Complexité et automates cellulaires linéaires* Complexity and linear cellular automata

Valérie BERTHÉ
I.M.L., UPR 9016
Case 907, 163 av. de Luminy
F-13288 Marseille Cedex 09
berthe@iml.univ-mrs.fr

Résumé

Nous montrons que la fonction de complexité rectangulaire de suites doubles engendrées par un automate cellulaire linéaire à coefficients dans $\mathbb{Z}/l\mathbb{Z}$ et à condition initiale polynomiale est quadratique quand l est un nombre premier et qu'elle croît en proportion du nombre de facteurs premiers distincts de l.

Abstract

We prove that the complexity function (in rectangles) of two-dimensional sequences generated by a linear cellular automaton with coefficients in $\mathbb{Z}/l\mathbb{Z}$, and polynomial initial condition, is quadratic when l is a prime and that it increases with respect to the number of distinct prime factors of l.

1 Introduction

Cet article étudie l'ordre de croissance de la fonction de complexité rectangulaire de suites doubles engendrées par un automate cellulaire linéaire à condition initiale polynomiale (c'est-à-dire à support fini). Rappelons que la fonction de complexité en rectangles $P(m,n)$ compte le nombre de facteurs rectangulaires de taille (m,n) d'une suite double donnée. Une suite double $(a(u,v))_{(u,v)\in\mathbb{N}^2}$ est dite engendrée par l'automate cellulaire linéaire de

*1991 MSC classification: 68R15, 11B85, 68Q80, 05A10 polynôme $R(X)$ et de condition initiale $P(X)$ (où R et P sont des polynômes à coefficients dans $\mathbb{Z}$) si

$$\forall u \in \mathbb{N},\ \sum_{v\in\mathbb{N}} a(u,v)X^v = P(X)R(X)^u.$$

Nous considérons alors les réductions $a_l = (a_l(u,v))_{(u,v)\in\mathbb{N}^2}$ modulo un entier l de ces suites.

Cette étude prolonge [3] où le cas du triangle de Pascal est traité en détails. Nous montrons que l'ordre de croissance de la fonction de complexité d'un automate cellulaire linéaire a le même comportement asymptotique que dans le cas du triangle de Pascal : la croissance de la fonction de complexité $P(m,n)$ est quadratique en $\sup(m,n)$ quand on réduit modulo une puissance d'un nombre premier et croît en proportion du nombre de facteurs premiers de l'entier selon lequel on réduit.

Théorème *Soit a la suite double engendrée par le polynôme $R = r_dX^d + \ldots + r_vX^v$, avec la condition initiale polynomiale $P = p_tX^t + \ldots + p_0$. Soit $l \geq 1$. Soit $P_l(m,n)$ la complexité de la suite a réduite modulo l. On suppose que $v < d$ (c'est-à-dire que R n'est pas réduit à un monôme), et que r_d, r_v et p_t sont inversibles modulo l. On note $\omega(l)$ le nombre de facteurs premiers distincts de la décomposition de l. Il existe alors deux constantes A et B strictement positives (qui dépendent de l) telles que, quels que soient $m \geq 1$ et $n \geq d$, on ait*

$$A \sup(m,n)^{2\omega(l)} \leq P_l(m,n) \leq B \sup(m,n)^{2\omega(l)}.$$

Notons que l'on peut calculer effectivement les constantes A et B.

Une suite double engendrée par un automate cellulaire linéaire (avec une condition initiale polynomiale) sur $\mathbb{Z}/l\mathbb{Z}$ est donc d'autant plus "désordonnée" que l'entier l selon lequel on réduit comporte de facteurs premiers distincts. On retrouve cette idée dans [7, 8] et aussi [13], où l'automaticité de la suite double a_l est considérée : la suite a_l est automatique si et seulement si l est une puissance d'un nombre premier. Voir également [15, 16, 17, 18] pour un lien entre ce type de conditions arithmétiques et certaines propriétés topologiques des automates cellulaires.

Le plan de la preuve du théorème précédent reprend principalement celui de [3] et se décompose en quatre temps. (La principale différence par rapport à [3] se situe au paragraphe 4). Nous donnons quelques lemmes techniques au paragraphe 3. Nous montrons en particulier que la complexité en rectangles peut être calculée en connaissant uniquement la complexité en ligne.

Puis nous montrons comment nous pouvons nous ramener au polynôme 1 pour la condition initiale, sans modifier l'ordre de croissance de la fonction de complexité. Nous achevons ce paragraphe par quelques considérations sur les ordres de croissance obtenus en considérant plus généralement des automates cellulaires, et des configurations initiales, quelconques. Le paragraphe 4 est consacré à étude du cas où l est une puissance d'un nombre premier. La difficulté réside dans la minoration de la complexité en ligne. Pour cela, nous allons minorer le nombre de facteurs en ligne dits spéciaux, c'est-à-dire tels qu'ils aient plusieurs extensions possibles dans la suite double. Cette idée est inspirée par les techniques de minoration de la complexité développées dans [20]. La majoration est une conséquence immédiate de l'automaticité de la suite a_l (voir [7, 8, 13]) : la complexité d'une suite double automatique est au plus quadratique. Nous montrons au paragraphe 5 que l'ordre de la complexité est "multiplicatif" en l, autrement dit que l'ordre de la complexité de la suite modulo $l_1 l_2$ est le produit des ordres des complexités modulo l_1 et modulo l_2 dès que l_1 et l_2 sont premiers entre eux. Nous concluons cet article en traitant le cas général.

Il est naturel de se demander si l'on peut étendre cette étude au cas de configurations initiales non plus à support fini mais périodiques ou plus généralement automatiques. Dans le cas de la réduction modulo une puissance d'un nombre premier, les résultats obtenus ici sont encore valables (l'ordre de croissance de la fonction de complexité reste quadratique). Néanmois nous nous sommes restreints au cadre de configurations initiales à support fini pour pouvoir appliquer le résultat de multiplicativité permettant d'obtenir l'ordre de croissance quand on réduit modulo un entier composé. Nous ignorons si ce dernier résultat est encore valide dans ce cadre étendu.

2 Définitions

2.1 Automates cellulaires linéaires

Nous travaillerons dans tout ce qui suit avec des automates cellulaires linéaires définis sur l'anneau $A = \mathbb{Z}/l\mathbb{Z}$, pour $l \geq 2$.

Soit $R = \sum_{i=0}^{d} r_i X^i$ un polynôme à coefficients dans A. Soit $\varphi_R : A^{d+1} \to A$ la *règle linéaire de transition locale* définie par

$$\varphi_R(x_0, \ldots, x_d) = \sum_{i=0}^{d} r_{d-i} x_i.$$

L'*automate cellulaire linéaire* $\mathcal{A}_R$ engendré par le polynôme R est défini sur l'ensemble $A^{\mathbb{N}}$ de toutes les *configurations* par :

$$\begin{aligned}\mathcal{A}_R : \quad & A^{\mathbb{N}} \rightarrow A^{\mathbb{N}} \\ & (f_n)_{n\in\mathbb{N}} \mapsto (g_n)_{n\in\mathbb{N}},\end{aligned}$$

avec

$$\forall n \in \mathbb{N},\ g_n = \varphi_R(f_{n-d}, \ldots, f_n) = r_d f_{n-d} + \ldots + r_0 f_n.$$

Les techniques que nous développons ici ne s'appliquant qu'à des configurations initiales finies ou automatiques, donc définies sur $\mathbb{N}$, nous nous restreignons à des automates cellulaires définis sur $\mathbb{N}$. Il est alors algébriquement intéressant de représenter les configurations par des séries formelles. Soit $A[[X]]$ l'anneau des séries formelles de Laurent à coefficients dans A :

$$A[[X]] = \{\sum_{n\geq 0} f_n X^n,\ f_n \in A\}.$$

On définit alors

$$\begin{aligned}\mathcal{A}_R : \quad & A[[X]] \rightarrow A[[X]] \\ & f(X) \mapsto R(X)f(X).\end{aligned}$$

On représente la série $f(X) = \sum_{i\geq 0} f_i X^i$ sur $\mathbb{N}$ en associant l'état f_i à la cellule de site i. On représente de même sur $\mathbb{N}^2$ l'évolution temporelle de la condition initiale f sous l'action de $\mathcal{A}_R$: la cellule de site (i,t) est dans l'état $a(i,t)$ à l'instant t, avec

$$\mathcal{A}_R^t(f) = f(X)R(X)^t = \sum_i a(i,t)X^i.$$

L'automate cellulaire engendre donc une suite double a à partir d'une condition initiale f. On considère un polynôme P à coefficients dans $\mathbb{Z}$. On définit les suites doubles $a = (a(u,v))_{(u,v)\in\mathbb{N}^2}$ (à coefficients dans $\mathbb{Z}$) et $a_l = (a_l(u,v))_{(u,v)\in\mathbb{N}^2}$ (à coefficients dans $\mathbb{Z}/l\mathbb{Z}$) de la manière suivante :

$$\forall u \in \mathbb{N},\ \sum_{v\in\mathbb{Z}} a(u,v)X^v := P(X)R(X)^u,$$

$$\forall (u,v) \in \mathbb{N}^2,\ a_l(u,v) = a(u,v) \bmod l.$$

On dit que la suite double a est *engendrée* par le polynôme R avec condition initiale P.

En particulier, si $P(X) = 1$ et $R(X) = 1 + X$, on obtient la suite double des coefficients binomiaux $(\binom{u}{v})_{u,v}$.

2.2 Complexité

Nous utiliserons dans tout ce qui suit la représentation suivante pour les suites doubles $(a(u,v))_{(u,v)\in\mathbb{N}^2}$: le premier indice u désigne l'indice de ligne (de bas en haut), alors que le deuxième indice v désigne l'indice de colonne (de gauche à droite).

Définition 2.1 *Soit $\mathcal{L}_l(m,n)$ l'ensemble des facteurs rectangulaires à m lignes et n colonnes qui apparaissent dans la suite double a_l. Soit*

$$P_l(m,n) = Card(\mathcal{L}_l(m,n)).$$

On note par abus d'écriture $P_l(n) = P_l(1,n)$: c'est le nombre de facteurs en ligne qui apparaissent dans la suite double a_l. La fonction $(m,n) \mapsto P_l(m,n)$ est appelée complexité en rectangles *de la suite double, la fonction $n \mapsto P_l(n) = P_l(1,n)$ est appelée* complexité en ligne.

Nous travaillerons principalement avec la complexité en ligne. Un moyen efficace de la calculer consiste à évaluer sa différence première $P_l(n+1) - P_l(n)$, qui s'exprime combinatoirement comme suit (pour une étude générale du sujet, voir [10]).

On appelle *facteur spécial à droite* un facteur en ligne w de la suite double a_l tel qu'il existe deux occurrences (à des indices de ligne éventuellement distincts) de w dans la suite a_l suivies par deux lettres différentes. Une *extension* du facteur w est une lettre x telle que wx est également facteur en ligne. Soit $\varphi(w)$ le nombre d'extensions distinctes de w dans la suite a_l. On a

$$\forall n,\ P_l(n+1) - P_l(n) = \sum_{|w|=n} \varphi(w).$$

Soit $s(n)$ le nombre de facteurs spéciaux à droite de longueur n de la suite a_l. On a

$$\forall n,\ p(n+1) - p(n) \geq s(n).$$

2.3 Automaticité

Il est naturel de se demander quels sont les liens entre l'engendrement par automate cellulaire linéaire et l'engendrement par automate fini bidimensionnel (au sens de [22, 23]). La question est complètement résolue dans [7, 8], où le théorème suivant est démontré (voir aussi [14] pour d'autres résultats faisant intervenir les propriétés arithmétiques des coefficients). Nous utiliserons ce résultat au cours de notre étude.

Théorème 2.1 (Allouche, von Haeseler, Peitgen, Petersen, Skordev) *Soit a la suite double engendrée par le polynôme R. Soit χ le nombre de diviseurs premiers p de l pour lesquels le polynôme R réduit modulo p n'est pas un monôme. Alors,*

- *si $\chi \geq 2$, il n'existe pas d'entier $k \geq 2$ pour lequel la suite double a_l est k-automatique;*
- *si $\chi = 1$ et si p désigne le nombre premier pour lequel la réduction n'est pas monomiale, la suite double a_l est p^s-automatique, pour tout entier $s \geq 1$, et n'est jamais k-automatique pour une autre valeur de k;*
- *si $\chi = 0$, la suite double a_l est k-automatique, pour tout $k \geq 2$.*

La preuve utilise les caractérisations suivantes des suites automatiques doubles (voir [22, 23]): une suite double $(a(m,n))_{(m,n)\in\mathbb{N}^2}$ est p-automatique si et seulement si la série $\sum a(m,n)X^mY^n$ est algébrique sur $\mathbb{Z}/p\mathbb{Z}(X,Y)$ ou de manière équivalente, si et seulement si elle est l'image par une projection littérale d'un point fixe d'une substitution uniforme qui associe à une lettre un motif carré. Pour plus de références sur le sujet, voir [8] et pour la notion de suites automatiques unidimensionnelles, voir [1].

Notons que la condition suffisante d'automaticité énoncée au théorème 2.1 est encore valable pour une condition initiale k-automatique (et non pas seulement à support fini) : il suffit pour cela de remarquer que le produit de Cauchy de deux suites k-automatiques est encore k-automatique. En effet, soit p premier tel que R modulo p ne soit pas réduit à un monôme. Soit $l = p^s$. Soit $f \in \mathbb{Z}/l\mathbb{Z}\,[[X]]$ une condition initiale dont la suite des coefficients est p-automatique. La suite double engendrée par le polynôme R de condition initiale f est encore p-automatique. Ceci se déduit de [4] en deux temps : le produit de deux suites k-régulières est encore une suite k-régulière ; une suite k-régulière prenant un nombre fini de valeurs est automatique.

On voit aisément, en calquant la preuve qui correspond au cas unidimensionnel [11], que la complexité d'une suite double automatique est alors au plus quadratique. Nous aurons besoin de ce résultat au cours de notre étude sur la complexité.

Proposition 2.1 *La complexité d'une suite double automatique satisfait :*

$$\exists C > 0,\ \forall (m,n),\ P(m,n) \leq C \sup(m,n)^2.$$

Preuve Soit b une suite double automatique. D'après [22, 23], il existe une projection p littérale, une substitution (carrée) σ de longueur k, telle que la suite b est l'image par la projection p d'un point fixe c de la substitution σ. Il suffit de démontrer le résultat pour la suite c, la complexité décroissant par projection littérale.

Soit (m, n) un couple d'entiers positifs fixés. Supposons $m \geq n$ par exemple. Soit i tel que $k^i \leq m < k^{i+1}$. Soit w facteur de taille (m, n) de la suite c et soit (u, v) un indice d'occurrence de w. Soit (r, s) tel que le point (u, v) appartienne au carré de taille k^{i+1} et de sommet inférieur gauche (rk^{i+1}, sk^{i+1}). Le facteur w est déterminé par le facteur de taille $(2, 2)$ $\begin{bmatrix} b(r+1, s) & b(r+1, s+1) \\ b(r, s) & b(r, s+1) \end{bmatrix}$ dont l'image par la $(i+1)$-ième itération de σ contient w, et par l'emplacement de (u, v) dans le carré de sommet inférieur gauche (rk^{i+1}, sk^{i+1}). Or $|u - rk^{i+1}|$ et $|v - rk^{i+1}| < k^{i+1} \leq km$. On a donc

$$P(m, n) \leq (\mathrm{Card}\mathcal{A})^4 k^2 m^2 \quad \blacksquare$$

3 Complexité en ligne

Le but de ce paragraphe est de montrer que l'étude de la complexité en rectangles peut se ramener à celle de la complexité en ligne d'une part, et d'autre part, à celle des automates cellulaires linéaires de condition initiale 1.

Dans tout ce qui suit, on considère un automate cellulaire linéaire engendré par le polynôme de degré d à coefficients dans $\mathbb{Z}/l\mathbb{Z}$: $R(X) = \sum_{0 \leq i \leq d} r_i X^i$.

Lemme 3.1 *On suppose que r_d est inversible dans $\mathbb{Z}/l\mathbb{Z}$. Soit $l \geq 2$. On a :*

$$\forall m \geq 1, \forall n \geq d, P_l(m, n) = P_l(1, d(m-1) + n).$$

Preuve Il suffit de montrer que l'on a : $\forall m \geq 2$, $\forall n \geq d$, $P_l(m, n) = P_l(m-1, n+d)$. Le résultat s'en déduit alors par récurrence finie.

Soit Φ l'application de l'ensemble des facteurs $\mathcal{L}_l(m-1, n+d)$ dans $\mathcal{L}_l(m, n)$, qui associe à un facteur B rectangulaire de taille $(m-1, n+d)$ le facteur rectangulaire de taille (m, n) qui apparaît à l'indice $(u, v+d)$, si B apparaît à l'indice (u, v). On vérifie que cette définition ne dépend pas de l'indice (u,v) choisi. On a plus précisément

$$\Phi\begin{pmatrix} b_{m-1,1} & \cdots & b_{m-1,n+d} \\ \vdots & & \vdots \\ b_{1,1} & \cdots & b_{1,n+d} \end{pmatrix} = \begin{pmatrix} c_{m,1} & \cdots & c_{m,n} \\ \vdots & & \vdots \\ c_{1,1} & \cdots & c_{1,n} \end{pmatrix}$$

avec pour tout $j \in [1,n]$:

$$\begin{array}{ll} c_{i,j} & = b_{i,j+d}, \quad \text{pour } i \in [1,m-1], \\ c_{m,j} & = r_d b_{m-1,j} + \cdots + r_0 b_{m-1,j+d}. \end{array}$$

Notons que l'on a

$$\forall i \in [2,m],\ \forall j \in [1,n]\ c_{i,j} = r_d b_{i-1,j} + \cdots + r_0 b_{i-1,j+d}. \tag{1}$$

Montrons que l'application Φ est bijective. Elle est surjective par construction. En effet, tout facteur de taille (m,n) qui apparaît à un indice (u,v) a pour antécédent le facteur de taille $(m-1,n+d)$ qui apparaît à l'indice $(u,v-d)$ (en complétant éventuellement par des 0 si $v < d$). Montrons qu'elle est injective. Soient $B = (c_{i,j})_{1\le i\le m-1,\ 1\le j\le n+d}$ et $B' = (b'_{i,j})_{1\le i\le m-1,\ 1\le j\le n+d}$ deux facteurs de taille $(m-1,n+d)$ tels que $\Phi(B) = \Phi(B')$. On a : $\forall i \in [1,m-1],\ \forall j \in [1,n]$, $b_{i,j+d} = b'_{i,j+d}$. On a $n \ge d$ et r_d est supposé inversible. On déduit donc de (1) pour tout $i \in [1,m-1]$ et en posant $j = d$:

$$r_d(b_{i,d} - b'_{i,d}) + \cdots + r_0(b_{i,2d} - b'_{i,2d}) = 0.$$

On a donc : $\forall i \in [1,m-1]$, $b_{i,d} = b'_{i,d}$, puis en itérant, on obtient que $b_{i,j} = b'_{i,j}$, pour $1 \le i \le m-1,\ 1 \le j \le d$. ∎

Lemme 3.2 *Soit $P(X) = p_0 + p_1X + \cdots + p_tX^t$ un polynôme à coefficients dans $\mathbb{Z}/l\mathbb{Z}$. On suppose p_t inversible. Soit $a_l^{(1)}$ (respectivement $a_l^{(P)}$) la suite double engendrée par le polynôme R (à coefficients dans $\mathbb{Z}/l\mathbb{Z}$) avec condition initiale 1 (respectivement avec condition initiale P). Les fonctions de complexité en lignes des suites doubles a_l et $a_l^{(P)}$ ont même ordre de croissance :*

$$\forall n \ge 1,\ l^{-t}\,Card(\mathcal{L}^{(1)}(n)) \le Card(\mathcal{L}^{(P)}(n)) \le l^t\ Card(\mathcal{L}^{(1)}(n)).$$

Preuve Soit $n \geq 1$ fixé. Considérons l'application de l'ensemble $\mathcal{L}^{(1)}(n+t)$ des facteurs (en ligne) de longueur $n+t$ de la suite double a_l dans l'ensemble $\mathcal{L}^{(P)}(n)$ des facteurs (en ligne) de longueur n de la suite double $a_l^{(P)}$, qui à un bloc $B = b_1 \cdots b_{n+t}$ associe le bloc $B' = b'_1 \cdots b'_n$, avec $b'_i = p_t b_i + \cdots + p_0 b_{t+i}$, pour $1 \leq i \leq n$. Cette application est surjective par définition et chaque bloc admet au plus l^t antécédents, car p_t est inversible. On a donc

$$l^{-t}\mathrm{Card}(\mathcal{L}^{(1)}(n+t)) \leq \mathrm{Card}(\mathcal{L}^{(P)}(n)) \leq \mathrm{Card}(\mathcal{L}^{(1)}(n+t)).$$

Or

$$\mathrm{Card}(\mathcal{L}^{(1)}(n)) \leq \mathrm{Card}(\mathcal{L}^{(1)}(n+t))$$

et

$$\mathrm{Card}(\mathcal{L}^{(1)}(n+t)) \leq \mathrm{Card}(\mathcal{L}^{(1)}(n))\mathrm{Card}(\mathcal{L}^{(1)}(t)) \leq \mathrm{Card}(\mathcal{L}^{(1)}(n))l^t.$$

Par conséquent, on a :

$$\forall n \geq 1,\ l^{-t}\mathrm{Card}(\mathcal{L}^{(1)}(n)) \leq \mathrm{Card}(\mathcal{L}^{(P)}(n)) \leq l^t\ \mathrm{Card}(\mathcal{L}^{(1)}(n)).$$

$\blacksquare$

Remarques Il serait tentant d'essayer de se ramener à la configuration initiale 1 par application du principe de superposition (voir par exemple [19]). Nénmoins il est impossible de déduire la complexité $P(m,n)$ d'une suite obtenue par superposition, des complexités $P_1(m,n)$ et $P_2(m,n)$ des suites initiales sans posséder d'information supplémentaire sur la localisation des facteurs. Seule peut être donnée a priori la majoration grossière suivante : $P(m,n) \leq P_1(m,n)P_2(m,n)$.

Notons que même à partir d'une configuration initiale de complexité maximale, la complexité ne peut croître arbitrairement : on ne peut ainsi pas atteindre une complexité d'entropie topologique strictement positive (rappelons que l'entropie topologique est définie comme $\lim_{m,n\to+\infty} \frac{\log(P(m,n))}{\sup(m,n)^2}$). En effet, on montre (par le même raisonnement que celui utilisé dans la preuve du lemme 3.1) que pour tout automate cellulaire (non forcément linéaire) défini sur un alphabet à l lettres avec une règle de transition locale faisant intervenir $d+1$ cellules voisines, on a :

$$\forall m \geq 2,\ n \geq 1,\quad P(m,n) \leq P(1, n+d(m-1)) \leq l^{n+d(m-1)}.$$

Ce phénomène qualifié "d'irréversibilité" est par exemple illustré dans [19]. En revanche, puisque l'on peut exhiber des suites de complexité unidimensionnelle exponentielle [12] ou polynomiale, on peut obtenir grâce au lemme

3.1 une complexité en rectangles $P(m,n)$ exponentielle ou polynomiale en $\sup(m,n)$.

Enfin, du point de vue sytèmes dynamiques, notons l'on considère ici l'orbite unilatère d'une configuration donnée. Pour un point de vue global sur les orbites de toutes les configurations possibles, voir le survol [9] sur les propriétés topologique métriques des automates cellulaires.

4 Réduction modulo une puissance d'un nombre premier

Le but de ce paragraphe est d'évaluer l'ordre de croissance de la fonction de complexité en ligne quand on réduit modulo une puissance d'un nombre premier. Nous allons commencer cette étude par le cas où l'on réduit modulo un nombre premier. Le cas d'une puissance d'un nombre premier s'en déduira aisément.

4.1 Réduction modulo un nombre premier

Soit p un nombre premier. On considère l'automate cellulaire linéaire engendré sur $\mathbb{Z}/p\mathbb{Z}$ par le polynôme $R(X) = r_d X^d + \cdots + r_0$, avec $r_d \neq 0$. *On suppose de plus que R n'est pas réduit à un monôme.* La règle linéaire de transition locale est définie par

$$\varphi_R(x_0, \ldots, x_d) = \sum_{i=0}^{d} r_{d-i} x_i.$$

Rappelons que pour tout entier k positif, on a

$$R(X)^{p^k} = r_0 + r_1 X^k + \cdots + r_d X^{dp^k}. \tag{2}$$

Cette propriété est essentielle dans le traitement de la réduction modulo p; nous l'utiliserons à de nombreuses reprises dans les preuves suivantes.

Considérons une condition initiale polynomiale P non nulle. D'après le lemme 3.2, on peut supposer la condition initiale égale à 1 (tout nombre non nul est inversible modulo p, donc le coefficient dominant p_t de la condition initiale P l'est).

Soit $a_p = (a_p(u,v))_{(u,v)\in\mathbb{N}^2}$ la suite double des coefficients de l'automate ainsi défini. Le but de ce paragraphe est de montrer le résultat suivant.

Théorème 4.1 *Soit R un polynôme de degré $d \geq 1$ défini sur $\mathbb{Z}/p\mathbb{Z}$. On suppose que R n'est pas réduit à un monôme. Soit $P_p(n)$ la complexité en* *ligne de la suite double a_p engendrée par l'automate cellulaire linéaire $\mathcal{A}_R$ de condition initiale 1. Il existe deux constantes $C_1, C_2 > 0$ telles que*

$$\forall n,\ C_1 n^2 \leq\ P_p(n) \leq C_2 n^2.$$

Preuve La majoration quadratique résulte de l'automaticité (théorème 2.1 et proposition 2.1). Nous supposerons de plus que $r_0 \neq 0$. En effet, la complexité en ligne de l'automate cellulaire engendré par $XR(X)$ est égale à la complexité en ligne de l'automate engendré par $R(X)$: les lignes sont simplement décalées par cette opération.

Rappelons qu'on appelle facteur spécial à droite un facteur en ligne w de la suite double a_p tel qu'il existe deux occurrences de w dans la suite a_p suivies par deux lettres différentes. Soit $s(n)$ le nombre de facteurs spéciaux à droite de longueur n de la suite a. On a $P_p(n+1) - P_p(n) \geq s(n)$. Il suffit donc pour minorer quadratiquement $P_p(n)$ de montrer qu'il existe une constante C_0 telle que $s(n) \geq C_0 n$, pour n assez grand. La preuve du théorème 4.1 est donc une conséquence directe des deux lemmes suivants.

Pour toute lettre a et pour tout entier naturel n, a^n désigne le mot de longueur n formé par la lettre a concaténée n fois avec elle-même.

Lemme 4.1 *Pour tout entier i assez grand, il existe un entier n_i, avec*

$$i(d-1) \leq n_i < (i+1)(d-1),$$

il existe deux lettres x_i, y_i non nulles, un mot w_i de longueur n_i tels que les mots

$$w_i x_i 0^{n_i} y_i \quad et \quad w_i x_i 0^{n_i+1}$$

soient des facteurs en ligne de la suite double a; en d'autres termes, le facteur $w_i x_i 0^{n_i}$ (de taille $2n_i + 1$) est un facteur spécial à droite d'extensions 0 et y_i.

Lemme 4.2 *Il existe une constante $C_0 > 0$ telle que pour tout entier n non nul, il existe au moins $C_0 n$ facteurs spéciaux à droite.*

Preuve du lemme 4.1 La preuve se fait par récurrence sur l'entier i. Initialisons la récurrence en exhibant un entier $i \geq 1$ et un entier n_i qui conviennent. Soit n le plus petit indice non nul des indices des coefficients non nuls du polynôme R. On a donc

$$R(X) = r_0 + r_n X^n + \ldots + r_d X^d,$$

avec $r_0 \neq 0$, $r_n \neq 0$ et $r_d \neq 0$ (avec éventuellement $n = d$ mais $d \neq 0$). Le facteur $0^{n-1}r_0 0^{n-1}r_n$ apparaît à l'indice $(1, 1-n)$. Soit k tel que $p^k n - 1 \geq (d-1)$. D'après (2), le facteur $0^{p^k n-1}r_0 0^{p^k n-1}r_n$ apparaît à l'indice $(p^k, 1-p^k n)$ et le facteur $0^{p^k n-1}r_0 0^{p^k n}$ apparaît à l'indice $(p^{k+1}, 1-p^k n)$. On a donc initialisé la récurrence avec l'entier $i \geq 1$ satisfaisant $i(d-1) \leq p^k n - 1 < (i+1)(d-1)$, en posant $n_i = p^k n - 1$.

Supposons donc la propriété de récurrence réalisée pour un entier $i \geq 1$. Il existe un entier n_i, avec

$$i(d-1) \leq n_i < (i+1)(d-1),$$

tel que les mots

$$W_i^1 = w_i x_i 0^{n_i} y_i \quad \text{et} \quad W_i^2 = w_i x_i 0^{n_i+1}, \text{ avec } |w_i| = n_i, \text{ et} x_i, y_i \neq 0,$$

soient des facteurs en ligne de la suite double a_p. Soient (u, v) et (u', v') des indices d'occurrence respectifs de W_i^1 et W_i^2.

Nous allons insérer dans un premier temps des plages de $p-1$ zéros entre les lettres de W_i^1 et W_i^2 en travaillant aux lignes d'indice pu et pu'. Plus précisément, soit X_{i+1} le facteur de longueur $2pn_i + 2p - 1$ qui apparaît à l'indice $(pu, pv + 1 - p)$; d'après (2), il est constitué de 0^{p-1} suivi de la première lettre de w_i, puis de nouveau de 0^{p-1} suivi de la seconde lettre de w_i et ainsi de suite jusqu'au n_i-ième 0, lui-même suivi de 0^{p-1}; le facteur X_{i+1} apparaît également à l'indice $(pu', pv' + 1 - p)$. Nous "réduirons" dans un second temps la plage de zéros (dans X_{i+1}) obtenue après x_i (qui est alors de longueur $pn_i + p - 1$) en considérant les facteurs en ligne successifs qui se déduisent de X_{i+1} par la règle locale φ_R de l'automate cellulaire, c'est-à-dire en travaillant avec les lignes d'indice de la forme $pu + k$ et $pu' + k$, pour k judicieusement choisi.

Soient q_i et r_i les quotient et reste de la division euclidienne de $(p-1)(n_i+1)$ par $d-1$. On a $q_i \geq 1$ car $i \geq 1$. Soient

$$\begin{cases} r_i' = & r_i \text{ et } q_i' = q_i, \text{ si } n_i + r_i \geq (i+1)(d-1), \\ r_i' = & r_i + d - 1 \text{ et } q_i' = q_i - 1, \text{ sinon.} \end{cases}$$

On a donc $(p-1)(n_i+1) = (d-1)q_i' + r_i'$, avec $n_i + r_i' \geq (i+1)(d-1)$. On pose

$$n_{i+1} = n_i + r_i' = pn_i + p - 1 - (d-1)q_i'. \tag{3}$$

On a

$$(i+1)(d-1) \leq n_{i+1} < (i+2)(d-1).$$

On a vu que le facteur en ligne X_{i+1} apparaît aux indices $(pu, pv+1-p)$ et $(pu', pv'+1-p)$, c'est-à-dire

$$X_{i+1} = \begin{cases} a_p(pu, pv+1-p)\dots a_p(pu, pv+2pn_i+p-1) \\ a_p(pu', pv'+1-p)\dots a_p(pu', pv'+2pn_i+p-1). \end{cases}$$

Par conséquent, en appliquant q_i' fois la règle locale de l'automate cellulaire à X_{i+1}, on voit que le facteur en ligne Y_{i+1} de longueur $2pn_i+2p-1-(q_i'(d-1))$ qui apparaît à l'indice $(pu+q_i', pv+1-p+q_i'(d-1))$ est égal au facteur en ligne de même longueur qui apparaît à l'indice $(pu'+q_i', pv'+1-p+q_i'(d-1))$:

$$Y_{i+1} \begin{cases} = a_p(pu+q_i', pv+1-p+q_i'(d-1)) \\ \dots a_p(pu+q_i', pv+2pn_i+p-1) \\ = a_p(pu'+q_i', pv'+1-p+q_i'(d-1)) \\ \dots a_p(pu'+q_i', pv'+2pn_i+p-1). \end{cases} \tag{4}$$

Soit w_{i+1} le facteur en ligne de longueur n_{i+1} qui apparaît à l'indice

$$(pu+q_i', p(v+n_i)+q_i'(d-1)-n_{i+1}).$$

Montrons que le facteur w_{i+1} apparaît également à l'indice $(pu'+q_i', p(v+n_i)+q_i'(d-1)-n_{i+1})$. Il suffit pour cela de montrer que w_{i+1} est un sous-facteur de Y_{i+1}. Or d'après (3), on a

$$p(v+n_i)+q_i'(d-1)-n_{i+1} = pv+2q_i'(d-1)+1-p \geq pv+q_i'(d-1)+1-p,$$

et

$$p(v+n_i)+q_i'(d-1)-1 \leq pv+2pn_i+p-1.$$

Soit $x_{i+1} = a_p(pu+q_i', p(v+n_i)+q_i'(d-1))$. D'après (4), on a $x_{i+1} = a_p(pu'+q_i', p(v'+n_i)+q_i'(d-1))$. Montrons que $x_{i+1} = r_d^{q_i'} x_i$ et par conséquent, $x_{i+1} \neq 0$. En effet, comme $w_i x_i$, situé à l'indice (u, v), est suivi par 0^{n_i}, on a

$$a_p(pu, pv+pn_i) = x_i,$$

et

$$a_p(pu, pv+pn_i+1) = \dots = a_p(pu, pv+2pn_i+p-1) = 0. \tag{5}$$

Comme selon (3), on a $pn_i+p-1 \geq (d-1)q_i'$, le résultat s'en déduit en appliquant q_i' fois la règle locale φ_R de l'automate cellulaire :

$$x_{i+1} = a_p(pu+q_i', p(v+n_i)+q_i'(d-1)) = r_d^{q_i'} a_p(pu, p(v+n_i)) = r_d^{q_i'} x_i.$$

Notons de plus que l'on déduit de (5), comme $2pn_i + p - 1 = pn_i + q_i'(d-1) + n_{i+1}$, que :

$$a_p(pu+q_i', p(v+n_i)+q_i'(d-1)+1) \cdots a_p(pu+q_i', p(v+n_i)+q_i'(d-1)+n_{i+1}) = 0^{n_{i+1}}$$

$$a_p(pu'+q_i', p(v'+n_i)+q_i'(d-1)+1) \cdots a_p(pu'+q_i', p(v'+n_i)+q_i'(d-1)+n_{i+1}) = 0^{n_{i+1}}.$$

On a donc

$$Y_{i+1} = w_{i+1}x_{i+1}0^{n_{i+1}}.$$

Enfin, soit $y_{i+1} = a_p(pu' + q_i', p(v' + n_i) + q_i'(d-1) + n_{i+1} + 1)$. On a de même $y_{i+1} = y_i r_0^{q_i'} \neq 0$. De plus,

$$a_p(pu' + q_i', p(v' + n_i) + q_i'(d-1) + n_{i+1} + 1) = r_0^{q_i'} a_p(pu', pv' + n_{i+1} + 1) = 0.$$

Par conséquent, $w_{i+1}x_{i+1}0^{n_{i+1}}y_{i+1}$ apparaît à l'indice $(pu+q_i', p(v+n_i)+q_i'(d-1) - n_{i+1})$ et $w_{i+1}x_{i+1}0^{n_{i+1}}0$ apparaît à l'indice $(pu' + q_i', p(v' + n_i) + q_i'(d-1) - n_{i+1})$.

La propriété de récurrence est donc démontrée pour $i + 1$. ■

La preuve du lemme 4.2 s'en déduit immédiatement.

Preuve du lemme 4.2 Montrons en effet que pour tout entier n assez grand, il existe au moins $\frac{n+1}{2(d-1)} - 2$ facteurs spéciaux à droite.

D'après le lemme 4.1, le facteur $w_i x_i 0^{n_i}$ est spécial à droite. Soit D l'opérateur qui associe à un mot ce même mot privé de sa première lettre s'il est non vide, et qui associe au mot vide le mot vide. Soit n assez grand pour qu'il existe i tel que $2n_i + 1 \leq n < 2n_{i+1} + 1$. On a

$$n_{i+1} < n_{i+2} < \ldots < n_{2i-1} < 2i(d-1) \leq 2n_i \leq n - 1.$$

Par conséquent, les $i-1$ facteurs suivants sont des facteurs spéciaux à droite distincts de longueur n

$$D^{2n_{i+1}+1-n}[w_{i+1}x_{i+1}0^{n_{i+1}}],$$

$$D^{2n_{i+2}+1-n}[w_{i+2}x_{i+2}0^{n_{i+2}}],$$

$$\cdots$$

$$D^{2n(2i-1)+1-n}[w_{2i-1}x_{2i-1}0^{n_{2i-1}}],$$

$$0^n.$$

De plus, $n \leq 2n_{i+1} \leq 2(i+1)(d-1) - 1$, d'où $i - 1 \geq \frac{n+1}{2(d-1)} - 2$. ■

4.2 Réduction modulo une puissance d'un nombre premier

Nous pouvons maintenant obtenir facilement des bornes pour la complexité de la suite double a_{p^e} modulo une puissance d'un nombre premier.

Théorème 4.2 *Soit $l = p^e$ où p est un nombre premier. Soit R un polynôme de degré $d \geq 1$ défini sur $\mathbb{Z}/l\mathbb{Z}$. On suppose de plus que R n'est pas réduit à un monôme. Soit $P_l(n)$ la complexité en ligne de la suite double a_l engendrée par l'automate cellulaire linéaire $\mathcal{A}_R$ de condition initiale 1. Il existe alors deux constantes C_3 et C_4 (qui dépendent de p^e) telles que :*

$$\forall n,\ C_3 n^2 \leq P_l(n) \leq C_4 n^2.$$

Preuve On déduit encore la majoration de l'automaticité de la suite double a modulo p^e (théorème 2.1 et proposition 2.1).

Pour la minoration, il suffit de re-réduire modulo p la suite double a_{p^e}. On a alors, pour $n \geq 1$:

$$P_{p^e}(n) \geq P_p(n).$$

■

Remarque Ce résultat est encore valable avec une condition initiale f p-automatique. En effet, on a toujours p-automaticité de la suite double d'où la majoration. La minoration se montre de la même manière que précédemment (le lemme 4.1 est encore valable; il suffit pour initialiser la récurrence d'obtenir deux coefficients non nuls sur une même ligne, ce qui est possible si R n'est pas réduit à un monôme et si la condition initiale f est non nulle). On déduit ainsi la proposition suivante du lemme 3.1.

Proposition 4.1 *Sot $l = p^e$ où p est un nombre premier. Soit R un polynôme de degré $d \geq 1$ défini sur $\mathbb{Z}/l\mathbb{Z}$. On suppose de plus que R n'est pas réduit à un monôme. Soit a la suite double engendrée par le polynôme R, avec une condition initiale $f = \sum_{n \geq 0} f_n X^n \in \mathbb{Z}/l\mathbb{Z}\,[[X]]$ non nulle dont la suite des coefficients $(f_n)_{n \in \mathbb{N}}$ est p-automatique. Soit $P_l(m,n)$ la complexité de la suite a réduite modulo l. Il existe alors deux constantes A et B strictement positives (qui dépendent de l) telles que, quels que soient $m \geq 1$ et $n \geq d$, on ait*

$$A \sup(m,n)^2 \leq P_l(m,n) \leq B \sup(m,n)^2.$$

5 Réduction modulo deux entiers premiers entre eux

Le but de ce paragraphe est de montrer le résultat d'indépendance suivant sur la complexité en ligne.

Proposition 5.1 *Écrivons $l = l_1 l_2$, avec $l_1 \geq 2$, $l_2 \geq 2$ et $l_1 l_2$ premiers entre eux. Soit a_l la suite engendrée par l'automate cellulaire $R(X) = r_v X^v + \ldots + r_d X^d$ de condition initiale 1 sur $\mathbb{Z}/l\mathbb{Z}$. Soit v la valuation de R et d son degré. On suppose que r_d et r_v sont inversibles modulo l, et que $v < d$. Il existe une constante $C > 0$ (qui dépend de l_1 et l_2) telle que :*

$$\forall n \geq 1,\ C P_{l_1}(n) P_{l_2}(n) \leq P_{l_1 l_2}(n) \leq P_{l_1}(n) P_{l_2}(n).$$

Les arguments développés dans ce paragraphe reprennent en grande partie ceux de [3].

Notons que la majoration s'obtient en re-réduisant modulo l_1 et modulo l_2 un mot réduit modulo $l_1 l_2$:

$$\forall n \geq 1,\ P_{l_1 l_2}(n) \leq P_{l_1}(n) P_{l_2}(n).$$

Considérons maintenant la question de la minoration.

5.1 Quelques lemmes préliminaires

Nous allons d'abord démontrer quelques lemmes préliminaires. Montrons que l'on peut supposer $r_0 = r_d = 1$.

Soit $k \geq 1$. Soit a_l (respectivement $a_l^{(k)}$) la suite double engendrée par le polynôme $R(X)$ (respectivement $R^k(X)$). Les fonctions de complexité en ligne $P_l(n)$ et $P_l^{(k)}(n)$ des suites doubles a_l et $a_l^{(k)}$ vérifient respectivement : $\forall n,\ P_l^{(k)}(n) \leq P_l(n)$. En effet, un facteur en ligne de la suite $a_l^{(k)}$ est également un facteur en ligne de la suite a_l. Soit v la valuation de R et d son degré. On suppose que r_v et r_d sont inversibles dans $\mathbb{Z}/l\mathbb{Z}$. Soit φ la fonction indicatrice d'Euler. On a $r_v^{\varphi(l)} = r_d^{\varphi(l)} = 1$. D'après ce qui précède, la fonction de complexité en ligne de la suite double engendrée par le polynôme R est minorée par la fonction de complexité en ligne de la suite engendrée par $R(X)^{\varphi(l)}$. On supposera donc $r_v = r_d = 1$.

Soit a_l (respectivement a'_l) la suite double engendrée par le polynôme $R(X)$ (respectivement $X^{-v}R(X)$). Les fonctions de complexité en ligne $P_l(n)$ et $P'_l(n)$ des suites doubles a_l et a'_l sont égales, puisque les lignes de la suite a'_l sont des décalées des lignes de la suite a_l.

On supposera dans tout ce paragraphe que $v = 0$, $r_0 = 1 = r_d$. Rappelons de plus que $v < d$.

Le but du lemme suivant est de montrer que l'on peut produire en itérant le polynôme R, des lignes qui contiennent un facteur commençant par la lettre 1 suivie d'une plage arbitrairement grande de 0 et finissant par une plage arbitrairement grande de 0 suivie à son tour par la lettre 1. Nous utiliserons ensuite cette propriété afin d'exhiber une infinité d'occurrences, pour un facteur en ligne donné, situées en début et en fin de ligne. Notons que cette approche du problème n'aboutit que parce que nous nous limitons à des conditions initiales à support fini.

Lemme 5.1 *Soient $l \geq 2$ un entier et $l = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ sa décomposition en facteurs premiers. On se donne deux entiers fixés $\lambda \geq 1$ et $a \geq 1$. On a :*

$$R(X)^{\lambda l^a} = 1 + \gamma(l, \lambda, a) X^{(\inf p_i)^a} + \cdots + \delta(l, \lambda, a) X^{d\lambda l^a - (\inf p_i)^a} + X^{d\lambda l^a} \bmod l,$$

c'est-à-dire que les coefficients dans $R(X)^{\lambda l^a}$ de X^j pour $0 < j < (\inf p_i)^a$ et $d\lambda l^a - (\inf p_i)^a < j < d\lambda l^a$ sont nuls modulo l.

Preuve Travaillons dans un premier temps avec une puissance d'un nombre premier. Soit $\alpha \geq 1$ un entier fixé. On a (par exemple d'après [21])

$$R(X)^{p^\alpha} = R(X^p)^{p^{\alpha-1}} \bmod p^\alpha.$$

On en déduit par récurrence que, pour tout entier $a \geq 0$:

$$R(X)^{p^{a\alpha}} = R(X^{p^a})^{p^{a(\alpha-1)}} \bmod p^\alpha.$$

Par conséquent, on a pour tout entier $\lambda \geq 1$:

$$R(X)^{\lambda p^{a\alpha}} = R(X^{p^a})^{\lambda p^{a(\alpha-1)}} \bmod p^\alpha.$$

On a donc, pour tout $\lambda \geq 1$ et pour tout $1 \leq j \leq p^a - 1$:

$$a_{p^\alpha}(\lambda p^{a\alpha}, j) = a_{p^\alpha}(\lambda p^{a\alpha}, d\lambda p^{a\alpha} - j) = 0 \bmod p^\alpha.$$

Définissons maintenant, pour tout i, l'entier $l^{(i)}$ par $l = l^{(i)} p_i^{\alpha_i}$. Soit $j \in [1, (\inf p_i)^a - 1]$. On a alors d'après ce qui précède

$$a_{p_i^{\alpha_i}}(\lambda l^a, j) = a_{p_i^{\alpha_i}}((\lambda l^{(i)a}) p_i^{a\alpha_i}), j) = 0 \bmod p_i^{\alpha_i}$$

et

$$a_{p_i^{\alpha_i}}(\lambda l^a, d\lambda l^a - j) = a_{p_i^{\alpha_i}}((\lambda l^{(i)a})p_i^{a\alpha_i}), d\lambda l^a - j) = 0 \bmod p_i^{\alpha_i}.$$

Le lemme chinois permet de conclure que

$$\forall j \in [1, (\inf p^i)^a - 1],\ a_l(\lambda l^a, j) = a_l(\lambda l^a, d\lambda l^a - j) = 0 \bmod l. \blacksquare$$

Lemme 5.2 *Soit w un facteur en ligne de la suite a_l. Soit (u, v) un indice d'occurrence de w avec $v \geq 0$ et $du \geq v + r - 1$, où r est la longueur de w. Quels que soient $\lambda \geq 1$ et a tel que $\inf(p_i)^a > du$, le facteur w apparaît également dans la suite a_l aux indices $(u + \lambda l^a, v)$ et $(u + \lambda l^a, d\lambda l^a + v)$.*

Preuve La condition $du \geq v + r - 1$ garantit que les lettres de w apparaissent comme les coefficients du polynôme $R(X)^u$. Soit $\lambda \geq 1$. On déduit alors du lemme précédent que pour a assez grand ($\inf(p_i)^a > du$), les coefficients de $R^{u+\lambda l^a}(X)$ commencent et finissent par ceux de $R(X)^u$. $\blacksquare$

5.2 Preuve de la proposition 5.1

Rappelons qu'en re-réduisant modulo l_1 et modulo l_2 un mot réduit modulo $l_1 l_2$, on a la majoration triviale :

$$\forall n \geq 1,\ P_{l_1 l_2}(n) \leq P_{l_1}(n) P_{l_2}(n).$$

Pour montrer qu'il existe une constante $C > 0$ telle que

$$\forall n \geq 1,\ C P_{l_1}(n) P_{l_2}(n) \leq P_{l_1 l_2}(n),$$

nous allons montrer dans un premier temps la propriété d'indépendance suivante : soit $n \geq d$; soit $a_1 \cdots a_r$ un facteur (en ligne) de la suite double a_{l_1} et $b_1 \cdots b_r$ un facteur de la suite a_{l_2}, dont les indices d'occurrence en colonne respectifs v' et v'' satisfont

$$v' - v'' \equiv 0 \mod d;$$

il existe alors un *même* couple d'indices (u, v) tel que

$$a_{l_1}(u, v) \cdots a_{l_1}(u, v + n - 1) = a_1 \cdots a_n \bmod l_1$$

et

$$a_{l_2}(u, v) \cdots a_{l_2}(u, v + n - 1) = b_1 \cdots b_n \bmod l_2.$$

Le lemme chinois montre alors que le mot $c_1 \cdots c_n$ (modulo $l_1 l_2$), dont les réductions modulo l_1 et l_2 sont respectivement $a_1 \cdots a_n$ et $b_1 \cdots b_n$, apparaît (en particulier) en position (u,v) dans la suite $a_{l_1l_2}$. Nous utiliserons dans un deuxième temps ce résultat pour construire une application de $\mathcal{L}_{l_1}(n) \times \mathcal{L}_{l_2}(n+d-1)$ dans $\mathcal{L}_{l_1l_2}(n)$ telle que chaque élément de $\mathcal{L}_{l_1l_2}(n)$ n'admet au plus qu'un nombre borné (indépendemment de n) d'antécédents. Nous aurons bien alors l'autre inégalité :

$$\exists C > 0,\ \forall n \geq 1,\ P_{l_1l_2}(n) \geq CP_{l_1}(n)P_{l_2}(n).$$

Première étape Soient (u,v) et (u',v') tels que

$$a_{l_1}(u,v)\cdots a_{l_1}(u,v+n-1) = a_1\cdots a_n \bmod l_1$$

et

$$a_{l_2}(u',v')\cdots a_{l_2}(u',v'+n-1) = b_1\cdots b_n \bmod l_2,$$

avec $v-v' \equiv 0 \mod d$. Nous allons d'abord montrer que l'on peut supposer $v'=v$, c'est-à-dire trouver une autre occurrence de $a_1\cdots a_r$ et une autre occurrence de $b_1\cdots b_r$ dans leurs suites respectives, qui commencent en des colonnes de même indice. Puis nous montrerons que l'on peut aussi supposer $u'=u$.

Montrons que l'on peut supposer que les lettres des mots étudiés apparaissent comme des coefficients des polynômes $R(X)^u$ et $R(X)^{u'}$ (c'est-à-dire $v \geq 0$, $v' \geq 0$, $du \geq v+n-1$ et $du' \geq v'+n-1$). Appliquons pour cela le lemme 5.1, avec $l_1 = \prod p_i^{\alpha_i}$, et a tel que $\max\{|v|,|v'|\} < (\inf p_i)^a$ et considérons $R(X)^{u+\lambda l_1^a}$: la ligne d'indice $u+\lambda l_1^a$ contient donc le facteur $a_1\cdots a_n$ à l'indice $d\lambda l_1^a+v$ et l'on a $d\lambda l_1^a+v \geq 0$, pour λ assez grand. Le raisonnement est le même pour v'. Supposons donc maintenant $v,v' \geq 0$. Appliquons encore le lemme 5.1, avec $l_1 = \prod p_i^{\alpha_i}$, et a tel que $\max\{du, v+r-1\} < (\inf p_i)^a$ et considérons $R(X)^{u+\lambda l_1^a}$: la ligne d'indice $u+\lambda l_1^a$ contient donc le facteur $a_1\cdots a_n$ (avec des termes d'indices $< (\inf p_i)^a$) et l'on a $d(u+\lambda l_1^a) \geq v+n-1$, pour λ assez grand. Le raisonnement est le même pour u'.

Supposons donc $v \geq 0$, $v' \geq 0$, $du \geq v+n-1$ et $du' \geq v'+n-1$. Montrons que l'on peut supposer $v'=v$. Appliquons le lemme 5.2. Soit a tel que $(\min p_i)^a > du \geq v+n-1$, avec $l_1 = \prod p_i^{\alpha_i}$: quel que soit $\lambda \geq 1$, le mot $a_1\ldots a_n$ apprait aux indices $(u+\lambda l_1^a, v+d\lambda l_1^a)$. De même, pour tout $\mu \geq 1$, on montre qu'il existe un indice a' tel que le facteur $b_1\ldots b_n$ apparaît aux indices $(u'+\mu l_2^{a'}, v'+d\mu l_2^{a'})$. Pour simplifier les notations, on appellera encore a le plus grand de ces deux indices a et a'.

Supposons par exemple $v' \geq v$. Comme l_1 et l_2 sont premiers entre eux et comme $v - v' \equiv 0 \bmod d$, il existe deux entiers strictement positifs λ et μ tels que :

$$d\lambda l_1^a - d\mu l_2^a = v' - v,$$

c'est-à-dire

$$v' + d\mu l_2^a = v + d\lambda l_1^a.$$

Il suffit alors de remplacer u par $u + \lambda l_1^a$, v par $v + d\lambda l_1^a$, u' par $u' + \mu l_2^a$ et v' par $v' + d\mu l_2^a$ pour obtenir un indice d'occurrence en colonne commun, indice que l'on note encore v par abus de notation. Notons que l'on a alors toujours $v \geq 0$, $v' \geq 0$, $du \geq v + n - 1$, $du' \geq v + n - 1$.

Montrons qu'on peut maintenant, tout en gardant v, remplacer u et u' par un même indice. On applique encore le lemme 5.2. On choisit un a' tel que le plus petit nombre premier p qui divise l'un des nombres l_1 ou l_2 vérifie : $p^a > \max(du, du')$. Pour tout $\lambda' \geq 1$, $a_1 \ldots a_n$ apparaît à l'indice $(u + \lambda' l_1^{a'}, v)$. De la même façon, et quitte à remplacer a' par un entier plus grand, pour tout $\mu' \geq 1$, $b_1 \ldots b_n$ apparaît à l'indice $(u' + \mu' l_2^{a'}, v)$. Supposons $u' \geq u$, il existe comme précédemment deux entiers strictement positifs λ' et μ' tels que

$$\lambda' l_1^{a'} - \mu' l_2^{a'} = u' - u,$$

c'est-à-dire

$$u + \lambda' d_1^{a'} = u' + \mu' d_2^{a'}.$$

Nous avons donc montré que pour tout facteur $a_1 \ldots a_n$ de a_{l_1} et pour tout facteur $b_1 \ldots b_n$ de a_{l_2}, admettant des indices en colonne respectifs qui satisfaisont $v - v' \equiv 0 \bmod d$, il existe un indice d'occurrence commun dans $a_{l_1 l_2}$.

Deuxième étape Nous allons maintenant construire une application φ de $\mathcal{L}_{l_1}(n) \times \mathcal{L}_{l_2}(n + d - 1)$ dans $\mathcal{L}_{l_1 l_2}(n)$ telle que tout facteur de $\mathcal{L}_{l_1 l_2}(n)$ admet un nombre uniformément borné en n d'antécédents.

Soit $(a_1 \ldots a_n, b_1 \ldots b_{n+d-1}) \in \mathcal{L}_{l_1}(n) \times \mathcal{L}_{l_2}(n + d - 1)$.

- Supposons que toutes les ocurrences de $a_1 \ldots a_n$ et $b_1 \ldots b_{n+d-1}$ ont des indices de colonne v et v' respectivement, satisfaisant $v \equiv v' \mod d$. On applique alors ce qui a été fait précédemment pour en déduire qu'il existe (u'', v'') indice commun auquel ces deux facteurs apparaissent, respectivement dans a_{l_1} et a_{l_2}. On pose alors

$$\varphi(a_1 \ldots a_n, b_1 \ldots b_{n+d-1}) = c_1 \ldots c_n,$$

avec

$$c_1 \ldots c_n = a_{l_1 l_2}(u'', v'') \ldots a_{l_1 l_2}(u'', v'' + n - 1),$$

c'est-à-dire

$$c_1 \ldots c_n = a_1 \ldots a_n \mod l_1 \text{ et } c_1 \ldots c_n = b_1 \ldots b_n \mod l_2.$$

- Sinon, il existe un couple d'occurrences en colonne respectives (v, v') de $a_1 \ldots a_r$ dans a_{l_1} et de $b_1 \ldots b_{r+d-1}$ dans a_{l_2}, tel que $v \not\equiv v' \mod d$. Soit k le plus petit entier $1 \leq k \leq d-1$ tel qu'il existe un tel couple (v, v') avec $v - v' \equiv k \mod d$. Le facteur $b_{k+1} \ldots b_{k+n}$ apparaît à un indice de colonne v'' ($v'' = v' + k$) tel que $v \equiv v'' \mod d$. On applique ce qui a été fait précédemment pour poser $\varphi(a_1 \ldots a_n, b_1 \ldots b_{n+d-1}) = c_1 \ldots c_n$, avec

$$c_1 \ldots c_n = a_1 \ldots a_n \mod l_1 \text{ et } c_1 \ldots c_n = b_{k+1} \ldots b_{k+n} \mod l_2.$$

On voit que chaque élément de $\mathcal{L}_{l_1 l_2}(n)$ admet au plus dl_2^{d-1} antécédents par l'application φ. Soit $C = dl_2^{d-1}$.

On a donc

$$\forall n,\ P_{l_1}(n) P_{l_2}(n) \leq P_{l_1}(n) P_{l_2}(n + d - 1) \leq C P_{l_1 l_2}(n),$$

ce qui achève la preuve de la minoration. ■

6 Conclusion

Dans ce paragraphe nous allons rassembler les résultats de complexité déjà donnés pour établir un résultat général sur la complexité de la suite double a_l, puis conclure par quelques remarques.

6.1 Cas général

Théorème 6.1 *Soit a une suite double engendrée par le polynôme $R = r_d X^d + \ldots + r_v X^v$, avec une condition initiale polynomiale $P = p_t X^t + \ldots + p_0$. Soit $l \geq 1$. Soit $P_l(m, n)$ la complexité de la suite a réduite modulo l. On suppose que $v < d$, et que r_d, r_v et p_t sont inversibles modulo l. On note $\omega(l)$ le nombre de facteurs premiers distincts de la décomposition de l. Il existe alors deux constantes A et B strictement positives (qui dépendent de l) telles que, quels que soient $m \geq 1$ et $n \geq d$, on ait*

$$A \sup(m, n)^{2\omega(l)} \leq P_l(m, n) \leq B \sup(m, n)^{2\omega(l)}.$$

Preuve Ce théorème se déduit des lemmes 3.1, 3.2, du théorème 4.2 et de la proposition 5.1. ■

6.2 Remarques

Dans le cas où le polynôme R est de la forme $1 + X + \ldots + X^d$, (ou plus généralement si $r_v = r_{v-1} = 1$) on peut montrer de manière similaire que l'on a une propriété d'indépendance plus forte qui se traduit par la multiplicativité des complexités :

$$\forall n \geq d, \forall m \geq 1 \quad P_{l_1 l_2}(n) = P_{l_1}(n) P_{l_2}(n),$$

si l_1 et l_2 sont premiers entre eux. C'est en particulier le cas du triangle de Pascal [3]. Il semble raisonnable de conjecturer que cette propriété d'indépendance est vraie en général (sous les hypothèses de la proposition 5.1), l'introduction de la constante $C(l_1 l_2)$ étant due à une contrainte technique.

Notons que si l'on omet les hypothèse r_v et r_d inversibles, la conclusion de la proposition ne s'applique plus. Considérons la suite double engendrée par le ploynôme $3 + 2X$ modulo 6 avec condition initiale 1. Ni le coefficient de valuation, ni le coefficient dominant ne sont inversibles. Cette suite est automatique d'après le théorème 2.1 (on a $\chi = 0$). On a donc une majoration quadratique. Considérons de même la suite engendrée par le polynôme $2 + X$: la complexité est donc encore quadratique. Ici, seul le coefficient dominant est inversible.

Les conditions arithmétiques intervenant dans le théorème 6.1 appararaissent également dans l'étude de certaines propriétés métriques des automates comme la sensibilité aux conditions initiales, l'expansivité ou la transitivité topologique. La condition r_v et r_d inversibles dans $\mathbb{Z}/m\mathbb{Z}$ implique en particulier la sensibilité pour la distance de comptage (voir par exemple [15]), ou l'expansivité pour la distance classique de Tychonoff [17], voir aussi [16, 18].

Notons que la complexité de la suite unidimensionnelle des coefficients médiants du triangle de Pascal $(\binom{2n}{n})_{n \in \mathbb{N}}$ mod p croît linéairement en fonction de la longueur des mots, contrairement à la complexité des suites horizontales qui, elle, croît quadratiquement (pour plus de détails, voir [5]).

Nous nous sommes restreints ici à l'étude de suites indexées par $\mathbb{N}^2$ du fait que l'on a considéré tout au long de cet article des suites engendrées par condition initiale soit polynomiale, soit automatique. Pour une notion de suite automatique indexée par $\mathbb{Z}$ ou $\mathbb{Z}^2$, voir [6].

Une suite double définie sur $\mathbb{Z}^2$ est dite périodique si elle admet un vecteur de périodicité non nul. La fonction de complexité en rectangles ne permet pas de caractériser les suites périodiques : on peut en effet construire des suites doubles admettant un vecteur périodique non nul, et de complexité arbitrairement grande. Réciproquement, il est conjecturé que s'il existe un couple d'entiers non nuls (m_0, n_0) tels que $P(m_0, n_0) \leq m_0 n_0$, alors la suite double admet un vecteur périodique non nul. Notons que cette conjecture est fausse en dimension supérieure [24]. Les suites (non nulles) engendrées par automate cellulaire linéaire (considérées sur $\mathbb{Z}^2$ en complétant par des 0) sont non périodiques et ont effectivement des fonctions de complexité au moins égales à $mn + 1$ même dans le cas où R est réduit à un monôme.

Proposition 6.1 *Soit a une suite double non nulle définie sur $\mathbb{Z}^2$, engendrée par un automate cellulaire linéaire (avec condition initiale polynomiale). On a alors*

$$\forall (m, n),\ \ P(m, n) \geq mn + 1.$$

Preuve Considérons les mn facteurs rectangulaires de taille (m, n) dont l'indice d'occurrence (u, v) du coin inférieur gauche satisfait $1 - m \leq u \leq 0$ et $s + 1 - n \leq v \leq s$, où s est l'indice du plus petit coefficient non nul de la condition initiale P modulo l. Ces mn facteurs sont distincts. Il suffit alors de considérer le facteur rectangulaire nul de taille (m, n) pour exhiber un $(mn + 1)$-ième facteur. ■

Remerciements Je remercie chaleureusement Jean-Paul Allouche, Dominique Bernardi et Michel Koskas pour les nombreuses discussions que nous avons eues au sujet de ce travail. Je remercie également l'arbitre anonyme de cet article pour ses suggestions pertinentes.

Références

[1] J.-P. Allouche, Automates finis en théorie des nombres. *Expo. Math.* **5** (1987) 239–266.

[2] J.-P. Allouche, Sur la complexité des suites infinies. *Bull. Belg. Math. Soc.* **1** (1994) 133–143.

[3] J.-P. Allouche et V. Berthé, Triangle de Pascal, complexité et automates. *Bull. Belg. Math. Soc.* **4** (1997) 1–23.

[4] J.-P. Allouche et J. Shallit, The ring of k-regular sequences. *Theoret. Comput. Sci.* **98** (1992) 163–197.

[5] J.-P. Allouche et D. Berend, Complexity of the sequence of middle-binomial coefficients. *En préparation.*

[6] J.-P. Allouche, E. Cateland, W.J. Gilbert, H.-O. Peitgen, J. Shallit et G. Skordev, Automatic maps on semiring with digits. *Theory Comput. Syst. (Math. Systems Theory)* **30** (1997) 285–331.

[7] J.-P. Allouche, F. von Haeseler, H.-O. Peitgen et G. Skordev, Linear cellular automata, finite automata and Pascal's triangle. *Discrete Applied Mathematics* **66** (1996) 1–22.

[8] J.-P. Allouche, F. von Haeseler, H.-O. Peitgen, A. Petersen et G. Skordev, Automaticity of double sequences generated by one-dimensional linear cellular automata. *Theoret. Comput. Sci.* **88** (1997) 195–209.

[9] F. Blanchard, P. Kurka et A. Maass, Topological and measure-theoretic properties of one-dimensional cellular automata. *Phys.* **103** (1997) 86–99.

[10] J. Cassaigne, Special factors of sequences with linear subword complexity, in *Developments in Language Theory II (DLT'95)*, Magdeburg (Allemagne), World Scientific (1996) 25–34.

[11] A. Cobham, Uniform tag sequences. *Math. Systems Theory* **6** (1972) 164–192.

[12] C. Grillenberger, Construction of strictl y ergodic systems I. Given entropy. *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete* **25** (1973) 323–334.

[13] I. Korek, Pascal triangles modulo n and modular trellises. *Comput. Artificial Intelligence* **9** (1990) 105–113.

[14] B. Litow et P. Dumas, Additive cellular automata and algebraic series. *Theoret. Comput. Sci.* **119** (1993) 345–354.

[15] G. Manzini, Characterization of sensitive linear cellular automata with respect to the counting distance, in *MFCS'98*, Lecture Notes in Comput. Sci. **1450** (1998) 825–833.

[16] G. Manzini et L. Margara, Attractors of D-dimensional linear cellular automata, in *STACS 98*, Lecture Notes in Comput. Sci. **1373** (1998) 128–138.

[17] G. Manzini et L. Margara, Invertible cellular automata over $\mathbb{Z}_m$: algorithmic and dynamical aspects. *J. Comput. System Sci.* **56** (1998) 60–67.

[18] G. Manzini et L. Margara, A complete and efficiently computable topological classification of D-dimensional linear cellular automata over $\mathbb{Z}_m$, in *ICALP'97*, Theoret. Comput. Sci. **221** (1999) 157–177.

[19] O. Martin, A. Odlyzko et S. Wolfram, Algebraic properties of cellular automata. *Commun. Math. Phys.* **93** (1984) 219–258.

[20] J.-J. Pansiot, Complexité des facteurs des mots infinis engendrés par morphismes itérés, in *Lecture Notes Comput. Sci.* **172** (1984) 380–389.

[21] A. D. Robinson, Fast computation of additive cellular automata. *Complex Systems* **1** (1987) 211–216.

[22] O. Salon, Suites automatiques à multi-indices et algébricité. *C. R. Acad. Sci. Paris, Série I* **305** (1987) 501–504.

[23] O. Salon, Suites automatiques à multi-indices. *Séminaire de Théorie des Nombres de Bordeaux, Exposé 4* (1986-1987), 4-01–4-27; suivi par un Appendice de J. Shallit, 4-29A–4-36A.

[24] J. W. Sander, R. Tijdeman, The complexity of functions on lattices. *Theoret. Comput Sci.*, à paraître.