UNIVERSITÉ DE RENNES 1

Master de mathématiques

Probabilités et statistique pour la théorie de l'information

Travaux dirigés

UFR Mathématiques

Rennes

Septembre 2019

La notation utilisée dans ce recueil d'exercices est celle introduite dans le cours dont les notes sont accessibles à l'URL :

http://perso.univ-rennes1.fr/dimitri.petritis/enseignement/ptin/ptin.pdf

Ces notes sont mises à jour au fur et mesure de la progression dans le semestre.

Des informations utiles relatives à l'organisation du cours sont disponibles au journal de bord :

http://perso.univ-rennes1.fr/dimitri.petritis/enseignement/jdb/jdb-ptin.pdf

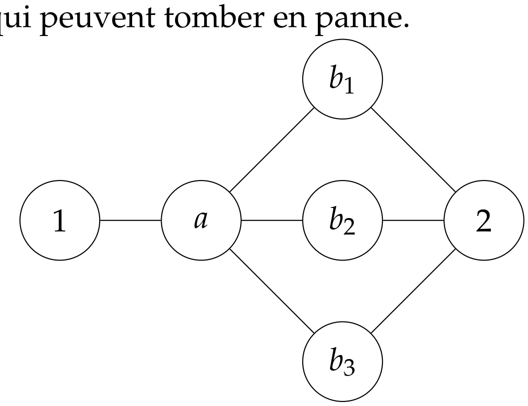
Les quatre types de dénombrement

1. On rappelle les quatre types de dénombrement :
   - n tirages discernables à choisir parmi M possibilités avec remise ($n > 0, M > 0$) :
   $$\Omega_1 = \{\omega = (\omega_1, \dots, \omega_n); \omega_i \in \{1, \dots, M\}, i = 1, \dots, n\}.$$
   $\text{card}\Omega_1 = M^n$.
   - n tirages discernables à choisir parmi M possibilités sans remise ($0 < n \leq M$) :
   $$\Omega_2 = \{\omega = (\omega_1, \dots, \omega_n); \omega_i \in \{1, \dots, M\}, i = 1, \dots, n; \omega_i \neq \omega_j, \text{pour } i \neq j\}.$$
   $\text{card}\Omega_2 = \frac{M!}{(M-n)!}$.
   - n tirages indiscernables à choisir parmi M possibilités sans remise ($0 < n \leq M$) :
   $$\Omega_3 = \{\omega = [\omega_1, \dots, \omega_n]; \omega_i \in \{1, \dots, M\}, i = 1, \dots, n; \omega_i \neq \omega_j, \text{pour } i \neq j\}.$$
   $\text{card}\Omega_3 = \frac{M!}{n!(M-n)!} = C_M^n$.
   - n tirages indiscernables à choisir parmi M possibilités avec remise ($n > 0, M > 0$) :
   $$\Omega_4 = \{\omega = [\omega_1, \dots, \omega_n]; \omega_i \in \{1, \dots, M\}, i = 1, \dots, n\}.$$
   $\text{card}\Omega_4 = C_{n+M-1}^n$.

   Pour chacun de ces quatres types,
   (a) démontrer les formules des cardinaux,
   (b) donner un exemple concret d'application.

Événements et ensembles

2. Sous quelles conditions les événements A et B satisfont l'égalité $A = A \cup B$? L'égalité $A = A \cap B$?
3. Soit $(A_i)_{i \in I}$ une collection d'ensembles. Déterminer $(\cup_{i \in I} A_i)^c$ et $(\cap_{i \in I} A_i)^c$.
4. La figure suivante décrit un circuit électrique entre les points 1 et 2 comportant les fusibles a, b_1, b_2 et b_3 qui peuvent tomber en panne.



   Noter A (resp. B_i) les événements : « le fusible a (resp. le fusible b_i) est en panne », pour $i = 1, 2, 3$ et C l'événement « le courant passe de 1 à 2 ». Déterminer C^c et C en termes des événements A, B_1, B_2 et B_3.

5. Une cible est constituée de 10 disques concentriques de rayons $r_k, k = 1, \ldots, 10$. L'événement A_k signifie « le projectile a touché la cible à l'intérieur du disque de rayon r_k », pour $k = 1, \ldots, 10$. Quelle est la signification des événements B et C définis par
$$B = \cup_{k=1}^{5} A_k \text{ et } C = \cap_{k=1}^{10} A_k?$$
6. 20 chevaux sont au départ d'une course. Trouver le nombre de tiercés, de quartés, de quintés dans l'ordre et dans le désordre.

Probabilités élémentaires

7. Un ouvrage de 4 volumes est placé dans un ordre aléatoire sur le rayonnage d'une bibliothèque. Quelle est la probabilité que les 4 volumes soient placés dans l'ordre (ascendant ou descendant) ? *Rép. : 1/12.*
8. Toutes les faces d'un cube en bois sont peintes. Ensuite le cube est découpé (selon des plans parallèles à ses faces) en 1000 cubes identiques. Un petit cube est choisi au hasard ; quelle est la probabilité qu'il comporte exactement 2 faces peintes ? *Rép. : 0,096.*
9. Dix livres sont placés dans un ordre aléatoire sur un rayonnage. Quelle est la probabilité que trois livres spécifiques se retrouvent côte-à-côte ? *Rép. : 1/15.*
10. Un sac contient 5 bâtonnets de longueurs 1, 3, 5, 7 et 9. On en extrait 3. Quelle est la probabilité que l'on puisse construire un triangle ayant ces bâtonnets comme côtés ? *Rappel : La longueur d'un côté d'un triangle ne peut pas excéder la somme des longueurs des autres côtés.*
11. Supposons qu'un entier entre 1 et 1000 est choisi au hasard. Quelle est la probabilité que les 2 derniers digits décimaux de son cube soient 1 ? *Suggestion : Il n'est pas nécessaire de consulter une table des cubes des tous les entiers entre 1 et 1000. Rép. : 0,01.*
12. Quelle est la probabilité qu'au moins deux étudiants suivant un cours auquel N étudiants sont inscrits ($N \geq 2$) aient leur anniversaire le même jour ? On néglige les années bissextiles et on suppose que tous les jours de l'année sont équiprobables en tant que jour de naissance.
13. Une tombola comporte M tickets dont n (avec $M \geq 2n$) sont gagnants. Une personne achète n tickets. Quelle est la probabilité pour qu'elle gagne au moins un lot ?
14. On gagne (au premier rang) une loterie si l'on coche 6 bons numéros parmi les 49 que comporte une grille. Quelle est la probabilité de gagner cette loterie au premier rang ?

Algèbres, tribus, espaces probabilisés

15. Soit $\mathcal{A}$ une algèbre sur Ω (fini) et soient A, B et C trois événements quelconques de $\mathcal{A}$. Exprimer les événements suivants. Parmi A, B, C
    (a) A seul se produit,

(b) A et B se produisent et C ne se produit pas,
(c) les trois événements se produisent,
(d) l'un au moins des événements se produit,
(e) au moins deux des événements se produisent,
(f) un seul événement se produit,
(g) aucun des événements ne se produit.

16. Soit $(\mathcal{A}_i)_{i\in I}$ une famille d'algèbres sur Ω. Montrer que $\cap_{i\in I}\mathcal{A}_i$ est une algèbre sur Ω. En déduire que si $\mathcal{C} \subseteq \mathcal{P}(\Omega)$ est une famille arbitraire de parties de Ω, il existe une algèbre minimale qui contient $\mathcal{C}$; on la note $\alpha(\mathcal{C})$ et on l'appelle **algèbre engendrée** par $\mathcal{C}$. La famille $\mathcal{C}$ est alors appelée **famille génératrice** de l'algèbre.
17. Soit $\mathcal{A}$ une algèbre d'événements sur un espace fini Ω. Montrer qu'il existe une unique partition $\mathcal{D}$ de Ω génératrice de $\mathcal{A}$, i.e. $\mathcal{A} = \alpha(\mathcal{D})$.
18. Soit $(\mathcal{F}_i)_{i\in I}$ une famille de tribus sur Ω. Montrer que $\cap_{i\in I}\mathcal{F}_i$ est une tribu [1] sur Ω. En déduire que si $\mathcal{G} \subseteq \mathcal{P}(\Omega)$ est une famille arbitraire (non-vide) de parties de Ω, il existe une tribu minimale qui contient $\mathcal{G}$; on la note $\sigma(\mathcal{G})$ et on l'appelle **tribu engendrée** par $\mathcal{G}$. La famille $\mathcal{G}$ est appelée **famille génératrice** de la tribu.

Propriétés des probabilités discrètes

19. Le but de cet exercice est de onner une interprétation géométrique de l'ensemble de vecteurs de probabilités $\mathcal{M}_1(\Omega, \mathcal{F})$ sur un univers fini Ω et $\mathcal{F}$ une tribu sur Ω.
   (a) Rappeler la définition d'un ensemble convexe.
   (b) Montrer que $\mathcal{M}_1(\Omega, \mathcal{F})$ est convexe.
   (c) Rappeler la définition d'un point extrémal d'un ensemble convexe et montrer que $\mathbb{P} \in \mathcal{M}_1(\Omega, \mathcal{F})$ est extrémal si, et seulement si, pour tout $F \in \mathcal{F}$, on a $\mathbb{P}(F) \in \{0, 1\}$. On note par $\partial_e\mathcal{M}_1(\Omega, \mathcal{F})$ l'ensemble des probabilités extrémales.
   (d) Conclure que $E = \{\varepsilon_\omega : \omega \in \Omega\}$ est un ensemble composé de probabilités qui sont toutes extrémales.
   (e) Donner un exemple où $E \neq \partial_e\mathcal{M}_1(\Omega, \mathcal{F})$.
   (f) Montrer que si $\mathcal{F}$ est dénombrablement engendrée et contient les singletons, alors $E = \partial_e\mathcal{M}_1(\Omega, \mathcal{F})$.
   (g) Donner la structure géométrique de $\mathcal{M}_1(\Omega, \mathcal{F})$ dans le cas où $|\Omega| < \infty$ et $\mathcal{F} = \mathcal{P}(\Omega)$. On peut utiliser sans démonstration les deux théorèmes suivants :
   Théorème A : *(Carathéodory) Tout point dans l'enveloppe convexe* $\mathrm{co}(A)$ *d'un ensemble* $A \subset \mathbb{R}^d$ *peut être exprimé comme combinaison convexe d'au plus* $d+1$ *points de* A.
   Théorème B : *(Krein-Milman) Si X est de dimension finie, toute partie convexe compacte non-vide de X est la combinaison convexe de ses points extrémaux.*
   (h) Lorsque $\mathrm{card}\Omega = 3$, dessiner la partie de $\mathbb{R}^2$ qui est isomorphe à $\mathcal{M}_1(\Omega, \mathcal{P}(\Omega))$ et y placer le point qui correspond au vecteur de probabilité $\mathbf{p} = (\frac{4}{19}, \frac{12}{19}, \frac{3}{19})$.

1. *Attention :* La réunion $\cup_{i\in I}\mathcal{F}_i$ n'est pas, en général, une tribu. Même dans le cas où $(\mathcal{F}_i)_{i\in\mathbb{N}}$ est une filtration dénombrable (i.e. une suite des tribus strictement emboîtées $\mathcal{F}_i \subset \mathcal{F}_{i+1}$, pour $i \in \mathbb{N}$), la réunion $\cup_{i\in\mathbb{N}}\mathcal{F}_i$ n'est **jamais** une tribu ; cf. [**?**]. La réunion engendre cependant une tribu par le procédé décrit dans cet exercice, notée $\vee_{i\in\mathbb{N}}\mathcal{F}_i$.

20. Supposons que Ω est dénombrable (fini ou infini) et qu'il existe une application $\rho : \Omega \to [0,1]$ telle que $\sum_{\omega\in\Omega} \rho(\omega) = 1$. Montrer que ρ définit une mesure de probabilité sur $(\Omega, \mathcal{F})$ définie par

$$\mathcal{F} \ni A \mapsto \mathbb{P}(A) = \sum_{\omega \in A} \rho(\omega) \in [0,1].$$

Suggestion : la seule chose à démontrer est la propriété d'additivité dénombrable disjointe.

21. Soit $\Omega = \{0,1\}^n$ l'espace des épreuves de n lancers d'une pièce, muni de sa tribu exhaustive $\mathcal{F} = \mathcal{P}(\Omega)$. L'espace des événements est probabilisé à l'aide du vecteur de probabilité uniforme ρ, chargeant chaque $\omega \in \Omega$ par $\rho(\omega) = \frac{1}{2^n}$. Pour chaque $k = 1, \ldots, n$, on définit l'application

$$\Omega \ni \omega = (\omega_1, \ldots, \omega_k, \ldots, \omega_n) \mapsto T_k\omega := (\omega_1, \ldots, 1-\omega_k, \ldots, \omega_n) \in \Omega.$$

L'application T_k est appelée « k^{th} bit-flip » (renversement du k^{e} bit). Montrer que pour tout $A \in \mathcal{F}$, on a l'invariance $\mathbb{P}(T_k A) = \mathbb{P}(A)$.

Variables aléatoires, fonctions de répartition

22. On lance une pièce lestée (donnant face avec probabilité $p \in [0,1]$) n fois.
    (a) Décrire très précisément l'espace $(\Omega, \mathcal{F}, \mathbb{P})$ qui décrit cette expérience.
    (b) Déterminer la densité discrète ρ de $\mathbb{P}$.
    (c) On s'intéresse au nombre de fois que la pièce tombe sur face. Décrire très précisément la variable aléatoire X qui décrit cette grandeur et déterminer sa loi $\mathbb{P}_X$ et la densité discrète ρ_X correspondante.
    (d) Vérifier que la fonction de répartition vérifie $F_X(x) = 1$ pour $x \geq n$.
23. Montrer les propriétés de la fonction de répartition F_X d'une variable aléatoire réelle X (à savoir qu'elle est croissante, continue à droite et vérifie $\lim_{x\to-\infty} F_X(x) = 0$ et $\lim_{x\to+\infty} F_X(x) = 1$).
24. Montrer que si F est une fonction de répartition, elle a *au plus* une infinité dénombrable de discontinuités. *Suggestion : étant donné que F est continue à droite, un point x est une discontinuité s'il est une discontinuité gauche, i.e. si $DF(x) = F(x) - F(x-) > 0$. Écrire alors $\{x \in \mathbb{R} : DF(x) > 0\}$ comme une réunion dénombrable de parties de $\mathbb{R}$ et ... réfléchir un peu sur le cardinal de chacun de ces ensembles.*
25. Soient $(\Omega, \mathcal{F}, \mathbb{P}) = ([0,1], \mathcal{B}([0,1]), \lambda)$ et $X : \Omega \to \mathbb{R}$ une application continue. Suppposons que l'espace image $\mathbb{R}$ est muni de sa tribu borélienne. Montrer que X est une variable aléatoire.
26. Soit $F : \mathbb{R} \to [0,1]$ une fonction croissante, continue à droite, vérifiant $\lim_{x\to-\infty} F(x) = 0$ et $\lim_{x\to+\infty} F(x) = 1$. Montrer qu'il existe un espace de probabilité $(\Omega, \mathcal{F}, \mathbb{P})$ et une variable aléatoire réelle X sur cet espace ayant F comme fonction de répartition.
27. Soit X une variable aléatoire réelle dont la loi admet une densité ρ_X (par rapport à la mesure de Lebesgue) sur $\mathbb{R}$. Montrer que sa fonction de répartition F_X s'exprime

comme l'intégrale

$$F_X(x) = \int_{]-\infty,x]} \rho_X(t)\lambda(dt).$$

Noter que si F_X a une densité comme ci-dessus, alors F_X est continue et différentiable avec $F_X' = \rho_X$.

Probabilité conditionelle

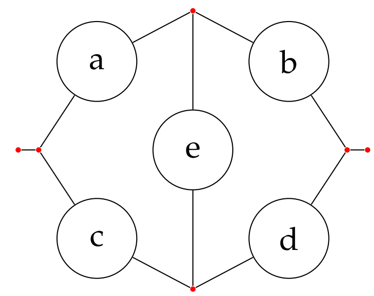
Dans tout ce paragraphe, on travaille sur un espace probabilité $(\Omega, \mathcal{A}, \mathbb{P})$. Tous les événements utilisés, $A, B, (A_k), \ldots$, appartiennent à $\mathcal{A}$.

28. Montrer que le formules suivantes :

$$\mathbb{P}(B|A) + \mathbb{P}(B|A^c) = 1 \text{ et } \mathbb{P}(B|A) + \mathbb{P}(B^c|A^c) = 1$$

sont fausses.
29. Pour une famille d'événements $(A_k)_{k=1,\ldots,n}$ indépendante, noter $p_k = \mathbb{P}(A_k)$. Calculer la probabilité de l'événement « aucun des (A_k) ne se réalise ».
30. Soient A et B deux événements indépendants, avec $p = \mathbb{P}(A)$ et $q = \mathbb{P}(B)$. Calculer les probabilités pour que
    (a) exactement k,
    (b) au moins k,
    (c) au plus k,

    des événements A et B se réalisent pour $k = 0, 1, 2$.
31. Exprimer $\mathbb{P}(\cup_{k=1}^n A_k)$ lorsque les A_k sont indépendants.
32. Un lot de 100 objets manufacturés subit un contrôle par échantillonnage : un échantillon de 5 objets est examiné et s'il contient un article défectueux, tout le lot est rejeté. Quelle est la probabilité qu'un lot soit rejeté s'il contient 5% d'objets défectueux ?
33. Une personne a oublié le dernier digit du numéro de téléphone de son correspondant ; elle compose donc au hasard. Quelle est la probabilité p qu'elle soit obligée de composer moins de 3 fois (≤ 3) ? Que devient cette probabilité, si la personne se souvient que le dernier digit est impair ?
34. Une personne écrit n lettres différentes, chacune destinée a un destinataire spécifique. Elle les a scellées et posées bien rangées en pile sur son bureau afin d'écrire le lendemain les adresses sur les enveloppes. Un plaisantin est passé par là, il a renversée la pile par erreur et il a remis les enveloppes sur le bureau mais dans un ordre aléatoire par rapport à l'ordre correct. Ignorant ce fait, la personne qui a rédigé les lettres a inscrit le lendemain les adresses. Quelle est la probabilité qu'une lettre parvienne à la personne à laquelle elle était destinée ?
35. Le circuit électrique suivant comporte 5 interrupteurs, notés a à e ; chacun d'eux peut être fermé (laisse le courant passer) avec probabilité p ou ouvert (coupe le courant) avec probabilité $q = 1 - p$.



(a) Quelle est la probabilité pour que le courant passe de gauche à droite ?

(b) Sachant que le courant passe de gauche à droite, quelle est la probabilité pour que l'interrupteur e soit fermé ?

Variables aléatoires ; probabilités conjointes

36. On lance une pièce honnête et on désigne par X_1 le résultat obtenu. Si $X_1 =$ face, on lance une pièce honnête sinon on lance une pièce lesté qui donne face avec probabilité $2/3$; on note X_2 le résultat du deuxième lancer. Si on a obtenu 2 fois face lors des 2 premiers lancers, on lance un dé honnête, sinon on lance un dé lesté qui donne 6 avec probabilité $1/2$ et les autres faces équiprobables.

(a) Calculer explicitement les vecteurs de probabilité ρ_1, ρ_{2,x_1} et $\rho_{3,(x_1,x_2)}$.

(b) Déterminer la probabilité conjointe $\mathbb{P}(X_1 = x_1, X_2 = x_2, X_3 = x_3)$ pour $x_1, x_2 \in \{0,1\}$ et $x_3 \in \{1,\ldots,6\}$.

(c) Calculer les probabilités marginales $\mathbb{P}(X_1 = x_1)$ et $\mathbb{P}(X_1 = x_1, X_2 = x_2)$.

Indépendance

37. Une urne contient n boules noires et r boules rouges et on considère l'espace $\Omega = \{1,\ldots,n+r\}^2$ (qui peut décrire toutes les expériences d'extraction de deux boules avec ou sans remise). On note

$$A = \{\text{la première boule est rouge}\} = \{\omega \in \Omega : \omega_1 \in \{1,\ldots,r\}\}$$

et

$$B = \{\text{la seconde boule est rouge}\} = \{\omega \in \Omega : \omega_2 \in \{1,\ldots,r\}\}.$$

(a) On en extrait une boule, on la remet dans l'urne et on en extrait une seconde ; on note $\mathbb{P}$ la probabilité uniforme sur Ω. Les événements A et B sont-ils indépendants (par rapport à $\mathbb{P}$) ?

(b) On extrait une première boule et sans la remettre dans l'urne, on en extrait une seconde. On note $\mathbb{P}'$ la probabilité uniforme sur

$$\Omega' = \{\omega = (\omega_1, \omega_2), \omega_i \in \{1,\ldots,n+r\}, \omega_1 \neq \omega_2\} \subset \Omega.$$

La probabilité $\mathbb{P}'$ peut être étendue en une probabilité, aussi notée $\mathbb{P}'$, sur Ω chargeant avec le masse 0 les éléments de $\Omega \setminus \Omega'$. Les événements A et B sont-ils indépendants (par rapport à $\mathbb{P}'$) ?

38. On jette un dé deux fois de suite et on note $\Omega = \{1, \ldots, 6\}^2$ l'espace des épreuves correspondant. On munit la tribu exhaustive de cet espace de la probabilité uniforme et on considère les événements $A = \{\text{la somme est } 7\}$ et $B = \{\text{le premier dé tombe sur } 6\}$.
    (a) Montrer que A et B sont indépendants (sous la probabilité uniforme).
    (b) Montrer que A est déterminé de B de manière causale.

Lois, espérance, variance

39. Soit α la variable aléatoire définie sur $(\Omega, \mathcal{F}, \mathbb{P})$ qui prend des valeurs dans $\mathbb{X} = \{0, \pi/2, \pi\}$ avec probabilité uniforme. On note $X = \sin \alpha$ et $Y = \cos \alpha$. Calculer
    (a) $\mathbb{E}X$,
    (b) $\mathbb{E}Y$,
    (c) $\mathsf{Cov}(X, Y)$,
    (d) $\mathbb{P}(X = 1, Y = 1)$.

    Quelle est votre conclusion ?
40. Soient $(\xi_k)_{k=1,\ldots,n}$ des variables aléatoires indépendantes sur $(\Omega, \mathcal{F}, \mathbb{P})$ prenant un nombre fini de valeurs réelles. Calculer la loi de $X = \max \xi_k, k = 1, \ldots, n$ et de $Y = \min\{\xi_k, k = 1, \ldots, n\}$.
41. Soient $(\xi_k)_{k=1,\ldots,n}$ des variables aléatoires indépendantes sur $(\Omega, \mathcal{F}, \mathbb{P})$ à valeurs dans $\mathbb{X} = \{0, 1\}$ et $(\lambda_k)_{k=1,\ldots,n}$ une suite de nombres strictement positifs fixés. On sait que $\mathbb{P}(\xi_k = 1) = \lambda_k \Delta$ avec Δ un petit nombre réel strictement positif.
    (a) Pouvez-vous donner une borne sur Δ qui traduit proprement la notion de « petitesse » ?
    (b) Estimer $\mathbb{P}(\xi_1 + \ldots + \xi_n = 1)$ en ordre Δ^2.
    (c) Estimer $\mathbb{P}(\xi_1 + \ldots + \xi_n > 1)$.
42. Soient X et Y deux variables aléatoires réelles sur $(\Omega, \mathcal{F}, \mathbb{P})$ avec $\mathsf{Var}X > 0$ et $\mathsf{Var}Y > 0$.
    (a) Montrer que $|r(X, Y)| \leq 1$.
    (b) Monter que $|r(X, Y)| = 1$ si et seulement si $X = aY + b$.
43. Soit ξ une variable aléatoire réelle avec $\mathbb{E}(\xi^2) < \infty$.
    (a) Montrer que $\mathbb{E}(|\xi|) < \infty$.
    (b) Montrer que $\inf_{a \in \mathbb{R}} \mathbb{E}((\xi - a)^2)$ est atteint pour une valeur $a_0 \in \mathbb{R}$. Déterminer ce a_0.
    (c) Déterminer la valeur de $\inf_{a \in \mathbb{R}} \mathbb{E}((\xi - a)^2)$ en termes d'une caractéristique de ξ.
44. Soit ξ une variable aléatoire réelle de loi $\mathbb{P}_\xi$ et fonction de répartition F_ξ.
    (a) Déterminer $F_{a\xi+b}$ pour $a > 0$ et $b \in \mathbb{R}$.
    (b) Déterminer F_{ξ^2}.
45. Soit $\xi^+ = \max(\xi, 0)$. Déterminer F_{ξ^+}.

46. Soient ξ, η de variables aléatoires réelles définies sur $(\Omega, \mathcal{F}, \mathbb{P})$ à valeurs dans une partie discrète $\mathbb{X} \subset \mathbb{R}$. On note $\mathbb{P}_{(\xi,\eta)}$ leur loi conjointe et on suppose que les marginales unidimensionnelles $\mathbb{P}_\xi$ et $\mathbb{P}_\eta$ sont symétriques et telles que $\mathsf{Var}\xi = \mathsf{Var}\eta = 1$. On note $r := r(\xi, \eta)$ le coefficient de corrélation de ξ et η. Monter que

$$\mathbb{E}(\max(\xi^2, \eta^2)) \leq 1 + \sqrt{1 - r^2}.$$

47. (Identité de Wald). Soient $(X_n)_{n\in\mathbb{N}}$ une suite de variables aléatoires réelles, indépendantes et identiquement distribuées définies sur $(\Omega, \mathcal{F}, \mathbb{P})$ et τ une variable aléatoire définie sur le même espace $(\Omega, \mathcal{F}, \mathbb{P})$, à valeurs dans $\mathbb{N}$. Nous supposons que $\mathbb{E}(|X_1|) < \infty$, $\mathbb{E}(\tau) < \infty$ et que pour tout $n \in \mathbb{N}$, l'événement $\{\tau \geq n\}$ est indépendant de la variable aléatoire X_n. Montrer que la variable aléatoire

$$S_\tau = \sum_{n=1}^{\tau} X_i$$

a une espérance et que $\mathbb{E}(S_\tau) = \mathbb{E}(\tau)\mathbb{E}(X_1)$. (La somme S_τ est une somme partielle de la série de terme général X_n comportant un nombre *aléatoire* de termes).

Fonctions génératrices

48. On rappelle qu'une variable aléatoire X est dite suivre la loi binomiale $\mathcal{B}_{n,p}$ de paramètres $p \in [0,1]$ et $n \geq 1$ si $\mathbb{P}(X = k) = C_n^k p^k (1-p)^{n-k}$, pour $k = 1, \ldots, n$.
    (a) Calculer la fonction génératrice $G := G_{\mathcal{B}_{n,p}}$ correspondante.
    (b) Calculer $\mathbb{E}(X)$ à l'aide de la fonction génératrice.
    (c) Calculer $\mathsf{Var}(X)$ à l'aide de la fonction génératrice.
49. On rappelle qu'une variable aléatoire X est dite suivre la loi exponentielle $\mathcal{E}_\lambda$ de paramètre $\lambda > 0$ si $\mathbb{P}(X = k) = \exp(-\lambda)\frac{\lambda^k}{k!}$, pour $k \in \mathbb{N}$.
    (a) Calculer la fonction génératrice $G := G_{\mathcal{E}_\lambda}$ correspondante.
    (b) Calculer $\mathbb{E}(X)$ à l'aide de la fonction génératrice.
    (c) Calculer $\mathsf{Var}(X)$ à l'aide de la fonction génératrice.
50. Soient X et Y deux variables aléatoires indépendantes sur $(\Omega, \mathcal{F}, \mathbb{P})$ à valeurs dans $\mathbb{N}$. Exprimer la fonction génératrice G_{X+Y} de la somme $X + Y$, en termes de fonctions génératrices G_X et G_Y des variables individuelles.
51. En se servant du résultat de l'exercice 50, déterminer $G_{\mathcal{B}_{n,p}}$ en termes de $G_{\mathcal{B}_{1,p}}$ et comparer avec le résultat direct, obtenu en exercice 48.
52. (Extrait du CC du 16 novembre 2017).
    Soit $\mathbf{p} := (p_n)_{n\in\mathbb{N}}$ la suite définie par

$$p_n = \frac{a^n}{(1+a)^{n+1}}, \text{ pour } n \in \mathbb{N} \text{ et } a > 0.$$

    (a) Montrer que pour tout $a > 0$, la suite $\mathbf{p}$ est un vecteur de probabilité sur $\mathbb{N}$.

(b) Soit X une variable aléatoire sur un espace probabilisé $(\Omega, \mathcal{F}, \mathbb{P})$ à valeurs dans $\mathbb{N}$ dont la loi est déterminée par le vecteur de probabilité $\mathbf{p}$. Calculer la fonction génératrice $G_X(z)$ de X pour $z \in [-1, 1]$.
(c) Calculer $G'_X(z)$ et $G''_X(z)$.
(d) En déduire $\mathbb{E}(X)$ et $\mathsf{Var}(X)$.

53. Une somme de variables aléatoires comportant un nombre aléatoire de termes. (Extrait de l'examen du 15 décembre 2018).
Soient $(X_n)_{n\geq 1}$ une suite de variables aléatoires réelles de carré intégrables et d'espérance nulle et N une variable aléatoire à valeurs dans $\mathbb{N}$, indépendante de la suite (X_n), de loi $\nu(k) = \mathbb{P}(N = k) = \frac{1}{2^{k+1}}$ pour tout $k \in \mathbb{N}$. On note $S_N = \sum_{n=1}^{N} X_n$ et $\sigma^2 = \mathsf{var}(X_1)$.
(a) Calculer la fonction génératrice $G(z) = \mathbb{E}(z^N)$ et s'en servir pour calculer $\mathbb{E}(N)$.
(b) Montrer que $\mathbb{E}(S_N) = 0$.
(c) Calculer $\mathsf{var}(S_N)$. (Utiliser l'indépendance !)

Inégalité de Bienaymé-Tchebychev, théorèmes des grands nombres

54. Dans cet exercice, les variables aléatoires utilisées sont à valeurs dans des parties finies de $\mathbb{R}$. Toutes les espérances utilisées dans l'énoncé existent.
(a) Soit ξ une variable aléatoire discrète à valeurs dans une partie de $\mathbb{R}_+$. Rappeler comment on démontre, pour tout $a > 0$, l'inégalité de Markov-Tchebychev
$$\mathbb{P}(\xi \geq a) \leq \frac{\mathbb{E}\xi}{a}.$$
(b) Soient $a > 0$ et $f : \mathbb{R} \to \mathbb{R}_+$ une fonction croissante telle que $f(a) > 0$. Montrer que
$$\mathbb{P}(\xi \geq a) \leq \frac{\mathbb{E}(f(\xi))}{f(a)}.$$
(c) En conclure que
$$\mathbb{P}(\xi \geq a) \leq \inf_{s>0} \left[\exp(-sa)\mathbb{E}(\exp(s\xi))\right].$$
(d) Soit $(X_i)_{i\in\mathbb{N}}$ une suite de variables aléatoires indépendantes à valeurs dans $\{0, 1\}$ et de même loi, chargeant 1 avec probabilité p, avec $p \in]0, 1[$. Calculer, pour un $s > 0$ arbitraire,
$$g(s) := \mathbb{E}\left(\exp(s\sum_{i=1}^{n} X_i)\right)$$
et utiliser cette formule explicite pour majorer, pour un $a \in]p, 1[$, la probabilité $\mathbb{P}(\frac{1}{n}\sum_{i=1}^{n} X_i \geq a)$.
(e) Déterminer $s_0 := \arg\max_{s>0} \exp(-nas)g(s)$.

(f) En conclure que

$$\mathbb{P}\left(\frac{1}{n}\sum_{i=1}^{n} X_i \geq a\right) \leq \exp\left(nh(a,p)\right),$$

où $h(a,p) := -a\log\frac{a}{p} - (1-a)\frac{1-a}{1-p}$.

55. Soit $(\xi_n)_{n\in\mathbb{N}}$ une suite de variables aléatoires indépendantes réelles et de même loi, vérifiant $\mathbb{P}(\xi_n = 1) = p = 1 - \mathbb{P}(\xi_n = -1)$, pour tout $n \in \mathbb{N}$. On note $S_n = \sum_{i=1}^{n} \xi_i$. Le but de l'exercice est d'établir, dans le cas particulier où $p = 1/2$, la formule (valable pour $p \in [0,1]$ arbitraire)

$$\forall \varepsilon > 0,\ \mathbb{P}\left(\left|\frac{S_n}{n} - (2p-1)\right| \geq \varepsilon\right) \leq 2\exp(-\alpha\varepsilon^2 n),$$

pour un $\alpha > 0$. (Il s'agit d'une amélioration de l'inégalité de Bienaymé-Tchebychev).

56. Dans une circonscription d'un million d'électeurs les candidats A et B sont en lice. Parmi ces électeurs, 2000 connaissent bien le candidat A et votent unanimement pour lui. Les autres 998000 choisissent purement au hasard en lançant une pièce honnête. Minorer la probabilité pour que le candidat A gagne.

57. Soit $(\Psi_n)_{n\geq 1}$ une suite de variables aléatoires indépendantes, uniformément distribuées sur $[0, 2\pi[$, définies sur $(\Omega, \mathcal{F}, \mathbb{P})$. Une particule se déplace aléatoirement dans le plan selon la règle suivante : lorsque à l'instant n elle est en position $\boldsymbol{\xi}_n \in \mathbb{R}^2$, à l'instant $n+1$ elle sera en une position $\boldsymbol{\xi}_{n+1} \in \mathbb{R}^2$ telle que la longueur du déplacement $\boldsymbol{\xi}_{n+1} - \boldsymbol{\xi}_n$ est une constante $r > 0$ et l'angle formé par ce déplacement et l'axe des abscisses est Ψ_{n+1}. Soit $D_n^2 = \|\boldsymbol{\xi}_n - \boldsymbol{\xi}_0\|^2$ la distance entre les positions initiale et au temps n de la particule.

(a) Calculer $\lim_{n\to\infty} \frac{\boldsymbol{\xi}_n}{n}$.
(b) Calculer $\mathbb{E}(D_n^2)$.
(c) Calculer $\lim_{n\to\infty} \frac{D_n^2}{n}$.

58. Soit $(T_n)_{n\in\mathbb{N}}$ une suite de variables aléatoires indépendantes et identiquement distribuées à valeurs réelles positives, bornées (donc intégrables), définies sur $(\Omega, \mathcal{F}, \mathbb{P})$. La variable aléatoire T_n sera interprétée comme représentant la durée de vie de la n^e ampoule changée. Dès qu'une ampoule est grillée on la remplace aussitôt. Pour tout $t > 0$, on note

$$N_t = \sup\{N \geq 1 : \sum_{n=1}^{N} T_n \leq t\}$$

le nombre d'ampoules utilisées jusqu'au temps t. Montrer que $\lim_{t\to\infty} \frac{N_t}{t} \overset{\text{p.s.}}{=} \frac{1}{\mathbb{E}(T_1)}$.

59. (Extrait du contrôle du 16 novembre 2017).
On considère un espace probabilisé $(\Omega, \mathcal{F}, \mathbb{P})$ suffisamment grand pour pouvoir contenir simultanément toutes les variables aléatoire dont on se servira dans cet exercice.

(a) Soient X et Y deux variables aléatoires sur $(\Omega, \mathcal{F}, \mathbb{P})$ à valeurs dans $\mathbb{X} = \{0, 1\}$. La loi de X est déterminée par le vecteur de probabilité $\mathbf{p} = (p, 1-p)$ et celle de

Y par le vecteur $\mathbf{q} = (q, 1-q)$, où $0 \leq p, q \leq 1$. Exprimer la valeur $r := \mathbb{P}(X = Y)$ en fonction des p et q.

(b) Calculer $\mathsf{Var}(\mathbb{1}_{\{X=Y\}})$.

(c) On considère maintenant deux suites définies sur $(\Omega, \mathcal{F}, \mathbb{P})$. La première est une suite $(X_n)_{n\in\mathbb{N}}$ de copies indépendantes de X (i.e. elle est indépendante et identiquement distribué selon la loi $\mathbf{p}$). La seconde est une suite $(Y_n)_{n\in\mathbb{N}}$ de copies indépendantes de Y (i.e. elle est indépendante et identiquement distribué selon la loi $\mathbf{q}$). La deux suites sont en outre mutuellement indépendantes. Utiliser un résultat du cours pour montrer que la suite $\frac{1}{N}\sum_{n=1}^{N} \mathbb{1}_{\{X_n=Y_n\}}$ converge en probabilité vers une constante qu'il faudra déterminer.

Chaînes de Markov ; matrices stochastiques

60. Soient $\mathbb{X} = \{0, 1, \ldots, m\}$ un ensemble fini d'états et une suite indépendante $(U_n)_{n\geq 1}$, identiquement distribuée selon la loi uniforme sur $\{1, \ldots, m\}$. On introduit la suite $(X_n)_{n\geq 0}$ de variables aléatoires, définies par $X_0 = 0$ et $X_{n+1} = \max(X_n, U_{n+1})$, pour $n \geq 0$.
    (a) Montrer que (X_n) est une chaîne de Markov et déterminer sa matrice de transition P.
    (b) Esquisser le graphe de la matrice stochastique lorsque m est petit.
    (c) En utilisant des arguments d'estimation directe, indiquer quels états sont récurrents et quels sont transients.
    (d) Pour $m = 4$, calculer P^2.
61. Soient $(\xi_n)_{n\geq 1}$ une suite de variables aléatoires indépendantes, identiquement distribuées sur l'ensemble $\{-1, 1\}$ selon une loi μ avec $\mu(-1) = p \in [0, 1]$. On construit la suite $X'_n = \sum_{k=1}^{n} \xi_k$, pour $n \in \mathbb{N}$ avec la convention que la somme sur une famille vide d'indices est nulle.
    (a) Montrer que (X'_n) est une chaîne de Markov sur l'espace des états $\mathbb{X}$, avec matrice de transition P et probabilité initiale ρ (on précisera $\mathbb{X}'$, P' et ρ').
    (b) Montrer que la suite (X_n) définie récursivement par $X_0 = x_0 \in \mathbb{Z}$ et $X_{n+1} = X_n + \xi_{n+1}$, pour $n \geq 0$, est aussi une $\mathsf{CM}(\mathbb{X}, P, \rho)$ (préciser $\mathbb{X}$, P et ρ). La suite X_n est appelée marche aléatoire simple en dimension 1.
    (c) Montrer que la marche aléatoire simple en dimension 1 est irréductible (faire un argument en utilisant le graphe de la matrice de transition).
    (d) Montrer que la marche aléatoire simple en dimension 1 est récurrente si $p = 1/2$, transiente si $p \neq 1/2$.
    (e) Soient $a, b \in \mathbb{Z}$ avec $a < b$. Pour un $x \in [a, b] \cap \mathbb{Z}$, on note $h(x) = \mathbb{P}_x(\tau_a^0 < \tau_b^0)$.
        — Pour $p = 1/2$, montrer que $h(x) = \frac{1}{2}h(x-1) + \frac{1}{2}h(x+1)$ pour $x \in [a+1, b-1] \cap \mathbb{Z}$. Par un argument géométrique simple résoudre cette équation en utilisant les valeurs au bord évidentes pour $h(a)$ et $h(b)$ pour montrer que $h(x) = 1 - \frac{x-a}{b-a}$.
        — Établir la relation analogue pour $h(x)$ lorsque $p \neq 1/2$ et résoudre explicitement la récurrence.

(f) Interpréter ces résultats pour le problème de la « ruine du joueur ».

62. (Extrait du contrôle du 16 novembre 2017).
Soit $(X_n)_{n\in\mathbb{N}}$ une chaîne de Markov $\mathsf{CM}(\mathbb{X}, P, \cdot)$, où $\mathbb{X} = \{1, 2, 3, \ldots, \} = \mathbb{N}_>$ et la matrice stochastique $P = (P_{x,y})_{x,y\in\mathbb{X}}$ est définie par

$$P_{x,y} = \begin{cases} \frac{x}{x+1} & \text{si } x \in \mathbb{X}, y = 1 \\ \frac{1}{x+1} & \text{si } x \in \mathbb{X}, y = x+1 \\ 0 & \text{sinon.} \end{cases}$$

(a) Soit $\mathbf{p} := (p_x)_{x\geq 1}$ la suite définie par $p_x = \frac{1}{(e-1)x!}$. Montrer que $\mathbf{p}$ est un vecteur de probabilité sur $\mathbb{X}$.
(b) Montrer que le vecteur de probabilité $\mathbf{p}$ est invariant pour P, i.e. le vecteur ligne $\mathbf{p}$ est vecteur propre gauche de P associé à la valeur propre 1). *Clin d'œil :* $\frac{x}{x+1} = 1 - \frac{1}{x+1}$.
(c) Déterminer la décomposition de $\mathbb{X}$ en classes de communication.

63. (Extrait de l'examen du 7 mai 2013).
Soit $\beta \in]0, 1[$. On considère la matrice

$$P := \begin{pmatrix} 1-\beta & \beta \\ \beta & 1-\beta \end{pmatrix}.$$

(a) On note $\mathsf{spec}(P)$ l'ensemble des valeurs propres de P. Vérifier que $\mathsf{spec}(P) = \{1, 1-2\beta\}$.
(b) Vérifier que les vecteurs $\mathbf{D}_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ et $\mathbf{D}_{1-2\beta} = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$ sont des vecteurs propres droits associés aux valeurs propres correspondantes.
(c) Pour chaque $\lambda \in \mathsf{spec}(P)$, on note $\mathbf{d}_\lambda = \frac{\mathbf{D}_\lambda}{\|\mathbf{D}_\lambda\|_{\sup}}$ et $\delta_\lambda = \frac{\mathbf{D}_\lambda}{\|\mathbf{D}_\lambda\|_1}$, où, pour tout $\mathbf{z} \in \mathbb{R}^2$, on note $\|\mathbf{z}\|_1 = |z_1| + |z_2|$ et $\|\mathbf{z}\|_{\sup} = \max\{|z_1|, |z_2|\}$. Déterminer $\mathbf{d}_\lambda$ et δ_λ, pour $\lambda, \lambda' \in \mathsf{spec}(P)$.
(d) Pour $\mathbf{a} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ et $\mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$ vecteurs arbitraires, on note $\mathbf{a} \otimes \mathbf{b}^t = \begin{pmatrix} a_1b_1 & a_1b_2 \\ a_2b_1 & a_2b_2 \end{pmatrix}$. Vérifier que $P = \sum_{\lambda\in\mathsf{spec}(P)} \lambda E_\lambda$, où $E_\lambda = \mathbf{d}_\lambda \otimes \delta_\lambda^t$.
(e) Montrer que $E_\lambda E_{\lambda'} = \delta_{\lambda,\lambda'} E_\lambda$.
(f) En déduire que pour un $n \geq 1$ arbitraire,

$$P^n = \begin{pmatrix} p_n & 1-p_n \\ 1-p_n & p_n \end{pmatrix}.$$

(g) On déterminera explicitement p_n. Quelle est la valeur de $\lim_{n\to\infty} p_n$?
(h) On note (X_n) la chaîne de Markov sur un espace $\mathbb{X}$ à deux états, dont la matrice de transition est $\mathbf{P}$ et la probabilité initiale ρ_0. Déterminer $\pi(y) := \lim_{n\to\infty} \mathbb{P}_{\rho_0}(X_n = y)$, pour $y \in \mathbb{X}$.
(i) Montrer que π est une probabilité invariante.

Simulations Monte Carlo, algorithme de Metropolis

64. Comment à partir d'une pièce truquée à mémoire, de matrice stochastique (des tentatives)
$$Q = \begin{pmatrix} \frac{3}{5} & \frac{2}{5} \\ \frac{1}{5} & \frac{4}{5} \end{pmatrix}$$
peut-on construire une matrice stochastique P qui admet $\pi = (\frac{1}{2}, \frac{1}{2})$ comme probabilité d'équilibre ?

65. (Marches aléatoires sans recoupement sur $\mathbb{Z}^d$). Une marche aléatoire simple sur $\mathbb{Z}^d$ est une chaîne de Markov (X_n) obtenue par la récurrence $X_{k+1} = X_k + \xi_{k+1}, k \in \mathbb{N}$, avec $X_0 = x \in \mathbb{Z}^d$ et $(\xi_k)_{k\geq 1}$ une suite de variables aléatoires indépendantes et uniformément distribuées sur $E_d = \{\pm \mathbf{e}_j, j = 1, \ldots, d\}$, où $\mathbf{e}_j, j = 1, \ldots, d$, sont les vecteurs de la base canonique de $\mathbb{Z}^d$. L'ensemble des trajectoires (de longueur N fixée) possibles de telles marches constitue l'ensemble $\mathbb{X}^{\mathrm{mas}}$
$$\mathbb{X}^{\mathrm{mas}} := \mathbb{X}^{\mathrm{mas}}_{x,N} = \{\mathbf{y} : \{0, \ldots, N\} \to \mathbb{Z}^d : [y_0 = x] \wedge [y_{k+1} - y_k \in E_d]\}.$$
On s'intéresse au sous-ensemble des trajectoires sans recoupement
$$\mathbb{X}^{\mathrm{msr}} := \mathbb{X}^{\mathrm{msr}}_{x,N} = \{\mathbf{y} \in \mathbb{X}^{\mathrm{mas}}_{x,N} : y(k) \neq y(l), 0 \leq k < l \leq N\}$$
muni de la probabilité uniforme. Ces ensembles, pour $N \simeq 10^4$, modélisent bien certains polymères tels que le poly-chloro-éthylène, mais la contrainte géométrique forte de non-recoupement ne nous permet même pas d'estimer le cardinal de $\mathbb{X}^{\mathrm{msr}}_{x,N}$ dès que N prenne de valeurs modérément grandes.
On note G_d le sous-groupe discret de transformations orthogonales de $\mathbb{R}^d$ qui laisse $\mathbb{Z}^d$ invariant. Par exemple, en dimension $d = 2$, le sous-groupe G_d devient
$$G_2 = \{e, \pm\frac{\pi}{2}, \text{réflexions/axes } Ox, Oy, \text{réflexions/diagonales } D_1, D_2\}.$$
Soit ρ une probabilité sur G_d telle que
— $\rho(e) = 0$,
— $\rho(g) = \rho(g^{-1}), \forall g \in G_d$,
— si g est un générateur de G_d, alors $\rho(g) > 0$.
Pour $k \in \{1, \ldots, N\}$ et $g \in G_d$ on introduit la transformation $(k, g) : \mathbb{X}^{\mathrm{msr}}_{x,N} \to \mathbb{X}^{\mathrm{msr}}_{x,N}$ par
$$(k, g)\mathbf{y} = \mathbf{y}' := (y_0, \ldots, y_{k-1}, y_{k-1} + g(y_k - y_{k-1}), \ldots, y_{N-1} + g(y_N - y_{N-1}), \forall \mathbf{y} \in \mathbb{X}^{\mathrm{msr}}_{x,N}.$$
Dans la suite on note simplement $\mathbb{X}^{\mathrm{mas}}$ et $\mathbb{X}^{\mathrm{msr}}$ au lieu de $\mathbb{X}^{\mathrm{mas}}_{x,N}$ et $\mathbb{X}^{\mathrm{msr}}_{x,N}$.

Algorithme de génération de marches aléatoires sans recoupement

Require: Générateur $g \in G_d$ selon ρ,
générateur $\mathsf{unif}(\{1,\ldots,N\}$
$\mathbf{y} \in \mathbb{X}^{\mathrm{msr}}$.
Ensure: $\mathbf{z} \in \mathbb{X}^{\mathrm{msr}}$.
Choisir $g \in G_d$ selon ρ.
Choisir $k \in \{1,\ldots,N\}$ selon $\mathsf{unif}(\{1,\ldots,N\})$.
if $(k,g)\mathbf{y} \in \mathbb{X}^{\mathrm{msr}}$ **then**
$\mathbf{z} \leftarrow (k,g)\mathbf{y}$
else
$\mathbf{z} \leftarrow \mathbf{y}$
end if

(a) Montrer que l'algorithme ci-dessus définit une matrice stochastique P sur $\mathbb{X}^{\mathrm{msr}}$ avec
$$P(\mathbf{y},\mathbf{z}) = \begin{cases} \frac{\rho(g)}{N} & \text{si } \mathbf{z} = (k,g)\mathbf{y} \\ \frac{1}{N}\sum_{k,g}\rho(g)\mathbb{1}_{\mathbb{X}^{\mathrm{mas}}\setminus\mathbb{X}^{\mathrm{msr}}}((k,g)\mathbf{y}) & \text{sinon.} \end{cases}$$
(b) Montrer que P est stochastique, apériodique, irréductible et bistochastique.
(c) Conclure que P admet la mesure uniforme sur $\mathbb{X}^{\mathrm{msr}}$ comme mesure d'équilibre.

Entropie, mesure de l'information

66. Les habitants d'un village sont divisés en deux parties. Une partie A contient des individus qui disent la vérité avec probabilité $1/2$, mentent avec probabilité $3/10$ et refusent de répondre avec probabilité $2/10$. La partie B contient des individus dont les probabilités pour chaque type de comportement sont respectivement $3/10$, $1/2$ et $2/10$. Soit $p \in [0,1]$ la probabilité qu'un habitant du village choisi au hasard appartienne au groupe A. On note $i := i(p)$ l'information sur son comportement vis-à-vis des questions posées qui est véhiculé par son appartenance à un groupe donné. Calculer $p_0 = \arg\max i(p)$ et $i(p_0)$.
67. Soient $(a_i)_{i=1,\ldots,n}$ des nombres positifs vérifiant $\sum_{i=1}^n a_i = 1$ et $(x_i)_{i=1,\ldots,n}$ des nombres strictement positifs. Établissez l'inégalité
$$x_1^{a_1}\cdots x_n^{a_n} \leq \sum_{i=1}^n a_i x_i.$$
68. Soit $\mathbf{p} = (p_1,\ldots,p_n)$ un vecteur de probabilité (i.e. ayant des coordonnées $p_i \geq 0$ et vérifiant la condition de normalisation $\sum_{i=1}^n p_i = 1$). Supposons que $p_1 > p_2$ et notons $\delta \in]0, \frac{p_2-p_1}{2}]$. On considère le nouveau vecteur de probabilité $\mathbf{p}'$ avec $p_1' = p_1 - \delta$, $p_2' = p_2 + \delta$ et $p_i' = p_i$ pour $i = 3,\ldots,n$. Les entropies $H(\mathbf{p}')$ et $H(\mathbf{p})$ se comparent-elles et si oui comment ?
69. Soient $A = (A_{ij})_{i,j=1,\ldots n}$ une matrice doublement stochastique (i.e. une matrice dont tous les termes sont positifs et dont chaque ligne et chaque colonne a une somme normalisée à 1), et $\mathbf{p} = (p_1,\ldots,p_n)$ un vecteur (ligne) de probabilité.

(a) Montrer que le vecteur (ligne) $\mathbf{p}' = \mathbf{p}A$ est un vecteur de probabilité.
(b) Comparer les entropies $H(\mathbf{p})$ et $H(\mathbf{p}')$.

Propriétés de différentes variantes d'entropie et relations entre elles

70. (a) Montrer l'inégalité de Jensen (dans un cas simple), à savoir que si f est une fonction convexe dérivable et $(a_n)_{i\in I}$ une famille finie de nombre positifs tels que $\sum_{i\in I} a_i = 1$, alors
$$\sum_{i\in I} a_i f(t_i) \geq f(\sum_{i\in I} a_i t_i).$$
(b) Soient $(a_i)_{i=1,\ldots,n}$ une famille de nombres positifs et $(b_i)_{i=1,\ldots,n}$ une famille de nombres strictement positifs. Montrer que
$$\sum_{i=1}^n a_i \log \frac{a_i}{b_i} \geq \sum_{i=1}^n \log \frac{\sum_{j=1}^n a_j}{\sum_{k=1}^n b_k}.$$
(c) Montrer que $D(\mathbf{p}\|\mathbf{q})$ est convexe en le couple $(\mathbf{p}, \mathbf{q})$, i.e. si $(\mathbf{p}, \mathbf{q})$ et $(\mathbf{p}', \mathbf{q}')$ sont deux couples de vecteurs de probabilité et $\lambda \in [0, 1]$ alors
$$D(\lambda\mathbf{p} + (1-\lambda)\mathbf{p}'\|\lambda\mathbf{q} + (1-\lambda)\mathbf{q}') \leq \lambda D(\mathbf{p}\|\mathbf{q}) + (1-\lambda)D(\mathbf{p}'\|\mathbf{q}).$$
71. En se servant du résultat précédent pour $\mathbf{q} = \mathbf{q}' = \mathbf{u}$, où $\mathbf{u}$ est le vecteur de probabilité de la loi uniforme, montrer que $H(\mathbf{p})$ est concave en $\mathbf{p}$.
72. (Extrait de l'examen du 19 décembre 2013).
Soient X_1 et X_2 deux variables aléatoires sur $(\Omega, \mathcal{F}, \mathbb{P})$ prenant des valeurs dans le même espace $\mathbb{X}$ avec des lois décrites par les vecteurs de probabilité $\mathbf{p}$ et $\mathbf{p}'$ respectivement. Soit Y une variable aléatoire sur le même espace $(\Omega, \mathcal{F}, \mathbb{P})$ prenant de valeurs dans $\mathbb{Y} = \{1, 2\}$ selon le vecteur de probabilité $(\lambda, 1-\lambda)$, avec $\lambda \in [0, 1]$; on note $Z = X_Y$ la variable aléatoire à valeurs dans $\mathbb{X}$.
(a) Calculer $\mathbb{P}(Z = x)$.
(b) En se servant du fait que le conditionnement réduit l'incertitude, i.e. $H(Z) \geq H(Z|Y)$, établir le résultat de concavité de $H(\mathbf{p})$ par rapport à $\mathbf{p}$ avec une méthode alternative à celle utilisée dans l'exercice précédent.

Compléments sur l'entropie

73. (Extrait de l'examen du 20 décembre 2017).
Le but de cet exercice est de montrer le
Théorème : *Soient $\mathbb{X}$ un ensemble fini, β un paramètre positif et $U : \mathbb{X} \to \mathbb{R}_+$ une variable aléatoire réelle positive sur $\mathbb{X}$. Pour une mesure de probabilité arbitraire $\nu \in \mathcal{M}_1(\mathbb{X})$ sur $\mathbb{X}$, on note $\nu U := \sum_{x\in\mathbb{X}} \nu(x)U(x)$, l'espérance*[2] *de U sous ν. Alors,*

2. Le vecteur de probabilité ν est considéré comme un vecteur ligne, la variable aléatoire U comme un vecteur colonne ; pour ν fixé, l'espérance de U est la forme linéaire νU.

(a) *il existe une mesure de probabilité μ_β sur $\mathbb{X}$ qui sature le $\sup_{\nu\in\mathcal{M}_1(\mathbb{X})}(H(\nu)-\beta\nu U)$, où $H(\nu)$ désigne l'entropie de ν,*

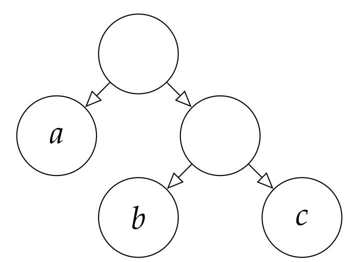
(b) *$\mu_\beta(x) = \frac{\exp(-\beta U(x))}{\mathcal{Z}(\beta)}$, pour tout $x\in\mathbb{X}$, où $\mathcal{Z}(\beta)=\sum_{y\in\mathbb{X}}\exp(-\beta U(y))$ est un facteur de normalisation.*

(a) Utiliser la concavité de la fonction log pour montrer que pour tout $\nu\in\mathcal{M}_1(\mathbb{X})$, on a $H(\nu)-\beta\nu U \le \log\mathcal{Z}(\beta)$.

(b) Calculer $H(\mu_\beta)-\beta\mu_\beta U$.

74. Simulation d'une loi arbitraire avec une pièce honnête. (Extrait de l'examen du 15 décembre 2014).
On dispose d'une pièce honnête (prenant de valeurs dans $\mathbb{B}=\{0,1\}$ selon le vecteur de probabilité $(1/2,1/2)$). Les lancers successifs de la pièce sont modélisés par des suites aléatoires de longueur arbitraire de bits indépendants, c'est-à-dire par des mots $\xi\in\mathbb{B}^+$ (on rappelle que $\mathbb{B}^+=\cup_{n=1}^\infty\mathbb{B}^n$). On veut simuler une variable aléatoire X à valeurs dans un ensemble fini $\mathbb{X}$ dont la loi est décrite par un vecteur de probabilité $\mathbf{p}$ arbitraire. Autrement dit, nous voulons exprimer X comme fonction de certains mots, choisis d'une certaine manière, parmi les mots de $\mathbb{B}^+$, de façon que la loi de X soit déterminée par les probabilités des mots choisis.

(a) Commencer par l'ensemble à trois éléments $\mathbb{X}=\{a,b,c\}$ et $\mathbf{p}=(1/2,1/4,1/4)$. Placer les lettres a,b,c comme des feuilles d'un arbre binaire complet (i.e. dont chaque nœud a 0 ou 2 descendants) comme dans la figure adjacente. En associant le bit 0 aux arêtes gauches et le bit 1 aux arêtes droites, on constate que l'ensemble de feuilles $\mathbb{F}=\{0,10,11\}$ de l'arbre se surjecte sur $\mathbb{X}$. On note $F:\mathbb{F}\to\mathbb{X}$ cette surjection (dans ce cas particulier, il s'agit d'une bijection). Expliciter l'algorithme de génération de X.



(b) Dans le cas particulier de la question précédente, estimer le nombre moyen de fois qu'il faudra lancer la pièce pour réaliser X et comparer ce résultat avec l'entropie $H(X)$.

(c) Considérer maintenant l'ensemble $\mathbb{X}=\{a,b\}$ et le vecteur de probabilité $\mathbf{p}=(2/3,1/3)$. *Suggestion : Observer que $\sum_{k=0}^\infty\frac{1}{2^{2k+1}}=\frac{2}{3}$ et utiliser cette égalité pour donner les représentations binaires des nombres $2/3$ et $1/3$; se servir de cette représentation pour déterminer l'ensemble $\mathbb{F}$ de feuilles et la surjection $F:\mathbb{F}\to\mathbb{X}$.*

(d) Estimer le nombre moyen de lancers nécessaires pour simuler X. *On peut utiliser sans démonstration l'identité $\sum_{k=0}^\infty\frac{k}{2^k}=2$. Si cette identité est démontrée, elle donnera lieu à un bonus.*

Question bonus. Pouvez-vous proposer une méthode générale pour un ensemble fini $\mathbb{X}$ arbitraire muni d'un vecteur de probabilité arbitraire $\mathbf{p}$?

Codes instantanés, codes uniquement décodables

75. Soit $C:\{\texttt{a},\texttt{b}\}\to\{0,1\}^*$ le code défini par

x	$C(x)$
a	1
b	101

(a) Le code C est-il instantané ?
(b) Est-il uniquement déchiffrable ?

76. Déterminer si les codes suivants — définis sur des ensembles à 7 ou 8 éléments selon le cas — sont instantanés ; sinon sont-ils uniquement décodables.

x_1	abc	0101	00	00
x_2	abcd	0001	112	11
x_3	e	0110	0110	0101
x_4	dba	1100	0112	111
x_5	bace	00011	100	1010
x_6	ceac	00110	201	100100
x_7	ceab	11110	212	0110
x_8	eabd	101011	22	

77. Soient $\mathbb{X}$ un ensemble de cardinal $M = 4$ et $\mathbf{p} = (1/2, 1/4, 1/8, 1/8)$ un vecteur de probabilité sur $\mathbb{X}$. On considère les quatre codes $C_k, k = 1, \ldots, 4$, définis ci-dessous.

X	$C_1(X)$	$C_2(X)$	$C_3(X)$	$C_4(X)$
a	0	00	0	0
b	10	01	1	01
c	110	10	00	011
d	111	11	11	111

(a) Calculer $H(\mathbf{p})$.
(b) Pour $k = 1, \ldots, 4$, calculer $\mathbb{E}|C_k(X)|$ et comparer avec $H(\mathbf{p})$.
(c) Pour $k = 1, \ldots, 4$, déterminer si C_k est un code instantané et sinon s'il est uniquement décodable.

Codes de Huffman

78. Soient $\mathbb{X}$ un ensemble de cardinal M et $\mathbf{p}$ un vecteur de probabilité sur $\mathbb{X}$. Calculer un code de Huffman et comparer l'espérance de sa longueur avec l'entropie dans les cas suivants :

(a) $M = 5$ et $\mathbf{p} = (0.25, 0.25, 0.2, 0.15, 0.15)$.
(b) $M = 6$ et $\mathbf{p} = (0.3, 0.25, 0.2, 0.1, 0.1, 0.05)$.

79. Soit $\mathbb{X} = \{0, 1\}$, $\mathbf{p} = (0.9, 0.1)$ et $\mathbf{p}' = (0.6, 0.4)$ deux vecteurs de probabilité et K un entier strictement positif. On note $X^K = (X_1, \ldots, X_K)$, où $(X_i)_{i=1,\ldots,K}$ sont de copies indépendantes de la même variable aléatoire sur $\mathbb{X}$.

(a) Calculer $H(X^K)$ lorsque X_1 est distribuée selon $\mathbf{p}$ et selon $\mathbf{p}'$.
(b) Calculer un code de Huffman C pour $K = 2, \ldots, 4$ dans les deux cas $\mathbf{p}$ et $\mathbf{p}'$.
(c) Calculer $\mathbb{E}_{\mathbf{p}}|C(X^K)|$ et $\mathbb{E}_{\mathbf{p}'}|C(X^K)|$ pour $K = 2, \ldots, 4$.

80. Déterminer un vecteur de probabilité $\mathbf{p}$ sur $\mathbb{X} = \{\mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d}\}$ qui donne lieu à deux codes de Huffman différents. Pour chacun de ces codes calculer l'espérance de sa longueur et comparer la avec $H(\mathbf{p})$.

Compléments sur les codes

81. Soient X une variable aléatoire à valeurs dans $\mathbb{X} = \{\mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d}\}$ distribuée selon une loi décrite par le vecteur de probabilité $\mathbf{p} = (1/2, 1/4, 1/8, 1/8)$ et $C : \mathbb{X} \to \mathbb{A}^+$ avec $\mathbb{A} = \{0, 1\}$ un code de Huffman. On note avec le même symbole C l'extension du code sur $\mathbb{X}^+$ et on considère un mot $\xi \in \mathbb{X}^+$ de longueur $L = |\xi|$. On désigne par $\alpha = C(\xi) \in \mathbb{A}^+$ la suite codant ξ. Quelle est la probabilité qu'un bit au hasard de cette suite prenne la valeur 1 lorsque $L \to \infty$?
82. On dispose d'une pièce honnête et on veut simuler une variable aléatoire $X \in \mathbb{X} = \{1, \ldots, M\}$ avec une loi $\mathbf{p}$.
    (a) Proposer un algorithme.
    (b) Combien de fois en moyenne doit-on lancer la pièce avec votre algorithme pour simuler $X \in \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$ avec loi $\mathbf{p} = (1/2, 1/4, 1/4)$?
    (c) Même question pour $X \in \{\mathtt{a}, \mathtt{b}\}$ et $\mathbf{p} = (2/3, 1/3)$?
83. Construire le dictionnaire de chaînes-préfixes du codage du mot

$$\alpha = \mathtt{the\ fat\ cat\ sat\ on\ the\ mat.}$$

par l'algorithme de Lempel-Ziv 78.
84. Coder et décoder selon LZ78 le mot

$$\beta = 0012121210210121012210 1$$

Codage du canal

85. Pour trois variables aléatoires X, W, Y discrètes arbitraires, établir les relations suivantes :
    (a) $H(W, Y|X) \leq H(W|X) + H(Y|X)$.
    (b) $H(W, Y|X) = H(W|X) + H(Y|X, W)$.
    (c) $H(Y|X, W) \leq H(Y|X)$.
86. Soient les canaux $\mathcal{K}_1 = (\mathbb{X}, \pi, \mathbb{W}, P)$ et $\mathcal{K}_2 = (\mathbb{W}, \rho, \mathbb{Y}, Q)$ où $\mathbb{X}, \mathbb{W}$ et $\mathbb{Y}$ sont des alphabets d'entrée ou de sortie et P et Q des matrices de transmission. On construit le canal $\mathcal{K} = (\mathbb{X}, \pi, \mathbb{Y}, PQ)$ en mettant les canaux $\mathcal{K}_1$ et $\mathcal{K}_2$ en cascade.
    (a) Comparer les probabilités conditionnelles $\mathbb{P}(Y = y|X = x, W = w)$ et $\mathbb{P}(Y = y|W = w)$.
    (b) Montrer que la capacité $C_{\mathcal{K}}$ du canal composé ne peut pas excéder la plus petite des capacités $C_{\mathcal{K}_1}$ et $C_{\mathcal{K}_2}$.
    (c) Commenter ce dernier résultat.

87. Soient $\mathbb{X}$ un espace fini, X une variable aléatoire à valeurs dans $\mathbb{X}$, $g : \mathbb{X} \to \mathbb{W}$ une application arbitraire et Y une variable aléatoire à valeurs dans $\mathbb{Y}$ de loi conjointe κ avec X. Monter par deux méthodes différentes que $H(Y|g(X)) \geq H(Y|X)$.
88. (Extrait de l'examen du 19 décembre 2013).
Soit un canal discret sans mémoire ayant un alphabet d'entrée $\mathbb{X}$, un alphabet de sortie $\mathbb{Y}$, une matrice stochastique de transmission P et une loi des symboles d'entrée déterminée par le vecteur de probabilité π. Lorsque un symbole $y \in \mathbb{Y}$ est transmis, on le décode par un schéma de décision qui peut être soit une fonction déterministe $d : \mathbb{Y} \to \mathbb{X}$ soit une variable aléatoire Δ définie sur $\mathbb{Y}$ à valeurs dans $\mathbb{X}$.
    (a) Déterminer le vecteur de probabilité ρ définissant la loi des symboles de sortie.
    (b) On se place dans le cas particulier $\mathbb{X} = \{x_1, x_2, x_3\}$, $\mathbb{Y} = \{y_1, y_2, y_3\}$, $\pi = (1/2, 1/4, 1/4)$ et $P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1/2 & 1/2 \end{pmatrix}$. Calculer ρ.
    (c) Dans le cas particulier ci-dessus, on utilise le schéma de décision déterministe $d(y_1) = x_1$, $d(y_2) = d(y_3) = x_3$. Calculer la probabilité globale de décision (=décodage) erronée.
    (d) Pour une règle de décision d, établir les formules générales des probabilités de décision correcte et erronée, notées respectivement $\mathsf{PTE}(d)$ et $\mathsf{PTC}(d)$.
    (e) Calculer la probabilité de décision correcte dans le cas particulier de la question b).
    (f) On appelle **observateur idéal** le choix de la règle de décision $d_o(y) = x_y$, où $y \in \mathbb{Y}$, le x_y maximise la probabilité conditionnelle $\mathbb{P}(X = x|Y = y)$, c'est-à-dire :
    $$x_y = \arg\max_x \mathbb{P}(X = x|Y = y).$$
    Monter que la règle de décision ainsi définie est optimale, c'est-à-dire, pour toute autre règle déterministe d', on $\mathsf{PTC}(d) \leq \mathsf{PTC}(d_o)$.
    (g) Si Δ est une règle de décision stochastique arbitraire correspondant à la probabilité conditionnelle $Q_{yx} = \mathbb{P}(\Delta(y) = x|Y = y)$, montrer que $\mathsf{PTC}(\Delta) \leq \mathsf{PTC}(d_o)$.
89. (Extrait de l'examen du 20 décembre 2017).
Soit $\mathcal{K} = (\mathbb{X}, \mathbb{Y}, P, \mu)$ un canal avec alphabets d'entrée et de sortie finis, notés respectivement $\mathbb{X}$ et $\mathbb{Y}$, matrice stochastique P et probabilité des symboles de la source μ. Nous écrirons $\mu(x)$ au lieu de $\mu(\{x\})$, i.e. nous identifierons — comme d'habitude — la mesure de probabilité μ avec le vecteur (ligne) de probabilité $(\mu(x))_{x\in\mathbb{X}}$. Déterminer, pour des variables d'entrée X et de sortie Y et pour des symboles $x \in \mathbb{X}$ et $y \in \mathbb{Y}$:
    (a) La mesure de probabilité conjointe $\kappa(x, y) := \mathbb{P}(X = x, Y = y)$.
    (b) La mesure de probabilité de sortie $\nu := \sum_{x\in\mathbb{X}} \mathbb{P}(X = x, Y = y)$.
    (c) La probabilité que l'entrée soit x, sachant que la sortie observée est y, i.e. $Q(y, x) := \mathbb{P}(X = x|Y = y)$.
    (d) On fixe maintenant les alphabets d'entrée et de sortie $\mathbb{X} = \mathbb{Y} = \{0, 1\}$ (canal

binaire) et la loi[3] de la source $\mu = (1/4, 3/4)$.

i. Si le canal est symétrique avec taux d'erreur $f = 1/16$,
   — Déterminer la matrice stochastique P du canal.
   — Determiner le vecteur probabilité de sortie ν.
   — Calculer $Q(1,0)$ et $Q(1,0)$.

ii. Si le canal est « en Z » avec taux d'erreur $f = 1/16$, i.e. sa matrice stochastique est $P = \begin{pmatrix} 1 & 0 \\ 1/16 & 15/16 \end{pmatrix}$, calculer
   — Le vecteur de probabilité de sortie ν
   — Les probabilités $Q(1,0)$ et $Q(1,1)$.

90. (Extrait de l'examen du 20 décembre 2017).
Soit $\mathcal{K} = (\mathbb{X}, \mathbb{Y}, P, \mu)$ un canal avec alphabets d'entrée et de sortie finis, notés respectivement $\mathbb{X}$ et $\mathbb{Y}$, matrice stochastique P et probabilité des symboles de la source μ. Nous écrirons $\mu(x)$ au lieu de $\mu(\{x\})$, i.e. nous identifierons — comme d'habitude — la mesure de probabilité μ avec le vecteur (ligne) de probabilité $(\mu(x))_{x\in\mathbb{X}}$. Déterminer, pour des variables d'entrée X et de sortie Y et pour des symboles $x \in \mathbb{X}$ et $y \in \mathbb{Y}$:

(a) La mesure de probabilité conjointe $\kappa(x, y) := \mathbb{P}(X = x, Y = y)$.
(b) La mesure de probabilité de sortie $\nu := \sum_{x\in\mathbb{X}} \mathbb{P}(X = x, Y = y)$.
(c) La probabilité que l'entrée soit x, sachant que la sortie observée est y, i.e. $Q(y, x) := \mathbb{P}(X = x | Y = y)$.
(d) On fixe maintenant les alphabets d'entrée et de sortie $\mathbb{X} = \mathbb{Y} = \{0, 1\}$ (canal binaire) et la loi[4] de la source $\mu = (1/4, 3/4)$.

i. Si le canal est symétrique avec taux d'erreur $f = 1/16$,
   — Déterminer la matrice stochastique P du canal.
   — Determiner le vecteur probabilité de sortie ν.
   — Calculer $Q(1,0)$ et $Q(1,0)$.

ii. Si le canal est « en Z » avec taux d'erreur $f = 1/16$, i.e. sa matrice stochastique est $P = \begin{pmatrix} 1 & 0 \\ 1/16 & 15/16 \end{pmatrix}$, calculer
   — Le vecteur de probabilité de sortie ν
   — Les probabilités $Q(1,0)$ et $Q(1,1)$.

91. Soient $\mathcal{K}_i$, avec $i = 1, 2$ deux canaux avec alphabets d'entrée $\mathbb{X}_i$, alphabets de sortie $\mathbb{Y}_i$ et matrices de transmission P_i. On note $\mathbb{X} = \mathbb{X}_1 \oplus \mathbb{X}_2$ (si les alphabets $\mathbb{X}_1$ et $\mathbb{X}_2$ sont distincts alors $\mathbb{X}_1 \oplus \mathbb{X}_2 = \mathbb{X}_1 \cup \mathbb{X}_2$; s'ils ne sont pas distincts, on commence par distinguer artificiellement les éléments de $\mathbb{X}_1$ et de $\mathbb{X}_2$ avant de prendre leur réunion). De même $\mathbb{Y} = \mathbb{Y}_1 \oplus \mathbb{Y}_2$. Finalement la matrice de transmission du canal « somme » est la matrice bloc $P = \begin{pmatrix} P_1 & 0 \\ 0 & P_2 \end{pmatrix}$.

3. Les valeurs numériques données pour les probabilités de la source et de l'erreur permettent de déterminer toutes les autres probabilités comme des rationnels calculables facilement à la main.

4. Les valeurs numériques données pour les probabilités de la source et de l'erreur permettent de déterminer toutes les autres probabilités comme des rationnels calculables facilement à la main.

(a) Soient X une variable aléatoire à valeurs dans $\mathbb{X}$ dont la loi est décrite par le vecteur de probabilité π et Y une variable aléatoire à valeurs dans $\mathbb{Y}$. On note κ la loi conjointe du couple (X, Y). Soit $p = \sum_{x\in\mathbb{X}_1} \pi(x)$ (donc $1 - p = \sum_{x\in\mathbb{X}_2} \pi(x)$). Pour $x \in \mathbb{X}_1$ on note $\rho_1(x) = \frac{\pi(x)}{p}$ et pour $x \in \mathbb{X}_2$ on note $\rho_2(x) = \frac{\pi(x)}{1-p}$. Montrer que $H(\pi) = H(p, 1-p) + pH(\rho_1) + (1-p)H(\rho_2)$.

(b) Montrer que

$$H(X|Y) = -p \sum_{x\in\mathbb{X}_1, y\in\mathbb{Y}_1} \rho_1(x)P_1(x,y) \log \mathbb{P}(X = x|Y = y)$$
$$- (1-p) \sum_{x\in\mathbb{X}_2, y\in\mathbb{Y}_2} \rho_2(x)P_2(x,y) \log \mathbb{P}(X = x|Y = y).$$

(c) On considère des variables aléatoires X_1 et X_2 respectivement à valeurs dans $\mathbb{X}_1$ et $\mathbb{X}_2$ et de lois ρ_1 et ρ_2 ; on note Y_1 et Y_2 les variables aléatoires obtenues par restriction de Y sur $\mathbb{Y}_1$ et $\mathbb{Y}_2$. Montrer que

$$H(X|Y) = pH(X_1|Y_1) + (1-p)H(X_2|Y_2)$$

et conclure que

$$C(p) = \sup_{\pi:\sum_{x\in\mathbb{X}_1} \pi(x)=p} I(X, Y) = H(p, 1-p) + pC_1 + (1-p)C_2.$$

(d) Montrer que la valeur de p qui maximise $C(p)$ est $p = \frac{2^{C_1}}{2^{C_1}+2^{C_2}}$.

(e) En conclure que la capacité du canal « somme » vérifie $2^C = 2^{C_1} + 2^{C_2}$.

Codes à répétition

Dans ce paragraphe, on considère un canal binaire symétrique ayant une probabilité d'erreur p. On note R_N le code à N répétitions pour chaque bit et $p_b(R_N, p)$ la probabilité de décoder de manière erronée un bit par la méthode de vote majoritaire.

92. Calculer $p_b(R_3, p)$ pour $p = 0.1$.
93. Pour N arbitraire,
    (a) Calculer $p_b(R_N, p)$.
    (b) Pour $p = 0.1$ quel est le terme dominant dans l'expression de $p_b(R_N, p)$.
    (c) À partir de quelle valeur de N, on obtient une valeur de $p_b(R_N, 0.1) \leq 10^{-15}$?
    (d) Quel est le taux de transmission pour R_N ?
    (e) Placer les couples $(R_N, \log p_b(R_N, p))$ pour $N \in \{1, 3, 5 \ldots, 101\}$ sur un graphique. Qu'observez-vous ?

Codes de Hamming

94. Décoder par le code de Hamming $\textsc{Ham}(7, 4)$ les messages suivants :

(a) $\mathbf{r} = 1101011$,
(b) $\mathbf{r} = 0110110$,
(c) $\mathbf{r} = 0100111$,
(d) $\mathbf{r} = 1111111$.

95. Calculer toutes les chaînes de bruit $\mathbf{b} \in \{0,1\}^7$ qui donnent un syndrome nul pour $\textsc{Ham}(7,4)$.
96. Pour le code $\textsc{Ham}(7,4)$ et le canal binaire symétrique avec $p = 0.1$,
    (a) déterminer la probabilité qu'un block de 7 bits ne soit pas décodé correctement,
    (b) en déduire la probabilité du taux d'erreur par bit, dans le cas où le poids du bruit est exactement $\|B\| = 2$.
97. La matrice de contrôle de parité du code $\textsc{Ham}(15,4)$ est donnée par

$$H := \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Décoder le mot $\mathbf{r} = 000010000011001$.