Utilisation de l'algèbre linéaire en théorie des automates*

Jean-Eric Pin
CNRS, Laboratoire d'Informatique Théorique et de Programmation

Abstract. Techniques from linear algebra are used to study the synchronization problem in automata theory. Let $\mathcal{A} = (Q, X)$ be a finite automaton. Each word m in X^* defines a map from Q to Q ; the *rank* of m in $\mathcal{A}$ is the integer $\text{Card}\{qm \mid q \in Q\}$. A word of rank 1 maps all states onto a unique state. Such a word is called a synchronizing word (if such a word exists the automaton itself is called a *synchronizing* automaton). Let $\mathcal{A}$ be a synchronizing automaton with n states. Our main result asserts that if there is a letter of rank $\leq 1 + \log_2 n$ in $\mathcal{A}$, then there exists a synchronizing word of rank $\leq (n-1)^2$.

1 Introduction

Suivant une habitude qui est devenue une tradition chez les informaticiens, on assimile souvent un automate fini à une *boîte noire*, ce qui signifie que l'on a acccès aux états d'entrée et de sortie mais que le fonctionnement interne de la machine nous échappe. On peut alors se livrer à des *expériences*, qui consistent à injecter une suite de symboles et à observer le comportement entrée-sortie de l'automate. C'est Moore [7], qui le premier, fit une étude détaillée de ces expériences connues sous le nom de *Gedanken Experiments*. Par la suite, de nombreux auteurs ont amplifié les résultats de Moore, sans pour autant parvenir à régler complètement cet aspect de la théorie des automates (cf [1, 6, 11]). En tête des questions encore ouvertes, figure le problème de la synchronisation : nous dirons qu'un mot (c'est-à-dire une suite de symboles) est synchronisant s'il a même action sur tous les états de l'automate. Lorsqu'un tel mot existe, on dit que l'automate est synchronisant. Le problème consiste à évaluer, dans un automate synchronisant fini donné, la longueur des mots synchronisants les plus courts. Černý [3] a en effet conjecturé le résultat suivant

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 cardinal de l'image de cette application. En particulier, les mots de rang 1 sont les mots synchronisants et on peut formuler une généralisation naturelle de la conjecture de Černý.

Conjecture 2 *Dans un automate synchronisant fini à n états, s'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, diverses bornes ont été proposées [2, 4, 5, 6, 9, 8, 10], dont la meilleure [8] est en $(\frac{1}{2} - \frac{\pi^2}{36})n^3 + o(n^3)$ (où $\frac{1}{2} - \frac{\pi^2}{36} \simeq 0,2258$).

Pour la conjecture 2, la meilleure borne connue est en $\frac{1}{3}(n-k)^3 + o(n-k)^3$. Nous démontrons la conjecture de Černý dans un cas particulier.

*Article paru dans les actes du premier colloque AFCET-SMF de Mathématiques Appliquées, publication AFCET (1978), p. 85–92.

Théorème 3 *Soit $\mathcal{A}$ un automate synchronisant à n états possédant une lettre de rang $r \leq 1 + \log_2 n$. Alors il existe un mot synchronisant de longueur inférieure ou égale à $(n-1)^2$.*

A l'égard de la conjecture généralisée, nous démontrons le

Théorème 4 *Soit $\mathcal{A}$ un automate synchronisant à n états possédant une lettre de rang r. S'il existe un mot de rang $\leq r-1$, il existe un tel mot de longueur inférieure ou égale à $n-r+3$. Cette borne est optimale.*

La démonstration de ces théorèmes s'appuie sur une interprétation du problème en termes d'algèbre linéaire, faisant notamment apparaître le cardinal d'une intersection comme un produit scalaire. Cette démarche permet d'ailleurs d'obtenir divers corollaires intéressants parmi lesquels figurent certains des résultats de Moore déjà cités.

2 Résultats

Soit $\mathcal{A} = (Q, X, \delta)$ un automate fini, où $Q = \{q_1, \ldots, q_n\}$ est l'ensemble des états, X est l'alphabet et δ la fonction de transition. Selon l'usage, nous noterons simplement qm (au lieu de $\delta(q,m)$) l'action du mot m de X^* sur l'état q. Par linéarité, cette action s'étend à l'espace vectoriel $\mathbb{R}^Q$ des combinaisons linéaires formelles d'éléments de Q. Pour mieux distinguer états et vecteurs, nous noterons $\underline{q}_i$ l'application de Q dans $\mathbb{R}$, image canonique de q_i dans $\mathbb{R}^Q$, définie par $\underline{q}_i(q_j) = \delta_{i,j}$ où $\delta_{i,j}$ est le symbole de Kronecker. On a donc par définition la formule

$$(1) \qquad (\sum \lambda_i \underline{q}_i)x = \sum \lambda_i (\underline{q}_i x)$$

Si K est une partie de q et m un mot de X^*, $|K|$ désignera le cardinal de K et $|m|$ la longueur de m, le contexte évitant toute confusion entre ces notations. On notera Km l'ensemble $\{qm \mid q \in K\}$ et $\underline{K}$ le vecteur caractéristique de K, $\underline{K} = \sum_{q \in K} \underline{q}$. Enfin le rang de m dans $\mathcal{A}$ est $r_{\mathcal{A}}(m) = |Qm|$.

Remarque. L'égalité $\underline{K}m = \underline{Km}$ a lieu si et seulement si la restriction de m à K est une injection.

Le produit scalaire défini par

$$\left\langle \sum \lambda_i \underline{q}_i, \sum \mu_i \underline{q}_i \right\rangle = \sum \lambda_i \mu_i$$

munit $\mathbb{R}^Q$ d'une structure d'espace euclidien. Les notions d'orthogonalité utilisées par la suite feront référence à ce produit scalaire. Si K_1 et K_2 sont des parties de Q, on a la relation

$$(2) \qquad |K_1 \cap K_2| = \langle \underline{K_1}, \underline{K_2} \rangle$$

Soit θ une équivalence d'index r définie sur Q et soient $S_1, \ldots, S_r$ les classes d'équivalence modulo θ. Nous dirons qu'un ensemble T est un *système de représentants* de θ, ou encore un *transversal* de θ, si $|T \cap S_i| = 1$ pour $1 \leq i \leq r$.

On peut associer à θ les sous-espaces E_θ et E^θ engendrés respectivement par les vecteurs $\underline{S_i}$ $(1 \leq i \leq r)$ et $\{\underline{q} - \underline{q'} \mid q \equiv q' \pmod{\theta}\}$. On a alors la proposition suivante :

Proposition 1

(1) *E_θ et E^θ sont deux sous-espaces orthogonaux supplémentaires, de dimension r et $n-r$ respectivement.*

(2) *Les vecteurs $\underline{S}_i$ $(1 \leq i \leq r)$ forment une base orthogonale de E_θ.*

Preuve. Pour montrer que E_θ et E^θ sont orthogonaux, il suffit de vérifier que leurs générateurs sont 2 à 2 orthogonaux. Or si $q \equiv q' \pmod{\theta}$, on a simultanément $q \in S_i$ et $q' \in S_i$ ou $q \notin S_i$ et $q' \notin S_i$ et donc $\langle \underline{S}_i, \underline{q} - \underline{q}' \rangle = 0$ pour tout i. Reste à prouver que $E_\theta + E^\theta = \mathbb{R}^Q$. Soit q un état donné : q est élément d'un certain $S_i = \{q, q_2, \ldots, q_p\}$. On a alors

$$\underline{q} = \frac{1}{p}(\underline{q} + \underline{q}_2 + \ldots + \underline{q}_p) + (\underline{q} - \underline{q}_p) + \ldots + (\underline{q} - \underline{q}_2)$$

Or $(\underline{q} + \underline{q}_2 + \ldots + \underline{q}_p) = \underline{S}_i \in E_\theta$ et les vecteurs $\underline{q} - \underline{q}_i$ $(2 \leq i \leq p)$ sont éléments de E^θ. L'espace $E_\theta + E^\theta$ contient donc tous les vecteurs $\underline{q}$: il est par conséquent égal à $\mathbb{R}^Q$.

Les $\underline{S}_i$ sont deux à deux orthogonaux d'après la relation (2). Ils sont donc en particulier linairement indépendants et donc $\dim E_\theta = r$ ce qui achève la démonstration de la proposition. □

Remarque. On peut démontrer que θ est une congruence de l'automate $\mathcal{A}$ si et seulement si l'espace E^θ est invariant (i.e. si $E^\theta x \subset E^\theta$ pour toute lettre $x \in X$).

La proposition qui suit est essentielle. Sa démonstration s'inspire de celle des théorèmes 6 et 8 de Moore [7].

Proposition 2 *Soit $A(\theta)$ un espace affine de direction E^θ et v un point de $A(\theta)$. Si vm est dans $A(\theta)$ pour tout mot m de longueur $\leq n-r+1$, alors vm est dans $A(\theta)$ pour tout mot m de X^*.*

Preuve. Pour tout $i \in \mathbb{N}$, notons A_i l'espace affine engendré par les points $\{vm \mid |m| \leq i\}$. La suite des A_i est croissante par construction. De plus A_{i+1} est engendré par la réunion $A_i \cup A_i X$: soit en effet un point a de A_i défini comme barycentre. Il s'écrit $a = \sum \lambda_j (vm_j)$ avec $|m_j| \leq i$ et $\sum \lambda_j = 1$. Pour toute lettre x, le point $ax = \sum \lambda_j (vm_j x)$ est un barycentre de points de A_{i+1}, donc est lui-même élément de A_{i+1}, ce qui prouve l'inclusion $A_i \cup A_i X \subset A_{i+1}$. Réciproquement, soit vm un des générateurs de A_{i+1}. Si $|m| \leq i$, $vm \in A_i$. Sinon, m s'écrit $m'x$ avec $|m'| = i$ et donc $vm = vm'x \in A_i X$, ce qui démontre que $vm \in A_i \cup A_i X$ dans tous les cas.

On en déduit par récurrence que si $A_i = A_{i+1}$ pour un certain indice i, alors $A_i = A_{i+n}$ pour tout n. Or puisque vm est dans $A(\theta)$ pour $|m| \leq n-r+1$, les espaces $A_0, A_1, \ldots, A_{n-r+1}$ forment une suite croissante de sous-espaces affines de $A(\theta)$. On a donc :

$$0 = \dim A_0 \leq \dim A_1 \leq \cdots \leq \dim A_i \leq \cdots \leq \dim A_{n-r+1} \leq \dim A(\theta) = n-r$$

puisque $\dim A(\theta) = \dim E^\theta = n-r$ d'après la proposition 1. La suite des dimensions ne peut être strictement croissante et on a par conséquent $A_i = A_{i+1}$ pour un $i \leq n-r+1$. Puisque dans ce cas $A_i = A_{i+n}$ pour tout n, on a finalement $A_p \subset A(\theta)$ pour tout $p \in \mathbb{N}$. En particulier $vm \in A(\theta)$ pour tout mot m de X^*. □

Cette proposition a deux corollaires importants : le premier de ces corollaires est un résultat bien connu de la théorie des automates, formulé ici d'une façon un peu différente (cf. les théorèmes 6 et 8 de Moore [7]). Le second corollaire est étroitement relié à la conjecture de Černý, comme nous le verrons plus loin.

Corollaire 3 *Soit θ une équivalence d'index r sur Q, q et q' deux états distincts de Q. Si qm et $q'm$ sont congrus modulo θ pour tout mot m de longueur $\leq n-r+1$, alors c'est encore vrai pour tout mot m de X^*.*

Preuve. Appliquons la proposition 2 avec $A(\theta) = E^\theta$ et $v = \underline{q} - \underline{q'}$. Puisque $vm = \underline{qm} - \underline{q'm}$, vm est élément de E^θ pour $|m| \leq n-r+1$. Il en résulte donc $\underline{qm} - \underline{q'm} \in E^\theta$ pour tout mot m de X^*. Si S est la classe de qm modulo θ, il vient, d'après la proposition 1, $\langle qm - q'm, S\rangle = 0$ d'où $\langle q'm, S\rangle = \langle qm, S\rangle = 1$ et donc $q'm \in S$ d'après (2). Autrement dit, $qm \equiv q'm \pmod{\theta}$ comme annoncé. $\square$

Corollaire 4 *Soit θ une équivalence d'index r sur Q et T une partie de Q. Si pour tout mot m de longueur $\leq n-r+1$, Tm est un transversal de θ, alors cette propriété est encore vraie pour tout mot m de X^*.*

Preuve. L'hypothèse appliquée à $m = 1$ nous dit déjà que T est un transversal de θ. De plus, si Tm est un transversal de θ, les ensembles T et Tm ont même cardinal, la restriction de m à T est une injection et il résulte d'une remarque faite plus haut que $\underline{T}m = \underline{Tm}$.

On se propose d'appliquer la proposition 2 avec $A(\theta) = \underline{T} + E^\theta$ et $v = \underline{T}$. Si $|m| \leq n-r+1$, on a d'après l'hypothèse $vm = \underline{T}m = \underline{Tm}$. Il s'agit donc de prouver que $vm \in A(\theta)$, ou encore que $\underline{Tm} - \underline{T} \in E^\theta$. Pour le vérifier, on peut par exemple calculer le produit scalaire $\langle \underline{Tm} - \underline{T}, \underline{S_i}\rangle$ pour $1 \leq i \leq r$ (les S_i sont, rappelons-le, les classes modulo θ) :

$$\langle \underline{Tm} - \underline{T}, \underline{S_i}\rangle = \langle \underline{Tm}, \underline{S_i}\rangle - \langle \underline{T}, \underline{S_i}\rangle = |Tm \cap S_i| - |T \cap S_i| = 0$$

en utilisant la relation (2) et le fait que Tm est un transversal. Par conséquent $\underline{Tm} - \underline{T}$ est orthogonal à tous les $\underline{S_i}$ et donc aussi à E_θ et il suffit d'appliquer la proposition 1 pour conclure.

On a donc (proposition 2) $vm = \underline{T}m \in A(\theta)$ pour tout m, ce qui revient à écrire, en reprenant le calcul ci-dessus

$$\langle \underline{Tm}, \underline{S_i}\rangle = \langle \underline{T}, \underline{S_i}\rangle = 1 \text{ pour } 1 \leq i \leq r.$$

Mais d'après la définition du produit scalaire, on a

$$\langle \underline{Tm}, \underline{S_i}\rangle = |\{q \in T \mid qm \in S_i\}|$$

Donc chaque S_i contient exactement un élément qm où $q \in T$ et Tm est un transversal de θ. $\square$

Remarque. La définition de $A(\theta)$ dans la démonstration qui précède ne dépend pas du transversal T choisi. En effet, si T_1 et T_2 sont deux transversaux, on voit facilement que $T_1 - T_2 \in E^\theta$. On déduit du corollaire 4 la proposition

Proposition 5 *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 $\leq r-1$ dans $\mathcal{A}$, il existe un tel mot de longueur $\leq 2|w| + n - r + 1$.*

Preuve. Si $r_{\mathcal{A}}(w) \leq r-1$, le résultat est évident. Si w est de rang r dans $\mathcal{A}$, w définit sur Q une équivalence θ d'index r en posant :

$$q \equiv q' \bmod \theta \Leftrightarrow qw = q'w$$

Un transversal T de cette équivalence est un ensemble vérifiant $|T| = |Tw| = r$. Si m est un mot de rang inférieur ou égal à $r-1$, on a aussi $r_{\mathcal{A}}(mwm) \leq r-1$. Par conséquent, si on pose $K = Qw$, l'ensemble Km n'est pas un transversal de θ puisque $|Kmw| < r$. D'après le corollaire 4, il existe un mot m de longueur inférieure ou égale à $n-r+1$ tel que Km ne soit pas un transversal de θ. On a donc $|Km| \neq r$ ou $|Kmw| \neq r$, mais comme $|K| = |Qw| = r_{\mathcal{A}}(w) = r$, il vient $|Km| < r$ ou $|Kmw| < r$ et finalement $|Qwmw| = |Kmw| \leq r-1$, puisque de toute façon $|Kmw| \leq |Km|$. Le mot wmw est donc de rang inférieur ou égal à $r-1$ et sa longueur est majorée par $2|w| + n - r + 1$.

Si on applique ce résultat au cas où w est une lettre, on obtient le théorème 4. L'optimalité de la borne $n-r+3$, dont nous omettons ici la preuve, est démontrée en [8, chap. 2].

La proposition suivante permettra de démontrer le théorème 3.

Proposition 6 *Soit $\mathcal{A}$ un automate à n états dont une lettre est de rang au plus $r < n$. S'il existe un mot de rang $\leq k$ (avec $k < r$), il existe un tel mot de longueur $\leq (2^{r-k}-1)(n-r+1) + 2^{r-k+1} - (r-k+1)$*

Preuve. La démonstration se fait par récurrence sur $p = r-k$. Si $p = 1$, on a $k = r-1$ et il suffit d'appliquer le théorème 4.
Passage de $p-1$ à p. Si le théorème est vrai pour $p-1 = r-(k+1)$, il existe un mot w vérifiant $r_{\mathcal{A}}(w) \leq k+1$ et $|w| \leq (2^{r-k-1}-1)(n-r+1) + 2^{r-k} - (r-k)$. Appliquons le corollaire 4 : il existe un mot m de rang $\leq p = r-k$ et de longueur $\leq 2|w|+n-(k+1)+1$. On en déduit (après calculs) $|m| \leq (2^{r-k}-1)(n-r+1) + 2^{r-k+1} - (r-k+1)$. $\square$

Exemples.

(1) Avec $n = 5, r = 3, k = 1$, on obtient l'énoncé suivant :
Dans un automate synchronisant à 5 états, possédant une lettre de rang ≤ 3, il existe un mot synchronisant de longueur ≤ 14.
La borne 14 n'est sans doute pas optimale (il semble que ce soit 12).

(2) Avec $r = n-1$ et $k = 1$, on retrouve la borne $2^n - n - 1$, qui est la première borne connue pour la conjecture (1) (Černý [2]), mais qui avait été obtenue par des voies tout à fait différentes.

Passons à la preuve du théorème 3 :

Théorème 3 *Soit $\mathcal{A}$ un automate synchronisant à n états possédant une lettre de rang $r \leq 1 + \log_2 n$. Alors il existe un mot synchronisant de longueur inférieure ou égale à $(n-1)^2$.*

Preuve. Appliquons la proposition 6 avec $k = 1$ et $r = 1 + \log_2 n$. Il existe un mot m de rang 1 (donc synchronisant) tel que

$$|m| \leq (2^{r-1}-1)(n-r+1) + 2^r - r \tag{3}$$

soit encore, puisque $2^{r-1} \leq n$, $|m| \leq (n-1)(n-r+1) + 2n - r = n^2 + (2-r)n - 1$.

Si $r = 4$, on a donc immédiatement $|m| \leq n^2 - 2n - 1 \leq (n-1)^2$. Si $r = 1$, il existe une lettre de rang 1 et le résultat est évident. Si $r = 2 < n$, on peut conclure directement en utilisant le théorème 4 : il existe un mot synchronisant de longueur $\leq (n+1)$ et $(n+1) \leq (n-1)^2$ pour $n \geq 3$.

Si $r = 3$, la formule (3) montre que $|m| \leq 3n-1$ et comme $(3n-1) \leq (n-1)^2$ pour $n \geq 5$, le théorème 3 est démontré... sauf dans le cas $r = 3$ et $n = 4$. Mais ce dernier cas a été résolu en 1971 par des méthodes complètement différentes (Černý, Pirickà, Rosenauerova [4]).

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] E. F. Moore, Gedanken-experiments, *Automata Studies, Ann. Math. Stud.* **34** (1956), 129–153.

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

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

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

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