Tutorat 1

Frédéric Chevy – chevy@lkb.ens.fr

Remarque liminaire : Deux sujets sont proposés. À chaque groupe de choisir celui qui sera traité au cours de la séance de tutorat. Le sujet 2 est un travail collectif et une seule copie par groupe sera suffisante.

Sujet 1 : Modèle d'Ehrenfest

1 Notion de fonction génératrice

Soit X une variable aléatoire à valeurs sur $\mathbb{N}$ dont on note P_n la distribution de probabilité.

1. Montrer que la série entière $\chi(s) = \sum_n P(n) s^n$ possède un rayon de convergence $R \geq 1$. Que vaut $\chi(1)$? Proposer deux exemples de distributions P_n pour lesquelles $R = 1$ et $R = \infty$.
2. On note $E(X)$ l'espérance de la variable aléatoire X. Montrer que si $E(X)$ est définie, alors χ possède une dérivée à gauche en 1 et $E(X) = \chi'(1)$. Montrer que s'ils existent, les différents moments de X sont reliés aux dérivées de χ en 1. Justifier le nom de "fonction génératrice" donné à χ.
3. Soient deux variables aléatoires indépendantes X_1 et X_2 à valeurs sur $\mathbb{N}$ et de fonction génératrice respectives $\chi_{i=1,2}$. On note χ_{1+2} la fonction génératrice de $X_1 + X_2$. Montrer que pour $s < 1$:

$$\chi_{1+2}(s) = \chi_1(s)\chi_2(s).$$

2 Modèle d'Ehrenfest

On considère N boules réparties deux boîtes A et B. À l'instant initial on suppose qu'il y a un probabilité $P_0(n)$ d'avoir n boules dans la boîte A.

On choisit ensuite une boule au hasard parmi les N et on la change de boîte. On répète cette opération q fois et on note $P_q(n)$ la probabilité d'avoir n boules dans la boîte A à cette étape.

1. Quel processus physique ce modèle peut-il décrire ?
2. Montrer que l'on a la relation de récurrence :

$$P_{q+1}(n) = \frac{n+1}{N} P_q(n+1) + \left(1 - \frac{n-1}{N}\right) P_q(n-1).$$

3. Vérifier explicitement que l'on a $\sum_{n=0}^{N} P_q(n) = 1$.

4. Soit $\chi_q(s)$ la fonction génératrice de la distribution P_q. Montrer que l'on a :

$$\chi_{q+1}(s) = s\chi_q(s) + \frac{1-s^2}{N}\chi_q'(s)$$

5. À quelle condition a-t-on $\chi_{q+1} = \chi_q$? Montrer que ceci correspond à une distribution binomiale équirépartie. Calculer en particulier le nombre moyen $\langle n \rangle$ de boules dans la boîte dans cette distribution. Commentaire.
6. Soit $\overrightarrow{\Delta}_q$ le vecteur constitué des dérivées successives χ_q en 1, soit :

$$\overrightarrow{\Delta}_q = \begin{pmatrix} \chi_q(s=1) \\ \chi_q'(s=1) \\ \chi_q''(s=1) \\ \vdots \\ \chi_q^{(N)}(s=1) \end{pmatrix}.$$

En notant Δ_q^k la $k^{\text{ème}}$ coordonnée de $\overrightarrow{\Delta}_q$, montrer que :

$$\Delta_{q+1}^k = \left(1 - \frac{2k}{N}\right)\Delta_q^k + k\left(1 - \frac{k-1}{N}\right)\Delta_q^{k-1}.$$

7. Résoudre explicitement cette relation pour $k = 1$. En déduire que $\langle n \rangle_q$, nombre moyen de boules dans la boîte A, tend vers une limite que l'on calculera. Commenter.
8. En déduire que la suite des $\overrightarrow{\Delta}_q$ est donnée par une relation de récurrence de la forme :

$$\overrightarrow{\Delta}_{q+1} = M \cdot \overrightarrow{\Delta}_q,$$

où M est une matrice trigonale dont on précisera les éléments diagonaux.
9. Montrer que M est diagonale. Si on choisit une base $\overrightarrow{X}_p$ de vecteurs propres de valeurs propres associées λ_p, montrer que l'on a :

$$\overrightarrow{\Delta}_q = \sum_p \delta_p \lambda_p^q \overrightarrow{X}_p,$$

où les δ^p sont des réels dépendant de P_0 que l'on ne cherchera pas à calculer explicitement.

10. En déduire que pour les grands q, on a :

$$\chi_q(s) \sim \frac{(1+s)^N}{2^N} + \epsilon(-1)^q \frac{(1-s)^N}{2^N},$$

avec $|\epsilon| < 1$.

11. Commenter.

Sujet 2 : Éléments de cryptographie

Lire l'article ci-joint et décrypter le message suivant :

xviYzrmh SfZTgrviD, nvnv D roh xPnQgvmY kZTnO oRh kMID ZmORmD
vY ovD nrRIc wvuOmOh, QvfBvmg tZTwRi fmR QzTY OmFRxrDv wZAh
ovfTh ornrYvD. QPIi yrRm wRh QZTrDORAD, ov SfziYOvi ozgOA D
ZiTvYR Zf DlnnvY wR oz WPmgZHmv hZrmgR HRmRerRev xlnWR ZI
YvWQh F ZNRoziw. NzoaZx hrYfR oz QRADOlm BZIjIvT ifR ARIBR hZr-
mYR tvAReveOvBv, ZIKlfTF JIO iIv glfimvGPig "RAgiR MR SIzTgORT
ozgOA vY Mv uzINPITH hzrmY WZTVRZI... wZAh VvD iIRh hRTTRvh
RAgiv ov FlWv FI eZM wv HiZxR vg ov wlnR wf kzmYsRPA". WZOh zI-
qlITw sfr, hIT ov evihzmg Dfw wR oZ WPAgzHAv, o RVPMR AlTnzoR
hIQvTrvIiv, MRD OAhgrgfYh wR TvVsviVJR Rg oRD GlbRTD w Rgf-
Frzmgh, ovh MZylTzYPOiRh JrDYlTrjfvD Fv kZhYRfT vg FR VfiOR, o
ImreRTDOgv xvmhORT, KfDgOGORmY QRIY RYTv SfR o Pm RgvmwR
ov jIzTgORT ozYrm qfDSI zIc tlyRMrmD.

RiOx JZazm, M rmevAgrPm FR kzTrD.