Examen du 20 mai 2015

Durée 3h, les notes de cours sont autorisées

Les trois exercices et le problème sont indépendants. Dans tous le sujet, les variables aléatoires considérées sont définies sur un espace de probabilités $(\Omega, \mathcal{F}, \mathbb{P})$.
Il est attendu que l'étudiant(e) CHOISISSE **de traiter l'exercice 1** OU **l'exercice 2**, et traite ensuite **l'exercice 3** ET **le problème.**

Exercice 1.— Cubes en grande dimension (au choix)

Pour tout $d \geq 1$, notons $C_d = [0,1]^d$, et $B_d(r)$ la boule de centre 0 et de rayon r dans $\mathbb{R}^d$ euclidien. Pour tout $a > 0$, on note $V(d,a)$ la mesure de Lebesgue de $C_d \cap B_d(a\sqrt{d})$. En interprétant $V(d,a)$ comme la probabilité d'un événement faisant intervenir des variables aléatoires indépendantes bien choisies, montrer les deux résultats suivants.

1. Montrer que $V(d,a)$ converge lorsque $d \to \infty$ vers 0 si $a < \sqrt{3}/3$, et vers 1 si $a > \sqrt{3}/3$.

2. Montrer que $\lim_{d\to\infty} V(d, \sqrt{3}/3) = 1/2$.

Exercice 2.— Asymptotique d'une marche aléatoire à pas gaussiens (au choix)

Soit $X_1, X_2, \ldots$ une suite de variables aléatoires à valeurs réelles indépendantes et de même loi gaussienne centrée réduite $\mathcal{N}(0,1)$. On note $S_n = \sum_{i=1}^n X_i$ pour tout $n \geq 0$.

1. Justifier que l'on a, pour tout $x > 0$,

$$\mathbb{P}(X_1 > x) \leq \frac{1}{x\sqrt{2\pi}} \exp\left(-\frac{x^2}{2}\right) .$$

2. Montrer que S_n a la même loi que $\sqrt{n}X_1$.

3. En déduire que pour tout $\varepsilon > 0$, l'on a que

$$\sum_{n\geq 1} \mathbb{P}\left(S_n > \sqrt{2(1+\varepsilon)n\ln(n)}\right) < \infty\,.$$

4. En conclure que presque surement, on a

$$\limsup_{n\to\infty} \frac{S_n}{\sqrt{2n\ln(n)}} \leq 1\,.$$

Exercice 3.— Produits de variables aléatoires

Soit $X_1, X_2, \ldots$ une suite de variables aléatoires à valeurs positives, indépendantes et de même loi, et telles que $\mathbb{E}[X_1] < \infty$. On s'intéresse au comportement asymptotique du produit $P_n = \prod_{i=1}^n X_i$ lorsque $n \to \infty$.

1. On suppose que $\mathbb{P}(X_1 = 0) > 0$. Que dire de la suite $(P_n, n \geq 0)$?

Dans toute la suite de l'exercice, on suppose que $\mathbb{P}(X_1 = 0) = 0$.

2. Montrer que si $\mathbb{E}[X_1] < 1$, alors P_n converge vers 0 dans L^1, et que si $\mathbb{E}[X_1] > 1$, alors P_n ne converge pas dans L^1.

3. Montrer que $\mathbb{E}[\ln(X_1)]$ est bien défini, et à valeurs dans $[-\infty, +\infty[$. Montrer que P_n converge p.s. vers 0 is $\mathbb{E}[\ln(X_1)] < 0$, et p.s. vers $+\infty$ si $\mathbb{E}[\ln(X_1)] > 0$.

4. On suppose que $\mathbb{E}[X_1] = 1$ et que X_1 n'est pas p.s. égale à 1. Montrer que P_n converge p.s. vers une limite qu'on déterminera. Montrer que la convergence n'a pas lieu dans L^1.

5. On suppose que $\mathbb{E}[\ln(X_1)] = 0$ et que X_1 n'est pas p.s. égale à 1. Montrer que la suite $(\sum_{i=1}^n \ln(X_i), n \geq 0)$ n'est p.s. pas bornée. En déduire que P_n ne converge pas p.s. vers une valeur finie strictement positive.

Problème — Extracteurs d'aléa

Pour réaliser des simulations utilisant de l'aléa, un ordinateur doit être capable de produire une suite de m bits aléatoires uniforme, c'est-à-dire une variable aléatoire de loi ν_m uniforme dans $\{0,1\}^m$, où $m \geq 1$ est un nombre entier.
Pour ce faire, l'ordinateur peut disposer d'une source faible d'aléa, c'est-à-dire d'une suite de bits aléatoires à valeurs dans $\{0,1\}^n$, mais de loi μ non nécessairement uniforme, où $n \geq 1$ est un autre nombre entier. Dans cet énoncé, les entiers n et m sont fixés une fois pour toutes, sauf dans la dernière question.

On se demande s'il existe un *extracteur d'aléa* pour la loi μ, c'est-à-dire une fonction $f : \{0,1\}^n \to \{0,1\}^m$ telle que la mesure image $f_*\mu$ de μ par f est le plus proche possible de ν_m, au sens de la norme $\|\cdot\|$ de variation totale. Ici, on prendra la convention que si μ, ν sont deux mesures de probabilités sur un espace mesuré $(X, \mathcal{X})$,

$$\|\mu - \nu\| = \sup_{A \in \mathcal{X}} |\mu(A) - \nu(A)| .$$

Si $\varepsilon \geq 0$, on dit ainsi que f est un ε-extracteur pour μ si

$$\|f_*\mu - \nu_m\| \leq \varepsilon .$$

On va s'intéresser à des conditions nécessaires et suffisantes pour l'existence d'extracteurs. On définit

$$H(\mu) = \inf_{x \in \{0,1\}^n} \log_2 \left(\frac{1}{\mu(\{x\})} \right)$$

1. On suppose que $H(\mu) = n$. Que dire de μ ? Et si $H(\mu) = 0$?

2. Montrer que si $H(\mu) < m$, alors il ne peut pas exister de 0-extracteur pour μ.

On cherche à établir une forme de réciproque à ce dernier énoncé. On fixe donc $\varepsilon \in]0,1[$ et on suppose que μ vérifie
$$H(\mu) \geq m + 2\log_2(1/\varepsilon)\,.$$
On cherche à montrer qu'il existe un ε-extracteur pour μ.

3. Soit F une variable aléatoire uniforme dans l'ensemble $\mathcal{M}$ des applications de $\{0,1\}^n$ dans $\{0,1\}^m$. Montrer que la famille $(F(x), x \in \{0,1\}^n)$ est une famille de variables aléatoires indépendantes et de loi ν_m.

Dans les deux questions suivantes, on fixe un $A \subset \{0,1\}^m$.

4. Justifier que si $f \in \mathcal{M}$, on a $f_*\mu(A) = \sum_{x\in\{0,1\}^n} \mu(x)\mathbf{1}_{\{f(x)\in A\}}$. En déduire que si F est comme dans la question précédente,
$$\mathbb{E}[F_*\mu(A)] = \nu_m(A)\,.$$

5. En utilisant l'inégalité de Hœffding, montrer que
$$\mathbb{P}\left(|F_*\mu(A) - \nu_m(A)| > \varepsilon\right) \leq 2\exp\left(-\frac{2\varepsilon^2}{\sum_{x\in\{0,1\}^n} \mu(\{x\})^2}\right)$$

6. En conclure que
$$\mathbb{P}(\|F_*\mu - \nu_m\| > \varepsilon) \leq 2^{2^m+1}\exp\left(-\varepsilon^2 2^{H(\mu)+1}\right)$$

7. Montrer que ce majorant est strictement plus petit que 1, et en conclure qu'il existe un ε-extracteur pour μ.

8. Dans cette question, on suppose que $m = 1$, c'est-à-dire que l'on veut produire une seule variable aléatoire de loi le plus proche possible de la loi de Bernoulli de paramètre $1/2$, mais cette fois, on voudrait trouver une fonction $f : \{0,1\}^n \to \{0,1\}$ qui soit un $1/10$-extracteur pour toute loi μ sur $\{0,1\}^n$ telle que $H(\mu) \geq n-1$ (par ce que l'on a vu précédemment, on doit demander au moins $H(\mu) \geq 1$).
Est-ce possible ?