La conjecture de Černý

Lucien Pech

12 février 2007

Un automate synchronisant amène tous les états d'un automate fini à un unique état. J. Černý a conjecturé que si un automate fini à n états admet un mot synchronisant, alors il admet un mot synchronisant de taille au plus $(n-1)^2$. La conjecture a été démontré pour les automates circulaires par L. Dubuc [3]. On montre ici un résultat plus faible, d'après un article de M.-P. Béal [1], mais dont la preuve est plus simple est s'appuie sur les séries rationnelles, dont on donnera une définition et quelques propriétés.

1 Automates synchronisants

1.1 Définitions

Définition 1 (automate rudimentaire)**.** Dans cette exposé, on ne considèrera que des *automates finis déterministes complets*. On ne s'intéressera pas aux états initiaux et finaux ; un automate $\mathcal{A}$ sera donc la donnée d'un alphabet fini A, d'un ensemble fini d'états Q, et d'une action $Q \times A^* \to Q : (q, w) \mapsto q \cdot w$ qui a tout mot de A^* et tout état de Q associe un état de Q. On notera donc $\mathcal{A} = (A, Q, \cdot)$.

L'état $q \cdot w$ de l'automate est l'état dans lequel on se trouve après avoir lu le mot w à partir de l'état q.

Exemple d'automate fini déterministe complet, qui nous servira pour illustrer les prochaines définitions :

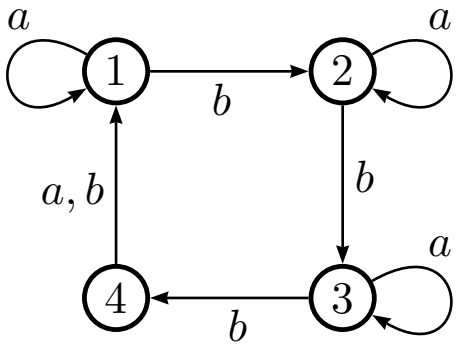

FIG. 1 – Exemple d'automate

Définition 2 (image directe, réciproque)**.** Étant donnés un automate fini $\mathcal{A} = (A, Q, \cdot)$, un mot $w \in A^*$ et un ensemble d'états $P \subseteq Q$, on définit l'image directe de P par $w : P \cdot w = \{p \cdot w : p \in P\}$, et l'image réciproque de P par $w : P \cdot w^{-1} = \{q \in Q : q \cdot w \in P\}$.

Intuitivement, $P \cdot w$ est l'ensemble des états de l'automate auxquels on accède en lisant le mot w depuis les états de l'ensemble P, et $P \cdot w^{-1}$ est l'ensemble des états depuis lesquels, si on lit le mot w, on arrive à un état de P.

Sur l'automate de la figure 1.1, on a $\{1, 2\} \cdot ab = \{2, 3\}$, $\{1\} \cdot ab^{-1} = \emptyset$, et $\{2\} \cdot ab^{-1} = \{1, 4\}$.

On a les propriétés évidentes :
- $P \subseteq (P \cdot w) \cdot w^{-1}$
- $(P \cdot w^{-1}) \cdot w = P$
- $P \cdot uv = (P \cdot u) \cdot v$
- $P \cdot (uv)^{-1} = (P \cdot v^{-1}) \cdot u^{-1}$

Définition 3 (rang, mot synchronisant)**.** Étant donnés $\mathcal{A} = (A, Q, \cdot)$ et $w \in A^*$, on définit le *rang* de w : $rang(w) = card(Q \cdot w)$. Un mot est dit *synchronisant* s'il est de rang égal à 1.

Un mot w est donc synchronisant s'il existe un état p de l'automate tel que quel soit l'état q, $q \cdot w = p$.

Pour l'automate de la figure 1.1, le mot $w = ab^3ab^3a$ est synchronisant : quel que soit l'état de départ, lire le mot w amène à l'état 1.

Définition 4 (automate synchronisant)**.** Un automate fini $\mathcal{A} = (A, Q, \cdot)$ est dit *synchronisant* s'il admet un mot synchronisant.

L'automate de la figure 1.1 est synchronisant pour le mot w.

Conjecture 1 (Černý)**.** *Soit $\mathcal{A} = (A, Q, \cdot)$ un automate fini à n états. Si $\mathcal{A}$ est synchronisant, alors il admet un mot synchronisant $w \in A^*$ de longueur $|w| \leqslant (n-1)^2$.*

C'est le cas de l'exemple de la figure 1.1 : l'automate a 4 états, et le mot synchronisant w est de longueur 9.

Définition 5 (mot augmentant)**.** Étant donnés $\mathcal{A} = (A, Q, \cdot)$, $w \in A^*$ et $P \subseteq Q$, on dit que w est un *mot augmentant* pour P si $card(P \cdot u^{-1}) > card(P)$.

Intituivement, un mot w est augmentant pour P si le nombre d'états tels qu'en lisant w on arrive dans P est plus grand que le nombre d'état de P.

On a déjà vu que sur notre exemple, $\{2\} \cdot ab^{-1} = \{1, 4\}$, donc le mot ab est augmentant pour le singleton $\{2\}$.

Définition 6 (ensemble k-augmentable)**.** Étant donnés $\mathcal{A} = (A, Q, \cdot)$ et $P \subseteq Q$, on dit que P est k-augmentable s'il existe un mot augmentant w pour P tel que $|w| \leqslant k$.

Sur notre exemple, $\{2\}$ est 2-augmentable.

1.2 Propriétés

Propriété 2. *Soit $\mathcal{A} = (A, Q, \cdot)$ synchronisant. Alors il existe un état $q \in Q$ tel que $\{q\}$ soit 1-augmentable.*

Démonstration. Soit $w = w_1...w_n \in A^*$ un mot synchronisant pour $\mathcal{A}$. Soit $i_0 = \min(i \in [\![1, n]\!] : card(Q \cdot w_1...w_i) = 1)$; alors $card(Q \cdot w_1...w_{i_0-1}) > 1$. Soit $p \in Q$ tel que $Q \cdot w_1...w_{i_0} = \{p\}$. Comme $Q \cdot w_1...w_{i_0-1} \subseteq \{p\} \cdot w_{i_0}^{-1}$, on a $card(\{p\}) = 1 < card(Q \cdot w_1...w_{i_0-1}) \leqslant card(\{p\} \cdot w_{i_0}^{-1})$, donc w_{i_0} est un mot (de longueur 1) augmentant pour $\{p\}$. Donc $\{p\}$ est 1-augmentable. □

Dans l'exemple de la figure 1.1, le singleton $\{1\}$ est 1-augmentable.

2 Matrices de transition, séries formelles

2.1 Matrices de transition

Définition 7 (matrice de transition)**.** Soit $\mathcal{A} = (A, Q, \cdot)$. Pour tout mot $w \in A^*$, on définit la matrice $M_w \in \mathbb{N}^{Q\times Q}$ de *transition* de l'action du mot w sur l'ensemble Q par : $\forall p, q \in Q,\ (M_w)_{p,q} = \begin{cases} 1 & \text{si } p \cdot w = q \\ 0 & \text{sinon} \end{cases}$.

Définition 8 (vecteur caractéristique)**.** Soient $\mathcal{A} = (A, Q, \cdot)$ et $P \subseteq Q$. On définit le *vecteur caractéristique* $I_P \in \mathbb{N}^{Q\times 1}$ de l'ensemble d'états P par $(I_P)_p = \begin{cases} 1 & \text{si } p \in P \\ 0 & \text{sinon} \end{cases}$.

Lemme 3. *Si $1_{Q,1}$ désigne le vecteur colonne dont toutes les composantes sont égales à 1, on a $I_P \cdot 1_{Q,1} = card(P)$ (où $\cdot$ désigne le produit scalaire de deux vecteurs).*

Démonstration.

$$\begin{aligned} I_P \cdot 1_{Q,1} &= \sum_{q\in Q} (I_P)_q (1_{Q,1})_q \\ &= \sum_{q\in Q} (I_P) \\ &= \sum_{q\in P} 1 \\ &= card(P) \end{aligned}$$

□

Lemme 4. $\forall u, v \in A^*,\ M_{uv} = M_u M_v$.

Démonstration. Soient $p, q \in Q$. $(M_u M_v)_{p,q} = \sum_{r\in Q} (M_u)_{p,r}(M_v)_{r,q}$. L'automate est déterministe et complet, donc il existe un unique $r \in Q$ tel que $p \cdot u = r$, *i.e.* $(M_u)_{p,r} = 1$. Donc $(M_u M_v)_{p,q} = (M_v)_{r,q}$. Donc $(M_v)_{r,q} = 1$ si et seulement si $r \cdot v = q$, soit comme $p \cdot u = r$, si et seulement si $p \cdot (uv) = q$, *i.e.* $M_{uv} = 1$. Donc $M_{uv} = M_u M_v$. □

Étant donnée notre définition des matrices de transitions (dans $\mathbb{N}$ et non dans l'anneau de Boole), ceci n'est vrai que parce les automates sont déterministes et complets.

Ce lemme montre que $w \in A^* \mapsto M_w$ est un morphisme de monoïdes.

On montre de même :

Lemme 5. *Pour tout mot $w \in A^*$, on a $M_w 1_{Q,1} = 1_{Q,1}$.*

Intuitivement, celui signifie que si on lit w depuis n'importe quel état, on arrive à un unique état (ce qui traduit le fait que l'automate est déterministe et complet).

2.2 Séries formelles

Définition 9 (série formelle)**.** Soit A un alphabet fini. Une *série formelle* sur le monoïde libre A^* à coefficients dans un semi-anneau $\mathbb{K}$ est une application de A^* dans $\mathbb{K}$. On note $\mathbb{K}\langle\langle A\rangle\rangle$ l'ensemble de ces séries. L'image d'un mot w de A^* par la série S est noté $\langle S, w\rangle$ et appelé le *coefficient* de w dans S.

Par exemple, si $A = \{a,\ b\}$, la fonction S de A^* dans le semi-anneau $\mathbb{K} = (\mathbb{N},\ +,\ \times)$, définie par $\langle S,\ w\rangle = |w|_b$ est une série formelle.

Définition 10 (série reconnaissable)**.** Une série formelle S de A^* dans $\mathbb{K}$ est dite *reconnaissable* s'il existe un entier $n \geqslant 0$, deux vecteurs $\lambda \in \mathbb{K}^{1\times n}$ et $\gamma \in \mathbb{K}^{n\times 1}$, et un morphisme de monoïdes $\mu : A^* \to \mathbb{K}^{n\times n}$ ($\mathbb{K}^{n\times n}$ monoïde pour la multiplication matricielle) tels que, pour tout $w \in A^*$, $\langle S,\ w\rangle = \lambda\mu(w)\gamma$. Le triplet $(\lambda,\ \mu,\ \gamma)$ est appelé *représentation* de S. L'entier n est appelé *rang* de la représentation $(\lambda,\ \mu,\ \gamma)$.

La série S de l'exemple précédent est reconnaissable ; il suffit de prendre la représentation linéaire de rang 2 suivante : $\lambda = \begin{bmatrix}1 & 0\end{bmatrix}$, μ définie par $\mu(a) = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ et $\mu(b) = \begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$, et $\gamma = \begin{bmatrix}0\\ 1\end{bmatrix}$.

Définition 11 (rang d'une série reconnaissable)**.** Soit S une série reconnaissable. Le *rang* de S, noté $rang(S)$, est le rang minimum des représentations linéaires de S.

La série de l'exemple précédent est de rang au plus 2 (puisqu'on en donne une représentation linéaire de rang 2). Elle ne peut pas être représentée par une représentation linéaire de rang 1, donc $rang(S) = 2$.

Théorème 6. *Si S est une série rationnelle sur A^* telle que $rang(S) \leqslant n$, et si $\forall w \in A^*,\ |w| \leqslant n-1 \Rightarrow \langle S,\ w\rangle = 0_{\mathbb{K}}$, alors $S = 0_{\mathbb{K}\langle\langle A\rangle\rangle}$.*

On remarque l'analogie avec un résultat sur les polynômes à une variable : un polynôme de degrés $n-1$ qui a n racines distinctes est nul.

Démonstration. Soit S une série rationnelle de rang n, telle que pour tout $w \in A^*$, si $|w| \leqslant n-1$, alors $\langle S,\ w\rangle = 0_{\mathbb{K}}$, et soit $(\lambda,\ \mu,\ \gamma)$ une réprésentation linéaire de S (avec les notations de la définition 10).

Si $\gamma = 0_{n,1}$, alors $S = 0_{\mathbb{K}\langle\langle A\rangle\rangle}$ et la démonstration est terminée. Sinon, la famille (γ) est de rang 1.

On raisonne par récurrence sur le rang de la famille $F_i = (\mu(w)\gamma)_{|w|\leqslant i}$. On vient de voir que $rang(F_0) = 1$. Soit $i \in \mathbb{N}$; comme $F_i \subseteq F_{i+1}$, $rang(F_i) \leqslant rang(F_{i+1})$. Si $rang(F_i) = rang(F_{i+1})$, alors $Vect(F_i) = Vect(F_{i+1})$. On a donc $\forall j \geqslant i,\ rang(F_i) = rang(F_j)$. En effet, pour toute lettre $a \in A$ et pour tout vecteur $x \in Vect(F_i)$, $\mu(a)x \in Vect(F_i)$, et donc par récurrence, pour tout mot $w = w_1...w_k \in A^*,\ \mu(w)x = \mu(w_1)...\mu(w_k)x \in Vect(F_i)$.

Comme le rang des familles F_i est strictement croissant avec i, jusqu'à être constant, majoré par n, il est maximal pour un $i_0 \leqslant n-1$. On a alors, pour tout $w \in A^*$, $\mu(w)\gamma \in Vect(F_{i_0})$. Or, pour tout $x \in F_{i_0}$, il existe un mot w, $|w| \leqslant n-1$, telle que $x = \mu(w)\gamma$. Donc $\lambda x = \langle S,\ w\rangle = 0_{\mathbb{K}}$. Donc pour tout $x \in Vect(F_{i_0}),\ \lambda x = 0_{\mathbb{K}}$.

Donc pour tout $w \in A^*$, $\lambda\mu(w)\gamma = \langle S,\ w\rangle = 0_{\mathbb{K}}$. Donc $S = 0_{\mathbb{K}\langle\langle A\rangle\rangle}$. □

2.3 Propriété d'être augmentable en termes de séries rationnelles

Propriété 7. *Soient $\mathcal{A} = (A,\ Q,\ \cdot)$, $P \subseteq Q$ et $w \in A^*$. Le mot w est un mot augmentant pour P si et seulement si $1_{1,Q}(M_w - I_{Q\times Q})I_P > 0$ (où $I_{Q\times Q}$ désigne la matrice identité de $\mathcal{M}_Q(\mathbb{Z})$).*

Démonstration. Par définition, w est un mot augmentant pour P ssi $card(P\cdot w^{-1}) > card(P)$. $I_{P\cdot w^{-1}} = M_w I_P$, et d'après le lemme 3, $card(P\cdot w^{-1}) = 1_{Q,1}\cdot M_w I_P = {}^t1_{Q,1}M_w I_P = 1_{1,Q}M_w I_P$, et $card(P) = 1_{Q,1}\cdot I_P = 1_{1,Q}I_P$. Donc :

$$\begin{aligned} w \text{ est un mot augmentant pour } P &\Leftrightarrow card(P\cdot w^{-1}) > card(P)\\ &\Leftrightarrow 1_{1,Q}M_w I_P > 1_{1,Q}I_P\\ &\Leftrightarrow 1_{1,Q}(M_w - I_{Q\times Q})I_P > 0 \end{aligned}$$

□

Soit $S_P \in \mathbb{Z}\langle\langle A\rangle\rangle$, définie par $\langle S_P, w\rangle = 1_{1,Q}(M_w - I_{Q\times Q})I_P$. La propriété 7 devient donc $card(P \cdot w^{-1}) > card(P) \Leftrightarrow \langle S_P, w\rangle > 0$.

Propriété 8. *La série S_P ainsi définie est reconnaissable.*

Démonstration. Avec les notations de la définition 10, il suffit de prendre, si $n = card(Q)$, $\lambda = \begin{bmatrix}1_{1,n} \mid -1_{1,n}\end{bmatrix}$, μ défini par $\forall w \in A$, $\mu(w) = \begin{bmatrix}M_w & 0_{n,n}\\ 0_{n,n} & I\end{bmatrix}$, et $\gamma = \begin{bmatrix}I_P\\ I_P\end{bmatrix}$. On vérifie aisément que $\mu(\epsilon) = I_{2n}$ et que $\forall u, v \in A^*$, $\mu(u)\mu(v) = \mu(uv)$: μ est donc bien un morphisme de monoïdes, et que $\forall w \in A^*$, $\langle S, w\rangle = \lambda\mu(w)\gamma$. □

Propriété 9. *Soient $\mathcal{A} = (A, Q, \cdot)$ et $P \subseteq Q$. La série $S_P \in \mathbb{Z}\langle\langle A\rangle\rangle$ définie comme précédemment est de rang au plus n.*

Démonstration. Le rang de la série S_P est majoré par le rang de la famille de vecteur $\lambda\mu(w)$, pour $w \in A^*$. Or $Vect(\lambda\mu(w)) = Vect((\begin{bmatrix}1_{1,n}M_w - 1_{1,n} \mid 0_{1,n}\end{bmatrix})_{w\in A^*} \cup (\begin{bmatrix}1_{1,n} \mid -1_{1,n}\end{bmatrix}))$. Donc $rang(S_P) \leqslant rang(V) + 1$, où $V = Vect((1_{1,n}(M_w - I_n))_{w\in A^*})$.

D'après le lemme 5, $\forall w \in A^*$, $M_w 1_{n,1} = 1_{n,1}$, donc ${}^t(1_{1,n}(M_w - I_n))\cdot 1_{n,1} = 1_{1,n}(M_w - I_n)1_{n,1} = 1_{1,n}(M_w - I_n)1_{n,1} = 0$. Donc $1_{1,n}(M_w - I_n)$ est orthogonal à $Vect(1_{n,1})$ pour tout $w \in A^*$, donc $dim(V) \leqslant n - 1$, et $rang(S_P) \leqslant n$. □

3 Borne quadratique sur la taille des mots synchronisants pour les automates circulaires

Définition 12 (automate circulaire)**.** Soient $\mathcal{A} = (A, Q, \cdot)$ automate à n états et $q \in Q$. L'automate $\mathcal{A}$ est dit *circulaire* s'il existe $a \in A$ tel que $\{q \cdot c^i,\ 1 \leqslant i \leqslant n\} = Q$.

En particulier, la matrice de transition M_a de la lettre a est une matrice de permutation.

L'automate de la figure 1.1 est un automate cirulaire : la lettre b produit une permutation des états. On observe que $M_b = \begin{bmatrix}0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0\end{bmatrix}$.

Propriété 10. *Un automate fini circulaire synchronisant à n états a un mot synchronisant de taille $2n^2 - 6n + 5$.*

Pour prouver cette propriété, on commence par montrer un lemme :

Lemme 11. *Soient $\mathcal{A} = (A, Q, \cdot)$ automate circulaire synchronisant, $a \in A$ une lettre qui induit une permutation des états de Q, P un ensemble strict de Q non vide. Alors $\sum_{i=0}^{n-1}\langle S_P, ua^i\rangle = 0$.*

Démonstration.

$$\begin{aligned}
\sum_{i=0}^{n-1}\langle S_P,\, ua^i\rangle &= \sum_{i=0}^{n-1} 1_{1,Q}(M_{ua^i} - I_{Q\times Q})I_P \\
&= \sum_{i=0}^{n-1} 1_{1,Q}(M_u M_{a^i} - I_{Q\times Q})I_P \\
&= \sum_{i=0}^{n-1} 1_{1,Q}M_u M_{a^i} I_P - 1_{1,Q}M_{a^i}I_P && (M_{a^i} \text{ matrice de permutation}) \\
&= \sum_{i=0}^{n-1} 1_{1,Q}(M_u - I_{Q\times Q})M_{a^i}I_P \\
&= 1_{1,Q}(M_u - I_{Q\times Q})\sum_{i=0}^{n-1} M_{a^i}I_P \\
&= card(P)1_{1,Q}(M_u - I_{Q\times Q})1_{Q,1} \\
&= 0 && (M_u 1_{Q,1} = 1_{Q,1} \text{ d'après le lemme 5})
\end{aligned}$$

□

Démonstration de la propriété 10. Soit $P \subset Q$, $P \neq \emptyset$ et $P \neq Q$.

Supposons que P ne soit pas $2(n-1)$-augmentable. Par contraposition de la propriété 7, pour tout $w \in A^*$ tel que $|w| \leqslant 2(n-1)$, $\langle S_P, w\rangle \leqslant 0$. Soit $u \in A^*$, $|u| \leqslant n-1$. $\forall i \in [\![0, n-1]\!]$, $\langle S_P, ua^i\rangle \leqslant 0$.

D'après le lemme 11, $\sum_{i=0}^{n-1}\langle S, ua^i\rangle = 0$, donc $\forall i \in [\![0, n-1]\!]$, $\langle S, ua^i\rangle = 0$. En particulier, pour $i = 0$, $\langle S, u\rangle = 0$.

Donc, $\forall u \in A^*$, $|u| \leqslant n-1 \Rightarrow \langle S, u\rangle = 0$. Donc d'après le théorème 6, $S_P = 0_{\mathbb{Z}\langle\langle A\rangle\rangle}$, *i.e.* $\forall w \in A^*$, $\langle S_P, w\rangle = 0$.

Or $\mathcal{A}$ est synchronisant, donc admet un mot w synchronisant, qui est un mot augmentant pour P, donc d'après la propriété 7 $\langle S_P, w\rangle > 0$. Contradiction.

Donc P est $2(n-1)$-augmentable. Comme d'après la propriété 2, il existe $q \in Q$ tel que $\{q\}$ est 1-augmentable.

Donc $\mathcal{A}$ admet un mot w de longueur au plus $1 + 2(n-1)(n-2)$ synchronisant. □

Références

[1] Marie-Pierre Béal, *A note on Černý's Conjecture and rational series*, 2003.

[2] J. Berstel et C. Reutenauer, *Les séries rationnelles et leurs langages*, Masson, 1984.

[3] L. Dubuc, *Sur les automates circulaires et la conjecture de Černý*, RAIRO Theoretical Informatics and Applications, 32 (1998), pages 21-34.

[4] Jacques Sakarovitch, *Éléments de théorie des automates*, Vuibert, 2003.