
Corrigé proposé pour la base de sujets et corrigés de l'UPS.

Preliminaires

1. Soit $x = (x_0, \dots, x_{n-1}) \in \mathbb{C}^n$, considéré comme vecteur colonne.

$$\bar{x}^T x = \sum_{i=0}^{n-1} \bar{x}_i x_i = \sum_{i=0}^{n-1} |x_i|^2 = \|x\|_2^2.$$

2. Soit $U \in \mathcal{M}_n(\mathbb{C})$ une matrice unitaire et $x \in \mathbb{C}^n$.

$$\|Ux\|_2^2 = \overline{Ux}^T Ux = \bar{x}^T \overline{U}^T Ux = \bar{x}^T I_n x = \bar{x}^T x = \|x\|_2^2.$$

3. Soit $D \in \mathcal{M}_n(\mathbb{C})$ une matrice diagonale dont les coefficients diagonaux sont $d_0, \dots, d_{n-1}$, et $x = (x_0, \dots, x_{n-1})$ un élément quelconque de $\mathbb{S}$.

$$\|Dx\|_2^2 = \sum_{i=0}^{n-1} |d_i x_i|^2 \leq \delta^2 \sum_{i=0}^{n-1} |x_i|^2 \text{ avec } \delta = \max_{i=0..n-1} |d_i|.$$

$$\|Dx\|_2^2 \leq \delta^2 \|x\|_2^2 = \delta^2 \text{ car } x \in \mathbb{S}. \text{ On a donc : } \|D\| = \max_{x \in \mathbb{S}} \|Dx\|_2 \leq \delta.$$

Mais soit j un indice tel que $\delta = |d_j|$ et $x = (0, \dots, 1, \dots, 0)$ le vecteur de $\mathbb{C}^n$ dont toutes les composantes sont nulles sauf la j -ème égale à 1. On a de manière évidente : $\|Dx\|_2 = \delta$. Comme cet x appartient à $\mathbb{S}$, $\delta \leq \|D\|$.

Finalement, par double inégalité : $\|D\| = \max_{i \in \{0, \dots, n-1\}} |d_i|$.

4. Remarquons que si U est une matrice unitaire, U^{-1} aussi car $\overline{U^{-1}}^T = \overline{U}^T = U = (U^{-1})^{-1}$.

D'autre part comme U conserve la norme, $\{Ux : x \in \mathbb{S}\} \subset \mathbb{S}$.

Réciproquement, si $y \in \mathbb{S}$, $x = U^{-1}y$ est de norme 1 et $y = U(U^{-1}y) = Ux \in \{Ux : x \in \mathbb{S}\}$.

D'où l'égalité : $\{Ux : x \in \mathbb{S}\} = \mathbb{S}$.

De même $\{U^{-1}x : x \in \mathbb{S}\} = \mathbb{S}$.

Soit donc $A, B \in \mathcal{M}_n(\mathbb{C})$ vérifiant $B = UAU^{-1}$ avec U matrice unitaire.

$$\forall x \in \mathbb{S}, \|Bx\|_2^2 = \bar{x}^T \overline{B}^T Bx = \bar{x}^T \overline{U^{-1}}^T \overline{A}^T \overline{U}^T UAU^{-1}x = \bar{y}^T \overline{A}^T I_n Ay \text{ avec } y = U^{-1}x.$$

$$\forall x \in \mathbb{S}, \|Bx\|_2^2 = \bar{y}^T \overline{A}^T Ay = \|Ay\|_2^2.$$

Avec la remarque du début on a de plus : $\{\|Ay\|_2 : y \in \mathbb{S}\} = \{\|Bx\|_2 : x \in \mathbb{S}\}$.

Finalement $\|A\| = \sup_{y \in \mathbb{S}} \|Ay\|_2 = \sup_{x \in \mathbb{S}} \|Bx\|_2 = \|B\|$.

Première partie

Le but de cette partie est de démontrer le résultat suivant.

Théorème 1. Soit $f \in \mathbb{C}[X]$ un polynôme. Alors

$$\sup_{z \in \mathbb{D}} |f(z)| = \sup_{z \in \mathbb{S}} |f(z)|$$

On admet le résultat suivant : si $M \in \mathcal{M}_m(\mathbb{C})$ est une matrice unitaire, il existe une matrice diagonale $D \in \mathcal{M}_m(\mathbb{C})$, dont tous les coefficients diagonaux ont module 1, et une matrice unitaire $U \in \mathcal{M}_m(\mathbb{C})$ telles que $M = UDU^{-1}$.

Soit $f \in \mathbb{C}[X]$ de degré $n \geq 1$ et $z \in \mathbb{D}$. Soit $M \in \mathcal{M}_{n+1}(\mathbb{C})$ et $P \in \mathcal{M}_{n+1,1}(\mathbb{C})$:

$$M = \begin{pmatrix} z & 0 & 0 & \dots & 0 & \sqrt{1-|z|^2} \\ \sqrt{1-|z|^2} & 0 & 0 & \dots & 0 & -\bar{z} \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \ddots & 0 & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix} = \begin{pmatrix} z & 0 & 0 & \dots & 0 & \sqrt{1-|z|^2} \\ \sqrt{1-|z|^2} & 0 & 0 & \dots & 0 & -\bar{z} \\ 0 & & & & & 0 \\ 0 & & & & & 0 \\ \vdots & & I_{n-1} & & & \\ 0 & & & & & 0 \end{pmatrix}$$

et

$$P = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

5. Notons $C_0, \dots, C_n$ les colonnes de M . Le coefficient général de $\overline{M}^T M$ est $\overline{C_i}^T C_j$. On vérifie facilement que :

- $\forall (i, j) \in \{1, \dots, n-1\}^2, \overline{C_i}^T C_j = \delta_{i,j}$.
- $\forall j \in \{1, n\}, \overline{C_1}^T C_j = \delta_{1,j}$.
- $\forall i \in \{0, n-1\}, \overline{C_i}^T C_n = \delta_{i,n}$.
- $\overline{C_0}^T C_0 = \bar{z}z + \sqrt{1-|z|^2} = 1 = \overline{C_n}^T C_n$.
- $\overline{C_0}^T C_n = \bar{z}\sqrt{1-|z|^2} - \sqrt{1-|z|^2}\bar{z} = 0$.

Par suite $\overline{M}^T M = I_n$. M est une matrice unitaire.

6. Pour toute matrice A de $\mathcal{M}_{n+1}(\mathbb{C})$, $P^T A P$ est le coefficient d'indice 0,0 de la matrice A .

Soit φ endomorphisme de $\mathbb{C}^{n+1}$ de matrice M dans une base $(e_0, \dots, e_n)$.

$\varphi(e_0) = ze_0 + \sqrt{1-|z|^2}e_1$ et $\varphi(e_k) = e_{k+1}$ pour $k = 1..n-1$.

Montrons par récurrence finie sur k que pour tout entier $k \in [[1, n]]$, $\varphi^k(e_0) = z^k e_0 + \varepsilon_k$ avec $\varepsilon_k \in \text{Vect}(e_1, \dots, e_k)$.

Cette propriété est vraie pour $k = 1$.

Soit k entier $k \geq 1$ et $k < n$. Supposons que la propriété soit vraie au rang k .

On a alors $\varphi^{k+1}(e_0) = z^k \varphi(e_0) + \varphi(\varepsilon_k)$ avec $\varepsilon_k \in \text{Vect}(e_1, \dots, e_k)$.

$\varphi^{k+1}(e_0) = z^{k+1}e_0 + z\sqrt{1-|z|^2}e_1 + \varphi(\varepsilon_k)$. Comme $k < n$, $\varphi(\text{Vect}(e_1, \dots, e_k)) \subset \text{Vect}(e_2, \dots, e_{k+1})$.

Notons $\varepsilon_{k+1} = z\sqrt{1-|z|^2}e_1 + \varphi(\varepsilon_k) \in \text{Vect}(e_1, \dots, e_{k+1})$. $\varphi^{k+1}(e_0) = z^{k+1}e_0 + \varepsilon_{k+1}$.

La propriété est vraie au rang $k+1$.

Le coefficient d'indice 0,0 de M^k est donc z^k pour $k \in [[1, n]]$. C'est vrai également pour $k = 0$.

On a donc bien : $z^k = P^T M^k P$ pour tout entier $0 \leq k \leq n$.

7. Soit $a_0, \dots, a_n$ les éléments de $\mathbb{C}$ tels que $f(z) = \sum_{k=0}^n a_k z^k$.

D'après la question précédente on obtient $f(z) = P^T (\sum_{k=0}^n a_k M^k) P = P^T f(M) P$.

Notons $y_0, \dots, y_n$ les coordonnées dans la base canonique de $\mathbb{C}^n$ du vecteur $Y = f(M)P$.

On a : $f(z) = P^T Y = y_0$; $|f(z)| = |y_0| \leq \sqrt{\sum_{k=0}^n |y_k|^2} = \|f(M)P\|_2 \leq \|f(M)\|$ car P est un vecteur de $\mathbb{S}$.

8. Comme M est une matrice unitaire, il existe D matrice diagonale de $\mathcal{M}_{n+1}(\mathbb{C})$ d'éléments diagonaux $d_0, \dots, d_n$ tous de module 1 et U matrice unitaire de $\mathcal{M}_{n+1}(\mathbb{C})$ vérifiant $M = UDU^{-1}$.

On montre facilement que $\forall k \in \mathbb{N}$, $M^k = UD^k U^{-1}$ donc $f(M) = \sum_{k=0}^n UD^k U^{-1} = Uf(D)U^{-1}$.

Comme U est unitaire, d'après la 4. question, $f(M)$ et $f(D)$ ont même norme. La matrice $f(D)$ est diagonale, d'éléments diagonaux $f(d_0), \dots, f(d_n)$. En utilisant le résultat de la question 3., $\|f(M)\| = \|f(D)\| = \max_{i=0, \dots, n} |f(d_i)|$.

Notons i_0 un indice pour lequel ce maximum est atteint.

D'après la question précédente $\forall z \in \mathbb{D}, |f(z)| \leq |f(d_{i_0})|$ avec $d_{i_0} \in \mathbb{S}$.

D'où la démonstration du **Théorème 1**. (principe du maximum dans le cas particulier des fonctions polynômes)..

Deuxième partie

Le but de cette partie est de démontrer l'énoncé suivant :

Théorème 2. Soit $n \geq 1$ un entier et $A(z) = \sum_{k=0}^{n-1} a_k z^k$ un polynôme non nul tel que $a_k \in \{-1, 0, 1\}$ pour tout $0 \leq k \leq n-1$. Alors pour tout entier $L \geq 1$ on a

$$\sup_{\theta \in [-\frac{\pi}{L}, \frac{\pi}{L}]} |A(e^{i\theta})| \geq \frac{1}{n^{L-1}}.$$

Soit $n \geq 1$ et $A(z) = \sum_{k=0}^{n-1} a_k z^k$ avec $a_k \in \{-1, 0, 1\}$ pour tout $0 \leq k \leq n-1$. Soit $L \geq 1$ entier fixé.

9. Soit $z \in \mathbb{C}$ avec $|z| = 1$. $\forall k \in [[0, n]]$, $|a_k z^k| = |a_k| \cdot |z|^k = |a_k| \leq 1$

$$|A(z)| = \left| \sum_{k=0}^{n-1} a_k z^k \right| \leq \sum_{k=0}^{n-1} |a_k z^k| \leq \sum_{k=0}^{n-1} 1 = n.$$

10. On suppose dans cette question que $a_0 = 1$, et on pose, pour tout $z \in \mathbb{C}$,

$$F(z) = \prod_{j=0}^{L-1} A\left(ze^{\frac{2i\pi j}{L}}\right)$$

- a. On a $A(0) = a_0 = 1$. D'après le **Théorème 1**, comme $0 \in \mathbb{D}$, $1 \leq \sup_{z \in \mathbb{S}} |A(z)|$.

Ce résultat est identique pour tous les polynômes $z \mapsto A\left(ze^{\frac{2i\pi j}{L}}\right)$ qui prennent tous la valeur 1 en $z = 0$. $|F(0)| \leq \sup_{z \in \mathbb{S}} |F(z)|$. Comme $z \mapsto |F(z)|$ est continue sur le fermé borné $\mathbb{S}$ et est à valeurs dans $\mathbb{R}$, F atteint son maximum en un point z_0 de $\mathbb{S}$. $z_0 \in \mathbb{S}$ et $|F(z_0)| \geq 1$.

- b. Les points du plan d'affixe $e^{-\frac{2i\pi j}{L} - \frac{i\pi}{L}}$, $j = 0, \dots, L-1$ sont les sommets d'un polygone régulier à L côtés inscrit dans le cercle unité.

Comme $z_0 \in \mathbb{S}$, il existe $j_0 \in [[0, L-1]]$ et $\theta_0 \in \mathbb{R}$ vérifiant $z_0 = e^{i\theta_0}$ et $\frac{-2\pi(j_0)}{L} - \frac{\pi}{L} \leq \theta_0 \leq \frac{-2\pi(j_0-1)}{L} - \frac{\pi}{L}$. On obtient $\frac{-\pi}{L} \leq \theta_0 + \frac{2\pi j_0}{L} \leq \frac{\pi}{L}$

On a pour $j \neq j_0$, $\left|A\left(ze^{\frac{2i\pi j}{L}}\right)\right| \leq n$ d'après la question 9.

On obtient $|F(z_0)| \leq n^{L-1} \left|A\left(z_0 e^{\frac{2i\pi j_0}{L}}\right)\right| = n^{L-1} \left|A\left(e^{\frac{2i\pi j_0}{L} + i\theta_0}\right)\right|$

Par suite $1 \leq |F(z_0)| \leq n^{L-1} \cdot \sup_{\theta \in [-\frac{\pi}{L}, \frac{\pi}{L}]} |A(e^{i\theta})|$.

11. Soit k_0 le plus petit indice tel que $a_{k_0} \neq 0$. On a $a_{k_0} = \pm 1$ et $A(z) = a_{k_0} z^{k_0} A_1(z)$ où A_1 est un polynôme de degré $n - k_0$ de coefficients tous égaux à 1, 0, ou -1 et avec $A_1(0) = 1$. On peut lui appliquer le résultat de la question précédente. De plus pour z de module 1, $|A(z)| = |A_1(z)|$.

$$\sup_{\theta \in [-\frac{\pi}{L}, \frac{\pi}{L}]} |A(e^{i\theta})| = \sup_{\theta \in [-\frac{\pi}{L}, \frac{\pi}{L}]} |A_1(e^{i\theta})| \geq \frac{1}{n^{L-1}} \text{ d'après 10b.}$$

Troisième partie

Le but de cette partie est de démontrer le résultat suivant :

Théorème 3. On fixe $p, q \in [0, 1]$. Soit $n \geq 1$ un entier et soit S_n une somme de n variables aléatoires à valeurs dans $\{0, 1\}$ mutuellement indépendantes de Bernoulli de paramètre p . Alors

$$\mathbb{P} \left(\left| \frac{S_n}{n} - q \right| \leq \left| \frac{S_n}{n} - p \right| \right) \leq e^{-n \frac{(p-q)^2}{2}}.$$

Soit $p, q \in [0, 1]$ et $(X_i)_{1 \leq i \leq n}$ une famille de n variables aléatoires à valeurs dans $\{0, 1\}$ mutuellement indépendantes de Bernoulli de paramètre p . On pose $S_n = \sum_{i=1}^n X_i$.

12. Soit $g : \mathbb{R}_+ \rightarrow \mathbb{R}$ la fonction définie par $g(x) = \ln(1 - p + pe^x)$ pour tout $x \geq 0$.

- a.** Pour tout $x \geq 0$, $e^x \geq 1$, $p \geq 0$ donc $pe^x \geq p$ et $1 - p + pe^x \geq 1$, ce qui assure la définition et le caractère C^2 de g sur $\mathbb{R}_+$.

$$\forall x \geq 0, g'(x) = \frac{pe^x}{1 - p + pe^x}; \quad g''(x) = \frac{pe^x(1 - p + pe^x) - pe^x pe^x}{(1 - p + pe^x)^2} = \frac{(1 - p)pe^x}{(1 - p + pe^x)^2}$$

On obtient bien la forme demandée.

- b.** Si α, β sont deux réels strictement positifs $-4\alpha\beta + (\alpha + \beta)^2 = \alpha^2 - 2\alpha\beta + \beta^2 = (\alpha - \beta)^2 \geq 0$.

$$\text{D'où } \frac{(\alpha + \beta)^2}{\alpha\beta} \geq 4 \text{ et } \frac{\alpha\beta}{(\alpha + \beta)^2} \leq \frac{1}{4}.$$

Compte-tenu de la factorisation de $g''(x)$ on a bien $g''(x) \leq \frac{1}{4}$ pour tout $x \geq 0$.

- c.** Soit h la fonction définie sur $\mathbb{R}_+$ par $h(x) = px + \frac{x^2}{8} - g(x)$.

$$\forall x \geq 0, h'(x) = p + \frac{x}{4} - g'(x) \text{ et } h''(x) = \frac{1}{4} - g''(x) \geq 0.$$

h' est croissante sur $\mathbb{R}_+$ avec $h'(0) = p - g'(0) = p - p = 0$. h' est positive sur $\mathbb{R}_+$; h est croissante sur $\mathbb{R}_+$ avec $h(0) = \ln(1) = 0$.

Par suite : $\forall x \geq 0, \ln(1 - p + pe^x) \leq px + \frac{x^2}{8}$ pour tout $x \geq 0$.

13. On suppose dans cette question que $p < q$.

- a.** Si a, b sont deux réels positifs, $a \leq b \Rightarrow a^2 \leq b^2$. Donc :

$$A = \left\{ \omega \in \Omega : \left| \frac{S_n(\omega)}{n} - q \right| \leq \left| \frac{S_n(\omega)}{n} - p \right| \right\} = \left\{ \omega \in \Omega : \left(\frac{S_n(\omega)}{n} - q \right)^2 \leq \left(\frac{S_n(\omega)}{n} - p \right)^2 \right\}.$$

En termes d'événements on peut écrire :

$$A = \left[\left| \frac{S_n}{n} - q \right| \leq \left| \frac{S_n}{n} - p \right| \right] = \left[\left(\frac{S_n}{n} - q \right)^2 \leq \left(\frac{S_n}{n} - p \right)^2 \right] = [(S_n - nq)^2 - (S_n - np)^2 \leq 0]$$

$$A = [-2nS_n(q - p) + n^2q^2 - n^2p^2 \leq 0] = [2S_n(q - p) \geq n(q - p)(q + p)]$$

Comme $q - p > 0$, $A = \left[S_n \geq \frac{p+q}{2}n \right]$. On a donc

$$\mathbb{P}(A) = \mathbb{P} \left(\left| \frac{S_n}{n} - q \right| \leq \left| \frac{S_n}{n} - p \right| \right) = \mathbb{P} \left(S_n \geq \frac{p+q}{2}n \right).$$

- b.** Soit X une variable aléatoire de Bernoulli de paramètre p et $u > 0$. $X(\Omega) = \{0, 1\}$.

$$\mathbb{E}(e^{uX}) = e^{u \times 0} \mathbb{P}(X = 0) + e^{u \times 1} \mathbb{P}(X = 1) = 1 - p + pe^u = e^{g(u)}.$$

- c.** Soit $u > 0$, par croissance de la fonction exponentielle :

$$A = \left[e^{uS_n} \geq e^{u \frac{(p+q)}{2}n} \right]. \text{ En appliquant l'inégalité de Markov :}$$

$$\mathbb{P} \left(e^{uS_n} \geq e^{u \frac{(p+q)}{2}n} \right) \leq \frac{\mathbb{E}(e^{uS_n})}{e^{u \frac{(p+q)}{2}n}} = e^{-u \frac{(p+q)}{2}n} \mathbb{E} \left(\prod_{i=1}^n e^{uX_i} \right) = e^{-u \frac{(p+q)}{2}n} \prod_{i=1}^n \mathbb{E}(e^{uX_i})$$

par indépendance des v.a.r. $e^{uX_1}, \dots, e^{uX_n}$. Puis d'après **b.** :

$$\mathbb{P}(A) = e^{-u \frac{(p+q)}{2}n} (e^{g(u)})^n = e^{-n \left(\frac{p+q}{2}u - \ln(1 - p + pe^u) \right)}, \text{ c.a.d. :}$$

$$\mathbb{P} \left(S_n \geq \frac{p+q}{2}n \right) \leq e^{-n \left(\frac{p+q}{2}u - \ln(1 - p + pe^u) \right)}.$$

- c.** En utilisant la majoration de la fonction g vue en **12c.** on a :

$$\mathbb{P}(A) \leq e^{-u \frac{(p+q)}{2}n} e^{n(pu + u^2/8)} = e^{nh_1(u)} \text{ avec } h_1 : u \mapsto u^2/8 + pu - u(p+q)/2.$$

La fonction h_1 atteint son minimum en $u_0 = -4p + 2(p+q) = 2(q-p) > 0$

D'où $\mathbb{P}(A) \leq e^{nh_1(u_0)} = e^{n\left(\frac{(q-p)^2}{2} + 2p(q-p) - (q-p)(p+q)\right)} = e^{-n\frac{(p-q)^2}{2}}$.

On obtient : $\mathbb{P}\left(S_n \geq \frac{p+q}{2}n\right) \leq e^{-n\frac{(p-q)^2}{2}}$.

Le théorème est démontré dans le cas $q > p$.

14. Dans le cas $p > q$ notons pour chaque i , $Y_i = 1 - X_i$. Y_i suit une loi de Bernoulli de paramètre $1 - p$ et $1 - q > 1 - p$.

On a donc $\mathbb{P}\left(\left|\frac{\sum_{i=1}^n Y_i}{n} - (1 - q)\right| \leq \left|\frac{\sum_{i=1}^n Y_i}{n} - (1 - p)\right|\right) \leq e^{-n\frac{(p-q)^2}{2}}$

car $(p - q)^2 = (1 - p + 1 - q)^2$.

En remplaçant Y_i par $1 - X_i$ on obtient exactement :

$$\mathbb{P}\left(\left|\frac{S_n}{n} - q\right| \leq \left|\frac{S_n}{n} - p\right|\right) \leq e^{-n\frac{(p-q)^2}{2}}.$$

Le cas $p = q$ est trivial ($1=1$).

Le **Théorème 3** est bien démontré.

Quatrième partie

Dans cette partie on s'intéresse à la reconstruction d'une suite de 0 ou 1 à partir d'un échantillon d'observations bruitées.

Plus précisément, étant donné un élément $x = (x_0, \dots, x_{n-1}) \in \{0, 1\}^n$ appelé la source, et un paramètre $p \in]0, 1[$ fixé, on considère la variable aléatoire $O(x)$ à valeurs dans $\{0, 1\}^n$ construite comme suit :

- soient $(B_i)_{0 \leq i \leq n-1}$ des variables aléatoires à valeurs dans $\{0, 1\}$ mutuellement indépendantes de Bernoulli de paramètre p ;
- on note N la variable aléatoire définie par

$$N = \text{Card}(\{0 \leq i \leq n-1 : B_i = 1\})$$

et $I_0 < I_1 < \dots < I_{N-1}$ les éléments de l'ensemble aléatoire $\{0 \leq i \leq n-1 : B_i = 1\}$ rangés dans l'ordre croissant ;

- on pose enfin

$$O(x) = (O_0(x), O_1(x), \dots, O_{n-1}(x)) = (x_{I_0}, x_{I_1}, \dots, x_{I_{N-1}}, 0, \dots, 0) \in \{0, 1\}^n$$

avec la convention $O(x) = (0, \dots, 0) \in \{0, 1\}^n$ si $N = 0$.

La variable aléatoire $O(x)$ est appelée *observation bruitée de source x* . Ainsi, $O(x)$ est obtenue à partir de x en gardant chaque coordonnée avec probabilité p , indépendamment les unes des autres (complétée par des 0 pour obtenir un vecteur de longueur n).

15. Soit $\theta \in [-\pi, \pi]$.

- a. On étudie de la fonction $\theta \mapsto \cos(\theta) - 1 + \frac{\theta^2}{2}$ sur $[-\pi, \pi]$.

(dérivée seconde positive, dérivée première croissante et qui prend la valeur 0 en 0, fonction décroissante sur $[-\pi, 0]$, croissante sur $[0, \pi]$ de valeur 0 en 0).

On a donc $\forall \theta \in [-\pi, \pi]$, $\cos(\theta) \geq 1 - \frac{\theta^2}{2}$.

Remarque : on peut également utiliser directement une inégalité de Taylor.

$$\begin{aligned} \text{b. } \left| \frac{e^{i\theta} - (1-p)}{p} \right|^2 &= \frac{(\cos(\theta) - 1 + p)^2 + \sin^2(\theta)}{p^2} = \frac{1 - 2\cos(\theta)(1-p) + (1-p)^2}{p^2} \\ \left| \frac{e^{i\theta} - (1-p)}{p} \right|^2 &\leq \frac{1 + (1-p)^2 - 2(1-p) + \theta^2(1-p)}{p^2} = \frac{p^2 + \theta^2(1-p)}{p^2} = 1 + \frac{\theta^2(1-p)}{p^2}. \end{aligned}$$

Or $\forall x \geq 0$, $1 + x \leq e^x$. D'où : $\left| \frac{e^{i\theta} - (1-p)}{p} \right|^2 \leq \exp\left(\frac{\theta^2(1-p)}{p^2}\right)$.

On a bien $\left| \frac{e^{i\theta} - (1-p)}{p} \right| \leq \exp\left(\frac{1-p}{2p^2} \theta^2\right)$.

16. Soit $x = (x_0, \dots, x_{n-1}) \in \{0, 1\}^n$ et considérons une observation bruitée

$$O(x) = (O_0(x), O_1(x), \dots, O_{n-1}(x))$$

de source x .

- a. Soit $0 \leq j \leq k \leq n-1$. Notons B l'événement $[N \geq j \text{ et } I_j = k]$.
 B est l'intersection de l'événement $B_k = 1$, de probabilité p et de l'événement $B' =$ "avant k il y a eu j var parmi $B_0, \dots, B_{k-1}$ qui ont pris la valeur 1".
 $\mathbb{P}(B') = \binom{k}{j} p^j (1-p)^{k-j}$. Par indépendance :
 $\mathbb{P}(B) = \mathbb{P}(N \geq j \text{ et } I_j = k) = p \binom{k}{j} p^j (1-p)^{k-j}$.
- b. Les valeurs prises par la var $O_j(x)$ sont 0 ou bien, si $j \leq N$, une valeur x_k avec $j \leq k \leq n-1$ avec la probabilité calculée dans la question précédente.
On a, pour tout $0 \leq j \leq n-1$, $\mathbb{E}[O_j(x)] = p \sum_{k=j}^{n-1} x_k \binom{k}{j} p^j (1-p)^{k-j}$.
- c. Soit $\omega \in \mathbb{C}$,

$$\mathbb{E} \left[\sum_{j=0}^{n-1} O_j(x) \omega^j \right] = \sum_{j=0}^{n-1} \omega^j \mathbb{E}(O_j(x)) = \sum_{j=0}^{n-1} p \left(\sum_{k=j}^{n-1} x_k \binom{k}{j} p^j (1-p)^{k-j} \right)$$

Cette somme double se fait sur une partie triangulaire finie de $\mathbb{N} \times \mathbb{N}$. En sommant d'abord sur l'indice k on a :

$$\mathbb{E} \left[\sum_{j=0}^{n-1} O_j(x) \omega^j \right] = p \sum_{k=0}^{n-1} x_k \left(\sum_{j=0}^k \binom{k}{j} \omega^j p^j (1-p)^{k-j} \right) = p \sum_{k=0}^{n-1} x_k (p\omega + 1 - p)^k.$$

Dans la suite, on pose $L_n = \lfloor n^{1/3} \rfloor$, où $\lfloor t \rfloor$ désigne la partie entière d'un nombre réel t .

17. Soient $x, y \in \{0, 1\}^n$ tels que $x \neq y$. Posons pour $z \in \mathbb{C}$, $A_{x,y}(z) = \sum_{k=0}^{n-1} (x_k - y_k) z^k$.

- a. Comme $x \neq y$, le polynôme A est non nul et vérifie les hypothèses du **Théorème 2**. avec $L = L_n$.

On a donc : $\sup_{\theta \in [-\frac{\pi}{L_n}, \frac{\pi}{L_n}]} |A(e^{i\theta})| \geq \frac{1}{n^{L_n-1}}.$

La fonction $\theta \mapsto |A(e^{i\theta})|$ est continue sur le fermé borné $[-\pi/L_n, \pi/L_n]$ et à valeurs dans $\mathbb{R}$. Elle est donc bornée sur ce segment et les bornes sont atteintes.

$\exists \theta_0 \in [-\frac{\pi}{L_n}, \frac{\pi}{L_n}]$ tel que $\sup_{\theta \in [-\frac{\pi}{L_n}, \frac{\pi}{L_n}]} |A(e^{i\theta})| = |A_{x,y}(e^{i\theta_0})| \geq \frac{1}{n^{L_n-1}}.$

- b. Soit $\omega \in \mathbb{C}$.

$$\sum_{j=0}^{n-1} (\mathbb{E}[O_j(x) \omega^j] - \mathbb{E}[O_j(y) \omega^j]) = \mathbb{E} \left[\sum_{j=0}^{n-1} O_j(x) \omega^j - O_j(y) \omega^j \right] = p \sum_{k=0}^{n-1} (x_k - y_k) (p\omega + 1 - p)^k$$

Choisissons ω tel que $p\omega + 1 - p = e^{i\theta_0}$.

$$\sum_{j=0}^{n-1} (\mathbb{E}[O_j(x)] - \mathbb{E}[O_j(y)] \omega^j) = p A(e^{i\theta_0})$$

En minorant la somme des modules par le module de la somme on a :

$$\sum_{j=0}^{n-1} |\mathbb{E}[O_j(x)] - \mathbb{E}[O_j(y)]| \cdot \left| \frac{e^{i\theta_0} - (1-p)}{p} \right|^j \geq \left| \sum_{j=0}^{n-1} (\mathbb{E}[O_j(x)] - \mathbb{E}[O_j(y)]) \omega^j \right| \geq p |A(e^{i\theta_0})|$$

On obtient

$$\sum_{j=0}^{n-1} |\mathbb{E}[O_j(x)] - \mathbb{E}[O_j(y)]| \cdot \left| \frac{e^{i\theta_0} - (1-p)}{p} \right|^j \geq \frac{p}{n^{L_n-1}}$$

- c. Si pour chaque j de $[0, n-1]$ on avait $|\mathbb{E}[O_j(x)] - \mathbb{E}[O_j(y)]| \cdot \left| \frac{e^{i\theta_0} - (1-p)}{p} \right|^j < \frac{p}{n^{L_n}}$, l'inégalité précédente ne serait pas réalisée.

Il existe donc un entier $j_n(x, y)$ tel que $0 \leq j_n(x, y) \leq n-1$ et

$$|\mathbb{E}[O_{j_n}(x)] - \mathbb{E}[O_{j_n}(y)]| \cdot \left| \frac{e^{i\theta_0} - (1-p)}{p} \right|^{j_n} \geq \frac{p}{n^{L_n}}$$

Or, d'après la question **15b**. $\left| \frac{e^{i\theta_0} - (1-p)}{p} \right| \geq 1$ et $\left| \frac{e^{i\theta_0} - (1-p)}{p} \right| \leq \exp\left(\frac{1-p}{2p^2} \theta_0^2\right)$.

On a donc : $\left| \frac{e^{i\theta_0} - (1-p)}{p} \right|^{j_n} \leq \left| \frac{e^{i\theta_0} - (1-p)}{p} \right|^n \leq \exp\left(n \frac{1-p}{2p^2} \theta_0^2\right) \leq \exp\left(n \frac{1-p}{2p^2} \frac{\pi^2}{L_n^2}\right)$.

(car $|\theta_0| \leq \frac{\pi}{L_n}$.) En remplaçant on obtient bien :

$$|\mathbb{E}[O_{j_n(x,y)}(x)] - \mathbb{E}[O_{j_n(x,y)}(y)]| \geq \frac{p}{n^{L_n}} \exp\left(-\frac{1-p}{2p^2} \cdot \frac{\pi^2}{L_n^2} n\right).$$

Dans la suite, on fixe une fois pour toutes un entier n qu'il faut considérer comme étant très grand. Pour chaque couple $(x, y) \in \{0, 1\}^n$ tel que $x \neq y$, on fixe un entier $j_n(x, y)$ dont l'existence est prouvée dans la question **17c**.

Soient $T \geq 1$ et $(E^1, E^2, \dots, E^T) \in (\{0, 1\}^n)^T$. Ainsi pour $1 \leq i \leq T$ et $0 \leq j \leq n-1$, on a $E_i^j \in \{0, 1\}$. On dit que x est meilleur que y compte tenu de $E^1, E^2, \dots, E^T$ si

$$\left| \frac{1}{T} \sum_{i=1}^T E_{j_n(x,y)}^i - \mathbb{E}[O_{j_n(x,y)}(x)] \right| < \left| \frac{1}{T} \sum_{i=1}^T E_{j_n(x,y)}^i - \mathbb{E}[O_{j_n(x,y)}(y)] \right|$$

On pose alors $R_{n,T}(E^1, E^2, \dots, E^T) = x$ si pour tout $y \neq x$, x est meilleur que y . Si l'on ne peut trouver de tel x on pose $R_{n,T}(E^1, E^2, \dots, E^T) = (0, 0, \dots, 0)$.

- 18.** L'événement $R_{n,T}(O^1(x), O^2(x), \dots, O^T(x)) \neq x$ est la réunion des événements x n'est pas meilleur que y compte-tenu de $O^1(x), O^2(x), \dots, O^T(x)$. On a donc :

$$\begin{aligned} & \mathbb{P}(R_{n,T}(O^1(x), O^2(x), \dots, O^T(x)) \neq x) \\ & \leq \sum_{y \in \{0,1\}^n, y \neq x} \mathbb{P}(x \text{ n'est pas meilleur que } y \text{ compte-tenu de } O^1(x), O^2(x), \dots, O^T(x)) \end{aligned}$$

On doit donc calculer $\mathbb{P}\left(\left|\frac{1}{T} \sum_{i=1}^T O_{j_n(x,y)}^i(x) - \mathbb{E}[O_{j_n(x,y)}(x)]\right| \geq \left|\frac{1}{T} \sum_{i=1}^T O_{j_n(x,y)}^i(x) - \mathbb{E}[O_{j_n(x,y)}(y)]\right|\right)$

En notant $S_T = \sum_{i=1}^T O_{j_n(x,y)}^i(x)$ somme de T variables de Bernoulli de même espérance

$p_1 = \mathbb{E}(O_{j_n(x,y)}(x))$ et en notant $q_1 = \mathbb{E}(O_{j_n(x,y)}(y))$ élément de $[0, 1]$ on peut majorer en utilisant le **Théorème 3** :

$$\mathbb{P}\left(\left|\frac{S_T}{T} - q_1\right| \leq \left|\frac{S_T}{T} - p_1\right|\right) \leq e^{-T \frac{(p_1 - q_1)^2}{2}}.$$

On retrouve $2^n - 1$ expressions de ce type dans la somme qui majore la probabilité étudiée.

Notons $\alpha_{R_{n,T}} = \mathbb{P}(R_{n,T}(O^1(x), O^2(x), \dots, O^T(x)) \neq x)$. On utilise alors l'inégalité vue en **17c**.

$$\alpha_{R_{n,T}} \leq 2^n e^{-T \frac{(p_1 - q_1)^2}{2}} \leq 2^n \exp\left(-\frac{T}{2} \frac{p^2}{n^{2L_n}} \exp\left(-2 \frac{1-p}{2p^2} \cdot \frac{\pi^2}{L_n^2} n\right)\right).$$

Prenons si $T_n \geq e^{3 \ln(n) n^{1/3}}$. $L_n \sim n^{1/3}$. $n/L_n^2 \sim n^{1/3}$. Le terme exponentiel à l'intérieur de la première exponentielle tend donc vers 0.

$$\alpha_{R_{n,T_n}} \leq e^{n \ln 2} \exp\left(-\frac{e^{3 \ln(n) n^{1/3}}}{2} \frac{p^2}{n^{2L_n}} \exp\left(-\frac{1-p}{p^2} \cdot \frac{\pi^2}{L_n^2} n\right)\right).$$

et $n^{2L_n} = e^{2L_n \ln n} = e^{2n^{1/3} \ln n + o(n^{1/3} \ln n)}$

D'où : $\alpha_{R_n, T_n} \leq \exp \left(-ce^{(\ln(n)n^{1/3} + o(\ln(n)n^{1/3}))} + n \ln 2 \right) = u_n$.

Comme $\lim_{n \rightarrow +\infty} \frac{n}{e^{\ln(n)n^{1/3} + o(\ln(n)n^{1/3})}} = 0$, $\lim_{n \rightarrow +\infty} u_n = 0$.

Le majorant ne dépend pas de x .

On obtient bien :

$$\max_{x \in \{0,1\}^n} \mathbb{P} \left(R_{n, T_n} (O^1(x), O^2(x), \dots, O^{T_n}(x)) \neq x \right) \leq u_n$$

où $(u_n)_{n \geq 1}$ est une suite tendant vers 0 lorsque n tend vers l'infini.

* *

*

N.B. : corrigé TEX rédigé pour la bourse de sujets et corrigés de l'UPS. Hugues Demongeot