DS8 (version B) /115

Partie I - Lois de Laplace - propriétés et simulation /...

Soit $\alpha \in \mathbb{R}$ et $\beta > 0$. On dit qu'une variable aléatoire réelle à densité suit une loi de Laplace de paramètre (α, β), notée $\mathcal{L}(\alpha, \beta)$, si elle admet comme densité la fonction f donnée par :

$$\forall t \in \mathbb{R},\ f(t) = \frac{1}{2\beta}\ \exp\left(-\frac{|t-\alpha|}{\beta}\right)$$

1. Vérifier que f est bien une densité de probabilité d'une variable aléatoire réelle.

- **1 pt : f continue**
- **1 pt : f positive**
- **2 pts : qq soit la méthode**
  Découpage possible :
  $\displaystyle\int_0^{+\infty} f(t)\ dt = \frac{1}{2}$ **(1 point)**
  $\displaystyle\int_{-\infty}^{0} f(t)\ dt = \frac{1}{2}$ **(1 point)**

2. Déterminer la fonction de répartition, notée Ψ, de la loi $\mathcal{L}(0,1)$.

- **1 pt : cas $x \leqslant 0$ ($\Psi(x) = \frac{1}{2}\mathrm{e}^{x}$)**
- **1 pt : cas $x > 0$ ($\Psi(x) = 1 - \frac{1}{2}\mathrm{e}^{-x}$)**

3. On suppose que X suit la loi $\mathcal{L}(0,1)$.

a) Montrer que $Y = \beta X + \alpha$ suit la loi $\mathcal{L}(\alpha, \beta)$.

- **1 pt : $F_Y(x) = \Psi\left(\dfrac{x-\alpha}{\beta}\right)$**
- **1 pt : expression de** $F_Y(x) = \begin{cases} \dfrac{1}{2}\exp\left(\dfrac{x-\alpha}{\beta}\right) & \textbf{si } x \leqslant \alpha \\ 1 - \dfrac{1}{2}\exp\left(\dfrac{-x+\alpha}{\beta}\right) & \textbf{si } x > \alpha \end{cases}$
- **1 pt : F_Y de classe $\mathcal{C}^1$ sur $\mathbb{R}$**
- **1 pt : $f_Y = F_Y' = f$**

b) En déduire la fonction de répartition de la loi $\mathcal{L}(\alpha, \beta)$.

- **1 pt : expression de F trouvée dans la question précédente**

4. *Espérance et variance.*

a) On suppose que X suit la loi $\mathcal{L}(0,1)$.
Montrer que $\mathbb{E}(X)$ et $\mathbb{V}(X)$ existent et valent respectivement 0 et 2.

- **1 pt :** X **admet une esp** $\Leftrightarrow \displaystyle\int_{-\infty}^{+\infty} t\ln(t)\ dt$ **(absolument) convergente**
- **1 pt :** $\displaystyle\int_{0}^{+\infty} t\ln(t)\ dt = -\int_{-\infty}^{0} t\ln(t)\ dt$ **car** f **impaire**
- **1 pt :** $\displaystyle\int_{0}^{+\infty} t\ln(t)\ dt$ **est convergente (on reconnaît l'espérance de** $Z \hookrightarrow \mathcal{E}(1)$**)**
- **1 pt :** $\mathbb{E}(X) = 0$
- **1 pt :** $\displaystyle\int_{-\infty}^{+\infty} t^2\ln(t)\ dt = 2\int_{0}^{+\infty} t^2\ln(t)\ dt$ **(parité)**
- **1 pt : on reconnaît le moment d'ordre 2 de** $Z \hookrightarrow \mathcal{E}(1)$
- **1 pt :** $E(Z^2) = 2$ **par la formule de Kœnig-Huygens**
- **1 pt :** $\mathbb{E}(X^2) = 2$ **et conclusion** $\mathbb{V}(X^2) = 2$**.**

b) En déduire l'existence et les valeurs de l'espérance et de la variance d'une variable aléatoire réelle qui suit la loi $\mathcal{L}(\alpha,\beta)$.

- **1 pt :** $\mathbb{E}(Y) = \alpha$ **(linéarité de l'espérance)**
- **1 pt** $\mathbb{V}(Y) = 2\beta^2$ **(propriété de la variance)**

5. *Simulation à partir d'une loi exponentielle.*
Soit U une variable aléatoire qui suit la loi exponentielle de paramètre 1 et V une variable aléatoire qui suit la loi de Bernoulli de paramètre $\frac{1}{2}$ et indépendante de U.

a) En utilisant le système complet naturellement associé à V, montrer que $X = (2V-1)\,U$ suit la loi $\mathcal{L}(0,1)$.

- **1 pt : formule des proba totales** $(\mathbb{P}([X \leqslant x]) = \mathbb{P}([V=1]\cap[X \leqslant x]) + \mathbb{P}([V=0]\cap[X \leqslant x])$
- **1 pt :** $= \mathbb{P}([V=1]\cap[U \leqslant x]) + \mathbb{P}([V=0]\cap[-U \leqslant x])$
- **1 pt : indépendance de** U **et** V
- **1 pt :** $F_X(x) = \dfrac{1}{2}F_U(x) + \dfrac{1}{2}(1 - F_U(-x))$
- **1 pt :** $F_X : x \mapsto \begin{cases} \frac{1}{2}\,\mathrm{e}^{x} & \textbf{si } x \leqslant 0 \\ 1 - \frac{1}{2}\,\mathrm{e}^{-x} & \textbf{si } x > 0 \end{cases}$
  et on reconnaît $\mathcal{L}(0,1)$

b) Compléter la définition **Scilab** ci-dessous pour que la fonction ainsi définie réalise la simulation d'une variable aléatoire qui suit la loi $\mathcal{L}(\alpha,\beta)$:

```
function r = Laplace(alpha, beta)
    if --- <= 1/2
        V = 1
    else
        V = 0
    end
    X = (2 * V - 1) * grand(1, 1, 'exp', 1)
    r = ---
endfunction
```

- **1 pt :** `if rand() <= 1/2 then`
- **1 pt :** `r = beta * X + alpha`

Partie II - Lois ε-différentielles /43

Soit $\varepsilon > 0$. On dit que (X,Y), un couple de variables aléatoires, est un couple ε-différentiel si, pour tout intervalle I de $\mathbb{R}$:

$$e^{-\varepsilon}\ \mathbb{P}([X \in I]) \ \leqslant\ \mathbb{P}([Y \in I]) \ \leqslant\ e^{\varepsilon}\ \mathbb{P}([X \in I])$$

Intuitivement, les lois de X et Y seront d'autant plus proches que le plus petit ε tel que (X,Y) soit un couple ε-différentiel est proche de 0.

6. Soit (X,Y,Z) un triplet de variables aléatoires réelles.

a) Montrer que si (X,Y) est ε-différentiel alors (Y,X) l'est aussi.

- 1 pt : multiplication par e$^{\varepsilon} > 0$ à gauche

- 1 pt : multiplication par e$^{-\varepsilon} > 0$ à droite

b) Montrer que si (X,Y) est ε-différentiel et (Y,Z) est ε'-différentiel alors (X,Z) est $(\varepsilon+\varepsilon')$-différentiel.

- 1 pt : $e^{-\varepsilon}\,\mathbb{P}([X \in I]) \leqslant \mathbb{P}([Y \in I])$ et $e^{-\varepsilon'}\,\mathbb{P}([Y \in I]) \leqslant \mathbb{P}([Z \in I])$ implique $e^{-(\varepsilon+\varepsilon')}\,\mathbb{P}([X \in I]) \leqslant \mathbb{P}([Z \in I])$

- 1 pt : $\mathbb{P}([Y \in I]) \leqslant e^{\varepsilon}\,\mathbb{P}([X \in I])$ et $\mathbb{P}([Z \in I]) \leqslant e^{\varepsilon'}\,\mathbb{P}([Y \in I])$ implique $\mathbb{P}([Z \in I]) \leqslant e^{\varepsilon+\varepsilon'}\,\mathbb{P}([X \in I])$

7. Soit (X,Y) un couple de variables aléatoires réelles discrètes.
On suppose que $X(\Omega)\ \cup\ Y(\Omega) = \{z_n \mid n \in J\}$ où J est un sous ensemble non vide de $\mathbb{N}$.

Montrer que (X,Y) est ε-différentiel si et seulement si

$$\forall n \in J,\ e^{-\varepsilon}\ \mathbb{P}([X = z_n]) \ \leqslant\ \mathbb{P}([Y = z_n]) \ \leqslant\ e^{\varepsilon}\ \mathbb{P}([X = z_n])$$

- 1 pt : $(\Rightarrow)$ (appliquer ε-différentiabilité à $I = \{z_n\}$)

- 3 pts : $(\Leftarrow)$

8. *Premier exemple.*
Dans cette question, on suppose que X suit la loi géométrique de paramètre $\frac{1}{2}$, Z suit la loi de Bernoulli de paramètre $p \in\ ]0,1[$ et elles sont indépendantes. On pose $Y = X + Z$.

a) Déterminer la loi de Y.

- 1 pt : $Y(\Omega) = \mathbb{N}^*$

- 1 pt : FPT $\mathbb{P}([Y = k]) = (1-p)\ \mathbb{P}([X = k]) + p\ \mathbb{P}([X = k-1])$

- 1 pt : cas $k = 1$ ($\mathbb{P}([Y = 1]) = \dfrac{1-p}{2}$)

- 1 pt : cas $k \geqslant 2$: $\mathbb{P}([Y = k]) = \dfrac{1+p}{2^k}$

b) Établir que pour tout $k \in \mathbb{N}^*$, $1-p\ \leqslant\ \dfrac{\mathbb{P}([Y = k])}{\mathbb{P}([X = k])}\ \leqslant\ \dfrac{1}{1-p}$.

- 2 pts : cas $k = 1$ ($1-p \leqslant \dfrac{\mathbb{P}([Y = 1])}{\mathbb{P}([X = 1])} = 1-p \leqslant \dfrac{1}{1-p}$)

- 2 pts : cas $k = 2$ ($\dfrac{\mathbb{P}([Y = k])}{\mathbb{P}([X = k])} = 1+p$)

c) En déduire que (X,Y) est $-\ln(1-p)$-différentiel.

- 1 pt : d'après qst précédente $e^{-\ln(1-p)} \leqslant \dfrac{\mathbb{P}([Y = k])}{\mathbb{P}([X = k])} \leqslant e^{-\ln(1-p)}$

d) Que se passe-t-il lorsque p s'approche de 0 ou lorsqu'il s'approche de 1 ? Était-ce prévisible ?

- **1 pt : si p s'approche de 0, alors la probabilité $\mathbb{P}([X = Y]) = \mathbb{P}([Z = 0]) = 1 - p$ se rapproche de 1.**
  Les lois de X et Y sont donc d'autant plus proche que p s'approche de 0.
- **1 pt : Lorsque p s'approche de 1, $-\ln(1 - p)$ s'approche de $+\infty$.**

9. On suppose que X et Y sont deux variables à densité de densités respectives f et g et de fonction de répartition F et G.

a) On suppose que pour tout $t \in \mathbb{R}$: $\mathrm{e}^{-\varepsilon} f(t) \leqslant g(t) \leqslant \mathrm{e}^{\varepsilon} f(t)$.
Montrer que (X, Y) est ε-différentiel.

- **1 pt : croissance de l'intégrale (bornes bien ordonnées)**

b) On suppose dans la suite de cette question que (X, Y) est ε-différentiel.
Soit $h > 0$ et $t \in \mathbb{R}$ où f et g sont continues.

Montrer que :

$$\mathrm{e}^{-\varepsilon} \frac{F(t+h) - F(t)}{h} \leqslant \frac{G(t+h) - G(t)}{h} \leqslant \mathrm{e}^{\varepsilon} \frac{F(t+h) - F(t)}{h}$$

En conclure que : $\mathrm{e}^{-\varepsilon} f(t) \leqslant g(t) \leqslant \mathrm{e}^{\varepsilon} f(t)$.

- **1 pt : appliquer définition ε-différentiabilité à $I = [t, t + h]$**
- **1 pt : F et G de classe $\mathcal{C}^1$ car f et g continues**
- **1 pt : passage à la limite quand h tend vers 0**

10. *Deuxième exemple : lois de Cauchy.*

a) Montrer que $\displaystyle\int_{-\infty}^{+\infty} \frac{1}{t^2+1}\, dt$ converge. On admet que cette intégrale est égale à π.

- **1 pt : $t \mapsto \dfrac{1}{1+t^2}$ continue sur segment $[0, 1]$, donc $\displaystyle\int_0^1 \frac{1}{1+t^2}\, dt$ bien définie**
- **2 pts : $\displaystyle\int_0^1 \frac{1}{1+t^2}\, dt$ converge (1pt pour équivalent + 1 pt pour le critère avec intégrale de Riemann impropre en $+\infty$ d'exposant 2, donc convergente)**
- **1 pt : $\displaystyle\int_{-\infty}^0 \frac{1}{1+t^2}\, dt = \int_0^{+\infty} \frac{1}{1+t^2}\, dt$ par parité**

b) On définit, pour $a > 0$, la fonction f_a sur $\mathbb{R}$ par, pour tout $t \in \mathbb{R}$, $f_a(t) = \dfrac{a}{\pi\ (t^2 + a^2)}$.
Montrer que f_a est une densité de probabilité d'une variable aléatoire à densité.

- **1 pt : f_a continue sur $\mathbb{R}$**
- **1 pt : f_a positive**
- **2 pts : changement de variable $u = \dfrac{t}{a}$ (1 pt pour classe $\mathcal{C}^1$, 1 pt pour reste)**

c) On suppose que X et Y sont deux variables aléatoires admettant comme densités repectives f_1 et f_a avec $a > 1$.
Montrer que (X, Y) est $\ln(a)$-différentiel.

- **1 pt : question *10* (on veut montrer : $\mathrm{e}^{-\ln(a)} f(t) \leqslant g(t) \leqslant \mathrm{e}^{\ln(a)} f(t)$)**
- **1 pt : $\dfrac{1}{a} \dfrac{1}{t^2+1} \leqslant \dfrac{a}{t^2+a^2} \Leftrightarrow 0 \leqslant (a^2-1)t^2$**
- **1 pt : $\dfrac{a}{t^2+a^2} \leqslant \dfrac{a}{t^2+1}$**

11. *Une première interprétation.*
On suppose que (X, Y) est un couple ε-différentiel et que U est une variable de Bernoulli de paramètre $p \in]0, 1[$ indépendante de X et Y.
On définit la variable aléatoire Z par :

$$\forall \omega \in \Omega,\ Z(\omega) = \begin{cases} X(\omega) & \text{si } U(\omega) = 1 \\ Y(\omega) & \text{sinon.} \end{cases}$$

a) Soit I un intervalle de $\mathbb{R}$ telle que $\mathbb{P}([Z \in I]) \neq 0$.

Montrer que :

$$\mathbb{P}_{[Z\in I]}([U = 1]) = p\ \frac{\mathbb{P}([X \in I])}{p\ \mathbb{P}([X \in I]) + (1 - p)\ \mathbb{P}([Y \in I])}$$

En déduire que :

$$\frac{p}{p + (1 - p)\ \mathrm{e}^{\varepsilon}} \leqslant \mathbb{P}_{[Z\in I]}([U = 1]) \leqslant \frac{p}{p + (1 - p)\ \mathrm{e}^{-\varepsilon}}$$

- 1 pt : proba conditionnelle $\mathbb{P}_{[Z\in I]}([U = 1]) = \dfrac{\mathbb{P}([Z \in I] \cap [U = 1])}{\mathbb{P}([Z \in I])}$)

- 1 pt : $\mathbb{P}([Z \in I] \cap [U = 1]) = p\ \mathbb{P}([X \in I])$

- 2 pts : FPT $\mathbb{P}([Z \in I]) = p\ \mathbb{P}([X \in I]) + (1 - p)\ \mathbb{P}([Y \in I])$ **dont indépendance**

b) Si ε est proche de zéro, le fait de disposer d'une information sur la valeur de Z change-t-il notablement le paramètre de la loi de U et par conséquent la probabilité d'en déduire la valeur prise par U ?

- 1 pt : si ε proche de 0, alors $\dfrac{p}{p + (1 - p)\mathrm{e}^{\varepsilon}}$ **et** $\dfrac{p}{p + (1 - p)\mathrm{e}^{-\varepsilon}}$ **proches de p**

- 1 pt : alors $p = \mathbb{P}([U = 1])$ **proche de** $\mathbb{P}_{[Z\in I]}([U = 1])$

- 1 pt : connaissance sur Z change peu la proba de déduire la valeur prise par U

Partie III - Confidentialité différentielle /40

- Soit $d \in \mathbb{N}^*$. On considère $D = [\![0, d]\!]$ et n un entier naturel plus grand que 2.
- On dira que deux éléments de D^n, a et b, sont voisins si ils ne différent que d'une composante au plus. On note $\mathcal{V}$ l'ensemble des couples de voisins.
- On considère q une application de D^n dans $\mathbb{R}$.

Concrètement, un élément de D^n représente une table d'une base de donnée et q une requête sur cette base. Étant donné $a = (a_1, \ldots, a_n)$, on s'intéresse au problème de la confidentialité de certains des a_i lorsque les autres a_i sont connus, ainsi que D, q et $q(a)$.

12. Dans cette question on suppose que $a_2, \ldots, a_n$ sont connus et on cherche à protéger a_1.

a) Quelle est probabilité d'obtenir la bonne valeur de a_1 si l'on choisit une valeur au hasard dans $[\![0, d]\!]$?

- 1 pt : $\dfrac{1}{d + 1}$

b) Dans cette question $q(a_1, \ldots, a_n) = \sum\limits_{i=1}^{n} a_i$.
Montrer que si $q(a)$ est publique alors on sait déterminer la valeur de a_1.

- 1 pt : si $q(a)$ publique, alors $a_1 = q(a) - a_2 - \cdots - a_n$

On dit que l'on dispose d'un procédé de ε-confidentialité de D^n pour q si :

(c1) pour tout $a \in D^n$, on dispose d'une variable aléatoire réelle X_a ;

(c2) pour tout $(a,b) \in \mathcal{V}$, (X_a, X_b) est ε-différentiel.

(c3) pour tout $a \in D^n$, $\mathbb{E}(X_a) = q(a)$.

13. *Majoration de la probabilité de trouver a_1.*
Dans cette question, nous allons justifier en partie la terminologie.
On suppose à nouveau que $a_2, \dots, a_n$ sont connus, que l'on cherche à protéger a_1 et que :

× le public connaît des d'intervalles $I_0, \dots, I_d$ disjoints de réunion $\mathbb{R}$ tels qu'avec les valeurs fixées de $a_2, \dots, a_n$, si $q(a) \in I_j$ alors $a_1 = j$. Cela signifie que si $q(a)$ est publique alors a_1 aussi.

× on dispose d'un procédé de ε-confidentialité de D^n pour q et que l'on rend X_a publique à la place de $q(a)$.

On considère alors que l'expérience aléatoire modélisée par $(\Omega, \mathscr{A}, \mathbb{P})$ comporte comme première étape le choix au hasard de a_1 dans $[\![0, d]\!]$ et on définit :

× A_1 la variable aléatoire associée à ce choix ;

× pour tout $j \in [\![0, d]\!]$, $Y_j = X_{(j, a_2, \dots, a_n)}$.
On suppose que A_1 et Y_j sont indépendantes pour tout $j \in D$.

× la variable aléatoire réelle R par :

$$\forall \omega \in \Omega, \text{ si } A_1(\omega) = j \text{ alors on détermine l'unique } k \text{ tel que } Y_j(\omega) \in I_k \text{ et on pose } R(\omega) = k$$

× $\theta = \mathbb{P}([R = A_1])$.

a) Montrer que $\theta = \sum\limits_{j=0}^{d} \mathbb{P}([Y_j \in I_j] \cap [A_1 = j])$.

- 1 pt : formule des proba totales sur le SCE associé à A_1, *i.e.* $([A_1 = i])_{i \in [\![1,d]\!]}$

- 1 pt : $[R = i] \cap [A_1 = i] = [Y_i = i] \cap [A_1 = i]$

b) En déduire que $\theta = \dfrac{1}{d+1} \sum\limits_{j=0}^{d} \mathbb{P}([Y_j \in I_j])$.

- 1 pt : indépendance Y_j et A_1

- 1 pt : $\mathbb{P}([A_1 = j]) = \dfrac{1}{d+1}$

c) En conclure que :

$$\theta \leqslant \frac{1}{d+1} \left(\mathrm{e}^{\varepsilon} - (\mathrm{e}^{\varepsilon} - 1)\, \mathbb{P}([Y_0 \in I_0])\right) \leqslant \frac{\mathrm{e}^{\varepsilon}}{d+1}$$

- 1 pt : $(j, a_2, \dots, a_n)$ et $(0, a_2, \dots, a_n)$ voisins donc (Y_j, Y_0) est ε-différentiel

- 1 pt : pour $I = I_j$, on a $\mathrm{e}^{-\varepsilon} \mathbb{P}([Y_j \in I_j]) \leqslant \mathbb{P}([Y_0 \in I_j])$

- 1 pt : on somme sur $[\![1, d]\!]$

- 1 pt : $\dfrac{1}{d+1} \sum\limits_{j=0}^{d} \mathbb{P}([Y_j \in I_j]) \leqslant \dfrac{1}{d+1} (\mathrm{e}^{\varepsilon} - (\mathrm{e}^{\varepsilon} - 1) \mathbb{P}([Y_0 \in I_0]))$

- 1 pt : $-(\mathrm{e}^{\varepsilon} - 1) \mathbb{P}([Y_0 \in I_0]) < 0$

d) On pose $\rho = \dfrac{1}{d+1}$ et $\tau = \dfrac{\theta - \rho}{\rho}$.
Donner une majoration de τ. Que représente cette quantité ?
Qu'en déduire concernant la méthode de confidentialité présentée dans cette question lorsque ε est proche de 0 ?

- **1 pt :** $\tau \leqslant \mathbf{e}^{\varepsilon} - 1$
- **1 pt : quand ε tend vers 0, la méthode de confidentialité n'augmente que peu la proba d'obtenir la bonne valeur de a par rapport à un choix aléatoire**

On pose $\delta = \displaystyle\max_{(a,b)\in\mathcal{V}} |q(a) - q(b)|$ et on suppose que $\delta > 0$.

14. Dans cette question, pour tout $a \in D^n$, on pose $X_a = q(a) + Y$ où Y suit la loi de Laplace de paramètre $(0, \beta)$.

a) Pour tout $a \in D^n$, déterminer $\mathbb{E}(X_a)$ et une densité de probabilité f_a de la loi de X_a en fonction de $q(a)$ et de β.

- **1 pt : d'après *3.a)*,** $X_a \hookrightarrow \mathcal{L}(q(a), \beta)$
- **1 pt :** $\mathbb{E}(X_a) = q(a)$
- **1 pt :** $f_a(t) = \dfrac{1}{2\beta} \exp\left(-\dfrac{|t - q(a)|}{\beta}\right)$

b) Montrer que pour tout $t \in \mathbb{R}$ et $(a, b) \in \mathcal{V}$, $f_a(t) \leqslant \exp\left(\dfrac{\delta}{\beta}\right) f_b(t)$.

En déduire que pour tout $(a, b) \in \mathcal{V}$, (X_a, X_b) est $\dfrac{\delta}{\beta}$-différentiel.

- **1 pt : inégalité triangulaire (**$|t - q(b)| - |t - q(a)| \leqslant \delta$
- **1 pt :** exp **strictement croissante sur $\mathbb{R}$ donc** $\exp\left(-\dfrac{|t - q(a)|}{\beta}\right) \leqslant \exp\left(\dfrac{\delta}{\beta}\right) \exp\left(-\dfrac{|t - q(b)|}{\beta}\right)$
- **1 pt :** $f_a(t) \leqslant \exp\left(\dfrac{\delta}{\beta}\right) f_b(t)$ **et** $f_b(t) \leqslant \exp\left(\dfrac{\delta}{\beta}\right) f_a(t)$

c) Comment choisir β pour disposer alors d'un procédé de ε-confidentialité de D^n pour q ?

- **2 pts :** $\beta = \dfrac{\delta}{\varepsilon}$

15. Dans cette question, pour tout $a = (a_1, \ldots, a_n)$ appartenant à D^n, $q(a) = \sum\limits_{k=1}^{n} a_k$.

a) Quelle est la valeur de δ ?

- **1 pt : pour a et b voisins de D,** $q(a) - q(b) = a_{i_0} - b_{i_0} \in [\![-d, d]\!]$
- **1 pt :** $|q(a) - q(b)| \leqslant d$**, donc** $\delta \leqslant d$

On utilise dans la suite le procédé de ε-confidentialité tel qu'il a été défini dans la question 14 mais au lieu de publier la valeur X_a, on procède ainsi :

× si $X_a < \frac{1}{2}$ on publie 0 ;
× si $X_a \in [k - \frac{1}{2}, k + \frac{1}{2}[$ où $k \in [\![1, nd - 1]\!]$, on publie k ;
× sinon on publie nd.

b) Montrer que la valeur aléatoire Z_a publiée vérifie : $Z_a = \begin{cases} 0 & \text{si } X_a < \frac{1}{2} \\ \lfloor X_a + \frac{1}{2} \rfloor & \text{si } X_a \in [\frac{1}{2}, nd - \frac{1}{2}[\\ nd & \text{si } X_a \geqslant nd - \frac{1}{2} \end{cases}$

- **1 pt : cas** $X_a < \dfrac{1}{2}$
- **1 pt : cas** $X_a \geqslant nd - \dfrac{1}{2}$
- **2 pts : cas** $X_a \in [\frac{1}{2}, nd - \frac{1}{2}[$ **(1 pt pour** $X_a + \dfrac{1}{2} \in [k, k+1[$**, 1 pt pour** $\lfloor X_a + \dfrac{1}{2} \rfloor = k = Z_a$**)**

c) Écrire un script qui pour d, n et ε saisis par l'utilisateur, génère une valeur aléatoire de $a \in D^n$ puis affiche $q(a)$ et Z_a.

- **1 pt : question *14* et *15.a)* donnent** $X_a = q(a) + Y$ **avec** $Y \hookrightarrow \mathcal{L}(0, \frac{d}{\varepsilon})$
- **6 pts**

```
d = input('d = ')
n = input('n = ')
a = grand(1,n,'uin',0,d)
disp(sum(a))
X = sum(a) + Laplace(0,d/eps)
if X < 1/2 then
    Z = 0
else
    if X < n * d - 1/2 then
        Z = floor(X + 1/2)
    else
        Z = n * d
    end
end
disp(Z)
```

d) Pour $n = 1000$, $d = 4$ et ε choisi par l'utilisateur, écrire un script qui estime la valeur moyenne de $\dfrac{|Z_a - q(a)|}{q(a)}$ (on considèrera que $q(a)$ est toujours non nul).

- **6 pts**

```
d = 4
n = 1000
eps = input('epsilon = ')
M = 0
for i = 1:10000
    a = grand(1,n,'uin',0,d)
    X = sum(a) + Laplace(0,d/eps)
    if X < 1/2 then
        Z = 0
    else
        if X < n*d - 1/2 then
            Z = floor(X + 1/2)
        else
            Z = n *d
        end
    end
    M = M + abs(Z - sum(a)) / sum(a)
end
disp(M/10000)
```