Sur un cas particulier de la conjecture de Černý*

Jean-Éric Pin
Institut de Programmation, CNRS et Université Paris 6
2 Place Jussieu, 75221 Paris Cedex 05, France

Abstract. Let $\mathcal{A}$ be a finite automaton. We are concerned with the minimal length of the words that send all states on a unique state (synchronizing words). J. Černý has conjectured that, if there exists a synchronizing word in $\mathcal{A}$, then there exists such a word with length $\leqslant (n-1)^2$ where n is the number of states of $\mathcal{A}$. As a generalization, we conjecture that, if there exists a word of rank $\leqslant k$ in $\mathcal{A}$, there exists such a word with length $\leqslant (n-k)^2$.
In this paper we deal only with automata in which a letter induces a circular permutation and prove the following results :

(1) the second conjecture is true for $\frac{n-1}{2} \leqslant k \leqslant n$,
(2) if n is prime, the first conjecture is true,
(3) if n is prime and if there exists a letter of rank $(n-1)$, the second conjecture is true.

1 Présentation des résultats

Dans son célèbre article « Gedanken Experiments » [9], Moore étudiait les automates (finis) du point de vue « expérimental », en s'attachant à élucider la structure interne de l'automate à partir d'expérimentations extérieures. Ce point de vue a été développé par de nombreux auteurs et constitue désormais un chapitre important de la théorie des automates : on pourra consulter à ce sujet les traités de Booth [1], Kohavi [6], ou Starke [18]. Parmi les questions non encore résolues dans ce domaine, l'une des plus attirantes demeure le problème de la synchronisation. Il est souvent utile, avant d'effectuer des contrôles sur une machine, de l'amener, à partir d'un état inconnu, à un état connu q_0. Lorsque ce résultat peut être obtenu à l'aide d'un seul mot (input sequence), on dit que la machine est synchronisable. Prenons l'exemple d'un décodeur : s'il reçoit par erreur une séquence incorrecte de symboles, il sera vraisemblablement déphasé par rapport au signal transmis et le message décodé sera inutilisable. En revanche, si le décodeur est synchronisable, on peut injecter de temps à autre un mot synchronisant de façon à resynchroniser le décodeur.

Pour suivre le plan de l'article de Moore déjà cité, on peut distinguer deux problèmes relatifs à la synchronisation : le premier, de nature qualitative, consiste à caractériser les automates finis synchronisants. Cette question a surtout été abordée du point de vue de la théorie des codes, mais est encore loin d'être résolue. On pourra consulter les articles de Perrin [10] et de Perrot [12] pour un exposé et une bibliographie plus complète. Le second problème, de nature quantitative, consiste à évaluer, dans un automate fini donné, la longueur des mots synchronisants les plus courts. C'est à ce problème que nous nous sommes particulièrement attachés. Černý [3] a en effet conjecturé le résultat suivant

*Article paru dans *5th ICALP*, Berlin, 1978, pp. 345–352, *LNCS* 62, Springer.

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

Plus généralement, puisqu'un mot m définit une application de l'ensemble des états dans lui-même, on peut définir le *rang* de m comme le le cardinal de l'image de cette application. Ainsi les mots de rang 1 sont les mots synchronisants et on peut formuler une généralisation assez naturelle de la conjecture de Černý :

Conjecture 2 *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 possède que des résultats partiels sur ces deux conjectures. Pour la conjecture de Černý (1), diverses bornes ont été proposées :

$2^n - n - 1$	(1964, Černý [2])
$\frac{1}{2}n^3 - \frac{3}{2}n^2 + n + 1$	(1966, Starke [17, 18])
$\frac{1}{2}n^3 - n^2 + \frac{n}{2}$	(1970, Kohavi [6])
$\frac{1}{3}n^3 - n^2 - \frac{1}{3}n + 6$	(1970 Paterson, communication personnelle à D.J. Kfoury [5])
$\frac{1}{3}n^3 - \frac{3}{2}n^2 + \frac{25}{6}n - 4$	(1971, Černý, Pirická et Rosenauerova [4])
$\frac{7}{27}n^3 - \frac{17}{18}n^2 + \frac{17}{6}n - 3$	pour n multiple de 3 (1977, Pin [15])

De plus, la conjecture (1) a été démontrée en [4] pour $1 \leqslant n \leqslant 5$. En 1971, Kohavi et Winograd [7] ont proposé la borne $\frac{1}{6}(n^3 - n)$, mais leur démonstration semble présenter une lacune. Pour la conjecture généralisée (2), la meilleure borne connue est :

$$\frac{1}{3}(n-k)^3 - \frac{1}{2}(n-k)^2 + \frac{13}{6}(n-k) - 1 \qquad \text{(1977, Pin [15])}$$

On pourra trouver d'autres résultats dans [13, 15, 14].

Le but du présent travail est d'étudier la conjecture de Černý et sa généralisation pour un type particulier d'automates, ceux pour lesquels une lettre induit une permutation circulaire sur l'ensemble des états. Ce type d'automate joue un rôle important en théorie des codes préfixes. En particulier, l'automate minimal d'un code préfixe dont le groupe des unités est non trivial est de cette forme (cf. Perrin et Schützenberger [11]) et on connait pour ces automates des conditions suffisantes de synchronisation (voir Perrin [10] et Schützenberger [16]) : autrement dit, on a dans ce cas particulier quelques renseignements sur le problème « qualitatif » évoqué plus haut. De plus, Černý [2] a montré, précisément à l'aide d'automates de ce type, que la borne $(n-1)^2$ était optimale pour la conjecture (1).

Afin de simplifier l'énoncé de nos résultats, nous appelerons *automate circulaire* un automate dans lequel une lettre induit une permutation circulaire sur l'ensemble des états. On a alors le

Théorème 1 *Si dans un automate circulaire à n états, il existe un mot de rang inférieur ou égal à k avec $\frac{n-1}{2} \leqslant k \leqslant n$, alors il existe un tel mot de longueur inférieure ou égale à $(n-k)^2$.*

Autrement dit, (2) est vérifiée dans le cas des automates circulaires pour $\frac{n-1}{2} \leqslant k \leqslant n$, mais la démonstration ne s'étend malheureusement pas aux autres valeurs de k. Cependant, si on se restreint au cas où n est premier, on sait (Perrin [10]) que l'automate est soit un groupe, soit synchronisant et on peut alors démontrer (1).

Théorème 2 *Dans un automate circulaire à n états (n premier) qui n'est pas un groupe, il existe un mot synchronisant de longueur inférieure ou égale à $(n-1)^2$.*

La preuve repose sur une interprétation adéquate du problème dans l'algèbre $\mathbb{Q}[\mathbb{Z}/n\mathbb{Z}]$. Elle ne permet cependant pas de résoudre (2) pour $1 < k < \frac{n-1}{2}$; en fait, on ne sait démontrer complètement la conjecture généralisée (2) que pour une classe encore plus restreinte d'automates :

Théorème 3 *Si dans un automate circulaire à n états (n premier) possédant une lettre de rang $(n-1)$, il existe un mot de rang inférieur ou égal à k, il existe un tel mot de longueur inférieure ou égale à $(n-k)^2$.*

La démonstration est essentiellement combinatoire et tout à fait différente de celle du théorème 2.

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 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 $r_{\mathcal{A}}(m) = |\{qm \mid q \in Q\}| = |Qm|$.

Puisqu'on suppose qu'une lettre y induit une permutation circulaire sur Q, on peut numéroter les états de 0 à $n-1$ de sorte que $0y^i = i$ pour $0 \leqslant i \leqslant n-1$. Nous identifierons à présent Q à $\mathbb{Z}/n\mathbb{Z}$, ce qui permet de définir une addition sur Q. On a alors pour tout entier r : $qy^r = q + r$. Enfin, si K est une partie de Q, nous noterons $r + K$ (resp. $r - K$) l'ensemble $Ky^r = \{r + k \mid k \in K\}$ (resp. $\{r - k \mid k \in K\}$).

2 Preuves

2.1 Démonstration du théorème 1

Si $\mathcal{A}$ est un groupe, tous les mots sont de rang n et le théorème est évident. Sinon, il existe au moins une lettre x qui n'est pas une permutation : on peut donc trouver deux états a et b tels que $ax = bx$. Si K est un ensemble vérifiant $|K| = r > \frac{n}{2}$, les ensembles $a - K$ et $b - K$ ont une intersection de cardinal supérieur ou égal à $(2r - n)$ et l'un des $2(n-r)+1$ entiers $0, 1, \ldots, 2(n-r)$ est élément de $(a-K) \cap (b-K)$. Soit $j = j(K)$ un tel entier. Il vient $\{a, b\} \subset K + j = Ky^j$ et donc $|Ky^jx| < |K|$ avec $|y^jx| \leqslant 2(n-r)+1$.

La preuve s'achève alors facilement par récurrence sur $n-k$: pour $n-k = 0$, il suffit de dire que le mot vide est de rang n. Si le résultat est acquis pour $(n-k)$ avec $k > \frac{n}{2}$, c'est qu'il existe un mot m vérifiant $|Qm| \leqslant k$ et $|m| \leqslant (n-k)^2$. Si $|Qm| \leqslant k-1$, le théorème est démontré puisque $(n-k)^2 \leqslant (n-k+1)^2$. Sinon $|Qm| = k > \frac{n}{2}$, et on applique le résultat précédent à Qm : il existe un entier $j \leqslant 2(n-k)$ tel que $|Qmy^jx| < |Qm|$. Le mot $w = my^jx$ est donc de rang inférieur ou égal à $(k-1)$ et sa longueur est bornée par $|m| + j + 1 \leqslant (n-k)^2 + 2(n-k) + 1 = (n-k+1)^2$. □

2.2 Démonstration du théorème 2

Comme nous l'avons déjà dit, si $\mathcal{A}$ n'est pas un groupe, il existe une lettre x qui n'est pas une permutation. La suite de la démonstration repose sur le

Lemme 1 *Si K est une partie de Q distincte de $\emptyset$ et de Q, il existe un entier r tel que $|(K+r)x^{-1}| > |K|$.*

En effet si la propriété est fausse on a pour tout r : $|(K+r)x^{-1}| \leqslant |K|$ et comme d'autre part

$$\sum_{r=0}^{n-1} |(K+r)x^{-1}| = \sum_{r=0}^{n-1} \sum_{q\in K+r} |qx^{-1}| = |K| \sum_{q\in Q} |\{q\}x^{-1}| = |K||Qx^{-1}| = |K|n,$$

il vient finalement $|(K+r)x^{-1}| = |K|$ pour tout r. Cela dit nous allons traduire ces données dans l'algèbre $Q[\mathbb{Z}/n\mathbb{Z}] = R$. Tout d'abord, Q étant déjà identifié à $\mathbb{Z}/n\mathbb{Z}$, on peut associer à chaque état q un élément $\underline{q}$ de R. De même, si K est une partie de Q, on posera $\underline{K} = \sum_{q\in K} \underline{q}$. L'opérateur x^{-1} se prolonge en un endomorphisme de R par la formule $(\sum_{q\in Q} \lambda_q \underline{q})x^{-1} = \sum_{q\in Q} \lambda_q (\underline{qx^{-1}})$. Enfin, l'application $K \to |K|$ qui, à une partie de Q, associe son cardinal a pour prolongement naturel la forme linéaire « somme des coordonnées dans la base Q », que nous noterons également $|\ |$: $|\sum_{q\in Q} \lambda_q| = \sum_{q\in Q} \lambda_q$.

La première chose à démontrer est que les vecteurs $(\underline{K+r})$ forment une base du $\mathbb{Q}$-espace vectoriel R. Or n étant premier, l'algèbre R est isomorphe au produit direct $\mathbb{Q}\times\mathbb{Q}[\zeta]$ où ζ est une racine primitive n-ième de l'unité (cf. Lang [8, p. 459]), l'isomorphisme étant donné par :

$$\Phi(\underline{q}) = (1, \zeta^q) \quad \text{pour } 0 \leqslant q \leqslant n-1$$

On a donc, en posant pour simplifier $u = \sum_{q\in K} \zeta^q$, $\Phi(\underline{K}) = (|K|, u)$ et $\Phi(\underline{K+r}) = (|K|, u\zeta^r)$.

Il en résulte en particulier

$$(1,0) = \frac{1}{|K|n} \sum_{0\leqslant r\leqslant n-1} \Phi(\underline{K+r})$$

Il suffit donc de prouver que les vecteurs uz^r engendrent le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[\zeta]$. Mais le vecteur $u = \sum_{q\in K} \zeta^q$ n'est pas nul puisque K est différent de $\emptyset$ et de Q et que le polynôme minimal de ζ est $\sum_{q=0}^{n-1} X^q$. Comme $\mathbb{Q}[\zeta]$ est un corps, u est inversible. Soit $\sum_{i=0}^{n-1} \lambda_i \zeta^i$ son inverse. Il vient $\zeta^r = \sum_{i=0}^{n-1} \lambda_i (u\zeta^{i+r})$, ce qui montre bien que $(u\zeta^r)$ $(0 \leqslant r \leqslant n-1)$ est un système générateur.

Revenons maintenant à l'hypothèse. Puisque $|(\underline{K+r)x^{-1}}| = |\underline{K}|$ et que la famille des $(\underline{K+r})$ est une base de R, on a $|vx^{-1}| = |v|$ pour tout vecteur v de R. En particulier $|\underline{q}x^{-1}| = |\underline{q}| = 1$, ce qui prouve que x est injective, contredisant ainsi l'hypothèse. Ceci achève la démonstration du lemme. $\square$

Revenons au théorème. Puisque x n'est pas injective, il existe un état c tel que $|cx^{-1}| > 1$. Montrons par récurrence sur k $(0 \leqslant k \leqslant n-2)$ qu'il existe un mot m tel que $|m| \leqslant 1+kn$ et $|cm^{-1}| \geqslant k+2$. Si $k=0$, on peut prendre $m=x$ d'après ce qui précède. Supposons le résultat acquis jusqu'au rang $k \leqslant n-3$. Ou bien $|cm^{-1}| \geqslant k+3$ et le résultat est vrai jusqu'au rang $(k+1)$, ou bien $|cm^{-1}| = k+2 < n$ et on peut appliquer le lemme 1 à l'ensemble cm^{-1} : il existe un entier r $(0 \leqslant r \leqslant n-1)$ tel que $|(cm^{-1})y^{-r}x^{-1}| > |cm^{-1}|$. Le mot $w = (xy^r m)$ vérifie donc : $|w| \leqslant 1+(k+1)n$ et $|cw^{-1}| \geqslant k+3$. Finalement on voit qu'il existe en particulier un mot f tel que $cf^{-1} = Q$ et $|f| \leqslant 1+n(n-2) = (n-1)^2$, et comme $Qf = (cf^{-1})f \subset \{c\}$, f est synchronisant. $\square$

2.3 Démonstration du théorème 3

Elle repose sur le lemme suivant :

Lemme 2 *Sous les hypothèses du théorème 3, on peut trouver une ensemble K et un mot m de X^* tels que, si on pose $h = \min(k, n-k)$, on ait*

(i) $|K| = k + h$
(ii) $|m| \leqslant h^2$
(iii) $|Km| \leqslant k$

Preuve. Nous désignerons par x la lettre de rang $(n-1)$, par a et b les deux états ayant même image c par x ($ax = bx = c$) et nous poserons enfin $Qx = Q \setminus \{q\}$.

On remarquera que $a \neq b$ et $c \neq q$. Pour déterminer K et m, on va construire deux suites d'ensembles K_i $(0 \leqslant i \leqslant h-1)$ et K'_i $(1 \leqslant i \leqslant h)$ et une suite d'entiers r_i $(1 \leqslant i \leqslant h)$ satisfaisant les conditions suivantes :
(1) $|K_i| = |K'_i| = 2i$ pour tout i
(2) $r_i \leqslant 2i$
(3) $q \notin K_i$

Nous allons maintenant décrire, puis justifier l'algorithme de construction. On pose $K_0 = \emptyset$ et on détermine K_i, K'_i et r_i à partir de K_{i-1} de la façon suivante :
(a) On pose $s_i = c$ si $c \notin K_{i-1}$. Si $c \in K_{i-1}$, on choisira s_i dans $Q \setminus (K_{i-1} \cup \{q\})$.
(b) On pose $K'_i = (K_{i-1} \cup \{s_i\})x^{-1}$.
(c) On détermine $r_i \leqslant 2i$ tel que $q + r_i \notin K'_i$.
(d) On pose $K_i = K'_i y^{-r_i}$.

Cet algorithme est effectivement réalisable. En effet, on a bien tout d'abord $|K_0| = 0$. Ensuite, en supposant la construction effectuée jusqu'au rang $i-1$ (avec $i \leqslant h$), on a $|K_{i-1}| \leqslant 2(h-1) \leqslant n-2$ et par conséquent l'ensemble $Q \setminus (K_{i-1} \cup \{q\})$ n'est pas vide ce qui prouve que l'étape (a) est réalisable. Passons à l'étape (b). Puisque q n'appartient pas à K_{i-1} par hypothèse et que s_i est différent de q par construction, on voit que q n'est pas un élément de $K_{i-1} \cup \{s_i\}$. En revanche, c est certainement contenu dans cet ensemble et comme c'est le seul élément ayant deux antécédents par x, il vient $|K'_i| = |K_{i-1} \cup \{s_i\}| + 1 = (2(i-1)+1)+1 = 2i$.

Il ne reste plus qu'à déterminer r_i. Or les ensembles $\{q, q+1, \ldots, q+2i\}$ et $Q \setminus K'_i$ ont une intersection non vide puisque la somme de leurs cardinaux est $(n+1)$. On peut donc trouver un $r_i \leqslant 2i$ tel que $q + r_i \notin K'_i$. Les propriétés (1) et (3) découlent alors immédiatement de (d).

Cela dit, on pose $K = K'_h \cup T$ où T est un ensemble à $(k-h)$ éléments disjoints de K'_h. Il vient :
(i) $|K| = 2h + (k-h) = k + h$

On pose également $m = xy^{r_{h-1}}xy^{r_{h-2}} \cdots y^{r_1}x$. On a alors :
(ii) $|m| \leqslant h + \sum_{i=1}^{h-1}(2i) = h^2$

D'autre part, on voit que $|Km| \leqslant |K'_h m| + |Tm| \leqslant |K'_h m| + (k-h)$. Or, si on pose $w_i = y^{r_{h-i}}x \cdots y^{r_1}x$, on peut montrer par récurrence sur i que pour $1 \leqslant i \leqslant h$:

$$(*) \qquad |K'_h m| \leqslant i + |K_{h-i} w_i|$$

En effet, si $i = 1$, on a

$$K'_h = K'_h x w_1 = (K_{h-1} \cup \{s_h\})x^{-1} x w_1 \subset (K_{h-1} \cup \{s_h\}) w_1 = K_{h-1} w_1 \cup \{s_h w_1\}$$

et donc $|K'_h m| \leqslant 1 + |K_{h-1} w_1|$. Si la propriété $(*)$ est établie pour i, on a :

$$K_{h-i} w_i = K'_{h-i} x w_{i+1} = (K_{h-(i+1)} \cup \{s_{h-i}\}) x^{-1} x w_{i+1} \subset K_{h-(i+1)} w_{i+1} \cup \{s_{h-i} w_{i+1}\}$$

d'où $|K_{h-i} w_i| \leqslant |K_{h-(i+1)} w_{i+1}| + 1$, ce qui démontre la propriété pour $i+1$ et achève ainsi la récurrence.

Si on applique $(*)$ avec $i = h$, il vient simplement $|K'_h m| \leqslant h$. Il en résulte
(iii) $|Km| \leqslant h + (k-h) = k$

et le lemme 2 est démontré. □

Revenons au théorème 3. Si $n \leqslant 2k$, on a $k+h=n$ et le lemme 2 suffit. Sinon $h=k$ et $|K|=2k$. Mais on démontre à l'aide du lemme 1, et en calquant la démonstration du théorème 2, qu'il existe un mot w tel que $Kw^{-1}=Q$ et $|w| \leqslant n(n-2k)$. On a alors $Qwm \subset Km$ et donc $r_{\mathcal{A}}(wm) = |Qwm| \leqslant |Km| = k$ et d'autre part $|wm| = n(n-2)+k^2 = (n-k)^2$. □

Remarque. Le lemme 2 n'utilise pas l'hypothèse « n premier » et fournit donc une démonstration du théorème 1 sous les hypothèses plus restrictives du théorème 3. On notera d'ailleurs que les algorithmes utilisés dans les deux démonstrations sont différents.

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

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

[7] Z. Kohavi and J. Winograd, Bounds on the length of synchronizing sequences and the order of information losslessness, in *Proc. of an international Symposium on the Theory of Machines and Computations*, Haifa, Israel, 1970.

[8] S. Lang, *Algebra*, *World Student Series*, Addison-Wesley, Reading, Massachussetts, 1965.

[9] 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.

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

[11] D. Perrin and M. Schützenberger, Codes et sous-monoïdes possédant des mots neutres, in *Theoretical Computer Science*, pp. 27–44, *Lect. Notes Comp. Sci.* vol. 48, Springer, 1977.

[12] 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.

[13] 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.

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

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

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

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

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