Corrigé de la feuille d'exercice 4

JB Angelelli

January 3, 2007

Exercice 2

Soient M,N deux monoïdes et $\varphi : M \to N$ un morphisme de monoïdes. Montrer que l'on définit une congruence $\equiv$ sur M en posant $x \equiv y$ si $\varphi(x) = \varphi(y)$.

Solution :

Il s'agit de démontrer que $\equiv$ est une congruence, c'est-à-dire une relation d'équivalence telle que si $x \equiv x'$ et $y \equiv y'$ alors $xy \equiv x'y'$. Ne pas oublier de démontrer que la relation est une équivalence.

- Réflexivité : $\forall x \in M$, on a $\varphi(x) = \varphi(x)$, donc $x \equiv x$.
- Symétrie : Supposons que $x \equiv y$, on a alors $\varphi(x) = \varphi(y)$, donc $\varphi(y) = \varphi(x)$, donc $y \equiv x$.
- Transitivité : Supposons que $x \equiv y$ et $y \equiv z$, alors $\varphi(x) = \varphi(y)$ et $\varphi(y) = \varphi(z)$, d'où $\varphi(x) = \varphi(z)$ donc $x \equiv z$.
- Congruence : Si $x \equiv x'$ et $y \equiv y'$, alors $\varphi(x) = \varphi(x')$ et $\varphi(y) = \varphi(y')$, d'où $\varphi(x)\varphi(y) = \varphi(x')\varphi(y')$, d'où $\varphi(xy) = \varphi(x'y')$ (car φ est un morphisme de monoïdes), et donc $xy \equiv x'y'$.

Exercice 4

Soit Σ un alphabet non vide. L'ordre préfixe $\sqsubseteq$ est défini sur Σ^* par $u \sqsubseteq v$ s'il existe un mot u' tel que $v = uu'$. Montrer que c'est une relation d'ordre sur Σ^*.

Réflexivité

$\forall u \in \Sigma^*, u = u\epsilon$ donc en posant $u' = \epsilon$ on a bien $uu' = u$, c'est à dire $u \sqsubseteq u$.

Antisymétrie

Supposons qu'on a $u \sqsubseteq v$ et $v \sqsubseteq u$. Il existe alors u' et v' tels que $uu' = v$ et $vv' = u$. Ce qui fait que $vv'u' = v$. En particulier la longueur de $vv'u'$ doit être égale à celle de v, c'est à dire $|vv'u'| = |v|$. Mais par définition on a

$|vv'u'| = |v| + |v'| + |u'|$, donc $|v'| + |u'| = 0$ et comme les longueurs sont des entiers positifs ou nuls on en déduit que $|v'| = |u'| = 0$. Or il n'y a qu'un seul mot de longueur nulle : le mot vide ; donc $v' = u' = \epsilon$. Comme $uu' = v$ et $u\epsilon = u$ (car ϵ est neutre pour la concaténation), on en déduit $u = v$.

Transitivité

Supposons qu'on a $u \sqsubseteq v \sqsubseteq w$. Il existe alors u' et v' tels que $v = uu'$ et $w = vv'$. Ce qui fait que $w = uu'v' = u(u'v')$ par associativité de la concaténation, d'où $u \sqsubseteq w$.

On a démontré que $\sqsubseteq$ est une relation d'ordre sur Σ^*.

Plus petit élément

$\forall u \in \Sigma^*$ on a $\epsilon u = u$, donc $\epsilon \sqsubseteq u$. Ce qui prouve que ϵ est le plus petit élément de Σ^* pour la relation $\sqsubseteq$.

Bornes inférieures

On rappelle que un mot u est défini par sa longueur $|u|$ sa fonction de lettres $\sigma_u : \{1, \ldots, |u|\} \mapsto \Sigma$.

Commençons par une remarque : si u est un préfixe de v alors on a :

- $|u| \leq |v|$;
- pour $0 < i \leq |u|$ on a $\sigma_u(i) = \sigma_v(i)$.

Ces deux propriétés sont conséquence immédiate du fait que $v = uu'$ pour un u' et de la définition de la concaténation.

Soient maintenant u et v deux mots quelconques. Remarquons que u et v ont au moins un préfixe commun, le mot vide, et que tout préfixe commun de u et de v est de longueur au plus égal à $\min(|u|, |v|)$. Autrement dit l'ensemble des préfixes communs de u et de v est non vide et fini. De plus il est totalement ordonné par la relation de préfixe : si x et y sont deux préfixes commun de u et de v alors on a soit $x \sqsubseteq y$, soit $y \sqsubseteq x$. En effet supposons par exemple que $|x| \leq |y|$. Comme x et y sont tous deux des préfixes communs de u et de v on a : $\sigma_u(i) = \sigma_v(i) = \sigma_x(i) = \sigma_y(i)$ pour $0 < i \leq |x|$. Donc x est un préfixe de y. Si par contre $|x| \not\leq |y|$ alors comme les longueurs sont des entiers on a $|y| \leq |x|$ (les entiers sont totalement ordonnés) et un raisonnement similaire montre que y est un préfixe de x.

Puisque les préfixes communs de u et de v sont en nombre fini (non nul) et qu'ils sont totalement ordonné par la relation préfixe, il y a un plus grand préfixe commun de u et de v. On a donc montré l'existence d'un borne inférieure de u et de v.

Bornes supérieures ?

Si Σ^* contient au moins deux lettres a et b alors les mots a et b (de longueur 1) ne peuvent être préfixe commun d'aucun mot. Ils n'ont donc aucun majorant commun, et a fortiori n'ont pas de borne supérieure. En fait on peut facilement se convaincre que deux mots u et v ont un majorant commun (c'est à dire sont préfixe commun d'un même mot) ssi l'un est préfixe de l'autre. Dans ce cas, mais seulement dans ce cas, ils ont une borne supérieure qui est le plus long des deux.

Exercice 5

Automate 1

$L = a^*(b(de)^* + b(de)^*d + c(ed)^* + c(ed)^*e)$

Automate 2

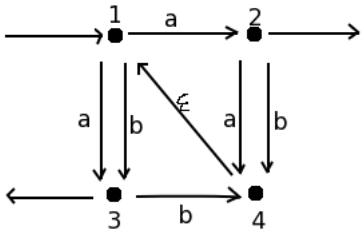
$L = u(v + w)^*(a + b)c^*d$

Automate 3

$L = (01)^*1((0 + 1)0^*1 + 0)$

Exercice 6

Afin de construire un automate détermiste, il faut d'abord numéroter les états, on obtient :

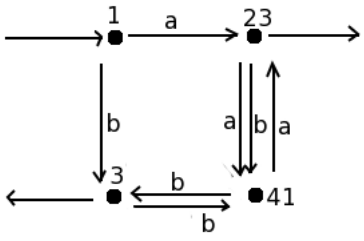


On vérifie que l'automate n'est pas déjà deterministe. Ici il n'est pas déterministe puisque deux flèches étiquetées par a partent de l'état 1. La présence de la *transition* ϵ montre également que l'automate n'est pas déterministe.

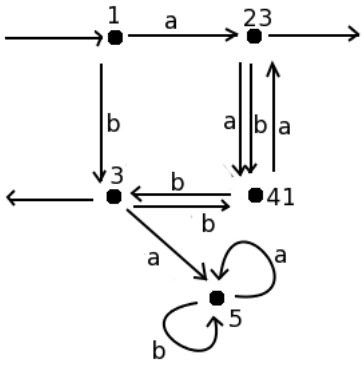
On construit un automate déterministe D dont les états correspondront à des sous-ensemble d'états de l'automate de départ non déterministe N. Le processus est le suivant :

- L'état initial de l'automate N est 1, on construit donc un état nommé 1 dans D. Il s'agira de l'état initial de D.
- Si on est en 1 dans D, ce qui correspond à être en 1 dans N, et on a la lettre a, on va en 2 ou en 3. On ajoute donc dans D un état nommé "23" et une flèche a de 1 vers 23.
- Si on est en 1 dans D, ce qui correspond à être en 1 dans N, et on a la lettre b, on va en 3. On ajoute donc dans D un état nommé "3" et une flèche b de 1 vers 3. ATTENTION : ne pas considérer que 3 est inclus dans 23, il s'agit bien de deux états différents.
- Si on est en 23 dans D, ce qui correspond à être en 2 ou en 3 dans N, et on a la lettre a, on va en 4, donc également en 1 grâce à la transition ϵ de 4 vers 1, on arrive donc en 4 ou 1. On ajoute donc à D un état nommé "41" et une flèche a de 23 vers 41.
- Si on est en 23 dans D, ce qui correspond à être en 2 ou en 3 dans N, et on a la lettre b, on va en 4, donc également en 1 grâce à la transition ϵ de 4 vers 1, on arrive donc en 4 ou 1. On ajoute donc à D une flèche b de 23 vers 41.
- Si on est en 41 dans D, ce qui correspond à être en 4 ou en 1 dans N, et on la lettre a, on va en 2 ou en 3, on ajoute donc à D une flèche b de 41 vers 23.
- Si on est en 41 dans D, ce qui correspond à être en 4 ou en 1 dans N, et on la lettre b, on va en 3, on ajoute donc à D une flèche b de 41 vers 3.
- Si on est en 3 dans D, ce qui correspond à être en 3 dans N, et on a la lettre a, il ne se passe rien, si on a la lettre b, on va en 4, donc également en 1 grâce à la transition ϵ de 4 vers 1, on arrive donc en 4 ou 1. On ajoute donc à D une flèche b de 3 vers 41.
- Les sorties de D sont des états qui correspondent à au moins une sortie dans N. Ici, les sorties de D sont donc les états 23 et 3.

On obtient donc l'automate suivant :



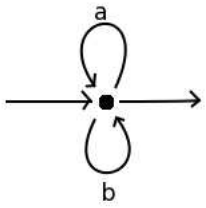
On peut vérifier facilement que D est bien déterministe, aucun état n'a plus d'une flèche partant de l'état avec la même lettre. Par contre il n'est pas complet puisqu'il ne part aucune flèche a de 3. On le complète en rajoutant un état "5" dit piège et une flèche a de 3 vers 5. On rajoute également deux flèches boucles a et b de 5 vers 5 afin que l'automate soit complet. On obtient l'automate complet déterministe suivant :



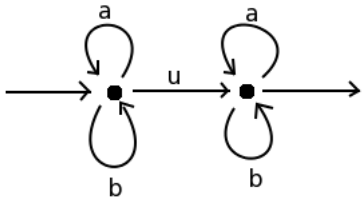
Exercice 7

On fixe l'alphabet $\Sigma = \{a, b\}$. Construire des automates reconnaissant les langages suivants :

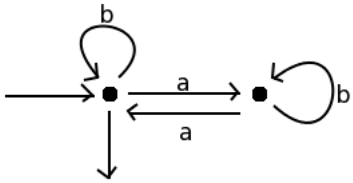
1. $L_1 = \Sigma^*$.



2. $L_2 = \Sigma^* u \Sigma^*$, où u est un mot de Σ^*fixé.

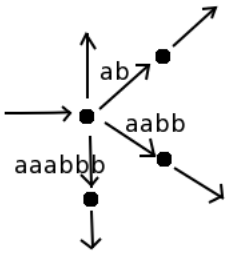


3. L_3 est l'ensemble des mots u de Σ^* qui contiennent un nombre pair de fois la lettre a.



4. $L_4 = \{a^k b^k, 0 \leq k \leq 3\}$.

   L_4est un langage fini. Il n'a que 4 mots, $L_4 = \{\epsilon, ab, aabb, aaabbb\}$. Il existe donc l'automate trivial suivant :

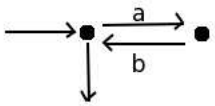


Exercice 8

On considère l'alphabet $\{a, b\}$. Dire si les langages suivants sont réguliers ou non :

1. Le langage $L_5 = \{(ab)^k, k \in \mathbb{N}\}$.

   Ce langage est reconnu par l'automate suivant :



   Il est donc automatique donc régulier.

2. Le langage $L_6 = \{a^k b^k, k \in \mathbb{N}\}$.

   On rappelle l'énoncé du lemme de pompage : si L_6 est régulier alors il existe un entier M tel que pour tout mot $u \in L_6$, si $|u| \geq M$ alors u se décompose en $u = u_1u_2u3$ où $|u_1u_2| \leq M$, $|u_2| > 0$ et pour tout n, $u_1u_2^nu_3 \in L_6$.

   Soit u un mot quelconque de L_6. On va montrer que quel que soit le choix de u_1, u_2 et u_3 vérifiant $u = u_1u_2u_3$ et $|u_2| > 0$, il y a toujours au moins un entier n tel que $u_1u_2^nu_3 \notin L_6$. On aura ainsi contredit le lemme de pompage et donc démontré que L_6 n'est pas régulier. Par commodité on note p_1, p_2 et p_3 les longueurs respectives de u_1, u_2 et u_3.

   Comme $u \in L_6$, on sait qu'il existe un k tel que $u = a^kb^k$. Il y a trois possibilités :

   (a) si $p_1 + p_2 \leq k$ alors comme $u_1u_2u_3 = a^kb^k$, on a $u_1 = a^{p_1}$, $u_2 = a^{p_2}$ et $u_3 = a^{k-p_1-p_2}b^k$. Donc $u_1u_2^nu_3 = a^{p_1}a^{np_2}a^{k-p_1-p_2}b^k$. En particulier pour $n = 0$, $u_1u_2^nu_3 = a^{p_1}a^{k-p_1-p_2}b^k = a^{k-p_2}b^k$. Comme $p_2 > 0$ on a bien $u_1u_2^nu_3 \notin L_6$ pour $n = 0$.

   (b) si $p_1 + p_2 > k$ et $p_1 < k$ alors $u_1 = a^{p_1}$, $u_2 = a^{k-p_1}b^{k-p_3}$ et $u_3 = b^{p_3}$. Donc $u_1u_2^nu_3 = a^{p_1}(a^{k-p_1}b^{k-p_3})^nb^{p_3}$. En particulier pour $n = 2$ on obtient $u_1u_2^nu_3 = a^{p_1}a^{k-p_1}b^{k-p_3}a^{k-p_1}b^{k-p_3}b^{p_3} = a^kb^{k-p_3}a^{k-p_1}b^k$ et comme $k - p_1 > 0$ on voit une fois de plus que $u_1u_2^nu_3 \notin L_6$ pour $n = 2$.

   (c) si $p_1 + p_2 > k$ et $p_1 \geq k$ alors on est dans une situation symétrique du premier cas et on voit de même que $u_1u_2^0u_3 \notin L_6$.

   Dans les trois cas on a donc trouvé un n tel que $u_1u_2^nu_3 \notin L_6$.

Exercice 9

Dire si l'implication suivante est vraie ou non : si L est un langage régulier et L' est un sous-langage de L, alors L' est alors régulier.

Solution :

Considérons l'alphabet $\Sigma = \{a, b\}$ et posons $L = \Sigma^*$. Alors L est régulier puisqu'il correspond à l'expression régulière $(a+b)^*$. Si l'implication était vraie, tout sous-langage L' de L, c'est à dire tout langage L' sur l'alphabet Σ, serait régulier, ce qui est faux. Par exemple $L' = \{a^k b^k, k \in \mathbb{N}\}$ n'est pas régulier d'après l'exercice 8.

Exercice 10

On considère l'ensemble des a^p où p est un nombre premier. Est-ce un langage régulier ?

Solution :

Notons P ce langage. On va encore contredire le lemme de pompage. Pour cela il suffit de montrer que pour tout M, il existe un $u \in P$ tel que $|u| \geq M$ et pour tout u_1, u_2, u_3 tels que $|u_1 u_2| \leq M$, $|u_2| > 0$ et $u = u_1 u_2 u_3$, il existe un k tel que $u_1 u_2^k u_3 \notin P$.

Soit donc M un entier quelconque. Comme il y a une infinité de nombres premiers on peut en trouver un plus grand que $2(M+1)$. Notons le p. On a donc $u = a^p \in P$. Soient u_1, u_2, u_3 tels que $|u_1 u_2| \leq M$, $|u_2| > 0$ et $u = u_1 u_2 u_3$. Notons p_1, p_2 et p_3 les longueurs respectives de u_1, u_2 et u_3. Comme $u = a^p$ on a donc $u_i = a^{p_i}$ pour $i = 1, 2, 3$ et $p = p_1 + p_2 + p_3$. De plus $p_1 + p_2 \leq M$ et $p \geq 2(M+1)$ donc $p_3 > M + 1$.

Il s'agit maintenant de trouver un k tel que $u_1 u_2^k u_3 \notin P$ c'est à dire tel que $p_1 + kp_2 + p_3$ ne soit pas premier. Prenons $k = p_1 + p_3$; alors $p_1 + kp_2 + p_3 = (p_1 + p_3)(1 + p_2)$. Comme $p_2 > 0$, $1 + p_2 \geq 2$ et comme $p_3 > M + 1$, $p_1 + p_3 \geq 2$. Donc $p_1 + kp_2 + p_3$ est un produit de deux entiers plus grands que 2, et n'est donc pas premier.

Le lemme de pompage ne s'applique donc pas au langage P qui n'est donc pas régulier.