Université Sultan Moulay Slimane
Ecole National des Sciences Appliquées
Khouribga

Théorie de la calculabilité et de la complexité

4ème Année Génie informatique
Semestre 4 / Année 2018/2019
Corrigés de TD N° 1

Exercice 1

Soit l'alphabet $\Sigma = \{a, b\}$. Donner en extension les langages suivants sur Σ :

1. $L_1 = \{w \in \Sigma^* \mid |w| = 3\}$.

   Réponse :

   $L_1 = \{aaa, aab, aba, abb, baa, bab, bba, bbb\}$

2. $L_2 = \{w \in \Sigma^* \mid |w| = 4 \text{ et } |w|_a = |w|_b\}$. La notation $|w|_a$ signifie le nombre d'occurrence du symbole a dans le mot w.

   Réponse :

   $L_2 = \{aabb, abab, abba, baab, baba, bbaa\}$

3. $L_3 = \{w \in \Sigma^* \mid |w| = 5 \text{ et } w^R = w\}$.

   Réponse :

   $L_3 = \{aaaaa, ababa, baaab, bbabb, aabaa, abbba, babab, bbbbb\}$

Exercice 2

Soient Σ un alphabet arbitraire et w un mot sur Σ.

- Un **facteur** de w est un mot y qui apparaît dans w, c'est-à-dire qu'il existe deux mots x et z tel que $w = xyz$.
- Un **préfixe** (ou **facteur gauche**) de w est un mot x qui débute w, c'est-à-dire qu'il existe un mot y tel que $w = xy$.
- Un **suffixe** (ou **facteur droit**) de w est un mot y qui termine w, c'est-à-dire qu'il existe un mot x tel que $w = xy$.
- Un **sous-mot** de w est un mot obtenu à partir de w en effaçant certains symboles de w.

1. Vérifier que ε est facteur, préfixe, suffixe et sous-mot de tout mot w.

Réponse :

- $w = w\cdot\varepsilon\cdot\varepsilon = \varepsilon\cdot w = w\cdot\varepsilon$. Cela montre que ε est un facteur, préfixe et suffixe de w.
- On obtient ε en effaçant tous les symboles de w ➔ ε est un sous-mot de w.

2. Vérifier que tout mot w est facteur, préfixe, suffixe et sous-mot de lui-même.

   Réponse :

   - $w = \varepsilon\cdot w\cdot\varepsilon = w\cdot\varepsilon = \varepsilon\cdot w$. Cela montre que w est un facteur, préfixe et suffixe de lui-même.
   - On obtient w en supprimant 0 symboles de w ➔ w est un sous-mot de lui-même.

On appelle **facteur propre** (respectivement **préfixe propre**, **suffixe propre**, **sous-mot propre**) d'un mot w, tout facteur (respectivement préfixe, suffixe, sous-mot) de w qui est différent de ε *et* w.

Soit $w = abcbaccba$ sur l'alphabet $\Sigma = \{a, b, c\}$.

3. Calculer $|w|$, $|w|_a$, $|w|_b$ et $|w|_{cba}$.

   Réponse :

   $|w| = |abcbaccba| = 9$.

   $|w|_a = |abcbaccba|_a = 3$.

   $|w|_b = |abcbaccba|_b = 3$.

   $|w|_{cba} = |abcbaccba|_{cba} = 2$.

4. Déterminer w^0, w^1, w^2 et w^R. Le mot w est-t-il un palindrome ?

   Réponse :

   - $w^0 = \varepsilon$ (par convention).
   - $w^1 = w = abcbaccba$.
   - $w^2 = ww = abcbaccbaabcbaccba$.
   - $w^R = (abcbaccba)^R = abccabcba$.
   - w n'est pas un palindrome, puisque $w^R \neq w$.

5. Déterminer tous les facteurs, préfixes et suffixes propres de w.

   Réponse :

Les facteurs propres de w sont : a, b, c, ab, ac, ba, bc, cb, cc, abc, acc, bac, bcb, cba, ccb, $abcb$, $accb$, $bacc$, $bcba$, $cbac$, $ccba$, $abcba$, $accba$, $baccb$, $bcbac$, $cbacc$, $abcbac$, $baccba$, $bcbacc$, $cbaccb$, $abcbacc$, $bcbaccb$, $cbaccba$, $abcbaccb$, $bcbaccba$.

Les préfixes propres de w sont : a, ab, abc, $abcb$, $abcba$, $abcbac$, $abcbacc$, $abcbaccb$.

Les suffixes propres de w sont : a, ba, cba, $ccba$, $accba$, $baccba$, $cbaccba$, $bcbaccba$.

6. Déterminer tous les sous-mots propres de w de longueur ≤ 4.

Réponse :

Les sous-mots de w de longueur ≤ 4 sont (ordonnés par longueur et par ordre lexicographique)

ε, a, b, c, aa, ab, ac, ba, bb, bc, ca, cb, cc, aaa, aab, aac, aba, abb, abc, aca, acb, acc, baa, bab, bac, bba, bbb, bbc, bca, bcb, bcc, caa, cab, cac, cba, cbb, cbc, cca, ccb, ccc,$aaba$, $aaca$, $aacb$, $aacc$, $abaa$, $abab$, $abac$, $abba$, $abbb$, $abbc$, $abca$, $abcb$, $abcc$, $acaa$, $acab$, $acac$, $acba$, $acbb$, $acbc$, $acca$, $accb$, $accc$, $baba$, $baca$, $bacb$, $bacc$, $bbaa$, $bbab$, $bbac$, $bbba$, $bbca$, $bbcb$, $bbcc$, $bcaa$, $bcab$, $bcac$, $bcba$, $bcbb$, $bcbc$, $bcca$, $bccb$, $bccc$, $caba$, $caca$, $cacb$, $cacc$, $cbaa$, $cbab$, $cbac$, $cbba$, $cbca$, $cbcb$, $cbcc$, $ccba$, $ccca$, $cccb$.

Exercice 3

Soient K, L et M des langages définis sur un même alphabet Σ. Prouver les propriétés suivantes :

1. $K \subseteq L \Rightarrow MK \subseteq ML$. La réciproque est-elle vraie ?

Réponse :

$$w \in MK \Leftrightarrow w = xy, \text{ avec } x \in M \text{ et } y \in K.$$

$$w \in MK \Rightarrow w = xy, \text{ avec } x \in M \text{ et } y \in L, \text{ puisque } K \subseteq L.$$

$$w \in MK \Rightarrow w \in ML.$$

Par suite, $MK \subseteq ML$.

- La réciproque n'est pas vraie, comme le montre le contre-exemple suivant :

  $M = \{\varepsilon, b\}$, $K = \{bc\}$, et $L = \{c, bbc\}$.

  $MK = \{bc, bbc\}$, et $ML = \{c, bc, bbc, bbbc\}$.

On a bien $MK \subseteq ML$, mais $K \not\subset L$.

2. $K \subseteq L \Rightarrow KM \subseteq LM$. La réciproque est-elle vraie ?

Réponse :

$$w \in KM \Leftrightarrow w = xy, \text{ avec } x \in K \text{ et } y \in M.$$

$$w \in KM \Rightarrow w = xy, \text{ avec } x \in L \text{ et } y \in M, \text{ puisque } K \subseteq L.$$

$$w \in KM \Rightarrow w \in LM.$$

Par suite, $KM \subseteq LM$.

- La réciproque n'est pas vraie, comme le montre le contre-exemple suivant :

  $M = \{\varepsilon, b\}$, $K = \{cb\}$, et $L = \{c, cbb\}$.

  $KM = \{cb, cbb\}$, et $LM = \{c, cb, cbb, cbbb\}$.

  On a bien $KM \subseteq LM$, mais $K \not\subset L$.

3. $K \subseteq L \Rightarrow K^* \subseteq L^*$.

Réponse :

- Il est clair que si $K \subseteq K'$ et $L \subseteq L'$, alors $KK' \subseteq LL'$. Par conséquent, si $K \subseteq L$, alors $K^2 = KK \subseteq LL = L^2$. En appliquant cette règle n fois, il vient que $K^n \subseteq L^n$, pour tout entier n (pour $n = 0$, $K^0 = L^0 = \{\varepsilon\}$).
- Soit maintenant un mot $w \in K^*$. Comme $K^* = \bigcup_{i=0}^{\infty} K^i$, alors il existe un entier naturel $i \geq 0$, pour lequel on a : $w \in K^i$. D'après ce qui précède, $w \in L^i$. Par suite, $w \in L^*$.

4. $(L^*)^* = L^*$.

Réponse :

- Tout d'abord, comme $L \subseteq L^*$, pour tout langage L, alors $L^* \subseteq (L^*)^*$.
- Soit maintenant un mot $w \in (L^*)^*$. Il existe un entier naturel $i \geq 0$ pour lequel on a : $w \in (L^*)^i$. Si $i = 0$, alors $w = \varepsilon \in L^*$. Sinon, $w = x_1x_2\ldots x_i$, avec $x_i \in L^*$. Chaque sous-mot x_i est la concaténation d'un nombre fini de mots de L. Par suite, w est lui-même concaténation d'un nombre fini de mots de L, ce qui prouve que $w \in L^*$.

5. $K^* \cup L^* \subseteq (K \cup L)^*$. La réciproque est-elle vraie ?

Réponse :

- On sait que : $K \subseteq (K \cup L)$ et $L \subseteq (K \cup L)$. Donc, $K^* \subseteq (K \cup L)^*$ et $L^* \subseteq (K \cup L)^*$. Par conséquent, $K^* \cup L^* \subseteq (K \cup L)^*$.
- La réciproque est fausse. Voici un contre-exemple : $K = \{a\}$ et $L = \{b\}$. On a : $K^* = \{\varepsilon, a, aa, aaa, \ldots\} = \{a^n \mid n \geq 0\}$ et $L^* = \{\varepsilon, b, b, bbb, \ldots\} = \{b^n \mid n \geq 0\}$. Mais, $(K \cup L)^* = \{\varepsilon, a, b, aa, ab, ba, bb, aaa, aab, \ldots\}$ contient par exemple le mot $ab \notin K^* \cup L^*$.

6. $L^+ = LL^* = L^*L$.

Réponse :

- Rappelons que : $L^+ = \bigcup_{i=1}^{\infty} L^i$. Soit w un mot de L^+. Par définition, il existe un entier naturel $i \geq 1$, tel que $w \in L^i = LL^{i\text{-}1}$. Or, $L^{i\text{-}1} \subseteq L^*$, car l'indice de la puissance $L^{i\text{-}1}$ est tel que $i - 1 \geq 0$. Par conséquent, $w \in LL^*$.
- Soit w un mot de LL^*. Par définition, il existe deux mots $x \in L$ et $y \in L^*$ tels que $= xy$. Comme $y \in L^*$, alors il existe un indice $i \geq 0$, tel que $y \in L^i$. Par suite, $w = xy \in LL^i = L^k$, avec $k = i + 1 \geq 1$. Par conséquent, $w \in L^+$.
- La preuve est identique pour $L^*L = L^+$.

7. $L^+ = L^* \Leftrightarrow \varepsilon \in L$. Sous quelle condition a-t-on $L^+ = L \setminus \{\varepsilon\}$?

Réponse :

- Si $L^+ = L^*$, alors le mot vide $\varepsilon \in L^+$. Il existe un indice $i \geq 1$, tel que $\varepsilon \in L^i$. Alors : $\varepsilon = x_1x_2\ldots x_i$, avec $x_j \in L$, $(\forall j)$. Forcément, $x_1 = x_1 = \ldots = x_1 = \varepsilon$. D'où $\varepsilon \in L$.
- Si $\varepsilon \in L$. Alors, $L = \{\varepsilon\} \cup L$. Donc, $L^+ = \bigcup_{i=1}^{\infty} L^i = L \cup L^2 \cup \ldots = \{\varepsilon\} \cup L \cup L^2 \cup \ldots = L^*$.
- On aura $L^+ = L \setminus \{\varepsilon\}$, si et seulement si $\varepsilon \notin L$.

8. $L \subseteq L^2 \Leftrightarrow \varepsilon \in L$.

Réponse :

- [$\Leftarrow$] Supposons que $\varepsilon \in L$. Cela signifie que $\{\varepsilon\} \subseteq L$. Par suite, $L = L\{\varepsilon\} \subseteq LL = L^2$.
- [$\Rightarrow$] Supposons que $L \subseteq L^2$. Soit w un mot de L de longueur minimale (w est l'un des mots les plus courts de L). Un tel mot existe bel et bien, puisque l'ensemble $\{|w| \mid w \in L\}$ est une partie minorée de IN, donc elle

admet un plus petit élément. Par hypothèse, $w \in L^2$. Par suite, $w = xy$ où x, y sont deux mots de L. Nous avons alors : $|w| = |x| + |y| \geq |w| + |w| = 2|w|$. On aura donc : $0 \geq |w| \geq 0 \Rightarrow |w| = 0 \Rightarrow w = \varepsilon$.

Exercice 4

1. Donner une définition récursive de l'image (ou le renversé) d'un mot w défini sur un alphabet arbitraire Σ.

   Réponse :

   Une définition récursive de w^R est la suivante :

$$\boxed{w^R = \begin{cases} \varepsilon;\ si\ |w| = 0 \\ au^R;\ si\ w = ua,\ a \in \Sigma,\ u \in \Sigma^* \end{cases}}$$

2. En utilisant cette définition récursive, démontrer les propriétés suivantes :

   a. $(xy)^R = y^R x^R$

   Réponse :

   Preuve par récurrence sur la longueur $|y| = n$ du mot $y \in \Sigma^*$.

- **Cas de base** : si $n = 0$, alors $y = \varepsilon$, et $(xy)^R = (x\varepsilon)^R = x^R = \varepsilon^R x^R = y^R x^R$.

  Hypothèse de récurrence : si $|y| = n \geq 0$, alors : $(xy)^R = y^R x^R$.

- **Cas indictif** : soit $y \in \Sigma^*$ tel que $|y| = n + 1$. Alors, $y = ua$, où $u \in \Sigma^*$, $|u| = n$ et $a \in \Sigma$. On a :

$$\begin{aligned}
(xy)^R &= (x(ua))^R && [y = ua] \\
&= ((xu)a)^R && [\text{Par associativité de la concaténation}] \\
&= a(xu)^R && [\text{Par définition récursive de } R] \\
&= a(u^R x^R) && [\text{Par hypothèse de récurrence}] \\
&= (au^R)x^R && [\text{Par associativité de la concaténation}] \\
&= ((ua)^R)x^R && [\text{Par définition récursive de } R] \\
&= y^R x^R && [y = ua]
\end{aligned}$$

   b. $(w^R)^R = w$.

   Réponse :

   Preuve par récurrence sur la longueur $|w| = n$ du mot $w \in \Sigma^*$.

- **Cas de base** : si $n = 0$, alors $w = \varepsilon$. On a : $(w^R)^R = (\varepsilon^R)^R = \varepsilon^R = \varepsilon = w$.

  Hypothèse de récurrence : si $|w| = n \geq 0$, alors : $(w^R)^R = w$.

- **Cas indictif** : soit $w \in \Sigma^*$ tel que $|w| = n + 1$. Alors, $w = ua$, où $u \in \Sigma^*$, $|u| = n$ et $a \in \Sigma$. On a :

$$
\begin{aligned}
(w^R)^R &= ((ua)^R)^R && [w = ua] \\
&= (au^R)^R && [\text{Par définition récursive de } R] \\
&= (u^R)^R a^R && [\text{D'après la question précédente}] \\
&= (u^R)^R a && [a^R = (\varepsilon a)^R = a\varepsilon^R = a,\ a \text{ est un symbole}] \\
&= ua && [\text{Par hypothèse de récurrence}] \\
&= w && [w = ua]
\end{aligned}
$$

c. Si x est un sous-mot de w, alors x^R est un sous-mot de w^R.

Réponse :

Preuve par récurrence sur la longueur $|w| = n$ du mot $w \in \Sigma^*$.

- **Cas de base** : si $n = 0$, alors $w = \varepsilon$. Il y'a un seul sous-mot de w : ε. Or, $\varepsilon^R = \varepsilon$. Donc, ε^R est un sous-mot de w^R.

Hypothèse de récurrence : si $|w| = n \geq 0$, pour tout sous-mot x de w, x^R est un sous-mot de w^R.

- **Cas indictif** : soit $w \in \Sigma^*$ tel que $|w| = n + 1$. Alors, $w = ua$, où $u \in \Sigma^*$, $|u| = n$ et $a \in \Sigma$. Soit x un sous-mot de w. Il y a deux cas
  - ✓ Si $|x| = 0$, alors $x = x^R = \varepsilon$, donc x^R est un sous-mot de w^R (puisque ε est sous-mot de n'importe quel mot).
  - ✓ Si $|x| = n + 1$, alors $x = w$ et $x^R = w^R$, donc x^R est un sous-mot de w^R (puisque tout mot est sous-mot de lui-même).
  - ✓ Si x est un sous-mot propre de w. Alors $1 \leq |x| \leq n$. Il y a trois cas :
    - ☞ x est un sous-mot de u et $0 \leq |u| \leq n$. On a : $w^R = au^R$. Par hypothèse de récurrence, x^R est un sous-mot de u^R (qui est un sous-mot de au^R). Donc, x^R est aussi un sous-mot de $au^R = w^R$, par transitivité de la relation « être sous-mot de ».
    - ☞ $x = a$ et x est obtenu en effaçant le préfixe u de w. Alors, $x^R = a$ qui est un sous-mot de $w^R = au^R$, obtenu en supprimant le suffixe au^R de w^R.
    - ☞ $x = ya$, où y est un sous-mot de u. On a : $0 \leq |y| < n$. Alors, $x^R = ay^R$. Par hypothèse de récurrence, y^R est un

sous-mot de u^R. Par conséquent, $x^R = ay^R$ est un sous-mot de $au^R = w^R$.

d. $(w^n)^R = (w^R)^n$, pour tout entier naturel n.

Preuve par récurrence sur la longueur $|w| = k$ du mot $w \in \Sigma^*$.

- **Cas de base** : si $k = 0$, alors $w = \varepsilon$, et $(\varepsilon^n)^R = \varepsilon^R = \varepsilon = (\varepsilon^R)^n$.

Hypothèse de récurrence : si $|w| = k \geq 0$, pour tout entier n, $(w^n)^R = (w^R)^n$.

- **Cas indictif** : soit $w \in \Sigma^*$ tel que $|w| = k + 1$. Alors, $w = ua$, avec $u \in \Sigma^*$, $|u| = k$ et $a \in \Sigma$. Soit $n \geq 1$ (pour n = 0, la propriété est triviale). On a :

$$
\begin{aligned}
(w^n)^R &= ((ua)^n)^R && [w = ua] \\
&= ((ua)(ua)^{n-1})^R && [\text{Par la relation : } x^n = xx^{n-1}] \\
&= ((ua)^{n-1})^R(ua)^R && [\text{Par la relation : } (xy)^R = y^Rx^R] \\
&= ((ua)^{n-1})^R au^R && [\text{Par définition récursive de R}] \\
&\ldots \\
&= au^Rau^R \ldots au^Rau^R && [n \text{ fois}] \\
&= w^Rw^R \ldots w^Rw^R && [n \text{ fois}] \\
&= (w^R)^n
\end{aligned}
$$