le cnam

Codes et Automates finis

Cours 11 Quotients à gauche

- Quotient à gauche d'un langage par un mot

On se donne un alphabet A et un langage $L \subset A^*$ sur cet alphabet. On se donne aussi un mot $u \in A^*$. Le quotient à gauche du langage L par le mot u est le langage noté $u^{-1}L$ et défini par $u^{-1}L = \{v \in A^*, u.v \in L\}$. On parle aussi d'inverse à gauche ou de "résiduel".
L'inverse à gauche est formé de tous les mots par lesquels il faut concaténer à droite le mot u pour obtenir un mot de L.
Par exemple, considérons le langage $L = A^3$ des mots de trois lettres sur l'alphabet $A = \{a, b\}$. Alors $L = \{aaa, aab, aba, abb, baa, bab, bba, bbb\}$. On a $a^{-1}L = A^2 = \{aa, ab, ba, bb\}$ et $b^{-1}L = A^2$ également.
Second exemple. Soit $L = (ab)^* = \varepsilon + ab + abab + ababab + \dots$. Alors
$a^{-1}L = b + bab + bababab + \dots = b(\varepsilon + ab + abab + \dots) = bL$. On a aussi $b^{-1}L = \emptyset$.

- Quotient à gauche d'un langage par un autre langage

On se donne deux langages K et L sur l'alphabet A. On a par définition $K^{-1}L = \cup_{k \in K} k^{-1}L$. On a bien entendu $\varepsilon^{-1}L = L$.

- Propriétés des quotient à gauche

Si $w \in A^*$, $K \subset A^*$ et $L \subset A^*$, $w^{-1}(K \cup L) = (w^{-1}K) \cup (w^{-1}L)$. On peut aussi écrire cette relation $w^{-1}(K + L) = (w^{-1}K) + (w^{-1}L)$.
Si $a \in A^*$, $K \subset A^*$ et $L \subset A^*$, on pose $\{\varepsilon\} \cap K = \emptyset$ si $\varepsilon \notin K$ et $\{\varepsilon\} \cap K = \{\varepsilon\}$ si $\varepsilon \in K$. On a alors $a^{-1}(KL) = (a^{-1}K)L + (\{\varepsilon\} \cap K)a^{-1}L$.
Si $a \in A^*$ et $L \subset A^*$, on a $a^{-1}L^* = (a^{-1}L)L^*$ car $L^* = \varepsilon + LL^*$.
Si u et v sont des mots sur l'alphabet A ($u \in A^*$ et $v \in A^*$) et L un langage sur cet alphabet ($L \subset A^*$), on a $(uv)^{-1}L = v^{-1}(u^{-1}L)$. En effet, pour un mot $\ell \in L$, si $\ell = uvw$, alors $w \in (uv)^{-1}L$ par définition de l'inverse à gauche. Mais alors $\ell = u(vw)$ donc $vw \in u^{-1}L$ par définition. On en déduit $w \in v^{-1}(u^{-1}L)$ par définition de l'inverse à gauche.

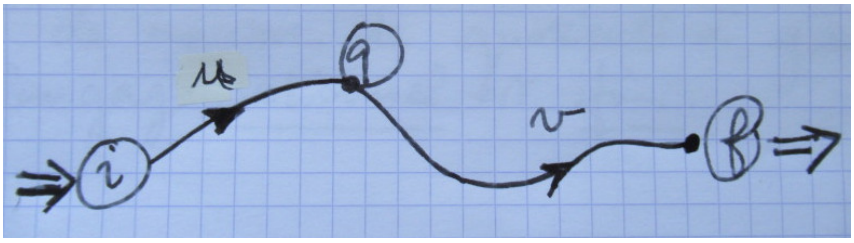
- Inverse d'un produit en théorie des groupes

La relation $(uv)^{-1}L = v^{-1}(u^{-1}L)$ où la non commutation induit un échange des arguments, peut être vue comme une variante du calcul de l'inverse d'un produit en théorie des groupes.
Rappelons qu'un groupe $(G, .)$ est la donnée d'un ensemble G et d'une loi de type multiplication entre deux éléments de G: $G \times G \ni (u, v) \longmapsto u.v \in G$. Cette loi doit satisfaire les trois propriétés suivantes :
(i) associativité : $(u.v).w = u.(v.w)$, $\forall u, v, w \in G$
(ii) existence d'un élément neutre : il existe $e \in G$ tel que $e.u = u.e = u$, $\forall u \in G$. L'élément neutre "e" a une action qui consiste à ne rien faire

(iii) tout élément du groupe admet un inverse. Quel que soit $u \in G$, il existe un inverse $u^{-1} \in G$ de sorte que $u.(u^{-1}) = (u^{-1}).u = e$.
On n'impose pas la commutativité ($u.v = v.u$) dans la définition générale d'un groupe. Même si de nombreux groupes sont commutatifs, comme par exemple le groupe $(\mathbb{Z}, +)$ des nombres entiers positifs ou négatifs pour l'addition. En effet, d'autres groupes ne sont pas commutatifs, comme par exemple l'ensemble des matrices réelles deux par deux $u = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de sorte que $ad - bc = 1$ muni de la multiplication des matrices. On a vu plus haut dans ce cours que si par exemple $u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $v = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ on a d'une part $u.v = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ et d'autre part $v.u = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$; ces deux matrices sont distinctes et $u.v \neq v.u$ en général.
Rappelons ici la propriété générale $(u.v)^{-1} = v^{-1}.u^{-1}$. Une idée naïve serait de penser que $(u.v)^{-1} = u^{-1}.v^{-1}$ et nous invitions le lecteur à se convaincre que cette relation est en défaut lorsque u et v ne commutent pas. Par contre, on a $(u.v)^{-1} = v^{-1}.u^{-1}$, comme le montre le double calcul suivant : $(u.v).(v^{-1}.u^{-1}) = u.(v.v^{-1}).u^{-1} = u.e.u^{-1} = u.u^{-1} = e$ et $(v^{-1}.u^{-1}).(u.v) = v^{-1}.(u^{-1}.u).v = v^{-1}.e.v = v^{-1}.v = e$.

- Une propriété fondamentale

On se donne un automate fini $\mathscr{A} = (Q, A, T, I, F)$ et on suppose que l'ensemble des états initiaux I est composé du seul état $i \in Q$. Soit $L = \mathscr{L}(\mathscr{A})$ le langage des mots acceptés par l'automate, $u \in A^*$ un mot quelconque formé à partir des lettres de l'alphabet A et $i \xrightarrow{u} q$ un chemin qui part de l'état initial i et aboutit à un état $q \in Q$. Alors
$u^{-1}L = \{v \in A^*,\ q \xrightarrow{v} f,\ f \in F\} = X_q$; c'est l'ensemble des mots qui pilotent un chemin qui permet d'aller de l'état q à un état final.



En effet, si v pilote un chemin de l'automate qui va de l'état q à un état final $f \in F$, alors le mot $\ell = u.v$ paramètre un chemin qui va de l'état initial i à l'état $q \in Q$ puis de cet état q jusqu'à un état final $f \in F$ (voir la figure ci-dessus). Donc le mot $\ell = u.v$ est un mot reconnu par l'automate, on a $\ell \in L$ et $v \in u^{-1}L$.
Réciproquement, si $v \in u^{-1}L$, alors $\ell = u.v$ est un mot du langage L, c'est à dire accepté par l'automate $\mathscr{A}$. Donc le mot ℓ pilote un chemin qui va d'abord de l'état i à un état q puis à l'aide du mot v, qui va de l'état q à un état final $f \in F$. D'où le résultat. □

- Conséquences de la propriété fondamentale

Conséquence 1. Le nombre de quotients à gauche du langage L est inférieur ou égal au nombre d'états d'un automate fini $\mathscr{A}$ qui accepte ce langage L.
Conséquence 2. Le nombre de quotients à gauche d'un langage rationnel est fini.

- Deux exemples

Exemple 1. Nous reprenons le langage $L = A^3$ des mots de trois lettres sur l'alphabet $A = \{a, b\}$. Nous avons vu que $a^{-1}L = b^{-1}L = A^2$, ensemble des mots de deux lettres. On en déduit que $a^{-1}(a^{-1}L) = a^{-1}(b^{-1}L) = b^{-1}(a^{-1}L) = b^{-1}(b^{-1}L) = A$, ensemble des mots formés d'une seule lettre. On continue l'épluchage du langage A^3. On a maintenant $a^{-1}(a^{-1}(a^{-1}L)) = a^{-1}(a^{-1}(b^{-1}L)) = \cdots = b^{-1}(b^{-1}(b^{-1}L)) = \{\varepsilon\}$. Puis $a^{-1}\varepsilon = b^{-1}\varepsilon = \emptyset$, car le mot sans lettre ne commence ni par la lettre a ni par la lettre b. L'ensemble de tous les quotients à gauche est finalement composé du langage L lui-même (car $\varepsilon^{-1}L = L$) et des langages A^2, A, ε et $\emptyset$. On a donc cinq quotients à gauche au total.

Exemple 2. Soit $L = (ab)^*$. Nous avons vu que $a^{-1} = bL$ et $b^{-1}L = \emptyset$. On a ensuite $a^{-1}(a^{-1}L) = a^{-1}(bL) = \emptyset$ et $b^{-1}(a^{-1}L) = b^{-1}(bL) = L$. On a bien entendu $a^{-1}(b^{-1}L) = b^{-1}(b^{-1}L) = \emptyset$. En conséquence, l'ensemble des quotients à gauche du langage $L = (ab)^*$ est composé de L lui-même, de bL et de l'ensemble vide. On a dans ce cas trois quotients à gauche, même si le langage L comporte une infinité de mots !

- Caractérisation des langages rationnels

Rappelons que la classe des langages rationnels comporte l'ensemble vide, les mots d'une lettre sur l'alphabet A et qu'elle est stable par réunion, concaténation et action de l'opérateur étoile.

Théorème. Un langage L sur un alphabet A est rationnel si et seulement si il a un nombre fini de quotients à gauche $u^{-1}L$ pour $u \in A^*$.

Exemple. Pour $L = \{(ab)^n, n \in \mathbb{N}\}$, on a $L = (ab)^*$ qui a un nombre fini de quotients à gauche : L, bL et $\emptyset$.

Le langage défini par $L = \{a^n b^n, n \in \mathbb{N}\} = \varepsilon + ab + aabb + aaabbb + \ldots$ n'est pas un langage rationnel. En effet, $a^{-1}L = Lb$, $b^{-1}L = \emptyset$, $a^{-2}L = a^{-1}(a^{-1}L) = Lb^2$ puis de proche en proche, $a^{-n}L = Lb^n$ pour $n \in \mathbb{N}$. Ce langage a un nombre infini de quotients à gauche et ne peut pas être un langage rationnel.

- Automate minimal

On se donne un langage rationnel L sur l'alphabet A. Nous allons construire un automate fini $\mathscr{A}$ dont le langage $\mathscr{L}(\mathscr{A})$ des mots acceptés est exactement égal à L. Cet automate est dit "automate minimal" car il comporte un nombre minimal d'états Q est défini de la façon suivante : $\mathscr{A}(L) = (Q, A, T, I, F)$ où

$Q = \{u^{-1}L, u \in A^*\}$, ensemble (fini !) de tous les quotients à gauche du langage L

A est l'alphabet qui sous-tend le langage L ($L \subset A^*$)

T ensemble des transitions défini de la façon suivante. On se donne $u \in A^*$ et $a \in A$. Le quotient à gauche $p = u^{-1}L$ est un état Q. La transition $q = \delta(p, a)$ est définie par $\delta(u^{-1}L, a) = (ua)^{-1}L = a^{-1}(u^{-1}L)$ qui est un nouveau quotient à gauche

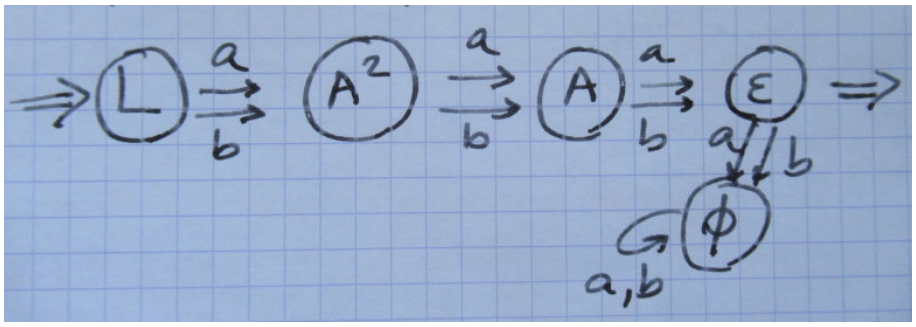
$I = \{L\}$: un unique état initial

$F = \{u^{-1}L, u \in L\}$ ensemble des états finals. On note bien la petite différence formelle entre les définitions de l'ensemble des états Q et l'ensemble F des états finals. Il n'y a pas de condition sur le mot $u \in A^*$ pour définir $u^{-1}L \in Q$ alors que $u^{-1}L \in F$ si et seulement si $u \in L$.

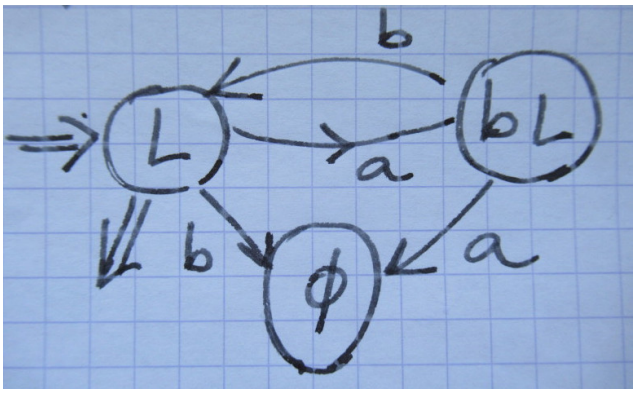
Une fois l'automate minimal $\mathscr{A}(L)$ défini, on peut montrer que $\mathscr{L}(\mathscr{A}(L)) = L$; l'automate minimal $\mathscr{A}(L)$ accepte le langage L.

- Exemples d'automate minimaux

Exemple 1 : $L = A^3$. On a calculé plus haut les quotients à gauche. On a vu que $a^{-1}L = b^{-1}L = A^2$, $a^{-1}A^2 = b^{-1}A^2 = A$, $a^{-1}A = b^{-1}A = \{\varepsilon\}$ et $a^{-1}\varepsilon = b^{-1}\varepsilon = \emptyset$. On dispose de cinq quotients à gauche : L, A^2, A, ε et $\emptyset$. Compte tenu de la construction de l'automate minimal présentée plus haut, on a les transitions suivantes : $\delta(L,a) = a^{-1}L = A^2$, $\delta(L,b) = b^{-1}L = A^2$, $\delta(A^2,a) = a^{-1}A^2 = A$, $\delta(A^2,b) = b^{-1}A^2 = A$, $\delta(A,a) = a^{-1}A = \varepsilon$, $\delta(A,b) = b^{-1}A = \varepsilon$, $\delta(\varepsilon,a) = a^{-1}\varepsilon = \emptyset$, $\delta(\varepsilon,b) = b^{-1}\varepsilon = \emptyset$. L'ensemble F des états finals est égal à $\{u^{-1}L, u \in L\}$, soit les quotients à gauche de la forme $a^{-1}(a^{-1}(a^{-1}L)) = a^{-1}(a^{-1}(b^{-1}L)) = \cdots = b^{-1}(b^{-1}(b^{-1}L)) = \{\varepsilon\}$. Donc $F = \{\varepsilon\}$. L'ensemble de ces résultats est synthétisé avec le graphe de l'automate minimal représenté ci-dessous.



Exemple 2 : $L = (ab)^*$. On a vu plus haut que $a^{-1}L = bL$ et $b^{-1}L = \emptyset$, $a^{-1}(a^{-1}L) = a^{-1}(bL) = \emptyset$ et $b^{-1}(a^{-1}L) = b^{-1}(bL) = L$. On dispose de trois quotients à gauche du langage L, bL et de l'ensemble vide. Les transitions se calculent avec la même approche que pour l'exemple précédent : $\delta(L,a) = a^{-1}L = bL$, $\delta(L,b) = b^{-1}L = \emptyset$, $\delta(bL,a) = a^{-1}(bL) = \emptyset$, $\delta(bL,b) = b^{-1}(bL) = L$ et bien entendu $\delta(\emptyset,a) = \emptyset$ et $\delta(\emptyset,b) = \emptyset$. L'ensemble F des états finals est égal à la réunion des $((ab)^n)^{-1}L$, soit simplement L, puisque $(\varepsilon)^{-1}L = L$ et $(ab)^{-1}L = b^{-1}(a^{-1}L) = b^{-1}(bL) = L$. Le graphe de l'automate minimal correspondant est décrit à la figure ci-dessous.



Exercices

- Quotients à gauche du langage $L = a^* b^*$

a) Déterminer tous les quotients à gauche du langage $L = a^* b^*$.

b) En déduire le graphe de l'automate minimal $\mathscr{A}(L))$ associé à ce langage.

c) Vérifier que le langage des mots acceptés par cet automate est exactement égal au langage L. On pourra utiliser le système des équations de départ.

- Quotients à gauche du langage $(b + ab^* a)^*$

Reprendre l'exercice précédent avec le langage $(b + ab^* a)^*$ des mots construits sur l'alphabet $A = \{a, b\}$ qui comptent un nombre pair de fois la lettre "a".

- Quotients à gauche du langage $(a + bb^* a)^* b$

Reprendre l'exercice précédent avec le langage $(a + bb^* a)^* b$.