INFORMATIQUE THÉORIQUE ET APPLICATIONS

L. DUBUC

Sur les automates circulaires et la conjecture de Černý

Informatique théorique et applications, tome 32, n° 1-3 (1998), p. 21-34.

<http://www.numdam.org/item?id=ITA_1998__32_1-3_21_0>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 32, n° 1-2-3, 1998, pp. 21-34)

SUR LES AUTOMATES CIRCULAIRES ET LA CONJECTURE DE ČERNÝ (*)

par L. DUBUC (1)

Communiqué par C. CHOFFRUT

Résumé. – *Un mot synchronisant amène tous les états d'un automate fini à un unique état. Černý a conjecturé que la longueur minimale des mots synchronisants d'un automate à n états est au plus $(n-1)^2$. Dans cet article, nous généralisons notre précédent résultat (la confirmation de la conjecture pour les automates circulaires biaisés) aux automates circulaires.* © Elsevier, Paris

Abstract. – *A reset word takes all states of a finite automaton to a single state. Černý conjectured that every n-state automaton admitting a reset word admits a short reset word, i.e. one of length at most $(n-1)^2$. In this paper, we generalize our earliest result (the proof of the conjecture about biaised circular automata) to all circular automata.* © Elsevier, Paris

1. INTRODUCTION

La conjecture de Černý traite de la longueur des *mots synchronisants*, susceptibles de ramener, aussi vite que possible, un automate déterministe complet fini à un même état, quel que soit l'état où il se trouve. Si un tel mot existe l'automate est dit *synchronisant* et il s'agit alors de borner le *temps de synchronisation*, c'est-à-dire la longueur d'un plus court mot synchronisant, en fonction de la taille n de l'automate. Cet article présente les progrès réalisés dans l'étude de la conjecture sur les automates circulaires (où l'une des lettres agit comme une permutation circulaire). Il se situe dans le prolongement de notre article antérieur, en généralisant les résultats de [Dub96]. Il hérite de plus de la méthode employée, méthode d'augmentation réciproque [Dub96], [Sav], [Pin78b]. Afin d'exploiter l'efficacité de l'algèbre linéaire, on étudie le problème à partir d'une structure linéaire, technique déjà abordée par d'autres auteurs ([Pin78e], [Sav]), bien adaptée à cette

(*) Reçu juin 1997, accepté mars 1998.

(1) Laboratoire d'Informatique de Rouen, Faculté des Sciences et des Techniques, 76821 Mont-Saint-Aignan Cedex, France. dubuc@dir.univ-rouen.fr

classe d'automates. Nous confirmons de cette façon la conjecture de Černý pour les automates circulaires.

2. NOTATIONS ET DÉFINITIONS

Pour étudier les phénomènes de synchronisation, il suffit de considérer les automates déterministes complets finis sous la forme très rudimentaire d'un ensemble fini d'états soumis à une action

$$X \times A^* \to X : (x, w) \mapsto x * w$$

du monoïde libre A^* sur un alphabet fini A. On va noter un tel automate par (X, A), l'action étant sous-entendue.

Etant donné un automate (X, A), on définit, pour un mot $w \in A^*$ et pour un ensemble d'états $S \subseteq X$, les notions suivantes : l'*image (directe)* de S par $w, S * w = \{x * w \mid x \in S\}$; l'*image réciproque* de S par $w, S * w^{-1} = \{x \in X \mid x * w \in S\}$; le *rang* de $w, rang(w) = card(X * w)$.

Tout mot w de rang 1 pour (X, A) est appelé un *mot synchronisant* de (X, A), et (X, A) est un *automate synchronisant* s'il admet un mot synchronisant.

CONJECTURE 2.1 (J. Černý) : *Soit (X, A) un automate à n états. S'il est synchronisant, alors il admet un mot synchronisant $w \in A^*$ de longueur $|w| \leq (n-1)^2$.*

Soient (X, A) un automate à n états (n-automate), S une partie de X. S est dit *réciproquement augmenté* par w où $w \in A^*$ si $card(S * w^{-1}) > card(S)$. Soit $m \in \mathbb{N}$. S est dit *réciproquement augmentable* (*réciproquement m-augmentable*) dans (X, A) s'il existe un mot $w \in A^*$ (de longueur $|w| \leq m$) tel que $card(S * w^{-1}) > card(S)$.

Soit E un ensemble de mots sur A. On note par $||E||$ le maximum des longueurs des mots de E. L'ensemble E est dit *régressif* si pour toute partie propre T ($\emptyset \neq T \neq X$) de X, il existe un mot w dans E tel que T est réciproquement augmenté par w. Si (X, A) admet un ensemble E régressif, alors il admet un mot synchronisant de longueur $|w| \leq 1 + (n-2)||E||$. En effet, cela est évident après avoir remarqué qu'il existe nécessairement un état qui soit augmenté par une lettre.

On va confirmer la conjecture de Černý pour les automates circulaires en prouvant que, si (X, A) est circulaire synchronisant alors $\{w \in A^* \mid |w| \leq n\}$

est un ensemble régressif autrement dit toute partie propre de X est n-augmentable. On en déduira qu'il existe un mot synchronisant de longueur majorée par $1 + (n-2)n = (n-1)^2$.

Soit x_0 un état fixé de X. Un automate (X, A) à n états est un *automate circulaire* s'il existe $c \in A$ telle que $\{x_0 * c^i \mid 1 \leq i \leq n\} = X$. Notons désormais $x_i = x_0 * c^i$ pour $i = 1, \ldots n$.

3. LA STRUCTURE LINÉAIRE

L'idée maîtresse à l'origine de la linéarisation consiste à poser le problème dans un cadre où l'on puisse appliquer les acquis de l'algèbre linéaire. Étant donné (X, A) un automate circulaire à n états, considérons le plongement de l'ensemble $\mathcal{P}(X)$ des parties de X dans l'espace vectoriel réel $\mathbb{R}^{1\times n}$. Nous allons associer à toute partie $S \subseteq X$ son vecteur (ligne) caractéristique, défini comme une $(1 \times n)$-matrice $[S] = (s_1, \ldots, s_n)$ sur le corps des réels $\mathbb{R}$ où

$$s_i = \begin{cases} 1 \text{ si } x_i \in S, \\ 0 \text{ sinon} \end{cases} \quad \text{pour } i = 1, \ldots, n.$$

Ainsi, les vecteurs caractéristiques des singletons $\{x_i\}, i = 1, \ldots, n$, sont confondus avec la base $e_1, \ldots, e_n$ canonique de l'espace vectoriel $\mathbb{R}^{1\times n}$ des $(1 \times n)$-matrices sur $\mathbb{R}$.

Sur cet espace, nous disposons de la notion d'orthogonalité, issue du produit scalaire usuel $\langle x, y\rangle = xy^T$ (produit matriciel de x et du transposé y^T de y). Les vecteurs x et y de $\mathbb{R}^{1\times n}$ sont orthogonaux, $x \perp y$, ssi $\langle x, y\rangle = 0$. La forme linéaire "somme des coordonnées" sur $\mathbb{R}^{1\times n}$ définie par $x \mapsto \langle x, [X]\rangle$, généralise l'opérateur "cardinal" pour les parties de X, de manière que $card(S) = \langle [S], [X]\rangle$ pour $S \subseteq X$. A toute lettre $g \in A$, nous allons associer une $(n \times n)$-matrice $[g]$ sur $\mathbb{R}$, définie par

$$[g]_{i,j} = \begin{cases} 1 \text{ si } x_i * g = x_j, \\ 0 \text{ sinon} \end{cases} \quad \text{pour } i = 1, \ldots, n.$$

S'agissant d'un automate déterministe complet, nécessairement chaque ligne de la matrice $[g]$ comporte exactement une valeur non nulle, on parle de matrice monômiale en lignes. De plus ici la valeur est égale à 1. Puis évidemment, à tout mot $w \in A^*$ est associé la $(n \times n)$-matrice $[w]$ sur $\mathbb{R}$, définie par

$$[w]_{i,j} = \begin{cases} 1 \text{ si } x_i * w = x_j, \\ 0 \text{ sinon} \end{cases} \quad \text{pour } i = 1, \ldots, n.$$

Il est alors clair que pour tout $w \in A^*$ s'écrivant $w = a_1 \cdots a_k$, nous avons $[w] = [a_1] \cdots [a_k]$. Là aussi la matrice $[w]$ fait partie des $(n \times n)$-matrices monômiales en lignes dont les valeurs non nulles sont égales à 1, celles-ci formant un monoïde (pour le produit matriciel). La matrice associée à c est ainsi la matrice circulante

$$c_{i,j} = \begin{cases} 1 \text{ si } j = i+1 \text{ pour } 1 \leq i \leq n-1 \text{ ou } (i,j) = (n,1), \\ 0 \text{ sinon.} \end{cases}$$

L'action réciproque par $w \in A^*$ sur $\mathcal{P}(X)$ a alors la représentation matricielle très commode

$$[S * w^{-1}] = [S][w]^T, \text{ pour } S \subseteq X.$$

Le lemme suivant rappelle des résultats d'algèbre linéaire appliqués à la situation présente.

LEMME 3.1 : *Soit l'espace vectoriel* $\mathbb{V} = \mathbb{R}^{1 \times n}$ *muni de l'endomorphisme* $[c]$ *agissant comme permutation circulaire sur les vecteurs de la base canonique.*

a) Soit $P(x)$ *un polynôme qui divise le polynôme minimal de* $[c]$

$$M_{[c]}(x) = x^n - 1 = P(x)Q(x).$$

Alors $\mathbb{V} = Ker(P([c])) \oplus Im(P([c]))$, $Ker(P([c])) = Im(Q([c]))$ *et* $Ker(Q([c])) = Im(P([c]))$.

b) Soit F *un sous-espace vectoriel de* $\mathbb{V}$, *stable par* $[c]$. *Alors*

$$F = Ker\ P([c]),$$

où $P(x)$ *désigne le polynôme minimal annulateur de la restriction de* $[c]$ *sur* F.

Preuve :

a) Comme $M_c([c]) = 0$, on a déjà $Im\ Q([c]) \subseteq Ker\ P([c])$ et $Im\ P([c]) \subseteq Ker\ Q([c])$. $M_{[c]}(x)$ se décompose dans $\mathbb{C}$ en

$$x^m - 1 = \prod_{\alpha \in U} (x - \alpha),$$

où U est l'ensemble des racines n-èmes de l'unité. Aussi P et Q sont nécessairement premiers entre eux. D'après le théorème de Bezout, il existe des polynômes $G_1(x)$ et $G_2(x)$ tels que

$$1 = P(x)G_1(x) + Q(x)G_2(x),$$

ce qui se traduit par

$$I = P([c])G_1([c]) + Q([c])G_2([c]) = G_1([c])P([c]) + G_2([c])Q([c]),$$

I désignant l'identité sur $\mathbb{V}$. De $I = G_1([c])P([c]) + G_2([c])Q([c])$ on tire que pour tout vecteur y de $\mathbb{V}$

$$y = y\,G_1([c])P([c]) + y\,G_2([c])Q([c]),$$

donc $\mathbb{V} = Im\ P([c]) + Im\ Q([c])$. De $I = P([c])G_1([c]) + Q([c])G_2([c])$ on tire que si $y \in Ker\ P([c]) \cap Ker\ Q([c])$, alors nécessairement $y = 0$. De tout ceci on déduit $\mathbb{V} = Ker\ P([c]) + Ker\ Q([c])$ puis $\mathbb{V} = Ker\ P([c]) \oplus Ker\ Q([c])$ et $Ker\ P([c]) = Im\ Q([c])$, $Ker\ Q([c]) = Im\ P([c])$.

b) D'abord $F \subseteq Ker\ P([c])$ et $deg\ P(x) \leq dim\ F$. Par ailleurs, l'endomorphisme $M_{[c]}$ est nul sur $\mathbb{V}$, donc à fortiori sur F. D'où le polynôme $M_{[c]}$ est multiple du polynôme minimal annulateur de la restriction de $[c]$ sur F nommé P. Posons donc $M_{[c]}(x) = P(x)Q(x)$. D'après a), on a $Ker\ Q([c]) = Im\ P([c])$. Puisque P divise $M_{[c]}$, nécessairement il est le polynôme minimal annulateur de la restriction de c à $Ker\ P(c)$. De même Q est le polynôme minimal annulateur de la restriction de $[c]$ à $Ker\ Q([c])$. Donc $deg\ P \leq dim\ Ker\ P([c])$ et $deg\ Q \leq dim\ Im\ P([c])$. Cela implique

$$n = deg\ P + deg\ Q \leq dim\ Ker\ P([c]) + dim\ Im\ P([c]) = n.$$

Donc $deg\ P = dim\ Ker\ P([c])$ puis $dim\ Ker\ P([c]) = deg\ P \leq dim\ F$. Or $F \subseteq Ker\ P([c])$. D'où le résultat

$$F = Ker\ P([c]). \quad \square$$

4. RÉSULTATS

Sachant que dans un automate circulaire synchronisant toute partie propre est augmentable, il suffit finalement de démontrer que toute partie propre augmentable d'un automate circulaire est n-augmentable. Il s'agit donc d'une généralisation du résultat prouvé dans l'article [Dub96] qui appliquait la même stratégie de preuve.

LEMME 4.1 : *Soient (X, A) un n-automate et f une lettre dans A. Alors $[X]([f] - I)$ est la projection orthogonale sur $[X]^{\perp}$ de $[X][f]$, I désignant la $(n \times n)$−matrice identité.*

Preuve : Remarquons immédiatement que $[X]([f] - I) - [X][f]$ est orthogonal à $[X]^{\perp}$. Il reste à montrer que $[X]([f] - I)$ appartient à $[X]^{\perp}$. Il a été vu plus haut que chaque ligne de $[f]$ comporte exactement une valeur non nulle, valeur égale à 1. Ainsi

$$[f][X]^T = [X]^T.$$

Par conséquent

$$\langle [X]([f] - I), [X] \rangle = [X][f][X]^T - [X][X]^T = n - n = 0 \quad \square$$

DÉFINITION 4.2 : *Soit (X, A) un n-automate circulaire où c désigne la permutation circulaire. Pour toute lettre f dans A, notons $u_f \stackrel{def}{=} [X]([f] - I)$ projection orthogonale sur $[X]^{\perp}$ de $[X][f]$ d'après le lemme 4.1. Notons $\delta_c(w)$ le mot obtenu de $w \in A^*$ par suppression de toutes les occurrences de la lettre c. Définissons pour toute lettre f dans A*

$$L_{-1}(f) \stackrel{def}{=} \{0_{\mathbb{R}^{1\times n}}\}$$

et pour tout $r \in \mathbb{N}$ le sous-espace de $\mathbb{R}^{1\times n}$ $L_r(f)$ par son ensemble de générateurs :

$$L_r(f) \stackrel{def}{=} \mathcal{L}\left(u_f[w] \mid w \in A^*,\ |\delta_c(w)| \leq r\right),$$

où $\mathcal{L}$ désigne l'espace vectoriel engendré.

Remarquons que, pour tout $f \in A$, la suite des espaces vectoriels $L_r(f)$ pour $r \geq -1$ est croissante. L'intérêt du lemme suivant est d'obtenir pour $L_r(f)$ un ensemble de générateurs de la forme $\{u_f[w] \mid |w| \leq n-1\}$, ce qui s'avèrera primordial pour la suite.

LEMME 4.3 : *Pour tous $f \in A$ et $r \in \mathbb{N}$, notons $K_{-1}(f) = L_{-1}(f)$ et*

$$K_r(f) \stackrel{def}{=} \mathcal{L}\left(u_f[w] \mid w \in A^*,\ |\delta_c(w)| \leq r \text{ et } |w| \leq n-1\right).$$

Alors $L_r(f) = K_r(f)$.

Preuve : La définition de $L_r(f)$ donne facilement

$$(1) \qquad L_r(f) \stackrel{def}{=} \mathcal{L}\left(L_{r-1}(f), v[gc^k] \mid v \in L_{r-1}(f), g \in A, k \in \mathbb{N}\right).$$

Donc, en notant p_r le polynôme minimal annulateur de la restriction de $[c]$ sur $L_r(f)$, de $L_0(f) \subseteq L_1(f) \subseteq \cdots$, on tire p_0 divise p_1 divise $\cdots$. Notons

$$J_r(f) \stackrel{def}{=} \mathcal{L}\left(u_f[c^{h_0}(g_1c^{h_1})\cdots(g_rc^{h_r})]\right.$$
$$\left. \mid h_0 \leq deg(p_0)-1, h_j \leq deg\left(\frac{p_j}{p_{j-1}}\right)-1,\ g_j \in A \text{ pour } 1 \leq j \leq r\right).$$

Puisque dans la définition de $J_r(f)$, la lettre g_r peut être égale à c, on a facilement

$$(2)\ J_r(f) = \mathcal{L}\left(J_{r-1}(f), v[gc^k] \mid v \in J_{r-1}(f), g \in A, k \leq deg\left(\frac{p_r}{p_{r-1}}\right)-1\right).$$

Montrons par récurrence sur $r \geq 0$ $L_r(f) = J_r(f)$. Le cas $r = 0$ est trivial. Supposons (hypothèse de récurrence) que $L_{r-1}(f) = J_{r-1}(f)$ et montrons $L_r(f) = J_r(f)$. Soient $v \in J_{r-1}(f)$ et $g \in A$. Alors $v[g] \in L_r(f)$ et $v[g]\left(\frac{p_r}{p_{r-1}}\right)([c]) \in Ker\ p_{r-1}([c])$. Or, d'après le lemme 3.1 b) et l'hypothèse de récurrence

$$Ker\ p_{r-1}([c]) = L_{r-1}(f) = J_{r-1}(f).$$

Ainsi

$$\mathcal{L}\left(J_{r-1}(f), v[gc^k] \mid v \in J_{r-1}(f), g \in A, k \leq deg\left(\frac{p_r}{p_{r-1}}\right)-1\right)$$
$$= \mathcal{L}\left(J_{r-1}(f), v[gc^k] \mid v \in J_{r-1}(f), g \in A, k \in \mathbb{N}\right).$$

Grâce aux égalités (1) et (2) et à l'hypothèse de récurrence, il en découle l'égalité

$$J_r(f) = L_r(f)$$

ce qui achève la preuve par récurrence. Pour conclure, il suffit de remarquer que, vu les définitions de $L_r(f), J_r(f)$ et $K_r(f)$, trivialement

$$J_r(f) \subseteq K_r(f) \subseteq L_r(f). \quad \square$$

Les définitions de partie réciproquement augmentée et augmentable traduisent des inégalités sur des cardinaux d'ensembles. Or dans le théorème final, les égalités correspondantes seront absolument nécessaires au raisonnement. Aussi le lemme suivant permettra justement de passer aux égalités.

LEMME 4.4 : *Soient (X, A) un n-automate circulaire et $f \in A$. Soient un entier $r \geq 0$ et $g_1, \cdots, g_r$ des lettres de A. Alors*

$$\sum_{\substack{h_0,\ldots,h_r \in \mathbb{N} \\ h_0+\cdots+h_r \leq n-1-r}} u_f[c^{h_0} g_1 c^{h_1} \cdots g_r c^{h_r}] \in L_{r-1}(f).$$

Preuve : La démarche pour prouver ce lemme est de montrer la propriété plus forte suivante :

Pour tous $r, p, k, l \in \mathbb{N}$, $f, g_1, \ldots, g_r \in A$ et $w \in A^*$ tel que $|\delta_c(w)| = p$,

$$\sum_{\substack{t_0,\ldots,t_r \in \mathbb{N} \\ t_0+\cdots+t_r \leq n-1-r}} u_f[wc^{t_0+k}(g_1 c^{t_1}) \cdots (g_{r-1} c^{t_{r-1}}) g_r c^{t_r+l}] \in L_{p+r-1}(f).$$

La propriété originelle sera retrouvée en affectant le mot vide à w et 0 à k et l. La nouvelle propriété va être prouvée par récurrence sur $r \in \mathbb{N}$. Tout d'abord les propriétés

$$u_f \in [X]^{\perp},\ \sum_{j=0}^{n-1} [c^j] = [X]^T [X] \text{ et } [g][X]^T = [X]^T \text{ pour tout } g \in A$$

sont déduites des définitions et impliquent

$$u_f[w] \sum_{j=0}^{n-1} [c^j] = (0, \ldots, 0) \in \mathbb{R}^{1 \times n} \text{ pour tout } w \in A^*.$$

La formule pour $r = 0$ en découle

$$\sum_{\substack{t_0 \in \mathbb{N} \\ t_0 \leq n-1}} u_f[wc^{t_0+k}] \in L_{p-1}(f)$$

Le cas initial $r = 0$ est prouvé. Adoptons dès à présent les notations suivantes. Notons $t = (t_0, \ldots, t_r) \in \mathbb{N}^{r+1}$ et les parties de $\mathbb{N}^{r+1}$

$$T_{r+1} = \left\{ (t_0, \ldots, t_r) \mid \sum_{i=0}^{r} t_i \leq n-1-r \right\},$$

$$U_{r+1} = \left\{ (t_0, \ldots, t_r) \mid \sum_{i=0}^{r} t_i \leq n-r \right\}.$$

Les entiers p, k, l et le mot $w \in A^*$ (tel que $|\delta_c(w)| = p$) étant fixés, on note

$$mot(t) = u_f[wc^{t_0+k}(g_1c^{t_1})\cdots(g_{r-1}c^{t_{r-1}})g_rc^{t_r+l}].$$

Il faut donc démontrer par récurrence sur $r \geq 0$ que, pour tous $p, k, l \in \mathbb{N}$, $f, g_1, \ldots, g_r \in A$ et $w \in A^*$ tel que $|\delta_c(w)| = p$,

$$\sum_{t\in T_{r+1}} mot(t) \in L_{p+r-1}(f).$$

Le cas initial a été montré plus haut. Supposons (hypothèse de récurrence) que pour tous $p, k, l \in \mathbb{N}$, $f, g_1, \ldots, g_{r-1} \in A$ et $w \in A^*$ tel que $|\delta_c(w)| = p$,

$$\sum_{t\in T_r} mot(t) \in L_{p+r-2}(f)$$

et montrons la propriété au rang suivant. Analysons les termes de cette égalité triviale

$$(3) \qquad \sum_{\substack{t\in U_{r+1}\\ t_r\neq 0}} mot(t) - \sum_{\substack{t\in U_{r+1}\\ t_0\neq 0}} mot(t) = \sum_{\substack{t\in U_{r+1}\\ t_0=0}} mot(t) - \sum_{\substack{t\in U_{r+1}\\ t_r=0}} mot(t).$$

Par hypothèse de récurrence,

$$\sum_{(t_0,\ldots,t_{r-1})\in T_r} u_f[wc^{t_0+k}(g_1c^{t_1})\cdots(g_{r-2}c^{t_{r-2}})g_{r-1}c^{t_{r-1}+l}] \in L_{p+r-2}(f).$$

Or,

$$\sum_{\substack{t\in U_{r+1}\\ t_r=0}} mot(t)$$
$$= \Big(\sum_{(t_0,\ldots,t_{r-1})\in T_r} u_f[wc^{t_0+k}(g_1c^{t_1})\cdots(g_{r-2}c^{t_{r-2}})g_{r-1}c^{t_{r-1}}]\Big)[g_rc^l],$$

donc

$$\sum_{\substack{t\in U_{r+1}\\ t_r=0}} mot(t) \in \mathcal{L}\,(v[gc^k] \mid v \in L_{p+r-2}(f), g \in A, k \in \mathbb{N}) \subseteq L_{p+r-1}(f).$$

Par ailleurs,

$$\sum_{\substack{t\in U_{r+1}\\ t_0=0}} mot(t) = \sum_{(t_1,\ldots,t_r)\in T_r} u_f[wc^k(g_1c^{t_1})\cdots(g_{r-1}c^{t_{r-1}})g_rc^{t_r+l}]$$
$$= \sum_{(t_1,\ldots,t_r)\in T_r} u_f[(wc^kg_1)c^{t_1}(g_2c_{t_2})\cdots(g_{r-1}c^{t_{r-1}})g_rc^{t_r+l}]$$
$$\in L_{(p+1)+r-2}(f) \text{ par hypothèse de récurrence. Ainsi}$$

la partie gauche de l'égalité (3)

$$\sum_{\substack{t\in U_{r+1}\\ t_r\neq 0}} mot(t) \; - \sum_{\substack{t\in U_{r+1}\\ t_0\neq 0}} mot(t) \in L_{p+r-1}(f).$$

Or, d'une part

$$\sum_{\substack{t\in U_{r+1}\\ t_r\neq 0}} mot(t) = \sum_{T_{r+1}} mot(t)[c],$$

et d'autre part

$$\sum_{\substack{t\in U_{r+1}\\ t_0\neq 0}} mot(t) = \sum_{T_{r+1}} u_f[wc^{t_0+k}c(g_1c^{t_1})\cdots(g_{r-1}c^{t_{r-1}})g_rc^{t_r+l}].$$

Donc

$$\sum_{T_{r+1}} u_f[wc^{t_0+k}(g_1c^{t_1})\cdots(g_{r-1}c^{t_{r-1}})g_rc^{t_r+l}][c]$$
$$- \sum_{T_{r+1}} u_f[wc^{t_0+k}][c][(g_1c^{t_1})\cdots(g_{r-1}c^{t_{r-1}})g_rc^{t_r+l}] \in L_{p+r-1}(f).$$

Ceci étant valable pour tous naturels k et l, on peut généraliser à tout polynôme P

$$\sum_{T_{r+1}} u_f[wc^{t_0+k}(g_1c^{t_1})\cdots(g_{r-1}c^{t_{r-1}})g_rc^{t_r+l}]P([c])$$
$$- \sum_{T_{r+1}} u_f[wc^{t_0+k}]P([c])[(g_1c^{t_1})\cdots(g_{r-1}c^{t_{r-1}})g_rc^{t_r+l}] \in L_{p+r-1}(f).$$

En particulier, avec le polynôme minimal annulateur de $[c]$ sur $L_{p+r-1}(f)$ noté $P_{L_{p+r-1}(f)}$, le second terme se trouve annulé car $u_f[w] \in L_p(f) \subseteq L_{p+r-1}(f)$, et on obtient

$$\sum_{T_{r+1}} u_f[wc^{t_0+k}(g_1c^{t_1})\cdots(g_{r-1}c^{t_{r-1}})g_rc^{t_r+l}]P_{L_{p+r-1}(f)}([c]) \in L_{p+r-1}(f).$$

Or, d'après le lemme 3.1,

$$L_{p+r-1}(f) = Ker\ P_{L_{p+r-1}(f)}([c])$$

et

$$Ker\ P_{L_{p+r-1}(f)}([c]) \cap Im\ P_{L_{p+r-1}(f)}([c]) = \{0_{\mathbb{R}^{1\times n}}\}.$$

Ainsi

$$\sum_{T_{r+1}} u_f [w c^{t_0+k} (g_1 c^{t_1}) \cdots (g_{r-1} c^{t_{r-1}}) g_r c^{t_r+l}] P_{L_{p+r-1}(f)}([c]) = 0,$$

ce qui termine la preuve par récurrence. On conclut la preuve du lemme lui-même en appliquant ce résultat avec $k = l = 0$ et w le mot vide. □

LEMME 4.5 : *Soient (X, A) un n-automate circulaire et S une partie quelconque de X. Alors, pour tout $r \in \mathbb{N}$,*

$$[S] \in (\bigcup_{f\in A} L_{r-1}(f))^{\perp} \implies \begin{array}{c} \forall w \in A^* \mid |\delta_c(w)| \leq r, \\ card(S) = card(S * w^{-1}). \end{array}$$

Preuve : La partie droite de l'implication signifie : le cardinal de S est inchangé par application réciproque de tout mot dont le nombre de lettres distinctes de c est au plus r. Le lemme va être démontré par récurrence sur $r \in \mathbb{N}$. Le cas initial $r = 0$ est évident. Il consiste à remarquer que pour toute partie S de X et tout naturel i,

$$card(S) = card(S * (c^i)^{-1})$$

En effet les seuls mots $w \in A^*$ vérifiant $|\delta_c(w)| = 0$ sont les puissances c^i de c. Supposons (hypothèse de récurrence) la propriété établie au rang $r-1$ et établissons-la au rang r. Soit donc une partie S telle que

$$[S] \in (\bigcup_{f\in A} L_{r-1}(f))^{\perp}. \tag{4}$$

La suite des espaces $L_r(f)$ pour $r \geq -1$ étant croissante, cela implique

$$[S] \in (\bigcup_{f\in A} L_{r-2}(f))^{\perp}.$$

L'hypothèse de récurrence donne alors

$$\forall w \in A^* \mid |\delta_c(w)| \leq r-1,\ \ \langle [S], [X] \rangle = \langle [S * w^{-1}], [X] \rangle.$$

Par ailleurs, la propriété (4) peut s'écrire (pour tout $f \in A$),

$$\forall w \in A^* |\ |\delta_c(w)| \leq r-1,\ \ \langle [S], [X]([f]-I)[w] \rangle = 0$$

puis

$$\forall w \in A^* |\ |\delta_c(w)| \leq r-1,\ \ \langle [S * w^{-1} * f^{-1}], [X] \rangle = \langle [S * w^{-1}], [X] \rangle.$$

Appliquons l'hypothèse de récurrence pour avoir

$$\forall w \in A^* |\ |\delta_c(w)| \leq r-1,\ \ card(S * (fw)^{-1}) = card(S).$$

Le cardinal de toute partie étant inchangé par application réciproque de n'importe quelle puissance c^i de la permutation c, $card\big(S * (c^i fw)^{-1}\big) = card(S * (fw)^{-1})$ et donc

$$\forall w \in A^* |\ |\delta_c(w)| \leq r-1, \forall i \in \mathbb{N},\ \ card(S * (c^i fw)^{-1}) = card(S).$$

Pour conclure, il suffit de reconnaître en la forme $c^i fw$ tout mot $w' \in A^*$ tel que $|\delta_c(w')| \leq r$. □

PROPOSITION 4.6 : *Soient (X, A) un n-automate circulaire et S une partie quelconque de X. Si S est réciproquement augmentable alors S est réciproquement n-augmentable.*

Preuve : Prouvons la contraposée de l'assertion, à savoir : si S est non réciproquement n-augmentable alors S est non réciproquement augmentable. Il suffit de montrer que si S est non réciproquement n-augmentable alors

$$[S] \in \Big(\bigcup_{r \in \mathbb{N},\ f \in A} L_{r-1}(f) \Big)^{\perp}.$$

En effet si ceci est vrai, on en déduit le résultat grâce au lemme 4.5 appliqué pour r décrivant $\mathbb{N}$.

Nous allons donc montrer (par récurrence sur $r \in \mathbb{N}$) que, si S est non réciproquement n-augmentable alors pour tous $f \in A$ et $r \in \mathbb{N}$, nous avons $[S] \in K_{r-1}(f)^{\perp}$ $(= L_{r-1}(f)^{\perp}$ d'après le lemme 4.3).

Pour $r = 0$, on a bien évidemment $[S] \in \{0\}^{\perp} = K_{-1}(f) = L_{-1}(f)$. Supposons (hypothèse de récurrence) que $[S] \in L_{r-1}(f)^{\perp}$ pour toute lettre f et démontrons que $[S] \in K_r(f)^{\perp} = L_r(f)^{\perp}$.

Soient $t_0, t_1, \ldots, t_r \in \mathbb{N}$ vérifiant $t_0+\cdots+t_r \leq n-1-r$ et $f,\ g_k \in A$ pour $k = 1, \ldots, r$ et notons $w = c^{t_0} g_1 c^{t_1} \cdots g_r c^{t_r}$. Ce mot vérifie $|w| \leq n-1$. Aussi S est non réciproquement augmenté par fw

$$card(S * w^{-1} * f^{-1}) \leq card(S).$$

Par hypothèse de récurrence, $[S] \in L_{r-1}(g)^{\perp}$ pour toute lettre $g \in A$. Le lemme 4.5 implique alors $card(S) = card(S * w^{-1})$. Il vient $card(S * w^{-1} * f^{-1}) \leq card(S * w^{-1})$ c'est-à-dire

$$\langle [S], u_f[w] \rangle \leq 0.$$

Or par hypothèse de récurrence, $[S] \in L_{r-1}(f)^{\perp}$. Aussi, par le lemme 4.4, on a pour tous $g_1, \ldots, g_r \in A$

$$\langle [S], \sum_{0 \leq i_0+\cdots+i_r \leq n-1-r} u_f[c^{i_0} g_1 c^{i_1} \cdots g_r c^{i_r}] \rangle = 0.$$

Par conséquent, de l'inégalité on passe à l'égalité

$$\langle [S], u_f[w] \rangle = 0$$

$[S]$ est donc orthogonal à tout générateur de $K_r(f) = L_r(f)$. □

REMERCIEMENTS

Je tiens à remercier le Laboratoire d'Informatique Rouennais pour son accueil chaleureux.

BIBLIOGRAPHIE

[Čer64] J. Černý, Poznámka k homogénnym experimenton s konečnými automatmi, *Mat. fyz. čas. SAV.*, 1964, *14*, p. 208-215.

[Čer71] J. Černý, On directable automata, *Kybernetika*, 1971, *7*, p. 4.

[Dub96] L. Dubuc, Les automates circulaires biaisés vérifient la conjecture de Černý, *Informatique théorique et Applications*, 1996, *30*, n° 6, p. 495-505.

[Epp90] D. Eppstein, Reset sequences for monotonic automata, *SIAM J. Comput*, June 1990, *19*, 3, p. 500-510.

[Fra82] P. Frankl, An extremal problem for two families of sets, *Europ. J. Combinatorics*, 1982, p. 125-127.

[Gor92] P. Goralčík et V. Koubek, Rank problems for composite transformations, *IJAC*, 1995, *5*, n° 3, p. 309-316.

[Koh70] Z. Kohavi, *Switching and Finite Automata Theory*, McGraw-Hill, New York, 1970, p. 414-416.

[Pin77] J.-E. Pin, Sur la longueur des mots de rang donné d'un automate fini, *C. R. Acad. Sc. A*, 1977, *284*, p. 1233-1235.

[Pin78a] J.-E. Pin, *Sur un cas particulier de la conjecture de Černý*, Communication faite au 5e colloque "On automata languages and programming" 1978, Udine (Italie).

[Pin78b] J.-E. Pin, *Le problème de la synchronisation*, Contribution à l'étude de la conjecture de Černý, Thèse de 3e cycle à l'Université Pierre et Marie Curie (Paris 6), 1978.

[Pin78c] J.-E. Pin, Sur un cas particulier de la conjecture de Černý, *Proc. 5th ICALP, Lect. Notes in Comp. Sci.*, Springer Verlag, Berlin, Heidelberg, New York, 1978, *62*, p. 345-352.

[Pin78d] J.-E. Pin, Sur les mots synchronisants dans un automate fini, *Elektron. Informationsverarb. Kybernet.*, 1978, *14*, p. 293-303.

[Pin78e] J.-E. Pin, Utilisation de l'algèbre linéaire en théorie des automates, Actes du 1er Colloque AFCET-SMF de Mathématiques Appliquées, *AFCET*, 1978, p. 85-92.

[Pin81] J.-E. Pin, Le problème de la synchronisation et la conjecture de Černý, Non-commutative structures in algebra and geometric combinatorics, De Luca, A. ed., *Quaderni de la Ricerca Scientifica*, CNR, Roma, 1981, *109*, p. 37-48.

[Pin83] J.-E. Pin, On two combinatorial problems arising from automata theory, *Annals of Discrete Mathematics*, 1983, *17*, p. 535-548.

[Rys95] I. K. Rystsov, Quasioptimal bounds for the length of reset words for regular automata, *Acta Cybernetica*, 1995, *12*, n° 2, p. 145-152.

[Sav] P. Savický et S. Vaněček, *Search of synchronizing words for finite automata with aid of linear algebra*, unpublished manuscript.

[Sta66] P. H. Starke, Eine Bemerkung über homogene Experimente, *Elektron. Information-verarbeit. Kybernetik*, 1966, *2*, p. 257-259.

[Sta69] P. H. Starke, Abstrakte Automaten, VEB Deutscher Verlag der Wissenschaft, (1969), Abstract Automata, North Holland, Amsterdam, (1972).