Quelques propriétés des fonctions globales d'automates cellulaires

Sylvain Perifel

Le 18 janvier 2004

Résumé

Nous présentons ici quelques résultats de l'article *Endomorphisms and Automorphisms of the Shift Dynamical System* de Hedlund ([Hed69]). L'espace des configurations des automates cellulaires muni d'une métrique naturelle est compact. L'auteur utilise cette compacité pour montrer que les fonctions globales des automates cellulaires sont exactement les fonctions continues qui commutent avec le décalage. Par des méthodes mathématiques variées, et souvent grâce à cette caractérisation, il montre également de nombreux autres résultats, notamment sur les fonctions surjectives, injectives ou bijectives.

1 Introduction

L'article [Hed69] de Hedlund que l'on étudie ici aborde les automates cellulaires d'un point de vue purement mathématique. Il s'intéresse à des fonctions de $\mathcal{S}^n$ dans $\mathcal{S}$, où $\mathcal{S}$ est un ensemble fini, et n un entier strictement positif. Dans le langage des automates cellulaires, une telle fonction est la fonction de transition d'un automate cellulaire unidirectionnel de dimension 1 ayant un voisinage de n cellules, et ayant pour ensemble d'états $\mathcal{S}$. Puis il prolonge cette fonction f sur les suites bi-infinies de $\mathcal{S}$ afin d'obtenir la fonction globale f_∞ de l'automate unidirectionnel. Pour considérer les automates cellulaires en toute généralité, et pas uniquement les automates unidirectionnels, il compose ensuite ces fonctions avec le décalage σ (*shift* en anglais).

L'article est le recueil de plusieurs travaux dans ce domaine, datant des années 1960 environ. Il montre notamment des résultats de M. L. Curtis, A. M. Gleason, G. A. Hedlund, R. C. Lyndon, O. S. Rothaus et L. R. Welch. Il donne les preuves détaillées des résultats de [Hed68]. L'article est divisé en 20 parties.

On considère une métrique naturelle sur les suites bi-infinies, qui fait de cet ensemble un espace compact. Hedlund montre dans un premier temps (partie 3) que les fonctions globales des automates cellulaires sont exactement les fonctions continues qui commutent avec le décalage (Curtis, Hedlund et Lyndon). On notera cet ensemble $\mathrm{Cont}(\mathcal{S})$. Il montre ensuite (partie 5) quelques résultats intéressants sur les fonctions surjectives de $\mathrm{Cont}(\mathcal{S})$: le cardinal de l'image réciproque de tout élément est uniformément borné. Réciproquement, pour toute fonction globale non surjective il existe une configuration qui a une infinité d'antécédents. Puis il démontre le fait qu'une fonction continue, injective qui commute avec le décalage est bijective.

On définit $\mathrm{Surj}(\mathcal{S})$, $\mathrm{Bij}(\mathcal{S})$ et $\Sigma(\mathcal{S})$ comme étant les sous-ensemble de $\mathrm{Cont}(\mathcal{S})$ constitués des fonctions surjectives, bijectives, et des puissances du décalage, respectivement. Alors les inclusions $\Sigma(\mathcal{S}) \subseteq \mathrm{Bij}(\mathcal{S}) \subseteq \mathrm{Surj}(\mathcal{S}) \subseteq \mathrm{Cont}(\mathcal{S})$ sont immédiates ; en revanche, montrer que chacun des ensembles $\mathrm{Bij}(\mathcal{S}) - \Sigma(\mathcal{S})$, $\mathrm{Surj}(\mathcal{S}) - \mathrm{Bij}(\mathcal{S})$ et $\mathrm{Cont}(\mathcal{S}) - \mathrm{Surj}(\mathcal{S})$ sont infinis requiert un peu de travail, que Hedlund effectue dans la partie 6.

À partir de la partie 7, l'auteur étudie une classification des suites bi-infinies en éléments périodiques, régulièrement quasi-périodiques, isochrones, et quasi-périodiques. Il montre notamment des propriétés de densités de ces ensembles de suites. Dans les parties 8 à 12, il étudie certaines propriétés qui sont préservées par l'application d'une fonction de $\mathrm{Cont}(\mathcal{S})$ ou par sa réciproque. En particulier, il montre qu'en un certain sens, lorsque $\phi \in \mathrm{Surj}(\mathcal{S})$, le cardinal de $\phi^{-1}(x)$ est le même pour presque toute suite x (Gleason et Welch). Nous ne parlerons pas de ces travaux ici.

Dans les dernières parties, et suivant les résultats de Welch, Hedlund associe un entier à des fonctions de transition. Cela permet alors de discuter l'existence de racines continues de fonctions de $\mathrm{Surj}(\mathcal{S})$. Par exemple, il montre à la section 18 que le décalage σ n'a pas de racine continue non triviale si le cardinal de $\mathcal{S}$ est un nombre premier.

Dans ce rapport, nous présentons quelques résultats de l'article de Hedlund. Ils ont été choisis pour leur importance ou leur beauté, et pour la variété des techniques mises en œuvre dans leurs preuves. Nous espérons que ce choix reflète assez fidèlement l'esprit de l'article original.

Pour simplifier les preuves et les notations, dans ce rapport (et contrairement à Hedlund) nous prolongeons symétriquement les fonctions de transition, ce qui nous évite souvent une étape dans les preuves (celle de composition des fonctions avec le décalage).

Dans la section 2, nous introduisons les notions utiles d'ensemble de symboles, de blocs, de suites bi-infinies, etc. Nous montrons grâce au théorème de Tychonoff que la métrique introduite sur l'ensemble des suites bi-infinies le rend compact. Nous introduisons quelques ensembles de fonctions particulièrement intéressants.

Le premier résultat que nous présentons est la caractérisation de $\mathrm{Cont}(\mathcal{S})$ par les fonctions globales d'automates cellulaires (section 3). Puis nous montrons dans la section 4 que les antécédents de toute configuration par une fonction de $\mathrm{Surj}(\mathcal{S})$ sont en nombre uniformément borné. La partie suivante (section 5) est consacrée une étude (partielle) du groupe $\mathrm{Bij}(\mathcal{S})$; notamment nous déduisons que $\mathrm{Bij}(\mathcal{S}) - \Sigma(\mathcal{S})$ est infini. Enfin, la partie 6 présente certains résultats quant à l'existence de racines du décalage.

2 Préliminaires et notations

Notations générales

On note $\mathbf{Z}$ l'ensemble des entiers relatifs ; nous parlerons d'entiers pour les entiers naturels. $\mathbf{R}_+^*$ désigne l'ensemble des réels strictement positifs. Pour un réel x (ou en particulier un entier relatif), $|x|$ désigne sa valeur absolue. Si E est un ensemble, on note $|E|$ le cardinal de E. Si E et F sont deux ensembles, on note $E - F$ l'ensemble des éléments de E qui ne sont pas dans F. Si E, F

et G sont trois ensembles, et $f : E \to F$, $g : F \to G$ deux applications, on note leur composition $gf : E \to G$, *i.e.* l'application définie par $gf(x) = g(f(x))$. Si f est une application d'un ensemble E dans lui-même, et k un entier, on note f^k la fonction f itérée k fois, c'est-à-dire l'application définie inductivement par $f^0 = \mathrm{id}$, et $f^{i+1} = ff^i$ pour i entier.

Espace des suites bi-infinies

On fixe un ensemble fini $\mathcal{S}$, avec $|\mathcal{S}| > 1$. Un élément de $\mathcal{S}$ est appelé un symbole, et $\mathcal{S}$ est appelé l'ensemble des symboles. On pourra supposer sans perte de généralité que $\mathcal{S} = \{0, \dots, s-1\}$ où $s = |\mathcal{S}|$.

Si n est un entier, l'ensemble des fonctions de $\{-n, \dots, n\}$ dans $\mathcal{S}$ (mots de taille $2n+1$ sur l'alphabet $\mathcal{S}$) est noté $\mathrm{Blocs}(\mathcal{S}, n)$. Chaque élément de $\mathrm{Blocs}(\mathcal{S}, n)$ est appelé un bloc de taille n. Si u est un bloc de taille n, et $i \in \{-n, \dots, n\}$, nous écrirons u_i pour $u(i)$. Nous noterons un bloc u de taille n par l'ensemble de ses images, c'est-à-dire que nous écrirons $u = u_{-n} \dots u_n$.

Si m et n sont des entiers, en concaténant un bloc $u \in \mathrm{Blocs}(\mathcal{S}, n)$ avec un mot $v = v_1 \dots v_{2m}$ sur $\mathcal{S}$ de taille $2m$, on obtient un nouveau bloc de taille $n + m$ noté uv et défini par $uv = u_{-n} \dots u_n v_1 \dots v_{2m}$. Si V est un ensemble de mots de taille $2m$, et $u \in \mathrm{Blocs}(\mathcal{S}, n)$, on note uV l'ensemble de blocs de taille $m + n$ défini par $uV = \{uv : v \in V\}$. Par la suite, pour k entier, on notera $\mathcal{S}^k$ l'ensemble des mots de taille k sur $\mathcal{S}$. Il faut être prudent sur la notion de taille, qui diffère selon qu'on parle de bloc ou de mot : rappelons qu'un bloc de taille n est un mot de taille $2n + 1$.

En concaténant 3 blocs u, v et w de tailles respectives n_1, n_2 et n_3, on obtient un nouveau bloc noté uvw de taille $n_1 + n_2 + n_3 + 1$, défini par $uvw = u_{-n_1} \dots u_{n_1} v_{-n_2} \dots v_{n_2} w_{-n_3} \dots w_{n_3}$. Si U, V et W sont des ensembles de blocs de taille n_1, n_2, n_3 respectivement, on note UVW l'ensemble $\{uvw : u \in U, v \in V, w \in W\}$ de blocs de taille $n_1 + n_2 + n_3 + 1$. Lorsque u est un bloc, $\{u\}VW$ (resp. $V\{u\}W$, $VW\{u\}$) est abrégé par uVW (resp. VuW, VWu).

L'ensemble $\mathrm{Suites}(\mathcal{S})$ est l'ensemble $\mathcal{S}^{\mathbf{Z}}$ des fonctions de $\mathbf{Z}$ dans $\mathcal{S}$. On appelle suite bi-infinie sur $\mathcal{S}$, ou plus simplement suite si le contexte le permet, un élément de $\mathrm{Suites}(\mathcal{S})$. Si $x \in \mathrm{Suites}(\mathcal{S})$, et $i \in \mathbf{Z}$, nous écrirons x_i pour $x(i)$. Pour toute suite $x \in \mathrm{Suites}(\mathcal{S})$, et tout entier n, on note $x|_n$ la restriction de x à n, c'est-à-dire le bloc de taille n défini par $x_{-n} \dots x_n$.

Sur l'ensemble $\mathrm{Suites}(\mathcal{S})$, nous définissons une distance d par $d(x, y) = 0$ si $x = y$, et $d(x, y) = (1+k)^{-1}$ sinon, où $k = \min\{i \text{ entier} : x_i \neq y_i \text{ ou } x_{-i} \neq y_{-i}\}$. Vérifions qu'il s'agit d'une distance :

- d est à valeurs réelles positives ;
- pour tous $x, y \in \mathrm{Suites}(\mathcal{S})$, $d(x, y) = 0$ si et seulement si $x = y$;
- pour tous $x, y \in \mathrm{Suites}(\mathcal{S})$, $d(x, y) = d(y, x)$;
- inégalité triangulaire : pour tous $x, y, z \in \mathrm{Suites}(\mathcal{S})$, $d(x, z) \leq d(x, y) + d(y, z)$. En effet, c'est clair si $x = z$ ou $x = y$ ou $y = z$; on peut donc les supposer différents, et en particulier $d(x, z) = (1+k)^{-1}$ pour un entier k. Par symétrie, on peut supposer que $x_k \neq z_k$. Alors on n'a pas $x_k = y_k = z_k$, donc $d(x, y) \geq (1+k)^{-1}$ ou $d(y, z) \geq (1+k)^{-1}$, ce qui conclut.

On munit $\mathcal{S}$ de la topologie discrète (toute partie de $\mathcal{S}$ est ouverte). On vérifie alors sans difficulté que la topologie induite par la distance d est la topologie produit sur $\mathcal{S}^{\mathbf{Z}}$. En effet, une base d'ouverts pour la topologie produit est $\{\{x \in \mathrm{Suites}(\mathcal{S}) : x|_n = b\} : n \text{ entier et } b \in \mathrm{Blocs}(\mathcal{S}, n)\}$. Or $\{x \in \mathrm{Suites}(\mathcal{S}) : x|_n =$

$b\} = B(x^{(b)}, (1+n)^{-1})$ où $x^{(b)} \in \text{Suites}(\mathcal{S})$ est tel que $x^{(b)}|_n = b$, et où $B(x,r)$, pour $x \in \text{Suites}(\mathcal{S})$ et r réel, désigne la boule ouverte de centre x et de rayon r. Réciproquement, $B(x,r) = \{y \in \text{Suites}(\mathcal{S}) : y|_n = x|_n\}$ où n est le plus petit entier tel que $(1+n)^{-1} \leq r$. Donc les deux topologies coïncident.

Or la topologie discrète sur $\mathcal{S}$ en fait un compact (nombre fini d'ouverts), donc par le théorème de Tychonoff, la topologie produit fait de $\text{Suites}(\mathcal{S})$ un espace compact. Ainsi, on a la proposition suivante.

2.1 Proposition $(\text{Suites}(\mathcal{S}), d)$ est un espace métrique compact.

Rappelons qu'en particulier toute fonction continue définie sur $\text{Suites}(\mathcal{S})$ est uniformément continue (théorème de Heine). De plus, l'inverse de toute fonction continue bijective de $\text{Suites}(\mathcal{S})$ dans $\text{Suites}(\mathcal{S})$ est continu. Rappelons également que l'image d'un compact par une application continue est compacte.

Ensembles de fonctions

On note σ, et on appelle le décalage (*shift* en anglais), la fonction $\sigma : \text{Suites}(\mathcal{S}) \to \text{Suites}(\mathcal{S})$ définie par $[\sigma(x)]_i = x_{i+1}$ pour tout $i \in \mathbf{Z}$. Intuitivement, il s'agit d'un décalage vers la gauche. On note $\text{Cont}(\mathcal{S})$ l'ensemble des fonctions continues de $\text{Suites}(\mathcal{S})$ dans $\text{Suites}(\mathcal{S})$ qui commutent avec le décalage. $\text{Surj}(\mathcal{S})$ désigne le sous-ensemble de $\text{Cont}(\mathcal{S})$ constitué des fonctions surjectives. $\text{Bij}(\mathcal{S})$ est le sous-ensemble de $\text{Cont}(\mathcal{S})$ constitué des fonctions bijectives. Ainsi, $\text{Bij}(\mathcal{S}) \subseteq \text{Surj}(\mathcal{S})$. Enfin, on note $\Sigma(\mathcal{S})$ l'ensemble $\{\sigma^n : n \in \mathbf{Z}\}$ des puissances du décalage. On vérifie aisément que $\Sigma(\mathcal{S}) \subseteq \text{Bij}(\mathcal{S})$. En effet, pour tout $n \in \mathbf{Z}$, σ^n commute avec σ, et est bijectif. Il reste à montrer que σ^n est continu. Soient $x, y \in \text{Suites}(\mathcal{S})$ et $\epsilon \in \mathbf{R}_+^*$. Soit k un entier tel que $(1+k)^{-1} < \epsilon$. Alors $d(x,y) < (1+k+|n|)^{-1} \Rightarrow d(\sigma^n(x), \sigma^n(y)) < (1+k)^{-1} < \epsilon$. Donc σ^n est continue. Ces inclusions sont résumées dans la proposition suivante.

2.2 Proposition $\Sigma(\mathcal{S}) \subseteq \text{Bij}(\mathcal{S}) \subseteq \text{Surj}(\mathcal{S}) \subseteq \text{Cont}(\mathcal{S})$.

Pour un entier n, l'ensemble des fonctions de $\text{Blocs}(\mathcal{S}, n)$ dans $\mathcal{S}$ est noté $\text{F}(\mathcal{S}, n)$. Si $f \in \text{F}(\mathcal{S}, n)$ et m est un entier, f_m désigne la fonction de $\text{Blocs}(\mathcal{S}, n+m)$ dans $\text{Blocs}(\mathcal{S}, m)$ définie par

$$f_m(u_{-n-m} \dots u_{n+m}) =$$
$$f(u_{-n-m} \dots u_{n-m}) f(u_{-n-m+1} \dots u_{n-m+1}) \dots f(u_{-n+m} \dots u_{n+m})$$

On remarque que $f_0 = f$.

2.3 Remarque Dans son article [Hed69], Hedlund définit les blocs de taille n comme des mots $x_1 \dots x_n$ de taille n, et à partir d'une fonction f des blocs de taille n dans $\mathcal{S}$, il définit $[f_m(x_1 \dots x_{n+m-1})]_i = f(x_i \dots x_{i+n-1})$. Cette définition non symétrique l'oblige ensuite à composer les fonctions avec des puissances du décalage pour obtenir la classe $\text{F}_\infty(\mathcal{S})$ que l'on considère plus loin. Nous préférons la définition symétrique d'un bloc de taille n comme étant un mot de taille $2n+1$, car elle permet de simplifier les preuves et les notations, ce qui a demandé toutefois de remanier certains passages techniques.

De la même façon, on définit $f_\infty : \text{Suites}(\mathcal{S}) \to \text{Suites}(\mathcal{S})$ par $[f_\infty(x)]_i = f(x_{i-n} \dots x_{i+n})$ pour tout $i \in \mathbf{Z}$. Pour n entier, $f \in \text{F}(\mathcal{S}, n)$ peut être vue comme la fonction de transition d'un automate cellulaire de dimension 1, avec un voisinage de plus proches voisins de taille $2n+1$. f_∞ correspond alors à la fonction globale de l'automate cellulaire.

2.4 Remarque Pour tous $k \in \mathbf{Z}$, n entier et $f \in \mathrm{F}(\mathcal{S}, n)$, $f(\sigma^k(x)|_n) = [f_\infty(x)]_k$.

Pour n entier, $\mathrm{F}_\infty(\mathcal{S}, n)$ désigne l'ensemble de fonctions $\{f_\infty : f \in \mathrm{F}(\mathcal{S}, n)\}$. On note $\mathrm{F}_\infty(\mathcal{S}) = \cup_{n\geq 0}\mathrm{F}_\infty(\mathcal{S}, n)$.

3 Caractérisation de $\mathrm{Cont}(\mathcal{S})$

Curtis, Hedlund et Lyndon ont montré que les fonctions continues qui commutent avec le décalage sont exactement les fonctions globales des automates cellulaires. Ce résultat découle immédiatement des deux lemmes qui suivent.

3.1 Lemme Soient n un entier, et $f \in \mathrm{F}(\mathcal{S}, n)$. Alors f_∞ est continue et commute avec le décalage.

Preuve Soit $x \in \mathrm{Suites}(\mathcal{S})$ et posons $y = f_\infty(x)$. Montrons tout d'abord que f_∞ est continue en x. Soit $\epsilon \in \mathbf{R}_+^*$. Soient k entier tel que $(1+k)^{-1} < \epsilon$, et $\eta \in \mathbf{R}_+^*$ tel que $\eta < (1+k+n)^{-1}$. Prenons $u \in \mathrm{Suites}(\mathcal{S})$ tel que $d(x, u) < \eta$. Alors pour $i \in \mathbf{Z}$ tel que $-n-k \leq i \leq n+k$, $u_i = x_i$. Donc si l'on appelle $v = f_\infty(u)$, on a $v|_k = y|_k$, d'où $d(y, v) < (1+k)^{-1} < \epsilon$. Donc f_∞ est continue.

Montrons maintenant que f_∞ commute avec σ. Pour $i \in \mathbf{Z}$, $[\sigma f_\infty(x)]_i = y_{i+1}$, et $[f_\infty \sigma(x)]_i = f([\sigma(x)]_{i-n} \dots [\sigma(x)]_{i+n}) = f(x_{i-n+1} \dots x_{i+n+1}) = y_{i+1}$, donc f_∞ commute avec σ. □

3.2 Lemme Soit $\phi \in \mathrm{Cont}(\mathcal{S})$. Alors il existe un entier n et $f \in \mathrm{F}(\mathcal{S}, n)$ tels que $\phi = f_\infty$.

Preuve On suppose que $\mathcal{S} = \{0, \dots, s-1\}$, où $s = |\mathcal{S}|$. Pour i entier, $i < s$, on pose $U_i = \{x \in \mathrm{Suites}(\mathcal{S}) : x_0 = i\}$, et $V_i = \phi^{-1}(U_i)$. Alors pour $i \neq j$, pour $x \in U_i$ et $y \in U_j$, $d(x, y) = 1$. L'espace $\mathrm{Suites}(\mathcal{S})$ étant compact (proposition 2.1), ϕ est uniformément continue : il existe $\eta \in \mathbf{R}_+^*$ tel que pour tous $x, y \in \mathrm{Suites}(\mathcal{S})$, $d(x, y) < \eta \Rightarrow d(\phi(x), \phi(y)) < 1$. On en déduit que pour $i \neq j$, pour tous $x \in V_i$ et $y \in V_j$, $d(x, y) \geq \eta$. On fixe un entier n tel que $(1+n)^{-1} \leq \eta$.

Soit B_i le sous-ensemble de $\mathrm{Blocs}(\mathcal{S}, n)$ défini par $\{x|_n : x \in V_i\}$. Alors $\cup_{i=0}^{s-1} B_i = \mathrm{Blocs}(\mathcal{S}, n)$. En effet, puisque $\mathrm{Suites}(\mathcal{S}) = \cup_{i=0}^{s-1} U_i$, on a $\mathrm{Suites}(\mathcal{S}) = \cup_{i=0}^{s-1} V_i$, et tout bloc de $\mathrm{Blocs}(\mathcal{S}, n)$ est la restriction d'un élément d'un V_i. De plus, par le choix de n, les ensembles B_i $(0 \leq i < s)$ sont disjoints. En effet, si $i \neq j$, et $b \in B_i$, $c \in B_j$, alors $b = x|_n$, $c = y|_n$ et $d(x, y) \geq (1+n)^{-1}$. Donc b et c ne coïncident pas.

On définit $f : \mathrm{Blocs}(\mathcal{S}, n) \to \mathcal{S}$ par $f(b) = i$ si $b \in B_i$. Par les remarques précédentes, f est bien définie. Montrons alors que $\phi = f_\infty$. Soit $x \in \mathrm{Suites}(\mathcal{S})$ et $y = \phi(x)$. Soit $i = y_0$: $y \in U_i$ donc $x \in V_i$ donc $x|_n \in B_i$ donc $f(x|_n) = i = y_0 = [\phi(x)]_0$. De la même façon, si $k \in \mathbf{Z}$ on a $f(\sigma^k(x)|_n) = [\phi(\sigma^k(x))]_0 = [\sigma^k(\phi(x))]_0 = y_k$ (car ϕ commute avec le décalage), ce qui montre que $f_\infty = \phi$ par la remarque 2.4. □

On en déduit le théorème suivant.

3.3 Théorème (Curtis, Hedlund et Lyndon) $\mathrm{F}_\infty(\mathcal{S}) = \mathrm{Cont}(\mathcal{S})$

3.4 Corollaire Cont($\mathcal{S}$) est infini dénombrable.

Preuve $\mathrm{F}_\infty(\mathcal{S})$ est infini, puisque pour tout n, si $f, g \in \mathrm{F}(\mathcal{S}, n)$ sont différentes, alors $f_\infty \neq g_\infty$. Donc $|\mathrm{F}_\infty(\mathcal{S})| \geq |\mathrm{F}(\mathcal{S}, n)| = |\mathcal{S}|^{|\mathcal{S}|^{2n+1}}$ pour tout n. En outre, $\mathrm{F}_\infty(\mathcal{S})$ est la réunion dénombrable des ensembles finis $\mathrm{F}_\infty(\mathcal{S}, n)$, donc est dénombrable. □

4 Quelques propriétés de Surj($\mathcal{S}$)

Nous montrons ici quelques résultats concernant la classe Surj($\mathcal{S}$) des fonctions continues surjectives commutant avec le décalage.

4.1 Proposition Soient n un entier et $f \in \mathrm{F}(\mathcal{S}, n)$. Alors f_∞ est surjective si et seulement si pour tout entier m, f_m est surjective.

Preuve Supposons que f_∞ est surjective. Soient m un entier et $b \in \mathrm{Blocs}(\mathcal{S}, m)$, $b = b_{-m} \ldots b_m$. Soit $y \in \mathrm{Suites}(\mathcal{S})$ défini par $y_i = b_i$ pour $-m \leq i \leq m$ et y_i quelconque pour $|i| > m$. f_∞ étant surjective, il existe $x \in \mathrm{Suites}(\mathcal{S})$ tel que $f_\infty(x) = y$. En particulier, $f_m(x|_{n+m}) = b$. Ainsi, f_m est surjective.

Supposons maintenant que pour tout entier m, f_m est surjective. Soient $u \in \mathrm{Suites}(\mathcal{S})$ et m un entier. Alors il existe $b \in \mathrm{Blocs}(\mathcal{S}, n+m)$ tel que $f_m(b) = u|_m$. On définit $x \in \mathrm{Suites}(\mathcal{S})$ par $x_i = b_i$ si $-n-m \leq i \leq n+m$, et x_i quelconque si $|i| > n+m$. Soit $y = f_\infty(x)$. Alors $y|_m = u|_m$, donc $d(y, u) < (1+m)^{-1}$. On a choisi u et m arbitraires, donc $f_\infty(\mathrm{Suites}(\mathcal{S}))$ est dense dans Suites($\mathcal{S}$). Or f_∞ est continue, et Suites($\mathcal{S}$) est compact, donc $f_\infty(\mathrm{Suites}(\mathcal{S}))$ est compact, donc fermé. Ainsi, $f_\infty(\mathrm{Suites}(\mathcal{S})) = \mathrm{Suites}(\mathcal{S})$, d'où la surjectivité de f_∞. □

Nous allons maintenant montrer que si $\phi \in \mathrm{Surj}(\mathcal{S})$, alors il existe un entier M tel que pour tout $x \in \mathrm{Suites}(\mathcal{S})$, $|\phi^{-1}(x)| \leq M$. Pour cela, nous passons par deux lemmes techniques.

4.2 Lemme Soient n un entier et $f \in \mathrm{F}(\mathcal{S}, n)$. Supposons qu'il existe un entier m et un bloc $v \in \mathrm{Blocs}(\mathcal{S}, m)$ tels que $k = |f_m^{-1}(v)| > 0$. Si pour tous $a, b \in \mathcal{S}$, $|f_{m+1}^{-1}(avb)| \geq k$, alors pour tous $a, b \in \mathcal{S}$, $|f_{m+1}^{-1}(avb)| = k$.

Preuve Notons $U = f_m^{-1}(v)$. Alors $f_{m+1}^{-1}(\mathcal{S}v\mathcal{S}) = \mathcal{S}U\mathcal{S}$. En effet, pour $u \in \mathrm{Blocs}(\mathcal{S}, m)$ et $a, b \in \mathcal{S}$, $f_{m+1}(aub) \in \mathcal{S}v\mathcal{S}$ si et seulement si $f_m(u) = v$, donc $\{x \in \mathrm{Blocs}(\mathcal{S}, m+1) : f_{m+1}(x) \in \mathcal{S}v\mathcal{S}\} = \mathcal{S}U\mathcal{S}$.

Ainsi, puisque $|U| = k$, $|f_{m+1}^{-1}(\mathcal{S}v\mathcal{S})| = k|\mathcal{S}|^2 = \sum_{a,b\in\mathcal{S}} |f_m^{-1}(avb)|$. Comme la somme a $|\mathcal{S}|^2$ termes, on en déduit que, si pour tous $a, b \in \mathcal{S}$, $|f_{m+1}^{-1}(avb)| \geq k$, alors pour tous $a, b \in \mathcal{S}$, $|f_{m+1}^{-1}(avb)| = k$. □

4.3 Lemme Soient n un entier, et $f \in \mathrm{F}(\mathcal{S}, n)$. Supposons qu'il existe un entier m et un bloc $v \in \mathrm{Blocs}(\mathcal{S}, m)$ tels que $k = |f_m^{-1}(v)| > 0$, et tels que pour tous mots w et w' sur $\mathcal{S}$ de taille $2n$, $|f_{3m+2n+1}^{-1}(vwvw'v)| = k$. Alors $k = |\mathcal{S}|^{2n}$.

Preuve Notons $U = f_m^{-1}(v)$, de cardinal k. Pour simplifier les notations, notons $W = \mathcal{S}^{2n}$ l'ensemble des mots sur $\mathcal{S}$ de taille $2n$. Alors $f_{3m+2n+1}^{-1}(vWvWv) = UUU$. En effet, si $x \in UUU$, alors $x = u_1u_2u_3$ avec $u_1, u_2, u_3 \in U$. Ainsi, $f_{3m+2n+1}(x) = vwvw'v$ où w et w' sont des mots de taille $2n$. Réciproquement, supposons que $f_{3m+2n+1}(x) = vwvw'v$ où $w, w' \in W$ et $x \in \mathrm{Blocs}(\mathcal{S}, 3m+3n+$

1). Alors $x = x_1x_2x_3$ avec $x_i \in \text{Blocs}(\mathcal{S}, m+n)$, et $f_m(x_i) = v$, donc $x_i \in U$, pour $1 \leq i \leq 3$.

Par hypothèse, pour tous mots $w, w' \in W$, $|f_{3m+2n+1}^{-1}(vwvw'v)| = k$, donc $k|\mathcal{S}|^{4n} = \sum_{w,w' \in W} |f_{3m+2n+1}^{-1}(vwvw'v)| = |UUU| = k^3$. Ainsi, $k = |\mathcal{S}|^{2n}$. □

4.4 Théorème Soient n un entier et $f \in \mathrm{F}(\mathcal{S}, n)$. Alors f_∞ est surjective si et seulement si pour tout entier m et tout $v \in \text{Blocs}(\mathcal{S}, m)$, $|f_m^{-1}(v)| = |\mathcal{S}|^{2n}$.

Preuve Si pour tout entier m et tout $v \in \text{Blocs}(\mathcal{S}, m)$, $|f_m^{-1}(v)| = |\mathcal{S}|^{2n}$, alors en particulier f_m est surjective quelque soit m. Donc par la proposition 4.1, f_∞ est surjective.

Supposons maintenant f_∞ surjective. Posons $k = \min(\cup_{m \geq 0}\{|f_m^{-1}(v)| : v \in \text{Blocs}(\mathcal{S}, m)\})$. Par la proposition 4.1, $k \geq 1$. Soit m un entier et $u \in \text{Blocs}(\mathcal{S}, m)$ tels que $|f_m^{-1}(u)| = k$. Alors pour tous $a, b \in \mathcal{S}$, $|f_{m+1}^{-1}(aub)| \geq k$. Par le lemme 4.2, on a donc $|f_{m+1}^{-1}(aub)| = k$ pour tous $a, b \in \mathcal{S}$. Par induction, on obtient que pour tout entier p et tous blocs $x, y \in \text{Blocs}(\mathcal{S}, p)$, $|f_{m+2p+1}^{-1}(xuy)| = k$. En particulier, pour tous mots w et w' sur $\mathcal{S}$ de taille $2n$, on a $|f_{3m+2n+1}^{-1}(uwuw'u)| = k$. Par le lemme 4.3, on obtient que $k = |\mathcal{S}|^{2n}$, et ainsi $|f_p^{-1}(v)| \geq |\mathcal{S}|^{2n}$ pour tout entier p et tout $v \in \text{Blocs}(\mathcal{S}, p)$.

Supposons maintenant qu'il existe un entier p et un bloc $u \in \text{Blocs}(\mathcal{S}, p)$ tel que $|f_p^{-1}(u)| > |\mathcal{S}|^{2n}$. Puisque pour tout $v \in \text{Blocs}(\mathcal{S}, p)$, $|f_p^{-1}(v)| \geq |\mathcal{S}|^{2n}$, on en déduit que $\sum_{v \in \text{Blocs}(\mathcal{S},p)} |f_p^{-1}(v)| > |S|^{2n+2p+1}$. Mais d'un autre côté, $f_p^{-1}(\text{Blocs}(\mathcal{S}, p)) = \text{Blocs}(\mathcal{S}, p+n)$, donc $\sum_{v \in \text{Blocs}(\mathcal{S},p)} |f_p^{-1}(v)| = |\text{Blocs}(\mathcal{S}, p+n)| = |S|^{2n+2p+1}$. Contradiction. Ainsi, pour tous p entier et $v \in \text{Blocs}(\mathcal{S}, p)$, $|f_p^{-1}(v)| = |\mathcal{S}|^{2n}$. □

4.5 Corollaire Soient n un entier, et $f \in \mathrm{F}(\mathcal{S}, n)$ telle que f_∞ soit surjective. Alors pour tout $x \in \text{Suites}(\mathcal{S})$, $|f_\infty^{-1}(x)| \leq |\mathcal{S}|^{2n}$.

Preuve Supposons que pour un certain $y \in \text{Suites}(\mathcal{S})$, $|f_\infty^{-1}(y)| > |\mathcal{S}|^{2n}$. Alors il existe un entier $r > |\mathcal{S}|^{2n}$ et un ensemble $\{x^{(i)} \in \text{Suites}(\mathcal{S}) : 1 \leq i \leq r\}$ tel que $f_\infty(x^{(i)}) = y$ pour $1 \leq i \leq r$. Puisque r est fini, il existe un entier $k \geq n$ pour lequel $x^{(i)}|_k \neq x^{(j)}|_k$ dès que $i \neq j$. Alors $f_{k-n}(x^{(i)}|_k) = y|_{k-n}$, donc $|f_{k-n}^{-1}(y|_{k-n})| \geq r > |\mathcal{S}|^{2n}$, contradiction avec le théorème 4.4. □

4.6 Corollaire Si $\phi \in \text{Surj}(\mathcal{S})$, alors il existe un entier M tel que pour tout $x \in \text{Suites}(\mathcal{S})$, $|\phi^{-1}(x)| \leq M$.

Preuve ϕ s'écrit f_∞ pour un certain $f \in \mathrm{F}(\mathcal{S}, n)$ et pour un certain entier n, d'après le théorème 3.3. On conclut par le corollaire 4.5 en prenant $M = |\mathcal{S}|^{2n}$. □

Comme indiqué dans l'introduction, la réciproque est vraie. Nous n'en détaillons pas la preuve (plus technique) ici. On obtient alors la caractérisation suivante.

4.7 Théorème Soit $\phi \in \text{Cont}(\mathcal{S})$. Alors ϕ est surjective si et seulement s'il existe un entier M tel que pour tout $x \in \text{Suites}(\mathcal{S})$, $|\phi^{-1}(x)| \leq M$.

5 $\text{Bij}(\mathcal{S}) - \Sigma(\mathcal{S})$ est infini

Rappelons que nous supposons que $|\mathcal{S}| \geq 2$. En effet, dans le cas où $\mathcal{S}$ ne contient qu'un seul symbole, il n'y a qu'une suite bi-infinie sur $\mathcal{S}$, ce qui n'est guère intéressant.

5.1 Remarque $\text{Bij}(\mathcal{S})$ est un groupe pour la composition de fonctions. En effet,

- la composition est une opération interne, puisque si ϕ et ψ sont continues, commutent avec le décalage et sont bijectives, alors $\phi\psi$ aussi ;
- la composition est associative ;
- l'élément neutre est l'identité ;
- si ϕ est continue, commute avec le décalage et est bijective, alors ϕ^{-1} est continue (puisque $\text{Suites}(\mathcal{S})$ est compact), bijective, et commute avec le décalage, car $\phi^{-1}\sigma(x) = (\sigma^{-1}\phi)^{-1}(x) = (\phi\sigma^{-1})^{-1}(x) = \sigma\phi^{-1}(x)$.

Nous allons montrer que tout groupe fini est isomorphe à un sous-groupe de $\text{Bij}(\mathcal{S})$. Pour cela, nous avons besoin d'un lemme technique (lemme 5.3), qui repose sur la définition suivante.

5.2 Définition Soient m et n deux entiers, $u \in \text{Blocs}(\mathcal{S}, m)$ et $v \in \text{Blocs}(\mathcal{S}, n)$. On dit que u et v se recouvrent lorsqu'il existe un entier k tel que $1 \leq k \leq \min(2m+1, 2n+1)$ et $u_{-m} \dots u_{-m+k-1} = v_{n-k+1} \dots v_n$ ou $u_{m-k+1} \dots u_m = v_{-n} \dots v_{-n+k-1}$. Si u et v se recouvrent, on dit que la paire (u, v) se recouvre.

On suppose $\mathcal{S}$ de la forme $\mathcal{S} = \{0, 1, \dots, s-1\}$ où $s = |\mathcal{S}| \geq 2$.

5.3 Lemme Soit n un entier. Soient $e, e' \in \text{Blocs}(\mathcal{S}, n+1)$ définis par $e = 1^{2n+3} = 11\dots1$ et $e' = (01)^{n+1}0 = 0101\dots010$. On pose B le sous-ensemble de $\text{Blocs}(\mathcal{S}, 3n+4)$ défini par $B = e0\text{Blocs}(\mathcal{S}, n)0e'$. Alors aucune paire d'éléments de B ne se recouvre.

Preuve Soient $u, v \in B$ tels que $u \neq v$. Alors $u = e0c_{-n} \dots c_n 0e'$ et $v = e0d_{-n} \dots d_n 0e'$ avec $c_{-n} \dots c_n \neq d_{-n} \dots d_n$. Supposons que u et v se recouvrent. Par symétrie, on peut supposer qu'il existe un entier $1 \leq k < 6n+9$ tel que $u_{-3n-4} \dots u_{-3n-5+k} = v_{3n+5-k} \dots v_{3n+4}$.

Supposons que $k \leq 2n+3$. Alors le début de e coïncide avec la fin de e', contradiction car e ne contient pas 0. Ainsi, $k > 2n+3$. Donc v contient une copie de e, ailleurs qu'au début, ce qui est impossible puisque la taille de e est strictement supérieure à $2n+1$. □

Curtis, Hedlund et Lyndon ont montré le résultat suivant.

5.4 Théorème Tout groupe fini est isomorphe à un sous-groupe de $\text{Bij}(\mathcal{S})$.

Preuve L'on sait par le théorème de Cayley que tout groupe fini d'ordre n est isomorphe à un sous-groupe du groupe symétrique $\mathfrak{S}_n$ (tout groupe fini agit sur lui-même par translation, ce qui définit un morphisme injectif du groupe dans $\mathfrak{S}_n$). Or $\mathfrak{S}_n$ est un sous-groupe du groupe $\mathfrak{P}_n$ des permutations sur $\text{Blocs}(\mathcal{S}, n)$ ($\mathfrak{P}_n \simeq \mathfrak{S}_{|\mathcal{S}|^{2n+1}}$), puisque lorsque $|\mathcal{S}| \geq 2$, $|\mathcal{S}|^{2n+1} \geq n$. Il suffit donc de montrer que $\text{Bij}(\mathcal{S})$ contient un sous-groupe isomorphe à $\mathfrak{P}_n$ pour tout entier n.

Pour cela, à toute permutation $\pi \in \mathfrak{P}_n$, on associe une fonction $\phi_\pi \in \mathrm{Bij}(\mathcal{S})$, de sorte que $\pi \mapsto \phi_\pi$ soit un morphisme injectif. Si $\pi \in \mathfrak{P}_n$, on définit $\phi_\pi \in \mathrm{Bij}(\mathcal{S})$ comme suit. Soit $x \in \mathrm{Suites}(\mathcal{S})$; décrivons $y = \phi_\pi(x)$. Soient B défini comme dans le lemme 5.3, et $i_B = 6n + 9$ la taille des mots de B. Soit $i \in \mathbf{Z}$. S'il existe $k \in \mathbf{Z}$ tel que $k \leq i < k + i_B$ et $x_k \dots x_{k+i_B-1} = e0c_{-n} \dots c_n 0e' \in B$, alors on définit $y_k \dots y_{k+i_B-1} = e0\pi(c_{-n} \dots c_n)0e'$. Sinon, on définit $y_i = x_i$. Puisque deux blocs de B ne peuvent pas se recouvrir, y est bien défini.

Par la définition de ϕ_π, il est clair que $\phi_{\mathrm{id}} = \mathrm{id}$ et que $\phi_{\pi^{-1}}\phi_\pi = \mathrm{id}$, ce qui montre en particulier que ϕ_π est bijectif. Plus généralement, on remarque que $\phi_\alpha\phi_\beta = \phi_{\alpha\beta}$ pour toutes permutations $\alpha, \beta \in \mathfrak{P}_n$. En outre, on voit que ϕ_π commute avec le décalage. Enfin, $\pi \mapsto \phi_\pi$ est injectif puisque dès que $\alpha, \beta \in \mathfrak{P}_n$ diffèrent, disons $\alpha(a) \neq \beta(a)$ pour un certain $a \in \mathrm{Blocs}(\mathcal{S}, n)$, alors si $x \in \mathrm{Suites}(\mathcal{S})$ est tel que $x|_{3n+4} = e0a0e'$, $\phi_\alpha(x) \neq \phi_\beta(x)$.

Il reste donc seulement à montrer que ϕ_π est continue. Soient $x \in \mathrm{Suites}(\mathcal{S})$ et $\epsilon \in \mathbf{R}_+^*$. Soit un entier m tel que $(1+m)^{-1} < \epsilon$. Alors dès que $y \in \mathrm{Suites}(\mathcal{S})$ est tel que $d(x, y) < (1 + m + i_B)^{-1}$, $\phi_\pi(x)|_m = \phi_\pi(y)|_m$, donc $d(\phi_\pi(x), \phi_\pi(y)) < \epsilon$. □

5.5 Corollaire $\mathrm{Bij}(\mathcal{S}) - \Sigma(\mathcal{S})$ est infini.

Preuve Par le théorème 5.4, pour tout entier $n > 1$ il existe un élément de $\mathrm{Bij}(\mathcal{S})$ d'ordre n (par exemple l'image du n-cycle $(12 \dots n)$). Il n'est pas dans $\Sigma(\mathcal{S})$ puisque tous les éléments de $\Sigma(\mathcal{S})$ sont soit d'ordre infini, soit d'ordre 1 (l'identité). Donc $\mathrm{Bij}(\mathcal{S}) - \Sigma(\mathcal{S})$ est infini. □

6 Racines de puissances du décalage

Dans cette section, pour $p \in \mathbf{Z}$, on s'intéresse aux fonctions $\phi \in \mathrm{Cont}(\mathcal{S})$ telles qu'il existe un entier q tel que $\phi^q = \sigma^p$. Le diagramme espace-temps d'un tel automate cellulaire est régulier, en ce sens qu'après q itérations, on retrouve la configuration initiale décalée de p. On montre que lorsque $|\mathcal{S}|$ est un nombre premier, alors q divise p. Pour cela, pour n entier quelconque, si $f \in \mathrm{F}(\mathcal{S}, n)$ est telle que $f_\infty \in \mathrm{Surj}(\mathcal{S})$, on associe à f un entier $R(f)$, tel que pour des fonctions f et g, $R(fg) = R(f)R(g)$ (proposition 6.4).

La majeure partie du travail consiste en la proposition 6.4. Le lemme 6.1 est général et sert dans le théorème 6.5 ; le lemme 6.2 permet de définir $R(f)$; le lemme 6.3 est utile pour établir la proposition 6.4. On suppose encore dans cette partie que $|\mathcal{S}| \geq 2$.

Soient m et n deux entiers. Lorsque cela ne prête pas à confusion, si $f \in \mathrm{F}(\mathcal{S}, m)$ et $g \in \mathrm{F}(\mathcal{S}, n)$, nous écrirons fg pour désigner la fonction de $\mathrm{F}(\mathcal{S}, n+m)$ définie par $fg = f(g_m)$. Cet abus de notation allège l'écriture. f^0 désigne alors l'identité sur $\mathrm{Blocs}(\mathcal{S}, 0) = \mathcal{S}$, et pour $k \geq 1$ entier, f^k est définie inductivement par $f^k = ff^{k-1}$.

Nous utiliserons des dessins pour représenter la situation dans les preuves. Soient m et n des entiers, et $f \in \mathrm{F}(\mathcal{S}, n)$. Si $x \in \mathrm{Blocs}(\mathcal{S}, n + m)$ et $y \in \mathrm{Blocs}(\mathcal{S}, m)$ sont tels que $y = f_m(x)$, alors on dessine un trapèze dont la base est de longueur $2(n + m) + 1$ et est étiquetée par x, et le côté opposé est de longueur $2m + 1$ et étiqueté par y. Pour la composition fg de deux fonctions $f \in \mathrm{F}(\mathcal{S}, m)$ et $g \in \mathrm{F}(\mathcal{S}, n)$, on empile deux trapèzes. Voir figure 1. S'il y a ambiguïté sur la place des mots dans les dessins, on ajoute de petits délimiteurs verticaux.

FIG. 1 – Exemples de représentation graphique.

6.1 Lemme Soient n un entier, $f \in \mathrm{F}(\mathcal{S}, n)$ et $p \in \mathbf{Z}$. Si $f_\infty = \sigma^p$, alors $n \geq |p|$.

Preuve Supposons que $n < |p|$. Soient $x, y \in \mathrm{Suites}(\mathcal{S})$ tels que $x|_n = y|_n$ et $x_p \neq y_p$. Si $f_\infty = \sigma^p$, alors $x_p = [f_\infty(x)]_0 = [f_\infty(y)]_0 = y_p$: contradiction. Donc f_∞ ne peut pas être égal à σ^p. □

Soient m, n et k des entiers, avec $n \leq k \leq n+m$. À chaque triplet (f, u, v) où $f \in \mathrm{F}(\mathcal{S}, n)$ est telle que $f_\infty \in \mathrm{Surj}(\mathcal{S})$, et où $u \in \mathrm{Blocs}(\mathcal{S}, k)$, $v \in \mathrm{Blocs}(\mathcal{S}, m)$, on associe un entier $R(f, u, v)$ défini par $R(f, u, v) = |u\mathcal{S}^{2(m+n-k)} \cap f_m^{-1}(v)| = |\{w \in \mathcal{S}^{2(m+n-k)} : f_m(uw) = v\}|$. C'est le nombre de façons de prolonger u de sorte que son image par f (plus précisément, par f_m) soit v. Voir figure 2. Notons que par le théorème 4.4, $R(f, u, v) \leq |S|^{2n}$. On peut donc définir maintenant $R(f, u) = \max_{m \geq k-n} \max_{v \in \mathrm{Blocs}(\mathcal{S}, m)} R(f, u, v)$. C'est le nombre maximal de façons de prolonger u pour obtenir toujours la même image par f. Remarquons que $R(f, u) \geq R(f, u, f_{k-n}(u)) = 1$.

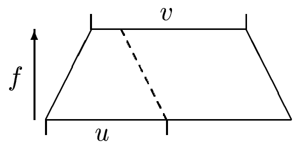

FIG. 2 – Illustration de $R(f, u, v)$.

6.2 Lemme Soient n, k et k' des entiers, $k, k' \geq n$, et $f \in \mathrm{F}(\mathcal{S}, n)$ telle que $f_\infty \in \mathrm{Surj}(\mathcal{S})$. Alors pour tous $u \in \mathrm{Blocs}(\mathcal{S}, k)$ et $u' \in \mathrm{Blocs}(\mathcal{S}, k')$, $R(f, u) = R(f, u')$.

Preuve Soient m entier tel que $m + n \geq k$, $v \in \mathrm{Blocs}(\mathcal{S}, m)$ et $W = u\mathcal{S}^{2(m+n-k)} \cap f_m^{-1}(v)$ tels que $|W| = R(f, u)$. Alors pour tout $a \in \mathcal{S}$, tous les $u'auw \in u'aW$ ont la même image par f, car la taille du bloc u est $k \geq n$. Voir figure 3. Ainsi, si l'on prolonge u' par un mot de aW, on obtient toujours la même image par f : en symboles, cela s'écrit

$$u'aW \subseteq u'\mathcal{S}^{2(m+n+1)} \cap f_{m+k'+1}^{-1}(f_{k+k'-n+1}(u'au)v_{-m+2(k-n)+1} \cdots v_m)$$

Donc $R(f, u') \geq |u'aW| = |W| = R(f, u)$.

Symétriquement, on a $R(f, u) \geq R(f, u')$. □

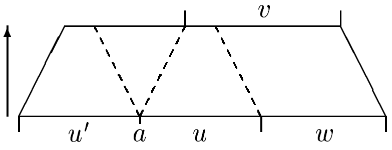

FIG. 3 – Illustration du lemme 6.2.

Pour n entier et $f \in \mathrm{F}(\mathcal{S}, n)$ telle que $f_\infty \in \mathrm{Surj}(\mathcal{S})$, en vertu du lemme précédent, on peut donc définir $R(f)$ par $R(f, u)$ pour $u \in \mathrm{Blocs}(\mathcal{S}, k)$ $(k \geq n)$ quelconque. En particulier, pour tout $u \in \mathrm{Blocs}(\mathcal{S}, k)$, il existe un bloc v (de taille au moins $k - n$) tel que $R(f, u, v) = R(f)$.

6.3 Lemme Soient m, n et k des entiers, $f \in \mathrm{F}(\mathcal{S}, n)$, $u \in \mathrm{Blocs}(\mathcal{S}, k)$, $v \in \mathrm{Blocs}(\mathcal{S}, m)$, avec $n \leq k \leq n + m$ et $f_\infty \in \mathrm{Surj}(\mathcal{S})$. Si $R(f, u, v) = R(f)$, alors pour tout mot w de taille $2l$ où $l > n$, $R(f, u, vw) = R(f)$.

Preuve Soient $l > n$ un entier, et w un mot de taille $2l$. Soient w' et w'' les deux mots tels que $w = w'w''$ et w' est de taille $2n + 1$. Nous allons montrer que pour tout z de la taille de w', $R(f, u, vzw'') = R(f)$.

Soient x un mot de taille $2(m + n - k)$ et y un mot de taille $2l - 1$ tels que $f_m(ux) = v$ et $f_{l-n-1}(y) = w''$. L'image des blocs $uxay$, où $a \in \mathcal{S}$, est $f_{m+l}(uxay) = vzw''$ pour un certain z de la taille de w' (mot de taille $2n + 1$). De plus, on sait par le théorème 4.4 que $|f_{l-n-1}^{-1}(w'')| = |\mathcal{S}|^{2n}$. Ainsi, si l'on prend la somme sur tous les mots z de la taille de w', on a $\sum_z R(f, u, vzw'') \geq R(f, u, v)|f^{-1}(w'')||\mathcal{S}| = R(f)|\mathcal{S}|^{2n+1}$, car pour tout x tel que $f_m(ux) = v$ (il y en a $R(f, u, v)$), on peut choisir a quelconque ($|\mathcal{S}|$ possibilités), et y parmi tous les antécédents de w'' ($|\mathcal{S}|^{2n}$ possibilités), afin de compléter u de sorte que l'image par f soit de la forme vzw'' pour un certain z (*cf* figure 4). Or la somme comprend $|\mathcal{S}|^{2n+1}$ termes inférieurs à $R(f)$, donc pour tout z, $R(f, u, vzw'') = R(f)$. Ainsi, en particulier pour $z = w'$, $R(f, u, vw) = R(f)$. □

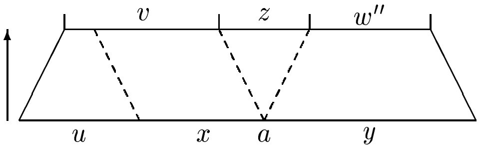

FIG. 4 – Illustration du lemme 6.3.

6.4 Proposition Soient m et n deux entiers, et $f \in \mathrm{F}(\mathcal{S}, m)$, $g \in \mathrm{F}(\mathcal{S}, n)$ telles que $f_\infty, g_\infty \in \mathrm{Surj}(\mathcal{S})$. Alors $R(fg) = R(f)R(g)$.

Preuve Cette preuve est illustrée par la figure 5. Montrons d'abord que $R(fg) \leq R(f)R(g)$. Soient $u \in \mathrm{Blocs}(\mathcal{S}, n + m)$ et $v \in \mathrm{Blocs}(\mathcal{S}, k)$ pour un certain entier k. Il y a $R(f, g_m(u), v)$ façons de prolonger $g_m(u)$ de sorte que l'image par f_k soit v. Pour chaque tel prolongement w, c'est-à-dire $f_k(g_m(u)w) = v$, il y a $R(g, u, g_m(u)w) \leq R(g)$ façons de prolonger u de sorte que l'image par g_{m+k} soit $g_m(u)w$. Ainsi, il y a au plus $R(f, g_m(u), v)R(g)$ façons de prolonger u de sorte que l'image par $(fg)_k$ soit v. Donc $R(fg) \leq R(f)R(g)$.

Montrons maintenant que $R(fg) \geq R(f)R(g)$. Soient $u \in \mathrm{Blocs}(\mathcal{S}, n+m)$ et $x \in \mathrm{Blocs}(\mathcal{S}, k)$, pour un certain entier $k \geq m$, tels que $R(g,u,x) = R(g)$. Soit $v \in \mathrm{Blocs}(\mathcal{S}, l)$ pour un certain entier $l \geq k-m$, tel que $R(f,x,v) = R(f)$. Quitte à appliquer le lemme 6.3, on peut supposer $l > n+k-m$. Pour tout mot y (de taille $2(l+m-k) > 2n$) tel que $f_l(xy) = v$, par le lemme 6.3, $R(g,u,xy) = R(g)$. Il y a donc $R(g)$ façons de compléter u de sorte que l'image par g soit xy. Pour $y \neq y'$, les ensembles des façons de compléter u de sorte que l'image par g soit xy ou xy' respectivement sont disjoints. Or il y a $R(f)$ façons de choisir y, donc le nombre total de façons de compléter u tel que l'image par fg soit v est $R(f)R(g)$. Donc $R(fg) \geq R(f)R(g)$. □

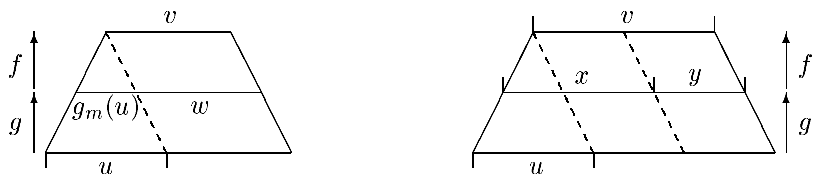

FIG. 5 – $R(fg) \leq R(f)R(g)$ à gauche ; $R(fg) \geq R(f)R(g)$ à droite.

6.5 Théorème (L. R. Welch) Supposons que $|\mathcal{S}|$ soit un nombre premier. Soit $\phi \in \mathrm{Cont}(\mathcal{S})$ telle qu'il existe $q \geq 1$ un entier et $p \in \mathbf{Z}$ avec $\phi^q = \sigma^p$. Alors q divise p.

Preuve Par le théorème 3.3, il existe un entier n et une fonction $f \in \mathrm{F}(\mathcal{S}, n)$ tels que $\phi = f_\infty$. Soit $g = f^q \in \mathrm{F}(\mathcal{S}, qn)$. Alors $g_\infty = f_\infty^q = \sigma^p$, donc par le lemme 6.1, on a $|p| \leq qn$. Mais $g_\infty \in \mathrm{Surj}(\mathcal{S})$, et $R(g) = |\mathcal{S}|^{qn-p}$. En effet, pour tout $v \in \mathrm{Blocs}(\mathcal{S}, k)$, où k est un entier tel que $2k+1 \geq qn-p+1$, pour tout $u \in \mathrm{Blocs}(\mathcal{S}, qn)$, si x est un mot de taille $2k+1-(qn-p+1)$, y mot de taille $qn-p$, tels que $g_k(uxy) = v$, alors x est déterminé par le choix de v (car $g_\infty = \sigma^p$), mais y peut être librement choisi (*cf* figure 6).

Or $f_\infty \in \mathrm{Surj}(\mathcal{S})$ (puisque $f_\infty^q \in \mathrm{Surj}(\mathcal{S})$), et par la proposition 6.4, $R(g) = R(f)^q$, donc $R(f)^q = |\mathcal{S}|^{qn-p}$. Comme $|\mathcal{S}|$ est premier, q divise $qn-p$, donc q divise p. □

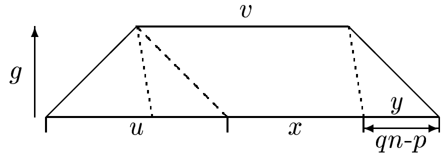

FIG. 6 – $R(g) = |\mathcal{S}|^{qn-p}$.

6.6 Corollaire Lorsque $|\mathcal{S}|$ est premier, le décalage n'a pas de racine non triviale.

6.7 Remarque On a en fait montré un peu plus que l'énoncé du théorème. En effet, plaçons-nous dans les notations de l'énoncé. Si l'on décompose $|\mathcal{S}|$ en produits de facteurs premiers, $|\mathcal{S}| = \prod_i p_i^{\alpha_i}$, alors q divise $p\alpha_i$ pour tout i, donc q divise $p.\text{pgcd}\{\alpha_i\}$.

Notons que lorsque q divise p, on a quelques candidats simples pour les racines q-ièmes de σ^p. L'idée est de composer le décalage avec une permutation de $\mathcal{S}$. Plus précisément, si π est une permutation de $\mathcal{S}$ d'ordre divisant q, alors $(\tau\pi)_\infty^q = \sigma^p$, où $\tau \in \mathrm{F}(\mathcal{S}, p/q)$ est définie par $\tau(u) = u_{p/q}$.

Enfin, pour clore cette section, signalons que dans le cas où $|\mathcal{S}|$ est composé, on peut trouver ϕ, q et p, tels que $\phi^q = \sigma^p$ et q ne divise pas p. Par exemple, si $|\mathcal{S}| = 4$, on peut prendre $\mathcal{S} = \{0,1\} \times \{0,1\}$; pour $p = 1$ et $q = 2$, on peut prendre l'automate cellulaire unidirectionnel de voisinage contenant 2 cellules, dont la fonction de transition est donnée par

$$\delta((a,b),(c,d)) = (d,a)$$

(où $a, b, c, d \in \{0,1\}$). Alors

$$\delta^2((a,b),(c,d),(e,f)) = \delta((d,a),(f,c)) = (c,d)$$

donc $\delta_\infty^2 = \sigma$. Cette construction fonctionne dès que $|\mathcal{S}|$ est un carré. Elle montre l'importance de l'hypothèse $|\mathcal{S}|$ premier dans le théorème 6.5. Notons tout de même que la remarque 6.7 permet de prendre en compte cet exemple (puisque $\text{pgcd}\{\alpha_i\} = 2$ dans ce cas, et $q = 2$ divise $2p = 2$).

7 Conclusion

Nous espérons avoir donné un aperçu (relativement) clair de l'article de Hedlund, et surtout des méthodes employées. Ces méthodes sont issues des mathématiques plus que de l'informatique, comme d'ailleurs la rédaction de l'article original. Il est étonnant de voir l'auteur approfondir certains détails qui semblent faciles, et passer sur d'autres raisons plus profondes (par exemple, l'utilisation de la compacité n'est même pas citée dans la preuve du théorème 3.3, et apparemment il est trivial que la métrique corresponde à la topologie produit). Cependant, les preuves sont précises, et cette vision des automates cellulaires permet de profiter de la puissance des théories mathématiques utilisées (topologie en général, théorie des groupes à la section 5, arithmétique à la section 6, notamment).

L'article original contient trop de résultats pour les citer tous, mais parmi ceux que nous n'avons pas démontrés, notons les suivants.

- Injectivité et bijectivité sont équivalentes dans $\mathrm{Cont}(\mathcal{S})$.
- Si $\phi \in \mathrm{Cont}(\mathcal{S}) - \mathrm{Surj}(\mathcal{S})$, alors il existe $x \in \mathrm{Suites}(\mathcal{S})$ tel que $\phi^{-1}(x)$ soit infini (et même non dénombrable). Avec le corollaire 4.6, on en déduit le théorème 4.7.
- $\mathrm{Cont}(\mathcal{S}) - \mathrm{Surj}(\mathcal{S})$ et $\mathrm{Surj}(\mathcal{S}) - \mathrm{Bij}(\mathcal{S})$ sont infinis.

L'article de Hedlund a le défaut de ne traiter que les automates cellulaires de dimension 1. Pour des automates cellulaires de dimension supérieure, il faudrait introduire une autre métrique, qui serait vraisemblablement moins naturelle. De plus, le décalage σ ne peut plus être utilisé de façon si simple. Toutefois, Richardson a généralisé en 1972 (*cf* [Ric72]) le théorème 3.3 aux dimensions supérieures. Il est peut-être possible de reformuler certains autres résultats de sorte qu'ils restent valides en toute dimension, mais cela nécessite de reprendre minutieusement les travaux de l'article, car ils utilisent fréquemment le décalage σ. Insistons une dernière fois sur le fait que l'utilisation de σ est cachée dans le présent rapport, mais cela tient à la présentation que nous avons faite. En effet, en prolongeant symétriquement nos fonctions (ce qui paraît plus naturel lorsque l'on a déjà manipulé des automates cellulaires), nous évitons la composition avec des puissances du décalage pour obtenir la classe entière des fonctions globales des automates cellulaires. Cependant, cette présentation a demandé quelques contorsions. C'est en partie pour cette raison que nous n'avons pas toujours suivi Hedlund très fidèlement dans ses preuves, notamment dans la section 6. Dans cette partie, nous avons par ailleurs illustré les preuves par des dessins, dans l'espoir de rendre le résultat plus lisible que l'article original.

Références

[Hed68] G. A. Hedlund. Transformations commuting with the shift. In Joseph Auslander and Walter H. Gottschalk, editors, *Topological Dynamics*, 1968.

[Hed69] G. A. Hedlund. Endomorphisms and automorphisms of the shift dynamical system. *Mathematical Systems Theory*, 3(4):320–375, 1969.

[Ric72] D. Richardson. Tesselations with local transformations. *Journal of Computer and System Sciences*, 5:373–388, 1972.