1
Les langages.

- **Un mot** est une chaîne de caractères.
- **Un langage** est un ensemble de mots.

Dans ce chapitre, on étudie des propriétés générales des langages.
Deux types de langages seront étudiés par la suite. Leur application à la compilation donne lieu à deux types d'analyse :

- **Les langages réguliers :** l'analyse lexicale,
- **Les langages algébriques :** l'analyse syntaxique.

1 – Les mots.

• Un *alphabet* est un ensemble $\mathcal{A}$, dont les éléments sont appelés *lettres*, *caractères* ou *symboles*.

Les mots

Un mot u sur l'alphabet $\mathcal{A}$ est une application

$$u : \{1, \ldots, m\} \to \mathcal{A}$$

où

m est un entier appelé *la longueur* de u et noté $|u|$
$\{1, \ldots, m\}$ est l'ensemble des entiers naturels i tels que $1 \leq i \leq m$.

• $u(i)$ est appelée *la i–ème lettre*, *le i–ème caractère* ou *le i–ème symbole* de u.

• Si $u(i) = x$, on dira que $u(i)$ *est une occurrence de x dans u*.

• On peut noter $u[i]$ au lieu de $u(i)$: on constate alors que la définition des mots nous est très familière !

L'ensemble des mots sur l'alphabet $\mathcal{A}$ est désigné par $\mathcal{A}^*$

1.1 – Définitions de base.

Soit $u \in \mathcal{A}^*$.

• Lorsque $|u| = 0$, $u : \emptyset \to \mathcal{A}$ est *le mot sans caractère* (*mot vide*), noté ε.

• Lorsque $|u| = 1$, $u : \{1\} \to \mathcal{A}$ est défini par le seul caractère $u(1) \in \mathcal{A}$.

On convient d'identifier tout $x \in \mathcal{A}$ au mot de longueur 1 qu'il définit :

$$\boxed{\mathcal{A} \subseteq \mathcal{A}^*}$$

Ces identifications ne sont valables que parce que les éléments de $\mathcal{A}$ sont reconnaissables pour tels.

• **L'adjonction d'une occurrence à droite** d'un mot $\mathcal{A}^* \times \mathcal{A} \to \mathcal{A}^*$ se définit de la façon suivante :

pour tout mot $u : \{1, \ldots, m\} \to \mathcal{A}$ et tout symbole $x \in \mathcal{A}$, $ux : \{1, \ldots, m+1\} \to \mathcal{A}$ est le mot défini par :

$$ux(i) = u(i) \text{ pour tout } i \in \{1, \ldots, m\},$$
$$ux(m+1) = x.$$

Remarques.

• $\varepsilon x = x$ si, comme il a été convenu ci–dessus, on identifie le symbole x avec le mot de longueur 1 qu'il définit.

• $|ux| = |u| + 1$.

1.2 – Récurrence sur les mots basée sur l'adjonction d'occurrences à droite.

Tout élément de $\mathcal{A}^*$ ou bien est ε ou bien s'obtient à partir d'un élément de $\mathcal{A}^*$ par "adjonction d'un caractère à droite". Les deux clauses suivantes :

- $\varepsilon \in \mathcal{A}^*$ (le mot sans caractère)
- pour tout $x \in \mathcal{A}$: si $u \in \mathcal{A}^*$ alors $ux \in \mathcal{A}^*$ (adjonction de x à droite de u)

constituent donc une définition inductive de $\mathcal{A}^*$. Plus précisément, $\mathcal{A}^*$ est le plus petit ensemble vérifiant les deux propriétés ci–dessus.

Exemple :

Construction	résultat	en abrégé
mot initial	ε	ε
adjonction de a	εa	a
adjonction de a	εaa	aa
adjonction de b	εaab	aab

Lorsque l'on écrit les mots par simple juxtaposition de caractères, il faut que ceux–ci n'interagissent pas les uns avec les autres : chaque caractère doit être indécomposable en des éléments appartenant à l'alphabet en cause.

La condition que $\mathcal{A}$ doit satisfaire pour cela s'exprime sous la forme suivante :

Lecture unique des mots sur $\mathcal{A}$

Quels que soient $u, v \in \mathcal{A}^*$, et $x, y \in \mathcal{A}$:

$$ux = vy \text{ implique } u = v \text{ et } x = y$$

Voici maintenant le principe qui est à la base de nombreuses démonstrations : sa justification découle directement de la construction de $\mathcal{A}^*$.

Récurrence sur les mots

Soit $P[u]$ un énoncé au sujet de $u \in \mathcal{A}^*$. Alors, si les deux propriétés suivantes sont vraies :

- $P[\varepsilon]$
- *pour tout* $x \in \mathcal{A}$ *et tout* $u \in \mathcal{A}^*$, $P[u]$ *implique* $P[ux]$

la propriété $P[u]$ est vraie pour tout $u \in \mathcal{A}^*$.

Ce principe n'est cependant pas le seul que l'on puisse utiliser pour raisonner sur les mots. En voici d'autres :

- construction des mots et récurrence par adjonction de caractères à gauche,
- induction sur la longueur des mots,

enfin, on sait qu'un ensemble non vide d'entiers contient un plus petit élément :

- un ensemble non vide de mots contient un mot dont la longueur est la plus petite possible.

Les notions de base relatives aux mots peuvent se définir par récurrence sur les mots : une telle définition est le **schéma d'une procédure récursive**.

- *La longueur* d'un mot se redéfinit par la récurrence :

  $|\varepsilon| = 0$
  $|ux| = |u| + 1$ pour tout $u \in \mathcal{A}^*$ et tout $x \in \mathcal{A}$.

L'énoncé $P[u]$ est "$|u|$ est définie".

1.3 – La concaténation

est l'opération $\cdot \ : \mathcal{A}^* \times \mathcal{A}^* \to \mathcal{A}^*$ qui consiste à mettre deux mots "bout à bout".

La concaténation

Pour tout u et tout $v \in \mathcal{A}^*$, $u \cdot v$ est définie par récurrence sur v de la façon suivante :

1) $u \cdot \varepsilon = u$, $I(u)$
2) $u \cdot (vx) = (u \cdot v)x$ $S(u, v, x)$
   pour tout $v \in \mathcal{A}^*$ et tout $x \in \mathcal{A}$.

L'énoncé $P[v]$ qui est en cause ici est "pour tout $u \in \mathcal{A}^*$, $u \cdot v$ est défini". La récurrence définissant la concaténation correspond à une procédure récursive :

$$\begin{aligned} ab \cdot abba &= (ab \cdot abb)a && S(ab, abb, a) \\ &= ((ab \cdot ab)b)a && S(ab, ab, b) \\ &= (((ab \cdot a)b)b)a && S(ab, a, b) \\ &= ((((ab \cdot \varepsilon)a)b)b)a && S(ab, \varepsilon, a) \\ &= ((((ab)a)b)b)a && I(ab) \end{aligned}$$

Propriétés de la concaténation

Quels que soient u, v et $w \in \mathcal{A}^*$:

0) $|u \cdot v| = |u| + |v|$.
1) Neutralité : $\varepsilon \cdot u = u$ et $u \cdot \varepsilon = u$.
2) Associativité : $(u \cdot v) \cdot w = u \cdot (v \cdot w)$.

On écrit très souvent uv au lieu de $u \cdot v$ et uvw au lieu de $(u \cdot v) \cdot w$ ou $u \cdot (v \cdot w)$.

Lemme de Lévy.

Si u, v, α et $\beta \in \mathcal{A}^*$ vérifient : $uv = \alpha\beta$ et $|v| \leq |\beta|$ (et donc aussi $|u| \geq |\alpha|$) alors il existe $\delta \in \mathcal{A}^*$ tel que $u = \alpha\delta$ et $\beta = \delta v$.

☞ La preuve se fait par récurrence sur v : l'énoncé en cause a la forme $P[v]$ = quels que soient $u, \alpha, \beta \in \mathcal{A}^*$ ....

- Si $v = \varepsilon$ alors $\delta = \beta$ convient parfaitement ;
- supposons que $P[v]$ soit vrai : il faut montrer qu'alors, $P[vx]$ est vrai pour tout $x \in \mathcal{A}$.
  Supposons donc que l'on ait $u(vx) = \alpha\beta$ et $|vx| \leq |\beta|$.
  Cette dernière condition implique $\beta \neq \varepsilon$ et on a donc $\beta' \in \mathcal{A}^*$ et $y \in \mathcal{A}$ tels que $\beta = \beta' y$.
  La première peut alors s'écrire (définition de la concaténation !) $(uv)x = (\alpha\beta')y$, ce qui (lecture unique des mots) implique $uv = \alpha\beta'$ et $y = x$;
  l'hypothèse de récurrence s'applique puisque l'on a aussi $|v| \leq |\beta'|$: on a donc un mot δ vérifiant $u = \alpha\delta$ et $\beta' = \delta v$, et donc $\beta = \beta' x = (\delta v)x = \delta(vx)$.

2 – Les langages, opérations élémentaires sur les langages.

- *Un langage* L sur $\mathcal{A}$ est une partie de $\mathcal{A}^*$: $L \subseteq \mathcal{A}^*$.
- L'ensemble des langages sur $\mathcal{A}$ est désigné par $\mathcal{P}(\mathcal{A}^*)$.

Exemples.

- $\emptyset \subseteq \mathcal{A}^*$, $\mathcal{A} \subseteq \mathcal{A}^*$ et $\mathcal{A}^* \subseteq \mathcal{A}^*$ sont des langages sur $\mathcal{A}$.
- Pour tout $u \in \mathcal{A}^*$, $\{u\} \subseteq \mathcal{A}^*$ est un langage sur $\mathcal{A}$.

On convient d'identifier un mot au langage à un seul élément qu'il définit : $\mathcal{A}^* \subseteq \mathcal{P}(\mathcal{A}^*)$.

Le regroupement de nos deux conventions vaut la peine d'être encadré :

$$\boxed{\mathcal{A} \subseteq \mathcal{A}^* \subseteq \mathcal{P}(\mathcal{A}^*)}$$

C'est généralement la notation la plus simple qui est utilisée, par exemple :

- si $x \in \mathcal{A}$, x désigne aussi le langage $\{x\}$ dont le seul mot ne comporte que le seul caractère x.
- ε désigne aussi le langage $\{\varepsilon\}$ dont le seul élément est le mot sans caractère.

2.1 – Sommes de langages = Réunions de langages.

L'ensemble des langages $\mathcal{P}(\mathcal{A}^*)$ étant l'ensemble des parties d'un ensemble, est muni d'opérations bien connues : **réunion**, intersection, complémentaire.

Soient $L \subseteq \mathcal{A}^*$ et $M \subseteq \mathcal{A}^*$ alors $L + M \subseteq \mathcal{A}^*$ désigne la réunion de L et M. Ceci revient à poser :

La somme

Pour tout $u \in \mathcal{A}^*$: $u \in L + M$ ssi $u \in L$ ou $u \in M$

Une caractérisation de la somme.

Quels que soient $L \subseteq \mathcal{A}^*$, $M \subseteq \mathcal{A}^*$ et $N \subseteq \mathcal{A}^*$:

$$\boxed{L + M \subseteq N \text{ ssi } L \subseteq N \text{ et } M \subseteq N}$$

Propriétés de la somme

Quels que soient $L \subseteq \mathcal{A}^*$, $M \subseteq \mathcal{A}^*$ et $N \subseteq \mathcal{A}^*$:

1) Neutralité : $L + \emptyset = L$ et $\emptyset + L = L$.
2) Associativité : $(L + M) + N = L + (M + N)$
   (la valeur commune s'écrit souvent $L + M + N$)
3) Commutativité : $L + M = M + L$.
4) Idempotence : $L + L = L$.
5) Croissance : $M \subseteq N$ implique $L + M \subseteq L + N$.

2.2 – Sommes généralisées de langages.

Une famille de langages sur $\mathcal{A}$, indexée par un ensemble I, est la donnée, pour chaque $i \in I$, d'un langage $L_i \subseteq \mathcal{A}^*$. Une famille indexée par un ensemble d'entiers (naturels) s'appelle généralement *une suite*.
Soit $(L_i)_{i\in I}$ une telle famille, alors $\sum_{i\in I} L_i \subseteq \mathcal{A}^*$ est **la réunion** des langages L_i.

Somme généralisée

Pour tout $u \in \mathcal{A}^*$:

$$u \in \sum_{i\in I} L_i \text{ ssi il existe } i \in I \text{ tel que } u \in L_i.$$

Cas particuliers.

$$\sum_{i\in\emptyset} L_i = \emptyset \qquad \sum_{i\in\{1\}} L_i = L_1 \qquad \sum_{i\in\{1,2\}} L_i = L_1 + L_2$$

I peut être un ensemble d'entiers naturels, un langage,...

Une caractérisation de la somme généralisée.

Pour tout $M \subseteq \mathcal{A}^*$:

$$\boxed{\sum_{i\in I} L_i \subseteq M \text{ ssi pout tout } i \in I,\ L_i \subseteq M}$$

2.3 – Concaténation des langages.

Soient L et $M \subseteq \mathcal{A}^*$ deux langages sur $\mathcal{A}$, alors tout élément de $L \cdot M \subseteq \mathcal{A}^*$ est obtenu en concaténant un élément de L et un élément de M, dans cet ordre.

Concaténation des langages

Pour tout $u \in \mathcal{A}^*$:

$u \in L \cdot M$ ssi il existe $v \in L$ et $w \in M$ tels que $u = v \cdot w$

Remarque.

Lorsque $L = v$ et $M = w$ sont des langages réduits à un seul élément, $L \cdot M = v \cdot w$ est un langage réduit à un seul élément : on a étendu aux langages la définition relative aux mots.

Propriétés de la concaténation

Quels que soient L, M et $N \subseteq \mathcal{A}^*$:

1) Neutralité : $L \cdot \varepsilon = L$ et $\varepsilon \cdot L = L$
2) Associativité : $(L \cdot M) \cdot N = L \cdot (M \cdot N)$
3) Croissance :
   $M \subseteq N$ implique $L \cdot M \subseteq L \cdot N$ et $M \cdot L \subseteq N \cdot L$
4) Nullité : $L \cdot \emptyset = \emptyset$ et $\emptyset \cdot L = \emptyset$
5) Distributivité : $L \cdot (M + N) = L \cdot M + L \cdot N$ et $(M + N) \cdot L = M \cdot L + N \cdot L$

Lorsque $M = \varepsilon$, la propriété 3) peut s'énoncer :

$$\varepsilon \in N \text{ implique } L \subseteq L \cdot N \text{ et } L \subseteq N \cdot L.$$

Les deux propriétés suivantes sont des cas particuliers de la distributivité de la concaténation par rapport aux sommes généralisées :

$$L \cdot \left(\sum_{i \in I} M_i \right) = \sum_{i \in I} (L \cdot M_i)$$

$$\left(\sum_{i \in I} M_i \right) \cdot L = \sum_{i \in I} (M_i \cdot L)$$

On écrit très souvent LM au lieu de $L \cdot M$ et LMN au lieu de $(L \cdot M) \cdot N$ ou $L \cdot (M \cdot N)$.

2.4 – Quelques définitions.

L'ensemble $fg(u) \subseteq \mathcal{A}^*$ *des facteurs gauches (préfixes) du mot* u, défini par la récurrence :

$fg(\varepsilon) = \varepsilon$
$fg(ux) = fg(u)+ux$ pour tout $u \in \mathcal{A}^*$ et tout $x \in \mathcal{A}$

vérifie :

$v \in fg(u)$ ssi il existe $w \in \mathcal{A}^*$ tel que $u = vw$

pour tout $u \in \mathcal{A}^*$ et tout $v \in \mathcal{A}^*$.

L'ensemble $fd(u) \subseteq \mathcal{A}^*$ *des facteurs droits (suffixes) du mot* u, défini par la récurrence :

$fd(\varepsilon) = \varepsilon$
$fd(ux) = \varepsilon+fd(u)x$ pour tout $u \in \mathcal{A}^*$ et tout $x \in \mathcal{A}$

vérifie :

$v \in fd(u)$ ssi il existe $w \in \mathcal{A}^*$ tel que $u = wv$

pour tout $u \in \mathcal{A}^*$ et tout $v \in \mathcal{A}^*$.

L'ensemble $fact(u) \subseteq \mathcal{A}^*$ *des facteurs du mot* u, défini par la récurrence :

$fact(\varepsilon) = \varepsilon$
$fact(ux) = fact(u) + fd(u)x$ pour tout $u \in \mathcal{A}^*$ et tout $x \in \mathcal{A}$

vérifie :

$v \in fact(u)$ ssi il existe $w \in \mathcal{A}^*$ et $w' \in \mathcal{A}^*$ tels que $u = wvw'$

pour tout $u \in \mathcal{A}^*$ et tout $v \in \mathcal{A}^*$.

3 – Itération des langages.

L'ensemble $\mathcal{A}^i$ des mots que l'on obtient à partir du mot sans caractère, par i adjonctions successives d'un caractère à droite, se définit par la récurrence suivante sur l'entier i

- $\mathcal{A}^0 = \varepsilon$ (un mot sans caractère)
- $\mathcal{A}^{i+1} = \mathcal{A}^i\mathcal{A}$ pour tout i.
  (on adjoint un caractère à droite, si $\mathcal{A} \neq \emptyset$)

$\mathcal{A}^*$ est l'ensemble de tous les mots ainsi construits :

$$\boxed{\mathcal{A}^* = \sum_{i\geq 0} \mathcal{A}^i}$$

Plus généralement, soit $L \subseteq \mathcal{A}^*$:

Le langage itéré d'un langage

- La puissance $L^i \subseteq \mathcal{A}^*$ de L est définie pour tout entier naturel i par la récurrence :
  - $L^0 = \varepsilon$
  - $L^{i+1} = L^iL$ pour tout i.
- Le langage itéré de L est le langage $L^* \subseteq \mathcal{A}^*$ défini par :

$$L^* = \sum_{i\geq 0} L^i.$$

Remarques.

- Cas où $L = a$ est réduit à un seul mot de longueur 1 :
  - a^i est réduit au mot de longueur i ne comportant que des occurrences du seul caractère a, par exemple $a^5 = aaaaa$;
  - $a^* = \{a^i \mid i \geq 0\}$ est l'ensemble des mots ne comportant que des occurrences du seul caractère a.

- Si $\mathcal{A} \neq \emptyset$, on peut vérifier par récurrence sur i que, pour tout $u \in \mathcal{A}^*$:
  - $u \in \mathcal{A}^i$ ssi $|u| = i$,
  - $u \in (\varepsilon + \mathcal{A})^i$ ssi $|u| \leq i$.

Propriétés des puissances

Quels que soient $L \subseteq \mathcal{A}^*$ et les entiers naturels i, j et k :

1) $L^1 = L$.
2) $L^i L^j = L^{i+j}$.
3) $L^i L = L L^i = L^{i+1}$.
4) $(\varepsilon + L)^k = \sum_{0 \leq i \leq k} L^i$.

Propriétés de l'itération

Quels que soient $L \subseteq \mathcal{A}^*$, $M \subseteq \mathcal{A}^*$ et $N \subseteq \mathcal{A}^*$:

1) Stabilité par concaténation : si $M \subseteq L^*$ et $N \subseteq L^*$ alors $MN \subseteq L^*$.
2) Stabilité par itération : si $M \subseteq L^*$ alors $M^* \subseteq L^*$.
3) Croissance : si $M \subseteq L$ alors $M^* \subseteq L^*$.
4) $\emptyset^* = \varepsilon$ et $\varepsilon^* = \varepsilon$.
5) $L^*L = LL^*$.
6) $L^*L^* = L^{**} = L^*$.
7) $L^* = \varepsilon + L^*L = \varepsilon + LL^*$.
8) $(L + M)^* = (L^* + M^*)^*$
$= (L^*M^*)^* = L^*(ML^*)^* = (L^*M)^*L^*$.

Remarque.

Quels que soient $L \subseteq \mathcal{A}^*$ et $M \subseteq \mathcal{A}^*$, on a :

$$\boxed{L^* \subseteq M \text{ ssi pour tout entier } i,\ L^i \subseteq M}$$

Lorsque l'on veut montrer une propriété du type $L^* \subseteq M$, il suffit de vérifier que $L^i \subseteq M$ pour tout i, ce qui peut se faire par récurrence sur i.

4 – Systèmes d'équations linéaires.

La notation multiplicative pour la concaténation et additive pour la réunion nous permet d'écrire des équations algébriques dans l'ensemble des langages sur un alphabet $\mathcal{A}$ et de tenter leur résolution.

4.1 – Equations linéaires à une inconnue.

Soient $A \subseteq \mathcal{A}^*$ et $B \subseteq \mathcal{A}^*$.

Une *solution de l'équation*

$$(E) \qquad X = AX + B$$

est un langage $L \subseteq \mathcal{A}^*$ vérifiant la relation $L = AL + B$.

Résolution de (E)

1) $L = A^*B$ est une solution de (E).
2) L est la plus petite solution de (E).
3) Si $\varepsilon \notin A$, alors (E) admet une solution unique.

2) signifie que si $M \subseteq \mathcal{A}^*$ vérifie $M = AM + B$, alors $A^*B \subseteq M$.

1) $AL + B = AA^*B + B = (AA^* + \varepsilon)B = A^*B = L$.

2) Soit M une solution de (E) : on a $M = AM + B$ donc, en particulier, $B \subseteq M$ et $AM \subseteq M$. Pour montrer $A^*B \subseteq M$, il suffit de vérifier que $A^iB \subseteq M$ pour tout i. C'est une récurrence facile :
   - pour $i = 0$, on a $A^0B = B \subseteq M$,
   - supposons que $A^iB \subseteq M$ alors
   $$A^{i+1}B = A(A^iB) \subseteq AM \subseteq M.$$

3) montrons d'abord, par récurrence sur k, que si M est une solution de (E) alors :
   $$(E_k) \qquad M = A^{k+1}M + (\varepsilon + A)^kB$$
   pour tout entier naturel k.

   – (E_0) signifie simplement que M vérifie (E).
   – Si (E_k) est vraie, alors, en utilisant $M = AM + B$, on peut écrire :
   $$\begin{aligned} M &= A^{k+1}(AM + B) + (\varepsilon + A)^kB \\ &= A^{k+2}M + ((\varepsilon + A)^k + A^{k+1})B \\ &= A^{k+2}M + (\varepsilon + A)^{k+1}B \end{aligned}$$
   ce qui implique (E_{k+1}).

   Supposons que $\varepsilon \notin A$:

   • pour tout $u \in \mathcal{A}^*$ on a $u \notin A^{|u|+1}M$, puisque les éléments de A sont au moins de longueur 1 ;

   • si donc $u \in M$, $(E_{|u|})$ implique $u \in (\varepsilon + A)^{|u|}B \subseteq A^*B$: ceci signifie que $M \subseteq L$, c'est–à–dire $M = L$ par 2).

4.2 – Systèmes d'équations linéaires.

Soit m un entier naturel et soient $A_{i,j} \subseteq \mathcal{A}^*$ et $B_i \subseteq \mathcal{A}^*$ pour $i \leq m$ et $j \leq m$.
Une *solution du système*

$$(E) \quad X_i = \sum_{j \leq m} A_{i,j} X_j + B_i \quad \text{pour } i \leq m$$

est un $(m+1)$–uplet $L = \begin{pmatrix} L_0 \\ \vdots \\ L_m \end{pmatrix}$ de langages sur $\mathcal{A}$ satisfaisant

$$L_i = \sum_{j \leq m} A_{i,j} L_j + B_i \text{ pour tout } i \leq m.$$

Les $(m+1)$–uplets de langages se comparent terme à terme, c'est–à–dire que

$$\begin{pmatrix} L_0 \\ \vdots \\ L_m \end{pmatrix} \subseteq \begin{pmatrix} M_0 \\ \vdots \\ M_m \end{pmatrix} \text{ ssi } L_i \subseteq M_i \text{ pour tout } i \leq m.$$

Résolution de (E)

1) et 2) (E) admet une plus petite solution.
3) si $\varepsilon \notin A_{i,j}$ pour chaque i et chaque j, alors (E) admet une solution unique.

Méthode matricielle.

En utilisant la notation matricielle, on peut écrire (E) sous la forme $\mathbf{X} = \mathbf{AX} + \mathbf{B}$ où

$$\mathbf{X} = \begin{pmatrix} X_0 \\ \vdots \\ X_m \end{pmatrix} \qquad \mathbf{B} = \begin{pmatrix} B_0 \\ \vdots \\ B_m \end{pmatrix}$$

$$\mathbf{A} = \begin{pmatrix} A_{0,0} & \dots & A_{0,m} \\ \vdots & \ddots & \vdots \\ A_{m,0} & \dots & A_{m,m} \end{pmatrix}$$

et montrer que sa plus petite solution est bien $\mathbf{A}^*\mathbf{B}$.

Ce résultat a un intérêt formel évident, mais, la manipulation de l'itérée $\mathbf{A}^*$ de la matrice carrée $\mathbf{A}$ n'est pas très aisé !

Méthode de Gauss.

La méthode de résolution adoptée ici est une transposition de la **méthode de Gauss**, basée sur l'appliction itérée de deux opérations élémentaires :

- **la résolution partielle,**
- **la substitution.**

• L'équation de X_i peut s'écrire $X_i = A_{i,i}X_i + C_i$ où C_i ne dépend pas de X_i : sous cette forme, il est possible de la "résoudre" en appliquant le résultat relatif à une équation unique ; on obtient ainsi la "résolvante partielle de (l'équation de) X_i" :

$$X_i = A_{i,i}^* C_i$$

dont le second membre ne dépend plus de X_i.

On vérifie que pour tout entier naturel $i \leq m$:

Résolution partielle

Soit (F) le système obtenu à partir de (E) en remplaçant l'équation de X_i par sa résolvante partielle, alors :
la plus petite solution de (F) est égale à la plus petite solution de (E).

• On vérifie que, pour tout couple d'entiers naturels $i \leq m$ et $j \leq m$ tels que $i \neq k$:

Substitution

Soit (F) le système obtenu à partir de (E) en remplaçant X_i par le second membre $\sum_{j \leq m} A_{i,j}X_j + B_i$ de son équation dans celle de X_k, alors :
la plus petite solution de (F) est égale à la plus petite solution de (E).

Exemple.

Considérons le système

$$\begin{array}{lllllllll} X_0 & = & bX_0 & + & aX_1 & & & & \\ X_1 & = & & & & aX_2 & + & bX_3 & \\ X_2 & = & & & aX_1 & & + & bX_3 & + & \varepsilon \\ X_3 & = & & & bX_1 & & + & aX_3 & \end{array}$$

Les opérations successives

- résolution de X_0,
- résolution de X_3,
- substitution de X_3 dans les équations de X_1 et X_2,
- substitution de X_2 dans l'équation de X_1

le transforment en :

$$X_0 = b^*aX_1$$
$$X_1 = (aa + ba^*b + aba^*b)X_1 + a$$
$$X_2 = (a + ba^*b)X_1 + \varepsilon$$
$$X_3 = a^*bX_1$$

Enfin, la résolution de X_1 et des substitutions, conduisent à la solution cherchée :

$$X_0 = b^*a(aa + ba^*b + aba^*b)^*a$$
$$X_1 = (aa + ba^*b + aba^*b)^*a$$
$$X_2 = (a + ba^*b)(aa + ba^*b + aba^*b)^*a + \varepsilon$$
$$X_3 = a^*b(aa + ba^*b + aba^*b)^*a$$

Remarque.

- L'expression de la plus petite solution peut varier très sensiblement en fonction de l'ordre suivant lequel on effectue les opérations.

5 – Monoïdes et morphismes de monoïdes.

On a fait des conventions qui, pour un alphabet $\mathcal{A}$, peuvent se résumer par

$$\boxed{\mathcal{A} \subseteq \mathcal{A}^* \subseteq \mathcal{P}(A^*)}$$

Plus explicitement, $\mathcal{A}$ désigne un alphabet et

- le mot de longueur 1 défini par $x \in \mathcal{A}$ est identifié à la lettre x ;
- le langage $\{u\}$ comportant $u \in \mathcal{A}^*$ comme unique élément est identifié au mot u.

De plus

- la concaténation est notée par une simple juxtaposition, évoquant une multiplication ;
- la réunion est notée par le sympbole d'addition ou le symbole somme.

Toutes ces conventions offrent une facilité d'écriture dont il ne faut pas se cacher les dangers. En particulier, **il faut toujours avoir à l'esprit la nature des objets que l'on manipule** en précisant la signification des "lettres" que l'on utilise : une lettre, en soit, n'a aucun sens !

5.1 – Définition des monoïdes.

Les *monoïdes* sont des ensembles munis d'une structure algébrique fort courante.

Les monoïdes

Un monoïde est un triplet $(D, \times, e)$ *où*

- D *est un ensemble,*
- $\times : D \times D \to D$ *est une opération binaire que l'on notera* $(x, y) \mapsto x \times y$,
- $e \in D$ *est un élément particulier de* D ;

qui vérifie les propriétés suivantes :

- *Neutralité :* $x \times e = x$ *et* $e \times x = x$ *quel que soit* $x \in D$,
- *Associativité :* $(x \times y) \times z = x \times (y \times z)$ *quels que soient* $x \in D$, $y \in D$ *et* $z \in D$.

Exemples.

• L'ensemble $\mathbf{N}$ des entiers naturels est muni de deux structures de monoïdes : $(\mathbf{N}, +, 0)$ et $(\mathbf{N}, \times, 1)$.

• Les exemples qui suivent, où $L \subseteq \mathcal{A}^*$ est un langage sur $\mathcal{A}$, ne font que résumer quelques propriétés déjà vues :

- $(L^*, \cdot, \varepsilon)$, en particulier $(\mathcal{A}^*, \cdot, \varepsilon)$,
- $(\mathcal{P}(L^*), +, \emptyset)$, en particulier $(\mathcal{P}(\mathcal{A}^*), +, \emptyset)$,
- $(\mathcal{P}(L^*), \cdot, \varepsilon)$, en particulier $(\mathcal{P}(\mathcal{A}^*), \cdot, \varepsilon)$.

5.2 – Propriété principale de $\mathcal{A}^*$.

Lorsque l'on passe des ensembles aux applications, on est conduit à la définition suivante :

Morphismes de monoïdes

Soient $(D, \times, e)$ et $(D', \times', e')$ deux monoïdes.
Un morphisme $(D, \times, e) \to (D', \times', e')$ *est une application* $h : D \to D'$ *qui vérifie les propriétés suivantes :*

- $h(e) = e'$,
- $h(x \times y) = h(x) \times' h(y)$ *quels que soient* $x \in D$ *et* $y \in D$.

Par exemple, l'application "longueur" $u \mapsto |u|$ définit un morphisme $(\mathcal{A}^*, \cdot, \varepsilon) \to (\mathbf{N}, +, 0)$.

La plupart des morphismes de monoïdes provient de la construction suivante.

Propriété principale de $\mathcal{A}^*$

Soit $(D, \times, e)$ *un monoïde, alors*

toute application $f : \mathcal{A} \to D$ *s'étend de façon unique en un morphisme de monoïdes* $(\mathcal{A}^*, \cdot, \varepsilon) \to (D, \times, e)$.

Vérification de la propriété principale.

Si un tel morphisme $\overline{f}$ existe :

- "$\overline{f}$ étend f" signifie que $\overline{f}(x) = f(x)$ pour tout $x \in \mathcal{A}$;
- "$\overline{f}$ est un morphisme de monoïdes" implique $\overline{f}(\varepsilon) = e$ et, pour tout $u \in \mathcal{A}^*$ et tout $x \in \mathcal{A}$, $\overline{f}(ux) = \overline{f}(u) \times \overline{f}(x) = \overline{f}(u) \times f(x)$.

Or, les conditions

(1) $\overline{f}(\varepsilon) = e$

(2) $\overline{f}(ux) = \overline{f}(u) \times f(x)$ pour tout $u \in \mathcal{A}^*$ et tout $x \in \mathcal{A}$

définissent entièrement $\overline{f}$ par récurrence sur les mots sur $\mathcal{A}$.

L'application ainsi obtenue est un morphisme de monoïdes :

- on sait déjà que $\overline{f}(\varepsilon) = e$,
- il reste donc à vérifier que l'on a $\overline{f}(u \cdot v) = \overline{f}(u) \times \overline{f}(v)$ pour tout $u \in \mathcal{A}^*$ et tout $v \in \mathcal{A}^*$.

Ceci se fait par récurrence :

$$\begin{aligned} \overline{f}(u \cdot \varepsilon) &= \overline{f}(u) && (u \cdot \varepsilon = u) \\ &= \overline{f}(u) \times e && (e \text{ est neutre pour } \times) \\ &= \overline{f}(u) \times \overline{f}(\varepsilon) && (\text{par (1) ci–dessus}) \end{aligned}$$

Supposons que $\overline{f}(u \cdot v) = \overline{f}(u) \times \overline{f}(v)$ et soit $x \in \mathcal{A}$:

$$\begin{aligned} \overline{f}(u \cdot (vx)) &= \overline{f}((u \cdot v)x) && (u \cdot (ux) = (u \cdot v)x) \\ &= \overline{f}(u \cdot v) \times f(x) && (\text{par (2) ci–dessus}) \\ &= (\overline{f}(u) \times \overline{f}(v)) \times f(x) && (\text{HR}) \\ &= \overline{f}(u) \times (\overline{f}(v) \times f(x)) && (\text{associativité de } \times) \\ &= \overline{f}(u) \times \overline{f}(vx) && (\text{par (2) ci–dessus}) \end{aligned}$$

Intérêt de la propriété principale.

Dès que $\mathcal{A}$ n'est pas vide, $\mathcal{A}^*$ est infini, même lorsque $\mathcal{A}$ est fini, ce qui sera le cas dans toutes nos applications.

Vocabulaire et convention.

Nous dirons que l'application $\overline{f}$ ci–dessus est l'*extension de f aux mots* et, en nous inspirant de l'identification $\mathcal{A}$ à une partie de $\mathcal{A}^*$, nous la noterons simplement f : la propriété précédente nous le permet !

Application : les substitutions.

Soit $\mathcal{B}$ un second alphabet. L'extension aux mots d'une application $f : \mathcal{A} \to \mathcal{P}(\mathcal{B}^*)$, est un morphisme de monoïdes

$$(\mathcal{A}^*, \cdot, \varepsilon) \to (\mathcal{P}(\mathcal{B}^*), \cdot, \varepsilon).$$

Exemple.

Soit $\mathcal{A} = a + b$ un alphabet à deux lettres et soit f l'application définie par $f(a) = L$ et $f(b) = M$ où L et M sont deux langages sur $\mathcal{B}$, alors, par exemple

$$f(abaa) = LMLL.$$

Plus généralement, $f(u)$ est obtenu en remplaçant chaque caractère x de u par $f(x) \subseteq \mathcal{B}^*$.
Pour cette raison, une application du type $f : \mathcal{A} \to \mathcal{P}(\mathcal{B}^*)$ s'appelle souvent *une substitution*.

6 – Les substitutions.

Les substitutions jouent un grand rôle.

6.1 – Extension aux langages.

La somme (généralisée) est la réunion notée additivement :

pour tout ensemble I d'indices et toute famille $(L_i)_{i\in I}$ de langages sur $\mathcal{A}$, $\sum_{i\in I} L_i$ désigne la somme des membres de cette famille, c'est–à–dire le langage sur $\mathcal{A}$ défini par

$$u \in \sum_{i\in I} L_i \text{ ssi il existe } i \in I \text{ tel que } u \in L_i.$$

ar exemple, tout langage est la somme de ses sous langages à un seul mot :

$$L = \sum_{u\in L} u.$$

Applications préservant les sommes

Une application $f : \mathcal{P}(A^*) \to \mathcal{P}(B^*)$ *préserve les sommes* ssi on a

$$f(\sum_{i\in I} L_i) = \sum_{i\in I} f(L_i)$$

pour toute famille $(L_i)_{i\in I}$ de langages sur $\mathcal{A}$.

Remarques et propriétés immédiates.

Soit $f : \mathcal{P}(A^*) \to \mathcal{P}(B^*)$ une application préservant les sommes.

- $f(L) = \sum_{u \in L} f(u)$ pour tout $L \subseteq \mathcal{A}^*$ puisque $L = \sum_{u \in L} u$.
- f préserve aussi les sommes finies :
  - $f(\emptyset) = \emptyset$
  - $f(L + M) = f(L) + f(M)$.
- f est croissante c'est–à–dire que pour tout L et tout $M \subseteq \mathcal{A}^*$, $L \subseteq M$ implique $f(L) \subseteq f(M)$.

Extension aux langages

Toute application $f : \mathcal{A}^* \to \mathcal{P}(B^*)$ s'étend de façon unique en une application $\mathcal{P}(A^*) \to \mathcal{P}(B^*)$ préservant les sommes.

En effet, supposons qu'une telle application $\overline{f}$ existe :

- "$\overline{f}$ étend f" signifie que $\overline{f}(u) = f(u)$ pour tout $u \in \mathcal{A}^*$;
- "$\overline{f}$ préserve les sommes" implique alors que $\overline{f}(L) = \sum_{u \in L} \overline{f}(u)$ pour tout $L \subseteq \mathcal{A}^*$.

Or, ceci définit entièrement $\overline{f}$ à partir de f par

$$\overline{f}(L) = \sum_{u \in L} f(u)$$

et on peut vérifier que l'application ainsi obtenue préserve les sommes.

Vocabulaire et convention.

L'application $\overline{f}$ ci–dessus est appelée l'*extension de f aux langages* et, est notée simplement f.

$$\boxed{v \in f(L) \text{ ssi il existe } u \in L \text{ tel que } v \in f(u).}$$

Application.

Soit $f : \mathcal{A} \to \mathcal{P}(\mathcal{B}^*)$ une substitution.

Par ce qui précède :

- f admet une extension unique aux mots
$$f : \mathcal{A}^* \to \mathcal{P}(\mathcal{B}^*)$$
qui est un morphisme de monoïdes
$$(\mathcal{A}^*, \cdot, \varepsilon) \to (\mathcal{P}(\mathcal{B}^*), \cdot, \varepsilon)).$$
- Cette dernière admet à son tour une extension unique aux langages
$$f : \mathcal{P}(\mathcal{A}^*) \to \mathcal{P}(\mathcal{B}^*)$$
cette extension est encore un morphisme de monoïdes
$$f : (\mathcal{P}(\mathcal{A}^*), \cdot, \varepsilon) \to (\mathcal{P}(\mathcal{B}^*), \cdot, \varepsilon).$$

Plus explicitement :

- $f(\varepsilon) = \varepsilon$,
- $f(LM) = f(L)f(M)$,

quels que soient $L \subseteq \mathcal{A}^*$ et $M \subseteq \mathcal{A}^*$.

En particulier :

- $f(L^i) = f(L)^i$ pour tout entier naturel i,
- $f(L^*) = f(L)^*$.

Exemple.

Une propriété comme $(L + M)^* = (L^*M^*)^*$ est assez délicate à démontrer directement lorsque L et M sont des langages quelconques.
Démontrer que l'on a $(a + b)^* = (a^*b^*)^*$ lorsque a et b sont des caractères, est beaucoup plus facile à concevoir et à écrire ; cette preuve est cependant suffisante pour obtenir le cas général : il suffit de considérer l'application $f : a + b \to \mathcal{P}(\mathcal{A}^*)$ telle que $f(a) = L$ et $f(b) = M$ et d'appliquer la substitution qu'elle définit aux deux membres de l'égalité précédente.

Résumons :

Extension d'une substitution aux langages

Toute substitution $f : \mathcal{A} \to \mathcal{P}(\mathcal{B}^*)$ s'étend de façon unique en une application $\overline{f} : \mathcal{P}(\mathcal{A}^*) \to \mathcal{P}(\ B^*)$ qui vérifie les deux propriétés :

- *$\overline{f}$ préserve les sommes généralisées,*
- *$\overline{f}$ est un morphisme de monoïdes*

$$(\mathcal{P}(\mathcal{A}^*), \cdot, \varepsilon) \to (\mathcal{P}(\mathcal{B}^*), \cdot, \varepsilon).$$

$\overline{f}$ est appelée l'*extension de f aux langages* et est le plus souvent notée f.