MPRI, Fondations mathématiques de la théorie des automates

Olivier Carton, Jean-Éric Pin

Examen du 6 février 2007. Durée: 1h 30, tous documents non électroniques autorisés

⋆ ⋆ ⋆

Avertissement : On attachera une grande importance à la clarté, à la précision et à la concision de la rédaction.

Partie 1: Une variété de monoïdes finis

Question 1. Montrer que les monoïdes finis apériodiques M tels que $es = se$ pour tout $e \in E(M)$ et tout $s \in M$ forment une variété de monoïdes, que l'on notera $\mathbf{U}$ dans la suite.

Question 2. Montrer que tout monoïde de $\mathbf{U}$ possède un zéro.

Question 3. Soit M un monoïde de $\mathbf{U}$ et soit $e \in E(M)$. Montrer que l'application $\alpha : M \to eM$ définie par $\alpha(s) = es$ est un morphisme de monoïdes. On note π la projection de M sur M/MeM. Montrer que l'application $\gamma : M \to eM \times (M/MeM)$ définie par $\gamma(s) = (\alpha(s), \pi(s))$ est un morphisme injectif.

Question 4. En déduire que la variété $\mathbf{U}$ est engendrée par les monoïdes de la forme S^1, où S est un semigroupe nilpotent. (Indication: on pourra raisonner par récurrence sur le nombre d'idempotents d'un monoïde de $\mathbf{U}$).

Question 5. On note $\mathcal{U}$ la variété de langages correspondant à $\mathbf{U}$. Montrer que pour tout alphabet A, $\mathcal{U}(A^*)$ est l'algèbre de Boole engendrée par les langages de la forme $B^*a_1B^*a_2B^* \cdots a_nB^*$ où $a_1, \ldots, a_n \in A \setminus B$.

Partie 2: Monoïde des parties

Soit S un semigroupe. On note $\mathcal{P}(S)$ le semigroupe des parties de S, muni du produit des parties: pour tout $X, Y \in \mathcal{P}(S)$,

$$XY = \{xy \mid x \in X \text{ et } y \in Y\}$$

Si $\varphi : M \to N$ est un morphisme de monoïdes, on note $\bar{\varphi} : \mathcal{P}(M) \to \mathcal{P}(N)$ le morphisme défini, pour tout $X \in \mathcal{P}(M)$, par $\bar{\varphi}(X) = \{\varphi(x) \mid x \in X\}$.

Question 6. Montrer que si S divise T, alors $\mathcal{P}(S)$ divise $\mathcal{P}(T)$.

On rappelle que dans un semigroupe fini, toute $\mathcal{J}$-classe maximale (pour l'ordre $\leqslant_{\mathcal{J}}$) est soit régulière, soit réduite à un seul élément.

Question 7. Soit S un semigroupe fini. Montrer qu'une partie de S est un idempotent de $\mathcal{P}(S)$ si et seulement si c'est un sous-semigroupe de S dont les $\mathcal{J}$-classes maximales sont régulières.

Question 8. Soit $T = \{e, t, 0\}$ le semigroupe défini par les relations $e^2 = e$, $et = t$, $te = t^2 = t0 = 0t = 00 = 0$. Calculer, dans $\mathcal{P}(T)$, les produits $\{e, 0\}\{e, t, 0\}$ et $\{e, t, 0\}\{e, 0\}$. En déduire que $\mathcal{P}(T)$ n'est pas $\mathcal{R}$-trivial.

Question 9. Soit M un monoïde fini et e un idempotent de M. Montrer que eM et eMe sont des idempotents de $\mathcal{P}(M)$. En déduire que si $\mathcal{P}(M)$ est $\mathcal{R}$-trivial, on a $eM = eMe$. En déduire également que pour tout idempotent $e \in M$ et pour tout $s \in M$, on a $ese = es$.

Question 10. Montrer que si $\mathcal{P}(M)$ est $\mathcal{J}$-trivial, alors $M \in \mathbf{U}$.

Partie 3: Substitutions et morphismes alphabétiques

Une substitution de A^* dans B^* est un morphisme de A^* dans $\mathcal{P}(B^*)$. Une substitution σ de A^* dans B^* est donc entièrement définie par la donnée des langages $\sigma(a)$ pour $a \in A$. On a ensuite, par définition, $\sigma(1) = 1$ et $\sigma(a_1 \cdots a_n) = \sigma(a_1) \cdots \sigma(a_n)$.

Question 11. Si L est un langage de B^*, on pose

$$\sigma^{-1}(L) = \{u \in A^* \mid \sigma(u) \cap L \neq \emptyset\}$$

Montrer que si L est reconnu par un morphisme $\eta : B^* \to M$, alors $\sigma^{-1}(L)$ est reconnu par le morphisme $\bar{\eta} \circ \sigma : A^* \to \mathcal{P}(M)$.

On dit qu'un morphisme $\varphi : A^* \to B^*$ est *alphabétique* si, pour tout $a \in A$, $\varphi(a) \in B$.

Question 12. Montrer qu'un morphisme $\varphi : A^* \to B^*$ est alphabétique si et seulement si il préserve la longueur des mots (i.e. si, pour tout $u \in A^*$, $|\varphi(u)| = |u|$). En déduire que φ^{-1} est alors une substitution de B^* dans A^* et que si L est reconnu par un monoïde M, $\varphi(L)$ est reconnu par $\mathcal{P}(M)$.

Question 13. Soit $\eta : A^* \to \mathcal{P}(M)$ un morphisme. Pour chaque $a \in A$, on pose $B_a = \eta(a)$ et on note B l'union disjointe[1] des ensembles B_a, pour $a \in A$. On note également φ le morphisme de B^* dans A^* défini par $\varphi(b) = a$ si $b \in B_a$. Montrer que pour chaque partie P de M, il existe un langage L de B^* reconnu par M tel que $\varphi(L) = \{u \in A^* \mid \eta(u) \cap P \neq \emptyset\}$.

Partie 4: Variétés de langages correspondant à PV

Soit $\mathbf{V}$ une variété de monoïdes et $\mathcal{V}$ la variété de langages correspondante. On note $\mathcal{W}$ la variété de langages correspondant à $\mathbf{PV}$.

Question 14. Montrer que tout langage de $\mathcal{W}(A^*)$ est combinaison booléenne de langages de la forme $\{u \in A^* \mid \eta(u) \cap P \neq \emptyset\}$, où $\eta : A^* \to \mathcal{P}(M)$ est un morphisme, M est un monoïde de $\mathbf{V}$ et P est une partie de M.

Question 15. Montrer que pour tout alphabet B, $\mathcal{W}(B^*)$ est l'algèbre de Boole engendrée par les langages de la forme $\varphi(L)$, où $\varphi : A^* \to B^*$ est un morphisme alphabétique et $L \in \mathcal{V}(A^*)$. Montrer que $\mathcal{W}(B^*)$ est aussi l'algèbre de Boole engendrée par les langages de la forme $\sigma^{-1}(L)$, où $\sigma : B^* \to A^*$ est une substitution et $L \in \mathcal{V}(A^*)$.

Question 16. Montrer que $\mathbf{J}$ est contenu dans $\mathbf{PU}$. (On peut démontrer en fait que $\mathbf{PU} = \mathbf{J}$).

[1] Les ensembles B_a ne sont pas en général disjoints, mais on prend ici leur union disjointe.

Corrigé

Partie 1: Une variété de monoïdes finis

Question 1. Ces monoïdes sont caractérisés par les identités $es = se$ et $x^\omega = x^{\omega+1}$ et forment donc une variété.

Question 2. On a $(es)(et) = e(se)t = e(es)t = (ee)st = est$, ce qui montre que α est un morphisme. La restriction de π à $M \setminus MeM$ est injective, et la restriction de α à MeM est l'identité (car si $s = uev$, on a $es = euev = ueev = uev = s$). Il en résulte que γ est injective. Par conséquent M divise $eM \times M/MeM$.

Question 3. Soit $M \in \mathbf{U}$. Comme M est apériodique, l'idéal minimal de M est constitué d'idempotents. Mais comme ces idempotents doivent commuter, il ne peut y en avoir qu'un seul, qui est donc un zéro.

Question 4. Notons $\mathbf{V}$ la variété engendrée par les monoïdes de la forme S^1 avec S nilpotent. Soit $M \in \mathbf{U}$. Montrons par récurrence sur $|E(M)|$ que $M \in \mathbf{V}$. Si $|E(M)| = 1$, M est le monoïde trivial puisque M est apériodique. Si $|E(M)| = 2$, $M \setminus \{1\}$ est un semigroupe nilpotent et $M \in \mathbf{V}$. Si $|E(M)| > 2$, il existe un idempotent e différent de 1 et de 0. Comme $1 \notin E(eM)$, on a $|E(eM)| < |E(M)|$. De même, puisque MeM contient 0 et e, on a $|E(MeM)| < |E(M)|$. Par hypothèse de récurrence, on a $eM, M/MeM \in \mathbf{V}$. Or comme M divise $eM \times M/MeM$, on a aussi $M \in \mathbf{V}$.

Question 5. Il résulte de la question 4 et du théorème des variétés que $\mathcal{U}(A^*)$ est l'algèbre de Boole engendrée par les langages reconnus par un morphisme $\varphi : A^* \to S^1$, où S est un semigroupe nilpotent. Soit donc P une partie de S^1. Quitte à passer au complémentaire, on peut supposer que $0 \notin P$. Posons $B = \{a \in A \mid \varphi(a) = 1\}$ et $C = A \setminus B$. Alors φ induit un morphisme de semigroupe $\tilde{\varphi} : C^+ \to S$ et comme S est nilpotent, $\tilde{\varphi}^{-1}(P)$ est un langage fini. Il en résulte que $\varphi^{-1}(P)$ est union finie de langages de la forme $B^*a_1B^*a_2B^* \cdots a_nB^*$ où $a_1, \ldots, a_n \in C$.

Partie 2: Monoïde des parties

Question 6. Supposons φ injectif et soient $X, Y \in \mathcal{P}(S)$. Si $\bar{\varphi}(X) = \bar{\varphi}(Y)$, alors, pour tout $x \in X$, il existe $y \in Y$ tel que $\varphi(x) = \varphi(y)$. Il en résulte que $y = x$ et donc $Y \subseteq X$. Dualement, $Y \subseteq X$ et donc $X = Y$. Donc $\bar{\varphi}$ est injectif.

Supposons φ surjectif. Alors, pour tout $X \in \mathcal{P}(T)$, on a $X = \bar{\varphi}(\bar{\varphi}^{-1}(X))$ et donc $\bar{\varphi}$ est surjectif. Par conséquent, si S divise T, $\mathcal{P}(S)$ divise $\mathcal{P}(T)$.

Question 7. Soit T un idempotent de $\mathcal{P}(S)$. Comme $T^2 = T$, T est un semigroupe. Soit J une $\mathcal{J}$-classe maximale de T. Si J n'est pas régulière, elle se réduit à un élément non régulier s et on a $s^2 <_{\mathcal{J}} s$. Par conséquent $s^2 \notin T$ et $T^2 \neq T$, contradiction. Donc toutes les $\mathcal{J}$-classes maximales de T sont régulières.

Réciproquement, si cette condition est vérifiée, il existe pour tout $t \in T$ un idempotent e tel que $e \leqslant_{\mathcal{J}} t$. On a donc $t = t_1et_2$ avec $t_1, t_2 \in T^1$. Comme $t_1e, et_2 \in T$, il vient $t \in T^2$ ce qui montre que $T \subseteq T^2$. Il en résulte que $T = T^2$ puisque T est un semigroupe.

Question 8. On a $\{e, 0\}\{e, t, 0\} = \{e, t, 0\}$ et $\{e, t, 0\}\{e, 0\} = \{e, 0\}$ et donc $\{e, 0\}\ \mathcal{R}\ \{e, t, 0\}$. Donc $\mathcal{P}(T)$ n'est pas $\mathcal{R}$-trivial.

Question 9. On a $eMeM \subseteq eM$. De plus, si $x \in eM$, on a $x = es$ et donc $x = e(es) \in eMeM$. donc $eMeM = eM$. Raisonnement analogue pour eMe. Or $eM(eMe) = eMe$ et $(eMe)eM = eMeM = eM$. Donc on a toujours $eM \mathrel{\mathcal{R}} eMe$ dans $\mathcal{P}(M)$. Si pM est $\mathcal{R}$-trivial, on a donc $eM = eMe$.

Soit $s \in M$ et $e \in E(M)$. Comme $es \in eM = eMe$, il existe $t \in M$ tel que $es = ete$. On a alors $ese = (ete)e = ete = es$.

Question 10. Si $\mathcal{P}(M)$ est $\mathcal{J}$-trivial, $\mathcal{P}(M)$ est à la fois $\mathcal{R}$-trivial et $\mathcal{L}$-trivial. On a donc $ese = es$ et dualement $ese = se$ pour tout $s \in M$ et $e \in E(M)$. Donc $es = se$ et finalement $M \in \mathbf{U}$.

Partie 3: Substitutions et morphismes alphabétiques

Question 11. Soit $P = \eta(L)$ et $Q = \{X \in \mathcal{P}(M) \mid X \cap P \neq \emptyset\}$. On a

$$(\bar{\eta} \circ \sigma)^{-1}(Q) = \{u \in A^* \mid \bar{\eta}(\sigma(u)) \in Q\} = \{u \in A^* \mid \sigma(u) \cap P \neq \emptyset\} = \sigma^{-1}(L)$$

Donc le morphisme $\bar{\eta} \circ \sigma : A^* \to \mathcal{P}(M)$ reconnaît $\sigma^{-1}(L)$.

Question 12. Si $\varphi : A^* \to B^*$ est un morphisme alphabétique, il préserve la longueur. Réciproquement, si un morphisme préserve la longueur, il envoie une lettre sur une lettre et il est donc alphabétique. En particulier, si $v \in \varphi^{-1}(u_1u_2)$, v se factorise en v_1v_2 avec $\varphi(u_1) = v_1$ et $\varphi(u_2) = v_2$. Par conséquent, $\varphi^{-1}(u_1)\varphi^{-1}(u_2) = \varphi^{-1}(u_1u_2)$ et comme $\varphi^{-1}(1) = 1$, φ^{-1} est une substitution.

Il résulte alors de la question précédente que si L est reconnu par un monoïde M, $\varphi(L)$ est reconnu par $\mathcal{P}(M)$.

Question 13. Soit $\gamma : B^* \to M$ le morphisme défini par $\gamma(b) = b$. Si $a \in A$, on a $\varphi^{-1}(a) = B_a$ et donc $\bar{\gamma} \circ \varphi^{-1}(a) = \eta(a)$. Par conséquent, $\bar{\gamma} \circ \varphi^{-1} = \eta$. Posons $L = \gamma^{-1}(P)$. Ce langage est reconnu par M et

$$\begin{aligned}
\varphi(L) = (\varphi^{-1})^{-1}(L) &= \{u \in A^* \mid \varphi^{-1}(u) \cap L \neq \emptyset\} \\
&= \{u \in A^* \mid \varphi^{-1}(u) \cap \gamma^{-1}(P) \neq \emptyset\} \\
&= \{u \in A^* \mid \bar{\gamma} \circ \varphi^{-1}(u) \cap P \neq \emptyset\} \\
&= \{u \in A^* \mid \eta(u) \cap P \neq \emptyset\}
\end{aligned}$$

Partie 4: Variétés de langages correspondant à PV

Question 14. Puisque $\mathbf{PV}$ est engendrée par les monoïdes de la forme $\mathcal{P}(M)$, où $M \in \mathbf{V}$, $\mathcal{W}(A^*)$ est l'algèbre de Boole engendrée par les langages de la forme $\eta^{-1}(R)$, où $\eta : A^* \to \mathcal{P}(M)$ est un morphisme et M est un monoïde de $\mathbf{V}$. Puisque $\eta^{-1}(R) = \cup_{X \in R}\, \eta^{-1}(X)$, on peut se ramener au cas où R est constitué d'un seul élément $P = \{s_1, \ldots, s_k\}$ de $\mathcal{P}(M)$. On a alors

$$\eta^{-1}(\{P\}) = \Big(\bigcap_{1 \leqslant i \leqslant k} \{u \in A^* \mid \eta(u) \cap \{s_i\} \neq \emptyset\} \Big) \setminus \{u \in A^* \mid \eta(u) \cap (M \setminus P) \neq \emptyset\}$$

Question 15. Notons $\mathcal{W}_1(A^*)$ (resp. $\mathcal{W}_2(A^*)$) l'algèbre de Boole engendrée par les langages de la forme $\varphi(L)$ (resp. $\sigma^{-1}(L)$), où $L \in \mathcal{V}(B^*)$ et $\varphi : B^* \to A^*$ est un morphisme alphabétique (resp. $\sigma : A^* \to B^*$ est une substitution).

Comme tout morphisme alphabétique peut s'écrire comme l'inverse d'une substitution, on a $\mathcal{W}_1(A^*) \subseteq \mathcal{W}_2(A^*)$. De plus, si L est reconnu par M, alors $\sigma^{-1}(L)$ est reconnu par $\mathcal{P}(M)$. Il en résulte que $\mathcal{W}_2(A^*) \subseteq \mathcal{W}(A^*)$.

Il reste à montrer l'inclusion $\mathcal{W}(A^*) \subseteq \mathcal{W}_1(A^*)$. Or d'après la question 14, il suffit de vérifier que les langages de la forme $\varphi(L) = \{u \in A^* \mid \eta(u) \cap P \neq \emptyset\}$ sont dans $\mathcal{W}_1(A^*)$. Or d'après la question 13, ces langages sont dans $\mathcal{W}_1(A^*)$, ce qui conclut la démonstration.

Question 16. Notons encore $\mathcal{W}$ la variété de langages correspondant à **PU**. Soient $a_1, \ldots, a_n \in A$. Soit $\bar{A}$ une copie de A et soit $B = \bar{A} \cup \{a_1, \ldots, a_n\}$. Soit enfin $\varphi : B^* \to A^*$ le morphisme alphabétique défini par $\varphi(\bar{a}) = a$ pour tout $a \in A$ et par $\varphi(a_i) = a_i$ pour $1 \leqslant i \leqslant k$. Comme le langage $L = \bar{A}^* a_1 \bar{A}^* a_2 \bar{A}^* \cdots a_n \bar{A}^*$ est dans $\mathcal{U}(\bar{A}^*)$, le langage $\varphi(L) = A^* a_1 A^* \cdots A^* a_n A^*$ est dans $\mathcal{W}(A^*)$. Par conséquent, $\mathcal{W}$ contient tous les langages testables par morceaux et donc **J** est contenu dans **PU**.