PC 1(Modèles discrets)

EXERCICE 1 -limsup d'ensembles

Soit Ω un espace de probabilité, et $(A_n)_{n\geq 1}$ une suite d'événements, on rappelle la notation

$$\limsup_{n\to+\infty} A_n = \bigcap_{p\geq 1}\Big(\bigcup_{n\geq p} A_n\Big).$$

On prend $\Omega=\mathbb{R}$, et on pose

$$A_n=[-1/n;3+1/n]\,,\qquad B_n=[-2-(-1)^n;2+(-1)^n]\,,$$

Déterminer les lim sup des suites $(A_n),(B_n)$.

EXERCICE 2 -Application de Borel-Cantelli

On considère une urne qui à l'instant $t=1$ contient une boule rouge et une boule bleue. Pour chaque $t\geq 1$:

— On tire uniformément une boule au hasard dans l'urne ;

— On remet cette boule dans l'urne et on rajoute une boule bleue.

Pour $t\geq 1$ on note R_t l'événement {La t-ème boule tirée est rouge} et $\mathcal{N}_t$ le nombre de boules rouges tirées entre le 1er et le t-ème tirage.

1. Calculer $\mathbb{P}(R_t)$ et $\mathbb{E}(\mathcal{N}_t)$.
2. Décrire en Français l'événement "$\limsup_t R_t$". Que donne le Lemme de Borel-Cantelli ?
3. Mêmes questions si dans l'énoncé on remplace "on rajoute une boule bleue" par "on rajoute t boules bleues".

EXERCICE 3 -Espérance conditionnelle

Soit X_1,X_2 des variables aléatoires indépendantes de loi de Poisson de paramètre respectif $\theta_1>0$ et $\theta_2>0$.

1. Calculer la loi $\mathbb{P}(X_1+X_2=k)$ pour tout $k\geq 0$; quelle est la loi de X_1+X_2 ?
2. Pour $0\leq \ell\leq k$, calculer $\mathbb{P}(X_1=\ell \mid X_1+X_2=k)$.
3. Calculer $\mathbb{E}(X_1\mid X_1+X_2)$.

EXERCICE 4 -Codage avec masque jetable

Le *masque jetable* est un protocole probabiliste de cryptographie inventé au début du XXè siècle, le chiffrement est théoriquement impossible à casser.

Le principe est le suivant : imaginons que Alice cherche à envoyer de façon codée à Bob un mot de n lettres $w_1w_2\dots w_n$ sur l'alphabet $\{A,B,\dots,Z\}$ (identifié à $\{1,2,\dots,25,26\}$). Alice tire au sort un masque, c'est-à-dire un n-uplet $X_1,X_2,\dots,X_n$ de variables aléatoires indépendantes uniformes sur $\{1,2,\dots,25,26\}$. Alice communique par un canal sécurisé le masque à Bob, et par un autre canal le message formé des lettres $(Z_i)_{1\leq i\leq n}$ où $Z_i=w_i+X_i$ (mod 26). Par exemple :

Message	$(w_i)_i$	$C(3)$	$O(15)$	$U(21)$	$C(3)$	$O(15)$	$U(21)$
Masque	$(X_i)_i$	11	4	20	4	19	7
Message codé	$(Z_i)_i$	$N(14)$	$S(19)$	$O(15)$	$G(7)$	$L(12)$	$B(2)$

1. Comment déchiffrer le message ?
2. Démontrer que le message codé ne contient aucune information : les variables Z_i sont également uniformes et indépendantes sur $\{1,2,\dots,25,26\}$.
3. Pourquoi est-ce que ce protocole est toutefois inutilisable en pratique ?

EXERCICE 5 -Séquence de pile/face

On lance une infinité de fois une pièce équilibrée. Pour $n \geq 1$, on note M_n la longueur de la plus longue séquence de "piles" consécutifs durant les n premiers lancers. Par exemple :

n	1	2	3	4	5	6	7	8	9	...
tirage	F	P	P	F	P	P	P	F	P	...
M_n	0	1	2	2	2	2	3	3	3	...

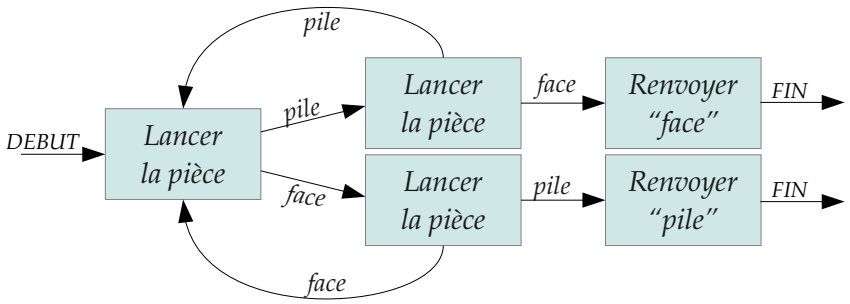
Le but de cet exercice est d'étudier le comportement asymptotique de la suite (M_n).

1. Démontrer que pour tout $k \leq n$ on a $\mathbb{P}(M_n \geq k) \leq (n-k+1)(1/2)^k$.
2. Démontrer que pour tout $k \leq n$ on a $\mathbb{P}(M_n < k) \leq \left(1-(1/2)^k\right)^{\lfloor n/k \rfloor}$.
3. En déduire le comportement asymptotique de (M_n) : pour tout $\varepsilon > 0$

$$\mathbb{P}\left(1-\varepsilon \leq \frac{M_n}{\log_2(n)} \leq 1+\varepsilon\right) \overset{n\to+\infty}{\to} 1.$$

EXERCICE 6 -Détruquer une pièce : l'algorithme de von Neumann

On dispose d'une pièce truquée qui renvoie "pile" avec une probabilité p et on souhaite s'en servir pour générer un pile ou face équilibré. John von Neumann [1] a imaginé l'algorithme suivant :



On note $T \in \mathbb{N}$ la variable aléatoire donnée par le nombre de lancers nécessaires pour que l'algorithme se termine, et $R \in \{\text{"pile"}, \text{"face"}\}$ le résultat de l'algorithme.

1. Que valent T et R si on obtient comme premiers tirages $PPPPFFPPPFFP$?
2. Pour tout $k \geq 1$, calculer $\mathbb{P}(T = k)$. En déduire que l'algorithme se termine presque-sûrement : $\mathbb{P}(T < +\infty) = 1$.
3. Démontrer que l'algorithme renvoie bien "pile" ou "face" avec même probabilité, c'est-à-dire que $\mathbb{P}(R = \text{"Pile"}) = 1/2$.
4. Démontrer que $\mathbb{E}[T] = \frac{1}{p(1-p)}$.
5. (Bonus) Comment améliorer l'algorithme de von Neumann pour diminuer $\mathbb{E}[T]$?

1. J.von Neumann. Various techniques used in connection with random digits. *Appl. Math Ser*, 12 (1951) p.36-38.