# Chapitre 8. Suites et Matrices

Boulanger Yann

03 juillet 2025

## Table des matières

# 1 Introduction

Une motivation : larithmétique est au cur du cryptage des communications.
Pour crypter un message on commence par le transformer en un (ou plusieurs) nombre(s).
Le processus de codage et décodage fait appel à plusieurs notions de ce chapitre :

— Choix de deux nombres premiers $p$ et $q$ que lon garde secrets, on pose $n = p \times q$.

— La clé secrète et la clé publique se calculent à laide de lalgorithme dEuclide
et des coefficients de Bézout.

# 2 Suites de matrices colonnes

**Définition 1**
Soit $n \in \mathbb{N}$. On appelle **suite de matrices colonnes**, notée $(U_n)$, une suite de matrices colonnes dont les éléments sont des termes de suites numériques.

**Exemple**
Soit

$$U_n = \begin{pmatrix} n^2 \\ n+1 \\ 3n \end{pmatrix}$$

Cest une suite de matrices colonnes de dimension $3 \times 1$, dont les coefficients sont les suites $a_n = n^2$, $b_n = n + 1$ et $c_n = 3n$.

Par exemple : $U_0 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad U_1 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \quad U_5 = \begin{pmatrix} 25 \\ 6 \\ 15 \end{pmatrix}$

**Remarque :** On peut définir de même des suites de matrices lignes.

**Propriété 1**
Soit $A$ une matrice carrée d'ordre $k$ et $(U_n)$ une suite de matrices colonnes de dimension $k \times 1$ telle que $U_{n+1} = AU_n$, alors pour tout $n \in \mathbb{N}$ :

$$U_n = A^n U_0$$

*Démonstration :* à faire en exercice (en classe).

**Exemples**

— Soit $A = \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix}, \quad U_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ Alors $U_{n+1} = AU_n$, et donc $U_5 = A^5 U_0$.

— Soit $a_0 = 1$, $b_0 = -1$, et $a_{n+1} = 2a_n - 3b_n, \quad b_{n+1} = 4a_n + b_n$.
On pose $U_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$, alors : $A = \begin{pmatrix} 2 & -3 \\ 4 & 1 \end{pmatrix}, \quad U_{n+1} = AU_n$

**Définition 2**
Une suite $(U_n)$ de matrices converge si et seulement si chacune des suites numériques constituant ses coefficients converge. Sa limite est alors la matrice formée des limites de ces suites.

**Définition 3**
Soit $A$ une matrice carrée d'ordre $k$ et $B$ une matrice colonne de dimension $k \times 1$.
Soit $(U_n)$ une suite de matrices colonnes définie par :

$$U_{n+1} = AU_n + B$$

Un **état stable** de cette suite est une matrice colonne $S$ telle que :

$$S = AS + B$$

**Propriété 2** Si la suite $(U_n)$ converge, alors sa limite est l'état stable $S$.

**Propriété 3** Si $I_k - A$ est inversible, alors la suite admet un état stable $S$ donné par :

$$S = (I_k - A)^{-1}B$$

# 3 Chaînes de Markov

## 3.1 Graphe probabiliste

**Définition 4**
Un graphe probabiliste est un graphe orienté et pondéré tel que :

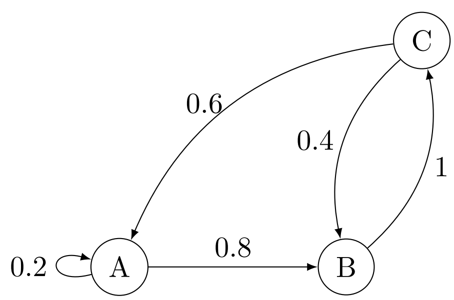
— Tous les poids sont compris entre 0 et 1 : ce sont des probabilités.

— La somme des poids des arcs issus dun même sommet est égale à 1.

La matrice dadjacence dun graphe probabiliste est une **matrice stochastique** :
une matrice carrée à coefficients positifs dont la somme sur chaque ligne est égale à 1.

Exercice

1. Donner la matrice dadjacence du graphe suivant et vérifier quil sagit dune matrice stochastique :

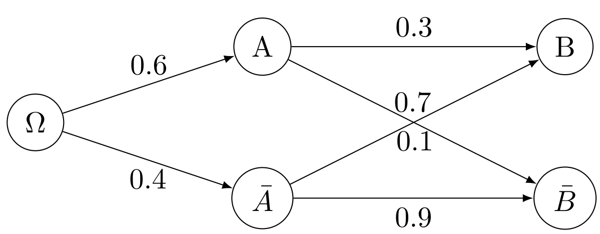



Matrice d'adjacence :

$$M = \begin{pmatrix} 0.2 & 0.8 & 0 \\ 0 & 0 & 1 \\ 0.6 & 0.4 & 0 \end{pmatrix}$$

2. Un arbre pondéré peut-être vu comme un graphe probabiliste avec deux événements $A$ et $B$ tels que : $P(A) = 0.6$ $P_A(B) = 0.3$ et $P_{\bar{A}}(B) = 0.1$.

Graphe



Déterminer les probabilités suivantes : $P(B)$, $P_B(A)$ et $P_{\bar{B}}(A)$ puis en déduire l'arbre de probabilité inversé.

Déterminer alors finalement le graphe orienté complet (à quatre sommets : $A$, $\bar{A}$, $B$, $\bar{B}$) et en donner la matrice d'adjacence.

### 3.2 Chaîne de Markov

**Définition 5**
Une **chaîne de Markov** est une suite de variables aléatoires $(X_n)$ définies sur un espace probabilisé et à valeurs dans un ensemble $E$ (appelé espace détats), telle que :

$$\mathbb{P}(X_{n+1} = e_{n+1} \mid X_n = e_n, X_{n-1} = e_{n-1}, \dots, X_0 = e_0) = \mathbb{P}(X_{n+1} = e_{n+1} \mid X_n = e_n)$$

Autrement dit, la situation du système à linstant $n+1$ dépend uniquement de celle à linstant $n$.

**Exemples**

(a) Une urne contient 10 boules noires et 10 boules blanches. On effectue une série de tirages : à chaque étape, on tire une boule et on remet celle de létape précédente.
On note $X_n$ la couleur de la boule tirée au rang $n$.
Lespace détats est : $E = \{\text{noire}, \text{blanche}\}$.

(b) Un jour donné, la météo peut être : beau ($B$), variable ($V$), ou mauvais ($M$).
- Si $X_n = B$ alors :
$$\begin{cases} \mathbb{P}(X_{n+1} = B) = \frac{1}{2}, \\ \mathbb{P}(X_{n+1} = V) = \frac{4}{10}, \\ \mathbb{P}(X_{n+1} = M) = \frac{1}{10}. \end{cases}$$
- Si $X_n = M$ alors :
$$\begin{cases} \mathbb{P}(X_{n+1} = M) = \frac{1}{2}, \\ \mathbb{P}(X_{n+1} = V) = \frac{4}{10}, \\ \mathbb{P}(X_{n+1} = B) = \frac{1}{10}. \end{cases}$$
- Si $X_n = V$ alors :
$$\mathbb{P}(X_{n+1} = B) = \mathbb{P}(X_{n+1} = M) = \mathbb{P}(X_{n+1} = V) = \frac{1}{3}.$$

L'espace détats est $E = \{B, V, M\}$.

**Définition 6**
Une chaîne de Markov est dite **homogène** si les probabilités de transition ne dépendent pas de $n$. On note alors $p_{i,j} = \mathbb{P}(X_{n+1} = j \mid X_n = i)$ et la matrice $P = (p_{i,j})$ est appelée **matrice de transition**.

**Remarque**
Dans une chaîne homogène, la probabilité de transition vers un état $j$ dépend uniquement de létat actuel $i$, pas de lindice $n$ :

$$\mathbb{P}(X_{n+1} = j \mid X_n = i) = \mathbb{P}(X_1 = j \mid X_0 = i) = p_{i,j}$$

**Propriétés 4**
— $P$ est une matrice stochastique.
— Si $\pi_0$ est la distribution initiale, alors la distribution au rang $n$ est donnée par :

$$\pi_n = \pi_0 P^n$$

*Démonstration*
Par définition :

$$p_{i,j} = \mathbb{P}(X_{n+1} = j \mid X_n = i) = \frac{\mathbb{P}(X_n = i,\ X_{n+1} = j)}{\mathbb{P}(X_n = i)} \quad (\text{si } \mathbb{P}(X_n = i) > 0)$$

Donc les $p_{i,j}$ sont des probabilités conditionnelles, et donc $0 \leq p_{i,j} \leq 1$.
De plus, pour chaque $i$, la somme des $p_{i,j}$ sur $j$ vaut :

$$\sum_{j=1}^{n} p_{i,j} = \sum_{j=1}^{n} \mathbb{P}(X_{n+1} = j \mid X_n = i) = \mathbb{P}(X_{n+1} \in E \mid X_n = i) = 1$$

Ainsi, chaque ligne de $P$ est une loi de probabilité.

**Propriété 5** Évolution de la distribution
Soit $\pi_n = (\mathbb{P}(X_n = i))_{i \in E}$ la distribution de la variable $X_n$.
Alors on a :

$$\pi_{n+1} = \pi_n P \quad \text{et par récurrence :} \quad \pi_n = \pi_0 P^n$$

Cela permet de déterminer les lois à tous les instants à partir de létat initial $\pi_0$.

**Démonstration de la formule $\pi_{n+1} = \pi_n P$**

La matrice de transition $P = (p_{i,j})$ contient les probabilités de transition dun état à lautre :

$$p_{i,j} = \mathbb{P}(X_{n+1} = j \mid X_n = i) = \frac{\mathbb{P}(X_n = i \text{ et } X_{n+1} = j)}{\mathbb{P}(X_n = i)}$$

Soit $\pi_n = (\pi_n(1), \pi_n(2), \ldots, \pi_n(k))$ la distribution de $X_n$, et $P = (p_{i,j})$ la matrice de transition.
Le produit matriciel $\pi_n P$ est défini par :

$$\pi_{n+1}(j) = \sum_{i=1}^{k} \pi_n(i) \cdot p_{i,j} = \sum_{i=1}^{k} \mathbb{P}(X_n = i) \cdot \mathbb{P}(X_{n+1} = j \mid X_n = i)$$

Mais cela correspond à la formule des probabilités totales :

$$\mathbb{P}(X_{n+1} = j) = \sum_{i=1}^{k} \mathbb{P}(X_n = i \text{ et } X_{n+1} = j) = \sum_{i=1}^{k} \mathbb{P}(X_n = i) \cdot \mathbb{P}(X_{n+1} = j \mid X_n = i)$$

Donc :

$$\pi_{n+1}(j) = \mathbb{P}(X_{n+1} = j) = (\pi_n P)_j$$

**Conclusion :** Pour tout $n$, la distribution à linstant $n+1$ est donnée par le produit de la distribution précédente par la matrice de transition :

$$\pi_{n+1} = \pi_n P \quad \text{et donc par récurrence :} \quad \pi_n = \pi_0 P^n$$

■

**Exemple 1** Chaîne de Markov à trois états $A$, $B$, $C$ avec :

$$P = \begin{pmatrix} 0.2 & 0 & 0.8 \\ 0.1 & 0.3 & 0.6 \\ 0.5 & 0.5 & 0 \end{pmatrix} \quad \text{et} \quad \pi_0 = (0.5, 0.5, 0)$$

**Exemple 2 :** Étudiants en grève :

$$P = \begin{pmatrix} 0.7 & 0.3 \\ 0.33 & 0.67 \end{pmatrix}, \quad \pi_0 = (0.2, 0.8)$$

### 3.3 Distribution invariante

**Définition 7**

Une **distribution invariante** dune chaîne de Markov de matrice de transition $P$ est une matrice ligne $\pi$ telle que : $\pi P = \pi$

**Remarque**

Cela revient à résoudre $\pi(I_n - P) = 0$, en imposant que $\pi$ est une distribution de probabilité (somme des coefficients = 1).

**Exemple :**

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad I - P = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \Rightarrow \det(I - P) = 0$$

Il existe une infinité de solutions, par exemple $\pi = \left(\frac{1}{2}, \frac{1}{2}\right)$.

**Théorème 1**

Si $(\pi_n)$ converge, alors la limite est une distribution invariante.

**Pour les chaînes à deux états :**

$$P = \begin{pmatrix} 1-p & p \\ q & 1-q \end{pmatrix}, \quad \pi = (x, y), \quad x + y = 1$$

En résolvant :

$$\begin{cases} x = (1-p)x + qy \\ y = px + (1-q)y \end{cases} \Rightarrow x = \frac{q}{p+q}, \quad y = \frac{p}{p+q}$$

Donc $\pi = \left(\frac{q}{p+q}, \frac{p}{p+q}\right)$ est la distribution invariante.

## Fin de chapitre