Exercice II

On introduit la fonction génératrice d'une variable aléatoire à valeurs dans $\mathbb{N}$ et applique cet outil à un problème de truquage de dés. On note $(\Omega, \mathcal{F}, \mathbf{P})$ un espace probabilisé. On rappelle qu'une variable aléatoire *discrète* définie sur Ω et à valeurs dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ est une application $\mathcal{F}$-Bor($\mathbb{K}$) mesurable et telle que $X(\Omega)$ soit une partie au plus dénombrable de $\mathbb{K}$.

1) Soit X une application $\Omega \to \mathbb{N}$ telle que

$$\forall n \in \mathbb{N}, \quad X^{-1}(\{n\}) \in \mathcal{F}. \tag{9}$$

Soit $B \in \mathcal{P}(\mathbb{N})$. Alors B est fini ou dénombrable et (9) combiné aux relations

$$B = \mathop{\cup}_{n\in B} \{n\}, \quad X^{-1}(B) = \mathop{\cup}_{n\in B} X^{-1}(\{n\}) \tag{10}$$

montre l'appartenance à $\mathcal{F}$ de $X^{-1}(B)$. Comme ceci est valable pour tout $B \in \mathcal{P}(\mathbb{N})$, la $\mathcal{F}$-$\mathcal{P}(\mathbb{N})$ mesurabilité de X est établie.

Considérons X comme une application de Ω dans $\mathbb{R}$ en *agrandissant* l'ensemble d'arrivée. Cette opération n'a bien sûr pas changé l'ensemble $X(\Omega)$ des valeurs possibles de X qui reste une partie de $\mathbb{N}$. Pour tout borélien A de $\mathbb{R}$, on a donc $X^{-1}(A) = X^{-1}(A \cap \mathbb{N})$, de sorte qu'en posant $B = A \cap \mathbb{N}$ on est ramené à (10) et $X^{-1}(A) \in \mathcal{F}$. L'application $X : \Omega \to \mathbb{R}$ est donc $\mathcal{F}$-Bor($\mathbb{R}$) mesurable, c'est bien une variable aléatoire réelle. Elle est discrète puisque $X(\Omega) \subset \mathbb{N}$ est au plus dénombrable.

Soit $(\Omega', \mathcal{G})$ un espace mesurable et f une application *quelconque* $\mathbb{N} \to \Omega'$, vérifions que l'application $f \circ X$ est $\mathcal{F}$-$\mathcal{G}$ mesurable. Soit C élément quelconque de la tribu $\mathcal{G}$. Alors $(f \circ X)^{-1}(C) = X^{-1}\bigl(f^{-1}(C)\bigr)$. Comme $f^{-1}(C)$ est une partie de $\mathbb{N}$, il suffit d'appliquer (10) avec $B = f^{-1}(C)$ pour voir que $(f \circ X)^{-1}(C)$ est bien un élément de $\mathcal{F}$ et conclure à la $\mathcal{F}$-$\mathcal{G}$ mesurabilité de $f \circ X$. On notera que ce résultat est obtenu pour n'importe quelle tribu $\mathcal{G}$ sur Ω' et n'importe quelle application $f : \mathbb{N} \to \Omega'$.

2) Soit z un nombre complexe fixé et $X : \Omega \to \mathbb{N}$ une variable aléatoire entière. On voit immédiatement que l'application

$$z^X : \Omega \to \mathbb{C}, \quad \omega \mapsto z^{X(\omega)}$$

est une variable aléatoire discrète à valeurs complexes en appliquant le résultat précédent avec $\Omega' = \mathbb{C}$, $\mathcal{G} = \mathrm{Bor}(\mathbb{C})$ et $f : \mathbb{N} \to \mathbb{C}$, $n \mapsto z^n$.

Puisque la mesurabilité de z^X est acquise, son intégrabilité équivaut à

$$\mathbf{E}|z^X| = \int_\Omega |z^X| \, \mathrm{d}\mathbf{P} < +\infty. \tag{11}$$

En notant $P_X = \mathbf{P} \circ X^{-1}$ la loi de X, on a pour tout n entier, $P_X(\{n\}) = \mathbf{P}(X = n)$. La loi P_X est la mesure discrète

$$P_X = \sum_{n\in\mathbb{N}} \mathbf{P}(X = n)\delta_n.$$

Le théorème de transfert entre Ω et $\mathbb{N}$ et le calcul d'une intégrale par rapport à une mesure discrète nous permettent d'écrire

$$\int_\Omega |z^X| \,\mathrm{d}\mathbf{P} = \int_{\mathbb{N}} |z^n| \,\mathrm{d}P_X(n) = \sum_{n\in\mathbb{N}} |z^n| \mathbf{P}(X = n).$$

La c.n.s. d'intégrabilité (11) équivaut ainsi à la convergence *absolue* au point z de la série entière de terme général $\mathbf{P}(X = n)z^n$:

$$z^X \text{ est } \mathbf{P}\text{-intégrable} \quad \Leftrightarrow \quad \sum_{n=0}^{+\infty} \mathbf{P}(X = n)|z|^n < +\infty. \tag{12}$$

Le domaine de définition D de la *fonction génératrice* G_X de X

$$G_X : z \mapsto G_X(z) := \mathbf{E}(z^X),$$

est donc l'ensemble des $z \in \mathbb{C}$ pour lesquels la série dans (12) a une somme finie. Cette condition est réalisée au moins pour tous les z du disque unité fermé puisque si $|z| \le 1$,

$$\sum_{n=0}^{+\infty} \mathbf{P}(X = n)|z|^n \le \sum_{n=0}^{+\infty} \mathbf{P}(X = n) = 1 < +\infty.$$

Pour tout $z \in D$, z^X est $\mathbf{P}$-intégrable et son espérance se calcule par transfert exactement comme pour $|z^X|$ ci-dessus, mais en supprimant le module :

$$\forall z \in D, \quad G_X(z) = \sum_{n=0}^{+\infty} \mathbf{P}(X = n)z^n.$$

Cette formule montre clairement que G_X ne dépend que de la *loi* de X. Deux variables aléatoires entières X et Y de même loi ont donc même fonction génératrice. Réciproquement si X et Y sont telles que $G_X = G_Y$, l'égalité des *séries entières* $G_X(z)$ et $G_Y(z)$ entraîne l'égalité de leurs coefficients[1]. On a donc $\mathbf{P}(X = n) = \mathbf{P}(Y = n)$ pour tout entier n, ce qui donne bien l'égalité des *lois* de X et Y. Ainsi la fonction génératrice d'une variable aléatoire entière caractérise sa loi, au même titre que la fonction de répartition.

3) Soit X une variable aléatoire entière dont l'ensemble des valeurs possibles $X(\Omega)$ est inclus dans $\{1, 2, 3, 4, 5, 6\}$. On a $P(X = 0) = 0$ et $P(X = n) = 0$ pour tout $n > 6$. La série entière $G_X(z)$ se réduit donc à la somme finie :

$$G_X(z) = \sum_{n=1}^{6} P(X = n)z^n.$$

G_X est un polynôme sans terme constant donc factorisable sous la forme

$$G_X(z) = zQ_X(z) \tag{13}$$

[1] Il suffit même pour cela que $G_X(z) = G_Y(z)$ sur un disque ouvert de centre 0 et de rayon ε puisque les coefficients d'une série entière $G(z) = \sum_n a_n z^n$ vérifient $n!a_n = G^{(n)}(0)$.

où Q_X est un polynôme. Si $P(X=6)\neq 0$, le degré de G_X est 6 donc celui de Q_X est 5 et un polynôme *à coefficients réels* de degré *impair* a toujours au moins une racine réelle.

Dans le cas particulier où X suit la loi uniforme sur $\{1,2,3,4,5,6\}$, l'ensemble des valeurs possibles $X(\Omega)$ est exactement$\{1,2,3,4,5,6\}$ et $P(X=n)=1/6$ pour $1\leq n\leq 6$ d'où :

$$G_X(z)=\frac{1}{6}(z+z^2+z^3+z^4+z^5+z^6) \quad \text{et} \quad Q_X(z)=\frac{1}{6}(1+z+z^2+z^3+z^4+z^5).$$

Pour factoriser complètement $Q_X(z)$ sous la forme

$$Q_X(z)=\prod_{k=1}^{5}(z-z_k),$$

on remarque que pour $z\neq 1$, $Q_X(z)=(z^6-1)/(z-1)$. Les zéros de Q_X sont donc les racines sixièmes de l'unité autres que 1, soit les

$$z_k=\exp\Big(\frac{2k\pi\mathrm{i}}{6}\Big), \quad k=1,\dots,5.$$

Une seule d'entre elles est réelle, c'est $z_3=-1$.

4) Soient X et Y deux variables aléatoires entières indépendantes (ceci équivaut à l'indépendance des événements $\{X=k\}$ et $\{Y=l\}$ pour tout couple d'entiers (k,l)). Montrons que pour tout z de module inférieur ou égal à 1 on a :

$$G_{X+Y}(z)=G_X(z)G_Y(z)$$

et que cette relation est valable pour tout complexe z lorsque $X(\Omega)$ et $Y(\Omega)$ sont des parties finies de $\mathbb{N}$.

Considérons l'événement $\{X+Y=n\}$. Il peut se décomposer en la réunion disjointe des $\{X=k,Y=l\}$ pour tous les couples d'entiers (k,l) tels que $k+l=n$. D'autre part l'indépendance de X et Y nous permet d'écrire $P(X=k,Y=l)=P(X=k)P(Y=l)$ d'où :

$$P(X+Y=n)=\sum_{k+l=n}P(X=k,Y=l)=\sum_{k+l=n}P(X=k)P(Y=l). \tag{14}$$

Ceci permet d'exprimer G_{X+Y} en fonction de G_X et G_Y de la manière suivante. Pour tout z tel que $|z| \leq 1$:

$$\begin{aligned}
G_{X+Y}(z) &= \sum_{n=0}^{+\infty} P(X+Y=n)z^n \\
&= \sum_{n=0}^{+\infty} \sum_{k+l=n} P(X=k, Y=l)\ z^n \\
&= \sum_{n=0}^{+\infty} \sum_{k+l=n} P(X=k)z^k\, P(Y=l)z^l \qquad (15) \\
&= \left(\sum_{k=0}^{+\infty} P(X=k)z^k\right)\left(\sum_{l=0}^{+\infty} P(Y=l)z^l\right) \qquad (16)
\end{aligned}$$

Sous réserve de justification de cette dernière égalité, on en déduit :

$$G_{X+Y}(z) = G_X(z)G_Y(z), \qquad \text{pour tout } z \text{ tel que } |z| \leq 1. \qquad (17)$$

Le passage de (15) à (16) se justifie en rappelant que si deux séries de terme généraux complexes respectifs u_n et v_n sont *absolument* convergentes, la série de terme général $w_n = \sum_{k+l=n} u_k v_l$ est absolument convergente et a pour somme le produit des sommes des deux séries de départ (série produit). Or les deux séries définissant G_X et G_Y sont absolument convergentes au moins pour $|z| \leq 1$ donc les seconds membres de (15) et (16) sont bien définis et égaux pour $|z| \leq 1$.

Lorsque $X(\Omega)$ et $Y(\Omega)$ sont des parties finies de $\mathbb{N}$, l'ensemble des valeurs possibles de $X+Y$ est aussi fini. Toutes les séries intervenant dans le calcul ci-dessus sont des polynômes, il n'y a donc plus aucun problème de convergence et (17) est valable pour tout complexe z.

5) On dispose de deux dés et on aimerait truquer *individuellement* chacun d'eux de façon que la somme des points suive la loi uniforme sur $\{2, 3, \dots, 12\}$...Le truquage de chaque dé étant *individuel*, la méthode de truquage doit préserver l'indépendance des deux dés.

Soit Z une variable aléatoire de loi uniforme sur $\{2, 3, \dots, 12\}$. Comme il y a onze valeurs possibles, $P(Z=n) = 1/11$ pour $2 \leq n \leq 12$. La fonction génératrice est donc :

$$G_Z(z) = \frac{1}{11}(z^2 + z^3 + \cdots + z^{12}) = \frac{z^2}{11}(1 + z + z^2 + \cdots z^{10}).$$

Les zéros de $1 + z + z^2 + \cdots + z^{10}$ sont les racines onzièmes des l'unité autres que 1 soit les $s_k = \exp\bigl(2k\pi\mathrm{i}/11\bigr)$ pour $k = 1, \dots, 10$. Si l'un des s_k était réel, il vaudrait soit -1 soit 1.

Le premier cas équivaut à :

$$\exists l \in \mathbb{Z}, \quad \frac{2k\pi}{11} = \pi + 2l\pi \ \Leftrightarrow\ \exists l \in \mathbb{Z}, \quad 2k = 11(2l+1),$$

ce qui est impossible puisque $11(2l+1)$ est impair.

Le deuxième cas équivaut à :

$$\exists l \in \mathbb{Z}, \quad \frac{2k\pi}{11} = 2l\pi \Leftrightarrow \exists l \in \mathbb{Z}, \quad k = 11l,$$

ce qui est impossible à cause de la restriction $1 \leq k \leq 10$.

On en déduit que la fonction génératrice de Z peut se factoriser sous la forme :

$$G_Z(z) = z^2 R(z), \tag{18}$$

où R est un polynôme de degré 10 sans racine réelle.

Supposons donc que l'on puisse réaliser un truquage individuel de chaque dé de façon que la somme des points $X + Y$ suive la loi uniforme sur $\{2, 3, \dots, 12\}$. Alors d'après (17), (13) et (18) on a :

$$G_{X+Y}(z) = G_X(z)G_Y(z) = z^2 Q_X(z)Q_Y(z) = z^2 R(z)$$

Comme R est de degré 10, Q_X et Q_Y sont nécessairement de degré 5. Ils ont donc au moins une racine réelle chacun, ce qui est contradictoire avec le fait que R n'en a aucune ($Q_X Q_Y = R$).

Il est donc impossible de réaliser un truquage préservant l'indépendance des deux dés et tel que la somme des points suive la loi uniforme sur $\{2, 3, \dots, 12\}$.

Problème

Dans tout le problème, $(\Omega, \mathcal{F}, \mu)$ est un espace mesuré et f une application $\Omega \to \mathbb{R}_+$, $\mathcal{F}$-Bor$(\mathbb{R}_+)$ mesurable telle que $\int_\Omega f \, \mathrm{d}\mu < +\infty$. Le but du problème est d'établir la formule

$$\int_\Omega f \, \mathrm{d}\mu = \int_{]0,+\infty[} \mu(\{f \geq t\}) \, \mathrm{d}\lambda(t), \tag{19}$$

où λ désigne la mesure de Lebesgue sur $\mathbb{R}$. Cette formule se démontre assez facilement lorsque l'on dispose du théorème de Fubini. Une approche alternative est exposée à partir de la question 2) ci-dessous. La question 1) a pour but d'établir une propriété classique des discontinuités d'une fonction monotone.

1) Soit I un intervalle de $\mathbb{R}$ et $g : I \to \mathbb{R}$ une fonction croissante. On rappelle qu'en tout point c intérieur à I, g a une limite à gauche notée $g(c^-)$ et une limite à droite notée $g(c^+)$ et que $g(c^-) \leq g(c) \leq g(c^+)$. On note

$$\mathrm{s}(g, c) := g(c^+) - g(c^-).$$

On dit que c est un *point de saut* pour g si $\mathrm{s}(g, c) \neq 0$. Remarquons qu'en raison de la croissance de g et de la définition de $g(c^-)$ et $g(c^+)$ comme limites à gauche et à droite de g au point c, on a pour toute paire de réels x, x' dans I tels que $x < c < x'$, $g(x) \leq g(c^-) \leq g(c^+) \leq g(x')$. Par conséquent,

$$\forall x, x' \in I, \quad x < c < x' \quad \Rightarrow \quad g(x') - g(x) \geq \mathrm{s}(g, c). \tag{20}$$