Option Informatique en Spé MP et MP*

Devoir à rendre après les vacances de Noël

Mots synchronisants d'un automate fini

Résumé

Un mot m est *synchronisant* pour un automate fini déterministe complet $\mathcal{A}$ si l'état $q \cdot m$ dans lequel on se trouve après lecture du mot m ne dépend pas de l'état q dans lequel on commence cette lecture.

Cette notion n'est pas que de pure théorie : lorsque l'on démarre un ordinateur, celui-ci se place dans un état particulier, toujours le même : ceci nous semble évident, mais pose des problèmes pratiques sérieux.

Nous étudierons quelques propriétés de l'ensemble des mots synchronisants d'un a.f.d.c.

En 1969, Černý a émis la conjecture suivante : si un a.f.d.c. à n états possède un mot synchronisant, alors il en possède un de longueur au plus $(n-1)^2$. Nous prouverons cette conjecture dans un cas particulier.

Veuillez rédiger chaque partie sur une copie séparée.

Table des matières

1 Mots synchronisants, automates synchronisables

▶ Dans tout le problème, Σ est un alphabet contenant au moins deux lettres. Soit $\mathcal{A} = (Q, \delta)$ un a.f.d.c. dont nous ne spécifions ni l'état initial, ni l'ensemble des états finals ; nous noterons $q \cdot m$ pour $\delta^*(q, m)$. Au mot $m \in \Sigma^*$, nous associons la fonction $\mathsf{m} : q \in Q \mapsto q \cdot m$; le *rang* de m est $\rho(m) = |\,\mathsf{m}(Q)|$.

Question 1 Existe-t-il des mots de rang nul ?

Question 2 Soient m_1 et m_2 deux mots ; notons $m = m_1 m_2$. Quelle relation existe-t-il entre les fonctions m_1, m_2 et m ?

Question 3 Soient u, v et m trois mots. Montrez que $\rho(umv) \leqslant \rho(m)$.

▶ Soit $m \in \Sigma^*$. Nous dirons que m est un mot *synchronisant* de $\mathcal{A}$ s'il est de rang 1, ce qui revient à dire que la fonction m est constante. $\mathcal{A}$ est *synchronisable* s'il admet au moins un mot synchronisant. Illustrons ces définitions par un exemple :

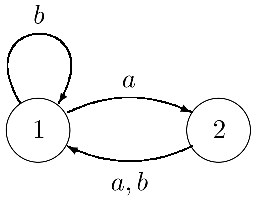

Figure 1: l'automate $\mathcal{A}_2$

b est un mot synchronisant de l'automate $\mathcal{A}_2$; c'est d'ailleurs le plus court. Nous noterons $\mathbf{S}(\mathcal{A})$ l'ensemble des mots synchronisants de l'automate $\mathcal{A}$.

Question 4 Déterminez $\mathbf{S}(\mathcal{A}_2)$.

▶ Soient $\mathcal{A}$ un automate et m un mot ; nous dirons que m est injectif pour $\mathcal{A}$ lorsque la fonction m l'est ; ceci revient à dire que $\rho(m) = n$. Clairement, ε est injectif. Pour l'automate $\mathcal{A}_2$, la lettre a est injective et la lettre b ne l'est pas.

Question 5 Soient $\mathcal{A}$ un automate synchronisable et m un mot synchronisant de $\mathcal{A}$, de longueur minimale. Montrez que ni la première lettre, ni la dernière lettre de m ne sont injectives pour $\mathcal{A}$.

Question 6 Quels sont les mots injectifs pour l'automate $\mathcal{A}_3$ ci-dessous ?

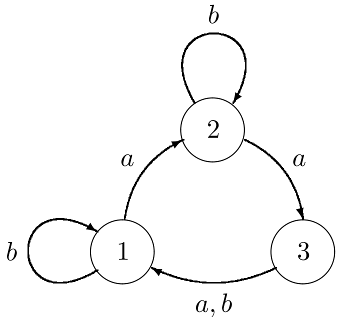

Figure 2: l'automate $\mathcal{A}_3$

Question 7 Montrez que l'automate $\mathcal{A}_3$ est synchronisable ; vous déterminez le(s) mot(s) synchronisants de longueur minimale de cet automate.

Question 8 Montrez que $\mathbf{S}(\mathcal{A}) = \Sigma^* \, \mathbf{S}(\mathcal{A}) \Sigma^*$.

Question 9 Soient s et t deux états de $\mathcal{A}$. Notons $L_{s \to t}$ le langage constitué des mot m tels que $s \cdot m = t$. Rappelez brièvement pourquoi $L_{s \to t}$ est rationnel.

Question 10 $\star$ Montrez que $\mathbf{S}(\mathcal{A})$ est rationnel.

Question 11 Supposons $\mathbf{S}(\mathcal{A})$ synchronisable. En observant l'action de m sur Q^n, montrez qu'il existe un mot synchronisant de longueur strictement inférieure à n^n.

Question 12 $\star\star$ Avec une autre action, améliorez le résultat précédent en montrant qu'il existe un mot synchronisant de longueur strictement inférieure à $2^n - n$.

2 Idéaux de Σ^*

▶ Un *idéal* de Σ^* est un langage L vérifiant $L = \Sigma^* L \Sigma^*$. Nous avons montré à la question 8 que $\mathbf{S}(\mathcal{A})$ est un idéal.

▶ Soient $L \subset \Sigma^*$ et $m \in L$. Nous dirons que m est *minimal* si aucun facteur de m (autre que m lui-même) n'appartient à L. Nous noterons $\mathcal{B}(L)$ l'ensemble des mots minimaux de L. Soit L un idéal de Σ^*.

Question 13 Montrez que L est vide ssi $\mathcal{B}(L)$ est vide.

Question 14 Montrez que $L = \Sigma^* \mathcal{B}(L) \Sigma^*$.

Question 15 Montrez que toute partie C de Σ^* telle que $L = \Sigma^* C \Sigma^*$ contient $\mathcal{B}(L)$.

▶ $\mathcal{B}(L)$ est donc la plus petite partie génératrice de L ; nous dirons que c'est la *base* de L. Nous dirons qu'un idéal est *de type fini* si sa base est finie.

Question 16 Justifiez rapidement l'affirmation suivante : tout idéal de type fini est rationnel.

Question 17 Exhibez un idéal rationnel qui ne soit pas de type fini.

Question 18 ⋆⋆ Exhibez un idéal non rationnel.

Question 19 Soient L et M deux idéaux de Σ^*. Le langage $L \cup M$ est-il un idéal de Σ^* ? Le langage $L \cdot M$ est-il un idéal de Σ^* ?

Question 20 Soit L un idéal de Σ^*. Donnez une condition nécessaire et suffisante pour que L^* soit un idéal de Σ^*.

3 Un peu d'algèbre (linéaire et bilinéaire)

▶ Le $\mathbb{R}$-e.v. $\mathbb{R}^n$ est muni du produit scalaire canonique ; le produit scalaire des vecteurs $\overrightarrow{u}$ et $\overrightarrow{v}$ sera noté $\overrightarrow{u} \cdot \overrightarrow{v}$ ou $\langle \overrightarrow{u} \mid \overrightarrow{v} \rangle$ selon le contexte. Nous identifierons les états de Q aux éléments de la base canonique de $\mathbb{R}^n$, que nous noterons $\mathcal{B} = (q_j)_{1 \leqslant j \leqslant n}$. Pour toute partie K de Q, nous noterons $\overrightarrow{K} = \sum_{q \in K} q$.

Question 21 Soient K_1 et K_2 deux parties de Q ; montrez que $|K_1 \cap K_2|$ est égal au produit scalaire $\langle \overrightarrow{K_1} \mid \overrightarrow{K_2} \rangle$.

▶ Soit $\sim$ une relation d'équivalence sur $\mathcal{B}$; notons $S_1, \ldots, S_r$ les classes modulo $\sim$: nous dirons que r est l'*index* de $\sim$.

Question 22 Soient $q \in Q$ et $i \in [\![1, r]\!]$. Montrez que $\langle q \mid \overrightarrow{S_i} \rangle$ est égal à 1 si q appartient à S_i, à 0 sinon.

Question 23 Montrez que la famille $\big(\overrightarrow{S_i}\big)_{1 \leqslant i \leqslant r}$ est libre.

▶ Notons F le s.e.v. de $\mathbb{R}^n$ engendré par la famille $\big(\overrightarrow{S_i}\big)_{1 \leqslant i \leqslant r}$; et G le s.e.v. de $\mathbb{R}^n$ engendré par les vecteurs $q_j - q_k$ tels que $q_j \sim q_k$.

Question 24 Justifiez l'affirmation suivante : si $q_j \sim q_k$, alors $q_j - q_k$ est orthogonal à chaque $\overrightarrow{S_i}$.

▶ Nous venons de montrer que les s.e.v. F et G sont orthogonaux.

Question 25 Montrez que tout élément de $\mathcal{B}$ est la somme d'un élément de F et d'un élément de G.

Question 26 Que pouvez-vous affirmer au sujet de deux s.e.v. F et G ?

▶ Soit $m \in \Sigma^*$; il existe un et un seul endomorphisme qui envoie chaque q_j sur $\mathsf{m}(q_j)$; nous le noterons m. Remarquons que $\rho(m)$ est aussi le rang de m.

Question 27 ⋆⋆ Soit $K \subset Q$. Montrez que $\overrightarrow{\mathsf{m}(K)} = \mathsf{m}\big(\overrightarrow{K}\big)$ ssi la restriction de m à K est injective.

▶ Soit $T = (t_i)_{1 \leqslant i \leqslant r}$ une famille de r éléments de Q. Nous dirons que T est un *transversal* de $\sim$ si T contient un et un seul élément de chaque classe modulo $\sim$.

Question 28 Montrez que T est un transversal de $\sim$ ssi $\langle \overrightarrow{T} \mid \overrightarrow{S_i} \rangle = 1$ pour tout $i \in [\![1, r]\!]$.

Question 29 Montrez que si $\mathsf{m}(T)$ est un transversal de $\sim$, alors T est lui aussi un transversal de $\sim$.

4 Un lemme à la façon de Moore

▶ Soient V un s.e.v. de $\mathbb{R}^n$ de dimension p et v un élément de V. Nous nous proposons d'établir le résultat suivant : si $\mathsf{m}(v)$ appartient à V pour tout mot m de longueur inférieure ou égale à p, alors $\mathsf{m}(v)$ appartient à V pour tout mot m.

Question 30 Réglez brièvement le cas où v est le vecteur nul.

▶ Nous supposons désormais v non nul. Notons W_i le s.e.v. de E engendré par l'ensemble des $\mathsf{m}(v)$, où m décrit l'ensemble des mots de longueur au plus i.

Question 31 Que pouvez-vous dire de W_0 ?

Question 32 Montrez que la suite $(\mathsf{W}_i)_{i\in\mathbb{N}}$ est croissante.

Question 33 Montrez que la suite $(\mathsf{W}_i)_{i\in\mathbb{N}}$ est stationnaire.

Question 34 Montrez que W_{i+1} est engendré par la réunion de W_i et de $\mathsf{W}_i \cdot\Sigma$.

Question 35 En déduire que, si $\mathsf{W}_{i+1} = \mathsf{W}_i$ pour un certain indice i, alors $\mathsf{W}_{i+k} = \mathsf{W}_i$ pour tout $k \in \mathbb{N}$.

Question 36 Montrez que la suite $(\mathsf{W}_i)_{0\leqslant i\leqslant p}$ ne peut être strictement croisante.

Question 37 Et maintenant, concluez !

Question 38 Soient V un s.e.v. de $\mathbb{R}^n$ de dimension p et v un vecteur n'appartenant pas à V ; notons $\mathcal{V}$ le sous-espace affine $v + \mathsf{V}$ de $\mathbb{R}^n$. En vous inspirant de la démarche qui vient d'être adoptée, établissez le résultat suivant : si $\mathsf{m}(v)$ appartient à $\mathcal{V}$ pour tout mot m de longueur inférieure ou égale à $p+1$, alors $\mathsf{m}(v)$ appartient à $\mathcal{V}$ pour tout mot m.

5 La conjecture de Černý dans un cas particulier

▶ Dans les deux questions suivantes, $\sim$ est une relation d'équivalence sur Q, d'index r.

Question 39 Soient q et q' deux éléments de Q. Montrez que si $\mathsf{m}(q) \sim \mathsf{m}(q')$ pour tout mot m de longueur inférieure ou égale à $n-r+1$, alors $\mathsf{m}(q) \sim \mathsf{m}(q')$ pour tout mot m.

Question 40 Soit Z une famille de r éléments de Q. Supposons que $\mathsf{m}(Z)$ est un transversal de $\sim$ pour tout mot m de longueur inférieure ou égale à $n-r+1$. Montrez que $\mathsf{m}(Z)$ est un transversal de $\sim$ pour tout mot m.

Question 41 Soit w un mot de rang au plus r. Montrez que s'il existe un mot de rang strictement inférieur à r, alors il existe un mot de rang strictement inférieur à r, et de longueur au plus égale à $2|w| + n - r + 1$.

Question 42 Supposons qu'il existe une lettre de rang $r < n$ et un mot de rang $k < r$. Montrez qu'il existe un mot de rang k et de longueur au plus égale à $(2^{r-k} - 1)(n - r + 1) + 2^{r-k+1} - (r - k + 1)$.

Question 43 En déduire que s'il existe une lettre de rang $r \leqslant 1 + \lg(n)$, alors il existe un mot synchronisant de longueur au plus $(n-1)^2$.

FIN