## PROBABILITÉS ET STATISTIQUES

### Notations et préliminaires.

**1.** *Variable aléatoire réelle.*

Dans tout le problème $X$ (avec ou sans indice) note une *variable aléatoire réelle* (une v.a.r. en abrégé), de loi notée $\mathbb{P}_X$, de *fonction de répartition* (en abrégé f.r.) $F_X(t) = \mathbb{P}(X \leq t)$, continue à droite. On notera $F_X(t^-)$ sa limite à gauche. $\mathbb{E}$ est l'espérance mathématique associée à $\mathbb{P}$. La *fonction caractéristique* de X est la fonction $\varphi_X(t) = \mathbb{E}(e^{itX})$.

La *transformée de Fourier* d'une fonction réelle de variable réelle $f$, Lebesgue-intégrable, est $\widehat{f}(t) = \int f(x)e^{itx}dx$. Si la loi de $X$ a une densité $f$, $\varphi_X$ n'est autre que $\widehat{f}$. Une *médiane* $\mu$ est un réel vérifiant $\mathbb{P}(X \leq \mu) \geq 1/2$, $\mathbb{P}(X \geq \mu) \geq 1/2$. On admet le

*Théorème de Radon-Nikodym* (sur $\mathbb{R}$): Si la loi de $X$ est *absolument continue*, c'est à dire que pour toute partie $N$ de mesure de Lebesgue nulle, $\mathbb{P}(X \in N) = 0$ alors elle a une densité, c'est-à-dire qu'il existe une fonction $p$ positive et intégrable telle que $\mathbb{P}(X \in A) = \int_A p(x)dx$.

Le *support topologique* de la loi de $X$ est le plus petit fermé $F$ tel que $\mathbb{P}_X(F) = 1$, soit encore $\mathbb{P}(X \in F) = 1$, et le réel $x$ appartient à ce support si et seulement si

$$\text{Pour tout } \varepsilon > 0, \mathbb{P}(X \in ]x-\varepsilon, x+\varepsilon[) > 0.$$

On dit la v.a.r. $X$ *dégénérée* (ou la loi de $X$ dégénérée) s'il existe un réel $a$ tel que $\mathbb{P}(X = a) = 1$.

La loi de $X$ est dite *diffuse* si la f.r. associée est continue, *discrète* si la f.r. ne croît que par sauts (elle est alors concentrée sur un ensemble dénombrable). Elle est dite *singulière* si elle est diffuse et s'il existe un ensemble $N$ de mesure de Lebesgue nulle avec $\mathbb{P}(X \in N) = 1$. Sa *fonction de concentration* (ou sa concentration) est la fonction définie sur $\mathbb{R}^+$ par

$$Q_X(t) = \sup_{y \in \mathbb{R}} \mathbb{P}(X \in [y, y+t]). \tag{1}$$

En particulier, $Q_X(0)$ n'est nul que si la loi de $X$ est diffuse, et sinon a pour valeur le saut maximum de cette loi. On fait la convention que $Q_X(t)$ vaut 0 pour $t < 0$.

Enfin, si $I = [a, b]$ est un segment fermé et $y$ un réel, $I + y$ note le segment translaté $[a + y, b + y]$.

**2.** *Convergence en loi, relative compacité.*

Une suite de v.a.r. $\{Y_n\}$ est dite *relativement compacte en loi* si:

$$\forall \varepsilon > 0, \ \exists M \text{ tel que } \forall n, \mathbb{P}(|Y_n| \geq M) \leq \varepsilon.$$

Cette condition équivaut à la propriété : De toute suite extraite on peut extraire une sous-suite convergente en loi.

**3.** *Nombres de Pisot-Salem.*

Ce paragraphe a pour but d'introduire les nombres de Pisot-Salem et d'en donner deux propriétés essentielles. Les Polynômes étudiés ici sont ceux de $\mathbb{Q}[X]$ (Polynômes à coefficients rationnels) ou de $\mathbb{Z}[X]$ (Polynômes à coefficients entiers).

Un Polynôme *unitaire* $P$ est un Polynôme de $\mathbb{Z}[X]$, dont le coefficient du terme de plus haut degré vaut 1. Un Polynôme est *irréductible* s'il n'a pas *dans* $\mathbb{Q}[X]$ d'autres diviseurs que les nombres rationnels. Rappelons deux propriétés de ces Polynômes (qu'*on ne demande pas de démontrer*):

p1: Dans $\mathbb{Q}[X]$, si $A$ est irréductible et s'il a une racine (dans $\mathbb{C}$) commune avec $B$, alors $A$ divise $B$.

p2: Si $A$ est unitaire et s'il est factorisable *dans* $\mathbb{Q}[X]$ en $A = B \cdot C$, alors on peut choisir $B$ et $C$ unitaires.

Un *entier algébrique* est (au sens strict) une racine d'un Polynôme unitaire irréductible mais aussi, grâce à p2, toute racine d'un Polynôme unitaire.

On peut donc associer à un entier algébrique $\theta$ un Polynôme $P_\theta$, à la fois irréductible et unitaire, *unique*, dont il est racine. Les autres racines de $P_\theta$ sont des entiers algébriques, dits *conjugués* de $\theta$.

Le *degré* de $\theta$ est le degré de $P_\theta$. Ainsi les entiers sont des entiers algébriques (de degré 1) et sont les seuls entiers algébriques sans conjugués.

*Nombres de Pisot*: $\theta$ est un nombre de Pisot si $\theta$ est un entier algébrique dont tous les conjugués sont de module strictement inférieur à 1. Leur ensemble est noté $\mathcal{S}$.

On remarquera que, le produit des racines d'un Polynôme unitaire étant un entier non nul si 0 n'est pas racine de ce Polynôme, $|\theta| > 1$ pour $\theta \in \mathcal{S}$ (sauf si $|\theta| = 0$ ou si $|\theta| = 1$).

**Dans tout le problème $\{X_i | i \in \mathbb{N}^*\}$ désigne une suite de v.a.r. indépendantes dont on note $\{S_n | n \in \mathbb{N}^*\}$ la suite des sommes partielles**

$$S_n = X_1 + X_2 + \cdots + X_n.$$

La partie **A** est consacrée à la démonstration de quelques propriétés élémentaires de la concentration.

L'une d'entre elles est utilisée dans la partie **B** pour prouver le Théorème de Jessen.

La partie **C**, indépendante, est consacrée à la preuve du Théorème de pureté.

Les parties **D** et **E** sont consacrées à la construction de Probabilités sur $\mathbb{R}$ vérifiant diverses conditions de support. Elles utilisent les résultats des parties précédentes.

**A.** *Propriétés de la fonction de concentration.*

La fonction de concentration $Q_X$ est définie par la formule (1).

1°) Montrer que si $t > 0$, $Q_X(t) > 0$ .

2°) Soit $t$ un réel positif ou nul fixé.

a) Soit $\{a_n\}$ une suite telle que $\mathbb{P}(X \in [a_n, a_n + t])$ converge vers une limite $q(t) > 0$. Montrer que la suite $\{a_n\}$ est bornée.

b) Soit $\{a_n\}$ une suite qui converge vers $a$. Montrer que

$$\text{limsup}_n \mathbb{P}(X \in [a_n, a_n + t]) \leq \mathbb{P}(X \in [a, a + t])$$

(se donnant $\varepsilon > 0$, on pourra minorer $\mathbb{P}(X \in ]a - \varepsilon, a + \varepsilon + t[)$ ). En déduire que si $\mathbb{P}(X \in [a_n, a_n + t])$ tend vers $Q_X(t)$, alors $\mathbb{P}(X \in [a, a + t]) = Q_X(t)$.

c) En déduire qu'il existe un segment $I_t$ de longueur $t$ tel que $Q_X(t) = \mathbb{P}(X \in I_t)$ (On dit que $I_t$ "réalise la concentration" ).

3°) Par un raisonnement analogue, prouver que $Q_X$ est continue à droite, puis que $Q_X$ est une fonction de répartition.

4°) Montrer qu'une CNS pour que $X$ soit dégénérée est que $Q_X(t) = 1$ pour tout $t > 0$.

5°) a) Soit $\mu$ une médiane de $X$ et $t$ tel que $Q_X(t) > 1/2$; soit $I_t$ réalisant cette concentration. Montrer que $\mu \in I_t$, et en déduire que

$$\mathbb{P}(|X| \leq t + |\mu|) \geq Q_X(t) \geq \mathbb{P}(|X| \leq t/2).$$

b) Soit $\{Y_n\}$ une suite de v.a.r. Démontrer qu'une CNS pour que cette suite soit relativement compacte en loi est que:

c1) l'ensemble de leurs médianes $\mu_n$ soit borné.

c2) il existe $Q$, f.r. sur $\mathbb{R}^+$ qui minore toutes les $Q_{Y_n}$ .

6°) Soient $s$ et $t$ deux réels positifs. Soit $I_t$ un segment de longueur $t$. Montrer que

$$\mathbb{P}(X \in I_t) + \mathbb{P}(X \in I_t - s) \leq Q_X(t + s) + Q_X(t - s).$$

Dans les deux questions suivantes, $X$ et $Y$ sont deux v.a.r *indépendantes.*

7°) Prouver que $\mathbb{P}(X + Y \in [a, a + t]) \leq Q_X(t)$ et en déduire

$$Q_{X+Y}(t) \leq \min[Q_X(t), Q_Y(t)]. \tag{2}$$

8°) Le but de cette question est de prouver l'assertion

**(3)** Sauf si $Y$ est dégénérée, il existe au moins un $t > 0$ où l'inégalité stricte $Q_{X+Y}(t) < Q_X(t)$ est vérifiée.

a) Montrer que si $Y$ n'est pas dégénérée, il existe $s > 0$ tel que le support de la loi de $Y$ contienne deux points distincts $u$ et $u + s$.

b) Soient $t > 0$ tel que $Q_{X+Y}(t) = Q_X(t)$, et $I_t$ réalisant $Q_{X+Y}(t)$; montrer que $\mathbb{P}(X \in I_t - y) = Q_X(t)$ pour $\mathbb{P}_Y$-presque tout $y$, puis, en utilisant 2°) b), que $\mathbb{P}(X \in I_t - y) = Q_X(t)$ pour tout $y$ du support de $\mathbb{P}_Y$.

c) Soit $t > 0$ tel que $Q_{X+Y}(t) = Q_X(t)$. Etablir l'inégalité

$$2Q_X(t) \leq Q_X(t + s) + Q_X(t - s) .$$

d) Conclure en étudiant les accroissements de la suite $\{Q_X(ns) | n \in \mathbb{N}\}$.

**B.** *Théorème de Jessen.*

On suppose que $\{S_n\}$ est presque surement convergente et on note $S$ sa limite p.s., $R_n$ le reste $S - S_n$. On utilisera les notations $p, p_n, q_n, r_n$ pour les sauts maximaux (les valeurs en 0 des différentes fonctions de concentrations) respectivement pour les lois de $S, X_n, S_n$ et $R_n$, de sorte que le cas où la loi de $S$ n'est pas diffuse se caractérise par

$$0 < p = Q_S(0). \tag{4}$$

Dans cette partie, par abus de langage, on parlera de "concentration" pour "valeur en 0 de la fonction de concentration".

1°) On note $\alpha$ le produit infini $\Pi_n p_n$.

a) Montrer que $p \leq q_n \leq p_n$ puis que si l'une des $X_n$ est diffuse, $S$ l'est.

b) Soit $x_n$ tel que $p_n = \mathbb{P}(X_n = x_n)$. Montrer que

$$\alpha \leq \mathbb{P}(\forall n, S_n = x_1 + x_2 + \cdots + x_n);$$

en déduire que si $\alpha > 0$, alors la série $\Sigma_n x_n$ converge.

c) Que peut on dire de $\mathbb{P}(S = \Sigma_n x_n)$? Prouver que:

$$\text{Si } \Pi_n p_n > 0, \text{ alors } p > 0.$$

d) Montrer que $q_n \downarrow p$.

On suppose $p > 0$ dans les questions 2°)3°)4°) qui suivent. On remarque que si $U$ et $V$ sont deux v.a.r. indépendantes, et si $a$ est un réel, alors

$$\mathbb{P}(U + V = a) = \Sigma_{x \in \mathcal{D}} \mathbb{P}(U = x)\mathbb{P}(V = a - x)$$

où $\mathcal{D}$ est l'ensemble des points de discontinuité de la f.r. de $U$. Dans la suite on allègera encore cette formule en l'écrivant

$$\mathbb{P}(U + V = a) = \Sigma_x \mathbb{P}(U = x)\mathbb{P}(V = a - x) \ .$$

2°) On se ramène par une translation au cas où $S$ réalise au point 0 sa concentration. Soit $\mathcal{V}$ un voisinage symétrique de 0. Etablir l'inégalité:

$$p = \mathbb{P}(S = 0) = \Sigma_x \mathbb{P}(S_n = x)\mathbb{P}(R_n = -x) \leq r_n \mathbb{P}(S_n \in \mathcal{V}) + q_n \mathbb{P}(R_n \notin \mathcal{V}). \tag{5}$$

Montrer que l'hypothèse de convergence entraîne $\lim_n \mathbb{P}(R_n \notin \mathcal{V}) = 0$, puis que $\lim_{\mathcal{V}} \limsup_n \mathbb{P}(S_n \in \mathcal{V}) = p$. Prouver que $r_n \to 1$, puis que $r_n \uparrow 1$ et que $p_n \to 1$.

3°) En déduire que pour $n$ grand, chacune des concentrations $r_n$ et $p_n$ est atteinte en un point unique. Posant $r_n = \mathbb{P}(R_n = y_n)$, $p_n = \mathbb{P}(X_n = x_n)$, en majorant convenablement $\mathbb{P}(X_n = x_n; R_n \neq y_n)$, $\mathbb{P}(X_n \neq x_n; R_n = y_n)$ et enfin $\mathbb{P}(X_n + R_n = y; X_n \neq x_n; R_n \neq y_n)$, prouver que pour $n$ grand:

a) $y_{n-1} = x_n + y_n$

b) $r_{n-1} = \mathbb{P}(R_{n-1} = y_{n-1}) = r_n p_n + \Sigma_{x \neq O} \mathbb{P}(R_n = y_n - x)\mathbb{P}(X_n = x_n + x)$.

4°) En déduire que $r_{n-1} \leq r_n p_n + (1 - r_n)(1 - p_n)$ ($n$ grand)

5°) Prouver le

*Théorème de Jessen*: Si les $X_i$ sont indépendantes et si leur série converge, une CNS pour que la loi de leur somme ne soit pas diffuse est que le produit infini des sauts maximum $\Pi_n p_n$ soit strictement positif.

**C.** *Théorème de Wintner.*

Dans cette partie comme dans la précédente $S_n$ converge presque surement et on note $S$ sa limite p.s. On suppose de plus que les lois des $X_i$ sont discrètes et concentrées sur les $A_i$ dénombrables. On note $B$ pour la réunion des $A_i$, qu'on suppose énuméré: $B = (b_m | m \in \mathbb{N})$. Enfin $C$ est l'ensemble des sommes *finies* de termes $\varepsilon_k b_k$ , où les $b_k$ sont pris dans $B$ (avec redoublements possibles) et les $\varepsilon_k$ valent 1 ou -1. Soit $\mathcal{B}_n$ la $\sigma$-algèbre du futur, c'est-à-dire celle engendrée par les $X_k, k > n$.

1°) Soit $E$ un Borélien.

a) Montrer que l'évenement $F = (S \in E + C)$ est un évenement de $\mathcal{B}_n$ (on calculera l'intersection de $F$ par $\cap_{i=1}^{n}(X_i = x_i)$ pour les $x_i$ dans $A_i$).

b) Que vaut $\mathbb{P}(F)$ pour un tel $F$ ?

2°) Montrer que $C$ est dénombrable et que $C + C = C - C = C$ (suivant la convention usuelle, $A + B$ désigne $\{a + b | a \in A, b \in B\}$ ).

3°) Montrer que si la loi de $S$ n'est pas diffuse, il existe un réel $a$ tel que $\mathbb{P}(S \in a + C) = 1$.

4°) S'il existe un Borélien $N$ de mesure de Lebesgue nulle tel que $\mathbb{P}(S \in N) > 0$, montrer qu'il existe un Borélien $M$ de mesure de Lebesgue nulle tel que $\mathbb{P}(S \in M) = 1$.

5°) Prouver le Théorème de Wintner (ou Théorème de pureté) ci-après:

*Théorème*: Soit la loi de $S = \Sigma X_i$, les $X_i$ indépendantes et de lois discrètes. Alors cette loi est ***pure***, c'est-à-dire que:

-Soit la loi est discrète.

-Soit la loi est absolument continue.

-Soit la loi est singulière.

**D.** *Construction de lois singulières.*

On se donne dans cette partie une suite $\{\varepsilon_i\}$ de v.a.r. indépendantes et de même loi: $\mathbb{P}(\varepsilon_i = 1) = \mathbb{P}(\varepsilon_i = -1) = 1/2$, qu'on appellera "signes". On se donne un réel $\xi$ de $]0, 1[$ et on considère la v.a.r.

$$S = \Sigma_{i>0} \varepsilon_i \xi^i. \tag{6}$$

Montrer que la série converge sûrement!

Le but de cette partie est de prouver l'assertion suivante:

(7) Si $1/\xi$ est un nombre de Pisot différent de 2, la loi de $S$ est singulière.

Les deux premières questions établissent des propriétés de $\mathcal{S}$ utiles dans la suite du problème .

1°) a)Prouver que si $\theta$ est un entier algébrique, racine du Polynôme $A$ de $\mathbb{Q}(X)$, alors ses conjugués sont aussi racines de $A$.

En déduire que, pour $m$ entier positif:

b) Si $\theta^m = 2$, sauf si $m = 1$ et $\theta = 2$, $\theta$ ne peut être élément de $\mathcal{S}$.

c) Si $\theta^m = h + 1/2$ où $h$ appartient à $\mathbb{Z}$, $\theta$ ne peut être élément de $\mathcal{S}$.

2 ° ) En utilisant les relations entre coefficients et racines d'un Polynôme, montrer que, si $\theta \in S$, alors il existe deux réels $C$ et $\rho$ avec $0 < \rho < 1$ tels que: pour tout $n$ de $\mathbb{N}$ il existe $k$ de $\mathbb{Z}$ avec $|\theta^n - k| \leq C\rho^n$ .

3 ° ) Vérifier que si $f$ est l'indicatrice de l'intervalle $[a, b]$ avec $-\infty < a < b < \infty$, sa transformée de Fourier $\widehat{f}(t)$ tend vers 0 quand $|t|$ tend vers l'infini. Par un argument de densité, vérifier le *Lemme de Riemann-Lebesgue*: Si f est Lebesgue-intégrable, alors $\lim_{|t|\to\infty} |\widehat{f}(t)| = 0$.

4 ° ) Soient $\theta$ un nombre de Pisot avec $0 < \xi = 1/\theta < 1$, $\theta$ différent de 2, et $\varphi$ la fonction caractéristique de la v.a.r. $S$ définie par (6). Justifier que $\varphi$ s'écrit sous forme d'un produit infini convergent. Montrer que la suite $\gamma_n$ définie par $\gamma_n = |\varphi(\theta^n\pi)|$ a une limite non nulle (on suggère d'étudier séparément

$$A_n = \Pi_{k<n}|\cos(\pi\theta^k)| \text{ et } B = |\Pi_{0\leq k}\cos(\pi\theta^{-k})|).$$

5 ° ) En combinant ces résultats avec les Théorèmes précédents prouver l'assertion (7).

6 ° ) Décrire la loi de $S$ quand $\xi = 1/2$.

**E.** *Etude des supports topologiques.*

Cette partie a pour but d'étudier le support topologique des Probabilités introduites dans la partie **D** dont on reprend les notations. Soit $S_n$ la v.a.r. somme des $n$ premiers termes: $S_n = \Sigma_{0<i\leq n}\varepsilon_i\xi^i$ .

La loi de $S_n$ accorde la masse $2^{-n}$ à chacun des nombres $\Sigma_{0<i\leq n} \pm \xi^i$ (qui ne sont pas nécéssairement distincts). On note $A_n$ l'ensemble de ces valeurs possibles. Dans ce qui suit, on se donne une suite de v.a.r. auxiliaires $\{U_n\}$, indépendante de la suite $\{\varepsilon_i\}$. On suppose $U_n$ de loi uniforme sur l'intervalle $J_n$ centré en 0 et de longueur $2\xi^{n+1}/(1-\xi)$. On définit les v.a.r. $T_n = S_n + U_n$. On note $C_n$ l'ensemble $C_n = \cup(a + J_n | a \in A_n)$.

**E.1** *Le cas* $\xi < 1/2$.

Dans ce paragraphe, $\xi$ est un réel tel que $0 < \xi < 1/2$.

1 ° ) Soit $a$ et $a'$ deux points distincts de $A_n$. Montrer que

$$|a' - a| \geq 2\xi^n.$$

En déduire que $C_n$ est composé de $2^n$ intervalles disjoints, que $C_{n+1} \subset C_n$ et que $T_n$ a une densité constante sur $C_n$ et nulle en dehors.

2 ° ) Montrer que $T_n$ tend en loi vers $S$, et que $\mathbb{P}(S \in C_n) = 1$.

3 ° ) Soit $C_\xi = \cap_n C_n$. Montrer que $C_\xi$ est un ensemble fermé, de mesure de Lebesgue nulle et que $\mathbb{P}(S \in C_\xi) = 1$. Montrer que $C_\xi$ est un ensemble *parfait*, c'est-à-dire que tout point $\alpha$ de $C_\xi$ est limite d'une suite $\{\alpha_n\}$ telle que: a) $\alpha_n \in C_\xi$; b) $\alpha_n \neq \alpha$ .

4 ° ) Construire la suite $\{F_n\}$ des fonctions de répartition des variables $T_n$ et vérifier qu'elle converge uniformément.

5 ° ) Conclure des quatre questions précédentes une preuve directe de ce que, quand $0 < \xi < 1/2$, la construction (6) donne une loi singulière dont le support topologique est de mesure de Lebesgue nulle.

**E.2** *Le cas* $1/2 < \xi < 1$.

Soit $J_\xi$ l'intervalle $[-\xi/(1-\xi), \xi/(1-\xi)]$. On se propose de prouver que le support topologique de la loi de $S$ est $J_\xi$. Soit $x$ vérifiant $0 < x < \xi/(1-\xi)$.

6°) Montrer qu'il existe un entier $\ell_1$ tel que

$$0 \leq \Sigma_{0<i<\ell_1} \xi^i < x \leq \Sigma_{0<i\leq \ell_1} \xi^i < \xi/(1-\xi).$$

7°) Construire par récurrence une suite croissante d'entiers distincts $\ell_k$ et un choix de signes $e_i$ tels que si $w_k = \Sigma_{0<i\leq \ell_k} e_i \xi^i$ on ait simultanément

a) $|x - w_k| \leq \xi^{\ell_k}$.

b) $\forall t \geq 0,\ w_{2t} \leq x \leq w_{2t+1}$

c) $\mathbb{P}(w_k - \xi^{\ell_k+1}/(1-\xi) \leq S \leq w_k + \xi^{\ell_k+1}/(1-\xi)) \geq 2^{-\ell_k}$

(On notera que les $w_k$ et les $e_i$, non aléatoires, sont fonction de $x$).

8°) En déduire que la loi de $S$ donne une Probabilité strictement positive à tout ouvert (non vide) de $J_\xi$.

9°) Le *nombre d'or* est le nombre $\theta_o = (1+\sqrt{5})/2$. Soit $\xi_o$ son inverse. Montrer que la loi de la variable S définie par la formule (6) où l'on porte $\xi = \xi_o$ a les propriétés suivantes:

- Le support topologique est un intervalle (d'intérieur non vide).
- Cependant il existe un Borélien $N$ de mesure de Lebesgue nulle tel que $\mathbb{P}(S \in N) = 1$.
- Cette loi est diffuse.
- La fonction caractéristique $\varphi_S$ ne tend pas vers 0 à l'infini.