Les quatre parties sont indépendantes entre elles.

Dans l'ensemble du sujet, pour répondre à une question, on pourra admettre les résultats des questions précédentes.

Notations

Dans l'ensemble du sujet m et n désignent des entiers strictement positifs. L'ensemble $\mathbb{C}$ désigne le corps des nombres complexes. Le module d'un nombre complexe z est noté $|z|$ et son conjugué est noté $\overline{z}$. On note $\overline{\mathbb{D}} = \{z \in \mathbb{C} : |z| \leqslant 1\}$ le disque unité fermé, et $\mathbb{S} = \{z \in \mathbb{C} : |z| = 1\}$.
On note $\mathcal{M}_{m,n}(\mathbb{C})$ l'ensemble des matrices à m lignes et à n colonnes à coefficients dans $\mathbb{C}$ et $\mathcal{M}_n(\mathbb{C}) = \mathcal{M}_{n,n}(\mathbb{C})$ l'ensemble des matrices à n lignes et à n colonnes à coefficients dans $\mathbb{C}$. On note I_n la matrice identité de $\mathcal{M}_n(\mathbb{C})$. La matrice transposée d'une matrice $A \in \mathcal{M}_{m,n}(\mathbb{C})$ est notée $A^{\intercal}$. Si $A = (a_{i,j})_{\substack{0\leqslant i\leqslant m-1\\ 0\leqslant j\leqslant n-1}} \in \mathcal{M}_{m,n}(\mathbb{C})$, on note $\overline{A}^{\intercal} \in \mathcal{M}_{n,m}(\mathbb{C})$ la matrice $(\overline{a_{j,i}})_{\substack{0\leqslant i\leqslant n-1\\ 0\leqslant j\leqslant m-1}}$.
On dit qu'une matrice $U \in \mathcal{M}_n(\mathbb{C})$ est *unitaire* si

$$U\overline{U}^{\intercal} = \overline{U}^{\intercal}U = \mathrm{I}_n\,.$$

Les coefficients d'un vecteur $x \in \mathbb{C}^n$ sont notés $x_0, \ldots, x_{n-1}$. Un vecteur $x \in \mathbb{C}^n$ sera vu comme un élément de $\mathcal{M}_{n,1}(\mathbb{C})$. Pour tous $x \in \mathbb{C}^n$ et $y \in \mathbb{C}^n$, la matrice $x^{\intercal}y \in \mathcal{M}_1(\mathbb{C})$ est identifiée au nombre complexe $\sum_{i=0}^{n-1} x_i y_i$. Nous munissons $\mathbb{C}^n$ de la norme $\|\ \|_2$ définie par

$$\forall x \in \mathbb{C}^n, \qquad \|x\|_2 = \left(\sum_{i=0}^{n-1} |x_i|^2\right)^{1/2}.$$

Si $A \in \mathcal{M}_{m,n}(\mathbb{C})$, on note

$$\|A\| = \sup_{\substack{x\in\mathbb{C}^n\\ \|x\|_2=1}} \|Ax\|_2\,.$$

Par convention, pour $A \in \mathcal{M}_n(\mathbb{C})$, on pose $A^0 = \mathrm{I}_n$.
Dans tout le sujet, $(\Omega, \mathcal{A}, \mathbb{P})$ désigne un espace probabilisé sur lequel seront définies les différentes variables aléatoires du sujet. On admettra que toutes les variables aléatoires introduites peuvent bien être construites sur cet espace. On notera $\mathbb{P}(A)$ la probabilité d'un événement $A \subset \Omega$ et $\mathbb{E}[\mathbf{X}]$ l'espérance d'une variable aléatoire $\mathbf{X}$ sur $(\Omega, \mathcal{A}, \mathbb{P})$ à valeurs réelles.

* * *

Préliminaires

Les résultats démontrés ici seront utiles dans la première partie.

1. Lorsque $x \in \mathbb{C}^n$, vérifier que $\|x\|_2^2 = \overline{x}^{\intercal}x$.

2. Soit $U \in \mathcal{M}_n(\mathbb{C})$ une matrice unitaire. Montrer que $\|Ux\|_2 = \|x\|_2$ pour tout $x \in \mathbb{C}^n$.

3. Si $D \in \mathcal{M}_n(\mathbb{C})$ est une matrice diagonale dont les coefficients diagonaux sont $d_0, \ldots, d_{n-1}$, montrer que $\|D\| = \max_{0\leqslant i\leqslant n-1} |d_i|$.

4. Soient $A, B \in \mathcal{M}_n(\mathbb{C})$. On suppose qu'il existe une matrice unitaire $U \in \mathcal{M}_n(\mathbb{C})$ telle que $B = UAU^{-1}$. Montrer que $\|A\| = \|B\|$.

Première partie

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

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

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

Pour cela, on admet le résultat suivant, qui pourra être utilisé sans démonstration.

A) 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 $M = UDU^{-1}$.

Pour démontrer le **Théorème 1**, on fixe un polynôme $f \in \mathbb{C}[X]$ de degré $n \geqslant 1$. On considère un nombre complexe $z \in \overline{\mathbb{D}}$ et on définit les matrices $M \in \mathcal{M}_{n+1}(\mathbb{C})$ et $P \in \mathcal{M}_{n+1,1}(\mathbb{C})$ par

$$M = \begin{pmatrix} z & 0 & 0 & \cdots & 0 & \sqrt{1-|z|^2} \\ \sqrt{1-|z|^2} & 0 & 0 & \cdots & 0 & -\overline{z} \\ 0 & & & & & 0 \\ 0 & & & \mathrm{I}_{n-1} & & 0 \\ \vdots & & & & & \vdots \\ 0 & & & & & 0 \end{pmatrix}$$

et

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

5. Montrer que M est une matrice unitaire.

6. Montrer que $z^k = P^{\intercal} M^k P$ pour tout entier $0 \leqslant k \leqslant n$.

7. Montrer que $|f(z)| \leqslant \|f(M)\|$.

8. Démontrer le **Théorème 1**.

Deuxième partie

Le but de cette partie est de démontrer l'énoncé suivant (on pourra utiliser le **Théorème 1**).

Théorème 2. Soit $n \geqslant 1$ 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 $0 \leqslant k \leqslant n-1$. Alors pour tout entier $L \geqslant 1$ on a

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

Pour démontrer ce résultat, on fixe un entier $n \geqslant 1$ et $A(z) = \sum_{k=0}^{n-1} a_k z^k$ un polynôme tel que $a_k \in \{-1, 0, 1\}$ pour tout $0 \leqslant k \leqslant n-1$. On fixe également un entier $L \geqslant 1$.

9. Si $z \in \mathbb{C}$ vérifie $|z| = 1$, montrer que $|A(z)| \leqslant n$.

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. Montrer qu'il existe $z_0 \in \mathbb{C}$ tel que $|z_0| = 1$ et $|F(z_0)| \geqslant 1$.

b. Montrer que $|F(z_0)| \leqslant n^{L-1} \cdot \sup_{\theta \in [-\frac{\pi}{L}, \frac{\pi}{L}]} |A(e^{i\theta})|$.

11. Démontrer le **Théorème 2**.

Troisième partie

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

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

$$\mathbb{P}\left(\left|\frac{\mathbf{S}_n}{n} - q\right| \leqslant \left|\frac{\mathbf{S}_n}{n} - p\right|\right) \leqslant e^{-n\frac{(p-q)^2}{2}}.$$

Pour démontrer ce résultat, on fixe $p, q \in [0,1]$ et $(\mathbf{X}_i)_{1 \leqslant i \leqslant n}$ une famille de n variables aléatoires à valeurs dans $\{0,1\}$ mutuellement indépendantes de Bernoulli de paramètre p. On pose alors $\mathbf{S}_n = \sum_{i=1}^n \mathbf{X}_i$.

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

a. Montrer que g est bien définie et de classe $\mathcal{C}^2$ sur $\mathbb{R}_+$. Pour $x \geqslant 0$, exprimer $g''(x)$ sous la forme $\frac{\alpha\beta}{(\alpha+\beta)^2}$, où α et β sont des réels positifs pouvant dépendre de x.

b. Montrer que $g''(x) \leqslant \frac{1}{4}$ pour tout $x \geqslant 0$.

c. Montrer que

$$\ln(1 - p + pe^x) \leqslant px + \frac{x^2}{8} \text{ pour tout } x \geqslant 0.$$

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

a. Justifier que

$$\mathbb{P}\left(\left|\frac{\mathbf{S}_n}{n} - q\right| \leqslant \left|\frac{\mathbf{S}_n}{n} - p\right|\right) = \mathbb{P}\left(\mathbf{S}_n \geqslant \tfrac{p+q}{2}n\right).$$

b. Soit $\mathbf{X}$ une variable aléatoire de Bernoulli de paramètre p. Pour $u > 0$, calculer $\mathbb{E}(e^{u\mathbf{X}})$.

c. Montrer que pour tout $u > 0$,

$$\mathbb{P}\left(\mathbf{S}_n \geqslant \tfrac{p+q}{2}n\right) \leqslant e^{-n\left(\frac{p+q}{2}u - \ln(1-p+pe^u)\right)}.$$

Indication. On pourra admettre que si $(\mathbf{Z}_i)_{1 \leqslant i \leqslant n}$ sont n variables aléatoires réelles mutuellement indépendantes et prenant un nombre fini de valeurs, alors $\mathbb{E}(\prod_{i=1}^n \mathbf{Z}_i) = \prod_{i=1}^n \mathbb{E}(\mathbf{Z}_i)$.

d. Montrer que $\mathbb{P}(\mathbf{S}_n \geqslant \frac{p+q}{2}n) \leqslant e^{-n\frac{(p-q)^2}{2}}$.

14. Démontrer le **Théorème 3**.

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 (on pourra utiliser le **Théorème 2** et le **Théorème 3**).
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 $\mathbf{O}(x)$ à valeurs dans $\{0,1\}^n$ construite comme suit :

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

$$\mathbf{N} = \mathrm{Card}(\{0 \leqslant i \leqslant n-1 : \mathbf{B}_i = 1\})$$

  et $I_0 < I_1 < \cdots < I_{\mathbf{N}-1}$ les éléments de l'ensemble aléatoire $\{0 \leqslant i \leqslant n-1 : \mathbf{B}_i = 1\}$ rangés dans l'ordre croissant ;
- on pose enfin

$$\mathbf{O}(x) = (\mathbf{O}_0(x), \mathbf{O}_1(x), \dots, \mathbf{O}_{n-1}(x)) = (x_{I_0}, x_{I_1}, \dots, x_{I_{N-1}}, 0, 0, \dots, 0) \in \{0,1\}^n$$

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

La variable aléatoire $\mathbf{O}(x)$ est appelée *observation bruitée de source x*. Ainsi, $\mathbf{O}(x)$ 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). Par exemple, si $x = (x_0, x_1, x_2, x_3, x_4) = (1,0,1,1,1)$ et si $\mathbf{B}_0 = 0$, $\mathbf{B}_1 = 1$, $\mathbf{B}_2 = 0$, $\mathbf{B}_3 = 1$, $\mathbf{B}_4 = 1$ (ce qui arrive avec probabilité $p^3(1-p)^2$), alors $\mathbf{O}(x) = (\mathbf{O}_0(x), \mathbf{O}_1(x), \dots, \mathbf{O}_4(x)) = (x_1, x_3, x_4, 0, 0) = (0,1,1,0,0)$.

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

a. Montrer que $\cos(\theta) \geqslant 1 - \frac{\theta^2}{2}$.

b. Montrer que $\left|\frac{e^{i\theta} - (1-p)}{p}\right| \leqslant \exp\left(\frac{1-p}{2p^2} \cdot \theta^2\right)$.

Indication. On pourra calculer $\left|\frac{e^{i\theta} - (1-p)}{p}\right|^2$.

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

$$\mathbf{O}(x) = (\mathbf{O}_0(x), \mathbf{O}_1(x), \dots, \mathbf{O}_{n-1}(x))$$

de source x.

a. Si $0 \leqslant j \leqslant k \leqslant n-1$, montrer que $\mathbb{P}(\mathbf{N} \geqslant j+1 \text{ et } I_j = k) = p\binom{k}{j} p^j (1-p)^{k-j}$.

b. Montrer que, pour tout $0 \leqslant j \leqslant n-1$, $\mathbb{E}[\mathbf{O}_j(x)] = p \sum_{k=j}^{n-1} x_k \binom{k}{j} p^j (1-p)^{k-j}$.

c. Montrer que pour tout $w \in \mathbb{C}$,

$$\mathbb{E}\left[\sum_{j=0}^{n-1} \mathbf{O}_j(x) w^j\right] = p \sum_{k=0}^{n-1} x_k (pw + 1 - p)^k.$$

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. Justifier l'existence de $\theta_0 \in [-\frac{\pi}{L_n}, \frac{\pi}{L_n}]$ tel que $|A_{x,y}(e^{i\theta_0})| \geqslant \frac{1}{n^{L_n - 1}}$.

b. Démontrer que

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

c. Justifier l'existence d'un entier $j_n(x,y)$ tel que $0 \leqslant j_n(x,y) \leqslant n-1$ et

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

Dans la suite, on fixe une fois pour toutes un entier n qu'il faut considérer comme étant très grand. Pour chaque couple $(x,y) \in (\{0,1\}^n)^2$ tel que $x \neq y$, on fixe un entier $j_n(x,y)$ dont l'existence est prouvée dans la question **17c**.

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

$$\left|\frac{1}{T}\sum_{i=1}^{T} E^i_{j_n(x,y)} - \mathbb{E}[\mathbf{O}_{j_n(x,y)}(x)]\right| < \left|\frac{1}{T}\sum_{i=1}^{T} E^i_{j_n(x,y)} - \mathbb{E}[\mathbf{O}_{j_n(x,y)}(y)]\right|.$$

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

18. Démontrer que si $T_n \geqslant e^{3\ln(n) n^{1/3}}$ alors pour tout $x \in \{0,1\}^n$ et toute suite

$$\mathbf{O}^1(x), \mathbf{O}^2(x), \ldots, \mathbf{O}^{T_n}(x)$$

de T_n variables aléatoires à valeurs dans $\{0,1\}^n$ mutuellement indépendantes de même loi que $\mathbf{O}(x)$, on a

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

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

Indication. On pourra commencer par écrire, en le justifiant, que

$$\begin{aligned}
&\mathbb{P}\left(R_{n,T}(\mathbf{O}^1(x), \mathbf{O}^2(x), \ldots, \mathbf{O}^T(x)) \neq x\right) \\
&\quad \leqslant \sum_{\substack{y \in \{0,1\}^n \\ y \neq x}} \mathbb{P}\left(x \text{ n'est pas meilleur que } y \text{ compte tenu de } \mathbf{O}^1(x), \mathbf{O}^2(x), \ldots, \mathbf{O}^T(x)\right).
\end{aligned}$$

On a donc démontré qu'en partant de $x \in \{0,1\}^n$ inconnu, on peut retrouver x à partir de la donnée d'une suite

$$\mathbf{O}^1(x), \mathbf{O}^2(x), \ldots, \mathbf{O}^T(x)$$

de T variables aléatoires à valeurs dans $\{0,1\}^n$ mutuellement indépendantes de même loi que $\mathbf{O}(x)$ (qui représentent la donnée de T échantillons bruités obtenus à partir d'une même source), avec grande probabilité à partir de $e^{3\ln(n) n^{1/3}}$ échantillons différents.

* * *