le cnam

Codes et Automates finis

Cours 1 Matrices

- Avant propos : le corps $\mathbb{F}_2$ des nombres modulo 2

Pour ce cours, nous utiliserons d'une part les nombres réels, supposés connus du lecteur, et d'autre part les nombres modulo 2, objet de ce paragraphe. On pose $\mathbb{F}_2 = \{0, 1\}$ et on définit sur cet ensemble composé de deux éléments une addition et une multiplication.
L'addition est définie par les quatre relations $0+0=0$, $0+1=1+0=1$ et enfin $1+1=0$.
Elle est associative : $\forall \alpha, \beta, \gamma \in \mathbb{F}_2$, $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$.
Elle est commutative : $\forall \alpha, \beta \in \mathbb{F}_2$, $\alpha+\beta = \beta+\alpha$.
Le nombre 0 est élément neutre : $\forall \alpha \in \mathbb{F}_2$, $\alpha+0 = 0+\alpha = \alpha$.
Tout élément de $\mathbb{F}_2$ admet un opposé : $\forall \alpha \in \mathbb{F}_2$, $\exists \alpha' \in \mathbb{F}_2$, $\alpha+\alpha' = \alpha'+\alpha = 0$. On peut remarquer que dans $\mathbb{F}_2$ l'opposé du nombre α est égal à α lui-même : tout nombre de $\mathbb{F}_2$ est égal à son oppsé.
Toutes ces propriétés font de $\mathbb{F}_2$ muni de l'addition un groupe commutatif. On l'exprime sous la forme suivante : $(\mathbb{F}_2, +)$ est un groupe commutatif.
La multiplication est définie par les quatre relations $0\times 0=0$, $0\times 1 = 1\times 0 = 0$, $1\times 1 = 1$.
Elle est associative : $\forall \alpha, \beta, \gamma \in \mathbb{F}_2$, $(\alpha\times\beta)\times\gamma = \alpha\times(\beta\times\gamma)$.
Elle est commutative : $\forall \alpha, \beta \in \mathbb{F}_2$, $\alpha\times\beta = \beta\times\alpha$.
Le nombre 1 est élément neutre : $\forall \alpha \in \mathbb{F}_2$, $\alpha\times 1 = 1\times\alpha = \alpha$.
Tout élément non nul de $\mathbb{F}_2$ admet un inverse : $\forall \alpha \in \mathbb{F}_2 \backslash \{0\}$, $\exists \alpha' \in \mathbb{F}_2$, $\alpha\times\alpha' = \alpha'\times\alpha = 1$.
En effet, le seul nombre inversible est le nombre 1.
La multiplication est distributive par rapport à l'addition :
$\forall \alpha, \beta, \gamma \in \mathbb{F}_2$, $\alpha\times(\beta+\gamma) = (\alpha\times\beta)+(\alpha\times\gamma)$,
$\forall \alpha, \beta, \gamma \in \mathbb{F}_2$, $(\alpha+\beta)\times\gamma = (\alpha\times\gamma)+(\beta\times\gamma)$.
L'ensemble de toutes ces propriétés se résume en disant que $(\mathbb{F}_2, +, \times)$ est un corps commutatif. Notons que pour les nombres réels, on a aussi la propriété de corps commutatif pour la structure $(\mathbb{R}, +, \times)$, mais l'addition n'est pas la même ! Pour les réels, on a $1+1=2$ alors que dans $\mathbb{F}_2$, on a $1+1=0$.

- Définition des matrices

On se donne deux nombres entiers n et m supérieurs ou égaux à 1. Une matrice A à n lignes et m colonnes est un tableau de nm nombres a_{ij}. L'entier i est l'indice de ligne $(1 \leq i \leq n)$ et j est l'indice de colonne $(1 \leq j \leq m)$. On note $A = \begin{pmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1m} \\ \vdots & & \vdots & & \vdots \\ a_{i1} & \cdots & a_{ij} & \cdots & a_{im} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nm} \end{pmatrix}$ ou plus

---

François Dubois, février 2024.

simplement $A = \big(a_{ij}\big)_{1\leq i\leq n,\,1\leq j\leq m}$. Le nombre a_{ij} est appelé "élément de matrice $(i,\,j)$ de la matrice A".
Pour $n = m = 1$, une matrice est un simple nombre. Pour $n = 2$ et $m = 1$, la matrice $A = \begin{pmatrix} a \\ b \end{pmatrix}$ est une matrice colonne ; on parle aussi un "vecteur colonne" si $m = 1$. Si $n = 1$ et $m = 2$, on a par exemple $A = \begin{pmatrix} \alpha & \beta \end{pmatrix}$ et la matrice A est dans ce cas un "vecteur ligne". Si $n = m = 2$, la matrice A est une matrice carrée d'ordre deux : $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
Nous notons $\mathscr{M}_{nm}$ l'ensemble des matrices à n lignes et m colonnes s'il n'y a pas d'ambiguïté sur les nombres qui composent ses éléments. S'il faut préciser où vivent les éléments de matrice, on introduit la notation $\mathscr{M}_{nm}(\mathbb{R})$ dans le cas des nombres réels ou $\mathscr{M}_{nm}(\mathbb{F}_2)$ pour les nombres modulo 2. Pour les matrices carrées, on simplifie la notation et $\mathscr{M}_n \equiv \mathscr{M}_{nn}$.
Dans $\mathscr{M}_{nm}$, la matrice nulle, notée simplement 0, est composée uniquement de zéros : $0_{ij} = 0$ pour toute ligne i et toute colonne j.

• Égalité de deux matrices

On dit que les matrices A et B sont égales lorsque les trois propriétés suivantes sont satisfaites :
(i) le nombre n de lignes de la matrice A est égal au nombre de lignes de la matrice B
(ii) le nombre m de colonnes de la matrice A est égal au nombre de colonnes de la matrice B
(iii) pour tout i et j tel que $1 \leq i \leq n$ et $1 \leq j \leq m$, les éléments de matrice a_{ij} et b_{ij} sont égaux : $a_{ij} = b_{ij}$ pour toute ligne i et toute colonne j.
On retiendra surtout qu'on ne peut pas comparer deux matrices qui n'ont pas les mêmes dimensions.

• Somme de deux matrices

On peut ajouter deux matrices qui ont toutes deux le même nombre de lignes et le même nombre de colonnes. Si $A \in \mathscr{M}_{nm}$ et $B \in \mathscr{M}_{nm}$, alors $A+B \in \mathscr{M}_{nm}$ et l'élément de matrice $(i,\,j)$ de la matrice $A+B$ vaut $a_{ij} + b_{ij}$.

• Multiplication d'un scalaire par une matrice

Si λ est un nombre et $A \in \mathscr{M}_{nm}$ une matrice à n lignes et m colonnes, alors λA est une matrice à n lignes et m colonnes et son élément de matrice $(i,\,j)$ est égal à $\lambda\, a_{ij}$ pour toutes les valeurs de i et j tels que $1 \leq i \leq n$ et $1 \leq j \leq m$.
On a toujours $(\lambda+\mu)A = (\lambda A) + (\mu A)$, $(\lambda\,\mu)A = \lambda(\mu A)$ et $\lambda\,(A+B) = (\lambda A) + (\lambda B)$.

• Transposition

Si $A \in \mathscr{M}_{nm}$, sa transposée A^{t} appartient à $\mathscr{M}_{mn}$: on l'obtient en échangeant les lignes et les colonnes de la matrice A. Si l'élément de matrice $(i,\,j)$ de A est égal à a_{ij}, l'élément (j,i) de A^{t} vaut également a_{ij}.

• Produit de deux matrices

On se donne deux matrices $A \in \mathscr{M}_{nm}$ et $B \in \mathscr{M}_{mp}$: le nombre de colonnes de la matrice A et égal au nombre de lignes de la matrice B. Dans ce cas, et dans ce cas uniquement, on peut effectuer le produit AB de la matrice A par la matrice B. L'élément de matrice (i,k) de la matrice AB est égal à $(AB)_{ik} = \sum_{j=1}^{m} a_{ij}\, b_{jk} = a_{i1}b_{1k} + a_{i2}b_{2k} + \ldots + a_{im}b_{mk}$. En général, même si le produit AB existe, le produit BA n'existe pas.

On considère l'exemple très courant $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $X = \begin{pmatrix} x \\ y \end{pmatrix}$. On a alors $AX = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$.
On remarque que le produit XA n'est pas défini car le nombre [1] de colonnes de X n'est pas égal au nombre [2] de lignes de A.
Même si les deux produits AB et BA peuvent être calculés, ils définissent en général des matrices d'ordres différents. On pose par exemple $A = \begin{pmatrix} \alpha & \beta \end{pmatrix}$ (matrice d'une seule ligne et deux colonnes) et $B = \begin{pmatrix} a \\ b \end{pmatrix}$ (matrice de deux lignes et une colonne). Alors $AB = (\alpha\, a + \beta\, b)$ est une matrice à une seule ligne et une seule colonne. Par ailleurs $BA = \begin{pmatrix} a\alpha & a\beta \\ b\alpha & b\beta \end{pmatrix}$ est cette fois une matrice à deux lignes et deux colonnes.
Dès que les opérations écrites ci-dessous ont un sens, on a (A, B et C sont des matrices, λ et μ des nombres) : $A\,(B+C) = AB+AC$, $(A+B)C = AC+BC$, $A\,(\lambda\, B) = (\lambda\, A)B = \lambda\,(AB)$.

- Associativité du produit des matrices

On se donne trois matrices $A \in \mathscr{M}_{nm}$, $B \in \mathscr{M}_{mp}$ et $C \in \mathscr{M}_{pq}$. Quand on effectue le produit AB, on trouve une matrice à n lignes et p colonnes. On peut donc multiplier cette matrice AB à droite par la matrice C et le produit de matrices $(AB)C$ est bien défini dans $\mathscr{M}_{nq}$. De façon analogue, on peut effectuer le produit BC des matrices B et C: c'est une matrice à m lignes et q colonnes. On peut donc la multiplier à gauche par la matrice A: la matrice $A\,(BC)$ est bien définie et elle appartient encore à $\mathscr{M}_{nq}$. L'associativité du produit des matrices exprime que $(AB)C = A\,(BC)$: on place les parenthèses comme on veut quand on doit faire le produit de trois matrices ou plus.

- Transposition et produit

Si le produit AB des deux matrices A et B est bien défini, alors le produit $B^{\mathrm{t}}A^{\mathrm{t}}$ des transposées est lui aussi bien défini et on a $(AB)^{\mathrm{t}} = B^{\mathrm{t}}A^{\mathrm{t}}$.

- Produit de matrices carrées

Rappelons qu'une matrice carrée a le même nombre de lignes et de colonnes, appelé aussi ordre de la matrice. Si A et B sont deux matrices carrées de même ordre, le produit AB est toujours défini et c'est une matrice carrée d'ordre n. On remarque qu'il en est de même du produit BA.
La matrice identité I a tous ses éléments nuls, sauf ses élémets diagonaux $(j = i)$ pour lesquels $\mathrm{I}_{ij} = 1$. Si on introduit le symbole de Kronecker δ_{ij} tel que $\delta_{ii} = 1$ et $\delta_{ij} = 0$ si $i \neq j$, on a $\mathrm{I}_{ij} = \delta_{ij}$. Tout comme le nombre 1 pour la multiplication des nombres usuels, la matrice identité est un élément neutre pour la multiplication des matrices : $A\mathrm{I} = \mathrm{I}A = A$ pour toute matrice carrée A.
Si A et B sont deux matrices carrées d'ordre n, on peut toujours calculer les produits AB et BA. Il sont en général différents. L'ordre dans lequel on effectue le produit de deux matrices est toujours important ; le produit des matrices carrée n'est pas commutatif.
On a par exemple, avec $n = 2$:
$\begin{pmatrix} -1 & 1 \\ 3 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ 0 & 3 \end{pmatrix} \neq \begin{pmatrix} 3 & 0 \\ -2 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 3 & 0 \end{pmatrix}$ et

$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$

- Diviseurs de zéro

Dans l'ensemble $\mathscr{M}_n$ (qui a une structure d'anneau pour l'addition des matrices et leur multiplication), il existe des "diviseurs de zéro". On peut trouver des matrices A et B toutes deux non nulles telles que leur produit est nul. Le produit de deux matrices carrées peut être nul sans qu'aucun des facteurs ne soit nul : on peut avoir $AB = 0$ avec $A \neq 0$ et $B \neq 0$.

Par exemple avec $A = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, on a $AB = 0$, matrice nulle. On a aussi

$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = 0.$

- Inverse d'une matrice carrée

On se donne une matrice carrée A d'ordre n. Si on peut trouver une matrice B telle que $AB = BA = \mathrm{I}$, la matrice A est inversible. On pose $B = A^{-1}$.

Si la matrice carrée A est inversible, la matrice inverse A^{-1} est unique.

On a par exemple $\begin{pmatrix} -1 & 1 \\ 3 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & \frac{1}{3} \\ 1 & \frac{1}{3} \end{pmatrix}$, $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ -a & 1 \end{pmatrix}$.

La matrice carrée deux par deux générale $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est inversible si et seulement si le déterminant de A, $\det A \equiv ad - bc$ est non nul. Dans ce cas $A^{-1} = \dfrac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Pour déterminer la matrice inverse de A, on résout le système linéaire général $AX = B$, d'inconnue $X = \begin{pmatrix} x \\ y \end{pmatrix}$ et de second membre $B = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$. L'expression de x en fonction de α et β détermine la première ligne de A^{-1} ; l'expression de y en fonction de α et β détermine la seconde ligne de la matrice inverse [exercice : vérifier ces propriétés].

Si $ad - bc = 0$, les matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $\widetilde{A} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ sont deux diviseurs de zéro : $A\widetilde{A} = 0$. On a aussi $\widetilde{A}A = 0$.

Exercices

- Opérations matricielles (d'après Françoise Santi)

On considère les matrices suivantes $A = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ et $C = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

a) Parmi les opérations suivantes, indiquer celles qui sont possibles et celles qui sont impossibles : $A+B$, $A+C$, $B+C$, AC, CA, BC, A^2, B^2, A^{-1} et B^{-1}.

b) Effectuer les opérations possibles, en considérant les matrices à coefficients dans $\mathbb{R}$.

$$\left[CA = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 2 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}\right]$$

c) Effectuer les opérations possibles, en considérant cette fois les matrices comme étant à coefficients dans $\mathbb{F}_2$.

- Transposition (d'après Françoise Santi)

On pose $A = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$, $a = \begin{pmatrix} 1 & 0 & 1 & 0 \end{pmatrix}$ et $b = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$.

a) Parmi les opérations suivantes, effectuer celles qui sont possibles :
AB, $A\,(A^{\mathrm{t}})$, $A\,a$, aA, $A\,(a^{\mathrm{t}})$, $(b^{\mathrm{t}})A$, $B\,a$ et $B\,b$.

b) Des résultats de la question précédente, déduire (sans calcul) les valeurs de
$a\,(A^{\mathrm{t}})$, $(B\,b)^{\mathrm{t}}$ et $(b^{\mathrm{t}})\,B$.

c) Déterminer $a\,(A^{\mathrm{t}})\,B\,b$ et $(b^{\mathrm{t}})\,A\,(A^{\mathrm{t}})\,b$.

- Un résultat général pour la transposition

On se donne trois entiers n, m et p positifs non nuls et deux matrices $A \in \mathscr{M}_{nm}$ et $B \in \mathscr{M}_{mp}$. Les éléments de ces matrices sont notés a_{ij} et b_{jk} respectivement pour $1 \leq i \leq n$, $1 \leq j \leq m$ et $1 \leq k \leq p$.

a) Pour $1 \leq i \leq n$ et $1 \leq k \leq p$, rappeler l'expression de l'élément de matrice $(AB)_{ik}$ en fonction des a_{ij} et des b_{jk}.

b) Pourquoi le produit de matrices $B^{\mathrm{t}}A^{\mathrm{t}}$ est-il bien défini ?

c) Pour $1 \leq k \leq p$ et $1 \leq i \leq n$, calculer l'élément de matrice $\left(B^{\mathrm{t}}A^{\mathrm{t}}\right)_{ki}$.

d) Déduire des questions précédentes la relation générale $(AB)^{\mathrm{t}} = B^{\mathrm{t}}A^{\mathrm{t}}$.

- Grandes puissances (d'après Françoise Santi)

Dans cet exercice, toutes les matrices sont des matrices carrées d'ordre deux. Leurs coefficients sont définis dans $\mathbb{F}_2$. On pose $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.

a) Calculer A^2 et A^3.

b) Que vaut A^{71} ? $\left[\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\right]$

c) Quelles sont les matrices M telles que $(M^{\mathrm{t}})AM = A^2$?

- Grandes puissances avec des matrices trois par trois (d'après Françoise Santi)

Dans cet exercice, toutes les matrices sont des matrices carrées d'ordre trois. Leurs coefficients sont définis dans $\mathbb{F}_2$. On pose $\mathrm{I} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ et $m = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

a) Calculer m^2 et m^3.

b) Trouver deux coefficients α et β dans $\mathbb{F}_2$ de sorte que $m^3 = \alpha\mathrm{I} + \beta m$.

c) De la relation précédente déduire successivement m^4, m^5, m^6 et m^7 en fonction de I, m et m^2.

d) En utilisant l'expression de m^7, préciser la valeur de la matrice m^{71}.

e) Que vaut $(m^{\mathrm{t}})^{71}$?