Le problème de la synchronisation et la conjecture de Černý*

Jean-Éric Pin
Institut de Programmation, CNRS et Université Paris 6 (France)

Riassunto. — *Il problema della sincronizzazione e la congettura di Černý.*

Noi diamo una panoramica sul seguende problema (detto il problema della sincronizzazione). Sia $\mathcal{A} = (Q, X)$ un automa finito. Ogni parola m in X^* definisce una funzione da Q in Q ; il *rango* di m in $\mathcal{A}$ è l'intero $\mathrm{Card}\{qm \mid q \in Q\}$. Una parola di rango 1 associa a tutti gli stati un unico stato ed è detta una parola *sincronizzante* (se una tale parola esiste l'automa stesso è detto "sincronizzante"). Sia $\mathcal{A}$ un automa con n stati. Černý ha fatto la congettura che se $\mathcal{A}$ è sincronizzante, allora esiste una parola sincronizzante di lunghezza $\leqslant (n-1)^2$. Una generalizzazione di questa congettura è che se esiste una parola di rango $\leqslant k$ in $\mathcal{A}$, allora esiste una parola cosifatta di lunghezza $\leqslant (n-k)^2$.

1 Introduction

Ainsi qu'on peut le constater en parcourant le *Science Citation Index*, le concept de synchronisation est utilisé dans de nombreux domaines des sciences exactes et il faut donc préciser le sens que nous donnons ici à ce mot.

Rappelons qu'un automate fini $\mathcal{A}$ est un triplet composé d'un ensemble Q (l'ensemble des états), d'un ensemble fini X (l'alphabet) et d'une action de chaque élément de X sur l'ensemble des états, action qui s'étend par associativité au monoïde libre X^* ; nous noterons simplement qm l'action du mot m sur l'état q. Nous dirons alors qu'un mot m est *synchronisant* dans $\mathcal{A}$ s'il existe un état q_0 tel que $qm = q_0$ pour tout élément q de Q. Si un tel mot existe, nous dirons que l'automate $\mathcal{A}$ lui-même est synchronisant.

Intuitivement, un mot synchronisant permet de se ramener à un état connu q_0 à partir de n'importe quel état de l'automate, donc de réaliser une sorte de réinitialisation. Prenons l'exemple d'un décodeur : s'il reçoit par erreur une séquence de symboles incorrecte, il sera vraisemblablement déphasé par rapport au signal transmis et le message décodé sera inutilisable. Toutefois si le décodeur est synchronisable, on peut injecter de temps à autre un mot synchronisant de façon à « resynchroniser » le décodeur. Cet exemple explique l'importance de la synchronisation en théorie du codage : pour plus de détails, nous renvoyons le lecteur à [16, 17].

L'étude des mots synchronisants s'inscrit également dans le cadre des « Gedanken Experiments » sur les automates (Moore [12]). Ce chapitre classique de la théorie des automates a été développé par de nombreux auteurs [1, 9, 26] il y a une dizaine d'années. Il demeure néanmoins plusieurs questions non résolues, dont justement le problème de la synchronisation, qui consiste à évaluer dans un automate synchronisant donné, la longueur des mots synchronisants les plus courts. Ce point de vue est dominé par la conjecture suivante, due à Černý.

*Article paru dans *Non-commutative structures in algebra and geometric combinatorics*, A. De luca (éd.), pp. 37–48, *Quaderni de la Ricerca Scientifica* vol. 109, CNR, Roma, 1981.

Conjecture C1 *Dans un automate synchronisant fini à n états, il existe un mot synchronisant de longueur inférieure ou égale à $(n-1)^2$.*

La conjecture originale de Černý concerne uniquement les automates synchronisants, mais on peut en donner une généralisation valable pour tous les automates : puiqu'un mot m définit une application de l'ensemble des états dans lui-même, nous définirons le *rang* de m (noté $r_{\mathcal{A}}(m)$) comme le cardinal de l'image de cette application (formellement, $r_{\mathcal{A}}(m) = \mathrm{Card}\{qm \mid q \in Q\}$. Ainsi les mots de rang 1 sont les mots synchronisants et on peut proposer l'énoncé :

Conjecture C2 *Si dans un automate à n états, il existe un mot de rang inférieur ou égal à k, il existe un tel mot de longueur inférieure ou égale à $(n-k)^2$.*

On ne connaît aucun contre-exemple à cette hypothèse dont la vraisemblance a été soulignée par des calculs sur ordinateur. Il nous parait d'autre part important de souligner un aspect remarquable de cette nouvelle conjecture, obtenu en intervertissant k et $n-k$ dans l'énoncé précédent :

Conjecture C3 *Si dans un automate à n états, il existe un mot de rang inférieur ou égal à $n-c$, il existe un tel mot de longueur inférieure ou égale à c^2.*

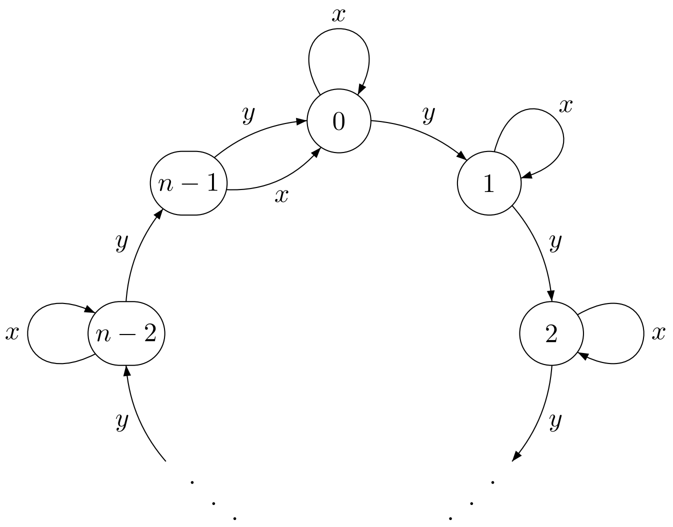
En d'autres termes, un mot de 9 lettres au plus doit suffire pour « descendre » au rang $n-3$, un mot de 16 lettres au plus doit suffire pour descendre au rang $n-4$, etc. et cela, *indépendamment du nombre d'états de l'automate.*

Le but de cet article est d'exposer les résultats obtenus jusqu'ici sur ces questions en insistant particulièrement sur les diverses méthodes utilisées.

Nous aurons besoin dans la suite de quelques notations. Soit $\mathcal{A} = (Q, X, \delta)$ un automate fini où Q est l'ensemble des états, X est l'alphabet et δ la fonction de transition. On notera qm l'action d'un mot m de X^* sur l'état q et, si S est un sous-ensemble de Q, Sm l'ensemble $\{qm \mid q \in S\}$. De même, on notera qm^{-1} l'ensemble $\{q' \mid q'm = q\}$ et Sm^{-1} l'ensemble $\{q \mid qm \in S\}$. $|K|$ désignera le cardinal de l'ensemble K et, si m est un mot de X^*, $|m|$ désignera la longueur de m, le contexte évitant toute confusion entre ces deux notations. Le rang de m dans $\mathcal{A}$ est noté $r_{\mathcal{A}}(m) = |\{qm \mid q \in Q\}| = |Qm|$.

2 L'optimalité des bornes $(n-1)^2$ et $(n-k)^2$.

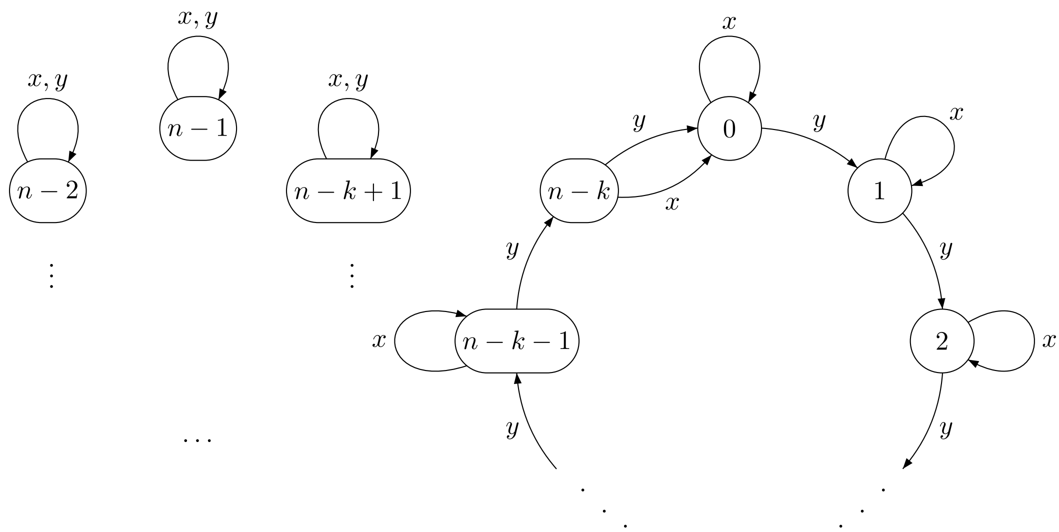
Černý [2] a dès l'abord démonté l'optimalité de la borne $(n-1)^2$ en considérant les automates suivants.
$\mathcal{A}_n = (Q, X, \delta)$ où $Q = \{0, 1, \ldots, n-1\}$, $X = \{x, y\}$, $ix = i$ et $iy = i+1$ si $i \neq n-1$, $(n-1)x = (n-1)y = 0$. $\mathcal{A}_n$ peut être représenté par le diagramme



On voit alors que le mot $(xy^{n-1})^{n-2}$ est synchronisant de longueur $(n-1)^2$. On peut en fait montrer que ce mot synchronisant est le plus court que l'on puisse trouver.

En modifiant légèrement l'automate précédent, on peut aussi démontrer l'optimalité de la borne $(n-k)^2$. Soit $Q = \{0, 1, \ldots, n-1\}$ et $K = \{0, \ldots, n-k\}$ et considérons l'automate $\mathcal{A}_{n,k} = (Q, X, \delta)$ où $ix = iy = i$ si $i \in Q \setminus K$, $ix = i$, $iy = i+1$ si $i \in \{0, 1, \ldots, n-k-1\}$, $(n-k)x = (n-k)y = 0$.

$\mathcal{A}_{n,k}$ est représenté par le diagramme



Comme x et y laissent fixe tout état de $Q \setminus K$ et que le sous-automate $\mathcal{A}_K = (K, X, \delta_K)$ est isomorphe à $\mathcal{A}_{n-k+1}$, tout mot de rang inférieur ou égal à k dans $\mathcal{A}_{n,k}$ est en fait de rang k exactement et synchronise $\mathcal{A}_K$. Puisque $\mathcal{A}_K$ est isomorphe à $\mathcal{A}_{n-k+1}$, sa longueur est minorée par $(n-k)^2$.

3 La méthode d'analyse descendante et ses conséquences

Cette méthode, inaugurée par Starke [25] est la méthode qui semble la plus naturelle et c'est aussi celle qui a été le plus fréquemment utilisée. Elle conduit à des problèmes de nature combinatoire qui ne sont d'ailleurs pas entièrement résolus (cf. [19, chapitres 7 et 8].

Le principe est extrèmement simple : considérons un automate $\mathcal{A} = (K, X, \delta)$ à n états et recherchons un mot de rang au plus k dans $\mathcal{A}$. Nous chercherons tout d'abord une lettre x de rang différent de n et nous poserons $K_1 = Qx$. L'ensemble K_1 vérifiera donc $|K_1| < n$. Si K_1 a moins de k éléments, c'est terminé ; sinon, on cherchera un mot m_1 de longueur minimale tel que l'ensemble $K_2 = K_1m_1$ vérifie $|K_2| < |K_1|$. Si $|K_2| \leqslant k$, c'est terminé. Sinon, on applique le même procédé à K_2, etc. jusqu'à ce qu'un des K_i vérifie $|K_i| \leqslant k$, ce que nous résumerons par un schéma

$$Q \xrightarrow{x} K_1 \xrightarrow{m_1} K_2 \xrightarrow{m_2} \cdots\ K_{r-1} \xrightarrow{m_{r-1}} K_r \quad \text{avec } |K_r| \leqslant k.$$

Le mot $xm_1 \cdots m_{r-1}$ est alors au plus de rang k. Comme on le voit, la méthode d'analyse descendante se ramène pour l'essentiel à la résolution du problème suivant :

Problème 1 *Déterminer un entier $p(n,k)$ tel que pour tout automate $\mathcal{A}$ à n états et pour toute partie K à k éléments de l'ensemble des états de $\mathcal{A}$, $p(n,k)$ majore la longueur du plus petit mot (s'il existe) tel que $|Km| < |K|$.*

Bien que ce problème n'ait jamais été formulé pour lui-même, on s'aperçoit qu'il a été étudié par tous les auteurs ayant travaillé sur le problème de la synchronisation. Ainsi, diverses majorations de $p(n,k)$ ont été obtenues, notamment :

$$p(n,k) \leqslant \binom{n}{2} \qquad \text{Starke [25]}$$

$$p(n,k) \leqslant \binom{n}{2} - \binom{k}{2} - k + 3 \qquad \text{Černý, Pirická et Rosenauerova [4]}$$

$$p(n,n) = 0,\ p(n,n-1) = 3 \text{ et, si } k \leqslant n-2,$$

$$p(n,k) \leqslant (n-k)^2 - (n-k) + 4 \qquad \text{Pin [19]}$$

$$p(n,k) \leqslant \binom{n}{2} - a\left[\binom{k}{2} - 1\right] - \max\left(r(k-r) + \binom{r}{2} - 1, 0\right) \qquad \text{Pin [19]}$$

où a et r sont respectivement le quotient et le reste de la division de n par k.

Une amélioration des méthodes développées en [19] semble pouvoir conduire à la majoration $p(n,k) \leqslant \binom{n-k+2}{2}$, mais cet énoncé est encore à l'état de conjecture.

Mais revenons à l'étude de la méthode. Comme on choisit à chaque étape un mot m_i de longueur minimale, on pourrait espérer que le mot $xm_1 \cdots m_{r-1}$ finalement obtenu soit un mot de rang $\leqslant k$ de longueur minimale. En fait, il n'en est rien, comme le montre l'exemple suivant. Considérons l'automate $\mathcal{A}_4$ décrit au paragraphe précédent et cherchons un mot synchronisant par l'analyse descendante. On constate successivement que x est la seule lettre de rang différent de 4 et que $Qx = K_1 = \{0, 1, 2\}$, puis que $m_1 = yyx$ est le mot le plus court vérifiant $|K_1m_1| \leqslant 2$. On pose donc $K_2 = K_1yyx = \{1, 3\}$ et on voit alors que $yxyyyx$ est le mot m_2 le plus court tel que $|K_2m_2| = 1$. Le mot $xm_1m_2 = xyyxyxyyyx$ est effectivement synchronisant, mais sa longueur est 10 alors qu'il existe comme on l'a vu un mot synchronisant de longueur 9...

Cet exemple et quelques autres que l'on pourra trouver en [19, chapitre 3] illustrent assez bien les difficultés que l'on rencontre lorsqu'on cherche à résoudre la conjecture généralisée (version (3)) pour $c = 3$. La méthode précédente ne suffit plus, et on doit avoir recours à des arguments combinatoires passablement compliqués.

Malgré ses imperfections, la méthode d'analyse descendante permet cependant d'aboutir à des résultats substantiels. Pour la conjecture C1, on a obtenu successivement les majorations suivantes :

$2^n - n - 1$	(Černý [2] 1964)
$\frac{1}{2}n^3 - \frac{3}{2}n^2 + n + 1$	(Starke [25, 26] 1966)
$\frac{1}{2}n^3 - n^2 + \frac{n}{2}$	(Kohavi [9] 1970)
$\frac{1}{3}n^3 - n^2 - \frac{1}{3}n + 6$	(Paterson, communication personnelle à Kfoury [8] 1970)
$\frac{1}{3}n^3 - \frac{3}{2}n^2 + \frac{25}{6}n - 4$	(Černý, Pirická et Rosenauerova [4] 1971)
$\frac{7}{27}n^3 - \frac{17}{18}n^2 + \frac{17}{6}n - 3$	pour n multiple de 3 (Pin [20] 1977)
$(\frac{1}{2} - \frac{\pi^2}{36})n^3 + o(n^3)$	(Pin [19] 1978)

Pour la conjecture C3, la meilleure borne est

$\frac{1}{3}c^3 - c^2 + \frac{14}{3}c - 5$	(Pin [19] 1978)

(En fait on connait des bornes un peu meilleures pour $\binom{n}{2} \leqslant c \leqslant n-1$, mais leur expression est trop compliquée pour être reproduite ici. On trouvera la valeur de ces bornes pour $n \leqslant 12$ en [19, p.117]).

4 La méthode d'analyse ascendante

Dans la méthode descendante, on cherchait à faire descendre le rang de n à k. La méthode ascendante utilise un procédé inverse puisqu'on cherche à augmenter le rang de k jusqu'à n.

On commence par chercher un ensemble K à k éléments et une lettre x telle que $|Kx^{-1}| > |K|$. Posant alors $K_1 = Kx^{-1}$, on cherche alors un mot m_1 de longueur minimale tel que l'ensemble $K_2 = K_1 m_1^{-1}$ vérifie $|K_2| > |K_1|$, puis on applique le même procédé à K_2 etc. jusqu'à ce que l'un des K_i soit égal à l'ensemble Q de tous les états, ce que nous résumerons par le schéma suivant :

$$K \xrightarrow{x^{-1}} K_1 \xrightarrow{m_1^{-1}} K_2 \xrightarrow{m_2^{-1}} K_3 \;\cdots\; K_{r-1} \xrightarrow{m_{r-1}} K_r = Q$$

On constate alors que le mot $m_{r-1}m_{r-2}\cdots m_1 x$ est de rang $\leqslant k$. A priori cette méthode peut sembler aussi valable que la précédente, mais en réalité il y a une différence fondamentale. Prenons le cas d'un automate synchronisant. Si l'analyse descendante permettait dans tous les cas de trouver un mot synchronisant, l'analyse ascendante peut en revanche échouer comme le montre l'exemple suivant :

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

avec $Q = \{1,2,3,4,5\}$, $X = \{x\}$, $1x = 5x = 5$, $2x = 3x = 4x = 1$.

Le mot x^2 est synchronisant. Mais si on applique l'analyse ascendante à partir de $\{1\}$, on trouve

$$1x^{-1} = \{2,3,4\} \text{ mais } \{2,3,4\} = \emptyset$$

(En fait, il aurait fallu partir de $\{5\}$).

Ce phénomène s'explique par le fait suivant : si K est une partie de l'ensemble des états et x une lettre, on a $|Kx| \leqslant |K|$ (le rang décroit) mais par contre on ne peut comparer les entiers $|Kx^{-1}|$ et $|K|$.

Si l'analyse ascendante s'avère inefficace dans le cas général, elle conduit cependant à des majorations beaucoup plus précises pour une classe particulière d'automates, les automates fortement transitifs, dont voici la définition.

Definition. Soit $\mathcal{A} = (Q, X, \delta)$ un automate à n états et Y la partie de X formée des lettres de rang n (ce sont donc les lettres dont l'action est une bijection de Q sur Q). Si Y^* opère transitivement sur Q (c'est-à-dire si pour tout $q_1, q_2 \in Q$, il existe $m \in Y^*$ tel que $q_1 m = q_2 m$), on dit que $\mathcal{A}$ est fortement transitif.

On a alors le

Théorème 1 *Soit $\mathcal{A} = (Q, X, \delta)$ un automate fortement transitif à n états, avec $Q = \{1, 2, \ldots, n\}$. On suppose qu'il existe une lettre x dont l'équivalence d'application soit $1, 2, \ldots, c{+}1 \,/\, c{+}2 \,/\, c{+}3 \,/ \ldots /\, n$ (i.e. telle que $1x = 2x = \ldots = (c{+}1)x$ et $r_{\mathcal{A}} = n{-}c$) avec $c \geqslant 1$. Alors, pour tout entier k tel que $\frac{n-1}{2} \leqslant k \leqslant n$, il existe un mot de rang $\leqslant k$ et de longueur $\leqslant (n-k)^2 - (n-k-1)(c-1)$ (et donc a fortiori de longueur $\leqslant (n-k)^2$).*

Il est à remarquer que pour $c \geqslant 2$, ce théorème donne une *meilleure* borne que la borne conjecturée $(n-k)^2$. On notera d'autre part que, contrairement aux énoncés précédents, on ne suppose pas *a priori* l'existence d'un mot de rang $\leqslant k$ mais on *démontre* l'existence d'un tel mot.

5 Méthodes d'algèbre linéaire

Le principe n'est pas nouveau et a déjà été utilisé avec succès en théorie des automates (voir par exemple les articles de Schützenberger [23] et de Perrin [15, 16] ou le livre d'Eilenberg [6, p. 145]).

L'idée de base est qu'un automate $\mathcal{A} = (Q, X, \delta)$ opère sur le $\mathbb{R}$-espace vectoriel $\mathbb{R}^Q$ formé des combinaisons linéaires formelles de ses états. Un mot m de X^* apparait alors comme un endomorphisme de $\mathbb{R}^Q$ et on peut lui associer une matrice $\mu(m)$. On constate alors sans peine que $\mu(uv) = \mu(u)\mu(v)$ et que le rang de la matrice $\mu(m)$ est précisément égal au rang de m dans $\mathcal{A}$.

Une première idée, sur laquelle nous reviendrons, consiste à essayer de formuler, puis à résoudre, une « conjecture de Černý » pour les matrices. En fait, comme nous le verrons plus loin, le problème est en général sans solution et on doit se contenter du résultat partiel suivant :

Théorème 2 *Soit $\mathcal{A} = (Q, X, \delta)$ un automate à n états tel que les matrices $\{\mu(x) \mid x \in X\}$ soient simultanément triangulables dans $\mathbb{C}$. Alors, s'il existe un mot de rang $\leqslant k$ dans $\mathcal{A}$, il existe un tel mot de longueur $\leqslant (n-k)^2$.*

La seconde méthode utilisant l'algèbre linéaire a été exposée en détail en [22] (ou en [19, chap. 2]). Nous nous contenterons ici d'en rappeler les principales conséquences pour le problème de la synchronisation en signalant toutefois qu'elle permet de retrouver les résultats classiques de Moore [12] en théorie des automates.

Les énoncés qui suivent reposent sur la

Proposition 1 *Soit $\mathcal{A}$ un automate à n états et w un mot de rang au plus r dans $\mathcal{A}$. S'il existe un mot de rang $\leqslant r-1$ dans $\mathcal{A}$, il existe un tel mot de longueur $\leqslant 2|w| + n - r + 1$.*

Le cas particulier où w est une lettre mérite qu'on s'y arrête.

Théorème 3 *Soit $\mathcal{A} = (Q, X, \delta)$ un automate à n états dont une lettre est de rang $r < n$. S'il existe un mot de rang $\leqslant r-1$, il existe un tel mot de longueur $\leqslant n-r+3$. Cette borne est optimale.*

On constate que cet énoncé permet de résoudre d'une part la conjecture C2 — dans un cas bien particulier il est vrai — mais également le problème 1, et c'est d'ailleurs l'un des rares cas où l'on sache le résoudre complètement.

En partant du théorème 3 et en appliquant la méthode d'analyse descendante, on aboutit aux résultats suivants :

Théorème 4 *Dans un automate synchronisant à 5 états dont une lettre est de rang $\leqslant 3$, il existe un mot synchronisant de longueur $\leqslant 14$. (N.B. La borne optimale est sans doute 12, mais le problème reste ouvert).*

Théorème 5 *Dans un automate synchronisant à n états possédant une lettre de rang $\leqslant 1 + \log_2 n$, il existe un mot synchronisant de longueur $\leqslant (n-1)^2$.*

6 Une autre méthode algébrique

Nous ferons ici appel aux polynômes à coefficients dans $\mathbb{Z}$ pour étudier une classe particulière d'automates, les automates circulaires. On dit qu'un automate $\mathcal{A} = (Q, X, \delta)$ est *circulaire* s'il existe une lettre (que nous noterons toujours y) qui induit une permutation circulaire sur l'ensemble des états. La classe des automates circulaires est donc une sous-classe de la classe des automates fortement transitifs décrits au paragraphe précédent. On peut également remarquer que les automates $\mathcal{A}_n$ (cf. section 2) sont circulaires.

L'énoncé qui suit va permettre une étude algébrique de la méthode d'analyse ascendante.

Proposition 2 *Soit $\mathcal{A} = (Q, X, \delta)$ un automate circulaire à n états dont une lettre x n'est pas de rang n et soit K une partie non vide $Q = \{0, 1, \dots, n-1\}$. On supposera que la lettre y induit la permutation $(0, 1, \dots, n-1)$ sur Q. Si les polynômes $X^K = \sum_{x \in K} X^k$ et $X^Q = \sum_{x \in Q} X^q$ sont premiers entre eux dans $\mathbb{Z}[X]$, alors il existe un entier $r \leqslant n-1$ tel que $|K(xy^r)^{-1}| > |K|$.*

Si le nombre d'états est *premier*, le polynôme $X^Q = 1 + X + \cdots X^{n-1}$ est irréductible dans $\mathbb{Z}[X]$ et tout polynôme $X^Q = 1 + X + \ldots + X^{n-1}$ est irréductible dans $\mathbb{Z}[X]$ et tout polynôme X^K avec $K \neq \emptyset, Q$ est premier avec X^Q, ce qui permet une application répétée de la proposition précédente. Par analyse descendante, on obtient le

Théorème 6 *Dans un automate circulaire à n états (n premier) dont une lettre x n'est pas de rang n, il existe un mot synchronisant de longueur inférieure ou égale à $(n-1)^2$.*

En utilisant simultanément le théorème 1, on obtient le

Théorème 7 *Soit $\mathcal{A} = (Q, X, \delta)$ un automate circulaire à n états avec n premier. On suppose qu'il existe une lettre x de rang $n - c \neq n$ et vérifiant $|sx^{-1}| = c + 1$ pour un état s de Q. Alors, pour tout entier k tel que $1 \leqslant k \leqslant n$, il existe un mot de rang $\leqslant k$ et de longueur $\leqslant (n-k)^2$.*

Le théorème 6 démontre la conjecture (C1) pour les automates circulaires dont le nombre d'états est premier. On sait d'autre part que la borne $(n-1)^2$ est optimale puisqu'elle est atteinte par les automates $\mathcal{A}_n$ (qui sont effectivement des automates circulaires comme nous l'avons dit), mais on peut se demander si ce sont les seuls automates à atteindre cette borne. La réponse est oui, à peu de choses près, pour $n \geqslant 5$ premier :

Théorème 8 *Dans un automate circulaire $\mathcal{A} = (Q, X, \delta)$ à n états (n premier) dont une lettre x n'est pas de rang n, il existe un mot synchronisant de longueur inférieure ou égale à $(n-1)^2$. Si la borne $(n-1)^2$ est optimale et si $n \geqslant 5$, l'automate $\mathcal{A}_n$ s'obtient à partir de $\mathcal{A}$ en identifiant les lettres qui ont la même action sur Q et en supprimant celles qui induisent l'identité.*

7 Extensions et réductions du problème de la synchronisation

En guise de conclusion, nous allons essayer de replacer le problème de la synchronisation dans un contexte aussi général que possible. Parallèlement nous montrerons comment ramener l'étude générale de la conjecture au cas des automates transitifs. Commençons par une définition :

Nous appellerons *automate non complètement spécifié* un triplet $\mathcal{A} = (Q, X, \delta)$ où Q est l'ensemble des états, X l'alphabet et où la fonction de transition δ définit une action *partielle* des éléments de X sur Q (autrement dit δ est une application d'une partie de $Q \times X$ vers Q). La notion de rang est définie de la même façon que pour les automates et on peut énoncer une conjecture analogue à (C2) :

Conjecture C4 *Si dans un automate non complètement spécifié à n états, il existe un mot de rang inférieur $\leqslant k$, il existe un tel mot de longueur $\leqslant (n-k)^2$.*

En fait cette généralisation n'est qu'apparente, en vertu du

Théorème 9 *Les conjectures (C2) et (C4) sont équivalentes.*

Une autre extension à laquelle nous avons déjà fait allusion concerne les automates probabilistes, dont nous ne redonnerons pas ici la définition précise : il nous suffira de savoir que l'on dispose d'un morphisme de monoïde μ de X^* dans un monoïde de matrices $n \times n$ à coefficients dans $\mathbb{Q}$ (ou dans un corps K quelconque si on veut encore généraliser). Le rang d'un mot m se définit alors comme le rang de la matrice $\mu(m)$ et un mot synchronisant est un mot de rang $\leqslant 1$.

Malheureusement, Kfoury [8] a prouvé, en s'appuyant sur un résultat de Paterson [13], que pour $n \geqslant 4$, la question de savoir si un automate probabiliste à n états était synchronisant ou pas était un problème récursivement indécidable, ce qui exclut la possibilité d'envisager une conjecture de Černý pour ce type d'automates.

Cependant on peut songer à étudier de façon analogue certains semigroupes engendrés par un nombre fini de matrices à coefficients dans un corps puisqu'on sait, depuis les travaux de Jacob [7], que la finitude d'un tel semigroupe est décidable. Un autre cas intéressant où interviennent les matrices est celui des "monoïdes de relations".

On peut en effet associer à toute relation R sur l'ensemble $E = \{1, 2, \ldots, n\}$ une matrice d'incidence $\mu(R)$ définie par

$$(\mu(R))_{i,j} = \begin{cases} 1 & \text{si } i \mathrel{R} j \\ 0 & \text{sinon.} \end{cases}$$

Si R et S sont deux relations, la matrice $\mu(RS)$ est égale au produit booléen des matrices $\mu(R)$ et $\mu(S)$. Si J désigne la relation universelle, sa matrice $\mu(J)$ est la matrice dont tous les coefficients sont égaux à 1.

Il existe à propos des matrices de relations un problème bien connu qui semble être dû à Wielandt [27]. Soit R une relation dont l'une des puissances R^k est égale à J. Montrer que l'on peut choisir k inférieur ou égal à $(n-1)^2 + 1$ (la borne $(n-1)^2 + 1$ est optimale, cf. Wielandt [27]).

Ce problème a été résolu par de nombreux auteurs. La meilleure démonstration nous paraît être celle de Perkins [14], mais le lecteur désireux d'avoir une bibliographie plus complète sur la question pourra consulter les articles de Markowsky [11] et de Dulmage et Mendelsohn [5]. Quoi qu'il en soit, l'analogie avec la conjecture de Černý est frappante et nous conduit à proposer le problème plus général suivant :

Soient $R_1, \ldots, R_p$ des relations sur l'ensemble $R = \{1, \ldots, n\}$. Ces relations engendrent un certain monoïde de relations M. Si la relation J est dans M, J s'écrit comme produit de relations prises parmi les $R_1, \ldots, R_p$. Considérons alors un produit ayant le moins de facteurs possibles :

$$J = R_{\sigma(1)} R_{\sigma(2)} \cdots R_{\sigma(m)}$$

où σ est une application de $\{1, \ldots, m\}$ dans $\{1, \ldots, p\}$.

Problème 2 *Montrer qu'il existe un entier $K(n)$ ne dépendant que de n tel que $m \leqslant k(n)$. Déterminer la meilleure valeur pour $K(n)$.*

On montre très facilment que $K(n)$ existe, et avec un peu d'optimisme, on peut toujours espérer que $K(n)$ est un polynôme du second degré en n...

Pour finir nous allons maintenant montrer comment restreindre le problème de la synchronisation grâce au résultat suivant :

Proposition 3 *Soit $\mathcal{A}$ un automate, $\mathcal{A}_2$ un sous-automate de $\mathcal{A}$ et $\mathcal{A}_1$ l'automate quotient $\mathcal{A}/\mathcal{A}_2$. Si la conjecture (C1) — resp. (C2) — est vérifiée par $\mathcal{A}_1$ et $\mathcal{A}_2$, elle est vérifiée pour $\mathcal{A}$.*

On en déduit alors sans trop de difficultés le résultat annoncé plus haut (rappelons à ce sujet qu'un automate $\mathcal{A} = (Q, X, \delta)$ est transitif si pour tout $q_1, q_2 \in Q$, il existe $m \in X^*$ tel que $q_1 m = q_2$).

Théorème 10 *Si la conjecture (C1) — resp. (C2) — est vraie pour tous les automates transitifs, elle est vraie pour tous les automates.*

Références

[1] T. Booth, *Sequential Machines and Automata Theory*, John Wiley and Sons, Inc., New-York, 1967.

[2] J. Černý, Poznámka k. homogénnym experimentom s konecnými automatmi, *Mat. fyz. čas SAV* **14** (1964), 208–215.

[3] J. Černý, Communication, in *Bratislava Conference on Cybernetics*, 1969.

[4] J. Černý, A. Pirická and B. Rosenauerova, On directable automata, *Kybernetica* **7** (1971), 289–298.

[5] A. L. Dulmage and N. S. Mendelsohn, Graphs and matrices, in *Graph Theory and Theoretical Physics*, pp. 167–227. (loose errata), Academic Press, London, 1967.

[6] S. Eilenberg, *Automata, languages, and machines. Vol. A*, Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], New York, 1974. Pure and Applied Mathematics, Vol. 58.

[7] G. Jacob, Un algorithme calculant le cardinal, fini ou infini, des demi-groupes de matrices, *Theoret. Comput. Sci.* **5**,2 (1977/78), 183–204.

[8] D. Kfoury, Synchronizing Sequences for Probabilistic Automata, *Stud. Appl. Math.* **49** (1970), 101–103.

[9] Z. Kohavi, *Switching and finite automata theory*, McGraw Hill, New-York, 1970.

[10] Z. Kohavi and J. Winograd, Establishing Certain Bounds Concerning Finite Automata., *J. Comput. Syst. Sci.* **7**,3 (1973), 288–299.

[11] G. Markowsky, Bounds on the index and period of a binary relation on a finite set, *Semigroup Forum* **13**,3 (1976/77), 253–259.

[12] E. F. Moore, Gedanken-experiments on sequential machines, in *Automata studies*, pp. 129–153, *Annals of mathematics studies, no. 34*, Princeton University Press, Princeton, N. J., 1956.

[13] M. S. Paterson, Unsolvability in 3×3 matrices, *Studies in Appl. Math.* **49** (1970), 105–107.

[14] P. Perkins, A theorem on regular matrices, *Pacific J. Math.* **11** (1961), 1529–1533.

[15] D. Perrin, The Characteristic Polynomial of a Finite Automaton., in *MFCS*, pp. 453–457, 1976.

[16] D. Perrin, Codes asynchrones, *Bull. Soc. Math. France* **105**,4 (1977), 385–404.

[17] J.-F. Perrot, Informatique et algèbre : la théorie des codes à longueur variable, in *Theoretical computer science (Third GI Conf., Darmstadt, 1977)*, pp. 27–44. Lecture Notes in Comput. Sci., Vol. 48, Springer, Berlin, 1977.

[18] J.-E. Pin, Sur la longueur des mots de rang donné d'un automate fini, *C. R. Acad. Sci. Paris Sér. A-B* **284** (1977), 1233–1235.

[19] J.-E. Pin, *Le problème de la synchronisation et la conjecture de Černý*, Thèse de 3ème cycle, Université Paris VI, 1978.

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

[21] J.-E. Pin, Sur un cas particulier de la conjecture de Černý, in *5th ICALP*, Berlin, 1978, pp. 345–352, *LNCS* n° 62, Springer.

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

[23] M.-P. Schützenberger, Sur certains sous-monoïdes libres, *Bull. Soc. Math. France* **93** (1965), 209–223.

[24] M.-P. Schützenberger, On synchronizing prefix codes, *Information and Control* **11** (1967), 396–401.

[25] P. H. Starke, Eine Bemerkung über homogene Experimente., *Elektr. Informationverarbeitung und Kyb.* **2** (1966), 257–259.

[26] P. H. Starke, *Abstrakte Automaten*, V.E.B. Deutscher Verlag der Wissenschaften, Berlin, 1969.

[27] H. Wielandt, Unzerlegbare, nicht negative Matrizen, *Math. Z.* **52** (1950), 642–648.