unilatéraux.

DÉFINITION 2.5. *Soit A un alphabet fini. Un automate cellulaire (unilatéral) est une application $F : A^{\mathbb{N}} \to A^{\mathbb{N}}$ définie par :*

$$\forall\ \underline{x} = (x_i)_{i\in\mathbb{N}} \in A^{\mathbb{N}},\ i \in \mathbb{N} \quad F(\underline{x})_i = f(x_i x_{i+1} \ldots x_{i+r})$$

où $f : A^{r+1} \to A$ est une application donnée. L'entier r est appelé le rayon de l'automate cellulaire.

Soit $F : A_p^{\mathbb{N}} \to A_p^{\mathbb{N}}$ un automate cellulaire et r son rayon. F peut être vu comme un transducteur. L'ensemble d'états du transducteur est A_p^r et un état $(ab_1 \ldots b_{r-1}) \in A_p^r$ est connecté par un arc avec $(b_1 \ldots b_{r-1}b) \in A_p^r$ pour tout $b \in A$. On étiquette ce graphe par $(a, F(a, b_1, \ldots, b_{r-1}, b))$ sur l'arc qui relie les états $(a, b_1, \ldots, b_{r-1})$ et $(b_1, \ldots, b_{r-1}, b)$. De cette façon pour chaque $\underline{x} = (x_i)_{i\in\mathbb{N}} \in A_p^{\mathbb{N}}$ il existe un unique état $q = (x_1, \ldots, x_r)$ du graphe depuis lequel on lit (de gauche à droite) $\underline{x}$. On lui associe les couplages Z_d et Z_g définis ci-dessus pour les transducteurs. On dit que $f : \mathbb{T} \to \mathbb{T}$ est réalisable par automate cellulaire en base p si Z_d ou Z_g représente f (on garde la notation pour indiquer de gauche à droite et l'inverse). Dans ce cas Z_g est simplement le graphe d'une application.

3. Résultats.

Rappelons d'abord un lemme classique qui va nous servir immédiatement.

LEMME 3.1. *Soit $f : \mathbb{T} \to \mathbb{T}$ une fonction continue du tore. Il existe une fonction $g : [0,1] \to \mathbb{R}$ continue telle que $\forall\ x \in \mathbb{T},\ f(x) = [g(x)]_1$, $g(0) = f(0)$ et $(g(1) - g(0)) \in \mathbb{Z}$.*

Le résultat suivant, qui est une description complète du commutant topologique des multiplications entières (mod 1) sur le tore, est connu depuis longtemps de H. Furstenberg et B. Weiss, et affirmé sous une forme un peu plus faible dans [JR]. Nous en donnons ici une preuve simple.

PROPOSITION 3.2. *Si la fonction $f:\mathbb{T}\to\mathbb{T}$ est continue et commute avec la multiplication par $p\in\mathbb{N}$ (mod 1) alors il existe $u\in\mathbb{Z}, m\in A_p$ tels que $f(x)=[ux+\frac{m}{p-1}]_1$.*

Preuve. On obtient le résultat en résolvant une équation de récurrence relative à la fonction g du lemme précédent.

L'hypothèse de commutation se traduit, indépendamment de la continuité, par l'égalité suivante :

$$(1)\qquad (f(x)-p^l f(\frac{k+x}{p^l}))\ \in\mathbb{Z},\ \forall\ l\in\mathbb{N},\ k\in\{0,...,p^l-1\},\ x\in\mathbb{T}.$$

En fait (1) est aussi vrai pour $x=1$, en posant $f(0)=f(1)$.

D'après la proposition 2.1 et le lemme 3.1, il existe $g:[0,1]\to\mathbb{R}$ telle que pour tout $x\in[0,1],\ f(x)=[g(x)]_1$. Il s'ensuit que

$$(2)\qquad \begin{aligned} C(k,l,x)=&(g(x)-p^l g(\frac{k+x}{p^l}))\ \in\mathbb{Z},\\ &\forall\ l\in\mathbb{N},\ \forall\ k\in\{0,...,p^l-1\},\ x\in[0,1]. \end{aligned}$$

Mais toute fonction à valeurs entières continue sur l'intervalle est constante, d'où $C(k,l,x)=C(k,l)$. Calculons ces constantes. Si on évalue (2) aux points $x=0$ et $x=1$ on obtient,

$$C(k,l)=(g(0)-p^l g(\frac{k}{p^l}))\quad\text{et}\quad C(k,l)=(g(1)-p^l g(\frac{k+1}{p^l}))$$

En conséquence, si $k\in\{0,...,p^l-2\}$, $C(k+1,l)-C(k,l)=g(0)-g(1)$, qui est donc entier, et $C(0,l)=(1-p^l)g(0)$, d'où

$$C(k,l)=k(g(0)-g(1))+g(0)(1-p^l),\quad\forall\ k\in\{0,...,p^l-1\}$$

et

$$\begin{aligned} g(\frac{k}{p^l}) &= \frac{g(0)}{p^l}-\frac{C(k,l)}{p^l}\\ &= \frac{g(0)}{p^l}-\frac{k(g(0)-g(1))+g(0)(1-p^l)}{p^l}\\ &= \frac{k}{p^l}(g(1)-g(0))+g(0) \end{aligned}$$

Donc pour tous les p-adiques de $[0,1]$, $g(x) = x(g(1) - g(0)) + g(0)$; par continuité c'est aussi valable pour tout l'intervalle. Mais $g(1) - g(0) = u \in \mathbb{Z}$ et $g(0) = f(0) = v \in \mathbb{T}$, d'où $f(x) = [ux + v]_1$.

Pour finir il suffit de calculer $f(0)$. D'après (3.2), et en considérant $l = 1$, $k = 0$ et $x = 0$, on obtient que $pf(0) - f(0) = (p-1)f(0) = m \in \mathbb{Z}$. Mais $m \in A_p$, d'où le résultat.

THÉORÈME 3.3. *Si la fonction* $f : \mathbb{T} \to \mathbb{T}$ *a une représentation en base* $p \in \mathbb{N}$ *alors il existe* $u \in \mathbb{Z}, m \in A_p$ *tels que* $f(x) = [ux + \frac{m}{p-1}]_1$.

Preuve. Elle s'obtient en enchaînant les Propositions 2.2 et 3.2.

En particulier le théorème 3.2 montre que les rotations irrationnelles du tore ne sont pas représentables en base p.

On a montré dans la deuxième partie de l'article qu'avec des transducteurs agissant de droite à gauche on pouvait représenter les fonctions $f(x) = [ux]_1$, $u \in \mathbb{N}$. En fait, avec une construction analogue on peut prouver le corollaire suivante.

COROLLAIRE 3.4 Soit $p \in \mathbb{N}$. Toutes les fonctions $f(x) = [ux + \frac{m}{p-1}]_1$, $u \in \mathbb{Z}$, $m \in A_p$, sont transductorielles en base p à gauche.

Preuve. Il suffit de modifier le transducteur de multiplication par u [BDT], décrit dans la deuxième partie, de façon qu'il additionne au produit le nombre $\frac{m}{p-1}$, dont le développement est m^∞.

Un calcul simple montre que l'ensemble des retenues peut alors devenir A_{k+1}. Alors un état (une retenue) c_1 est lié à un autre, c_2, par un arc d'étiquette $(a, b) \in A_p \times A_p$, si et seulement si $ka + c_1 + \sigma = c_2 p + b$. La preuve découle des arguments de [BDT].

Maintenant on caractérise les fonctions du tore qui sont représentables par automate cellulaire. Pour les automates cellulaires on considère seulement la transduction à droite; le cas à gauche est une conséquence de l'interprétation comme transducteur.

COROLLAIRE 3.5 Une fonction $f : \mathbb{T} \to \mathbb{T}$ est réalisable par un automate cellulaire en base p à droite si et seulement si $f(x) = [ux]_1$, où u est un entier qui divise une puissance positive de p.

Preuve. Soient $p \in \mathbb{N}$ une base fixe et F un automate cellulaire de rayon r qui réalise f à droite. D'après le théorème 3.3 il existe $u \in \mathbb{Z}$ et $\sigma \in A_p$ tels que $f(x) = [ux + \frac{m}{p-1}]_1$.

Supposons r minimal : c'est donc qu'il existe $B = b_1 ... b_r \in A_p^r$ et $b \in A_p \setminus \{0\}$ tels que $F(b_1...b_r b) = a \neq F(b_1...b_r(b-1))$. Comme $\underline{x} = Bb0^\infty$ et $\underline{y} = B(b-1)(p-1)^\infty$ représentent le même élément $x \in \mathbb{T}$, $F(\underline{x})$ et $F(\underline{y})$ représentent $f(x)$. Alors, forcément, $F(\underline{x}) = a0^\infty$ et $F(\underline{y}) = (a-1)(p-1)^\infty$ ou inversement. En conséquence $f(0) = 0 = m$.

Pour finir on va calculer les valeurs de u possibles pour la représentation en base p. On considère seulement les u positifs, pour les négatifs le calcul est analogue.

Soit $u \in \mathbb{N}$ tel que u/p. D'après le lemme 2.4 (ii), pour tout $a \in A_p$, $f_a + u - 1 \leq p - 1$. Cela signifie que quel que soit $R \in A_u$, $f_a + R \leq p - 1$, et donc la retenue associée à $ua + R$ est l_a indépendamment de R. Ainsi l'algorithme de la multiplication par un entier est local. Cela nous permet de bien définir un automate cellulaire qui représente $[ux]_1$ en base p :

$$\forall\ x_0,\ x_1 \in A_p \text{ on pose } F(x_0, x_1) = [ux_0 + l_{x_1}]_p = f_{x_0} + l_{x_1}.$$

En général, si u divise p^r, d'après le lemme 2.4 (i), l'automate cellulaire est :

$$\forall\ x_0,\ x_1, ...,\ x_r \in A_p,\ F(x_0, x_1, ..., x_r) = [ux_0 + l_{x_1,...,x_r}]_p$$

où $l_{x_1,...,x_r} = l_{a,p^r}$ et $a = \sum_{i=1}^{r} x_i p^{r-i} \in A_{p^r}$.

Maintenant montrons que si u ne divise aucun puissance de p alors il n'existe pas d'automate cellulaire qui réalise la multiplication par u en base p. D'après le lemme 2.4 (i), et de façon analogue au cas précédent, on peut se restreindre au cas $u < p$.

Toujours par le lemme 2.4 (iii), il existe $a_0, ..., a_{n-1} \in A_p$ tels que pour tout $j \in A_n$: $f_{a_j} + l_{a_{[j+1]_n}} = p - 1$ avec $l_{a_j} \in A_{u-1}$. Il s'ensuit que la retenue associée à chaque a_j dans l'algorithme de la multiplication par u est soit l_{a_j} soit $(l_{a_j} + 1)$; $(l_{a_j} + 1)$ est attendu lorsque $u < p$ et ne divise pas p.

Quand a_j reçoit comme retenue $l_{a_{[j+1]_n}}$, $ua_j + l_{a_{[j+1]_n}} = l_{a_j}p + f_{a_j} + l_{a_{[j+1]_n}} = l_{a_j}p + p - 1$ et il donne comme retenue l_{a_j}, d'autre part s'il reçoit $(l_{a_{[j+1]_n}} + 1)$ il donne $l_{a_j} + 1$.

Choisissons $b,\ b' \in A_p$ tels que $ub' - f_{b'} = (l_{a_1} + 1)p$ et $ub - f_b = l_{a_1}p$.

Soit $l \in \mathbb{N}$. Si $\underline{x}^l = (a_0....a_{n-1})^l a_0 b 0^\infty$ et $\underline{y}^l = (a_0....a_{n-1})^l a_0 b' 0^\infty$, donc $[u\underline{x}^l]_1 = ((p-1)....(p-1))^l (p-1) f_b 0^\infty$ et $[u\underline{y}^l]_1 = (0....0)^l 0 f_{b'} 0^\infty$. En conséquence, s'il existe un automate cellulaire, F, qui réalise $f(x) = [ux]_1$ en base p, $F((a_0 \dots . a_{n-1})^\infty) = (p-1)^\infty$ et $F((a_0 \dots . a_{n-1})^\infty) = 0^\infty$, ce qui est une contradiction.

Remarque 3.6. Le corollaire 3.5 montre aussi une façon de construire des transducteurs à droite qui réalisent la multiplication par u en base p, quand u divise une puissance de p.

Remarque 3.7. Soit $p = p_0^{n_0} \dots p_l^{n_l} \in \mathbb{N}$, où les p_i sont des nombres premiers. Si l'on note F_{p_i} l'automate cellulaire qui réalise $f(x) = [p_i x]_1$, on obtient une factorisation du décalage, $\sigma = F_{p_0}^{n_0} \circ \dots \circ F_{p_l}^{n_l}$, où les automates F_{p_i} commutent deux à deux. Au surplus, si on considère maintenant leur action sur $A_p^{\mathbb{Z}}$, ils sont bijectifs, et donc des automorphismes du shift.

BIBLIOGRAPHIE

[B] N. Bourbaki, *Espaces vectoriels topologiques*, Masson.

[BDT] F. Blanchard, J.M. Dumont, A. Thomas, *Generic sequences, transducers and multiplication of normal numbers*, Israel journal of Math **80**, 257–287.

[BG] F. Botelho, M. Garzon, *On dynamical properties of neural networks*, Complex Systems **5** (1991), 401-413.

[JR] A. Johnson, D. J. Rudolph, *Commuting endomorphisms of the circle*, Ergodic Th. Dynam. Systems (1992).

[M] J.M. Muller, *Some characterizations of functions computable in on-line arithmetic*, Rapport LIP, 91–15.

François BLANCHARD et Bernard HOST
Laboratoire de Mathématiques Discrètes
Case 930 - 163 avenue de Luminy
13288 Marseille Cedex 09, France

Alejandro MAASS
Departamento de Ingeniería Matemática
Universidad de Chile
Casilla 170/correo 3
Santiago, Chile