Module Langages Formels
TD 1 : Mots et langages

Correction

Exercice 1 `Une histoire de moutons...`

Soit Σ un alphabet non vide. Montrez que le language Σ^* est infini dénombrable.

Exercice 2 `Révisons les conjugaisons`

Deux mots u et v sur un alphabet Σ sont dits **conjugués** s'il existe des mots s et t sur Σ tels que $u = st$ et $v = ts$.

2.1. Montrer que la relation binaire $\sim$ sur Σ^* définie par $u \sim v$ ssi u et v sont conjugués est une relation d'équivalence.

- Les propriétés de réflexivité et de symétrie sont immédiates.
- Transitivité : si $u \sim v$ (avec s et t) et $v \sim w$ (avec s' et t'), alors en posant a tq $s = at'$ et $s' = ta$ on a $u = st = at't$ et $w = t'ta$ d'où le résultat voulu avec $s'' = a$ et $t'' = t't$.

2.2. Montrer que pour tout $n \geq 1$, $u \sim v \iff u^n \sim v^n$.

$\Rightarrow$ On a $u = st$ et $v = ts$ par hypothèse, d'où le résultat en prenant $s' = (st)^{n-1}$ et $t' = st$.
$\Leftarrow$ Supposons $u^n \sim v^n$ avec un couple (s, t). Il existe des entiers i et j tels que $s = u^i x$ et $t = yu^j$ avec $i + j + 1 = n$ et $u = xy$. Donc $s = (xy)^i x$ et $t = y(xy)^j$, d'où $v^n = ts = y(xy)^j(xy)^i x = (yx)^n$. Donc $v = yx$, d'où le résultat.

2.3. Montrer que $u \sim v$ si et seulement s'il existe un mot w tel que $uw = wv$.

$\Rightarrow$ Si $u \sim v$ avec (s,t) on a directement le résultat en prenant $w = s$.
$\Leftarrow$ Soit w de longueur minimale tel que $uw = wv$.
- Si $|w| > |u|$, on a $w = uw' = w'v$, ce qui contredit la minimalité de w.
- On peut donc supposer $|w| \leq |u|$. Il existe alors w' tel que $u = ww'$ et $v = w'w$, donc le couple (w, w') fournit $u \sim v$.

Exercice 3 `On and On and On`

On appelle **code** sur un alphabet Σ tout langage X sur Σ tel que pour toutes familles $(x_i) \in X^{[\![1,p]\!]}$ et $(y_i) \in X^{[\![1,q]\!]}$, $x_1x_2 \dots x_p = y_1y_2 \dots y_q$ entraine $p = q$ et $x_i = y_i$ pour tout i. Dire que X est un code revient donc à dire que tout élément de X^* se factorise de manière unique sur X.

3.1. Les langages suivants sont-ils des codes ?
- $X_1 = \{ab, baa, abba, aabaa\}$
- $X_2 = \{b, ab, baa, abaa, aaaa\}$
- $X_3 = \{aa, ab, aab, bba\}$
- $X_4 = \{a, ba, bba, baab\}$

- X_1 n'est pas un code : $abbaabaabaa = x_1^1x_1^2x_1^2x_1^2 = x_1^3x_1^1x_1^4$
- X_2 est un code :
  - Supposons un contre exemple commençant par a,
    Alors ses deux écritures commencent par ab ou $abaa$,
    La deuxième compte 2 a de plus en fin, donc la première doit se poursuivre avec $aaaa$
    Du coup, la première compte maintenant 2 a de plus en fin, et doit donc se poursuivre avec $aaaa$
    ... On obtient donc un mot infini.
  - Si le contre-exemple commence par b,
    Ses deux écritures commencent nécessairement par b et baa
    Même raisonnement qu'au-dessus.

  $\Rightarrow$ Il n'existe donc pas de contre exemple de longueur finie.
- X_3 est un code (même type de raisonnement que ci-dessus).
- X_4 n'est pas un code : $baabba = x_4^2x_4^1x_4^3 = x_4^4x_4^2$

3.2. Soit u un mot de Σ^*, montrer que l'ensemble $\{u\}$ est un code si et seulement si $u \neq \epsilon$.

Par uncicité de l'écriture dans l'alphabet, un mot ne peut avoir deux décompositions différentes dans $\{u\}$ que si $u = \epsilon$.

3.3. Soient u et v deux mots distincts de Σ^*, montrer que la partie $\{u, v\}$ est un code si et seulement si u et v ne commutent pas.

Cette preuve se fait par récurrence sur $|u| + |v|$
- Si $|u| + |v| = 2$, le seul cas interressant est pour $|u| = |v| = 1$
  u et v étant distincts, ce sont deux lettres de Σ.
  Par unicité de l'écriture d'un mot dans Σ, $\{u, v\}$ est un code.
  u et v ne peuvent commuter donc la réciproque est aussi vraie.
- On suppose que la propriété est vraie pour tous les couples $\{u, v\}$ tels que $|u| + |v| < n$. Soient u et v tels que $|u| + |v| = n$.
  - Si u et v commutent, alors le mot $m = uv = vu$ a deux écritures distinctes.
    $\{u, v\}$ n'est donc pas un code.
  - Si $\{u, v\}$ n'est pas un code,
    Il existe $m = m_1 \dots m_k = m'_1 \dots m_q$ (on prend le plus petit).
    Nécéssairement, $m_1 \neq m'_1$ car c'est le plus petit.
    On a donc u préfixe de v (ou le contraire), donc il existe x tel que $v = ux$ avec $|x| < |v|$.
    On peut donc écrire $m_2 \dots m_k = xm'_2 \dots m_q$ dans la base $\{u, x\}$ de deux manières différentes (l'une commence par u et l'autre par x).
    Or $|x| < |v|$ donc $|u| + |x| < n$, et $\{u, x\}$ n'est pas un code.
    Ainsi, u et x commutent, donc $uv = uux = uxu = vu$.
    Donc u et v commutent !

3.4. Soit X une partie de Σ^* ne contenant pas ϵ et telle qu'aucun mot de X ne soit préfixe propre d'un autre mot de X. Montrer que X est un code (un tel code est appelé code préfixe).

Supposons que X ne soit pas un code,
Soit $m = x_i m_1 \dots m_p = x_j m'_1 \dots m'_q$ le plus petit mot de Σ^* avec deux factorisations différentes.
$i \neq j$ (sinon ce n'est pas le plus petit).
- Si $|x_i| \leq |x_j|$ alors x_i est préfixe de x_j, ce qui est absurde.
- Si $|x_i| > |x_j|$ alors c'est x_j qui est préfixe de x_i, ce qui est tout aussi absurde !

X est donc un code.

Exercice 4 `Mots multiplicativement dépendants`

Deux mots u et v sont dits **multiplicativement dépendants** s'ils sont puissances d'un même troisième, c'est à dire s'il existe un mot w et deux entiers m et n tels que

$$u = w^n \text{ et } v = w^m$$

Deux mots u et v sont dits **commutatifs** si $uv = vu$.

4.1. Donner un exemple de deux mots commutatifs de longueur supérieure à 2

D'après le résultat suivant, il est inutile de chercher trop compliqué, donc par exemple :
ab et *abab*
ϵ et *pouet*
...

4.2. Prouver la proposition suivante :

Proposition :
Deux mots u et v commutent si et seulement si ils sont multiplicativement dépendants.

1. Trivialement, si u et v sont multiplicativement dépendants, ils commutent.
2. Pour la réciproque, nous allons faire une récurrence sur la longueur du mot uv, soit $|u| + |v|$.
   - Si $|uv| = 0$, alors $u = v = \epsilon$, donc u et v sont triviallement multiplicativement dépendants.
   - Soit $n \in \mathbb{N}^+$, on suppose le résultat vrai pour tout $m < n$. Soient u et v tels que $|uv| = n$. On a alors les cas suivants :
     – Si $u = \epsilon$ ou $v = \epsilon$, le résultat est acquis ;
     – Si $|u| = |v|$, alors les mots sont égaux lettre à lettre car $uv = vu$ et son écriture est unique ;
     – Sinon, on suppose $|u| < |v|$. D'après l'égalité $uv = vu$, u est nécéssairement préfixe de v. Il existe donc w tel que $uw = v$, donc $uuw = uwu$ et en simplifiant, $uw = wu$. On applique alors l'hypothèse de récurrence et on obtient que u et w sont multiplicativement dépendants, et donc que u et v le sont aussi.