INFORMATIQUE THÉORIQUE ET APPLICATIONS

L. DUBUC

Les automates circulaires biaisés vérifient la conjecture de Černý

Informatique théorique et applications, tome 30, n° 6 (1996), p. 495-505.

<http://www.numdam.org/item?id=ITA_1996__30_6_495_0>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 30, n° 6, 1996, pp. 495-505)

LES AUTOMATES CIRCULAIRES BIAISÉS VÉRIFIENT LA CONJECTURE DE ČERNÝ (*)

par L. DUBUC ([1])

Communiqué par C. CHOFFRUT

Abstract. – *An action $X \times A^+ \to X : (x, w) \mapsto x * w$ of the free semigroup A^+ over the alphabet A is* synchronised *by a word $w \in A^+$ if $x * w = y * w$ for all $x, y \in X$. Černý conjectured that if there is such a w and $|X| = n$, then there is one of length $\leq (n-1)^2$. The conjecture remains open, except for particular classes of actions. An action is* circular *if there is $c \in A$ acting as a circular permutation, and* biaised *if there is $b \in A$ with only one $x \in X$ such that $|x * b^{-1}| \geq 2$. We confirm here Černý conjecture for biaised circular actions.*

Résumé. – *Une action $X \times A^+ \to X : (x, w) \mapsto x * w$ du semigroupe libre A^+ sur un alphabet A est dit* synchronisé *par un mot $w \in A^+$ si $x * w = y * w$ pour tous $x, y \in X$. Černý a conjecturé, que si un tel mot existe, alors il en existe un de longueur $|w| \leq (n-1)^2$, où $n = |X|$. Cette conjecture reste ouverte, sauf pour certaines classes d'actions. Une action est dite* circulaire *s'il existe $c \in A$ agissant comme une permutation circulaire, et* biaisée *s'il existe $b \in A$ tel que $|x * b^{-1}| \geq 2$ pour un unique $x \in X$. Nous vérifions ici la conjecture de Černý pour les actions circulaires biaisées.*

1. INTRODUCTION

La conjecture de Černý traite de la longueur des *mots synchronisants*, susceptibles de ramener, aussi vite que possible, un automate déterministe 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. Bizarrement, la taille de l'alphabet, tant qu'il y a au moins deux lettres, ne semble pas jouer de rôle dans cette minimisation. Toutes les bornes supérieures connues, valables simultanément pour tous les automates synchronisants à n états, sont d'ordre cubique $O(n^3)$ [Pin 78a, Pin 78b]. Pour cette raison la borne quadratique $(n-1)^2$ conjecturée en 1964 par J. Černý [Čer 64], qui est en fait une borne inférieure exacte,

(*) Reçu le 12 mai 1995, accepté le 25 juin 1996.

([1]) LIR, Université de Rouen, pl. E. Blondel, 76821 Mont-Saint-Aignan.

Informatique théorique et Applications/Theoretical Informatics and Applications
0988-3754/96/06/$ 7.00/

est d'autant plus surprenante qu'elle a su résister jusqu'à maintenant à tous les efforts de réfutation.

Peut-être, l'une des raisons de cette résistance est la difficulté de décider s'il existe ou non, pour un automate et un entier l fournis en données, un mot synchronisant de longueur inférieure ou égale à l. En fait, ce problème a été classé par P. Goralčik et V. Koubek [Gor 92] comme NP-complet. En tout cas, la conjecture de Černý semble être très bien protégée par cette NP-complétude contre les attaques à l'aide d'ordinateur.

La borne de Černý $(n-1)^2$ est inférieurement atteinte déjà sur une classe d'automates assez restreinte que nous appelons les *automates circulaires biaisés*, où l'une des lettres agit comme une permutation circulaire et pour une autre il existe un seul état à plusieurs antécédents (*cf.* [Pin 78a, Pin 78b]). L'intérêt énorme de cette classe, par rapport à la conjecture de Černý, vient du fait que d'après Savický et Vaněček [Sav], tout automate circulaire synchronisant à n états admet un mot synchronisant de longueur inférieure ou égale à $(n-1)^2+(n-2)^2$, donc soumis à une borne quadratique et très proche de celle de Černý.

Nous nous attachons à démontrer, en nous appuyant sur ce résultat, que les automates circulaires biaisés vérifient la conjoncture de Černý. La seule autre classe non triviale pour laquelle le même résultat définitif a été connu est celle des automates circulaires dont le nombre d'états n est un entier premier (*cf.* [Pin 78a, Pin 78b]). Il nous paraît que la conjecture soit vraie pour tous les automates circulaires, mais si c'est le cas, la preuve sera assez compliquée.

2. LA MÉTHODE D'AUGMENTATION RÉCIPROQUE

Pour étudier les phénomènes de synchronisation, il suffit de considérer les automates déterministes 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 semigroupe libre A^+ sur un alphabet fini A. On va noter un tel automate par $\mathcal{A} = (X, A)$, l'action étant sous-entendue.

Étant donné un automate $\mathcal{A}$, 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

$$S * w = \{x * w | x \in S\}$$

• l'*image réciproque* de S par w

$$S * w^{-1} = \{x \in X | x * w \in S\}$$

• le *rang* de w

$$rang(w) = |X * w|$$

Tout mot w de rang 1 pour $\mathcal{A}$ est appelé un *mot synchronisant* de $\mathcal{A}$, et $\mathcal{A}$ est un *automate synchronisant* s'il admet un mot synchronisant.

CONJONCTURE 2.1 (J. Černý) : *Tout automate synchronisant $\mathcal{A}$ à n états admet un mot synchronisant $w \in A^+$ de longueur*

$$|w| \leq (n-1)^2$$

La définition et les deux propositions qui suivent sont dues à Savický et Vaněček [Sav].

DÉFINITION 2.2 : *Soient m un entier positif et $\mathcal{A} = (X, A)$ un automate. Une partie S de X est dit* réciproquement m-augmentable *(dans $\mathcal{A}$) s'il existe un mot $w \in A^+$ de longueur $|w| \leq m$ tel que $|S * w^{-1}| > |S|$. L'automate $\mathcal{A}$ est dit* réciproquement m-augmentable *si pour toute partie propre $S \subseteq X$, $\emptyset \neq S \neq X$, il existe un mot $w \in A^+$ de longueur $|w| \leq m$ tel que $|S * w^{-1}| > |S|$.*

PROPOSITION 2.3 : *Tout automate réciproquement* m-augmentable *$\mathcal{A}$ de taille n admet un mot synchronisant w de longueur $|w| \leq 1 + m(n-2)$. Par conséquent, tout automate réciproquement* n-augmentable *de taille n vérifie la conjecture de Černý.*

Un automate $\mathcal{A}$ à n états est un *automate circulaire* s'il existe $c \in A$ telle que $\{x * c^k | 0 \leq k < n\} = X$ pour tout $x \in X$.

PROPOSITION 2.4 : *Tout automate circulaire synchronisant $\mathcal{A}$ de taille n est réciproquement $2(n-1)$-augmentable et donc admet un mot synchronisant w de longueur $|w| \leq (n-1)^2 + (n-2)^2$.*

Rappelons qu'une congruence dans un automate $\mathcal{A} = (X, A)$ est une relation d'équivalence $\sim$ dans X telle que

$$\forall x, y \in X (x \sim y \Rightarrow x * w \sim y * w)$$

L'automate quotient $\mathcal{A}/\sim = (X/\sim, A)$ est alors défini par l'action

$$(x/\sim) * w = (x * w)/\sim \quad \text{pour } x \in X \qquad \text{et} \qquad w \in A^+$$

Pour toute partie $S \subseteq X$, la *congruence syntactique* σ_S de $\mathcal{A}$ associée à S, définie par

$$x \sigma_S y \Leftrightarrow \forall w \in A^* (x * w \in S \Leftrightarrow y * w \in S)$$

est la plus grossière parmi les congruences saturant S. La condition s'écrit aussi comme

$$x \sigma_S y \Leftrightarrow \forall w \in A^* (x \in S * w^{-1} \Leftrightarrow y \in S * w^{-1})$$

donc toutes les images réciproques de S sont aussi saturées par σ_S. La partie S est dite *disjonctive* si σ_S est l'égalité dans X, $\sigma_S = \Delta_X = \{(x, x) | x \in X\}$.

Un automate circulaire $\mathcal{A} = (X, A)$ est dit *biaisé* s'il existe une lettre $b \in A$ telle qu'un unique état $x_b \in X$ est réciproquement augmenté par b, $|x_b * b^{-1}| > 1$ et $|x * b^{-1}| \leq 1$ pour tout $x \neq x_b$.

Il est commode d'identifier X à l'ensemble d'entiers $\{0, 1, \ldots, n-1\}$, avec $n = |X|$, par $x_b * c^k \mapsto k$ pour $0 \leq k < n$. C'est alors l'état 0 qui a plusieurs antécédents sous l'action de b. De plus X devient, sous l'addition définie par $x + y = 0 * c^{x+y}$ un groupe cyclique $(X, +)$ sur lequel c agit comme la translation associée au générateur 1 de $(X, +), x * c = x + 1$. Une conséquence très importante par la suite en est que toute congruence $\sim$ de $\mathcal{A}$ est une congruence de $(X, +)$, donc l'équivalence modulo le sous-groupe $H = 0/\sim = \{x \in X | x \sim 0\}$ de $(X, +)$,

$$x \sim y \Leftrightarrow x - y \in H$$

Toutes les classes modulo $\sim$ étant de même taille, on a

$$|S * w^{-1}| > |S| \Leftrightarrow |(S/\sim) * w^{-1}| > |S/\sim|$$

quel que soit $S \subseteq X$ et $w \in A^+$.

LEMME 2.5 : *Soit $\mathcal{A} = (X, A)$ un automate circulaire biaisé et synchronisant à n états. Alors toute partie propre $S \subseteq X$ qui n'est pas réciproquement n-augmentable est disjonctive.*

Preuve: Supposons que $\sigma_S \neq \Delta_X$. Alors $|X/\sigma_S| \leq n/2$ (puisque toutes les σ_S-classes sont d'une même taille), donc d'après la proposition 2.4 l'automate quotient $\mathcal{A}/\sigma_S$ est réciproquement $2(\frac{n}{2} - 1)$-augmentable. Si maintenant S n'est pas réciproquement n-augmentable dans $\mathcal{A}$ alors S/σ_S n'est pas réciproquement n-augmentable dans $\mathcal{A}/\sigma_S$, une contradiction. □

Notre but sera de démontrer qu'en fait dans un automate circulaire biaisé et synchronisant à n états toute partie propre est réciproquement n-augmentable. A cette fin, nous allons établir la proposition suivante qui, avec le lemme précédent, implique cette assertion.

PROPOSITION 2.6 : *Soit $\mathcal{A} = (X, A)$ un automate circulaire biaisé et synchronisant à n états. Alors toute partie $S \subseteq X$ disjonctive est réciproquement n-augmentable.*

Le fait que toute partie propre est réciproquement n-augmentable permettra immédiatement de conclure, en vertu de la proposition 2.3, que le résultat annoncé dans le titre est vrai :

THÉORÈME 2.7 : *Tout automate circulaire biaisé et synchronisant*

$$\mathcal{A} = (X, A)$$

à n états admet un mot synchronisant $w \in A^+$ de longueur

$$|w| \leq (n-1)^2$$

Cette borne est exacte pour la classe des automates circulaires biaisés.

La clé de voûte est donc la proposition 2.6. La preuve (par l'absurde) de celle-ci fait l'objet des deux sections suivantes.

3. CONGRUENCE ENGENDRÉE PAR UN COUPLE D'ÉTATS

Soit $\mathcal{A} = (X, A)$ un automate circulaire biaisé et synchronisant où $X = \{0, 1, \ldots, n-1\}$ et $(X, +)$ le groupe cyclique tel que $x + y = 0 * c^{x+y}$ pour tout $x, y \in X$. Pour une famille d'états $\{x_i | i \in I\}$, on note par $\langle x_i | i \in I \rangle$ le sous-groupe de $(X, +)$ engendré par la famille. Comme d'habitude, on note par $[X : H]$ l'indice d'un sous-groupe H de $(X, +)$ (c'est la taille du quotient X/H).

L'équivalence $\sim_H$ modulo un sous-groupe H de $(X, +)$ est une congruence de $\mathcal{A}$ si et seulement si H vérifie la condition suivante d'*invariance* :

$$\forall w \in A^*(x - y \in H \Rightarrow x * w - y * w \in H)$$

clairement équivalente à

$$\forall a \in A(x - y \in H \Rightarrow x * a - y * a \in H)$$

Le sous-groupe H sera appelé un *groupe invariant* de $\mathcal{A}$ dans ce cas.

Evidemment, l'ensemble des sous-groupes invariants de $\mathcal{A}$ étant fermé par intersection, tout sous-groupe H de $(X,+)$ est contenu dans un plus petit sous-groupe invariant H de $(X,+)$, sa *fermeture invariante* dans $\mathcal{A}$.

PROPOSITION 3.1 : *Soit H un sous-groupe de $(X,+)$. Alors la suite de sous-groupes de $(X,+)$ définie par*

$$H_0 = H, \quad H_{r+1} = \langle y * a - x * a | y - x \in H_r,\ a \in A \rangle$$

est croissante et se stabilise à la fermeture invariante $\hat{H}$ de H.

Preuve : Parmi les générateurs de H_{r+1} on a tous les $y*c-0*c = y \in H_r$ d'où $H_r \leq H_{r+1}$. Si $H_r = H_{r+1}$ alors H_r est invariant et $H_r = H_{r+k}$ pour tout $k \geq 1$. □

Nous aurons besoin d'une meilleure description de la fermeture invariante d'un sous-groupe donné H de $(X,+)$. A cette fin, associons à toute relation binaire $\mathcal{R} \subseteq X \times X$ le *groupe différentiel* associé à $\mathcal{R}$, défini comme un sous-groupe de $(X,+)$

$$\partial\mathcal{R} = \langle y - x | x\mathcal{R}y \rangle$$

Si E est la plus petite équivalence dans X telle que $\mathcal{R} \subseteq E$, on dira que E est l'équivalence *engendrée* par $\mathcal{R}$ ou bien que $\mathcal{R}$ est un *réduit* de E.

Pour tout ensemble de mots $W \subseteq A^*$ et pour toute relation binaire $\mathcal{R} \subseteq X \times X$, on définit la relation

$$\mathcal{R} * W = \{(x,y) * w | x\mathcal{R}y,\ w \in W\}$$

où $(x,y) * w = (x * w,\ y * w)$. Pour $Y \subseteq X$, on pose

$$c^Y = \{c^k | k \in Y\}$$

LEMME 3.2 : *Si $\mathcal{R}$ est un réduit d'une équivalence E dans X alors $\partial E = \partial\mathcal{R}$ et par conséquent aussi $\partial(E * A) = \partial(\mathcal{R} * A)$.*

Preuve : On peut supposer $\mathcal{R}$ symétrique, puisque évidemment $\partial\mathcal{R} = \partial\mathcal{R}^{-1}$. L'inclusion $\partial E \supseteq \partial\mathcal{R}$ étant triviale on montre la réciproque. Si xEy alors il existe un $\mathcal{R}$-chemin $x = x_0\mathcal{R}x_1\mathcal{R}\ldots\mathcal{R}x_m = y$ et $y - x = \sum_{i=1}^{m}(x_i - x_{i-1})$, donc $y - x \in \partial\mathcal{R}$ et donc $\partial E \subseteq \partial\mathcal{R}$.

Pour la conséquence, il suffit de noter que $E * A$ et $\mathcal{R} * A$ engendrent la même équivalence. □

LEMME 3.3 : *Soit une relation $\mathcal{R} \subseteq X \times X$. Notons $q = [X : \partial\mathcal{R}]$. Alors la relation $\mathcal{R} * c^{[0,n-q[}$ engendre $\sim_{\partial\mathcal{R}}$, l'équivalence modulo $\partial\mathcal{R}$.*

Preuve : Il est clair que $\mathcal{R} * c^{[0,n-q[}$ est contenue dans $\sim_{\partial\mathcal{R}}$.

Soit $x\mathcal{R}y$. Pour tout $z \in X$, la relation $(x,y) * c^{z-x+\langle y-x\rangle}$ est un circuit sur la classe $z + \langle y-x\rangle$ modulo $\sim_{\langle y-x\rangle}$. Cette classe contient au plus un seul $t \geq n-q$, puisque $y - x \in \partial\mathcal{R} = \langle q\rangle$. En enlevant éventuellement cet exposant t on obtient $(x,y) * c^{(z-x+\langle y-x\rangle)\setminus\{t\}}$, toujours connexe sur $z + \langle y-x\rangle$, mais cette fois entièrement contenue dans $(x,y) * c^{[0,n-q[}$, qui est donc un réduit de $\sim_{\langle y-x\rangle}$.

Pour conclure, $(x,y) * c^{[0,n-q[}$ étant connexe sur toute $\sim_{\langle y-x\rangle}$-classe $z + \langle y-x\rangle$, la relation $\bigcup_{x\mathcal{R}_y}(x,y) * c^{[0,n-q[} = \mathcal{R} * c^{[0,n-q[}$ est connexe sur toute $\sim_{\partial\mathcal{R}}$-classe $z + \partial\mathcal{R}$. □

COROLLAIRE 3.4 : *Si une relation $\mathcal{R} \subseteq X \times X$ contient un réduit de l'équivalence $\sim_G$ pour un sous-groupe propre G de $\partial\mathcal{R}$, avec $[X : \partial\mathcal{R}] = q < s = [X : G]$, alors $\mathcal{R} * c^{[0,s-q[}$ engendre $\sim_G$.*

Preuve : Considérons le sous-groupe

$$\partial\mathcal{R}/G = \langle y - x + G | x\mathcal{R}y\rangle$$

d'indice $[X/G : \partial\mathcal{R}/G] = [X : \partial\mathcal{R}] = q$ du groupe X/G de taille s. Définissons une relation quotient $\mathcal{R}/G$ dans X/G par

$$(x+G)(\mathcal{R}/G)(y+G) \text{ssi } x\mathcal{R}y$$

Le groupe $\partial\mathcal{R}/G$ apparaît alors comme le groupe différentiel

$$\partial(\mathcal{R}/G) = \langle (y+G) - (x+G), (x+G)(\mathcal{R}/G)(y+G)\rangle$$

on peut appliquer le lemme 3.3 pour dire que $(\mathcal{R}/G) * c^{[0,s-q[}$ engendre $\sim_{\partial(\mathcal{R}/\mathcal{G})}$. Autrement dit, $(\mathcal{R}/G) * c^{[0,s-q[}$ est connexe sur toute $\sim_{\partial\mathcal{R}/G}$-classe $(x + \partial\mathcal{R})/G$ de X/G. Mais on a

$$(\mathcal{R}/G) * c^{[0,s-q[} = (\mathcal{R} * c^{[0,s-q[})/G$$

donc finalement, la relation $\mathcal{R}$ et donc aussi $\mathcal{R} * c^{[0,s-q[}$ étant connexe sur toute $\sim_G$-classe $x + G$, on conclut que $\mathcal{R} * c^{[0,s-q[}$ est connexe sur toute $\sim_{\partial\mathcal{R}}$-classe $x + \partial\mathcal{R}$. □

Soit maintenant un sous-groupe $H = \langle e\rangle$ de $(X,+)$, avec la suite strictement croissante d'après la proposition 3.1

$$H = H_0 < H_1 < \ldots H_{r-1} < H_r$$

jusqu'au premier indice r tel que $H_r = H_{r+1}$. Notons $q_k = [X : H_k]$ et $E_k = \sim_{H_k}$ pour $k \in [0, r]$.

Définissons les relations $\mathcal{R}_0, \mathcal{R}_1, \ldots, \mathcal{R}_r$ par la récurrence suivante :

$$\mathcal{R}_0 = \{(0, e)\}, \quad \mathcal{R}_1 = R_0 * c^{[0, n-q_0[},$$
$$\mathcal{R}_k = (\mathcal{R}_{k-1} * A) * c^{[0, q_{k-2}-q_{k-1}[} \qquad \text{pour} \quad 2 \leq k \leq r$$

A l'aide de ces relations, le premier groupe de notre suite s'écrit comme

$$H_0 = \langle e \rangle = \partial \mathcal{R}_0$$

Dans l'écriture du groupe suivant

$$H_1 = \langle y * a - x * a | x E_0 y, a \in A \rangle$$

on peut remplacer E_0, d'après le lemme 3.2, par un quelconque réduit de E_0, par exemple R_1, en vertu du lemme 3.3, donc on a

$$H_1 = \langle y * a - x * a | x \mathcal{R}_1 y, a \in A \rangle = \partial(\mathcal{R}_1 * A)$$

La relation $\mathcal{R}_1 * A$ contient un réduit $\mathcal{R}_1 * c = R_0 * c^{[0, n-q_0]}$ de E_0, donc par le corollaire 3.4 la relation $\mathcal{R}_2 = (R_1 * A) * c^{[0, q_1 - q_0[}$ est un réduit de E_1 et on a

$$H_2 = \partial(E_1 * A) = \partial(\mathcal{R}_2 * A)$$

En continuant cette récurrence et en remontant la récurrence définissant les relations $\mathcal{R}_k$ on obtient une description explicite de la fermeture invariante $\hat{H} = H_r$ de $H = \langle e \rangle$, et par ce biais donc de la congruence de $\mathcal{A}$ engendrée par le couple $(0, e)$.

PROPOSITION 3.5 : *Pour tout* $k \in [1, r]$,

$$H_k = \partial(\mathcal{R}_k * A) = \partial(0, e) * W_k$$

où

$$W_k = c^{[0, n-q_0[} A c^{[0, q_0 - q_1[} A \ldots c^{[0, q_{k-2} - q_{k-1}[} A$$

4. CONGRUENCE SYNTACTIQUE

On suppose maintenant que dans notre automate circulaire $\mathcal{A} = (X, A)$ la lettre $b \in A$ est telle que

$$|0 * b^{-1}| > 1 \qquad \text{et} \quad \forall x \in X (x \neq 0 \Rightarrow |x * b^{-1}| \leq 1)$$

Par conséquent, toute partie S réciproquement non-augmentable par b, $|S * b^{-1}| \leq |S|$, et telle que $0 \in S$ doit contenir tous les états $e \in X$ tels que $|e * b^{-1}| = 0$. Cette observation est le point de départ du raisonnement qui permettra d'établir la proposition suivante.

PROPOSITION 4.1 : *Soit $e \in X$ tel que $|e * b^{-1}| = 0$, et soient $H_k, q_k, E_k, \mathcal{R}_k, W_k$ pour $0 \leq k \leq r$ comme dans la section précédente. Alors toute partie $S \subseteq X$ de $\mathcal{A}$ réciproquement non n-augmentable est saturée par E_r, c'est-à-dire $S * c^{q_r} = S$.*

EXEMPLE 1 : *L'automate circulaire $\mathcal{A} = (\mathbf{Z}_{12}, \{\mathbf{c}, \mathbf{b}\})$ où $\mathbf{c}$ est la permutation circulaire et*

x	0	1	2	3	4	5	6	7	8	9	10	11
$x * \mathbf{b}$	3	2	5	0	9	8	7	1	11	4	10	0

est biaisé, synchronisant, $H_0 = \langle 6 \rangle$, $H_1 = \langle 1 \rangle = H_2$.

Preuve (de la proposition) : Soit S réciproquement non n-augmentable. Alors pour tout $x \in X$ on a

$$|S * c^{-x}| = |S| \geq |S * (bc^x)^{-1}| = |(S * c^{-x}) * b^{-1}|$$

donc toutes les "rotations" $S * c^{-x}$ de S sont non-augmentables par b, d'où

$$\forall x \in X (x \in S \Rightarrow 0 \in S * c^{-x} \Rightarrow e \in S * c^{-x} \Rightarrow x + e \in S)$$

Autrement dit, S est saturée par E_0, $S * c^{q_0} = S$.

Supposons qu'on a déjà démontré que $S * c^{q_{k-1}} = S$, pour un $k \in [1, r]$. Pour tout $0 \leq x < q_{k-1}$ et tout mot $w \in W_k * A$ on a

$$|wc^x| \leq (n - q_0 - 1) + (q_0 - q_1) + \ldots + (q_{k-2} - q_{k-1}) + q_{k-1} - 1 = n - 1$$

d'où

$$\forall x \in [0, q_{k-1}[(|S * c^{-x}) * w^{-1}| = |S * (wc^x)^{-1}| \leq |S|)$$

On peut enlever la restriction sur x, puisque $S * c^{q_{k-1}} = S$, donc

$$\forall x \in X (|S * c^{-x}) * w^{-1}| = |S * (wc^x)^{-1}| \leq |S|)$$

D'autre part,

$$\sum_{x \in X} |(S * c^{-x}) * w^{-1}| = |S| \cdot |X * w^{-1}| = |S| \cdot n$$

puisque tout état $y \in X$ est couvert $|S|$ fois par les rotations $S * c^{-x}$ de S par $x \in X$, d'où

$$\forall x \in X(|S * c^{-x}) * w^{-1}| = |S|)$$

La partie S est aussi réciproquement non augmentable par les mots bwc^x tels que $0 \leq x < q_{k-1}$ et $w \in W_k * A$, puisque $|bwc^x| \leq n$. Par conséquent,

$$\begin{aligned}\forall x \in [0, q_{k-1}[(&|((S * c^{-x}) * w^{-1}) * b^{-1}| \\ &= |S * (bwc^x)^{-1}| \leq |S| = |(S * c^{-x}) * w^{-1}|\end{aligned}$$

et là aussi on peut enlever la restriction sur x,

$$\forall x \in X(|((S * c^{-x}) * w^{-1}) * b^{-1}| \leq |(S * c^{-x}) * w^{-1}|)$$

Ainsi, nous avons démontré que pour tout $x \in X$ et pour tout $w \in W_k * A$, la partie $(S * c^{-x}) * w^{-1}$ n'est pas réciproquement augmentable par b. Par conséquent,

$$\forall x \in X(0 \in (S * c^{-x}) * w^{-1} \Rightarrow e \in (S * c^{-x}) * w^{-1})$$

ou encore

$$\forall x \in X(0 * w + x \in S \Rightarrow 0 * w + x \in S)$$

En posant $x = y - 0 * w$ on a finalement

$$\forall y \in X \forall w \in W_k * A(y \in S \Rightarrow y + (e * w - 0 * w) \in S)$$

d'où la conclusion que $S * c^{q_k} = S$, et cela pour tout $0 \leq k \leq r$.

S est saturée par une congruence non triviale E_r de $\mathcal{A}$, donc $\sigma_S \neq \Delta_X$ et la proposition 2.6 est démontrée par l'absurde. □

Je tiens à remercier Pavel Goralčik, mon directeur de thèse, pour son aide précieuse apportée à la préparation de cet article, ainsi que le Laboratoire d'Informatique Rouennais pour son accueil chaleureux.

RÉFÉRENCES

[Čer 64] J. Černý et K. Poznámka, Homogénnym experimenton s Konečnými automatmi. Mat. fyz. cas. SAV., 1964, *14*, p. 208-215.

[Čer 71] J. Černý, On directable automata, *Kybernetika 7*, 1971, p. 4.

[Fra 82] P. Frankl, An extremal problem for two families of sets, *Europ. J. Combinatorics*, 1982, p. 125-127.

[Gor 92] P. GORALČÍK et V. KOUBEK, Rank problems for composite transformations, à paraître dans IJAC.

[Koh 70] Z. KOHAVI, Switching and Finite Automata Theory, McGraw-Hill, New York, 1970, p. 414-416.

[Pin 77] 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.

[Pin 78a] 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).

[Pin 78b] 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.*

[Pin 78c] J. E. PIN, Sur un cas particulier de la conjoncture de Černý, Proc. 5th ICALP, Lect. Notes in Comp. Sci 62, Springer Verlag, Berlin, Heidelberg, New York, 1978, p. 345-352.

[Pin 78d] J. E. PIN, Sur les mots synchronisants dans un automate fini, *Elektron. Informationsverarb. Kybernet.*, 1978, *14*, p. 293-303.

[Pin 78e] 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.

[Pin 81] 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.

[Pin 83] J. E. PIN, On two combinatorial problems arising from automata theory, *Annals of Discrete Mathematics*, 1983, *17*, p. 535-548.

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

[Sta 66] P. H. STARKE, Eine Bemerkung über homogene Experimente, *Elektron. Information-verarbeit. Kybernetik*, 1966, *2*, p. 257-259.

[Sta 69] P. H. STARKE, Abstrakte Automaten, VEB Deutscher Verlag der Wissenschaft, 1969, Abstract Automata, North Holland, Amsterdam, 1972.