THÉORIE DE L'INFORMATION

Trois théorèmes de Claude Shannon

Antoine Chambert-Loir

Antoine Chambert-Loir
Université de Paris.
E-mail : antoine.chambert-loir@u-paris.fr

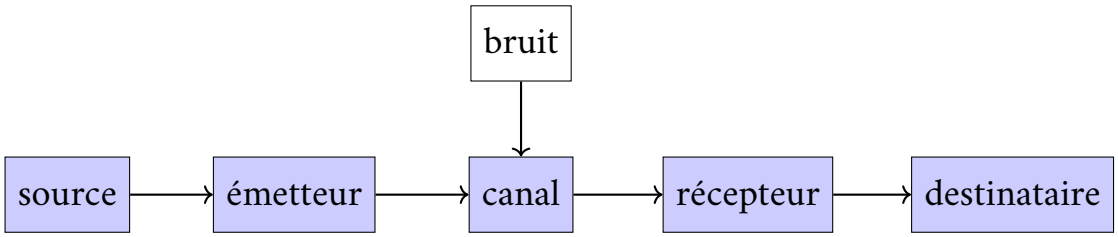
Version du 30 juin 2021, 9h33
La version la plus à jour de ce texte devrait être accessible en ligne, à l'adresse http://webusers.imj-prg.fr/~antoine.chambert-loir/enseignement/2020-21/shannon/shannon.pdf

TABLE DES MATIÈRES

INTRODUCTION

La *théorie mathématique de la communication* vise à étudier de façon mathématiques dans quelles conditions on peut transmettre des données, en particulier à quelle vitesse, et avec quelle fiabilité.

Dans l'article fondateur de Shannon (1948), un système de communication est modélisé par le diagramme suivant :



– La *source* est l'entité qui possède une information, un *message*, à transmettre à son *destinataire*. La source peut-être une station de radio ou de télévision, un journal, un site web, vous ou moi désirant annoncer une mauvaise nouvelle au téléphone ou par courrier électronique, une sonde spatiale prenant des photos des planètes qu'elle survole, etc. Le message peut-être un texte, une photographie, un morceau de musique, une combinaison de ceux-ci.

– L'*émetteur* est l'appareil physique par lequel nous allons diffuser ce message, c'est par exemple un émetteur de radio ou de télévision. À l'époque de Shannon, la transmission était souvent analogique. Dans le cas du téléphone ou de la radio, le son est représenté par l'amplitude de la pression sur le micro que ce dernier transforme en un signal électrique proportionnel. Il s'agit donc de transmettre cette amplitude, représentée par une fonction du temps, ou par deux telles fonctions pour un signal stéréo. Dans le cas de la télévision couleur, il s'agira de transmettre trois amplitudes pour la couleur (rouge/vert/bleu) en chaque point de l'écran, deux amplitudes pour le son, le tout dépendant du temps. De nos jours, la

transmission des signaux — télévision, téléphone, Internet — est essentiellement numérique, à l'exception notable de la radio FM, la radio numérique terrestre (DAB) qui peine à décoller : le message est transformé en une suite de nombres qu'il s'agit de transmettre.

– Le *récepteur* est l'appareil par lequel le destinataire reçoit ce message, c'est un poste de radio ou de télévision, éventuellement associé à un « décodeur » dans le cas de la télévision numérique terrestre ou de la télévision par Internet, un téléphone, un ordinateur relié au réseau Internet, etc.

– Le *canal* est le medium physique par lequel l'information est transmise de l'émetteur au récepteur : l'air pour la transmission de la radio/télévision par voie hertzienne, la fibre optique du fournisseur Internet, les câbles en cuivre du réseau de téléphone, etc. Comme tout objet physique, ce canal est sujet à des perturbations — du *bruit* — par lesquelles le signal qui parvient au récepteur diffère de celui envoyé par l'émetteur, de sorte que le message reçu par le destinataire diffère de celui envoyé par la source.

La théorie mathématique de la communication vise à analyser dans quelles conditions un canal donné, soumis à un certain bruit, peut, ou pas, transmettre un message donné. Deux théorèmes de Shannon (1948) répondent ainsi aux questions suivantes :

a) À quelle vitesse est-il possible de transmettre un message ?

b) En présence de bruit, est-il possible de transmettre un message de manière fiable ?

Si le canal permet de diffuser c symboles par unité de temps, il semble évident qu'on peut transmettre un message de N symboles pendant un temps N/c, mais peut-on faire mieux ? Ensuite, comment détecter une mauvaise transmission de certains symboles et, éventuellement, les corriger ?

Le présupposé de base de la théorie est que les messages à transmettre, du fait-même de leur origine, ne sont pas arbitraires. Si c'est un texte, certaines lettres seront plus fréquentes que d'autres ; si c'est l'enregistrement d'une voix ou d'un morceau de musique certaines fréquences seront absentes du signal, sans même tenir compte du fait que les hauts-parleurs peuvent ne pas les restituer ou l'oreille humaine les percevoir.

Dans son article, Shannon (1948) propose une mesure de la « quantité d'information » contenue dans un message, qu'il appelle *entropie*. Plus exactement, il s'agit de la quantité d'information contenue dans l'ensemble des signaux susceptibles

d'être transmis. Sa définition est de nature probabiliste et son étude fait l'objet du chapitre 1. Nous y définissons l'entropie d'une variable aléatoire et plusieurs variantes :

– L'entropie conditionnelle, qui représente l'information supplémentaire qu'offre une variable aléatoire par rapport à une autre ;
– L'information mutuelle entre deux variables aléatoires, qui représente de façon symétrique l'information que chacune dit de l'autre ;
– Le taux d'entropie d'un processus aléatoire, c'est-à-dire d'une suite de variables aléatoires, qui représente l'information moyenne apportée par chacune d'entre elles.

En particulier, nous calculons le taux d'entropie dans le cas important des *processus markoviens*, dans lesquels chaque variable aléatoire est indépendante de l'ensemble de celles qui précèdent.

Comme ce chapitre est assez théorique, nous l'avons fait précéder d'un chapitre de « rappels » de théorie de probabilités.

Le chapitre 2 est consacré au *codage*, c'est-à-dire aux deux théorèmes de Shannon évoqués plus haut qui permettent d'analyser deux aspects de la transmission d'un signal : la possibilité de la compression, et la possibilité de corriger les erreurs. Ces deux faits sont à la base de toute la théorie moderne des télécommunications numériques.

Dans un dernier chapitre, nous discutons la question de l'*échantillonnage* : c'est la première phase de la numérisation d'un signal qui le voit transformé en une suite de nombres. Le « théorème d'échantillonnage », classiquement attribué à Shannon mais que ce dernier, dans son article (Shannon, 1949), présente comme bien connu, fournit des hypothèses sous lesquelles cet échantillonnage peut se faire sans perte d'information. L'outil principal de ce chapitre est la théorie de Fourier qui permet de séparer les différentes fréquences qui apparaissent dans un signal et une partie importante de ce chapitre est consacrée à en établir les principaux résultats de la théorie des séries de Fourier et de la transformation de Fourier.

Chaque chapitre se clôt par un bon nombre d'exercices, puis par leurs solutions.

La littérature anglophone propose beaucoup d'ouvrages d'introduction à la théorie de l'information. Écrits par des mathématiciens plus compétents que moi en théorie de l'information, ces livres sont souvent excellents, plus complets, et vont parfois beaucoup plus loin. En particulier, le livre de Cover & Thomas

(2006) m'a été très utile, tant pour la présentation générale que pour de nombreux exercices, et les lecteur·ices qui sauront en profiter reconnaîtront ma dette à son égard. J'espère que le présent livre, de taille et d'ambition limitée, pourra servir d'introduction aimable à ces belles questions.

J'ai enseigné ce cours pendant trois années à l'université de Paris (ex-Diderot), au sein du Master 1 maths-info. Je remercie Georges Skandalis et Justin Salez de m'avoir confié les notes et des énoncés d'exercices qu'ils utilisaient pour ce cours. Je remercie aussi Guillaume Garrigos pour avoir assuré diligemment les séances de travaux dirigés et pour avoir insisté que les arguments que je donnais méritaient souvent de plus amples détails. Je remercie enfin les étudiantes et les étudiantes du master pour leur participation, en particulier au cours de l'année universitaire 2020–2021 pendant laquelle la pandémie de CoVid-19 les a contraint d'étudier à distance.

CHAPITRE 0

ÉLÉMENTS DE THÉORIE DES PROBABILITÉS

Ce chapitre a pour but de rappeler quelques définitions et résultats élémentaires en théorie des probabilités discrètes.

On doit à Kolmogorov (1956) (la première édition, en allemand, date de 1933) d'avoir fondé la théorie des probabilités sur la base de l'intégrale de Lebesgue. Les variables aléatoires discrètes que nous considérons dans tout ce petit livre ne nécessitent pas un tel bagage et, dans la plupart des cas, les calculs résulteront de manipulations de sommes finies. Parfois, les variables aléatoires discrètes peuvent prendre une infinité de valeurs et les sommes finies doivent alors être remplacées par des séries ou plutôt par des familles sommables, car leur ensemble d'indices n'est pas naturellement bien ordonné. Le premier paragraphe rappelle cette théorie ; il est peut-être malin de ne pas y prêter une trop grande attention.

Nous donnons ensuite une définition formelle, un peu trop formelle même, d'un espace probabilisé et d'une variable aléatoire discrète sur un tel espace. Pour nous éviter des contorsions liées à d'éventuels évènements de probabilité nulle, j'ai été conduit à supposer l'univers « complet »pour la probabilité considérée.

La section suivante rappellent les définitions de variables aléatoires (discrètes), de leur loi, leur espérance et leur variance (quand elles existent).

Nous rappelons enfin la notion d'indépendance, cruciale en théorie des probabilités. Elle est relativement élémentaire en ce qui concerne l'indépendance de deux évènements, un peu plus subtile lorsqu'il s'agit d'indépendance de deux variables aléatoires. On termine cette section par les notions d'espérance et de variance conditionnelle.

0.1. Familles sommables

On va être amenés à manipuler des sommes infinies, indexées par un ensemble qui n'est pas forcément l'ensemble des entiers, ni en bijection évidente avec l'ensemble des entiers. La théorie des familles sommables a pour but de préciser dans quel contexte ces sommes existent et de les calculer.

Définition **(0.1.1)**. — *Soit* A *un ensemble et soit* $(z_a)_{a\in A}$ *une famille de nombres complexes indexée par l'ensemble* A*. On dit que cette famille est* sommable *s'il existe un nombre complexe* z *tel que, pour tout* $\varepsilon > 0$*, il existe une partie finie* B *de* A *telle que*

$$|z - \sum_{a\in C} z_a| \leqslant \varepsilon$$

pour toute partie finie C *de* A *telle que* $B \subset C$*. On dit alors que* (z_a) *est sommable de somme* z*.*

Si l'ensemble A est fini, la famille $(z_a)_{a\in A}$ est sommable de somme la somme $z = \sum_{a\in A}$ de cette famille finie : dans la définition, il suffit de prendre $B = A$.

Lemme **(0.1.2)**. — *Soit* (z_a) *une famille, soit* z, z' *des nombres complexes. Supposons que la famille* (z_a) *soit sommable de somme* z *et soit sommable de somme* z'*. Alors,* $z = z'$*.*

Compte tenu de ce lemme, il est légitime d'appeler *somme* d'une famille sommable (z_a) l'unique nombre complexe z tel qu'elle soit sommable de somme z ; on la note $\sum_{a\in A} z_a$.

Toute la théorie des familles sommables vise à donner des moyens de calculer cette somme, en particulier de justifier sous quelles conditions elle se comporte « comme » une somme finie.

Démonstration. — Soit ε un nombre réel > 0. Soit B une partie finie de A telle que $|z - \sum_{a\in C} z_a| \leqslant \varepsilon$ pour toute partie finie C contenant B. Choisissons B′ de façon analogue pour z' et posons $C = B \cup B'$. Alors, $|z - \sum_{a\in C} z_a| \leqslant \varepsilon$, et $|z' - \sum_{a\in C} z_a| \leqslant \varepsilon$, de sorte que $|z - z'| \leqslant 2\varepsilon$. Comme ε est arbitraire, cela entraîne $z = z'$. □

Lemme **(0.1.3)**. — *Pour qu'une famille* $(z_a)_{a\in A}$ *de nombres réels positifs soit sommable, il faut et il suffit que les sommes* $\sum_{a\in B} z_a$ *soient majorées, lorsque* B *parcourt l'ensemble*

des parties finies de A. *Alors,*

$$\sum_{a\in \mathrm{A}} z_a = \sup_{\substack{\mathrm{B}\subset \mathrm{A}\\ \mathrm{B}\ \textit{fini}}} \left(\sum_{a\in \mathrm{B}} z_a \right).$$

Lorsque ces sommes ne sont pas majorées, on pose $\sum_{a\in \mathrm{A}} z_a = +\infty$.

Démonstration. — Soit z la borne supérieure de l'ensemble des sommes $\sum_{a\in \mathrm{B}} z_a$, où B parcourt l'ensemble des parties finies de A. Soit $\varepsilon > 0$. Soit B une partie finie de A telle que $z - \varepsilon < \sum_{a\in \mathrm{B}} z_a \leqslant z$. Soit C une partie finie de A telle que $\mathrm{B} \subset \mathrm{C}$. On a $\sum_{a\in \mathrm{C}} z_a \leqslant z$, par définition de z. Par ailleurs, comme $z_a \geqslant 0$ pour tout $a \in \mathrm{A}$, on a

$$\sum_{a\in \mathrm{C}} z_a = \sum_{a\in \mathrm{B}} z_b + \sum_{a\in \mathrm{C}-\mathrm{B}} z_a \geqslant \sum_{a\in \mathrm{B}} z_b \geqslant z - \varepsilon.$$

Par conséquent, $|z - \sum_{a\in \mathrm{C}} z_a| \leqslant \varepsilon$. Cela démontre que la famille $(z_a)_{a\in \mathrm{A}}$ est sommable, de somme z. □

0.1.4. — Donnons quelques propriétés des familles sommables.

a) *Si les familles* $(z_a)_{a\in \mathrm{A}}$ *et* $(z'_a)_{a\in \mathrm{A}}$ *sont sommables, il en est de même de la famille* $(z_a + z'_a)_{a\in \mathrm{A}}$, *et l'on a*

$$\sum_{a\in \mathrm{A}} (z_a + z'_a) = \sum_{a\in \mathrm{A}} z_a + \sum_{a\in \mathrm{A}} z'_a.$$

Posons $z = \sum_{a\in \mathrm{A}} z_a$ et $z' = \sum_{a\in \mathrm{A}} z'_a$. Soit $\varepsilon > 0$. Soit B une partie finie de A telle que $|z - \sum_{a\in \mathrm{C}} z_a| < \varepsilon/2$ pour toute partie finie C de A telle que $\mathrm{B} \subset \mathrm{C}$. De même, soit B′ une partie finie de A telle que $|z' - \sum_{a\in \mathrm{C}} z'_a| < \varepsilon/2$ pour toute partie finie C de A telle que $\mathrm{B} \subset \mathrm{C}$. L'ensemble $\mathrm{B} \subset \mathrm{B}'$ est fini ; de plus, pour toute partie finie C de A telle que $\mathrm{B} \subset \mathrm{B}' \subset \mathrm{C}$, on a

$$|(z + z') - \sum_{a\in \mathrm{C}} (z_a + z'_a)| \leqslant |z - \sum_{a\in \mathrm{C}} z_a| + |z' - \sum_{a\in \mathrm{C}} z'_a| < \varepsilon/2 + \varepsilon/2 = \varepsilon.$$

Cela démontre que la famille $(z_a + z'_a)_{a\in \mathrm{A}}$ est sommable et que sa somme est égale à $z + z'$.

b) *Soit* λ *un nombre complexe. Si la famille* $(z_a)_{a\in \mathrm{A}}$ *est sommable, il en est de même de la famille* $(\lambda z_a)_{a\in \mathrm{A}}$, *et l'on a*

$$\sum_{a\in \mathrm{A}} \lambda z_a = \lambda \sum_{a\in \mathrm{A}} z_a.$$

Soit $\varepsilon > 0$. Soit $z = \sum_{a\in A} z_a$. Soit B une partie finie de A telle que pour toute partie finie C de A telle que $B \subset C$, on ait $|z - \sum_{a\in C} z_a| < \varepsilon/(1+|\lambda|)$. Alors, pour toute telle partie C, on a

$$|\lambda z - \sum_{a\in C} \lambda z_a| = |\lambda||z - \sum_{a\in C} z_a| < \varepsilon \frac{|\lambda|}{1+|\lambda|} < \varepsilon,$$

ce qui démontre que la famille $(\lambda z_a)_{a\in A}$ est sommable et que sa somme est égale à λz.

c) *Si la famille $(z_a)_{a\in A}$ est sommable, il en est de même de la famille $(\overline{z_a})_{a\in A}$, et l'on a*

$$\sum_{a\in A} \overline{z_a} = \overline{\sum_{a\in A} z_a}.$$

Soit $\varepsilon > 0$. Soit $z = \sum_{a\in A} z_a$. Soit B une partie finie de A telle que pour toute partie finie C de A telle que $B \subset C$, on ait $|z - \sum_{a\in C} z_a| < \varepsilon$. Alors, pour toute telle partie C, on a

$$|\overline{z} - \sum_{a\in C} \overline{z_a}| = |z - \sum_{a\in C} z_a| < \varepsilon,$$

ce qui démontre que la famille $(\overline{z_a})_{a\in A}$ est sommable et que sa somme est égale à $\overline{z}$.

Proposition **(0.1.5)**. — a) (Critère de Cauchy) *Pour qu'une famille $(z_a)_{a\in A}$ soit sommable, il faut et il suffit que pour tout $\varepsilon > 0$, il existe une partie finie* B *de* A *telle que l'on ait $|\sum_{a\in C} z_a| \leqslant \varepsilon$ pour toute partie finie* C *de* A *qui est disjointe de* B.

b) *Pour qu'une famille $(z_a)_{a\in A}$ soit sommable, il faut et il suffit qu'il existe un nombre réel* M *tel que $|\sum_{a\in B} z_a| \leqslant M$ pour toute partie finie* B *de* A.

Démonstration. — a) La nécessité de ce critère est tout à fait semblable à celle du critère de Cauchy pour les séries. Supposons que la famille (z_a) soit sommable de somme z. Soit $\varepsilon > 0$; choisissons une partie finie B de A telle que $|z - \sum_{a\in C} z_a| \leqslant \varepsilon/2$ pour toute partie finie C de A contenant B. Soit alors une partie finie C de A qui est disjointe de B ; on a

$$|\sum_{a\in C} z_a| = |\sum_{a\in B\cup C} z_a - \sum_{a\in B} z_a| \leqslant |\sum_{a\in B\cup C} z_a - z| + |\sum_{a\in B} z_a - z| \leqslant 2\varepsilon/2 = \varepsilon.$$

Pour démontrer que cette condition est suffisante, définissons par récurrence une suite croissante (B_n) de parties finies de A en posant $B_0 = \emptyset$, puis, si $n \geqslant 1$ est tel que B_{n-1} est définie, prenons pour partie B_n une partie finie de A contenant B_{n-1} telle que l'on ait $|\sum_{a\in C} z_a| \leqslant 1/n$ pour toute partie finie C de A qui est

disjointe de B_n. Posons alors, pour tout entier n, $u_n = \sum_{a\in B_n} z_a$. Si m et n sont des entiers tels que $n \geqslant m \geqslant 1$, et l'on a

$$|u_m - u_n| = |\sum_{a\in B_n} z_a - \sum_{a\in B_m} z_a| = |\sum_{a\in B_n - B_m} z_a| \leqslant \frac{1}{m}.$$

Ainsi, la suite (u_n) de nombres complexes vérifie le critère de Cauchy, donc converge dans $\mathbf{C}$; notons u sa limite. Faisant tendre n vers $+\infty$, on en déduit l'inégalité $|u_m - u| \leqslant 1/m$ pour tout entier $m \geqslant 1$.

Démontrons que la famille (z_a) est sommable de somme z. Soit $\varepsilon > 0$, soit m un entier tel que $\frac{2}{m} < \varepsilon$. Soit C une partie finie de A contenant B_m ; on a

$$|u - \sum_{a\in C} z_a| = |(u - u_m) - \sum_{a\in C - B_m} z_a| \leqslant |u - u_m| + |\sum_{a\in C - B_m} z_a| \leqslant \frac{1}{m} + \frac{1}{m} \leqslant \varepsilon.$$

Cela prouve le résultat voulu.

b) La condition est nécessaire. Supposons en effet que la famille $(z_a)_{a\in A}$ soit sommable, de somme z, et soit C_1 une partie finie de A telle que $|z - \sum_{a\in C} z_a| < 1$ pour toute partie finie C de A telle que $C_1 \subset C$. Soit alors B une partie finie de A. L'ensemble $B \cup C_1$ est fini, et l'on a

$$\sum_{a\in B} z_a = z - z + \sum_{a\in B\cup C_1} z_a - \sum_{a\in C_1 - B} z_a,$$

de sorte que

$$|\sum_{a\in B} z_a| \leqslant |z| + |z - \sum_{a\in B\cup C_1} z_a| + \sum_{a\in C_1 - B} |z_a| \leqslant |z| + 1 + \sum_{a\in C_1} |z_a|.$$

Cela prouve la majoration voulue, avec $M = |z| + 1 + \sum_{a\in C_1} |z_a|$.

Démontrons inversement que cette condition est suffisante. On commence par traiter le cas où la famille $(z_a)_{a\in A}$ est à valeurs réelles positives. Par hypothèse, la famille $(\sum_{a\in B} z_a)_B$, indexée par l'ensemble des parties finies B de A, est majorée ; d'après le lemme 0.1.3, la famille $(z_a)_{a\in A}$ est sommable.

On suppose maintenant que la famille (z_a) est à valeurs réelles. Pour tout $a \in A$, posons $z_a^+ = \sup(z_a, 0)$ et $z_a^- = \sup(-z_a, 0)$, de sorte que $z_a = z_a^+ - z_a^-$. Les deux familles $(z_a^+)_{a\in A}$ et $(z_a^-)_{a\in A}$ sont à termes positifs. Vérifions qu'elles satisfont la condition de l'énoncé. Soit $M > 0$ tel que pour toute partie finie B de A, on ait $|\sum_{a\in B} z_a| \leqslant M$. Soit B une partie finie de A ; soit B^+ l'ensemble des $a \in B$ tels que $z_a \geqslant 0$. Par hypothèse, on a $|\sum_{a\in B^+} z_a| \leqslant M$; comme $z_a^+ = z_a$ si $a \in B^+$ et $z_a^+ = 0$

sinon, on a donc

$$|\sum_{a\in B} z_a^+| = |\sum_{a\in B^+} z_a| \leqslant M.$$

On démontre de même que $|\sum_{a\in B} z_a^-| \leqslant M$. Par le premier cas traité, les deux familles $(z_a^+)_{a\in A}$ et $(z_a^-)_{a\in A}$ sont ainsi sommables, et il en est donc de même de la famille $(z_a)_{a\in A}$.

On traite enfin le cas général. Pour tout $a \in A$, posons $x_a = \Re(z_a)$ et $y_a = \Im(z_a)$, de sorte que $z_a = x_a + iy_a$. Soit M un nombre réel tel que pour toute famille finie B de A, on ait $|\sum_{a\in B} z_a| \leqslant M$. Pour toute famille finie B de A, on a donc

$$|\sum_{a\in B} x_a| \leqslant |\sum_{a\in B} x_a + i\sum_{a\in B} y_a| \leqslant M$$

et

$$|\sum_{a\in B} y_a| \leqslant |\sum_{a\in B} x_a + i\sum_{a\in B} y_a| \leqslant M.$$

Cela démontre que les familles $(x_a)_{a\in A}$ et $(y_a)_{a\in A}$ vérifient la condition de l'énoncé. Comme elles sont à valeurs réelles, le cas déjà traité entraîne qu'elles sont sommables. La famille $(z_a)_{a\in A}$ est alors sommable. □

Corollaire **(0.1.6)**. — *Soit* $(z_a)_{a\in A}$ *une famille sommable et soit* B *une partie de* A. *La famille* $(z_a)_{a\in B}$ *est alors sommable.*

Supposons, de plus, que la famille (z_a) *soit à termes réels positifs. Alors, on a* $\sum_{a\in B} z_a \leqslant \sum_{a\in A} z_a$.

Démonstration. — La première assertion découle de l'un ou l'autre des deux critères de la proposition 0.1.5. Pour démontrer la seconde, rappelons que $\sum_{a\in B} z_a$ est la borne supérieure, pour toutes les parties finies B_1 de B, des sommes $\sum_{a\in B_1} z_a$, tandis que $\sum_{a\in A} z_a$ est la borne supérieure, pour toutes les parties finies A_1 de A, des sommes $\sum_{a\in A_1} z_a$. On a donc $\sum_{a\in B_1} z_a \leqslant \sum_{a\in A} z_a$ pour toute partie finie B_1 de B. Par suite, $\sum_{a\in B} z_a \leqslant \sum_{a\in A} z_a$. □

Remarque **(0.1.7)**. — Soit $(z_a)_{a\in A}$ une famille sommmable de nombres complexes. Soit n un entier naturel tel que $n \geqslant 1$ et appliquons le critère de Cauchy avec $\varepsilon = 1/n$. Il existe une partie finie B_n de A telle que pour tout $a \in A - B_n$, on a $|z_a| \leqslant 1/n$. Soit B la réunion des B_n ; c'est une partie dénombrable de A. Si $a \in A - B$, alors $|z_a| \leqslant 1/n$ pour tout n, donc $|z_a| = 0$.

Autrement dit, le *support* de la famille (z_a), c'est-à-dire l'ensemble des $a \in A$ tels que $z_a \neq 0$, est dénombrable.

Proposition **(0.1.8)**. — *Soit* A *un ensemble et soit* $(z_a)_{a\in A}$ *une famille sommable de nombres complexes.*

a) *Soit* $(A_1,\dots,A_n)$ *une partition finie de* A. *Pour tout* $j\in\{1,\dots,n\}$, *la famille* $(z_a)_{a\in A_j}$ *est sommable. De plus, on a*

$$\sum_{j=1}^{n}\left(\sum_{a\in A_j} z_a\right)=\sum_{a\in A} z_a.$$

b) *Soit* $\varphi : A\longrightarrow B$ *une application. Pour tout* $b\in B$, *la famille* $(z_a)_{a\in\varphi^{-1}(b)}$ *est sommable ; notons* u_b *sa somme. La famille* $(u_b)_{b\in B}$ *est sommable et sa somme est égale à* $\sum_{a\in A} z_a$. *Autrement dit, on a*

$$\sum_{b\in B}\left(\sum_{a\in\varphi^{-1}(b)} z_a\right)=\sum_{a\in A} z_a.$$

L'assertion *a*) est un cas particulier de l'assertion *b*), appliquée au cas où $B=\{1,\dots,n\}$ et φ est l'application qui vaut j sur A_j. Néanmoins, nous devons la démontrer comme une étape intermédiaire.

Démonstration. — Le corollaire 0.1.6 entraîne que les familles $(z_a)_{a\in A_j}$ (pour $j\in\{1,\dots,n\}$) ou $(z_a)_{a\in\varphi^{-1}(b)}$ (pour $b\in B$) sont sommables.

a) Pour $j\in\{1,\dots,n\}$, posons $u_j=\sum_{a\in A_j} z_a$. Soit $\varepsilon>0$ et soit ε' un nombre réel tel que $n\varepsilon'\leqslant\varepsilon$. Pour tout $j\in\{1,\dots,n\}$, il existe par définition de u_j une partie finie B_j de A_j telle que pour toute partie finie C_j de A_j telle que $B_j\subset C_j$, on ait $|u_j-\sum_{a\in C_j}|\leqslant\varepsilon'$. Soit B la réunion des B_j, pour $j\in\{1,\dots,n\}$ et soit C une partie finie de A contenant B ; pour $j\in\{1,\dots,n\}$, posons $C_j=C\cap A_j$, de sorte que $(C_j)_{1\leqslant j\leqslant n}$ est une partition de C et que l'on a $B_j\subset C_j$ pour tout j. Alors

$$\begin{aligned}\Big|\sum_{j=1}^{n} u_j-\sum_{a\in C} z_a\Big| &= \Big|\sum_{j=1}^{n}\Big(u_j-\sum_{a\in C_j} z_a\Big)\Big|\\ &\leqslant \sum_{j=1}^{n}\Big|u_j-\sum_{a\in C_j} z_a\Big|\\ &\leqslant n\varepsilon'\leqslant\varepsilon.\end{aligned}$$

Cela entraîne l'égalité voulue.

b) Démontrons que la famille $(u_b)_{b\in B}$ est sommable et que sa somme est égale à $z = \sum_{a\in A} z_a$. Soit $\varepsilon > 0$. D'après la définition de z, il existe une partie finie A_1 de A telle que $|z - \sum_{a\in C} z_a| \leqslant \varepsilon/2$ pour toute partie finie C de A telle que $A_1 \subset C$.

Comme dans la preuve du critère de Cauchy, il en découle aussi que pour toute partie A′ de A qui est disjointe de A_1, on a $|\sum_{a\in A'} z_a| \leqslant \varepsilon$. Posons en effet $z' = \sum_{a\in A'} z_a$. Soit $\delta > 0$ et soit A'_1 une partie finie de A′ telle que $|z' - \sum_{a\in C'} z_a| \leqslant \delta$ pour toute partie finie C′ de A′ telle que $A'_1 \subset C'$. En écrivant

$$z' = (z' - \sum_{a\in C'} z_a) + (z - \sum_{a\in A_1} z_a) - (z - \sum_{a\in A_1\cup C'} z_a),$$

on en déduit que $|z'| \leqslant \delta + \varepsilon$. Comme δ est arbitraire, on a donc $|z'| \leqslant \varepsilon$.

Soit $B_1 = \varphi(A_1)$ et soit C une partie finie de B qui contient B_1. D'après ce qui précède, on a $\sum_{b\in C} u_b = \sum_{a\in\varphi^{-1}(C)} z_a$, et $\varphi^{-1}(C)$ contient $\varphi^{-1}(B) = \varphi^{-1}(\varphi(A))$, donc contient A. Par ailleurs, le premier cas, appliqué à la partition $(\varphi^{-1}(b))_{b\in C}$ de $\varphi^{-1}(C)$, entraîne l'égalité

$$\sum_{b\in C} u_b = \sum_{a\in\varphi^{-1}(C)} z_a.$$

Appliqué à la partition $(\varphi^{-1}(C), A - \varphi^{-1}(C))$ de A, il entraîne aussi l'égalité

$$z = \sum_{a\in A} z_a = \sum_{a\in\varphi^{-1}(C)} z_a + \sum_{a\in A-\varphi^{-1}(C)} z_a,$$

de sorte que

$$z - \sum_{b\in C} u_b = \sum_{a\in A-\varphi^{-1}(C)} z_a.$$

Si $a \in A_1$, alors $\varphi(a) \in B_1$, donc $\varphi(a) \in C$, ce qui prouve que $A_1 \subset \varphi^{-1}(C)$; autrement dit, $A - \varphi^{-1}(C)$ est disjoint de A_1. Par conséquent, le membre de droite de l'égalité précédente est majoré, en valeur absolue, par ε. On a donc $|z - \sum_{b\in C} u_b| \leqslant \varepsilon$.

Cela prouve que la famille $(u_b)_{b\in B}$ est sommable et que sa somme est z. □

0.2. Probabilités

0.2.1. — La théorie des probabilités est aujourd'hui formalisée dans le cadre de la théorie de la mesure. On se donne (imaginons-le fixé une fois pour toutes) un ensemble Ω, un ensemble $\mathscr{E}$ de parties de Ω et une application $\mathbf{P} : \mathscr{E} \to [0; 1]$.

L'ensemble Ω est appelé l'univers et les éléments de $\mathscr{E}$ des *évènements* ; si A est un évènement, $\mathbf{P}(A)$ est sa *probabilité*.

L'ensemble $\mathscr{E}$ des évènements et la probabilité $\mathbf{P}$ sont supposées satisfaire les axiomes suivants.

(P_1) On a $\Omega \in \mathscr{E}$;

(P_2) La réunion $\bigcup_{n\in\mathbf{N}} A_n$ d'une suite (A_n) d'évènements est un évènement ;

(P_3) Si A est un évènement, alors $\Omega - A$ est un évènement.

Ces trois premiers axiomes s'énoncent en disant que $\mathscr{E}$ est une *tribu* sur l'univers Ω.

Compte tenu de la formule

$$\bigcap_{n\in N} A_n = \Omega - \bigcup_{n\in\mathbf{N}} (\Omega - A_n),$$

l'intersection $\bigcap_{n\in N} A_n$ d'une suite d'évènements est aussi un évènement. En appliquant ces propriétés à une suite n'ayant que deux termes distincts A et B, on en déduit que si A et B sont des évènements, alors $A \cup B$ et $A \cap B$ sont des évènements.

Les trois axiomes supplémentaires concernent la probabilité $\mathbf{P}$ et s'énoncent en disant que $\mathbf{P}$ est une *mesure* positive de masse totale 1 sur la tribu des évènements pour laquelle cette tribu est complète.

(P_4) On a $\mathbf{P}(\Omega) = 1$;

(P_5) Si (A_n) est une suite d'évènements deux à deux disjoints, alors $\mathbf{P}(\bigcup_{n\in\mathbf{N}} A_n) = \sum_{n\in\mathbf{N}} \mathbf{P}(A_n)$.

(P_6) Si A est un évènement tel que $\mathbf{P}(A) = 0$, alors toute partie B de A est un évènement.

En prenant $A_n = \emptyset$ pour tout n, on voit que $\mathbf{P}(\emptyset) = 0$.

Soit A et B des évènements disjoints et considérons alors la suite $(A, B, \emptyset, \emptyset, \dots)$; on trouve $\mathbf{P}(A \cup B) = \mathbf{P}(A) + \mathbf{P}(B)$.

En prenant $B = \Omega - A$, on trouve $\mathbf{P}(\Omega - A) = 1 - \mathbf{P}(A)$.

Soit A un évènement et soit C un évènement tel que $C \subset A$, alors $A - C = (\Omega - C) \cap A$ est un évènement et l'on a $\mathbf{P}(A - C) = \mathbf{P}(A) - \mathbf{P}(C)$.

Plus généralement, soit A et B des évènements. Alors, $A - (A \cap B)$ est un évènement disjoint de B et l'on a

$$\mathbf{P}(A\cup B) = P((A-(A\cap B))\cup B) = \mathbf{P}(A-(A\cap B))+\mathbf{P}(B) = \mathbf{P}(A)+\mathbf{P}(B)-\mathbf{P}(A\cap B).$$

0.2.2. Exemple : probabilités discrètes. — Soit Ω un ensemble dénombrable (par exemple, fini).

Supposons que $\{a\}$ est un évènement, pour tout $a \in \Omega$; posons alors $p_a = \mathbf{P}(\{a\})$. Alors, toute partie de Ω est un évènement et l'on a

$$\mathbf{P}(\mathrm{A}) = \sum_{a \in \mathrm{A}} p_a.$$

En particulier, $1 = \mathbf{P}(\Omega) = \sum_{a \in \Omega} p_a$.

Inversement, soit $p : \Omega \to \mathbf{R}_+$ une application telle que $\sum_{a \in \Omega} p(a) = 1$. Pour toute partie A de Ω, posons $\mathbf{P}(\mathrm{A}) = \sum_{a \in \mathrm{A}} p(a)$. On vérifie que $(\mathfrak{P}(\Omega), \mathbf{P})$ est une probabilité sur Ω.

Supposons l'ensemble Ω fini. La probabilité équiprobable sur Ω est donnée par $p_a = 1/\mathrm{Card}(\Omega)$ pour tout $a \in \Omega$. Dans ce cas, on a $\mathbf{P}(\mathrm{A}) = \mathrm{Card}(\mathrm{A})/\mathrm{Card}(\Omega)$ pour tout évènement A : la théorie des probabilités généralise la combinatoire.

Exemple **(0.2.3)** (Dés). — Un exemple classique serait donné par le tirage d'un dé à 6 faces, de sorte que $\Omega = \{1, \dots, 6\}$. Si le dé est équilibré, on a $p_a = 1/6$ pour tout $a \in \Omega$. La probabilité que la valeur du dé soit paire est la probabilité de l'évènement $\{2, 4, 6\}$, c'est-à-dire $3/6 = 1/2$.

Cet exemple ne permet pas de modéliser une suite de tirages de dés, mais on peut le généraliser. Si l'on souhaite par exemple considérer des tirages de 5 dés à 6 faces (pour étudier le jeu de Yam's, par exemple), on pourra poser $\Omega = \{1, \dots, 6\}^5$: c'est l'ensemble des 5-uplets d'éléments de $\{1, \dots, 6\}$. Si les dés sont équilibrés et indépendants les uns des autres, on aura $p(a_1, \dots, a_5) = 1/6^5$ pour tout élément $(a_1, \dots, a_5) \in \Omega$.

On propose comme exercice de calculer les probabilités d'avoir un Yam's (5 dés identiques), un carré (4 dés identiques), un brelan (3 dés identiques), une paire (2 dés identiques), un full (simultanément un brelan et une paire) ou une suite (5 dés consécutifs).

Lorsqu'on veut s'intéresser à un grand nombre de tirages de dés (équilibrés, indépendants), on peut poser $\Omega = \{1, \dots, 6\}^{\mathbf{N}}$, ensemble dont les éléments sont les suites infinies $(a_0, a_1, \dots,)$ d'éléments de $\{1, \dots, 6\}$. On démontre qu'il est possible de le munir d'une tribu et d'une probabilité de sorte que, pour tout entier n et tout élément $(a_0, \dots, a_{n-1})$, l'ensemble des tirages (x_m) tels que $x_m = a_m$ pour $0 \leqslant m < n$ soit un évènement de probabilité $1/6^n$.

0.3. Variables aléatoires discrètes

Soit $\mathbf{P}$ une probabilité sur un univers Ω.

Définition **(0.3.1)**. — *Une* variable aléatoire discrète *à valeurs dans un ensemble* A *est une application* $X : \Omega \to A$ *qui vérifie les propriétés suivantes :*

a) *Pour tout* $a \in A$, *l'ensemble* $X^{-1}(a) = \{\omega \in \Omega ; X(\omega) = a\}$ *est un évènement, que l'on note* $(X = a)$.

b) *La famille* $(\mathbf{P}(X = a))_{a\in A}$ *est sommable, de somme* 1.

En particulier, l'ensemble des $a \in A$ tels que $\mathbf{P}(X = a) > 0$ est dénombrable, et non vide. Ses éléments seront appelés les *valeurs possibles* (ou, plus simplement, les valeurs) de la variable aléatoire discrète X ; par définition, l'ensemble des $\omega \in \Omega$ tels que $X(\omega)$ n'est pas une valeur possible de X est un évènement de probabilité nulle.

La famille $(\mathbf{P}(X = a))_{a\in A}$ est la *loi* de la variable aléatoire discrète X. Son support est l'ensemble des valeurs de la variable aléatoire discrète X.

Lemme **(0.3.2)**. — a) *Soit* X *et* Y *des variables aléatoires discrètes sur* Ω, *à valeurs dans des ensembles* A *et* B. *Alors l'application* $\omega \mapsto (X(\omega), Y(\omega))$ *est une variable aléatoire discrète sur* Ω, *à valeurs dans* $A \times B$.

b) *Soit* X *une variable aléatoire discrète sur* Ω *à valeurs dans un ensemble* A *et soit* $f : A \to B$ *une application. Alors l'application* $f \circ X$, *plutôt notée* $f(X)$, *est une variable aléatoire discrète sur* Ω, *à valeurs dans* B.

Par exemple, la somme (ou le produit) de deux variables aléatoires discrètes à valeurs dans $\mathbf{C}$ est une variable aléatoire discrète. On applique en effet l'assertion *b*) du lemme à la variable aléatoire (X, Y) et à l'application somme $s : \mathbf{C}^2 \to \mathbf{C}$ (ou à l'application produit $\pi : \mathbf{C}^2 \to \mathbf{C}$).

Démonstration. — a) Posons $Z(\omega) = (X(\omega), Y(\omega))$. Pour $(a, b) \in A \times B$, l'ensemble $Z^{-1}(a, b)$ est égal à $(X = a) \cap (Y = b)$; c'est donc un évènement. Pour toute partie finie C de $A \times B$, il existe des parties finies A_1 de A et B_1 de B telles que $C \subset A_1 \times B_1$. Alors,

$$\sum_{(a,b)\in C} \mathbf{P}(X = a \text{ et } Y = b) \leqslant \sum_{a\in A_1} \sum_{b\in B_1} \mathbf{P}(X = a \text{ et } Y = b) \leqslant \sum_{a\in A_1} \mathbf{P}(X = a) \leqslant 1.$$

Cela prouve que la famille $(\mathbf{P}(X = a \text{ et } Y = b))_{(a,b)\in A\times B}$ est sommable. Pour prouver que sa somme est 1, on applique la proposition 0.1.8 à cette famille et à l'application $(a, b) \mapsto a$. Soit $a \in A$. L'ensemble $(X = a)$ est réunion disjointe de la famille dénombrable d'évènements $(X = a \text{ et } Y = b)$, et d'un ensemble contenu dans l'évènement de probabilité nulle des $\omega \in \Omega$ tels que $Y(\omega)$ ne soit

pas une valeur de Y. Par suite, on a

$$\mathbf{P}(\mathrm{X} = a) = \sum_{b \in \mathrm{B}} \mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b).$$

Alors, la proposition 0.1.8 entraîne que

$$\sum_{(a,b) \in \mathrm{A} \times \mathrm{B}} \mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b) = \sum_{a \text{ß} n \mathrm{A}} \mathbf{P}(\mathrm{X} = a) = 1.$$

b) Soit A' l'ensemble des $a \in \mathrm{A}$ tels que $\mathbf{P}(\mathrm{X} = a) > 0$ et soit $\mathrm{B}' = f(\mathrm{A}')$. L'ensemble B' est une partie dénombrable de B. Pour tout $b \in \mathrm{B}$, l'ensemble $f(\mathrm{X})^{-1}(b)$ est la réunion disjointe des ensembles $\mathrm{X}^{-1}(a)$, où a parcourt $f^{-1}(b)$; c'est la réunion disjointe de la famille dénombrable des $\mathrm{X}^{-1}(a)$, pour $a \in \mathrm{A}' \cap f^{-1}(b)$ et d'un ensemble contenu dans $\mathrm{X}^{-1}(\mathrm{A} - \mathrm{A}')$ qui est de probabilité nulle. Par suite, $f(\mathrm{X})^{-1}(b)$ est un évènement. Cela prouve que $f(\mathrm{X})$ est une variable aléatoire. □

0.3.3. Exemples de lois. —

a) On dit que X suit une *loi uniforme* si l'ensemble A des valeurs de X est fini et que l'on a $\mathbf{P}(\mathrm{X} = a) = 1/\mathrm{Card}(\mathrm{A})$ pour tout $a \in \mathrm{A}$. On dit aussi que X est une variable aléatoire uniforme sur A. Lorsque A ne possède qu'un élément, a, on dit que la variable aléatoire X est *certaine*.

b) Lorsque l'ensemble des valeurs de X est égal à $\{0, 1\}$, la loi de X est caractérisé par $p = \mathbf{P}(\mathrm{X} = 1)$; on a alors en effet $\mathbf{P}(\mathrm{X} = 0) = 1 - p$. On dit que X suit une *loi de Bernoulli* de paramètre p.

c) Soit p un nombre réel dans $[0; 1]$. Une variable aléatoire X suit une *loi géométrique* de paramètre p si elle prend ses valeurs dans $\mathbf{N}^*$ et si $\mathbf{P}(\mathrm{X} = n) = (1 - p)p^{n-1}$ pour tout entier $n \geqslant 1$.

d) Soit p un nombre réel positif. Une variable aléatoire X suit une *loi de Poisson* de paramètre p si elle prend ses valeurs dans $\mathbf{N}$ et si $\mathbf{P}(\mathrm{X} = n) = e^{-p}p^n/n!$ pour tout entier n.

0.3.4. Espérance. —

Soit X une variable aléatoire discrète à valeurs dans $\mathbf{C}$.

Supposons d'abord que X est à valeurs réelles, positives ou nulles. On appelle alors espérance de X la somme (dans $[0; +\infty]$) de la famille $(a\mathbf{P}(\mathrm{X} = a))$ de nombres réels positifs ou nuls ; on la note $\mathbf{E}(\mathrm{X})$.

Dans le cas général, on dit que X admet une *espérance* si la famille $(a\mathbf{P}(\mathrm{X} = a))_{a\in\mathbf{C}}$ est sommable ; l'espérance de X est alors la somme, notée $\mathbf{E}(\mathrm{X})$, de cette famille.

Si X admet une espérance, l'ensemble de ses valeurs possibles, c'est-à-dire l'ensemble des $a \in \mathbf{C}$ tels que $\mathbf{P}(\mathrm{X} = a) > 0$, est dénombrable.

0.3.5. — L'espérance vérifie les propriétés suivantes.

a) *Si* X *admet une espérance, alors* tX *admet une espérance pour tout nombre complexe* t*, et on a* $\mathbf{E}(t\mathrm{X}) = t\mathbf{E}(\mathrm{X})$.

Si $t = 0$, la variable tX est certaine, de valeur 0, et $\mathbf{E}(t\mathrm{X}) = 0$. Sinon, pour tout nombre complexe a, on a $\mathbf{P}(t\mathrm{X} = a) = \mathbf{P}(\mathrm{X} = a/t)$, donc $a\mathbf{P}(t\mathrm{X} = a) = t(a/t)\mathbf{P}(\mathrm{X} = a/t)$. La famille $((a/t)\mathbf{P}(\mathrm{X} = a/t))_{a\in\mathbf{C}}$ diffère de la famille $(a\mathbf{P}(\mathrm{X} = a))_{a\in\mathbf{C}}$ par le reparamétrage $a \mapsto a/t$; elle est donc sommable et de même somme, à savoir $\mathbf{E}(\mathrm{X})$. Par suite, la famille $(a\mathbf{P}(t\mathrm{X} = a))_{a\in\mathbf{C}}$ est sommable, de somme $t\mathbf{E}(\mathrm{X})$.

b) *Si des variables aléatoires discrètes* X *et* Y *admettent une espérance, alors la variable aléatoire discrète* X+Y *admet une espérance et on a* $\mathbf{E}(\mathrm{X}+\mathrm{Y}) = \mathbf{E}(\mathrm{X})+\mathbf{E}(\mathrm{Y})$.

Soit A l'ensemble des valeurs de la variable aléatoire X, c'est-à-dire l'ensemble des $a \in \mathbf{C}$ tels que $\mathbf{P}(\mathrm{X} = a) > 0$; comme la famille $(a\mathbf{P}(\mathrm{X} = a))_{a\in\mathbf{C}}$ est sommable, l'ensemble A est dénombrable. De même, l'ensemble B des valeurs de la variable aléatoire Y est dénombrable. Soit $s : \mathbf{C}\times\mathbf{C} \to \mathbf{C}$ l'application somme, donnée par $s(a, b) = a + b$ et soit $\mathrm{C} = s(\mathrm{A}\times\mathrm{B}) = \mathrm{A} + \mathrm{B}$; l'ensemble C est une partie dénombrable de $\mathbf{C}$.

Pour $c \in \mathbf{C}$, l'ensemble $(\mathrm{X} + \mathrm{Y})^{-1}(c)$ est la réunion disjointe des évènements $\mathrm{X}^{-1}(a) \cap \mathrm{Y}^{-1}(b)$, où (a, b) parcourt l'ensemble des couples $(a, b) \in \mathrm{A}\times\mathrm{B}$ tels que $a + b = c$, ainsi que d'une partie de l'évènement $\mathrm{X}^{-1}(\complement\mathrm{A}) \cap \mathrm{Y}^{-1}(\complement\mathrm{B})$. Comme ce dernier évènement est de probabilité nulle, chacune de ses parties est un évènement, également de probabilité nulle. Cela entraîne que $(\mathrm{X} + \mathrm{Y})^{-1}(c)$ est un évènement et que

$$\mathbf{P}(\mathrm{X} + \mathrm{Y} = c) = \sum_{\substack{(a,b)\in\mathrm{A}\times\mathrm{B}\\ a+b=c}} \mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b) = \sum_{\substack{(a,b)\in\mathbf{C}\times\mathbf{C}\\ a+b=c}} \mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b).$$

Démontrons que la famille $(a\mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b))_{(a,b)\in\mathbf{C}\times\mathbf{C}}$ est sommable de somme $\mathbf{E}(\mathrm{X})$. Soit K une partie finie de $\mathbf{C}\times\mathbf{C}$ et soit K_1 l'ensemble des $a \in \mathrm{A}$ tels

qu'il existe $b \in \mathbf{C}$ tel que $(a, b) \in \mathrm{K}$. On a

$$\sum_{(a,b)\in \mathrm{K}} |a\mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b)| = \sum_{a\in \mathrm{K}_1} |a| \sum_{\substack{b\in\mathbf{C}\\(a,b)\in\mathrm{K}}} \mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b)$$
$$\leqslant \sum_{a\in \mathrm{K}_1} |a|\mathbf{P}(\mathrm{X} = a) \leqslant \mathbf{E}(|\mathrm{X}|),$$

ce qui prouve que la famille considérée est sommable. Appliquons la proposition 0.1.8 à l'application $(a, b) \mapsto a$ de $\mathbf{C} \times \mathbf{C}$ dans $\mathbf{C}$; il vient

$$\sum_{(a,b)\in\mathbf{C}\times\mathbf{C}} a\mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b) = \sum_{a\in\mathbf{C}} a\Big(\sum_{b\in\mathbf{C}} \mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b)\Big).$$

Pour $a \in \mathbf{C}$, l'évènement $(\mathrm{X} = a)$ est réunion disjointe de la famille dénombrable d'évènements $(\mathrm{X} = a \text{ et } \mathrm{Y} = b)$, pour $b \in \mathrm{B}$, et de l'évènement $(\mathrm{X} = a \text{ et } \mathrm{Y} \notin \mathrm{B})$ dont la probabilité est nulle puisqu'il est contenu dans $(\mathrm{Y} \notin \mathrm{B})$. On en déduit l'égalité

$$\mathbf{P}(\mathrm{X} = a) = \sum_{b\in\mathrm{B}} \mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b).$$

Par suite,

$$\sum_{(a,b)\in\mathbf{C}\times\mathbf{C}} a\mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b) = \sum_{a\in\mathbf{C}} a\mathbf{P}(\mathrm{X} = a) = \mathbf{E}(\mathrm{X}).$$

De même, la famille $(b\mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b))_{(a,b)\in\mathbf{C}\times\mathbf{C}}$ est sommable de somme $\mathbf{E}(\mathrm{Y})$. Par suite, la famille $((a + b)\mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b))_{(a,b)\in\mathbf{C}\times\mathbf{C}}$ est sommable, de somme $\mathbf{E}(\mathrm{X}) + \mathbf{E}(\mathrm{Y})$.

Appliquons la proposition 0.1.8 à l'application s. Pour $c \in \mathbf{C}$, la famille $((a + b)\mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b))_{a+b=c}$ est sommable et sa somme est égale à

$$\sum_{\substack{(a,b)\in\mathbf{C}\times\mathbf{C}\\a+b=c}} (a+b)\mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b) = c \sum_{\substack{(a,b)\in\mathbf{C}\times\mathbf{C}\\a+b=c}} \mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b) = c\mathbf{P}(\mathrm{X}+\mathrm{Y} = c).$$

Par suite, la famille $(c\mathbf{P}(X+Y=c))_{c\in\mathbf{C}}$ est sommable et l'on a

$$\begin{aligned}\mathbf{E}(X+Y) &= \sum_{c\in C} c\mathbf{P}(X+Y=c)\\ &= \sum_{c\in\mathbf{C}}\left(\sum_{\substack{(a,b)\in\mathbf{C}\times\mathbf{C}\\ a+b=c}} (a+b)\mathbf{P}(X=a \text{ et } Y=b)\right)\\ &= \sum_{(a,b)\in\mathbf{C}\times\mathbf{C}} (a+b)\mathbf{P}(X=a \text{ et } Y=b)\\ &= \mathbf{E}(X)+\mathbf{E}(Y).\end{aligned}$$

c) *Si* Y *admet une espérance et si* $|X|\leqslant Y$*, alors* X *et* $|X|$ *admettent une espérance et l'on a* $|\mathbf{E}(X)|\leqslant\mathbf{E}(|X|)\leqslant\mathbf{E}(Y)$.

On commence par traiter le cas où l'ensemble A des valeurs de X est fini et formé de nombres réels positifs. Soit $Z=Y-X$. Vérifions que c'est une variable aléatoire. Pour $c\in\mathbf{C}$, l'ensemble $Z^{-1}(c)$ est la réunion disjointe des évènements $(X=a \text{ et } Y=c-a)$, pour $a\in A$, et d'un ensemble contenu dans l'évènement de probabilité nulle $\{X\notin A\}$, qui est donc un évènement. Comme $Y=X+Z$, On a donc $\mathbf{E}(Y)=\mathbf{E}(X)+\mathbf{E}(Z)\geqslant\mathbf{E}(X)$ puisque $Z\geqslant 0$.

Supposons maintenant que X est à valeurs réelles et positives, c'est-à-dire $0\leqslant X\leqslant Y$. Soit A un ensemble fini dans $\mathbf{C}$; soit $\varphi_A:\mathbf{C}\to\mathbf{C}$ la fonction telle que $\varphi_A(a)=0$ si $a\notin A$ et $\varphi_A(a)=a$ sinon. Soit X_A la variable aléatoire discrète $\varphi_A(X)$; on a $X_A(\omega)=X(\omega)$ si $X(\omega)\in A$ et $X_A(\omega)=0$ sinon.

On a évidemment $0\leqslant X_A\leqslant X\leqslant Y$. En appliquant le cas traité à la variable aléatoire discrète X_A, on obtient $\mathbf{E}(X_A)\leqslant\mathbf{E}(Y)$. Par ailleurs, on a $\mathbf{P}(X_A=a)=\mathbf{P}(X=a)$ si $a\in A-\{0\}$ et $\mathbf{P}(X_A=a)=0$ si $a\notin A$. Autrement dit, $a\mathbf{P}(X_A=a)=a\mathbf{P}(X=a)$ pour tout $a\in A$, si bien que $\sum_{a\in A} a\mathbf{P}(X=a)=\mathbf{E}(X_A)\leqslant\mathbf{E}(Y)$. La famille $(a\mathbf{P}(X=a))_{a\in\mathbf{R}_+}$ est donc sommable, et sa somme est majorée par $\mathbf{E}(Y)$. Cela entraîne que X admet une espérance et que $\mathbf{E}(X)\leqslant\mathbf{E}(Y)$.

Traitons maintenant le cas général. D'après le cas traité, $|X|$ possède une espérance, et $\mathbf{E}(|X|)\leqslant\mathbf{E}(Y)$. D'autre part, on peut décomposer X sous la forme $X=\Re(X)^+-\Re(X)^-+i\Im(X)^+-i\Im(X)^-$ d'une somme de quatre variables aléatoires discrètes, et chacune d'entre elles est majorée par Y. D'après ce qui précède, elles admettent toutes une espérance, si bien que X admet une espérance.

Il reste à démontrer l'inégalité $|\mathbf{E}(X)|\leqslant\mathbf{E}(|X|)$. Pour cela, on applique la proposition 0.1.8 à la famille $(a\mathbf{P}(X=a))$ et à l'application $|\cdot|$ de $\mathbf{C}$ dans $\mathbf{C}$. Pour

tout $r \in \mathbf{R}_+$, $\mathbf{P}(|\mathrm{X}| = r)$ est la réunion disjointe de la famille dénombrable d'évènements $(\mathrm{X} = a)$, où a parcourt l'ensemble des valeurs a de X telles que $|a| = r$, et d'un ensemble de probabilité nulle. On a donc

$$\mathbf{P}(|\mathrm{X}| = r) = \sum_{\substack{a \in \mathrm{A} \\ |a|=r}} \mathbf{P}(\mathrm{X} = a).$$

Alors,

$$\mathbf{E}(\mathrm{X}) = \sum_{a \in \mathbf{C}} a\mathbf{P}(\mathrm{X} = a) = \sum_{r \in \mathbf{R}_+} \sum_{|a|=r} a\mathbf{P}(\mathrm{X} = a).$$

Pour $r \in \mathbf{R}_+$, on a aussi

$$\left| \sum_{|a|=r} a\mathbf{P}(\mathrm{X} = a) \right| \leqslant \sum_{|a|=r} |a|\mathbf{P}(\mathrm{X} = a) = r \sum_{|a|=r} \mathbf{P}(\mathrm{X} = a) = r\mathbf{P}(|\mathrm{X}| = r).$$

Par suite,

$$|\mathbf{E}(\mathrm{X})| \leqslant \sum_{r \in \mathbf{R}_+} r\mathbf{P}(|\mathrm{X}| = r) = \mathbf{E}(|\mathrm{X}|),$$

ce qu'il fallait démontrer.

0.3.6. Moments, variance. — Soit k un entier naturel. On dit que la variable aléatoire discrète X admet un *moment* d'ordre k si la variable aléatoire X^k admet une espérance, ou, c'est équivalent, si l'espérance de la variable aléatoire réelle positive $|\mathrm{X}|^k$ est finie ; cette espérance $\mathbf{E}(\mathrm{X}^k)$ est alors appelée le *moment d'ordre k* de la variable aléatoire X.

Lorsque la variable aléatoire discrète X possède des moments d'ordre 1 et 2, on définit sa *variance* comme $\mathbf{V}(\mathrm{X}) = \mathbf{E}(|\mathrm{X} - \mathbf{E}(\mathrm{X})|^2)$. Comme $|\mathrm{X} - \mathbf{E}(\mathrm{X})|^2 = |\mathrm{X}|^2 - \overline{\mathrm{X}}\mathbf{E}(\mathrm{X}) - \mathrm{X}\overline{\mathbf{E}(\mathrm{X})} + |\mathbf{E}(\mathrm{X})|^2$, On a aussi

$$\mathbf{V}(\mathrm{X}) = \mathbf{E}(|\mathrm{X}|^2) - \mathbf{E}(\overline{\mathrm{X}})\mathbf{E}(\mathrm{X}) - \mathbf{E}(\mathrm{X})\overline{\mathbf{E}(\mathrm{X})} + |\mathbf{E}(\mathrm{X})|^2 = \mathbf{E}(|\mathrm{X}|^2) - |\mathbf{E}(\mathrm{X})|^2.$$

Proposition **(0.3.7).** — *Soit* X *et* Y *des variables aléatoires discrètes à valeurs dans* **C** *qui possèdent un moment d'ordre 2.*

a) (Young) *La variable aléatoire* XY *possède une espérance et l'on a*

$$|\mathbf{E}(\mathrm{XY})| \leqslant \frac{1}{2}\left(\mathbf{E}(|\mathrm{X}|^2) + \mathbf{E}(|\mathrm{Y}|^2)\right).$$

b) (Cauchy–Schwarz) *La variable aléatoire* XY *possède une espérance et l'on a*

$$|\mathbf{E}(XY)| \leqslant \mathbf{E}(|X|^2)^{1/2}\mathbf{E}(|Y|^2)^{1/2}.$$

c) *En particulier, la variable aléatoire* X *possède une espérance et* $|\mathbf{E}(X)| \leqslant \mathbf{E}(|X|^2)^{1/2}$.

d) (Minkowski) *On a*

$$\mathbf{E}(|X+Y|^2)^{1/2} \leqslant \mathbf{E}(|X|^2)^{1/2} + \mathbf{E}(|Y|^2)^{1/2}.$$

Démonstration. — a) Quitte à remplacer X et Y par |X| et |Y|, on les suppose à valeurs réelles positives. Si x et y sont des nombres réels, on a $x^2 + y^2 - 2xy = (x-y)^2 \geqslant 0$, de sorte que $xy \leqslant (x^2+y^2)/2$. qui découle de ce que pour tous nombres réels x et y, Pour tout $\omega \in \Omega$, on a donc

$$|XY(\omega)| = |X(\omega)||Y(\omega)| \leqslant \frac{1}{2}|X(\omega)|^2 + \frac{1}{2}|Y(\omega)|^2,$$

d'où l'inégalité de variables aléatoires réelles positives $|XY| \leqslant \frac{1}{2}(|X|^2 + |Y|^2)$. Puisque X^2 et Y^2 admettent une espérance finie, il en est donc de même de XY, et

$$\mathbf{E}(|XY|) \leqslant \frac{1}{2}\left(\mathbf{E}(|X|^2) + \mathbf{E}(|Y|^2)\right).$$

b) Soit a et b des nombres réels strictement positifs tels que $\mathbf{E}(|X|^2) \leqslant a^2$ et $\mathbf{E}(|Y|^2) \leqslant b^2$. Appliquons l'inégalité de Young aux variables aléatoires X/a et Y/b. On a donc

$$\frac{1}{ab}\mathbf{E}(|XY|) \leqslant \frac{1}{2a^2}\mathbf{E}(|X^2|) + \frac{1}{2b^2}\mathbf{E}(|Y|^2) \leqslant 1,$$

soit encore $\mathbf{E}(|XY|) \leqslant ab$. En faisant tendre a et b vers $\mathbf{E}(|X|^2)^{1/2}$ et $\mathbf{E}(|Y|^2)^{1/2}$, on obtient l'inégalité $\mathbf{E}(|XY|) \leqslant \mathbf{E}(|X|^2)^{1/2}\mathbf{E}(|Y|^2)^{1/2}$.

c) Prenons pour Y la variable aléatoire certaine de valeur 1 ; puisque $\mathbf{E}(1) = 1$, elle admet un moment d'ordre 2 et l'on a $\mathbf{E}(|X|) = \mathbf{E}(|XY|) \leqslant \mathbf{E}(|X|^2)^{1/2}$.

d) On a $|X+Y|^2 \leqslant |X|^2 + 2|X|\,|Y| + |Y|^2$, donc

$$\begin{aligned}\mathbf{E}(|X+Y|^2) &\leqslant \mathbf{E}(|X|^2) + 2\mathbf{E}(|X|\,|Y|) + \mathbf{E}(|Y|^2)\\ &\leqslant \mathbf{E}(|X|^2) + 2\mathbf{E}(|X|^2)^{1/2}\mathbf{E}(|Y|^2)^{1/2} + \mathbf{E}(|Y|^2)\\ &= \left(\mathbf{E}(|X|^2)^{1/2} + \mathbf{E}(|Y|^2)^{1/2}\right)^2,\end{aligned}$$

d'où l'inégalité de Minkowski. □

0.4. Indépendance, espérance conditionnelle

0.4.1. — Soit $\mathbf{P}$ une probabilité sur un univers Ω. Soit A et B des évènements tels que $\mathbf{P}(\mathrm{B}) > 0$; on définit la *probabilité conditionnelle* de A selon B, ou « sachant B », comme

$$\mathbf{P}(\mathrm{A} \mid \mathrm{B}) = \frac{\mathbf{P}(\mathrm{A} \cap \mathrm{B})}{\mathbf{P}(\mathrm{B})}.$$

On observe que $\mathrm{A} \mapsto \mathbf{P}(\mathrm{A} \mid \mathrm{B})$ est une probabilité $\mathbf{P}_{\mathrm{B}}$ sur l'ensemble des évènements de Ω.

On dit que des évènements A et B sont *indépendants* si l'on a $\mathbf{P}(\mathrm{A} \cap \mathrm{B}) = \mathbf{P}(\mathrm{A})\mathbf{P}(\mathrm{B})$. Plus généralement, on dit qu'une suite (A_n) (finie ou infinie) d'évènements est indépendante si pour toute ensemble fini I d'indices, on a

$$\mathbf{P}\Big(\bigcap_{i\in \mathrm{I}} \mathrm{A}_i\Big) = \prod_{i\in \mathrm{I}} \mathbf{P}(\mathrm{A}_i).$$

Proposition **(0.4.2)** (Formule de Bayes). — *Soit* A *et* B *des évènements tels que* $\mathbf{P}(\mathrm{A}) > 0$ *et* $\mathbf{P}(\mathrm{B}) > 0$*. On a*

$$\mathbf{P}(\mathrm{A} \mid \mathrm{B}) = \frac{\mathbf{P}(\mathrm{B} \mid \mathrm{A})\,\mathbf{P}(\mathrm{A})}{\mathbf{P}(\mathrm{B})}.$$

Démonstration. — Par définition, $\mathbf{P}(\mathrm{A} \mid \mathrm{B}) = \mathbf{P}(\mathrm{A} \cap \mathrm{B})/\mathbf{P}(\mathrm{B})$ et $\mathbf{P}(\mathrm{B} \mid \mathrm{A}) = \mathbf{P}(\mathrm{A} \cap \mathrm{B})/\mathbf{P}(\mathrm{A})$. On a donc $\mathbf{P}(\mathrm{B} \mid \mathrm{A})\,\mathbf{P}(\mathrm{A}) = \mathbf{P}(\mathrm{A} \cap \mathrm{B})$, d'où

$$\frac{\mathbf{P}(\mathrm{B} \mid \mathrm{A})\,\mathbf{P}(\mathrm{A})}{\mathbf{P}(\mathrm{B})} = \frac{\mathbf{P}(\mathrm{A} \cap \mathrm{B})}{\mathbf{P}(\mathrm{B})} = \mathbf{P}(\mathrm{A} \mid \mathrm{B}).$$

Cela démontre la formule. □

Proposition **(0.4.3)** (Formule des probabilités totales). — *Soit* (B_n) *une suite (éventuellement finie) d'évènements deux à deux disjoints tels que* $\Omega = \bigcup \mathrm{B}_n$ *et* $\mathbf{P}(\mathrm{B}_n) > 0$ *pour tout n. Pour tout évènement* A*, on a*

$$\mathbf{P}(\mathrm{A}) = \sum_n \mathbf{P}(\mathrm{A} \mid \mathrm{B}_n)\mathbf{P}(\mathrm{B}_n).$$

Démonstration. — Par définition de la probabilité conditionnelle, on a $\mathbf{P}(\mathrm{A} \mid \mathrm{B}_n)\mathbf{P}(\mathrm{B}_n) = \mathrm{P}(\mathrm{A} \cap \mathrm{B}_n)$. Les évènements $\mathrm{A} \cap \mathrm{B}_n$ sont deux à deux disjoints et sa réunion est A puisque $\Omega = \bigcup \mathrm{B}_n$. On a donc $\mathbf{P}(\mathrm{A}) = \sum \mathbf{P}(\mathrm{A} \cap \mathrm{B}_n)$. □

0.4.4. — Soit X et Y des variables aléatoires discrètes. On dit que X et Y sont *indépendantes* si pour tous a, b, on a $\mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b) = \mathbf{P}(\mathrm{X} = a)\mathbf{P}(\mathrm{Y} = b)$.

Démontrons que si X et Y sont à valeurs complexes et admettent une espérance, alors XY admet une espérance et $\mathbf{E}(\mathrm{XY}) = \mathbf{E}(\mathrm{X})\mathbf{E}(\mathrm{Y})$.

Soit C une partie finie de $\mathbf{C}^2$ et soit A, B des parties finies de $\mathbf{C}$ telles que $\mathrm{C} \subset \mathrm{A} \times \mathrm{B}$. Alors,

$$\sum_{(a,b)\in \mathrm{C}} |ab\mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b)| \leqslant \sum_{a\in \mathrm{A}} \sum_{b\in \mathrm{B}} |a||b|\mathbf{P}(\mathrm{X} = a)\mathbf{P}(\mathrm{Y} = b) \leqslant \mathbf{E}(|\mathrm{X}|)\mathbf{E}(|\mathrm{Y}|).$$

Cela démontre que la famille $(ab\mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b))_{(a,b)\in\mathbf{C}^2}$ est sommable. Appliquons alors la proposition 0.1.8 à cette famille et à l'application $(a, b) \mapsto a$ de $\mathbf{C}^2$ dans $\mathbf{C}$.

Soit $a \in \mathbf{C}$. On a

$$\sum_{b\in\mathbf{C}} ab\mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b) = a\mathbf{P}(\mathrm{X} = a) \sum_{b\in\mathbf{C}} b\mathbf{P}(\mathrm{Y} = b) = a\mathbf{P}(\mathrm{X} = a)\mathbf{E}(\mathrm{Y}).$$

Par suite,

$$\sum_{(a,b)\in\mathbf{C}^2} ab\mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b) = \sum_{a\in\mathbf{C}} a\mathbf{P}(\mathrm{X} = a)\mathbf{E}(\mathrm{Y}) = \mathbf{E}(\mathrm{X})\mathbf{E}(\mathrm{Y}).$$

Appliquons maintenant la proposition 0.1.8 à cette famille mais à l'application $(a, b) \mapsto ab$. Soit A l'ensemble des valeurs de X et soit B l'ensemble des valeurs de Y. Soit $c \in \mathbf{C}$. L'évènement $(\mathrm{XY} = c)$ est réunion disjointe de la famille dénombrable d'évènements $(\mathrm{X} = a \text{ et } \mathrm{Y} = b)$, où (a, b) parcourt l'ensemble des couples de $\mathrm{A} \times \mathrm{B}$ tels que $ab = c$, et d'un ensemble contenu dans l'évènement de probabilité nulle $(\mathrm{X} \notin \mathrm{A}) \cup (\mathrm{Y} \notin \mathrm{B})$. Par suite, on a

$$\sum_{\substack{(a,b)\in\mathbf{C}\times\mathbf{C}\\ ab=c}} ab\mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b) = c \sum_{\substack{(a,b)\in\mathbf{C}\times\mathbf{C}\\ ab=c}} \mathbf{P}(\mathrm{X} = a)\mathbf{P}(\mathrm{Y} = b) = c\mathbf{P}(\mathrm{XY} = c),$$

si bien que

$$\mathbf{E}(\mathrm{X})\mathbf{E}(\mathrm{Y}) = \sum_{(a,b)\in\mathbf{C}^2} ab\mathbf{P}(\mathrm{X} = a \text{ et } \mathrm{Y} = b) = \sum_{c\in\mathbf{C}} c\mathbf{P}(\mathrm{XY} = c) = \mathbf{E}(\mathrm{XY}).$$

0.4.5. — Soit X une variable aléatoire discrète qui possède une espérance.

Soit B un évènement tel que $\mathbf{P}(\mathrm{B}) > 0$. Pour tout $a \in \mathbf{C}$, on a $\mathbf{P}(\mathrm{X} = a \mid \mathrm{B}) = \mathbf{P}((\mathrm{X} = a) \cap \mathrm{B})/\mathbf{P}(\mathrm{B}) \leqslant \mathbf{P}(\mathrm{X} = a)/\mathbf{P}(\mathrm{B})$; par suite, la famille $(a\mathbf{P}(\mathrm{X} = a \mid \mathrm{B}))_{a\in\mathbf{C}}$ est sommable. Sa somme est appelée *espérance conditionnelle de* X *relativement à l'évènement* B, et notée $\mathbf{E}(\mathrm{X} \mid \mathrm{B})$.

On peut observer que c'est l'espérance de la variable aléatoire X pour la probabilité $\mathbf{P}_B = \mathbf{P}(\cdot \mid B)$ sur Ω. On en déduit en particulier les propriétés :

a) Pour tout $t \in \mathbf{C}$, on a $\mathbf{E}(tX \mid B) = t\mathbf{E}(X \mid B)$;

b) Si Y est une variable aléatoire discrète qui possède une espérance, il en est de même de $X + Y$ et l'on a $\mathbf{E}(X + Y \mid B) = \mathbf{E}(X \mid B) + \mathbf{E}(Y \mid B)$;

c) Si $|X| \leqslant Y$, alors $|\mathbf{E}(X \mid B)| \leqslant \mathbf{E}(|X| \mid B) \leqslant \mathbf{E}(Y \mid B)$.

0.4.6. — Plus généralement, on dit qu'une suite (X_n) (finie ou infinie) de variables aléatoires discrètes est indépendante ou, par abus, que les variables aléatoires X_n sont indépendantes, si, pour tout n, tout $(a_1, \ldots, a_n)$, on a

$$\mathbf{P}(X_1 = a_1 \text{ et } X_2 = a_2 \text{ et } \ldots \text{ et } X_n = a_n) = \mathbf{P}(X_1 = a_1)\mathbf{P}(X_2 = a_2) \ldots \mathbf{P}(X_n = a_n).$$

Cela revient à dire que pour tout entier n, la variable aléatoire X_n est indépendante de la variable aléatoire discrète $(X_1, \ldots, X_{n-1})$.

Considérons une suite indépendante $(X_1, \ldots, X_n)$ de variables aléatoires discrètes à valeurs complexes. Si elles ont une espérance, alors leur produit $X_1 \ldots X_n$ a également une espérance et

$$\mathbf{E}(X_1 \ldots X_n) = \mathbf{E}(X_1) \ldots \mathbf{E}(X_n).$$

Cela se déduit du cas $n = 2$ par récurrence.

0.4.7. — Soit X et Y des variables aléatoires discrètes ; on suppose que X possède une espérance. On définit alors comme suit une variable aléatoire $\mathbf{E}(X \mid Y)$ sur Ω.

Soit $\omega \in \Omega$. Si $\mathbf{P}(Y = Y(\omega)) = 0$, c'est-à-dire si $Y(\omega)$ n'est pas une valeur de Y, on pose $\mathbf{E}(X \mid Y)(\omega) = 0$. Sinon, on pose $\mathbf{E}(X \mid Y)(\omega) = \mathbf{E}(X \mid Y = Y(\omega))$.

On peut démontrer qu'il s'agit effectivement d'une variable aléatoire discrète, en particulier que pour tout $a \in \mathbf{C}$, l'ensemble des $\omega \in \Omega$ tels que $\mathbf{E}(X \mid Y)(\omega) = a$ est un évènement. On l'appelle l'*espérance conditionnelle de* X *relativement à* Y.

On définit de façon analogue la variance conditionnelle de X relativement à Y, $\mathbf{V}(X \mid Y)$: si $\mathbf{P}(Y = Y(\omega)) = 0$, on pose $\mathbf{V}(X \mid Y)(\omega) = 0$; sinon, on pose $\mathbf{V}(X \mid Y)(\omega) = \mathbf{V}(X \mid Y = Y(\omega))$.

0.5. Exercices

Exercice **(0.5.1)** (Loi uniforme). — Soit $n \in \mathbb{N}^\star$ et X une variable aléatoire *uniforme* sur $\{1, \ldots, n\}$, c'est-à-dire que toutes les probabilités $\mathbf{P}(X = a)$ sont égales, pour $a \in \{1, \ldots, n\}$.

a) Calculer $\mathbf{P}(\mathrm{X} = a)$ pour $a \in \{1, \ldots, n\}$.

b) Calculer la probabilité que X soit un entier pair. Plus généralement, si a est un entier $\geqslant 1$, calculer la probabilité que X soit un multiple de a.

c) Calculer l'espérance de X.

d) Calculer la variance de X.

Exercice **(0.5.2)**. — *a*) Trois prisonniers risquent l'exécution. L'un d'eux apprend de source sûre que l'un des trois a été gracié en dernière minute. Le gardien refuse de lui donner le nom du gracié, mais accepte de lui donner le nom de l'un des condamnés, qui n'est pas le sien. Le prisonnier doit-il se montrer rassuré en entendant le nom d'un des deux autres ?

b) Un jeu télévisé met en scène trois portes ; derrière l'une se trouve une voiture. Le présentateur propose au candidat de désigner celle des trois portes qu'il souhaite ouvrir et ouvre alors une des deux autres portes qui ne masque pas la voiture. Le candidat souhaite gagner la voiture ; doit-il ouvrir la porte qu'il avait initialement désignée, ou bien ouvrir la troisième porte ?

Exercice **(0.5.3)** (Loi de Poisson). — Soit p un nombre réel tel que $p \geqslant 0$. Soit X une variable aléatoire dont la loi est la loi exponentielle de paramètre p : cela signifie que pour tout entier $n \geqslant 0$, on a $\mathbf{P}(\mathrm{X} = n) = e^{-p}p^n/n!$.

a) Calculer l'espérance de X.

b) Calculer l'espérance de X^2 et la variance de X.

c) Démontrer qu'il existe, pour tout entier $k \geqslant 1$, un polynôme L_k de degré k tel que l'espérance de X^k soit égale à $\mathrm{L}_k(p)$.

Exercice **(0.5.4)** (Loi géométrique). — Soit p et q des nombre réels strictement positifs tels que $p + q = 1$. Soit X une variable aléatoire dont la loi est la loi géométrique de paramètre p : cela signifie que pour tout entier $n \geqslant 1$, on a $\mathbf{P}(\mathrm{X} = n) = qp^{n-1}$.

a) Calculer l'espérance de X.

b) Calculer la variance de X.

c) Démontrer qu'il existe, pour tout entier $k \geqslant 1$, un polynôme unitaire S_k de degré k tel que l'espérance de X^k soit égale à $\mathrm{S}_k(p)/q^k$.

Exercice **(0.5.5)**. — Un tricheur dispose d'un dé à 6 faces pipé qui sort 1 avec probabilité $2/3$ et chacune des autres faces avec probabilité $1/15$. Cependant, son dé pipé est dans un sac qui contient aussi deux dés équilibrés (chaque face sort avec probabilité $1/6$). Ces trois dés sont apparemment indiscernables.

a) Notre tricheur prend un des trois dés au hasard. Quelle est la probabilité qu'il ait choisi le dé pipé ? (On pourra noter A la variable aléatoire « le tricheur a choisi le dé pipé » à valeurs vrai/faux.)

b) Il lance le dé qu'il a pris et obtient 1. Conditionnellement à ce résultat, quelle est alors la probabilité qu'il ait choisi le dé pipé ? (On pourra introduire la variable aléatoire X qui donne la valeur du lancer du dé.)

c) Il relance ce dé et obtient de nouveau 1. Quelle est maintenant la probabilité qu'il ait choisi le dé pipé ? (On pourra introduire la variable aléatoire Y qui donne la valeur du deuxième lancer du dé et justifier que X et Y sont indépendantes conditionnellement à A.)

Exercice **(0.5.6)**. — Dans les trois premières questions, on suppose que X et Y sont les résultats de deux lancers indépendants d'un dé à 6 faces, équilibré, et on pose $Z = X + Y$.

a) Calculer la loi de Z.

b) Pour tout $a \in \{1; \dots ; 12\}$, calculer $\mathbf{E}(X \mid Z = a)$.

c) En déduire que $\mathbf{E}(X \mid Z) = Z/2$.

d) Plus généralement, soit X et Y des variables aléatoires discrètes à valeurs complexes, de même loi, et posons $Z = X + Y$. Démontrer que $\mathbf{E}(X \mid Z) = Z/2$.

e) On suppose que X et Y sont indépendantes et suivent une loi de Bernoulli de paramètre p. Calculer $\mathbf{E}(X \mid XY = a)$ pour tout a.

Exercice **(0.5.7)** (Espérance et variance conditionnelles)
Soit X et Y des variables aléatoires discrètes.

a) On suppose que X possède une espérance. Démontrer que $\mathbf{E}(X) = \mathbf{E}(\mathbf{E}(X \mid Y))$.

b) On suppose que X possède une variance. Démontrer que $\mathbf{V}(X) = \mathbf{E}(\mathbf{V}(X \mid Y)) + \mathbf{V}(\mathbf{E}(\mid Y))$.

0.6. Solutions des exercices

Solution de l'exercice (0.5.1). — *a*) Notons p la valeur commune des probabilités $\mathbf{P}(\mathrm{X} = a)$ pour $a \in \{1, \dots, n\}$. On a

$$1 = \mathbf{P}(\mathrm{X} \in \{1, \dots, n\}) = \mathbf{P}(\mathrm{X} = 1) + \mathbf{P}(\mathrm{X} = 2) + \cdots + \mathbf{P}(\mathrm{X} = n) = np,$$

d'où $p = 1/n$.

b) Soit $m = \lfloor n/2 \rfloor$ la partie entière de $n/2$; on a donc $m = n/2$ si n est pair et $m = (n-1)/2$ si n est impair. Les entiers pairs entre 1 et n sont les entiers $2, 4, \dots, 2m$, de sorte que $\mathbf{P}(\mathrm{X} \text{ est pair}) = \mathbf{P}(\mathrm{X} = 2) + \mathbf{P}(\mathrm{X} = 4) + \cdots + \mathbf{P}(\mathrm{X} = 2m) = m/n$.

Par le même argument, $\mathbf{P}(\mathrm{X} \text{ est multiple de } a) = \lfloor n/a \rfloor / n$.

c) On a

$$\begin{aligned}
\mathbf{E}(\mathrm{X}) &= \mathbf{P}(\mathrm{X} = 1) + 2\mathbf{P}(\mathrm{X} = 2) + \cdots + n\mathbf{P}(\mathrm{X} = n) \\
&= (1 + 2 \cdots + n)\frac{1}{n} \\
&= \frac{n(n+1)}{2}\,\frac{1}{n} \\
&= (n+1)/2.
\end{aligned}$$

d) On rappelle la formule $\mathbf{V}(\mathrm{X}) = \mathbf{E}(\mathrm{X}^2) - \mathbf{E}(\mathrm{X})^2$. Or,

$$\begin{aligned}
\mathbf{E}(\mathrm{X}^2) &= \mathbf{P}(\mathrm{X} = 1) + 2^2\mathbf{P}(\mathrm{X} = 2) + \cdots + n^2\mathbf{P}(\mathrm{X} = n) \\
&= (1^2 + 2^2 \cdots + n^2)\frac{1}{n} \\
&= \frac{n(n+1)(2n+1)}{6}\,\frac{1}{n} \\
&= (n+1)(2n+1)/6.
\end{aligned}$$

Par conséquent,

$$\begin{aligned}
\mathbf{V}(\mathrm{X}) &= \frac{(n+1)(2n+1)}{6} - \frac{(n+1)^2}{4} \\
&= \frac{n+1}{12}(2(2n+1) - 3(n+1)) = \frac{n+1}{12}(n-1) \\
&= \frac{n^2-1}{12}.
\end{aligned}$$

Solution de l'exercice (0.5.2). — *a*) Deux raisonnements intuitifs sont possibles :

– Le premier raisonnement consiste pour le prisonnier à se dire qu'il avait deux chances sur trois d'être condamné, mais qu'il n'en a maintenant plus qu'une chance sur deux — position optimiste ;

– Le second raisonnement consiste à ne pas raisonner du tout et à se dire qu'une fois les décisions prises, rien n'a changé — position neutre.

Lequel de ces deux raisonnements est correct ?

Soit X la variable aléatoire indiquant le numéro (1, 2 ou 3) du prisonnier gracié et soit Y celle indiquant le numéro du prisonnier annoncé par le gardien. S'il entend que le prisonnier n° 2 est condamné, l'information dont dispose le condamné n° 1 est $X \neq 2$ et il s'agit de comparer $\mathbf{P}(X = 1 \mid Y = 2)$ et $\mathbf{P}(X = 1)$.

Par définition d'une probabilité conditionnelle, on a

$$\mathbf{P}(X = 1 \mid Y = 2) = \frac{\mathbf{P}(X = 1 \text{ et } Y = 2)}{\mathbf{P}(Y = 2)}.$$

Si l'on applique la formule de Bayes, on trouve

$$\begin{aligned}
&\mathbf{P}(X = 1 \mid Y = 2) \\
&\quad = \frac{\mathbf{P}(Y = 2 \mid X = 1)\mathbf{P}(X = 1)}{\mathbf{P}(Y = 2 \mid X = 1)\mathbf{P}(X = 1) + \mathbf{P}(Y = 2 \mid X = 2)\mathbf{P}(X = 2) + \mathbf{P}(Y = 2 \mid X = 3)\mathbf{P}(X = 3)} \\
&\quad = \frac{\mathbf{P}(Y = 2 \mid X = 1)\mathbf{P}(X = 1)}{\mathbf{P}(Y = 2 \mid X = 1)\mathbf{P}(X = 1) + \mathbf{P}(X = 3)},
\end{aligned}$$

car $\mathbf{P}(Y = 2 \mid X = 2) = 0$ et $\mathbf{P}(Y = 2 \mid X = 3) = 1$ (le gardien donne l'identité d'un condamné, qui ne peut pas être égal à 2 si le prisonnier n° 2 est gracié, et est forément égal à 2 si le condamné n° 3 est condamné). On doit comparer cette expression à $\mathbf{P}(X = 1)$.

Prenons des valeurs numériques et supposons que le condamné gracié l'a été par tirage au sort (uniforme) : $\mathbf{P}(X = 1) = \mathbf{P}(X = 2) = \mathbf{P}(X = 3) = 1/3$. Par ailleurs, si le prisonnier n° 1 est gracié, imaginons que le gardien ait tiré au sort l'une de ses deux réponses possibles : $\mathbf{P}(Y = 2 \mid X = 1) = 1/2$. Alors,

$$\mathbf{P}(X = 1 \mid Y = 2) = \frac{(1/2) \cdot (1/3)}{(1/2) \cdot (1/3) + (1/3)} = \frac{1/6}{3/6} = \frac{1}{3}.$$

Autrement dit, $\mathbf{P}(X = 1 \mid Y = 2) = \mathbf{P}(X = 1) = 1/3$ et rien n'a changé.

Pour le cas général, notons $a_i = \mathbf{P}(X = i)$ et $p = \mathbf{P}(Y = 2 \mid X = 1)$. Alors,

$$\mathbf{P}(X = 1 \mid Y = 2) - \mathbf{P}(X = 1) = \frac{pa_1}{pa_1 + a_3} - a_1 = \frac{p(1 - a_1) - a_1 a_3}{pa_1 + a_3} a_1$$

de sorte que la conclusion — être optimiste ou pessimiste — dépend des valeurs de a_1, a_2, a_3, p. Si p est nul, c'est-à-dire si le gardien indique le prisonnier n° 3 s'il a le choix, notre prisonnier doit s'inquiéter — dans ce cas, puisque le gardien a indiqué le prisonnier n° 2, c'est qu'il ne pouvait pas indiquer le prisonnier n° 3, c'est-à-dire que ce dernier était gracié et donc le prisonnier n° 1 serait exécuté. Lorsque $p = 1$, c'est-à-dire que le gardien indique le prisonnier n° 2 dès qu'il le peut, on a $p(1-a_1) - a_1a_3 = 1 - a_1 - a_3a_1 = a_2 + a_3 - a_1a_3 = a_2 + a_3(1-a_1) \geqslant 0$, et notre prisonnier n° 1 peut être optimiste.

b) Le candidat avait une chance sur trois de choisir la porte derrière laquelle se trouve la voiture ; nous allons voir que la probabilité que la voiture se trouve derrière la troisième porte est maintenant égale à $2/3$.

C'est en fait le même problème que dans la première question, sous un déguisement moins dramatique : la voiture correspond à la grâce et la porte ouverte par le présentateur à un condamné parmi les deux autres. On a donc $\mathbf{P}(\mathrm{X} = 1 \mid \mathrm{Y} = 2) = 1/3$. Par conséquent, $\mathbf{P}(\mathrm{X} = 3 \mid \mathrm{Y} = 2) = 1 - \mathbf{P}(\mathrm{X} = 1 \mid \mathrm{Y} = 2) = 2/3$, Le candidat a donc intérêt à ouvrir la troisième porte !

Solution de l'exercice (0.5.3). — *a*) La variable aléatoire X est à valeurs positives ; son espérance, éventuellement infinie, est donnée par la somme

$$\mathbf{E}(\mathrm{X}) = \sum_{n=0}^{\infty} n\mathbf{P}(\mathrm{X} = n) = \sum_{n=0}^{\infty} ne^{-p}p^n \frac{1}{n!}.$$

En écrivant $n/n! = 0$ pour $n = 0$ et $1/(n-1)!$ pour $n \geqslant 1$, on obtient

$$\mathbf{E}(\mathrm{X}) = \sum_{n=1}^{\infty} \frac{1}{(n-1)!} p^n e^{-p} = \sum_{n=0}^{\infty} \frac{1}{n!} p^n e^{-p}\, p = p$$

puisque $\sum_{n=0}^{\infty}(p^n/n!) = e^p$.

b) On a $\mathbf{E}(\mathrm{X}^2) = \sum_{n=0}^{\infty} n^2 p^n e^{-p} \frac{1}{n!}$. En écrivant $n^2 = n(n-1) + n$, on obtient

$$\begin{aligned}\mathbf{E}(\mathrm{X}^2) &= \sum_{n=0}^{\infty} \frac{n(n-1)}{n!} p^n e^{-p} + \sum_{n=0}^{\infty} \frac{n}{n!} p^n e^{-p} \\ &= \sum_{n=2}^{\infty} \frac{1}{(n-2)!} p^n e^{-p} + \sum_{n=1}^{\infty} \frac{1}{(n-1)!} p^n e^{-p} \\ &= p^2 \sum_{n=0}^{\infty} \frac{1}{n!} p^n e^{-p} + p \sum_{n=0}^{\infty} \frac{1}{n!} p^n e^{-p} \\ &= p^2 + p.\end{aligned}$$

Pour calculer la variance de X, on écrit alors

$$\mathbf{V}(\mathrm{X}) = \mathbf{E}(\mathrm{X}^2) - \mathbf{E}(\mathrm{X})^2 = (p^2 + p) - p^2 = p.$$

c) Pour calculer

$$\mathbf{E}(\mathrm{X}^k) = \sum_{n=0}^{\infty} n^k p^n e^{-p} \frac{1}{n!},$$

on s'inspire de l'astuce utilisée dans les questions précédentes. Les polynômes $1 = \binom{n}{0}$, $n = \binom{n}{1}$, $n(n-1)/2 = \binom{n}{2}$, …, $n(n-1)\dots(n-k+1)/k! = \binom{n}{k-1}$ forment une base des polynômes de degré $\leqslant k$. Il existe donc des nombres réels $c_0, \dots, c_k$ tels que

$$n^k = c_0 \binom{n}{0} + \cdots + c_k \binom{n}{k}$$

pour tout entier n. Alors,

$$n^k \frac{1}{n!} = c_0 \frac{1}{n!} + c_1 \frac{1}{(n-1)!} + \cdots + c_k \frac{1}{(n-k)!}$$

et le même raisonnement qu'à la question *a*) entraîne

$$\mathbf{E}(\mathrm{X}^k) = c_0 + c_1 p + \cdots + c_k p^k.$$

Pour tenter d'obtenir une « formule close » pour les coefficients c_i, faisons l'observation qu'en dérivant $e^p \mathbf{E}(\mathrm{X}^k)$ par rapport à p, le terme $n^k p^n$ devient $n^{k+1} p^{n-1}$. Autrement dit, à condition de pouvoir dériver terme à terme une famille sommable (et on admettra c'est possible dans le cas présent), on a

$$\mathbf{E}(\mathrm{X}^{k+1}) = p e^{-p} \frac{d}{dp} \big(e^p \mathbf{E}(\mathrm{X}^k) \big).$$

Pour $k = 0$, $X^0 = 1$ et on retrouve

$$\mathbf{E}(X) = pe^{-p}\frac{d}{dp}\big(e^p\big) = p.$$

Pour $k = 1$, cela donne

$$\mathbf{E}(X^2) = pe^{-p}\frac{d}{dp}\big(pe^p\big) = pe^{-p}(e^p + pe^p) = p(p+1),$$

et, pour $k = 3$,

$$\mathbf{E}(X^3) = pe^{-p}\frac{d}{dp}\big(p(p+1)e^p\big) = p\big(2p + 1 + p(p+1)\big) = p(p^2 + 3p + 1).$$

On obtient ainsi une suite $(L_k(p))$ de polynômes en p telle que $\mathbf{E}(X^k) = L_k(p)$ pour tout k. Ces polynômes sont déterminés par la relation $L_0(p) = 1$ et la relation de récurrence

$$L_{k+1}(p) = pe^{-p}\frac{d}{dp}\big(L_k(p)e^p\big) = pL_k'(p) + pL_k(p).$$

Solution de l'exercice (0.5.4). — *a*) La variable aléatoire discrète X étant positive ou nulle, son espérance, éventuellement infinie, est définie par la formule

$$\mathbf{E}(X) = \sum_{n=1}^{\infty} n\mathbf{P}(X = n) = \sum_{n=1}^{\infty} nqp^{n-1}.$$

On a d'autre part $\frac{1}{1-p} = \sum_{n=0}^{\infty} p^n$ qui, par dérivation terme à terme, fournit

$$\frac{1}{(1-p)^2} = \sum_{n=1}^{\infty} np^{n-1}.$$

Par suite,

$$\mathbf{E}(X) = q\frac{1}{(1-p)^2} = \frac{1}{q}.$$

Si on ne veut pas faire usage de ce résultat de dérivation terme à terme, on peut aussi écrire

$$\sum_{n=1}^{\infty} nqp^{n-1} = q\sum_{n=1}^{\infty}\sum_{m=1}^{n} p^{n-1} = q\sum_{m=1}^{\infty}\sum_{n=m}^{\infty} p^{n-1} = \sum_{m=1}^{\infty} p^{m-1} = \frac{1}{1-p} = \frac{1}{q},$$

comme précédemment.

b) La variance de X est donnée par $\mathrm{V}(\mathrm{X}) = \mathbf{E}(\mathrm{X}^2) - \mathbf{E}(\mathrm{X})^2$, et l'on a

$$\mathbf{E}(\mathrm{X}^2) = \sum_{n=1}^{\infty} n^2 \mathbf{P}(\mathrm{X} = n) = \sum_{n=1}^{\infty} n^2 q p^{n-1}.$$

Pour calculer l'espérance de X^2, la méthode de dérivation est la plus efficace. En dérivant l'égalité

$$\sum_{n=1}^{\infty} n p^n = p \sum_{n=1}^{\infty} n p^{n-1} = \frac{p}{(1-p)^2},$$

on obtient

$$\sum_{n=1}^{\infty} n^2 p^{n-1} = \frac{1}{(1-p)^2} + 2\frac{p}{(1-p)^3} = \frac{1+p}{(1-p)^3},$$

de sorte que

$$\mathbf{E}(\mathrm{X}^2) = \frac{1+p}{q^2}.$$

Alors,

$$\mathrm{V}(\mathrm{X}) = \frac{1+p}{q^2} - \frac{1}{q^2} = \frac{p}{q^2}.$$

c) Pour calculer l'espérance de X^k, la méthode de dérivation est la plus efficace. On a

$$\mathbf{E}(\mathrm{X}^k) = q \sum_{n=1}^{\infty} n^k p^{n-1}.$$

En dérivant $pq^{-1}\mathbf{E}(\mathrm{X}^k)$ par rapport à p, on trouve donc

$$\frac{d}{dp}\big(pq^{-1}\mathbf{E}(\mathrm{X}^k)\big) = \frac{d}{dp}\Big(\sum_{n=1}^{\infty} n^k p^n\Big) = \sum_{n=0}^{\infty} n^{k+1} p^{n-1} = \frac{1}{q}\mathbf{E}(\mathrm{X}^{k+1}).$$

Autrement dit,

$$q^{-1}\mathbf{E}(\mathrm{X}^{k+1}) = \frac{d}{dp}\big(pq^{-1}\mathbf{E}(\mathrm{X}^k)\big).$$

Pour tout k, posons $f_k(p) = q^{-1}\mathbf{E}(\mathrm{X}^k)$. Ces fonctions satisfont la relation de récurrence $f_{k+1}(p) = (pf_k)'(p)$. Pour $k = 0$, on a $f_0(p) = q^{-1}\mathbf{E}(\mathrm{X}^0) = 1/(1-p)$; on a aussi $f_1(p) = 1/(1-p)^2$ et $f_2(p) = (1+p)/(1-p)^3$.

Nous allons prouver par récurrence qu'il existe une suite $(\mathrm{S}_k(p))$ de polynômes unitaires, où S_k est de degré k, telle que $f_k(p) = \mathrm{S}_k(p)/(1-p)^{k+1}$. On vient de le voir pour $0 \leqslant k \leqslant 2$, avec $\mathrm{S}_0(p) = 1$, $\mathrm{S}_1(p) = p$ et $\mathrm{S}_2(p) = p + p^2$.

Si l'on a $f_k(p) = \mathrm{S}_k(p)/(1-p)^{k+1}$, alors

$$\begin{aligned} f_{k+1}(p) &= \frac{d}{dp}\left(\frac{p\mathrm{S}_k(p)}{(1-p)^{k+1}}\right) \\ &= \frac{\mathrm{S}_k(p) + p\mathrm{S}_k'(p)}{(1-p)^{k+1}} + (k+1)\frac{p\mathrm{S}_k(p)}{(1-p)^{k+2}} \\ &= \frac{(1-p)\mathrm{S}_k(p) + p(1-p)\mathrm{S}_k'(p) + (k+1)p\mathrm{S}_k(p)}{(1-p)^{k+2}}, \end{aligned}$$

ce qui est une relation comme celle demandée, avec

$$\mathrm{S}_{k+1}(p) = (k+1)p\mathrm{S}_k(p) + p(1-p)\mathrm{S}_k'(p) + (1-p)\mathrm{S}_k(p).$$

Si $\mathrm{S}_k(p)$ est unitaire de degré k, alors $\mathrm{S}_{k+1}(p)$ est de degré $\leqslant k+1$, et son coefficient de p^{k+1} est donné par $(k+1)-k = 1$, de sorte que $\mathrm{S}_{k+1}(p)$ est unitaire de degré $k+1$.

Solution de l'exercice (0.5.5). — *a*) Soit A l'événement « le dé choisi est le dé pipé ». On a $\mathbf{P}(\mathrm{A}) = 1/3$.

b) Soit X l'évènement « le dé choisi sort sur 1 ». On a donc $\mathbf{P}(\mathrm{X} \mid \mathrm{A}) = 2/3$ et $\mathbf{P}(\mathrm{X} \mid \overline{\mathrm{A}}) = 1/6$, d'où

$$\mathbf{P}(\mathrm{X}) = \mathbf{P}(\mathrm{A})\mathbf{P}(\mathrm{X} \mid \mathrm{A}) + \mathbf{P}(\overline{\mathrm{A}})\mathbf{P}(\mathrm{X} \mid \overline{\mathrm{A}}) = \frac{1}{3}\cdot\frac{2}{3} + \frac{2}{3}\cdot\frac{1}{6} = \frac{1}{3}.$$

Par suite, en appliquant la formule de Bayes, on a

$$\mathbf{P}(\mathrm{A} \mid \mathrm{X}) = \frac{\mathbf{P}(\mathrm{X} \mid \mathrm{A})\mathbf{P}(\mathrm{A})}{\mathbf{P}(\mathrm{X})} = \frac{(2/3)(1/3)}{1/3} = 2/3.$$

Compte tenu de cette expérience, la probabilité que le dé choisi soit pipé est maintenant de $2/3$!

c) Soit Y l'évènement « au deuxième tirage, le dé choisi sort sur 1 ». Cet évènement est indépendant de X conditionnellement à A, mais leurs lois sont identiques : $\mathbf{P}(\mathrm{Y} \mid \mathrm{A}) = 2/3$, $\mathbf{P}(\mathrm{Y} \mid \overline{\mathrm{A}}) = 1/6$, $\mathbf{P}(\mathrm{Y}) = 1/3$.

Par indépendance conditionnellement à A, on a aussi

$$\mathbf{P}(\mathrm{X} \cap \mathrm{Y} \mid \mathrm{A}) = \mathbf{P}(\mathrm{X} \mid \mathrm{A})\mathbf{P}(\mathrm{Y} \mid \mathrm{A}) = 4/9$$

et

$$\mathbf{P}(\mathrm{X} \cap \mathrm{Y} \mid \overline{\mathrm{A}}) = \mathbf{P}(\mathrm{X} \mid \overline{\mathrm{A}})\mathbf{P}(\mathrm{Y} \mid \overline{\mathrm{A}}) = 1/36.$$

Enfin,

$$\mathbf{P}(\mathrm{X} \cap \mathrm{Y}) = \mathbf{P}(\mathrm{A})\mathbf{P}(\mathrm{X} \cap \mathrm{Y} \mid \mathrm{A}) + \mathbf{P}(\overline{\mathrm{A}})\mathbf{P}(\mathrm{X} \cap \mathrm{Y} \mid \overline{\mathrm{A}}) = \frac{1}{3}\cdot\frac{4}{9} + \frac{2}{3}\cdot\frac{1}{36} = \frac{1}{6}.$$

Par suite,

$$\mathbf{P}(\mathrm{A} \mid \mathrm{X} \cap \mathrm{Y}) = \frac{\mathbf{P}(\mathrm{X} \cap \mathrm{Y} \mid \mathrm{A})\mathbf{P}(\mathrm{A})}{\mathbf{P}(\mathrm{X} \cap \mathrm{Y})} = \frac{(4/9)(1/3)}{1/6} = 8/9.$$

Compte tenu de cette deconde expérience, la probabilité que le dé choisi soit pipé est maintenant de $8/9$!

Solution de l'exercice (0.5.6). — *a*) La variable (X, Y) suit une loi uniforme : chacun des 36 couples (a, b), où $a, b \in \{1, \ldots, 36\}$, a probabilité $1/36$ d'apparaître. Leur somme appartient à $\{2; \ldots; 12\}$; la probabilité que la somme soit un entier s est égale à $n(s)/36$, où $n(s)$ est le nombre de couples d'entiers (a, b) tels que $1 \leqslant a, b \leqslant 6$ et $a + b = s$. On trouve $n(2) = 1$, $n(3) = 2$, …, $n(7) = 6$, puis $n(8) = 5$, …, et finalement $n(12) = 1$.

b) Si $\mathrm{Z} = 2$, on a nécessairement $\mathrm{X} = 1$, de sorte que $\mathbf{P}(\mathrm{X} = 1 \mid \mathrm{Z} = 2) = 1$, puis $\mathbf{E}(\mathrm{X} \mid \mathrm{Z} = 2) = 1$.

Conditionné à $\mathrm{Z} = 3$, on a $\mathrm{X} = 1$ ou $\mathrm{X} = 2$, chacune des deux possibilités ayant probabilité $1/2$, de sorte que $\mathbf{E}(\mathrm{X} \mid \mathrm{Z} = 3) = (1 + 2)/2 = 3/2$.

Plus généralement, si $\mathrm{Z} = a$, on a $\sup(a - 6, 1) \leqslant \mathrm{X} \leqslant \inf(a - 1, 6)$, et conditionné à cet évènement $(\mathrm{Z} = a)$, chacune de ces possibilité a même probabilité. L'espérance conditionnelle cherchée est donc

$$\mathbf{E}(\mathrm{X} \mid \mathrm{Z} = a) = \frac{1}{2}\big(\sup(a - 6, 1) + \inf(a - 1, 6)\big).$$

Pour $2 \leqslant a \leqslant 7$, on a $\sup(a - 6, 1) = 1$ et $\inf(a - 1, 6) = a - 1$, de sorte que $\mathbf{E}(\mathrm{X} \mid \mathrm{Z} = a) = (1 + (a - 1))/2 = a/2$. Pour $7 \leqslant a \leqslant 12$, on a $\sup(a - 6, 1) = a - 6$ et $\inf(a - 1, 6) = 6$, de sorte que $\mathbf{E}(\mathrm{X} \mid \mathrm{Z} = a) = ((a - 6) + 6)/2 = a/2$.

On trouve donc

$$\mathbf{E}(\mathrm{X} \mid \mathrm{Z} = a) = \frac{1}{2}a.$$

c) La variable aléatoire $\mathbf{E}(\mathrm{X} \mid \mathrm{Z})$ est définie par

$$\mathbf{E}(\mathrm{X} \mid \mathrm{Z})(\omega) = \mathbf{E}(\mathrm{X} \mid \mathrm{Z} = \mathrm{Z}(\omega))$$

pour tout ω dans l'univers Ω. On a donc

$$\mathbf{E}(\mathrm{X} \mid \mathrm{Z})(\omega) = \mathrm{Z}(\omega)/2.$$

Autrement dit, $\mathbf{E}(\mathrm{X} \mid \mathrm{Z}) = \mathrm{Z}/2$.

d) On peut démontrer cette relation en général : Par symétrie, on a $\mathbf{E}(X \mid Z = a) = \mathbf{E}(Y \mid Z = a)$. Par additivité de l'espérance conditionnelle, on a donc

$$\begin{aligned} 2\mathbf{E}(X \mid Z = a) &= \mathbf{E}(X \mid Z = a) + \mathbf{E}(Y \mid Z = a) \\ &= \mathbf{E}(X + Y \mid Z = a) = \mathbf{E}(Z \mid Z = a) = a, \end{aligned}$$

d'où la relation $\mathbf{E}(X \mid Z = a) = a/2$ puis, comme dans la question précédente, $\mathbf{E}(X \mid Z) = Z/2$.

e) Les variables aléatoires X et Y prennent les valeurs 0 et 1, et $\mathbf{P}(X = 1) = \mathbf{P}(Y = 1) = p$. Par suite, leur produit XY ne prend également que les valeurs 0 et 1. Comme $XY = 1$ entraîne $X = Y = 1$, on a $\mathbf{P}(XY = 1) = p^2$.

Puisque $\mathbf{P}(X = 1 \mid XY = 1) = 1$, il vient $\mathbf{E}(X \mid XY = 1) = 1$.

Le cas $XY = 0$, de probabilité $1 - p^2$, correspond aux trois autres possibilités pour le couple (X, Y), de probabilités respectives $\mathbf{P}((X, Y) = (1, 0)) = p(1-p) = \mathbf{P}((X, Y) = (0, 1))$ et $\mathbf{P}((X, Y) = (0, 0)) = (1 - p)^2$. Conditionnellement à l'évènement $XY = 1$, leurs probabilités sont donc $p(1 - p)/(1 - p^2) = p/(1 + p)$, $p/(1 + p)$ et $(1 - p)^2/(1 - p^2) = (1 - p)/(1 + p)$. Par suite,

$$\mathbf{E}(X \mid XY = 0) = 1 \cdot \frac{p}{1+p} + 0\frac{p}{1+p} + 0\frac{1-p}{1+p} = \frac{p}{1+p}.$$

Si l'on veut donner une formule analogue à celle de la question précédente, on peut chercher une fonction de a qui vaut $p/(1 + p)$ lorsque $a = 0$ et 1 lorsque $a = 1$. Une d'entre elles est $a \mapsto (p + a)/(p + 1)$, d'où, si l'on veut,

$$\mathbf{E}(X \mid XY) = (p + XY)/(p + 1).$$

Solution de l'exercice (0.5.7). — *a*) On part de la définition $\mathbf{E}(X) = \sum_x \mathbf{P}(X = x)x$ de l'espérance, en introduisant la formule des probabilités totales : $\mathbf{P}(X = x) =$

$\sum_y \mathbf{P}(\mathrm{X} = x \text{ et } \mathrm{Y} = y)$. On obtient

$$\begin{aligned}\mathbf{E}(\mathrm{X}) &= \sum_x \mathbf{P}(\mathrm{X} = x)x \\ &= \sum_{x,y} \mathbf{P}(\mathrm{X} = x \text{ et } \mathrm{Y} = y)x \\ &= \sum_{\substack{y \\ \mathbf{P}(\mathrm{Y}=y)>0}} \mathbf{P}(\mathrm{Y} = y) \sum_x \mathbf{P}(\mathrm{X} = x \mid \mathrm{Y} = y)x \\ &= \sum_{\substack{y \\ \mathbf{P}(\mathrm{Y}=y)>0}} \mathbf{P}(\mathrm{Y} = y)\mathbf{E}(\mathrm{X} \mid \mathrm{Y} = y).\end{aligned}$$

Par ailleurs, la variable aléatoire $\mathbf{E}(\mathrm{X} \mid \mathrm{Y})$ est constante de valeur $\mathbf{E}(\mathrm{X} \mid \mathrm{Y} = y)$ est constante en restriction à l'évènement $\mathrm{Y} = y$ si $\mathbf{P}(\mathrm{Y} = y) > 0$, et elle est nulle sur cet évènement si $\mathbf{P}(\mathrm{Y} = y) = 0$. Ainsi, cette dernière expression coïncide avec l'espérance $\mathbf{E}(\mathbf{E}(\mathrm{X} \mid \mathrm{Y}))$, d'où la question.

b) On a $\mathbf{V}(\mathrm{X}) = \mathbf{E}(\mathrm{X}^2) - \mathbf{E}(\mathrm{X})^2$. On a ensuite

$$\begin{aligned}\mathbf{E}(\mathbf{V}(\mathrm{X} \mid \mathrm{Y})) &= \sum_y \mathbf{P}(\mathrm{Y} = y)\mathbf{E}(\mathrm{X}^2 \mid \mathrm{Y} = y) - \sum_y \mathbf{P}(\mathrm{Y} = y)\mathbf{E}(\mathrm{X} \mid \mathrm{Y} = y)^2 \\ &= \mathbf{E}(\mathbf{E}(\mathrm{X}^2 \mid \mathrm{Y})) - \mathbf{E}(\mathbf{E}(\mathrm{X} \mid \mathrm{Y})^2) \\ &= \mathbf{E}(\mathrm{X}^2) - \mathbf{E}(\mathbf{E}(\mathrm{X} \mid \mathrm{Y})^2)\end{aligned}$$

d'après la première question. De même,

$$\mathbf{V}(\mathbf{E}(\mathrm{X} \mid \mathrm{Y})) = \mathbf{E}(\mathbf{E}(\mathrm{X} \mid \mathrm{Y})^2) - \mathbf{E}(\mathbf{E}(\mathrm{X} \mid \mathrm{Y}))^2 = \mathbf{E}(\mathbf{E}(\mathrm{X} \mid \mathrm{Y})^2) - \mathbf{E}(\mathrm{X})^2.$$

Ainsi,

$$\begin{aligned}\mathbf{E}(\mathbf{V}(\mathrm{X} \mid \mathrm{Y})) + \mathbf{V}(\mathbf{E}(\mathrm{X} \mid \mathrm{Y})) &= \mathbf{E}(\mathrm{X}^2) - \mathbf{E}(\mathbf{E}(\mathrm{X} \mid \mathrm{Y})^2) + \mathbf{E}(\mathbf{E}(\mathrm{X} \mid \mathrm{Y})^2) - \mathbf{E}(\mathrm{X})^2 \\ &= \mathbf{E}(\mathrm{X}^2) - \mathbf{E}(\mathrm{X})^2 = \mathbf{V}(\mathrm{X}),\end{aligned}$$

ce qu'il fallait démontrer.

CHAPITRE 1

ENTROPIE ET INFORMATION MUTUELLE

L'*entropie* est un concept fondamental en théorie de l'information, proposé par Shannon (1948). comme mesure Nous définissons d'abord l'entropie d'une variable aléatoire et verrons sur quelques exemples qu'elle a en fait une double interprétation, soit comme quantité de hasard, soit comme quantité d'information. Cette dualité information/hasard peut sembler mystérieuse ; elle est en fait au cœur de la formalisation probabiliste des phénomènes pour lesquels une information inconnue est mathématiquement considérée comme aléatoire. La pertinence de ce point de vue, pas forcément évidente a priori, est démontrée par l'importance du calcul des probabilités dans les mathématiques de la seconde moitié du 20^{e} siècle.

Deux variantes de l'entropie s'avèrent également très importantes, à la fois pour leur potentiel calculatoire et pour leur interprétation en théorie de l'information : l'*entropie conditionnelle* et l'*information mutuelle*.

En théorie de l'information, un signal est souvent présenté comme une suite de symboles, ou de signaux élémentaires, disons émis à intervalles de temps réguliers, et que l'on représente en théorie des probabilités comme une suite de variables aléatoires — un *processus stochastique*. Cela donne lieu à la notion de *taux d'entropie :* non pas l'entropie globale du signal, mais celle par unité de temps ou par symbole.

Parmi les processus stochastiques les plus simples, on trouve ceux qui sont totalement indépendants. Plus proche des phénomènes réels que l'on veut modéliser, on trouve les *processus markoviens* : ce sont ceux pour lesquels le symbole émis au temps $n + 1$ ne dépend que de celui émis au temps n — c'est bien sûr une dépendance/indépendance au sens de la théorie des probabilités. On analyse le taux d'entropie de ces processus, en particulier dans les cas où ils sont stationnaires ou ergodiques.

1.1. Entropie d'une variable aléatoire

1.1.1. — On désigne ici par log : $\mathbf{R}_{>0} \to \mathbf{R}$ la fonction logarithme usuelle, fonction réciproque de la fonction exponentielle, autrement dit le logarithme néperien. C'est une fonction de classe $\mathscr{C}^\infty$; comme sa dérivée est la fonction $x \mapsto 1/x$, la fonction logarithme est strictement croissante ; elle obéit à l'équation fonctionnelle

(1.1.1.1) $$\log(xy) = \log(x) + \log(y), \qquad \text{pour tous } x, y > 0.$$

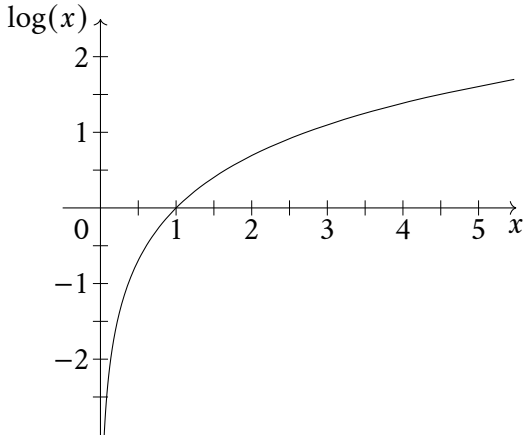


FIGURE 1.1.1.2. Graphe de la fonction « logarithme néperien »

On a les limites :

(1.1.1.3) $$\lim_{x\to 0^+} \log(x) = -\infty, \qquad \lim_{x\to+\infty} \log(x) = +\infty.$$

On a aussi les limites, pour tout nombre réel $\alpha > 0$:

(1.1.1.4) $$\lim_{x\to 0^+} x^\alpha \log(x) = 0, \qquad \lim_{x\to+\infty} x^{-\alpha} \log(x) = 0.$$

Sa dérivée seconde, la fonction $x \mapsto -1/x^2$, est strictement négative. Par conséquent, la fonction logarithme est strictement *concave* : elle est en-dessous de ses tangentes, au-dessus de ses cordes.

1.1.2. — Si a est un nombre réel > 0, le « logarithme en base a » est la fonction donnée par

$$\log_a(x) = \frac{\log(x)}{\log(a)}.$$

Elle vérifie des propriétés similaires au logarithme néperien, qui est le cas où $a = e = 2{,}718\,281\,828\ldots$. Le cas $a = 10$ est courant en physique ; en théorie de l'information, nous verrons qu'il est naturel de prendre $a = 2$.

1.1.3. — La fonction $x \mapsto -x\log(x)$ de $]0;1]$ dans $\mathbf{R}$ est à valeurs positives ou nulles. Elle a pour limite 0 en 0, ce qui permet de la prolonger par continuité en 0, de valeur 0. Cela justifie aussi la convention d'écriture $0 \times \log(0) = 0$, elle-même un avatar de la convention $0^0 = 1$. Cette fonction est aussi indéfiniment dérivable sur $]0;1[$, de dérivée $x \mapsto -\log(x) - 1 = -\log(ex)$; elle est donc strictement croissante sur l'intervalle $[0;1/e]$ et strictement décroissante sur l'intervalle $[1/e;1]$. Comme sa dérivée seconde est la fonction $x \mapsto -1/x$, de valeur strictement négative sur $]0;1]$, cette fonction est strictement concave.

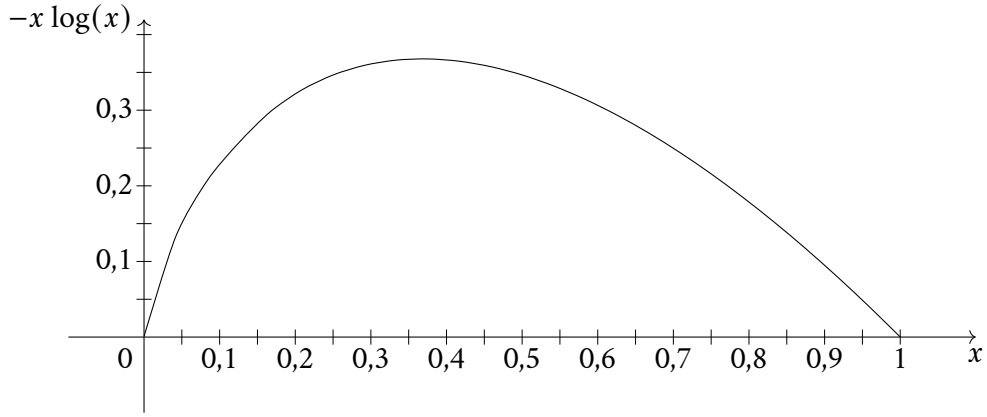


FIGURE 1.1.3.1. Graphe de la fonction $x \mapsto -x\log(x)$

Définition **(1.1.4)**. — *L'entropie d'une variable aléatoire discrète* X *est définie par*

(1.1.4.1) $$\mathrm{H}(\mathrm{X}) = \sum_x \left(-\mathbf{P}(\mathrm{X} = x)\log(\mathbf{P}(\mathrm{X} = x))\right).$$

L'entropie est donc définie comme la somme d'une famille de nombres réels positifs ou nuls, indexée par l'ensemble des valeurs possibles x de la variable aléatoire X. Dans cette définition, on utilie la convention $0\log(0) = 0$; on peut donc ne considérer, si l'on veut, que les valeurs x pour lesquelles $\mathbf{P}(\mathrm{X} = x)$ est strictement positive. Cette série est à termes positifs car une probabilité appartient à $[0;1]$, donc son logarithme est négatif. Il en résulte donc que la somme de cette série est bien définie, en tant qu'élément de $[0;+\infty]$. Elle est finie si X ne prend qu'un nombre fini de valeurs.

On peut bien sûr la définir dans toute base $a > 0$.

(1.1.4.2) $$\mathrm{H}_a(\mathrm{X}) = \sum_x \left(-\mathbf{P}(\mathrm{X}=x)\log_a(\mathbf{P}(\mathrm{X}=x))\right) = \frac{\mathrm{H}(\mathrm{X})}{\log(a)}.$$

1.1.5. Exemple : lancer d'un dé. — Considérons un dé à 6 faces, équilibré. La probabilité d'apparition de chacune des faces est donc $1/6$; l'entropie de la variable aléatoire correspondante est ainsi égale à $6 \cdot (-\frac{1}{6}\log(\frac{1}{6})) = \log(6)$.

Plus généralement, une variable aléatoire X prenant N valeurs, chacune avec probabilité $1/\mathrm{N}$, a pour entropie $\log(\mathrm{N})$. Imaginons que N soit une puissance de 2, $\mathrm{N} = 2^n$, et que X prenne ses valeurs parmi $\{0, \ldots, \mathrm{N}-1\}$. Alors, on peut connaître le résultat de X en posant successivement n questions « binaires », à savoir quels sont les chiffres du développement binaire de X. Dans ce cas, on a $\mathrm{H}_2(\mathrm{X}) = \log_2(\mathrm{N}) = n$.

Plus généralement, on verra comment le théorème de Shannon interprète l'entropie en base 2 d'une variable aléatoire comme, à une unité près, le nombre moyen de questions binaires qu'il faut poser pour espérer connaître son résultat.

Considérons maintenant deux dés à 6 faces, équilibrés, et prenons pour variable aléatoire Y la somme des valeurs des deux faces. Elle peut prendre les valeurs $2, 3, \ldots, 12$; la valeur 2 n'est possible que pour le tirage $(1,1)$, la valeur 3 apparaît pour deux tirages $(1,2)$ et $(2,1)$, etc. Les probabilités des évènements $\mathrm{X} = x$ sont ainsi résumées par le tableau :

x	2	3	4	5	6	7	8	9	10	11	12
$\mathbf{P}(\mathrm{X}=x)$	1/36	2/36	3/36	4/36	5/36	6/36	5/36	4/36	3/36	2/36	1/36

et son entropie en base 2 est égale à

$$\mathrm{H}_2(\mathrm{Y}) = -\frac{1}{36}\log_2\left(\frac{1}{36}\right) - \cdots - \frac{1}{36}\log_2\left(\frac{1}{36}\right) \approx 3{,}274\,401\,919\,288\,77$$

alors que l'entropie d'une variable aléatoire identiquement distribuée parmi $\{2, \ldots, 12\}$ est égale à

$$\log_2(11) \approx 3{,}459\,431\,618\,637\,30.$$

Il y a un peu moins de hasard dans le résultat de la somme de deux dés que dans le tirage d'un dé équilibré dont les onze faces indiqueraient les entiers de 2 à 12.

1.1.6. Exemple : variable de Bernoulli. — Soit p un élément de $[0;1]$. Rappelons qu'une variable aléatoire X suit une *loi de Bernoulli* de paramètre p si elle prend la valeur 1 avec probabilité p et la valeur 0 avec la probabilité $1-p$. L'entropie d'une telle variable aléatoire est donc égale à

$$h(p) = \begin{cases} -p\log(p) - (1-p)\log(1-p) & \text{si } 0 < p < 1, \\ 0 & \text{si } p = 0 \text{ ou } p = 1. \end{cases} \tag{1.1.6.1}$$

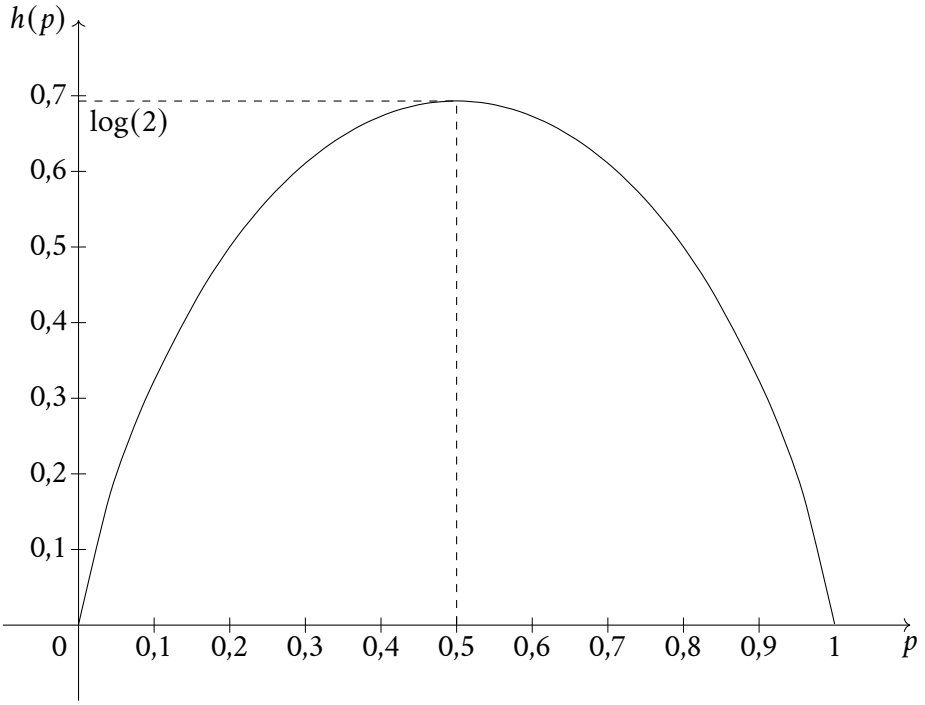


FIGURE 1.1.6.2. Graphe de la fonction « entropie »

Puisque la fonction $x \mapsto -x\log(x)$ est continue sur $[0;1]$, indéfiniment dérivable sur $]0;1[$, de dérivée $x \mapsto -\log(x) - 1$, la fonction h est continue, indéfiniment dérivable sur $]0;1[$, de dérivée

$$h'(p) = -\log(p) + \log(1-p).$$

Sa dérivée seconde, donnée par

$$h''(p) = -\frac{1}{p} - \frac{1}{1-p}$$

est strictement négative sur $]0;1[$, si bien que la fonction h est strictement concave. On a $h'(1/2) = 0$, ce qui entraîne que $h'(p) > 0$ pour $p \in]0;1/2[$ et $h'(p) < 0$ pour $p \in]1/2;1[$. La fonction h est donc strictement croissante sur $[0;1/2]$ et

strictement décroissante sur $[1/2; 1]$. Elle atteint son maximum en le point $p = 1/2$, de valeur $h(1/2) = \log(2)$.

On voit là l'intérêt de la base 2 : la fonction h_2 définie par

$$h_2(p) = h(p)/\log(2) = -p\log_2(p) - (1-p)\log_2(1-p)$$

a pour image $[0; 1]$.

1.2. Entropie conditionnelle

1.2.1. — Soit A un évènement de probabilité non nulle, c'est-à-dire une partie de l'univers probabiliste Ω telle que $\mathbf{P}(\mathrm{A}) > 0$. L'évènement A lui-même peut être vu comme un univers probabiliste, lorsqu'on pose, pour tout évènemetn B qui est contenu dans A,

$$\mathbf{P}(\mathrm{B} \mid \mathrm{A}) = \frac{\mathbf{P}(\mathrm{B})}{\mathbf{P}(\mathrm{A})}.$$

Si X est une variable aléatoire discrète, on peut alors la *conditionner* à A en considérant sa restriction à A, ici notée $\mathrm{X} \mid \mathrm{A}$.

Définition **(1.2.2)**. — *Soit* X *et* Y *des variables aléatoires discrètes. On appelle* entropie conditionnelle de X relativement à Y *(ou* sachant Y*) l'expression*

(1.2.2.1)
$$\mathrm{H}(\mathrm{X} \mid \mathrm{Y}) = \sum_{y} \mathbf{P}(\mathrm{Y} = y)\mathrm{H}(\mathrm{X} \mid \mathrm{Y} = y).$$

C'est la somme d'une famille de nombres réels positifs ou nuls, donc est un élément de $[0; +\infty]$. A priori, la variable aléatoire $\mathrm{X} \mid \{\mathrm{Y} = y\}$ n'est définie que si $\mathbf{P}(\mathrm{Y} = y) \neq 0$; dans le cas contraire, on enlève le terme correspondant de la somme. Cette somme est infinie s'il existe y tel que $\mathbf{P}(\mathrm{Y} = y) > 0$ et $\mathrm{H}(\mathrm{X} \mid \mathrm{Y} = y) = +\infty$; s'il n'existe pas de tel y, il est aussi possible que la somme vaille $+\infty$. Quoi qu'il en soit, si X et Y ne prennent qu'un nombre fini de valeurs, cette expression est finie.

Si la variable aléatoire Y est certaine, c'est-à-dire s'il existe y tel que $\mathbf{P}(\mathrm{Y} = y) = 1$, alors $\mathrm{H}(\mathrm{X} \mid \mathrm{Y}) = \mathrm{H}(\mathrm{X} \mid \mathrm{Y} = y) = \mathrm{H}(\mathrm{X})$.

Proposition **(1.2.3)**. — *Soit* X *et* Y *des variables aléatoires discrètes. On a*

(1.2.3.1)
$$\mathrm{H}(\mathrm{X}, \mathrm{Y}) = \mathrm{H}(\mathrm{Y}) + \mathrm{H}(\mathrm{X} \mid \mathrm{Y}).$$

Démonstration. — Partons des définitions de l'entropie et de l'entropie conditionnelle. Pour simplifier les notations, on écrit $p_x = \mathbf{P}(\mathrm{X} = x)$, $q_y = \mathbf{P}(\mathrm{Y} = y)$ et $r_{xy} = \mathbf{P}(\mathrm{X} = x \text{ et } \mathrm{Y} = y)$. En sommant sur les valeurs possibles de Y, c'est-à-dire les y tels que $q_y > 0$, on a donc :

$$\mathrm{H}(\mathrm{Y}) + \mathrm{H}(\mathrm{X} \mid \mathrm{Y}) = \sum_y -q_y \log(q_y) + \sum_y q_y \mathrm{H}(\mathrm{X} \mid \mathrm{Y} = y).$$

Par ailleurs, pour tout y tel que $q_y > 0$, la loi de la variable aléatoire $\mathrm{X} \mid \{\mathrm{Y} = y\}$ est donnée par

$$\mathbf{P}(\mathrm{X} = x \mid \mathrm{Y} = y) = \frac{\mathbf{P}(\mathrm{X} = x \text{ et } \mathrm{Y} = y)}{\mathbf{P}(\mathrm{Y} = y)} = \frac{r_{xy}}{q_y}.$$

Par conséquent, son entropie est égale à

$$\begin{aligned}\mathrm{H}(\mathrm{X} \mid \mathrm{Y} = y) &= \sum_x -\mathbf{P}(\mathrm{X} = x \mid \mathrm{Y} = y) \log(\mathbf{P}(\mathrm{X} = x \mid \mathrm{Y} = y)) \\ &= \sum_x -\frac{r_{xy}}{q_y} \log\left(\frac{r_{xy}}{q_y}\right).\end{aligned}$$

En ajoutant terme à terme ces deux familles à termes positifs,[(1)] on obtient

$$\mathrm{H}(\mathrm{Y}) + \mathrm{H}(\mathrm{X} \mid \mathrm{Y}) = \sum_y q_y \log\left(\frac{1}{q_y}\right) + \sum_{x,y} r_{xy} \log\left(\frac{q_y}{r_{xy}}\right).$$

Comme $q_y = \mathbf{P}(\mathrm{Y} = y) = \sum_x \mathbf{P}(\mathrm{X} = x \text{ et } \mathrm{Y} = y) = \sum_x r_{xy}$, il vient

$$\begin{aligned}\mathrm{H}(\mathrm{Y}) + \mathrm{H}(\mathrm{X} \mid \mathrm{Y}) &= \sum_{x,y} \left(r_{xy} \log\left(\frac{1}{q_y}\right) + r_{xy} \log\left(\frac{q_y}{r_{xy}}\right) \right) \\ &= \sum_{x,y} r_{xy} \log\left(\frac{1}{r_{xy}}\right) \\ &= \mathrm{H}(\mathrm{X}, \mathrm{Y}),\end{aligned}$$

par définition de l'entropie du couple (X, Y). □

Corollaire **(1.2.4)**. — *Soit* $\mathrm{X}, \mathrm{Y}, \mathrm{Z}$ *des variables aléatoires discrètes. On a*

$$\mathrm{H}(\mathrm{X}, \mathrm{Y} \mid \mathrm{Z}) = \mathrm{H}(\mathrm{Y} \mid \mathrm{Z}) + \mathrm{H}(\mathrm{X} \mid \mathrm{Y}, \mathrm{Z}).$$

(1) Ce résultat devrait être donné au chapitre précédent…

Démonstration. — Soit z une valeur de Z telle que $\mathbf{P}(\mathrm{Z}=z)>0$. Appliquons la proposition aux variables aléatoires $\mathrm{X} \mid \{\mathrm{Z}=z\}$ et $\mathrm{Y} \mid \{\mathrm{Z}=z\}$: on obtient

$$\mathrm{H}(\mathrm{X},\mathrm{Y} \mid \mathrm{Z}=z) = \mathrm{H}(\mathrm{Y} \mid \mathrm{Z}=z) + \mathrm{H}(\mathrm{X} \mid \mathrm{Y},\mathrm{Z}=z).$$

Multiplions cette égalité par $\mathbf{P}(\mathrm{Z}=z)$ et ajoutons-les ; par définition des entropies $\mathrm{H}(\mathrm{X},\mathrm{Y} \mid \mathrm{Z})$ et $\mathrm{H}(\mathrm{Y} \mid \mathrm{Z})$, il vient :

$$\mathrm{H}(\mathrm{X},\mathrm{Y} \mid \mathrm{Z}) = \mathrm{H}(\mathrm{Y} \mid \mathrm{Z}) + \sum_{z} \mathbf{P}(\mathrm{Z}=z)\mathrm{H}(\mathrm{X} \mid \mathrm{Y},\mathrm{Z}=z).$$

Pour calculer ce dernier terme, revenons à la définition de l'entropie conditionnelle $\mathrm{H}(\mathrm{X} \mid \mathrm{Y},\mathrm{Z}=z)$; on a

$$\mathrm{H}(\mathrm{X} \mid \mathrm{Y},\mathrm{Z}=z) = \sum_{y} \mathbf{P}(\mathrm{Y}=y \mid \mathrm{Z}=z)\mathrm{H}(\mathrm{X} \mid \mathrm{Y}=y,\mathrm{Z}=z),$$

de sorte que

$$\begin{aligned}
&\sum_{\mathbf{P}(\mathrm{Z}=z)>0} \mathbf{P}(\mathrm{Z}=z)\mathrm{H}(\mathrm{X} \mid \mathrm{Y},\mathrm{Z}=z) \\
&\qquad = \sum_{y} \sum_{\mathbf{P}(\mathrm{Z}=z)>0} \mathbf{P}(\mathrm{Z}=z)\mathbf{P}(\mathrm{Y}=y \mid \mathrm{Z}=z)\mathrm{H}(\mathrm{X} \mid \mathrm{Y}=y,\mathrm{Z}=z) \\
&\qquad = \sum_{y} \sum_{\mathbf{P}(\mathrm{Z}=z)>0} \mathbf{P}(\mathrm{Y}=y,\mathrm{Z}=z)\mathrm{H}(\mathrm{X} \mid \mathrm{Y}=y,\mathrm{Z}=z) \\
&\qquad = \sum_{\mathbf{P}(\mathrm{Y}=y,\mathrm{Z}=z)>0} \mathbf{P}(\mathrm{Y}=y,\mathrm{Z}=z)\mathrm{H}(\mathrm{X} \mid \mathrm{Y}=y,\mathrm{Z}=z) \\
&\qquad = \mathrm{H}(\mathrm{X} \mid \mathrm{Y},\mathrm{Z}).
\end{aligned}$$

Le corollaire est ainsi démontré. □

Remarque **(1.2.5)**. — On peut aussi démontrer simplement cette égalité lorsque l'entropie $\mathrm{H}(\mathrm{Y},\mathrm{Z})$ est finie. Dans ce cas, $\mathrm{H}(\mathrm{Z})$ est également finie et l'on a

$$\begin{aligned}
\mathrm{H}(\mathrm{X},\mathrm{Y} \mid \mathrm{Z}) &= \mathrm{H}(\mathrm{X},\mathrm{Y},\mathrm{Z}) - \mathrm{H}(\mathrm{Z}) \\
&= (\mathrm{H}(\mathrm{X},\mathrm{Y},\mathrm{Z}) - \mathrm{H}(\mathrm{Y},\mathrm{Z})) + (\mathrm{H}(\mathrm{Y},\mathrm{Z}) - \mathrm{H}(\mathrm{Z})) \\
&= \mathrm{H}(\mathrm{X} \mid \mathrm{Y},\mathrm{Z}) + \mathrm{H}(\mathrm{Y} \mid \mathrm{Z}).
\end{aligned}$$

Corollaire **(1.2.6)**. — *Soit $\mathrm{X}_1,\dots,\mathrm{X}_n$ des variables aléatoires discrètes. On a*

$$\mathrm{H}(\mathrm{X}_1,\dots,\mathrm{X}_n) = \sum_{k=1}^{n} \mathrm{H}(\mathrm{X}_k \mid \mathrm{X}_1,\dots,\mathrm{X}_{k-1}).$$

Démonstration. — En effet, on a

$$\begin{aligned}\mathrm{H}(\mathrm{X}_1,\dots,\mathrm{X}_n) &= \mathrm{H}(\mathrm{X}_1) + \mathrm{H}(\mathrm{X}_2,\dots,\mathrm{X}_n \mid \mathrm{X}_1)\\ &= \mathrm{H}(\mathrm{X}_1) + \mathrm{H}(\mathrm{X}_2 \mid \mathrm{X}_1) + \mathrm{H}(\mathrm{X}_3,\dots,\mathrm{X}_n \mid \mathrm{X}_1,\mathrm{X}_2)\\ &= \dots\\ &= \mathrm{H}(\mathrm{X}_1) + \mathrm{H}(\mathrm{X}_2 \mid \mathrm{X}_1) + \mathrm{H}(\mathrm{X}_3 \mid \mathrm{X}_1,\mathrm{X}_2) + \dots\\ &\qquad + \mathrm{H}(\mathrm{X}_n \mid \mathrm{X}_1,\mathrm{X}_2,\dots,\mathrm{X}_{n-1}),\end{aligned}$$

ce qu'il fallait démontrer □

1.3. Information mutuelle

Définition **(1.3.1)**. — *Soit p, q des lois discrètes sur un ensemble* A. *On appelle* divergence *de p par rapport à q l'expression*

$$\mathrm{D}(p \mid q) = \sum_{\substack{a\in\mathrm{A}\\ p(a)>0}} p(a)\log\left(\frac{p(a)}{q(a)}\right).$$

Rien ne garantit, a priori, que cette famille soit sommable ; d'ailleurs, s'il existe un élément a tel que $p(a) > 0$ et $q(a) = 0$, on a $\mathrm{D}(p \mid q) = +\infty$. On va en fait vérifier que la famille $(p(a) \inf \log(p(a)/q(a), 0))$ est sommable, ce qui entraîne que $\mathrm{D}(p \mid q)$ est un élément bien défini de $[0; +\infty]$.

Théorème **(1.3.2)**. — *Soit p, q des lois discrètes sur un ensemble* A. *La famille* $(p(a) \inf \log(p(a)/q(a), 0))$ *est sommable ; on a* $\mathrm{D}(p \mid q) \geqslant 0$*, avec égalité si et seulement si* $p = q$.

Démonstration. — La fonction logarithme est strictement concave ; son graphe donc en-dessous de sa tangente en tout point, et ne coupe cette tangente qu'un le point. En particulier, pour tout $x \in \mathbf{R}_{>0}$, on a $\log(x) \leqslant x - 1$ (inégalité que l'on peut aussi vérifier par analyse de fonction, ou bien par la formule de Taylor), et l'inégalité est stricte si $x \neq 1$. On écrit plutôt

$$\log\frac{1}{x} = -\log x \geqslant 1 - x,$$

avec égalité si et seulement si $x = 1$. Appliquons cette inégalité à $x = q(a)/p(a)$, pour $a \in \mathrm{A}$ tel que $p(a) > 0$. Il vient

$$\log \frac{p(a)}{q(a)} \geqslant 1 - \frac{q(a)}{p(a)} = \frac{p(a) - q(a)}{p(a)},$$

d'où

$$p(a) \log \frac{p(a)}{q(a)} \geqslant p(a) - q(a),$$

avec égalité si et seulement si $q(a) = p(a) > 0$. En sommant sur l'ensemble des valeurs de a telles que $p(a) > 0$, on obtient

$$\mathrm{D}(p \mid q) \geqslant 1 - \sum_{\substack{a \in \mathrm{A} \\ p(a)>0}} q(a) \geqslant 0.$$

Supposons qu'il y ait égalité $\mathrm{D}(p \mid q) = 0$. Alors $q(a) = p(a)$ pour tout a tel que $p(a) > 0$, d'où

$$\begin{aligned} 1 = \sum_{a \in \mathrm{A}} q(a) &= \sum_{p(a)=0} q(a) + \sum_{p(a)>0} q(a) \\ &= \sum_{p(a)=0} q(a) + \sum_{p(a)>0} p(a) = \sum_{p(a)=0} q(a) + 1, \end{aligned}$$

si bien que $q(a) = 0$ dès que $p(a) = 0$. On a donc $p = q$. Inversement, si $p = q$, la définition de la divergence entraîne immédiatement que $\mathrm{D}(p \mid q) = 0$. □

Remarque **(1.3.3)**. — Dans la littérature, la quantité $\mathrm{D}(p \mid q)$ s'appelle *divergence de Kullback-Leibler*, ou aussi distance de Kullback-Leibler. De fait, elle mesure la différence entre les deux lois de probabilité p et q : elle est positive, et ne s'annule que lorsque $p = q$. Mais ce n'est pas tout à fait une distance, car elle n'est pas symétrique et ne vérifie pas l'inégalité triangulaire. D'ailleurs, d'autres expressions ont les mêmes propriétés et peuvent rendre des services similaires ; comme nous ne les utiliserons pas dans ce cours, nous avons préféré l'expression *divergence*. Mentionnons aussi que sa notation habituelle est $\mathrm{D}(p \,||\, q)$.

1.3.4. — Soit X et Y des variables aléatoires discrètes. Sur l'ensemble des valeurs possibles du couple (X, Y), on dispose alors de deux lois discrètes :

a) La loi du couple (X, Y), c'est-à-dire $(x, y) \mapsto \mathbf{P}(\mathrm{X} = x, \mathrm{Y} = y)$;

b) Le produit des deux lois marginales de ce couple, c'est-à-dire $(x, y) \mapsto \mathbf{P}(\mathrm{X} = x)\mathbf{P}(\mathrm{Y} = y)$.

Définition **(1.3.5)**. — *Soit* X *et* Y *des variables aléatoires discrètes. On appelle* information mutuelle *de* X *et* Y *la divergence de la loi du couple* (X, Y) *par rapport à la loi* $(x, y) \mapsto \mathbf{P}(X = x)\mathbf{P}(Y = y)$*, produit des deux lois marginales du couple* (X, Y).

Explicitement, on a donc

$$I(X, Y) = \sum_{x,y} \mathbf{P}(X = x \text{ et } Y = y) \log\left(\frac{\mathbf{P}(X = x \text{ et } Y = y)}{\mathbf{P}(X = x)\mathbf{P}(Y = y)}\right).$$

Corollaire **(1.3.6)**. — *Soit* X *et* Y *des variables aléatoires discrètes. L'information mutuelle* $I(X, Y)$ *est un élément de* $[0; +\infty]$*; il est nul si et seulement si* X *et* Y *sont indépendantes.*

Démonstration. — L'inégalité $I(X, Y) \geqslant 0$ est un cas particulier du théorème. De plus, il y a égalité $I(X, Y) = 0$ si et seulement si

$$\mathbf{P}(X = x, Y = y) = \mathbf{P}(X = x)\mathbf{P}(Y = y)$$

pour tout couple (x, y), ce qui signifie exactement que X et Y sont indépendantes. □

Corollaire **(1.3.7)**. — *Soit* X *et* Y *des variables aléatoires discrètes. On a les égalités*

(1.3.7.1) $$H(X) = I(X, Y) + H(X \mid Y)$$

(1.3.7.2) $$H(X, Y) + I(X, Y) = H(X) + H(Y).$$

En particulier, on a l'inégalité

(1.3.7.3) $$H(X \mid Y) \leqslant H(X).$$

Dans le cas où l'entropie de X *est finie, on a égalité* $H(X) = H(X \mid Y)$ *si et seulement si* X *et* Y *sont indépendantes.*

Si l'entropie d'une variable aléatoire est une mesure d'incertitude, la conditionner à une seconde variable aléatoire diminue cette incertitude.

Démonstration. — Lorsque toutes ces quantités sont finies, on peut utiliser la proposition 1.2.3 et écrire

$$\begin{aligned} H(X) - H(X \mid Y) &= H(X) + H(Y) - H(X, Y) \\ &= \sum_{x,y} \sum_{x} \mathbf{P}(X = x, Y = y) \log \frac{\mathbf{P}(X = x)\mathbf{P}(Y = y)}{\mathbf{P}(X = x, Y = y)} \\ &= I(X, Y), \end{aligned}$$

d'où la première relation.

Dans le cas général, le fait que ces termes puissent a priori être infinis oblige à reprendre des calculs faits dans la démonstration de la proposition 1.2.3. Reprenons les notations introduites dans cette démonstration en posant $p_x = \mathbf{P}(\mathrm{X} = x)$, $q_y = \mathbf{P}(\mathrm{Y} = y)$ et $r_{xy} = \mathbf{P}(\mathrm{X} = x \text{ et } \mathrm{Y} = y)$. En revenant à la définition de l'information mutuelle $\mathrm{I}(\mathrm{X}, \mathrm{Y})$ et de l'entropie conditionnelle $\mathrm{H}(\mathrm{X} \mid \mathrm{Y})$, on écrit

$$\begin{aligned}
\mathrm{I}(\mathrm{X}, \mathrm{Y}) + \mathrm{H}(\mathrm{X} \mid \mathrm{Y}) &= \sum_{x,y} r_{xy} \log \frac{r_{xy}}{p_x q_y} + \sum_y q_y \mathrm{H}(\mathrm{X} \mid \mathrm{Y} = y) \\
&= \sum_{x,y} r_{xy} \log \frac{r_{xy}}{p_x q_y} + \sum_y q_y \sum_x -\frac{r_{xy}}{q_y} \log \frac{r_{xy}}{q_y} \\
&= \sum_{x,y} r_{xy} \log \frac{r_{xy}}{p_x q_y} + \sum_{x,y} q_y \sum_x -\frac{r_{xy}}{q_y} \log \frac{r_{xy}}{q_y} \\
&= \sum_{x,y} r_{xy} \log \frac{r_{xy}}{p_x q_y} + \sum_{x,y} r_{xy} \log \frac{q_y}{r_{xy}} \\
&= \sum_{x,y} r_{xy} \log \frac{1}{p_x} \\
&= \sum_x p_y \log \frac{1}{p_x} \\
&= \mathrm{H}(\mathrm{X}).
\end{aligned}$$

En ajoutant $\mathrm{H}(\mathrm{Y})$ aux deux termes de cette première relation, on obtient la seconde : $\mathrm{H}(\mathrm{X}, \mathrm{Y}) + \mathrm{I}(\mathrm{X}, \mathrm{Y}) = \mathrm{H}(\mathrm{Y}) + \mathrm{H}(\mathrm{X} \mid \mathrm{Y}) + \mathrm{I}(\mathrm{X}, \mathrm{Y}) = \mathrm{H}(\mathrm{Y}) + \mathrm{H}(\mathrm{X})$.

Comme $\mathrm{I}(\mathrm{X}, \mathrm{Y}) \geqslant 0$, l'inégalité finale découle également de la première relation, de même que son cas d'égalité lorsque l'entropie de X est finie. En effet, comme $\mathrm{I}(\mathrm{X}, \mathrm{Y})$ et $\mathrm{H}(\mathrm{X} \mid \mathrm{Y})$ appartiennent à $[0; +\infty]$ et comme leur somme est égale à $\mathrm{H}(\mathrm{X})$, ces quantités sont toutes finies ; l'égalité $\mathrm{H}(\mathrm{X}) = \mathrm{H}(\mathrm{X} \mid \mathrm{Y})$ équivaut alors à $\mathrm{I}(\mathrm{X}, \mathrm{Y}) = 0$, c'est-à-dire, d'après le corollaire 1.3.6, à l'indépendance de X et Y. □

Définition **(1.3.8).** — *Soit* X, Y, Z *des variables aléatoires discrètes. On dit que* X *et* Z *sont* indépendantes conditionnellement à Y, *et l'on note* $\mathrm{X} \perp_{\mathrm{Y}} \mathrm{Z}$ *si l'on a*

$$\mathbf{P}(\mathrm{X} = x, \mathrm{Z} = z \mid \mathrm{Y} = y) = \mathbf{P}(\mathrm{X} = x \mid \mathrm{Y} = y)\mathbf{P}(\mathrm{Z} = z \mid \mathrm{Y} = y)$$

pour tous x, y, z *tels que* $\mathbf{P}(\mathrm{Y} = y) > 0$.

Exemple **(1.3.9)**. — S'il existe une fonction f telle que $\mathrm{Z} = f(\mathrm{Y})$, alors $\mathrm{X} \perp_{\mathrm{Y}} \mathrm{Z}$. En particulier, X et Y sont indépendantes conditionnellement à Y.

Soit en effet x, y, z tels que $\mathbf{P}(\mathrm{Y} = y) > 0$. Si $z \neq f(y)$, on a $\mathbf{P}(\mathrm{X} = x, \mathrm{Z} = z \mid \mathrm{Y} = y) = 0$ et $\mathbf{P}(\mathrm{Z} = z \mid \mathrm{Y} = y) = 0$. En revanche, si $z = f(y)$, on a $\mathbf{P}(\mathrm{X} = x, \mathrm{Z} = z \mid \mathrm{Y} = y) = \mathbf{P}(\mathrm{X} = x \mid \mathrm{Y} = y)$ et $\mathbf{P}(\mathrm{Z} = z \mid \mathrm{Y} = y) = 1$. Dans les deux cas, l'égalité voulue est vérifiée.

1.3.10. — Pour étudier cette notion d'indépendance conditionnelle de X, Z relativement à la variable aléatoire Y, il est utile d'introduire la notion d'*information mutuelle de* X, Z *conditionnellement à* Y, définie par

$$\mathrm{I}(\mathrm{X}, \mathrm{Z} \mid \mathrm{Y}) = \sum_{y} \mathbf{P}(\mathrm{Y} = y)\mathrm{I}(\mathrm{X} \mid \mathrm{Y} = y, \mathrm{Z} \mid \mathrm{Y} = y).$$

C'est un élément de $[0; +\infty]$, nul si et seulement si $\mathrm{I}(\mathrm{X} \mid \mathrm{Y} = y, \mathrm{Z} \mid \mathrm{Y} = y)$ pour tout y tel que $\mathbf{P}(\mathrm{Y} = y) > 0$, c'est-à-dire si X et Z sont indépendantes conditionnellement à Y.

Par ailleurs,

$$\begin{aligned}
\mathrm{I}(\mathrm{X}, (\mathrm{Y}, \mathrm{Z})) &= \sum_{x,y,z} \mathbf{P}(\mathrm{X} = x, \mathrm{Y} = y, \mathrm{Z} = z) \log \frac{\mathbf{P}(\mathrm{X} = x, \mathrm{Y}, y, \mathrm{Z} = z)}{\mathbf{P}(\mathrm{X} = x)\mathbf{P}(\mathrm{Y} = y, \mathrm{Z} = z)} \\
&= \sum_{x,y,z} \mathbf{P}(\mathrm{X} = x, \mathrm{Y} = y, \mathrm{Z} = z) \log \frac{\mathbf{P}(\mathrm{X} = x, \mathrm{Y} = y, \mathrm{Z} = z)\mathbf{P}(\mathrm{Y} = y)}{\mathbf{P}(\mathrm{X} = x, \mathrm{Y} = y)\mathbf{P}(\mathrm{Y} = y, \mathrm{Z} = z)} \\
&\qquad + \sum_{x,y,z} \mathbf{P}(\mathrm{X} = x, \mathrm{Y} = y, \mathrm{Z} = z) \log \frac{\mathbf{P}(\mathrm{X} = x, \mathrm{Y} = y)}{\mathbf{P}(\mathrm{X} = x)\mathbf{P}(\mathrm{Y} = y))} \\
&= \sum_{y} \mathbf{P}(\mathrm{Y} = y) \times \\
&\times \left(\sum_{x,z} \mathbf{P}(\mathrm{X} = x, \mathrm{Z} = z \mid \mathrm{Y} = y) \log \frac{\mathbf{P}(\mathrm{X} = x, \mathrm{Z} = z \mid \mathrm{Y} = y)}{\mathbf{P}(\mathrm{X} = x \mid \mathrm{Y} = y)\mathbf{P}(\mathrm{Z} = z \mid \mathrm{Y} = y)} \right) \\
&\qquad + \sum_{x,y} \mathbf{P}(\mathrm{X} = x, \mathrm{Y} = y) \log \frac{\mathbf{P}(\mathrm{X} = x, \mathrm{Y} = y)}{\mathbf{P}(\mathrm{X} = x)\mathbf{P}(\mathrm{Y} = y))} \\
&= \mathrm{I}(\mathrm{X}, \mathrm{Z} \mid \mathrm{Y}) + \mathrm{I}(\mathrm{X}, \mathrm{Y}).
\end{aligned}$$

Par symétrie, on a également

$$\mathrm{I}(\mathrm{X}, (\mathrm{Y}, \mathrm{Z})) = \mathrm{I}(\mathrm{X}, \mathrm{Y} \mid \mathrm{Z}) + \mathrm{I}(\mathrm{X}, \mathrm{Z}),$$

de sorte que $\mathrm{I}(\mathrm{X}, \mathrm{Y} \mid \mathrm{Z}) \geqslant 0$, et $\mathrm{I}(\mathrm{X}, (\mathrm{Y}, \mathrm{Z})) \geqslant \mathrm{I}(\mathrm{X}, \mathrm{Z})$.

Dans l'hypothèse où X et Z sont conditionnellement indépendantes relativement à Y, on a $\mathrm{I}(\mathrm{X}, \mathrm{Z} \mid \mathrm{Y}) = 0$. Ces deux expressions pour $\mathrm{I}(\mathrm{X}, (\mathrm{Y}, \mathrm{Z}))$ entraînent alors l'inégalité du traitement de données — en anglais, *data processing inequality* :

Théorème **(1.3.11)**. — *Soit* X, Y, Z *des variables aléatoires discrètes. Si* $\mathrm{X} \perp_{\mathrm{Y}} \mathrm{Z}$*, alors* $\mathrm{I}(\mathrm{X}, \mathrm{Y}) \geqslant \mathrm{I}(\mathrm{X}, \mathrm{Z})$*, avec égalité si et seulement si* $\mathrm{X} \perp_{\mathrm{Z}} \mathrm{Y}$.

Démonstration. — Puisque, par hypothèse, X et Z sont conditionnellement indépendantes relativement à Y, on a $\mathrm{I}(\mathrm{X}, \mathrm{Z} \mid \mathrm{Y}) = 0$, d'où

$$\mathrm{I}(\mathrm{X}, (\mathrm{Y}, \mathrm{Z})) = \mathrm{I}(\mathrm{X}, \mathrm{Y} \mid \mathrm{Y}) + \mathrm{I}(\mathrm{X}, \mathrm{Y}) = \mathrm{I}(\mathrm{X}, \mathrm{Y}).$$

On a donc

$$\mathrm{I}(\mathrm{X}, \mathrm{Y}) - \mathrm{I}(\mathrm{X}, \mathrm{Z}) = \mathrm{I}(\mathrm{X}, (\mathrm{Y}, \mathrm{Z})) - \mathrm{I}(\mathrm{X}, \mathrm{Z}) = \mathrm{I}(\mathrm{X}, \mathrm{Y} \mid \mathrm{Z}).$$

Cela entraîne l'inégalité du traitement de données $\mathrm{I}(\mathrm{X}, \mathrm{Y}) \geqslant \mathrm{I}(\mathrm{X}, \mathrm{Z})$ ainsi que la caractérisation du cas d'égalité, par définition de l'information mutuelle conditionnelle $\mathrm{I}(\mathrm{X}, \mathrm{Y} \mid \mathrm{Z})$. □

Corollaire **(1.3.12)**. — *Soit* X, Y *des variables aléatoires discrètes et soit* f *une fonction. On a* $\mathrm{I}(\mathrm{X}, f(\mathrm{Y})) \leqslant \mathrm{I}(\mathrm{X}, \mathrm{Y})$*, avec égalité si et seulement si* $\mathrm{X} \perp_{f(\mathrm{Y})} \mathrm{Y}$.

Démonstration. — Posons $\mathrm{Z} = f(\mathrm{Y})$. On a vu dans l'exemple 1.3.9 que X et Z sont conditionnellement indépendantes relativement à Y. D'après le théorème 1.3.11, on a donc $\mathrm{I}(\mathrm{X}, f(\mathrm{Y})) = \mathrm{I}(\mathrm{X}, \mathrm{Z}) \geqslant \mathrm{I}(\mathrm{X}, \mathrm{Y})$, et le cas d'égalité s'obtient de même. □

1.4. Taux d'entropie

En théorie de l'information, les variables aléatoires ne représentent pas les messages (un texte, une photographie, un son) mais plutôt les éléments dont ce message est constitué (les lettres successives, les pixels et leur couleur, etc.). Dans le paragraphe précédent, nous avons appris à traiter plusieurs variables aléatoires comme une seule, en les regroupant en un vecteur, mais cette méthode fait perdre de vue l'idée d'une succession d'un grand nombre de symboles élémentaires.

C'est ainsi qu'on va maintenant s'intéresser à des suites infinies (X_n) de variables aléatoires indexées par l'ensemble des entiers naturels — ce qu'on appelle un *processus stochastique*.

Définition **(1.4.1)**. — *On appelle* taux d'entropie *d'un processus stochastique* $X = (X_n)$ *l'expression*

$$H(X) = \lim_{n\to\infty} \frac{1}{n+1} H(X_0, \dots, X_n),$$

pourvu que la limite existe.

En remplaçant la limite par des limites supérieure et inférieure, on définit les taux d'entropie supérieur, $\overline{H}(X)$, et inférieur, $\underline{H}(X)$. On a l'inégalité $\underline{H}(X) \leqslant \overline{H}(X)$; le taux d'entropie existe si et seulement si ces deux expressions coïncident, et il leur est alors égal.

Exemple **(1.4.2)**. — Soit (X_n) un processus stochastique. On suppose que les variables aléatoires X_n sont indépendantes. Alors,

$$\frac{1}{n+1} H(X_0, \dots, X_n) = \frac{1}{n+1} \sum_{k=0}^{n} H(X_k);$$

le taux d'entropie est alors la limite au sens de Cesáro de la suite $(H(X_n))$.

Supposons de plus que les variables aléatoires sont identiquement distribuées. Alors, $H(X_k) = H(X_0)$ pour tout k, et l'on a $H(X) = H(X_0)$.

Lemme **(1.4.3)** (Cesáro). — *Soit* (a_n) *une suite de nombres réels ; pour tout entier* $n \geqslant 0$, *posons* $A_n = (a_0 + \cdots + a_n)/(n+1)$. *On a les inégalités*

$$\underline{\lim}\, a_n \leqslant \underline{\lim}\, A_n \leqslant \overline{\lim}\, A_n \leqslant \overline{\lim}\, a_n.$$

En particulier, si la suite (a_n) *a une limite* ℓ *dans* $[-\infty; +\infty]$, *la suite* (A_n) *converge également vers* ℓ.

Démonstration. — Démontrons l'inégalité $\overline{\lim}\, A_n \leqslant \overline{\lim}\, a_n$. Il n'y a rien à démontrer lorsque $\overline{\lim}\, a_n = +\infty$; supposons donc que $\overline{\lim}\, a_n < \infty$ et soit λ un nombre réel tel que $\overline{\lim}\, a_n < \lambda$. Alors, par définition de la limite supérieure, il existe un entier N tel que, pour tout entier $n \geqslant N$, on ait $a_n \leqslant \lambda$. Pour $n \geqslant N$, on a alors

$$A_n = \frac{1}{n+1} \sum_{k=0}^{n} a_k = \frac{1}{n+1} \sum_{k=0}^{N-1} a_k + \frac{1}{n+1} \sum_{k=N}^{n} a_k \leqslant \frac{1}{n+1} \sum_{k=0}^{N-1} a_k + \frac{n+1-N}{n+1} \lambda.$$

Lorsque n tend vers l'infini, le membre de droite tend vers λ ; par suite, $\overline{\lim}\, A_n \leqslant \lambda$. Comme λ est arbitraire, on a $\overline{\lim}\, A_n \leqslant \overline{\lim}\, a_n$.

En remplaçant la suite (a_n) par la suite (b_n) définie par $b_n = -a_n$, la suite (A_n) est remplacée par la suite (B_n) définie par $B_n = -A_n$, et l'on a $\underline{\lim}\, a_n = -\overline{\lim}\, b_n$

et $\underline{\lim}\, \mathrm{A}_n = -\overline{\lim}\, \mathrm{B}_n$. L'inégalité de limites supérieures appliquée à la suite (b_n) entraîne alors que $\underline{\lim}\, a_n \leqslant \underline{\lim}\, \mathrm{A}_n$.

Lorsque la suite (a_n) converge vers un élément ℓ de $[-\infty;+\infty]$, on a $\underline{\lim}\, a_n = \ell = \overline{\lim}\, a_n$, et les inégalités précédentes entraînent que $\underline{\lim}\, \mathrm{A}_n = \overline{\lim}\, \mathrm{A}_n = \ell$, de sorte que la suite (A_n) converge vers ℓ. □

Définition **(1.4.4)**. — *On dit qu'un processus stochastique* (X_n) *est* stationnaire *si pour tout entier n et toute suite* $(x_0, \dots, x_m)$*, on a*

$$\mathbf{P}(\mathrm{X}_n = x_0, \mathrm{X}_{n+1} = x_1, \dots, \mathrm{X}_{n+m} = x_m) = \mathbf{P}(\mathrm{X}_0 = x_0, \mathrm{X}_1 = x_1, \dots, \mathrm{X}_m = x_m).$$

En particulier, pour $m = 0$, les termes d'un processus stationnaire ont même loi.

Proposition **(1.4.5)**. — *Soit* $\mathrm{X} = (\mathrm{X}_n)$ *un processus stochastique stationnaire. Alors, le taux d'entropie* $\mathrm{H}(\mathrm{X})$ *existe, et est donné par*

$$\mathrm{H}(\mathrm{X}) = \lim_{n\to\infty} \mathrm{H}(\mathrm{X}_n \mid \mathrm{X}_{n-1}, \dots, \mathrm{X}_0).$$

Démonstration. — Pour tout entier n, posons

$$\mathrm{H}'(\mathrm{X})_n = \mathrm{H}(\mathrm{X}_n \mid \mathrm{X}_{n-1}, \dots, \mathrm{X}_0).$$

Puisque l'entropie diminue par conditionnement, on a, pour tout entier n, l'inégalité

$$\mathrm{H}'(\mathrm{X})_{n+1} = \mathrm{H}(\mathrm{X}_{n+1} \mid \mathrm{X}_n, \dots, \mathrm{X}_0) \leqslant \mathrm{H}(\mathrm{X}_{n+1} \mid \mathrm{X}_n, \dots, \mathrm{X}_1).$$

Puisque le processus X est stationnaire,

$$\mathrm{H}(\mathrm{X}_{n+1} \mid \mathrm{X}_n, \dots, \mathrm{X}_1) = \mathrm{H}(\mathrm{X}_n \mid \mathrm{X}_{n-1}, \dots, \mathrm{X}_0) = \mathrm{H}'(\mathrm{X})_n.$$

Ainsi, la suite $(\mathrm{H}'(\mathrm{X}))_n$ est décroissante. Comme elle est positive, elle converge donc vers un élément de $[0;+\infty]$ que nous notons $\mathrm{H}'(\mathrm{X})$.

Alors, pour tout entier n, on a

$$\begin{aligned}\mathrm{H}(\mathrm{X}_0, \dots, \mathrm{X}_n) &= \mathrm{H}(\mathrm{X}_0) + \mathrm{H}(\mathrm{X}_1 \mid \mathrm{X}_0) + \cdots + \mathrm{H}(\mathrm{X}_n \mid \mathrm{X}_{n-1}, \dots, \mathrm{X}_0) \\ &= \sum_{k=0}^{n} \mathrm{H}'(\mathrm{X})_k,\end{aligned}$$

de sorte que la suite $(\frac{1}{n+1}\mathrm{H}(\mathrm{X}_0, \dots, \mathrm{X}_n))$ est la moyenne au sens de Cesáro de la suite $(\mathrm{H}'(\mathrm{X})_n)$. Elle converge donc vers sa limite, ce qu'il fallait démontrer. □

1.5. Taux d'entropie des processus markoviens

Deux hypothèses sur les variables aléatoires d'un processus stochastique nous ont permis d'étudier son taux d'entropie : l'indépendance et la stationarité. Ces deux hypothèses ne sont cependant pas très adaptées aux applications. L'indépendance contredit l'idée même que ces variables constituent un message qui a du sens ; de même, si un symbole est possible, tout redoublement, triplement, etc. de ce symbole sera possible, ce qui contredit l'absence de mots faisant intervenir 10 fois la lettre *t*, par exemple, ou bien l'observation qu'en français, la lettre *q* est presque toujours suivie d'un *u*. Quand à la stationarité néglige l'observation que le début ou la fin d'un message, ou encore le bord d'une image, sont de nature différente du cœur du message.

L'hypothèse markovienne que nous introduisons maintenant est déjà plus proche de la réalité. De manière intuitive, elle consiste à dire qu'une variable aléatoire X_{n+1} peut dépendre des précédentes, mais pas plus qu'au travers de la variable X_n. C'est le modèle des déambulations aléatoires dans une ville. Un exemple simple montrera ses limites en supposant que les X_n représentent des lettres : en permettant la sucession *tt*, il oblige à permettre le triplement *ttt*, etc.

Définition **(1.5.1)**. — *On dit qu'un processus stochastique* (X_n) *est* markovien *(ou est un processus de Markov, ou est une* chaîne de Markov*) si pour tout entier n,* $(X_0, \dots, X_{n-1})$ *et* X_{n+1} *sont conditionnellement indépendantes relativement à* X_n*.*

Cela signifie que pour tout entier n et toute suite $(x_0, \dots, x_{n+1})$, on a

$$\mathbf{P}(X_{n+1} = x_{n+1} \mid X_n = x_n, \dots, X_0 = x_0) = \mathbf{P}(X_{n+1} = x_{n+1} \mid X_n = x_n).$$

1.5.2. — Soit $X = (X_n)$ un processus markovien. On fait l'hypothèse supplémentaire qu'il est *homogène* c'est-à-dire que pour tout couple (a, b), on a

$$\mathbf{P}(X_{n+1} = b \mid X_n = a) = \mathbf{P}(X_1 = b \mid X_0 = a).$$

Supposons que l'ensemble A des valeurs possibles de (X_n) soit fini ; pour tout couple (a, b) d'éléments de A, posons $p_{a,b} = \mathbf{P}(X_1 = b \mid X_0 = a)$ et notons P la matrice $(p_{a,b})$.

C'est une matrice carrée à indices dans l'ensemble A ; même si A n'est pas forcément de la forme $\{1, \dots, m\}$, la théorie est identique. Les coefficients de la matrice P sont des probabilités conditionnelles ; ils sont donc positifs ou nuls.

Pour tout a, on a

$$\sum_{b\in \mathrm{A}} p_{a,b} = \sum_{b\in \mathrm{A}} \mathbf{P}(\mathrm{X}_1 = b \mid \mathrm{X}_0 = a) = 1.$$

Autrement dit la somme des coefficients de chaque ligne de P est égale à 1. On dit que P est une *matrice stochastique.*

La matrice P est appelée la *matrice de transition du processus markovien* X.

Dans le vocabulaire des chaînes de Markov, les éléments de A sont appelés *états*, et $p_{a,b}$ est la probabilité de passage de l'état a à l'état b. On représente souvent une telle chaîne par un *carquois* (ou *graphe orienté*) dont les *sommets* sont les états de la chaîne, muni pour chaque couple d'états (a, b), d'une *flèche* de l'état a à l'état b étiquetée de la probabilité $p_{a,b}$.

Ainsi, le carquois de la figure 1.5.2.1 représente une chaîne de Markov à deux états $\{a, b\}$. La probabilité de passer de a à b est égale à p, celle de passer de b à a est égale à q. Sa matrice de transition est ainsi donnée par

$$\mathrm{P} = \begin{pmatrix} 1-p & p \\ q & 1-q \end{pmatrix}.$$

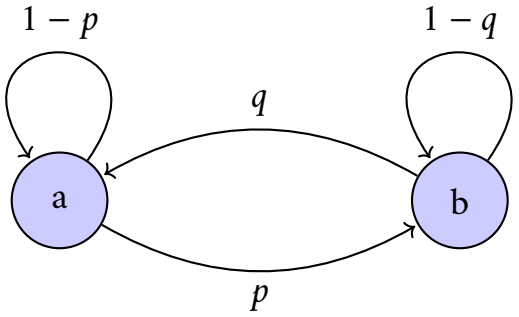


FIGURE 1.5.2.1. Une chaîne de Markov à deux états.

Si $\mathrm{M} = (\mu_a)$ est la loi de X_n, considérée comme un vecteur-ligne, la loi $\mathrm{M}' = (\mu'_a)$ de X_{n+1} est donnée par

$$\mu'_a = \mathbf{P}(\mathrm{X}_{n+1} = a) = \sum_{b\in \mathrm{A}} \mathbf{P}(\mathrm{X}_n = b) \cdot \mathbf{P}(\mathrm{X}_{n+1} = a \mid \mathrm{X}_n = b) = \sum_{b\in \mathrm{A}} \mu_b p_{b,a}.$$

Autrement dit, on a $\mathrm{M}' = \mathrm{MP}$.

Par récurrence, si le vecteur M représente la loi de X_0, la loi de X_n est représentée par le vecteur MP^n.

Proposition **(1.5.3)**. — *Soit* $X = (X_n)$ *un processus markovien homogène. Soit* A *l'ensemble des valeurs de* X_0*, soit* $P = (p_{a,b})$ *la matrice de transition de* X *et soit* $M = (\mu_a)$ *la loi de* X_0*. Pour que* X *soit stationnaire, il faut et il suffit que l'on ait* M = MP*. Dans ce cas, on a*

$$H(X) = -\sum_{a,b} \mu_a p_{a,b} \log(p_{a,b}).$$

Démonstration. — Si X est stationnaire, alors X_0 et X_1 ont même loi, donc M = MP. Supposons inversement que M = MP et prouvons que X est un processus stationnaire. On sait déjà que pour tout entier n, la loi de X_n est donnée par M. Démontrons par récurrence sur m que $\mathbf{P}(X_n = x_0, \dots, X_{n+m} = x_m) = \mathbf{P}(X_0 = x_0, \dots, X_m = x_m)$ pour tout entier m, tous $x_0, \dots, x_m \in A$ et tout $n \in \mathbf{N}$. Par définition d'un processus markovien homogène, on a

$$\begin{aligned}
&\mathbf{P}(X_n = x_0, \dots, X_{n+m} = x_m) \\
&= \mathbf{P}(X_{n+m} = x_m \mid X_n = x_0, \dots, X_{n+m-1} = x_{m-1}) \cdot \mathbf{P}(X_n = x_0, \dots, X_{n+m-1} = x_{m-1}) \\
&= \mathbf{P}(X_{n+m} = x_m \mid X_{n+m-1} = x_{m-1}) \cdot \mathbf{P}(X_n = x_0, \dots, X_{n+m-1} = x_{m-1}) \\
&= \mathbf{P}(X_1 = x_m \mid X_0 = x_{m-1}) \cdot \mathbf{P}(X_n = x_0, \dots, X_{n+m-1} = x_{m-1}).
\end{aligned}$$

Par l'hypothèse de récurrence, on a

$$\mathbf{P}(X_n = x_0, \dots, X_{n+m-1} = x_{m-1}) = \mathbf{P}(X_0 = x_0, \dots, X_{m-1} = x_{m-1}).$$

Ainsi

$$\begin{aligned}
&\mathbf{P}(X_n = x_0, \dots, X_{n+m} = x_m) \\
&\qquad = \mathbf{P}(X_1 = x_m \mid X_0 = x_{m-1}) \cdot \mathbf{P}(X_0 = x_0, \dots, X_{m-1} = x_{m-1}) \\
&\qquad = \mathbf{P}(X_0 = x_0, \dots, X_{m-1} = x_{m-1}, X_m = x_m)
\end{aligned}$$

en utilisant une fois de plus l'hypothèse que le processus X est markovien. Cela prouve que X est un processus stationnaire.

Supposons maintenant que X est stationnaire. Pour tout entier n, on a $H(X_n \mid X_{n-1}, \dots, X_0) = H(X_n \mid X_{n-1})$, par la propriété markovienne, puis $H(X_n \mid X_{n-1}) = H(X_1 \mid X_0)$ par stationarité. On a ainsi $H(X_n \mid X_{n-1}, \dots, X_0) = H(X_1 \mid X_0)$, d'où la formule $H(X) = H(X_1 \mid X_0)$ en vertu de la proposition 1.4.5.

Par ailleurs, la définition de l'entropie conditionnelle entraîne

$$H(X_1 \mid X_0) = \sum_a \mathbf{P}(X_0 = a) H(X_1 \mid X_0 = a) = -\sum_a \mu_a \sum_b p_{a,b} \log(p_{a,b}),$$

ainsi qu'il fallait démontrer. □

Exemple **(1.5.4)**. — Reprenons l'exemple d'une chaîne de Markov X à deux états $\{a, b\}$ représentée par le graphe de la figure 1.5.2.1.

Les lois de X_0 pour lesquelles cette chaîne est stationnaire sont données par un vecteur (μ, ν) tel que

$$\begin{cases} \mu(1-p) + \nu q &= \mu \\ \mu p + \nu(1-q) &= \nu \end{cases}$$

On obtient l'égalité $p\mu = q\nu$. Joint à la condition $\mu + \nu = 1$, on voit qu'il existe une unique telle loi, donnée par

$$(\mu, \nu) = \left(\frac{q}{p+q}, \frac{p}{p+q}\right).$$

Alors, le taux d'entropie de X est égal à

$$\begin{aligned} \mathrm{H}(\mathrm{X}) &= \frac{q}{p+q}\left(-(1-p)\log(1-p) - p\log(p)\right) \\ &\qquad + \frac{p}{p+q}\left(-q\log(q) - (1-q)\log(1-q)\right) \\ &= \frac{q}{p+q}h(p) + \frac{p}{p+q}h(q), \end{aligned}$$

où h est la fonction entropie représentée dans la figure 1.1.6.2.

Par ailleurs, la loi de X_n est, pour tout entier n, donnée par (μ, ν), de sorte que l'entropie de X_n est égale à

$$\mathrm{H}(\mathrm{X}_n) = -\frac{q}{p+q}\log\left(\frac{q}{p+q}\right) - \frac{p}{p+q}\log\left(\frac{p}{p+q}\right) = h\Big(\frac{p}{p+q}\Big).$$

On peut se demander quelles valeurs de p et q rendent ces expressions extrémales. Rappelons que la fonction h est nulle en 0 et 1, strictement croissante sur $[0; 1/2]$ et strictement décroissante sur $[1/2; 1]$. Ainsi, $\mathrm{H}(\mathrm{X}_n) = 0$ si et seulement si $p/(p+q) = 0$ ou 1, c'est-à-dire $p = 0$ ou $q = 0$; et $\mathrm{H}(\mathrm{X}_n)$ est maximal lorsque $p/(p+q) = 1/2$, c'est-à-dire $p = q$.

La fonction h est également concave. L'inégalité de concavité fournit :

$$\mathrm{H}(\mathrm{X}) = \frac{q}{q+p}h(p) + \frac{p}{p+q}h(q) \geqslant h\Big(\frac{q}{q+p}p + \frac{p}{p+q}q\Big) = h\Big(\frac{2pq}{p+q}\Big),$$

avec égalité si et seulement si $p = q$. D'autre part, $h(2pq/(p+q))$ est maximal lorsque $2pq/(p+q) = 1/2$, c'est-à-dire $4pq = p + q$. Finalement, on trouve que $\mathrm{H}(\mathrm{X})$ est maximal si et seulement si $p = q = 1/2$.

1.5.5. — Soit $X = (X_n)$ une chaîne de Markov homogène à ensemble d'états A fini ; soit $P = (p_{a,b})$ sa matrice de transition. On dit que la chaîne X, ou que la matrice stochastique P, est *primitive* s'il existe un entier $m \geqslant 1$ tel que tous les coefficients de la matrice P^m soient strictement positifs.

Théorème **(1.5.6)** (O. Perron, 1907). — *Soit* P *une matrice stochastique primitive. La suite de matrices* (P^n) *converge ; sa limite* Q *est une matrice stochastique de rang* 1.

Démonstration. — On munit $\mathbf{R}^A$ de la norme définie par $\|X\| = \sum_{a\in A}|x_a|$, pour $X = (x_a)$; on pose aussi $f(X) = \sum_{a\in A} x_a$.

La démonstration du théorème requiert plusieurs étapes. On note Σ l'ensemble des $X \in \mathbf{R}_+^A$ tels que $f(X) = 1$; c'est une partie convexe et compacte de $\mathbf{R}^A$. Soit m un entier $\geqslant 1$ tel que tous les coefficients $(p'_{a,b})$ de la matrice $P' = P^m$ soient strictement positifs ; notons c leur borne inférieure.

a) *Pour tout* $X \in \mathbf{R}^A$, *on a* $\|XP\| \leqslant \|X\|$ *et* $f(XP) = f(X)$.

Soit $X \in \mathbf{R}^A$. Posons $Y = XP$; on a $Y = (y_b)$, avec $y_b = \sum_a x_a p_{a,b}$. Grâce à l'inégalité triangulaire, on a

$$\|Y\| = \sum_{b\in A}|y_b| \leqslant \sum_{a,b}|x_a|p_{a,b} = \sum_a|x_a| \sum_b p_{a,b} = \sum_a|x_a| = \|X\|,$$

ce qui prouve l'inégalité voulue.

De même,

$$f(Y) = \sum_b y_b = \sum_{a,b} x_a p_{a,b} = \sum_a x_a = f(X).$$

b) *Pour tout* $X \in \mathbf{R}_+^A$, *les coefficients de* XP *sont positifs, et ceux de* XP′ *sont supérieurs à* $c\,\|X\|$.

Soit $X \in \mathbf{R}_+^A$. Posons $Y = XP$ et notons $Y = (y_b)$. On a $y_b = \sum_a x_a p_{a,b}$; on voit donc que $y_b \geqslant 0$ pour tout b.

De même, posons $Z = XP' = (z_b)$. Puisque $p'_{a,b} \geqslant c$ et $x_a \geqslant 0$ pour tous a, b, on a

$$z_b = \sum_a x_a p'_{a,b} \geqslant \sum_a x_a c = c.$$

c) *Soit* $X \in \mathbf{R}^A$ *tel que* $f(X) = 0$. *Alors,* $\|XP'\| \leqslant (1 - c\,\mathrm{Card}(A))\,\|X\|$.

Soit $Z = XP'$; notons $Z = (z_b)$, de sorte que $z_b = \sum_a x_a p'_{a,b}$. Comme $\sum x_a = 0$, on a aussi $z_b = \sum_a x_a(p'_{a,b} - c)$, de sorte que

$$|z_b| \leqslant \sum_a|x_a|(p'_{a,b} - c) \leqslant \sum_a|x_a|p'_{a,b} - c\,\|X\|.$$

En sommant sur b, on obtient

$$\|Z\| \leqslant \|X\| - c\,\mathrm{Card}(A)\,\|X\| = (1 - c\,\mathrm{Card}(A))\,\|X\|\,.$$

d) *L'ensemble* Σ *est stable par l'application* $X \mapsto XP'$*, et cette application est contractante pour la norme* $\|\cdot\|$.

La stabilité de Σ découle de ce qui a été dit plus haut. Par ailleurs, soit X, X' des éléments de Σ ; posons $Y = XP'$ et $Y' = X'P'$. On a $f(X' - X) = 0$ et $Y' - Y = (X' - X)P'$; alors

$$\|Y' - Y\| \leqslant (1 - c\,\mathrm{Card}(A))\,\|X' - X\|\,,$$

d'où l'assertion pusique $1 - c\,\mathrm{Card}(A) < 1$.

e) *La suite de matrices* $((P')^n)$ *converge ; sa limite est une matrice stochastique de rang* 1.

D'après le théorème du point fixe de Picard, l'application $X \mapsto XP'$ possède un unique point fixe M dans Σ et, pour tout vecteur $X \in \Sigma$, la suite $(X(P')^n)$ converge vers M.

L'espace Σ contient les vecteurs X_a de la base canonique. Pour chacun d'entre eux, on a donc $X_a(P')^n \longrightarrow M$. Cela prouve que la ligne a de la suite de matrices $((P')^n)$ converge vers M. La suite $((P')^n)$ converge donc vers la matrice Q dont toutes les lignes sont égales à M ; c'est une matrice stochastique de rang 1.

f) *La suite de matrices* (P^n) *converge vers* Q.

En écrivant la division euclidienne de n par m, $n = mk + d$, où $0 \leqslant d \leqslant m - 1$, on a $P^n = P^d(P')^k$. Supposons que n tende vers l'infini en restant dans la classe de d modulo m ; on a donc $P^n \longrightarrow P^dQ$. Or, comme toutes les vecteurs-ligne de P^d appartiennent à Σ, on a $P^dQ = Q$. Par suite, toutes ces sous-suites ont même limite, Q, ce qui entraîne que P^n converge vers Q. □

Remarque **(1.5.7)**. — Toutes les lignes de la matrice Q sont égales à un même vecteur M à coefficients positifs, de somme égale à 1. On a $MP = M$, ce qui prouve que M est un « vecteur propre » à gauche de P, pour la valeur propre 1.

Soit N un vecteur propre à gauche de P pour une valeur propre λ. On a donc $NP = \lambda N$ puis, par itération, $NP^n = \lambda^n N$ pour tout n. Lorsque n tend vers l'infini, le membre de gauche tend vers NQ. Comme $N \neq 0$, cela entraîne que la suite (λ^n) converge : on a donc $\lambda = 1$ ou $|\lambda| < 1$.

Supposons $\lambda = 1$. Soit $X = N - f(N)M$, de sorte que $f(X) = 0$. D'après le point c) de la preuve, on a donc $\|XQ\| \leqslant (1 - c\,\mathrm{Card}(A))\,\|X\|$. Or, $X = XP = XQ$, ce qui entraîne $X = 0$ et $N = f(N)M$.

Sous les conditions du théorème, la matrice P possède une unique valeur propre de module $\geqslant 1$; cette valeur propre est égale à 1 et l'espace propre (à gauche) correspondant est de dimension 1, engendré par M.

Théorème **(1.5.8)**. — *Soit* X *une chaîne de Markov homogène, à ensemble d'états fini,* primitive. *Soit* $P = (p_{a,b})$ *sa matrice de transitions et soit* $M = (\mu_a)$ *son unique loi stationnaire. Alors, le taux d'entropie existe et est donné par*

$$H(X) = \lim_{n\to\infty} H(X_n \mid X_{n-1}) = -\sum_{a,b} \mu_a p_{a,b} \log(p_{a,b}).$$

Démonstration. — Soit A l'ensemble des états de X et soit $M_0 = (m_a^{(0)})$ le vecteur de $\mathbf{R}^A$ décrivant la loi de X_0. Pour tout entier n, la loi de X_n est représentée par le vecteur $M_n = M_0 P^n = (m_a^{(n)})$. Par suite,

$$H(X_n \mid X_{n-1}) = \sum_a m_a^{(n-1)} H(X_n \mid X_{n-1} = a) = -\sum_{a,b} m_a^{(n-1)} p_{a,b} \log(p_{a,b}).$$

Puisque $m_a^{(n)} \to \mu_a$ pour tout a, on a donc

$$H(X_n \mid X_{n-1}) \to -\sum_{a,b} \mu_a p_{a,b} \log(p_{a,b}).$$

Notons $H'(X)$ cette expression.

Par ailleurs, on a

$$H(X_1, \ldots, X_n) = H(X_1) + H(X_2 \mid X_1) + \cdots + H(X_n \mid X_{n-1}, \ldots, X_1).$$

Comme X est un processur markovien, on a l'égalité

$$H(X_n \mid X_{n-1}, \ldots, X_1) = H(X_n \mid X_{n-1}),$$

si bien que

$$H(X_1, \ldots, X_n) = H(X_1) + \sum_{k=2}^{n} H(X_k \mid X_{k-1}).$$

D'après le lemme de Cesáro, on a donc

$$\frac{1}{n} H(X_1, \ldots, X_n) \to H'(X),$$

ce qui prouve que le taux d'entropie de X existe et est égal à $H'(X)$. □

Remarque **(1.5.9)**. — Soit X une chaîne de Markov homogène à ensemble d'états A fini et soit $\mathrm{P} = (p_{a,b})$ sa matrice de transition. Il y a un moyen géométrique commode pour déterminer si cette chaîne est primitive ou non. Considérons le carquois représentant cette chaîne dont on n'a conservé que les flèches étiquetées par une probabilité strictement positive. Le coefficient $p_{a,b}^{(m)}$ de la matrice P^m est la probabilité de passer de l'état a à l'état b en exactement m étapes et l'on a

$$p_{a,b}^{(m)} = \sum_{a_1,\dots,a_{m-1}\in \mathrm{A}} p_{a,a_1} p_{a_1,a_2} \cdots p_{a_{m-1},b}.$$

Par suite, $p_{a,b}^{(m)} > 0$ si et seulement s'il existe une suite $(a_0, \dots, a_m)$ d'états telle que $a_0 = a$, $a_m = b$, et telle que pour tout $j \in \{1, \dots, m\}$, $p_{a_i,a_j} > 0$; autrement dit, un « chemin » de longueur m dans le carquois associé à X qui emprunte les flèches de le sens indiqué.

Pour que la chaîne de Markov soit primitive, une condition nécessaire est qu'il existe, pour tout couple (a, b) d'états, un chemin reliant le sommet a au sommet b ; on dit que ce carquois est *connexe* (dans la terminologie des graphes, que ce graphe orienté est fortement connexe), ou que la chaîne est *irréductible*.

Cette condition n'est pas suffisante : il faut interdire, par exemple, que les états puissent être coloriés en deux couleurs et qu'aucune flèche ne relie des états de la même couleur. Dans ce cas, tout chemin entre deux états est de longueur paire si ces états sont de même couleur, et impaire sinon. La période de la chaîne est le pgcd des longueurs des chemins reliant un état à lui-même ; on dit qu'elle est *apériodique* si cette période est égale à 1.

On constate alors que la chaîne est primitive si et seulement elle est irréductible est apériodique.

Lorsque ces conditions ne sont pas satisfaites, on peut cependant s'y ramener. Parmi les états $a \in \mathrm{A}$, on considère le sous-ensemble A' de ceux qui sont récurrents, c'est-à-dire pour lesquels il existe des chemins de longueur arbitrairement longue qui y aboutissent. Les états de $\mathrm{A} - \mathrm{A}'$ n'ont pas grande importance dans l'étude asymptotique de le chaîne de Markov : si $a \notin \mathrm{A}'$, la probabilité $\mathbf{P}(\mathrm{X}_n = a)$ est nulle pour n assez grand (il suffit que n soit au moins égal au cardinal de $\mathrm{A}-\mathrm{A}'$). On considère une chaîne d'ensemble d'états A' en supprimant du carquois les sommets de $\mathrm{A} - \mathrm{A}'$ et les flèches correspondantes. Le carquois se décompose comme une réunion de sous-carquois connexes, aucune flèche ne reliant l'un à l'autre, ce qui ramène l'étude de la chaîne de Markov à l'étude indépendante

de sous-chaînes irréductibles. Si, enfin, la période d'une chaîne de Markov irréductible (X_n) est $d \geqslant 2$, on vérifie que les suites $(X_{nd+r})_n$ sont irréductibles et apériodiques ; leur étude permet de comprendre le comportement de la chaîne initiale.

1.6. Exercices

Exercice **(1.6.1)** (Fonction d'une variable aléatoire, I). — Geneviève se rend régulièrement à l'hippodrome, où se déroule une course entre huit chevaux. À la fin de la course, les gains de Geneviève dépendent de la performance du cheval sur lequel elle a misé : selon qu'il arrive en position 1, 2, 3, .., 8, ses gains sont respectivement de 100, 50, 50, 0, −10, −50, −50, −100 euros. On supposera toujours que tous les chevaux sont aussi bons les uns que les autres.

a) On note X la variable aléatoire correspondant aux gains de Geneviève. Calculer l'espérance de ses gains $\mathbf{E}(X)$, ainsi que leur entropie $H_2(X)$.

Lassée de perdre de l'argent sur le long terme, Geneviève décide de monétiser son activité en mettant en ligne des vidéos de réaction aux résultats des courses. Elle passe un contrat avec un network : ses gains sont désormais sécurisés et correspondent à *la valeur absolue* de ses gains initiaux (car le public l'apprécie tout autant quand elle s'énerve après avoir perdu).

b) On note $Y = |X|$ la variable aléatoire correspondant aux nouveaux gains de Geneviève. Calculer la loi q correspondant à ces gains.
On rappelle qu'étant donné une fonction f, la loi de la variable aléatoire image $f(X)$ est donnée par

$$\mathbf{P}(f(X) = y) = \sum_{\{x \in \mathcal{X} \,|\, f(x) = y\}} \mathbf{P}(X = x).$$

c) Calculer $\mathbf{E}(Y)$ et $H_2(Y)$. Que constate-t-on ?

Exercice **(1.6.2)**. — Une urne contient b boules blanches et r boules rouges. On note $X = (X_1, \ldots, X_5)$ (resp. $Y = (Y_1, \ldots, Y_5)$) la variable aléatoire correspondant au tirage de 5 boules dans l'urne avec replacement (resp. sans replacement). Laquelle de ces deux variables a la plus grande entropie ? Justifier.

Exercice **(1.6.3)** (Loi uniforme sur un ensemble fini). — Soit X une variable aléatoire discrète qui suit une loi de probabilité uniforme sur un ensemble

$\mathcal{X} = \{x_1, ..., x_n\}$ fini. Soit Y une autre variable aléatoire discrète sur $\mathcal{X}$, quelconque.

a) Donner, pour tout $x \in \mathcal{X}$, la valeur de $p(x) = \mathbf{P}(\mathrm{X} = x)$. En déduire la valeur de l'entropie $\mathrm{H}(\mathrm{X})$.

b) Démontrer que la fonction $x \mapsto x \log(x)$ sur $[0; 1]$ est strictement convexe. En déduire que si $q_1, \ldots, q_n$ sont des nombres réels de $[0; 1]$, de moyenne q, on a $q \log(q) \leqslant \frac{1}{n} \sum_{i=1}^{n} q_i \log(q_i)$, avec égalité si et seulement si $q_i = q$ pour tout i.

c) Démontrer que l'entropie que peut avoir une variable aléatoire sur $\mathcal{X}$ est toujours inférieure ou égale à $\log n$ et que la loi uniforme est l'unique loi de probabilité maximisant cette entropie.

d) Soit $q : \mathcal{X} \to [0, 1]$ la loi de Y. Démontrer que $\mathrm{D}(q \mid p) = \mathrm{H}(\mathrm{X}) - \mathrm{H}(\mathrm{Y})$. Retrouver le résultat de la question précédente.

Exercice **(1.6.4)** (Loi géométrique sur $\mathbf{N}$). — On tire une pièce à pile ou face pendant plusieurs tours, et ce jusqu'à ce que l'on obtienne une face. On note X la variable aléatoire sur $\mathbf{N}$ qui désigne le numéro du tour au cours duquel on a obtenu une face. Pour des raisons pratiques, on considère que le premier tirage correspond au tour 0, le second tirage au tour 1, etc. On suppose que la pièce est déséquilibrée : la probabilité de tirer une face à chaque tour est de $\alpha \in]0, 1[$.

a) Calculer $\mathbf{P}(\mathrm{X} = 0), \mathbf{P}(\mathrm{X} = 1), \mathbf{P}(\mathrm{X} = 2)$. Calculer, pour tout $k \in \mathbf{N}$, $\mathbf{P}(\mathrm{X} = k)$.

b) Calculer l'espérance $\mathbf{E}(\mathrm{X})$. *(On pourra utiliser la relation* $\sum_{k \in \mathbf{N}} k\beta^k = \frac{\beta}{(1-\beta)^2}$ *pour* $\beta < 1$*.)*

c) Montrer que $\mathrm{H}(\mathrm{X}) = -\log(\alpha) - \frac{1-\alpha}{\alpha} \log(1 - \alpha)$.

d) Soit $h(\alpha)$ l'entropie de X lorsque la probabilité de tirer face est α. Montrer que h est décroissante sur $]0; 1[$.

e) Calculer la limite de $h(\alpha)$ lorsque α tend vers 0 et 1. Existe-t-il une loi d'entropie maximale sur $\mathbf{N}$? *(On pourra utiliser le fait que* $\lim_{t \to 0} t \log t = 0$*.)*

f) Soit Y une variable aléatoire sur $\mathbf{N}$ telle que $\mathbf{E}(\mathrm{Y}) = \mathbf{E}(\mathrm{X}) > 0$. On note p et q les lois de X et Y, respectivement. Montrer que $\mathrm{H}(\mathrm{X}) - \mathrm{H}(\mathrm{Y}) = \mathrm{D}(q \mid p)$. *(Comparer avec l'exercice 1.6.3.)*

g) Montrer que parmi toutes les lois sur $\mathbf{N}$ ayant pour espérance $m > 0$, la loi géométrique X avec $\alpha = \frac{1}{1+m}$ est l'unique loi maximisant l'entropie. Exprimer cette entropie maximale en fonction de m.

Exercice **(1.6.5)** (Fonction d'une variable aléatoire, II). — Soit X une variable aléatoire discrète qui suit une loi de probabilité sur un ensemble $\mathcal{X}$; on note p sa loi. Soit $\mathcal{Y}$ un autre ensemble, soit $f : \mathcal{X} \to \mathcal{Y}$ une application et soit $\mathrm{Y} = f(\mathrm{X})$ la variable aléatoire image de X par f.

a) En utilisant la définition de l'entropie conditionnelle, démontrer que $\mathrm{H}(f(\mathrm{X}) \mid \mathrm{X}) = 0$. En déduire que $\mathrm{H}(\mathrm{X}, f(\mathrm{X})) = \mathrm{H}(\mathrm{X})$.

b) Démontrer que $\mathrm{H}(\mathrm{X}) \geqslant \mathrm{H}(f(\mathrm{X}))$.

c) On suppose que f est injective ; démontrer que $\mathrm{H}(\mathrm{X} \mid f(\mathrm{X})) = 0$ et que $\mathrm{H}(\mathrm{X}) = \mathrm{H}(f(\mathrm{X}))$.

d) Plus généralement, démontrer que $\mathrm{H}(\mathrm{X}) = \mathrm{H}(f(\mathrm{X}))$ si et seulement si la restriction de f à l'ensemble $\mathcal{X}'$ des $x \in \mathcal{X}$ tels que $\mathbf{P}(\mathrm{X} = x) > 0$ est injective.

e) Soit Y une une variable aléatoire discrète sur $\mathcal{Y}$ telle que $\mathrm{H}(\mathrm{Y} \mid \mathrm{X}) = 0$. Démontrer qu'il existe une fonction $g : \mathcal{X} \to \mathcal{Y}$ telle que $\mathrm{Y} = g(\mathrm{X})$ (presque sûrement). (*L'existence d'une telle fonction est équivalente à ce que pour tout $x \in \mathcal{X}$ tel que $p(x) > 0$, il existe un unique $y \in \mathcal{Y}$ vérifiant $q(x, y) > 0$, où q désigne la loi de la variable aléatoire conjointe* (X, Y).)

Exercice **(1.6.6)** (Mélanger accroit l'entropie). — On considère X une variable aléatoire discrète à valeurs dans un jeu de cartes, assimilé à l'ensemble $\mathcal{X} = \{1, \ldots, 52\}$. On considère également une variable aléatoire discrète S à valeurs dans le groupe $\mathfrak{S}_{52}$ des permutations de $\mathcal{X}$. On suppose que S et X sont indépendantes et on note $\mathrm{Y} = \mathrm{S}(\mathrm{X})$. La variable aléatoire discrète Y représente ainsi un jeu de cartes aléatoire mélangé de façon aléatoire.

a) On suppose que la variable aléatoire S est uniforme. Démontrer que Y est uniforme ; quelle est son entropie ? Pourquoi a-t-on $\mathrm{H}(\mathrm{Y}) \geqslant \mathrm{H}(\mathrm{X})$?

b) En général, démontrer que $\mathrm{H}(\mathrm{Y}) \geqslant \mathrm{H}(\mathrm{X})$. (*Justifier que* $\mathrm{H}(\mathrm{X}, \mathrm{S}) = \mathrm{H}(\mathrm{Y}, \mathrm{S})$ *et évaluer cette quantité de deux façons différentes.*)

Exercice **(1.6.7)** (Piocher et tirer, I). — On considère un sac contenant deux pièces lestées, que nous appellerons a et b. Chacune a une probabilité de tomber sur face égale à p et q, respectivement (où $p, q \in]0, 1[$). On choisit uniformément au hasard une pièce dans le sac, et on la tire à pile ou face plusieurs fois. On note Y

la v.a. sur $\{a, b\}$ désignant la pièce qui a été choisie, et X_n la v.a. sur {pile, face} désignant le résultat du n-ième tirage.

a) En calculant leur lois de probabilité, démontrer que X_1 et X_2 sont identiquement distribuées.

b) Les v.a. X_1 et X_2 sont-elles indépendantes ? On donnera la réponse en fonction de p et q.

c) Calculer $I(X_1; X_2 \mid Y)$ et $I(X_1, X_2)$.

Exercice **(1.6.8)** (Somme de variables aléatoires). — Soit X et Y des variables aléatoires discrètes à valeurs dans $\mathbf{R}$, et soit $Z = X + Y$.

a) Vérifier que $H(Z) \leqslant H(X) + H(Y)$.

b) Montrer que $H(Z \mid X) = H(Y \mid X)$.

c) Si X et Y sont indépendantes, en déduire que $\sup(H(X), H(Y)) \leqslant H(Z)$.

d) Trouver un exemple pour lequel $\inf(H(X), H(Y)) > H(Z)$.

Exercice **(1.6.9)**. — Étant données deux variables aléatoires discrètes X et Y, identiquement distribuées, d'entropie finie et non nulle, on pose $\rho(X; Y) = 1 - \frac{H(Y|X)}{H(X)}$.

a) Montrer que $\rho(X; Y) = \frac{I(X,Y)}{H(X)}$. En déduire que ρ est symétrique.

b) Montrer que $\rho(X; Y) \in [0, 1]$. À quoi correspondent les cas $\rho(X; Y) = 0, 1$?

Exercice **(1.6.10)**. — Étant données deux variables aléatoires discrètes, X et Y, on définit $\rho(X, Y) = H(X|Y) + H(Y|X)$.

a) Vérifier que $\rho(X, Y) = H(X, Y) - I(X, Y) = 2H(X, Y) - H(X) - H(Y)$.

b) Montrer que ρ vérifie les propriétés :

(i) $\rho(X, Y) \geqslant 0$;
(ii) $\rho(X, Y) = \rho(Y, X)$;
(iii) $\rho(X, Z) \leqslant \rho(X, Y) + \rho(Y, Z)$.

À quelle condition a-t-on $\rho(X, Z) = \rho(X, Y) + \rho(Y, Z)$?

c) Trouver une condition nécessaire et suffisante sur X et Y pour que $\rho(X, Y) = 0$.

L'application ρ sur les couples de variables aléatoires discrètes vérifie les propriétés qu'on exige usuellement d'une distance, avec deux modifications : elle peut être infinie, et elle peut s'annuler en un couple de variables aléatoires distinctes.

Exercice **(1.6.11)**. — Soit $\boldsymbol{X} = (\mathrm{X}_n)_{n\in\mathbf{N}}$ un processus stochastique sur un ensemble A fini (de cardinal $a \geqslant 1$).

a) Montrer que le taux d'entropie supérieur $\overline{\mathrm{H}}(\boldsymbol{X})$ est toujours inférieur ou égal à $\log(a)$.

b) Cette borne est-elle optimale ?

c) Que se passe-t-il si on remplace $\mathscr{X}$ par $\mathbf{N}$?

Exercice **(1.6.12)** (Piocher et tirer, II). — On reprend les notations et le contexte de l'exercice 1.6.7. On note $\boldsymbol{X} = (\mathrm{X}_n)_{n\in\mathbf{N}^*}$ le processus aléatoire formé par les tirages successifs de la pièce choisie au début de l'expérience.

a) Calculer $\lim\limits_{n\to+\infty} \frac{1}{n}\mathrm{H}(\mathrm{X}_1,\dots,\mathrm{X}_n \mid \mathrm{Y})$.

b) En déduire le taux d'entropie $\mathrm{H}(\boldsymbol{X})$.

c) Est-ce que $\boldsymbol{X}$ est une chaine de Markov homogène ?

Exercice **(1.6.13)** (Convergence vers la loi stationnaire). — On considère la chaîne de Markov homogène à deux états étudiée dans l'exemple 1.5.4. On note $\mu_n = (u_n, v_n)$ la distribution que suit la variable X_n. Si la distribution μ_0 est stationnaire, alors la suite (μ_n) est constante. On se place ici dans le cas général et on s'intéresse à la convergence de la suite (μ_n).

a) Exprimer μ_n en fonction de la matrice P de probabilités de transitions et de la distribution initiale μ_0.

b) La suite $(\mu_n)_{n\in\mathbf{N}}$ admet-elle une limite lorsque $(p,q) = (1,1)$ ou $(0,0)$? Justifier, et calculer cette limite le cas échéant.

On suppose à partir de maintenant que $p+q \in]0,2[$.

c) Calculer le spectre de P.

d) Trouver une base de $\mathbf{R}^2$ composée de vecteurs propres de P, puis calculer P^n pour tout entier n.

e) En déduire la limite de μ_n lorsque $n \longrightarrow +\infty$. Que constate-t-on ?

Exercice **(1.6.14)**. — On considère une suite indépendante (X_n) de variables aléatoires soumises à une loi de Bernoulli de paramètre p. Pour $n \geqslant 1$, on pose $\mathrm{Y}_n = \mathrm{X}_n + \mathrm{X}_{n-1}$

a) Calculer la loi de Y_n et son entropie.

b) Calculer l'entropie conditionnelle $\mathrm{H}(\mathrm{Y}_n \mid \mathrm{Y}_{n-1})$.

c) Le processus (Y_n) est-il markovien ?

d) Quel est le taux d'entropie du processus (Y_n) ? (*Introduire* X_0.)

Exercice **(1.6.15)**. — *a*) Soit X, X', Y, Y' des variables aléatoires à valeurs dans le même ensemble fini A. Démontrer que

$$D((X, X') \mid (Y, Y')) = D(X, Y) + \sum_a \mathbf{P}(X = a) D((X' \mid X = a) \mid (Y' \mid Y = a)$$

b) Soit $(X_n)_{n\geqslant 0}$ et $(Y_n)_{n\geqslant 0}$ des chaînes de Markov homogènes à valeurs dans le même ensemble fini A, et possédant la même matrice de probabilités de transition P. On note p_n et q_n les lois respectives de X_n et Y_n.

c) Montrer que la suite $(D(p_n \mid q_n))_{n\geqslant 0}$ est décroissante.

d) Décrire cette suite lorsque ces chaînes de Markov sont irréductibles et apériodiques et (Y_n) est stationnaire.

e) On suppose de plus que la loi stationnaire de la chaîne (Y_n) est la loi uniforme sur A. Démontrer que la suite $(H(X_n))$ d'entropies augmente.

Exercice **(1.6.16)**. — On considère deux variables aléatoires discrètes T et X, à valeurs dans des ensembles Θ et A et l'on connaît la loi de X conditionnellement à T, c'est-à-dire les probabilités $\mathbf{P}(X = a \mid T = t)$; on voudrait estimer la valeur de T à partir de celle de X. C'est une question importante en statistique, où T correspondrait à une grandeur intéressante mais qu'on ne sait pas mesurer directement, et X à des mesures qu'on peut faire.

Soit f une fonction sur A. On dit que f est une *statistique suffisante* pour T si l'on a égalité $I(T, f(X)) = I(T, X)$.

a) Démontrer l'inégalité $I(T, f(X)) \leqslant I(T, X)$, et que f est une statistique suffisante pour T. si et seulement si X et T sont conditionnellement indépendantes relativement à $f(X)$.

b) On suppose que $X = (X_1, \ldots, X_n)$ et que, conditionnellement à $T = t$, les X_k sont indépendantes, à valeurs dans $\{0, 1\}$, et que leur loi est la loi de Bernoulli de paramètre t. On suppose que $f(a_1, \ldots, a_n) = a_1 + \cdots + a_n$. Démontrer que f est une statistique suffisante pour T.

c) Soit $\theta : A \to \Theta$ une fonction ; on considère que $\theta(X)$ est un *estimateur* de T. Si f est une statistique suffisante pour T, on note $\theta^* : A \to \Theta$ l'application $a \mapsto$

$\mathbf{E}(\theta(\mathrm{X}) \mid f(\mathrm{X}) = f(a))$. En utilisant les relations de l'exercice 0.5.7, démontrer que l'on a

$$\mathbf{E}(\theta^*(\mathrm{X})) = \mathbf{E}(\theta(\mathrm{X}))$$

et

$$\mathbf{V}(\theta^*(\mathrm{X}) - \mathrm{T}) = \mathbf{V}(\theta(\mathrm{X}) - \mathrm{T}) - \mathbf{E}(\mathbf{V}(\theta(\mathrm{X}) \mid f(\mathrm{X}))).$$

En particulier, on a l'*inégalité de Rao–Blackwell* :

$$\mathbf{E}((\theta^*(\mathrm{X}) - \mathrm{T})^2) \leqslant \mathbf{E}((\theta(\mathrm{X}) - \mathrm{T})^2)$$

Exercice **(1.6.17)**. — C'est l'histoire d'une étudiante qui travaille à la bibliothèque et qui, avec probabilité p, va prendre un café ; ceci fait, et avant de retourner travailler, elle peut, avec probabilité q, aller prendre l'air quelques minutes.

a) Décrire une chaîne de Markov à 3 états (qu'on pourra noter b, c, a) qui modélise cette histoire ; dessiner le graphe qui la représente.

b) Donner sa matrice de transitions. Vérifier qu'elle est stochastique.

c) Démontrer qu'elle possède une seule loi stationnaire et la déterminer.

d) Lorsque X_0 obéit à cette loi stationnaire, quel est le taux d'entropie du processus de Markov associé ?

e) On suppose que $0 < p < 1$ et $0 < q < 1$. Quel est le taux d'entropie du processus de Markov associé si X_0 obéit à la loi $\mathbf{P}(\mathrm{X}_0 = b) = 1$?

Exercice **(1.6.18)**. — Aux échecs, le roi peut se déplacer d'une case à une des cases voisines de l'échiquier ; il a donc huit possibilités à l'intérieur de l'échiquier, cinq sur le bord, et trois sur les coins. (On rappelle que l'échiquier est un carré de 8 cases sur 8.) On considère un roi erratique qui chaque seconde se déplacerait de façon aléatoire, suivant une loi uniforme (en respectant la règle), chaque déplacement étant indépendant des précédents. Soit (X_n) le processus stochastique tel que X_n est la position du roi à l'instant n.

a) Démontrer que (X_n) est une chaîne de Markov primitive. (*On pourra introduire le carquois dont les sommets sont les cases de l'échiquier et les arêtes orientées relient un sommet à un sommet voisin.*)

b) Calculer sa loi de probabilité stationnaire. (*On pourra chercher une telle loi de probabilité qui ne dépende que du type de case (intérieur, bord, coin).*)

c) En déduire son taux d'entropie.

1.7. Solutions des exercices

Solution de l'exercice (1.6.1). — *a*) On interprète l'hypothèse que les chevaux sont « aussi bons les uns que les autres » en considérant leur position à l'arrivée comme une variable aléatoire uniforme. Pour la variable aléatoire X qui donne le gain de Geneviève, cela donne les probabilités suivantes :

100	50	0	−10	−50	−100
1/8	2/8	1/8	1/8	2/8	1/8

Ainsi,

$$\begin{aligned}\mathbf{E}(X) &= \frac{1}{8}\cdot 100 + \frac{2}{8}\cdot 50 + \frac{1}{8}\cdot 0 + \frac{1}{8}\cdot(-10) + \frac{2}{8}\cdot(-50) + \frac{1}{8}\cdot(-100)\\ &= -\frac{10}{8} = -\frac{5}{4} = -1{,}25.\end{aligned}$$

Comme la loi de X fait apparaître 4 fois la probabilité 1/8 et 2 fois la probabilité 2/8, on a

$$\begin{aligned}\mathrm{H}_2(X) &= 4\cdot\left(-\frac{1}{8}\log_2(\frac{1}{8})\right) + 2\cdot\left(-\frac{2}{8}\log_2(\frac{2}{8})\right)\\ &= \frac{1}{2}\log_2(8) + \frac{1}{2}\log_2(4) = \frac{1}{2}\cdot 3 + \frac{1}{2}\cdot 2 = \frac{5}{2}.\end{aligned}$$

b) Pour calculer la loi de la variable aléatoire $Y = |X|$ qui donne la valeur absolue des gains de Geneviève, on additionne les probabilités que $X = x$ et que $X = -x$; cela donne les probabilités suivantes :

0	10	50	100
1/8	1/8	4/8	2/8

Ainsi,

$$\begin{aligned}\mathbf{E}(Y) &= \frac{1}{8}\cdot 0 + \frac{1}{8}\cdot 10 + \frac{4}{8}\cdot 50 + \frac{2}{8}\cdot 100\\ &= \frac{1}{8}\,(0 + 10 + 4\cdot 50 + 2\cdot 100) = \frac{1}{8}(410) = \frac{205}{4} = 51{,}25.\end{aligned}$$

Comme la loi de Y fait apparaître 2 fois la probabilité $1/8$, et une fois les probabilités $2/8$ et $4/8$, on a

$$\begin{aligned}\mathrm{H}_2(\mathrm{Y}) &= 2\cdot\left(-\frac{1}{8}\log_2(\frac{1}{8})\right)+\cdot\left(-\frac{2}{8}\log_2(\frac{2}{8})\right)+\cdot\left(-\frac{4}{8}\log_2(\frac{4}{8})\right)\\ &= \frac{1}{4}\log_2(8)+\frac{1}{4}\log_2(4)+\frac{1}{2}\log_2(2) = \frac{1}{4}\cdot 3+\frac{1}{4}\cdot 2+\frac{1}{2} = \frac{7}{4} = 1{,}75.\end{aligned}$$

On observe que l'entropie a augmenté : $\mathrm{H}_2(\mathrm{Y}) \geqslant \mathrm{H}_2(\mathrm{X})$.

Solution de l'exercice (1.6.2). — *a*) (*Avec replacement*) La probabilité de tirer une boule blanche est $b/(b+r)$, celle de tirer une boule rouge est $r/(b+r)$; puisqu'il y a replacement, cela ne change pas au cours des 5 tirages. Les variables aléatoires $\mathrm{X}_1,\dots,\mathrm{X}_5$ ont même loi (une loi de Bernoulli $\mathscr{B}(p)$, avec $p = b/(b+r)$). Elles sont également supposées indépendantes. Ainsi,

$$\mathrm{H}(\mathrm{X}) = \mathrm{H}(\mathrm{X}_1)+\mathrm{H}(\mathrm{X}_2)+\cdots+\mathrm{H}(\mathrm{X}_5) = 5h(p).$$

b) (*Sans replacement*) Dans ce cas, les variables aléatoires $\mathrm{Y}_1,\dots,\mathrm{Y}_5$ ne sont plus indépendantes. Par exemple, la probabilité que la première boule soit blanche est $b/(b+r)$; celle que les deux premières boules soient blanches est $b/(b+r)\cdot(b-1)/(b+r-1) = b(b-1)/(b+r)(b+r-1)$; en revanche, la probabilité que la seconde boule soit blanche correspond aux deux tirages (blanche, blanche) et (rouge, blanche), et a pour probabilité

$$\frac{b(b-1)}{(b+r)(b+r-1)}+\frac{rb}{(b+r)(b+r-1)} = \frac{b(r+b-1)}{(b+r)(b+r-1)} = \frac{b}{b+r-1}.$$

Puisque

$$\begin{aligned}\mathbf{P}(\mathrm{Y}_1 = \text{blanche et } \mathrm{Y}_2 = \text{blanche}) &= \frac{b(b-1)}{(b+r)(b+r-1)}\\ &\neq \frac{b^2}{(b+r)^2} = \mathbf{P}(\mathrm{Y}_1 = \text{blanche})\mathbf{P}(\mathrm{Y}_2 = \text{blanche}),\end{aligned}$$

les variables aléatoires Y_1 et Y_2 ne sont pas indépendantes.

On constate cependant sur cet exemple que Y_1 et Y_2 ont même loi ! Démontrons plus généralement que toutes les Y_m ont même loi. Le raisonnement qui suit est plus simple qu'une démonstration calculatoire. Imaginons un tirage sans remise de n boules parmi N numérotées de 1 à N : les suites $(a_1,\dots,a_n)$ de n éléments distincts ont alors toute même probabilité ; comme on peut permuter arbitrairement les numéros des n boules tirées, la symétrie de la situation montre

que la loi de chaque composante est la même, celle de la première boule. En ne retenant que la couleur des boules, on en déduit que chacune des Y_m suit une loi de Bernoulli de paramètre $b/(b+r)$.

On a donc

$$H(Y) = Y(Y_1, \dots, Y_5) = H(Y_1) + H(Y_2 \mid Y_1) + \cdots + H(Y_5 \mid Y_1, Y_2, Y_3, Y_4).$$

L'entropie décroît par conditionnement ; on a donc $H(Y_2 \mid Y_1) \leqslant H(Y_2)$, etc. Par conséquent,

$$H(Y) \leqslant H(Y_1) + \cdots + H(Y_5) = 5h(p) = H(X).$$

Solution de l'exercice (1.6.3). — *a*) Puisque la loi de X est uniforme, on a $p(x) = 1/n$ pour tout $x \in \mathcal{X}$. L'entropie de X est alors donnée par

$$H(X) = \sum_{i=1}^{n} -p(x_i)\log(p(x_i)) = n\left(-\frac{1}{n}\log(\frac{1}{n})\right) = \log(n).$$

b) La fonction $x \mapsto x\log(x)$ sur $[0;1]$ (prolongée par 0 en 0) est continue, et deux fois dérivable sur $]0;1]$. Sa dérivée est égale à $x \mapsto \log(x) + 1$, sa dérivée seconde est égale à $x \mapsto 1/x$, donc est strictement positive. Cela entraîne que la fonction considérée est strictement convexe. L'inégalité demandée est exactement l'inégalité de convexité.

c) On applique l'inégalité précédente avec $q_i = \mathbf{P}(Y = x_i)$; leur moyenne est $(\mathbf{P}(Y = x_1) + \cdots + \mathbf{P}(Y = x_n))/n = 1/n$. Ainsi

$$\frac{1}{n}\log(\frac{1}{n}) \leqslant \frac{1}{n}\sum_{i=1}^{n} \mathbf{P}(Y = x_i)\log(\mathbf{P}(Y = x_i)),$$

soit exactement $H(Y) \leqslant \log(n)$, avec égalité si seulement si les $\mathbf{P}(Y = x_i)$ sont tous égaux, c'est-à-dire si la loi de Y est uniforme.

d) Par définition,

$$\begin{aligned} D(q \mid p) &= \sum_{i=1}^{n} q(x_i)\log(q(x_i)/p(x_i)) \\ &= \sum_{i=1}^{n} q(x_i)\log(q(x_i)) - \sum_{i=1}^{n} q(x_i)\log(p(x_i)) \\ &= -H(Y) + \log(n) = H(X) - H(Y). \end{aligned}$$

Comme la divergence est toujours positive, on en déduit $\mathrm{H}(\mathrm{Y}) \leqslant \mathrm{H}(\mathrm{X})$, avec égalité si et seulement si $\mathrm{D}(q \mid p) = 0$, c'est-à-dire si $q = p$, soit encore que Y est uniforme.

Solution de l'exercice (*1.6.4*). — *a*) Si $\mathrm{X} = 0$, cela signifie qu'on a obtenu *face* au premier tirage ; la probabilité que ça se produise est égale à α ; donc $\mathbf{P}(\mathrm{X} = 0) = \alpha$.

L'égalité $\mathrm{X} = 1$ signifie qu'on a obtenu *pile* au premier tirage, et *face* au second ; par indépendance des deux tirages, la probabilité est $\mathbf{P}(\mathrm{X} = 1) = (1 - \alpha)\alpha$.

De même, l'égalité $\mathrm{X} = 2$ signifie qu'on a obtenu *pile* aux deux premiers tirages, et *face* au troisième ; sa probabilité est $\mathbf{P}(\mathrm{X} = 2) = (1 - \alpha)^2\alpha$.

Plus généralement $\mathbf{P}(\mathrm{X} = k) = (1 - \alpha)^k\alpha$.

b) On a $\mathbf{E}(\mathrm{X}) = \sum_{k=0}^{n} k\mathbf{P}(\mathrm{X} = k) = \sum_{k=0}^{n} k(1-\alpha)^k\alpha$. D'après la relation donnée, appliquée à $\beta = 1 - \alpha$, cela vaut

$$\mathbf{E}(\mathrm{X}) = \alpha\,\frac{1-\alpha}{(1-(1-\alpha))^2} = \frac{1-\alpha}{\alpha}.$$

c) Par définition, on a

$$\begin{aligned}\mathrm{H}(\mathrm{X}) &= -\sum_{k=0}^{\infty} \mathbf{P}(\mathrm{X} = k)\log(\mathbf{P}(\mathrm{X} = k)) \\ &= -\sum_{k=0}^{\infty} (1-\alpha)^k\alpha\log((1-\alpha)^k\alpha) \\ &= \sum_{k=0}^{\infty} k(1-\alpha)^k\alpha\log(1-\alpha) - \sum_{k=0}^{\infty}(1-\alpha)^k\alpha\cdot\log(\alpha).\end{aligned}$$

Le premier terme est l'espérance de X multipliée par $-\log(1-\alpha)$, le second vaut $-\log(\alpha)$; ainsi

$$\mathrm{H}(\mathrm{X}) = -\frac{1-\alpha}{\alpha}\log(1-\alpha) - \log(\alpha),$$

ce qu'il fallait démontrer.

d) Posons $h(t) = -(1-t)\log(1-t)/t - \log(t)$, de sorte que $\mathrm{H}(\mathrm{X}) = h(\alpha)$. C'est une fonction dérivable sur $]0;1[$, de dérivée

$$h'(t) = \frac{1}{t^2}\log(1-t) + \frac{1}{t} - \frac{1}{t} = \frac{1}{t^2}\log(1-t).$$

Par suite, h' est strictement négative sur $]0;1[$, donc h est strictement décroissante.

e) Quand t tend vers 0, $\log(1-t) \approx -t$, donc $\log(1-t)/t \to -1$; par ailleurs $1-t$ tend vers 1 et $-\log(t)$ vers $+\infty$; cela prouve que $\lim_{t\to 0} h(t) = +\infty$. En particulier, il y a des lois d'entropie finie, mais arbitrairement grande, sur $\mathbf{N}$, et pas de loi d'entropie maximale.

Quand t tend vers 1, $1-t$ tend vers 0, donc $(1-t)\log(1-t)$ tend vers 0 (par le résultat indiqué), puis $h(t)$ tend vers 0.

f) Par définition, on a

$$\begin{aligned} \mathrm{D}(q \mid p) &= \sum_{k=0}^{\infty} q(k)\log(q(k)/p(k)) \\ &= \sum_{k=0}^{\infty} q(k)\log(q(k)) - \sum_{k=0}^{\infty} q(k)\log(p(k)). \end{aligned}$$

Le premier terme est égal à $-\mathrm{H}(\mathrm{Y})$. Pour calculer le second, on se rappelle que $p(k) = \alpha^k(1-\alpha)$, si bien que

$$\sum_{k=0}^{\infty} q(k)\log(p(k)) = \sum_{k=0}^{\infty} kq(k)\log(\alpha) + \sum_{k=0}^{\infty} q(k)\log(1-\alpha) = \mathbf{E}(\mathrm{Y})\log(\alpha) + \log(1-\alpha).$$

On reconnaît $\mathrm{H}(\mathrm{X})$. Par conséquent, $\mathrm{D}(q \mid p) = \mathrm{H}(\mathrm{X}) - \mathrm{H}(\mathrm{Y})$.

g) Puisque d'une divergence est toujours positive ou nulle, on a ainsi $\mathrm{H}(\mathrm{Y}) \leqslant \mathrm{H}(\mathrm{X})$: l'entropie d'une variable aléatoire sur $\mathbf{N}$ est toujours inférieure ou égale à l'entropie de la variable aléatoire sur $\mathbf{N}$ de même moyenne qui a pour loi une loi géométrique. Le cas d'égalité n'est possible que si $p = q$, c'est-à-dire si la loi de Y est déjà une loi géométrique.

Puisque $\mathbf{E}(\mathrm{X}) = (1-\alpha)/\alpha$ si X a pour loi une loi géométrique de paramètre α, l'égalité $\mathbf{E}(\mathrm{X}) = m$ s'écrit $m = (1-\alpha)/\alpha = 1/\alpha - 1$, d'où $\alpha = 1/(1+m)$. Alors, $1-\alpha = m/(1+m)$, si bien que

$$\mathrm{H}(\mathrm{Y}) \leqslant -m\log(m/(1+m)) - \log(1/(1+m)) = (m+1)\log(m+1) - m\log(m),$$

avec égalité si et seulement si Y suit une loi géométrique d'espérance m.

Solution de l'exercice (1.6.5). — *a*) Par définition de l'entropie conditionnelle, on a

$$\mathrm{H}(f(\mathrm{X}) \mid \mathrm{X}) = \sum_{x\in\mathcal{X}} \mathbf{P}(\mathrm{X}=x)\mathrm{H}(f(\mathrm{X}) \mid \mathrm{X}=x),$$

où la somme est limitée aux $x \in \mathcal{X}$ tels que $\mathbf{P}(\mathrm{X}=x) > 0$. Une fois qu'on se restreint à l'évènement $\{\mathrm{X}=x\}$, la variable aléatoire discrète $f(\mathrm{X})$ devient

certaine de valeur $f(x)$; par suite, $\mathrm{H}(f(\mathrm{X}) \mid \mathrm{X} = x) = 0$. Cela entraîne $\mathrm{H}(f(\mathrm{X}) \mid \mathrm{X}) = 0$.

b) En appliquant la relation d'additivité pour l'entropie, on en déduit

$$\mathrm{H}(\mathrm{X}, f(\mathrm{X})) = \mathrm{H}(\mathrm{X}) + \mathrm{H}(f(\mathrm{X}) \mid \mathrm{X}) = \mathrm{H}(\mathrm{X}).$$

c) De même, on a

$$\mathrm{H}(\mathrm{X}, f(\mathrm{X})) = \mathrm{H}(f(\mathrm{X})) + \mathrm{H}(\mathrm{X} \mid f(\mathrm{X})) \geqslant \mathrm{H}(f(\mathrm{X})),$$

puisque $\mathrm{H}(\mathrm{X} \mid f(\mathrm{X})) \geqslant 0$. En combinant cette inégalité avec la question précédente, on en déduit l'inégalité voulue $\mathrm{H}(\mathrm{X}) \geqslant \mathrm{H}(f(\mathrm{X}))$.

d) Supposons que f est injective ; pour $y \in \mathrm{Y} y$ qui appartient à l'image de $\mathcal{X}$, notons $g(y)$ l'unique antécédent de y ; sinon, choisissons une valeur arbitraire pour $g(y)$. L'application $g : \mathcal{Y} \to \mathcal{X}$ ainsi définie vérifie $g \circ f(x) = x$ pour tout $x \in \mathcal{X}$, donc $g(f(\mathrm{X})) = \mathrm{X}$. D'après la question précédente, on a $\mathrm{H}(f(\mathrm{X})) \geqslant \mathrm{H}(g(f(\mathrm{X})) = \mathrm{H}(\mathrm{X})$. La double inégalité entraîne $\mathrm{H}(\mathrm{X}) = \mathrm{H}(f(\mathrm{X}))$.

e) Le même raisonnement qu'à la question précédente fonctionne si l'on suppose seulement que $f|_{\mathcal{X}'}$ est injective. Pour $y \in f(\mathcal{X}')$, on note en effet $g(y)$ l'unique antécédent de y dans $\mathcal{X}'$; sinon, on choisit pour $g(y)$ un élément arbitraire de $\mathcal{X}$. On a $g \circ f(x) = x$ pour tout $x \in \mathcal{X}'$; comme l'évènement $\mathrm{X} \in \mathcal{X}'$ a probabilité 1, les deux variables aléatoires discrètes $g(f(\mathrm{X}))$ et X sont presque sûrement égales. Elles ont donc même entropie et cela entraîne que $\mathrm{H}(\mathrm{X}) \geqslant \mathrm{H}(f(\mathrm{X})) \geqslant \mathrm{H}(g(f(\mathrm{X})) = \mathrm{H}(\mathrm{X})$, d'où de nouveau l'égalité $\mathrm{H}(\mathrm{X}) = \mathrm{H}(f(\mathrm{X}))$.

Inversement, supposons que $\mathrm{H}(\mathrm{X}) = \mathrm{H}(f(\mathrm{X}))$. Notons $\mathcal{X}'$ l'ensemble des $x \in \mathcal{X}$ tels que $\mathbf{P}(\mathrm{X} = x) > 0$. En reprenant la question *c*), on voit que $\mathrm{H}(\mathrm{X} \mid f(\mathrm{X})) = 0$. Par définition de l'entropie conditionnelle, on a

$$\begin{aligned} 0 &= \mathrm{H}(\mathrm{X} \mid f(\mathrm{X})) \\ &= \sum_{y \in \mathcal{Y}} \mathbf{P}(f(\mathrm{X}) = y) \mathrm{H}(\mathrm{X} \mid f(\mathrm{X}) = y) \\ &= \sum_{y \in \mathcal{Y}} \mathbf{P}(\mathrm{X} \in f^{-1}(y)) \mathrm{H}(\mathrm{X} \mid \mathrm{X} \in f^{-1}(y)), \end{aligned}$$

où la somme est restreinte à l'ensemble $\mathcal{Y}'$ des $y \in \mathcal{Y}$ tels que $\mathbf{P}(\mathrm{X} \in f^{-1}(y)) > 0$; en fait, $\mathcal{Y}' = f(\mathcal{Y})$. Cela signifie que pour tout $y \in \mathcal{Y}'$, la variable aléatoire conditionnée $\mathrm{X} \mid (\mathrm{X} \in f^{-1}(y))$ est certaine ; or elle prend avec probabilité

strictement positive toute valeur dans $\mathcal{X}' \cap f^{-1}(y)$. Par suite, $\mathcal{X}' \cap f^{-1}(y)$ n'a qu'un seul élément, ce qui signifie exactement que $f|_{\mathcal{X}'}$ est injective.

f) Reprenons la définition de l'entropie conditionnelle $\mathrm{H}(\mathrm{Y} \mid \mathrm{X})$: on a

$$\mathrm{H}(\mathrm{Y} \mid \mathrm{X}) = \sum_{x \in \mathcal{X}'} \mathbf{P}(\mathrm{X} = x)\mathrm{H}(\mathrm{Y} \mid \mathrm{X} = x).$$

Pour tout $x \in \mathcal{X}'$, la variable aléatoire discrète conditionnée $\mathrm{Y} \mid (\mathrm{X} = x)$ est donc certaine ; cela signifie qu'elle prend une unique valeur $y \in \mathcal{Y}$ avec probabilité 1 ; notons $g(x)$ cette valeur. On a donc $\mathbf{P}(\mathrm{Y} = g(x) \mid \mathrm{X} = x) = 1$, soit encore

$$\mathbf{P}(\mathrm{X} = x \text{ et } \mathrm{Y} = g(x)) = \mathbf{P}(\mathrm{X} = x),$$

et donc

$$\mathbf{P}(\mathrm{X} = x \text{ et } \mathrm{Y} \neq g(x)) = 0,$$

puisque l'évènement $(\mathrm{X} = x)$ est réunion disjointe des deux évènements $(\mathrm{X} = x \text{ et } \mathrm{Y} = g(x))$ et $(\mathrm{X} = x \text{ et } \mathrm{Y} \neq g(x))$. Pour $x \in \mathcal{X} - \mathcal{X}'$, choisissons un élément arbitraire $g(x)$. La probabilité que $\mathrm{Y} \neq g(\mathrm{X})$ est la somme des probabilités $\mathbf{P}(\mathrm{X} = x \text{ et } \mathrm{Y} \neq g(x))$, donc est nulle. Cela signifie que les variables aléatoires Y et $g(\mathrm{X})$ sont presque sûrement égales.

Inversement, si $\mathrm{Y} = g(\mathrm{X})$, la définition de l'entropie conditionnelle entraîne immédiatement que $\mathrm{H}(\mathrm{Y} \mid \mathrm{X}) = 0$.

Solution de l'exercice (1.6.6). — *a*) Pour $y \in \{1, \ldots, 52\}$, on a

$$\begin{aligned}
\mathbf{P}(\mathrm{Y} = y) &= \sum_{s \in \mathfrak{S}_{52}} \mathbf{P}(\mathrm{Y} = b \text{ et } \mathrm{S} = s) \\
&= \sum_{s \in \mathfrak{S}_{52}} \mathbf{P}(\mathrm{X} = s^{-1}(y) \text{ et } \mathbf{P}(\mathrm{S} = s)) \quad \text{puisque } \mathrm{Y} = \mathrm{S}(\mathrm{X}) \\
&= \sum_{s \in \mathfrak{S}_{52}} \mathbf{P}(\mathrm{X} = s^{-1}(y))\mathbf{P}(\mathrm{S} = s) \qquad \text{par indépendance de X et S} \\
&= \frac{1}{\mathrm{Card}(\mathfrak{S}_{52})} \sum_{s \in \mathfrak{S}_{52}} \mathbf{P}(\mathrm{X} = s^{-1}(y)),
\end{aligned}$$

puisque S est supposée uniforme. Lorsque s parcourt $\mathfrak{S}_{52}$, l'élément $x = s^{-1}(y)$ parcourt $\mathcal{X}$, et chaque élément apparaît le même nombre de fois, à savoir $\mathrm{Card}(\mathfrak{S}_{52})/\mathrm{Card}(\mathcal{X})$. Ainsi,

$$\mathbf{P}(\mathrm{Y} = y) = \frac{1}{\mathrm{Card}(\mathcal{X})} \sum_{x \in \mathcal{X}} \mathbf{P}(\mathrm{X} = x) = \frac{1}{\mathrm{Card}(\mathcal{X})}.$$

Cela prouve que la variable aléatoire discrète Y est uniforme dans $\mathfrak{X}$. Comme on l'a vu dans l'exercice 1.6.3, son entropie est en particulier plus grande que celle de X.

b) Considérons la variable aléatoire (S, X) ; par indépendance de X et S, on a $H(X, S) = H(X) + H(S)$. D'autre part, comme l'application $(x, s) \mapsto (s(x), s)$ est une bijection de $\mathfrak{X} \times \mathfrak{S}_{52}$, on a $H(X, S) = H(S(X), S) = H(Y, S)$. Par conditionnement, on a $H(Y, S) = H(S) + H(Y \mid S) \leqslant H(S) + H(Y)$. Finalement, on a bien $H(X) \leqslant H(Y)$.

Solution de l'exercice (*1.6.7*). — *a*) Par la formule des probabilités totales, on a

$$\begin{aligned}\mathbf{P}(X_1 = \text{face}) &= \mathbf{P}(X_1 = \text{face} \mid Y = a)\mathbf{P}(Y = a) + \mathbf{P}(X_1 = \text{face} \mid Y = b)\mathbf{P}(Y = b)\\ &= p \cdot \frac{1}{2} + q \cdot \frac{1}{2} = \frac{p+q}{2}.\end{aligned}$$

Le même calcul vaut pour X_2, en fait, si bien que X_1 et X_2 ont même loi.

b) Calculons par la même méthode la probabilité que la pièce soit tombée deux fois sur face :

$$\begin{aligned}\mathbf{P}(X_1 = \text{face et } X_2 = \text{face}) &= \mathbf{P}(X_1 = \text{face et } X_2 = \text{face} \mid Y = a)\mathbf{P}(Y = a)\\ &\quad + \mathbf{P}(X_1 = \text{face et } X_2 = \text{face} \mid Y = b)\mathbf{P}(Y = b)\\ &= p^2\frac{1}{2} + q^2\frac{1}{2}.\end{aligned}$$

En revanche,

$$\mathbf{P}(X_1 = \text{face})\mathbf{P}(X_2 = \text{face}) = (p+q)^2/4,$$

et

$$\frac{(p+q)^2}{4} - \frac{p^2+q^2}{2} = \frac{2pq - p^2 - q^2}{4} = -\frac{(p-q)^2}{4}.$$

Autrement dit, lorsque $p \neq q$, les deux variables aléatoires ne sont pas indépendantes.

Lorsque $p = q$, le calcul précédent prouve que

$$\mathbf{P}(X_1 = \text{face et } X_2 = \text{face}) = p^2 = \mathbf{P}(X_1 = \text{face})\mathbf{P}(X_2 = \text{face}).$$

Et de même pour les autres égalités, si bien que X_1 et X_2 sont indépendantes dans ce cas.

c) Par définition,

$$I(X_1, X_2 \mid Y) = \mathbf{P}(Y = a)I(X_1, X_2 \mid Y = a) + \mathbf{P}(Y = b)I(X_1, X_2 \mid Y = b).$$

Une fois choisie la pièce (choix dont témoigne la variable aléatoire Y), les tirages successifs sont indépendants. Autrement dit, conditionnées aux évènements $Y = a$ ou $Y = b$, les variables aléatoires X_1 et X_2 sont indépendantes et les informations mutuelles $I(X_1, X_2 \mid Y = a)$ et $I(X_1, X_2 \mid Y = b)$ sont nulles. On a donc $I(X_1, X_2 \mid Y) = 0$ et $X_1 \perp_Y X_2$.

Pour calculer $I(X_1, X_2)$, on donne le tableau des probabilités :

$X_1 \backslash X_2$	face	pile
face	$(p^2+q^2)/2$	$(p(1-p)+q(1-q))/2$
pile	$(p(1-p)+q(1-q))/2$	$((1-p)^2+(1-q)^2)/2$

qui découle du calcul de la question précédente et des calculs :

$$\begin{aligned}\mathbf{P}(X_1 = \text{face et } X_2 = \text{pile}) &= \mathbf{P}(X_1 = \text{face}) - \mathbf{P}(X_1 = \text{face et } X_2 = \text{face}) \\ &= \frac{p+q}{2} - \frac{p^2+q^2}{2} \\ &= \frac{p(1-p)+q(1-q)}{2},\end{aligned}$$

de même pour $\mathbf{P}(X_1 = \text{pile et } X_2 = \text{face})$, tandis que

$$\mathbf{P}(X_1 = \text{pile et } X_2 = \text{pile}) = \frac{(1-p)^2+(1-q)^2}{2},$$

puisqu'échanger les rôles de *pile* et *face* revient à changer p en $1-p$ et q en $1-q$. Alors, la définition de l'information mutuelle donne :

$$\begin{aligned}I(X_1, X_2) = {} & \frac{p^2+q^2}{2} \log\left(\frac{(p^2+q^2)/2}{(p+q)^2/4}\right) \\ & + 2\frac{p(1-p)+q(1-q)}{2} \log\left(\frac{(p(1-p)+q(1-q))/2}{(p+q)(2-p-q)/4}\right) \\ & + \frac{(1-p)^2+(1-q)^2}{2} \log\left(\frac{((1-p)^2+(1-q)^2)/2}{(2-p+q)^2/4}\right).\end{aligned}$$

Il n'est pas clair qu'on puisse simplifier cette formule.

Solution de l'exercice (1.6.8). — *a*) La variable aléatoire Z est de la forme $\sigma(X, Y)$, où σ est l'application somme de $\mathbf{R}^2$ dans $\mathbf{R}$. Par le résultat de l'exercice 1.6.5, on a donc $H(Z) \leqslant H(X, Y)$. D'autre part, $H(X, Y) \leqslant H(X) + H(Y)$. Cela démontre que $H(Z) \leqslant H(X) + H(Y)$.

b) Soit $x \in \mathbf{R}$ tel que $\mathbf{P}(X = x) > 0$; on a

$$\begin{aligned} H(Z \mid X = x) &= \sum_{z \in \mathbf{R}} -\mathbf{P}(Z = z \mid X = x) \log(\mathbf{P}(Z = z \mid X = x)) \\ &= \sum_{z \in \mathbf{R}} -\mathbf{P}(Y = z - x \mid X = x) \log(\mathbf{P}(Y = z - x \mid X = x)), \end{aligned}$$

puisque, par définition de la variable aléatoire $Z = X + Y$, les évènements $(Z = z \text{ et } X = x)$ et $(Y = z - x \text{ et } X = x)$ sont égaux. En faisant le changement d'indice $y = z - x$, on trouve alors

$$H(Z \mid X = x) = \sum_{y \in \mathbf{R}} -\mathbf{P}(Y = y \mid X = x) \log(\mathbf{P}(Y = y \mid X = x)) = H(Y \mid X = x).$$

Par définition de l'entropie conditionnelle, on a donc

$$H(Z \mid X) = \sum_{x \in \mathbf{R}} \mathbf{P}(X = x) H(Z \mid X = x) = \sum_{x \in \mathbf{R}} \mathbf{P}(X = x) H(Y \mid X = x) = H(Y \mid X).$$

c) Supposons X et Y indépendantes.Comme l'entropie décroît par conditionnement, on a $H(Z) \geqslant H(Z \mid X)$. D'après la question précédente, on a donc $H(Z) \geqslant H(Y \mid X)$. Comme X et Y sont indépendantes, on a aussi $H(Y \mid X) = H(Y)$. Par suite, $H(Z) \geqslant H(Y)$. L'autre inégalité $H(Z) \geqslant H(X)$ se démontre de même, par symétrie. Cela prouve l'inégalité

$$\sup(H(X), H(Y)) \leqslant H(Z).$$

d) Si X et Y sont indépendantes, on déduit de la question précédente que $\inf(H(X), H(Y)) \leqslant \sup(H(X), H(Y)) \leqslant H(Z)$. Il faut donc chercher un exemple où X et Y soient dépendantes. De fait, prenons $Y = -X$, de sorte que $Z = 0$ et donc $H(Z) = 0$. Si X n'est pas certaine, on a $H(X) = H(Y) > 0$, d'où l'inégalité $\inf(H(X), H(Y)) > H(Z)$.

Solution de l'exercice (*1.6.9*). — *a*) Puisque X et Y ont même loi, on a $H(X) = H(X)$. Alors,

$$\rho(X; Y) = \frac{H(X) - H(Y \mid X)}{H(X)} = \frac{H(Y) - H(Y \mid X)}{H(X)} = \frac{I(X, Y)}{H(X)}$$

compte tenu de l'égalité $H(Y) = H(Y \mid X) + I(X, Y)$. La formule $I(X, Y) + H(X, Y) = H(X) + H(Y)$ entraîne que l'information mutuelle $I(X, Y)$ est symétrique en X et Y. En utilisant de nouveau que $H(X) = H(Y)$, il vient $\rho(Y; X) = I(Y, X)/H(Y) = I(X, Y)/H(X) = \rho(X; Y)$.

b) Comme l'entropie est positive, on a $\rho(X;Y) \leqslant 1$. Comme l'entropie décroît par conditionnement, on a aussi $H(Y \mid X) \leqslant H(Y) = H(X)$, d'où $\rho(X;Y) \geqslant 0$.

Le cas $\rho(X;Y) = 0$ signifie que $I(X,Y) = 0$, c'est-à-dire que X et Y sont indépendantes.

Le cas $\rho(X;Y) = 1$ signifie que $H(Y \mid X) = 0$. D'après l'exercice 1.6.5, il existe une fonction f telle que $Y = f(X)$ (presque sûrement). Puisqu'on a supposé que X et Y ont même loi, la fonction f ne peut pas être arbitraire mais doit vérifier $\mathbf{P}(X = x) = \mathbf{P}(X = f(x))$ pour tout x. Inversement, pour toute fonction f vérifiant cette relation, les variables aléatoires X et $f(X)$ ont même loi et l'on a $\rho(X;Y) = 1$.

Solution de l'exercice (*1.6.10*). — *a*) On a $H(X \mid Y) = H(X,Y) - H(Y)$ et $H(Y \mid X) = H(X,Y) - H(X)$, donc $\rho(X,Y) = 2H(X,Y) - H(X) - H(Y)$. Puisque $H(X) + H(Y) = H(X,Y) + I(X,Y)$, on a aussi $\rho(X,Y) = H(X,Y) - I(X,Y)$.

b) Les entropies conditionnelles sont positives ou nulles, donc $\rho(X,Y) = H(X \mid Y) + H(Y \mid X) \geqslant 0$. L'expression qui définit $\rho(X,Y)$ est évidemment symétrique en X et Y, donc $\rho(X,Y) = \rho(Y,X)$.

Compte tenu de la formule $H(X \mid Y) = H(X,Y) - H(Y)$, on a

$$\begin{aligned}\rho(X,Y) + \rho(Y,Z) - \rho(X,Z) &= (2H(X,Y) - H(X) - H(Y)) + (2H(Y,Z) - H(Y) - H(Z)) \\ &\quad - (2H(X,Z) - H(X) - H(Z)) \\ &= 2(H(X,Y) + H(Y,Z) - H(X,Z) - H(Y)).\end{aligned}$$

D'autre part, en conditionnant par rapport à Y, on obtient

$$\begin{aligned}H(X,Y) + H(Y,Z) &= 2H(Y) + H(X \mid Y) + H(Z \mid Y) \\ &= 2H(Y) + H(X,Z \mid Y) + I(X,Z \mid Y) \\ &\geqslant 2H(Y) + H(X,Z \mid Y) \\ &= H(Y) + H(X,Z),\end{aligned}$$

ce qui prouve la relation (iii).

La démonstration montre aussi que l'égalité $\rho(X,Y) + \rho(Y,Z) = \rho(X,Z)$ équivaut à ce que $I(X,Z \mid Y) = 0$: les variables aléatoires X et Z sont conditionnellement indépendantes relativement à Y.

c) Puisque l'entropie conditionnelle est positive, l'égalité $\rho(X,Y) = 0$ équivaut à la conjonction des annulations de $H(X \mid Y)$ et $H(Y \mid X)$. D'après l'exercice 1.6.3, l'égalité $H(X \mid Y) = 0$ signifie qu'il existe une fonction g telle que $X = g(Y)$

(presque sûrement), tandis que l'égalité $\mathrm{H}(\mathrm{Y} \mid \mathrm{X}) = 0$ signifie qu'il existe une fonction f telle que $\mathrm{Y} = f(\mathrm{X})$ (presque sûrement). Autrement dit, f est injective sur l'ensemble des valeurs effectivement prises par X.

Solution de l'exercice (1.6.11). — *a*) Le taux d'entropie supérieur est la limite supérieure des expressions $\mathrm{H}(\mathrm{X}_0, \dots, \mathrm{X}_{n-1})/n$ quand n tend vers l'infini. Pour tout n, on a

$$\mathrm{H}(\mathrm{X}_0, \dots, \mathrm{X}_{n-1}) \leqslant \mathrm{H}(\mathrm{X}_0) + \cdots + \mathrm{H}(\mathrm{X}_{n-1}) \leqslant n \log(d),$$

puisque chaque X_j est à valeurs dans A et que $\mathrm{Card}(\mathrm{A}) = a$. Par conséquent, $\mathrm{H}(\mathrm{X}_0, \dots, \mathrm{X}_{n-1})/n \leqslant \log(a)$, et le taux d'entropie supérieur est majoré par $\log(a)$.

b) Cette borne est une égalité si les X_m sont indépendantes et de même loi, uniforme dans A. Mais cela fournit deux directions la rendant non optimale :

– Si les X_m sont indépendantes de même loi, on trouve $\overline{\mathrm{H}}(\boldsymbol{X}) = \mathrm{H}(\mathrm{X}_0)$, qui n'est égal à $\log(a)$ que si la loi de X_0 est uniforme ;

– Si les X_m ne sont pas indépendantes, et même si elles sont toutes uniformes dans A, l'égalité n'est pas non plus optimale. Prenons-les par exemple toutes égales à X_0 ; alors, $\mathrm{H}(\mathrm{X}_0, \dots, \mathrm{X}_{n-1}) = \mathrm{H}(\mathrm{X}_0)$, donc $\mathrm{H}(\mathrm{X}_0, \dots, \mathrm{X}_{n-1})/n = \mathrm{H}(\mathrm{X}_0)/n$, qui tend vers 0, de sorte que $\overline{\mathrm{H}}(\boldsymbol{X}) = 0$.

Solution de l'exercice (1.6.12). — *a*) Conditionnées à l'évènement $\mathrm{Y} = a$, les X_k forment une suite de variables aléatoires indépendantes, de même loi, la loi de Bernoulli de paramètre p. On a donc

$$\mathrm{H}(\mathrm{X}_1, \dots, \mathrm{X}_n \mid \mathrm{Y} = a) = n\mathrm{H}(\mathrm{X}_1 \mid \mathrm{Y} = a) = nh(p).$$

Conditionnées à l'évènement $\mathrm{Y} = b$, on trouve de même

$$\mathrm{H}(\mathrm{X}_1, \dots, \mathrm{X}_n \mid \mathrm{Y} = b) = n\mathrm{H}(\mathrm{X}_1 \mid \mathrm{Y} = b) = nh(q).$$

Par suite,

$$\begin{aligned}\mathrm{H}(\mathrm{X}_1, \dots, \mathrm{X}_n \mid \mathrm{Y}) &= \mathbf{P}(\mathrm{Y} = a)\mathrm{H}(\mathrm{X}_1, \dots, \mathrm{X}_n \mid \mathrm{Y} = a) \\ &\qquad + \mathbf{P}(\mathrm{Y} = b)\mathrm{H}(\mathrm{X}_1, \dots, \mathrm{X}_n \mid \mathrm{Y} = b) \\ &= \frac{1}{2}nh(p) + \frac{1}{2}nh(q)\end{aligned}$$

de sorte que

$$\lim_{n \to +\infty} \frac{1}{n}\mathrm{H}(\mathrm{X}_1, \dots, \mathrm{X}_n \mid \mathrm{Y}) = \frac{1}{2}\big(h(p) + h(q)\big).$$

b) Pour évaluer $\mathrm{H}(\mathrm{X}_1, \dots, \mathrm{X}_n)$, on introduit Y et on écrit

$$\begin{aligned}\mathrm{H}(\mathrm{X}_1, \dots, \mathrm{X}_n) &\leqslant \mathrm{H}(\mathrm{X}_1, \dots \mathrm{X}_n, \mathrm{Y}) \\ &= \mathrm{H}(\mathrm{Y}) + \mathrm{H}(\mathrm{X}_1, \dots, \mathrm{X}_n \mid \mathrm{Y}) \\ &= \log(2) + n\frac{1}{2}\big(h(p) + h(q)\big).\end{aligned}$$

Lorsqu'on divise par n et qu'on fait tendre n vers l'infini, on obtient la majoration

$$\overline{\mathrm{H}}(\boldsymbol{X}) \leqslant \frac{1}{2}\big(h(p) + h(q)\big).$$

D'autre part, on a aussi

$$\mathrm{H}(\mathrm{X}_1, \dots, \mathrm{X}_n, \mathrm{Y}) = \mathrm{H}(\mathrm{X}_1, \dots, \mathrm{X}_n) + \mathrm{H}(\mathrm{Y} \mid \mathrm{X}_1, \dots, \mathrm{X}_n) \leqslant \mathrm{H}(\mathrm{X}_1, \dots, \mathrm{X}_n) + \log(2)$$

puisque Y est à valeurs dans $\{a, b\}$. Cela entraîne l'inégalité

$$\begin{aligned}\mathrm{H}(\mathrm{X}_1, \dots, \mathrm{X}_n) &\geqslant \mathrm{H}(\mathrm{X}_1, \dots \mathrm{X}_n, \mathrm{Y}) - \log(2) \\ &= \mathrm{H}(\mathrm{Y}) - \log(2) + \mathrm{H}(\mathrm{X}_1, \dots, \mathrm{X}_n \mid \mathrm{Y}) \\ &= \mathrm{H}(\mathrm{Y}) - \log(2) + n\frac{1}{2}\big(h(p) + h(q)\big).\end{aligned}$$

Lorsqu'on divise par n et qu'on fait tendre n vers l'infini, on obtient la minoration

$$\underline{\mathrm{H}}(\boldsymbol{X}) \geqslant \frac{1}{2}\big(h(p) + h(q)\big).$$

Finalement, le taux d'entropie du processus $\boldsymbol{X}$ est égal à

$$\mathrm{H}(\boldsymbol{X}) = \frac{1}{2}\big(h(p) + h(q)\big).$$

c) Lorsque p et q sont très différents, par exemple lorsque p est proche de 0 et q est proche de 1, l'intuition suggère que le processus $\boldsymbol{X}$ n'est *pas* une chaîne de Markov. Si l'on a choisi initialement la pièce *a*, les tirages X_n vont majoritairement indiquer *pile*, tandis que si l'on a choisi la pièce *b*, les tirages vont majoritairement indiquer *face*. Par suite, en plus de la connaissance de X_n, celle de $(\mathrm{X}_1, \dots, \mathrm{X}_{n-1})$ apporte une information importante concernant le choix de la pièce et donc la loi de X_{n+1}.

Précisément, en écrivant 0/1 pour pile/face, on va calculer

$$\mathbf{P}(\mathrm{X}_{n+1} = 1 \mid \mathrm{X}_m = \cdots = \mathrm{X}_n = 1)$$

pour $m = 1$ et $m = n$. Par définition,

$$\mathbf{P}(\mathrm{X}_{n+1} = 1 \mid \mathrm{X}_m = \cdots = \mathrm{X}_n = 1) = \frac{\mathbf{P}(\mathrm{X}_m = \cdots = \mathrm{X}_{n+1} = 1)}{\mathbf{P}(\mathrm{X}_m = \cdots = \mathrm{X}_n = 1)}.$$

On calcule numérateur et dénominateur de façon analogue, via la formule des probabilités totales :

$$\begin{aligned}\mathbf{P}(\mathrm{X}_m = \cdots = \mathrm{X}_n = 1) &= \mathbf{P}(\mathrm{Y} = a)\mathbf{P}(\mathrm{X}_m = \cdots = \mathrm{X}_n = 1 \mid \mathrm{Y} = a) \\ &\quad + \mathbf{P}(\mathrm{Y} = b)\mathbf{P}(\mathrm{X}_m = \cdots = \mathrm{X}_n = 1 \mid \mathrm{Y} = b) \\ &= \frac{1}{2}p^{n+1-m} + \frac{1}{2}q^{n+1-m}.\end{aligned}$$

De même,

$$\mathbf{P}(\mathrm{X}_m = \cdots = \mathrm{X}_{n+1} = 1) = \frac{1}{2}p^{n+2-m} + \frac{1}{2}q^{n+2-m}.$$

Ainsi,

$$\mathbf{P}(\mathrm{X}_{n+1} = 1 \mid \mathrm{X}_m = \cdots = \mathrm{X}_n = 1) = \frac{p^{n+2-m} + q^{n+2-m}}{p^{n+1-m} + q^{n+1-m}}.$$

Si $p = q$, on obtient p. Dans ce cas, le processus $\boldsymbol{X}$ est markovien, et homogène (du point de vue probabiliste, les deux pièces sont indiscernables). Supposons en revanche que $p \neq q$, par exemple $q < p$. Quand $m = 1$ et $n \longrightarrow +\infty$, on trouve

$$\mathbf{P}(\mathrm{X}_{n+1} = 1 \mid \mathrm{X}_1 = \cdots = \mathrm{X}_n = 1) \longrightarrow p,$$

tandis que pour $m = n$, on a

$$\mathbf{P}(\mathrm{X}_{n+1} = 1 \mid \mathrm{X}_n = 1) = \frac{p^2 + q^2}{p + q} = p - \frac{(p-q)q}{p+q} < p,$$

et cela prouve que le processus $\boldsymbol{X}$ n'est pas markovien.

Solution de l'exercice (*1.6.13*). — *a*) On a $\mu_n = \mu_0 P^n$.

b) Si $(p, q) = (1, 1)$, alors $P = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, de sorte que $P^n = I_2$ si n est pair, et $P^n = P$ si n est impair. Autrement dit, $(u_n, v_n) = (u_0, v_0)$ pour n pair et $(u_n, v_n) = (v_0, u_0)$ pour n impair. Sauf si $u_0 = v_0$, la suite (μ_n) n'a pas de limite.

Si $(p, q) = (0, 0)$, alors $P = I_2$, toute distribution initiale est stationnaire, et la suite (μ_n) est constante.

c) On a

$$P = \begin{pmatrix} 1-p & p \\ q & 1-q \end{pmatrix}.$$

Sa trace est $2-p-q$, son déterminant est $(1-p)(1-q)-pq = 1-p-q$, de sorte que son polynôme caractéristique est égal à

$$\mathrm{T}^2-(2-p-q)\mathrm{T}+(1-p-q) = (\mathrm{T}-1)(\mathrm{T}-1+p+q).$$

Les deux valeurs propres de P sont 1 et $1-p-q \in]-1;1[$; elles sont simples.

d) Le vecteur colonne $U = \left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$ est vecteur propre (« à droite ») pour la valeur propre 1. Cherchons un vecteur propre pour la valeur propre $\lambda = 1-p-q$. Si ses coordonnées sont (x,y), cela correspond au système

$$(1-p)x+py = (1-p-q)x, \quad qx+(1-q)y = (1-p-q)y,$$

d'où $qx+py=0$. Ainsi $V = \left(\begin{smallmatrix}-p\\q\end{smallmatrix}\right)$ convient. Soit Q la matrice $(UV) = \left(\begin{smallmatrix}1&-p\\1&q\end{smallmatrix}\right)$. Son inverse est la matrice

$$Q^{-1} = \frac{1}{p+q}\begin{pmatrix} q & p \\ -1 & 1\end{pmatrix}.$$

On a $PQ = DQ$, où $D = \left(\begin{smallmatrix}1&0\\0&1-p-q\end{smallmatrix}\right)$. On a donc

$$\begin{aligned} P^n = QD^nQ^{-1} &= \frac{1}{p+q}\begin{pmatrix}1&-p\\1&q\end{pmatrix}\begin{pmatrix}1&0\\0&(1-p-q)^n\end{pmatrix}\begin{pmatrix}q&p\\-1&1\end{pmatrix} \\ &= \frac{1}{p+q}\begin{pmatrix}1&-(1-p-q)^np\\1&(1-p-q)^nq\end{pmatrix}\begin{pmatrix}q&p\\-1&1\end{pmatrix} \\ &= \frac{1}{p+q}\begin{pmatrix}q+(1-p-q)^np & p-(1-p-q)^np\\ q-(1-p-q)^nq & p+(1-p-q)^nq\end{pmatrix}. \end{aligned}$$

e) On a $|1-p-q|<1$. On en déduit donc que P^n converge vers la matrice

$$\frac{1}{p+q}\begin{pmatrix}q&p\\q&p\end{pmatrix}$$

lorsque $n \longrightarrow +\infty$. Puisque $\mu_n = \mu_0 P^n$, il en résulte que μ_n converge vers

$$\frac{1}{p+q}\begin{pmatrix}u_0&v_0\end{pmatrix}\begin{pmatrix}q&p\\q&p\end{pmatrix} = (u_0+v_0)\begin{pmatrix}\frac{q}{p+q}&\frac{p}{p+q}\end{pmatrix} = \begin{pmatrix}\frac{q}{p+q}&\frac{p}{p+q}\end{pmatrix}$$

puisque $u_0+v_0=1$. On constate bien la convergence vers la distribution stationnaire.

Remarquons au passage que la convergence vers cette distribution stationnaire est controlée par les termes $(1-p-q)^n$: il y a convergence exponentielle, d'autant plus rapide que l'on est loin des deux cas extrêmes $(p,q)=(0,0)$ et $(p,q)=(1,1)$.

Solution de l'exercice (*1.6.14*). — *a*) Les tirages successifs étant indépendants, on a $\mathbf{P}(Y_n = 2) = p^2$, $\mathbf{P}(Y_n = 0) = (1-p)^2$ et $\mathbf{P}(Y_n = 1) = 1-p^2-(1-p)^2 = 2(1-p)p$. Par suite,

$$\begin{aligned} H(Y_n) &= -2p^2 \log(p) - 2(1-p)^2 \log(1-p) - 2p(1-p)\log((1-p)p) \\ &= -(2p^2 + 2p(1-p))\log(p) - (2(1-p)^2 + 2(1-p)p)\log(1-p) \\ &= -2p\log(p) - 2(1-p)\log(1-p) = 2h(p). \end{aligned}$$

b) Pour calculer $H(Y_n \mid Y_{n_1})$, on écrit les diverses probabilités conditionnelles.

Supposons $Y_{n-1} = 0$; cela signifie que $X_{n-1} = X_{n-2} = 0$; conditionné à cet évènement, $Y_n = X_n$ suit une loi de Bernoulli de paramètre p, de sorte que $H(Y_n \mid Y_{n-1} = 0) = h(p)$.

Supposons $Y_{n-1} = 1$; il y a deux possibilités, équiprobables conditionnellement à l'évènement $Y_{n-1} = 1$: soit $X_{n-1} = 1$, soit $X_{n-2} = 1$. Dans le premier cas, $Y_n = 1 + X_n$ prend valeur 1 avec probabilité $1-p$, et la valeur 2 avec probabilité p ; dans le second, $Y_n = X_n$ prend valeur 1 avec probabilité p et 0 avec probabilité $1-p$. Ainsi,

$$\mathbf{P}(Y_n = 0 \mid Y_{n-1} = 1) = \frac{1}{2}(1-p),$$
$$\mathbf{P}(Y_n = 1 \mid Y_{n-1} = 1) = \frac{1}{2}(p + 1 - p) = \frac{1}{2},$$
$$\mathbf{P}(Y_n = 2 \mid Y_{n-1} = 1) = \frac{1}{2}p$$

et

$$\begin{aligned} H(Y_n \mid Y_{n-1} = 1) &= -\frac{1}{2}(1-p)\log(\frac{1}{2}(1-p)) - \frac{1}{2}\log(\frac{1}{2}) - \frac{1}{2}p\log(\frac{1}{2}) \\ &= \log(2) + \frac{1}{2}h(p). \end{aligned}$$

Supposons enfin $Y_{n-1} = 2$; ainsi, $X_{n-1} = X_{n-2} = 1$; dans ce cas, $Y_n = 1 + X_n$ prend deux valeurs avec probabilités p, $1-p$, de sorte que $H(Y_n \mid Y_{n_1} = 2) = h(p)$.

Pour finir, on a

$$\begin{aligned} H(Y_n \mid Y_{n-1}) &= (1-p)^2 h(p) + 2p(1-p)\big(\log(2) + \frac{1}{2}h(p)\big) + p^2 h(p) \\ &= (1 - 2p + p^2 + p(1-p) + p^2)h(p) + 2p(1-p)\log(2) \\ &= (1 - p + p^2)h(p) + 2p(1-p)\log(2). \end{aligned}$$

c) Sauf si $p = 1/2$, le processus (Y_n) n'est pas markovien. Étudions $\mathbf{P}(Y_3 = 1 \mid Y_1 = 0, Y_2 = 1)$. L'évenement $(Y_1 = 0, Y_2 = 1)$ par lequel on conditionne équivaut à $X_0 = 0$, $X_1 = 0$ et $X_2 = 1$, puis $Y_3 = X_2 + X_3$. Ainsi,

$$\mathbf{P}(Y_3 = 1 \mid Y_1 = 0, Y_2 = 1) = \mathbf{P}(X_3 = 0 \mid X_0 = 0, X_1 = 0, X_2 = 1) = 1 - p.$$

D'autre part, l'évènement $Y_2 = 1$ est la réunion de des évènements disjoints $((X_1, X_2) = (0, 1))$, et $((X_1, X_2) = (1, 0))$, chacun de probabilité $(1_p)p$, donc $\mathbf{P}(Y_2 = 1) = 2(1 - p)p$. En revanche, l'évènement $Y_2 = Y_3 = 1$ est la réunion des évènements disjoints $(X_1, X_2, X_3) = (0, 1, 0)$ et $(X_1, X_2, X_3) = (1, 0, 1)$, de probabilités $(1 - p)^2 p$ et $(1 - p)p^2$ respectivement ; ainsi,

$$\mathrm{P}(Y_2 = Y_3 = 1) = (1 - p)^2 p + (1 - p)p^2 = (1 - p)p.$$

Finalement,

$$\mathbf{P}(Y_3 = 1 \mid Y_2 = 1) = \frac{(1 - p)p}{2(1 - p)p} = \frac{1}{2} \neq 1 - p = \mathbf{P}(Y_3 = 1 \mid Y_1 = Y_2 = 1).$$

d) On a

$$\mathrm{H}(Y_1, \ldots, Y_n) \leqslant \mathrm{H}(X_0, Y_1, \ldots, Y_n) \leqslant \mathrm{H}(X_0) + \mathrm{H}(Y_1, \ldots, Y_n).$$

Or, la donnée de $(X_0, Y_1, \ldots, Y_n)$ équivaut à celle de $(X_0, \ldots, X_n)$, puisque $X_1 = Y_1 - X_0$, $X_2 = Y_2 - X_1$, etc. Ainsi,

$$\mathrm{H}(X_0, Y_1, \ldots, Y_n) = \mathrm{H}(X_0, X_1, \ldots, X_n) = (n + 1)h(p),$$

étant donné que la suite (X_k) est indépendante et que les variables aléatoires X_k ont toutes pour entropie $h(p)$. Cela démontre l'inégalité

$$nh(p) \leqslant \mathrm{H}(Y_1, \ldots, Y_n) \leqslant (n + 1)h(p),$$

d'où on déduit que le processus (Y_k) a pour taux d'entropie $h(p)$.

Solution de l'exercice (*1.6.15*). — *a*) En revenant à la définition, on a

$$\begin{aligned}
&\mathrm{D}((\mathrm{X},\mathrm{X}')\mid(\mathrm{Y},\mathrm{Y}'))-\mathrm{D}(\mathrm{X},\mathrm{Y})\\
&\quad=\sum_{a,b}\mathbf{P}(\mathrm{X}=a\ \text{ et }\ \mathrm{X}'=b)\log\frac{\mathbf{P}(\mathrm{X}=a\ \text{ et }\ \mathrm{X}'=b)}{\mathbf{P}(\mathrm{Y}=a\ \text{ et }\ \mathrm{Y}'=b)}\\
&\qquad\qquad-\sum_{a}\mathbf{P}(\mathrm{X}=a)\log\frac{\mathbf{P}(\mathrm{X}=a)}{\mathbf{P}(\mathrm{Y}=a)}\\
&\quad=\sum_{a,b}\mathbf{P}(\mathrm{X}=a\ \text{ et }\ \mathrm{X}'=b)\log\frac{\mathbf{P}(\mathrm{X}=a\ \text{ et }\ \mathrm{X}'=b)}{\mathbf{P}(\mathrm{Y}=a\ \text{ et }\ \mathrm{Y}'=b)}\\
&\qquad\qquad-\sum_{a}\mathbf{P}(\mathrm{X}=a\ \text{ et }\ \mathrm{X}'=b)\log\frac{\mathbf{P}(\mathrm{X}=a)}{\mathbf{P}(\mathrm{Y}=a)}\\
&\quad=\sum_{a,b}\mathbf{P}(\mathrm{X}=a\ \text{ et }\ \mathrm{X}'=b)\log\frac{\mathbf{P}(\mathrm{X}=a\ \text{ et }\ \mathrm{X}'=b)/\mathbf{P}(\mathrm{X}=a)}{\mathbf{P}(\mathrm{Y}=a\ \text{ et }\ \mathrm{Y}'=b)/\mathbf{P}(\mathrm{Y}=a)}\\
&\quad=\sum_{a}\mathbf{P}(\mathrm{X}=a)\sum_{b}\mathbf{P}(\mathrm{X}'=b\mid\mathrm{X}=a)\log\frac{\mathbf{P}(\mathrm{X}'=b\mid\mathrm{X}=a)}{\mathbf{P}(\mathrm{Y}'=b\mid\mathrm{Y}=a)}.
\end{aligned}$$

b) Pour simplifier les notations, on note $p=p_n$, $q=q_n$ et $p'=p_{n+1}$, $q'=q_{n+1}$, ainsi que $\mathrm{X}=\mathrm{X}_n$, $\mathrm{Y}=\mathrm{Y}_n$ et $\mathrm{X}'=\mathrm{X}_{n+1}$, $\mathrm{Y}'=\mathrm{Y}_{n+1}$. Il s'agit de démontrer que $\mathrm{D}(p'\mid q')\leqslant\mathrm{D}(p\mid q)$.

Appliquons d'abord la relation de la question précédente. Pour tout a, la loi de X' sachant $\mathrm{X}=a$ coïncide avec celle de Y' sachant $\mathrm{Y}=a$. On obtient donc $\mathrm{D}((\mathrm{X},\mathrm{X}')\mid(\mathrm{Y},\mathrm{Y}'))=\mathrm{D}(\mathrm{X},\mathrm{Y})$.

Par ailleurs, on peut l'appliquer de façon symétrique en échangeant les rôles de X,Y et X',Y' ; on obtient

$$\begin{aligned}
\mathrm{D}((\mathrm{X},\mathrm{X}')\mid(\mathrm{Y},\mathrm{Y}'))&=\mathrm{D}(\mathrm{X}',\mathrm{Y}')\\
&\quad+\sum_{a}\mathbf{P}(\mathrm{X}'=a)\sum_{b}\mathbf{P}(\mathrm{X}=b\mid\mathrm{X}'=a)\log\frac{\mathbf{P}(\mathrm{X}=b\mid\mathrm{X}'=a)}{\mathbf{P}(\mathrm{Y}=b\mid\mathrm{Y}'=a)}.
\end{aligned}$$

Pour a fixé, chacune des sommes du membre de droite s'interprète comme la divergence de loi conditionnelles de X et Y ; en particulier, elles sont positives ou nulles. Cela entraîne l'inégalité $\mathrm{D}((\mathrm{X},\mathrm{X}')\mid(\mathrm{Y},\mathrm{Y}'))\geqslant\mathrm{D}(\mathrm{X}',\mathrm{Y}')$.

Finalement, on a

$$\mathrm{D}(\mathrm{X}',\mathrm{Y}')\leqslant\mathrm{D}((\mathrm{X},\mathrm{X}')\mid(\mathrm{Y},\mathrm{Y}'))=\mathrm{D}(\mathrm{X},\mathrm{Y}),$$

comme il fallait démontrer.

c) Puisque la chaîne de Markov (Y_n) est stationnaire, la suite (q_n) est constante. Comme la chaîne de Markov est irréductible et apériodique, les lois (p_n) convergent vers l'unique loi stationnaire, qui est q_0. On a donc $D(p_n \mid q_n) = D(p_n \mid q_0) \to 0$.

d) Puisque la loi (q_0) est uniforme, on a

$$D(p_n \mid q_n) = D(p_n \mid q_0) = \sum_a p_n(a) \log \frac{p_n(a)}{1/\mathrm{Card}(A)} = \log(\mathrm{Card}(A)) - H(X_n),$$

soit encore $H(X_n) = \log(\mathrm{Card}(A)) - D(p_n \mid q_n)$. Cela prouve que la suite $(H(X_n))$ est croissante, de limite $\log(\mathrm{Card}(A))$.

Remarque : Cet énoncé est une variante du second principe de la thermodynamique : un gaz évolue vers l'équilibre et son entropie augmente.

Si X, Y sont des variables aléatoires de lois p, q, la divergence $D(p \mid q)$ est parfois appelée *entropie relative* de X et Y. Malgré cette terminologie proche, entropie et entropie relative se comportent donc différemment.

Solution de l'exercice (*1.6.16*). — *a*) C'est l'inégalité du traitement de données du corollaire 1.3.12, ainsi que la caractérisation du cas d'égalité.

b) Pour démontrer que f est une statistique suffisante pour T, on vérifie l'indépendance conditionnelle de T et X relativement à $f(X)$, c'est-à-dire les égalités

$$\mathbf{P}(T = t \mid X = a) = \mathbf{P}(T = t \mid f(X) = f(a))$$

pour tout $a \in \{0,1\}^n$ et tout $t \in \Theta$. Cette relation se récrit

$$\mathbf{P}(T = t \text{ et } X = a)\mathbf{P}(f(X) = f(a)) = \mathbf{P}(T = t \text{ et } f(X) = f(a))\mathbf{P}(X = a),$$

soit encore

$$\frac{\mathbf{P}(f(X) = f(a) \mid T = t)}{\mathbf{P}(X = a \mid T = t)} = \frac{\mathbf{P}(f(X) = f(a)}{\mathbf{P}(X = a)}.$$

Par hypothèse, on a

$$\mathbf{P}(X = a \mid T = t) = t^m(1-t)^{n-m},$$

de sorte que

$$\mathbf{P}(X = a \text{ et } T = t) = t^m(1-t)^{n-m}\mathbf{P}(T = t).$$

Comme il y a $\binom{n}{m}$ éléments $a \in \{0,1\}^n$ tels que $f(a) = m$, on a donc

$$\mathbf{P}(f(X) = f(a) \text{ et } T = t) = \binom{n}{m} t^m(1-t)^{n-m}\mathbf{P}(T = t).$$

Ainsi,

$$\frac{\mathbf{P}(f(\mathrm{X}) = f(a) \mid \mathrm{T} = t)}{\mathbf{P}(\mathrm{X} = a \mid \mathrm{T} = t)} = \frac{1}{\binom{n}{m}}.$$

Le point important est précisément que cette expression ne dépend pas de t, puisqu'alors,

$$\begin{aligned}\mathbf{P}(f(\mathrm{X}) = a) &= \sum_t \mathbf{P}(f(\mathrm{X}) = a \mid \mathrm{T} = t)\mathbf{P}(\mathrm{T} = t) \\ &= \frac{1}{\binom{n}{m}} \sum_t \mathbf{P}(\mathrm{X} = a \mid \mathrm{T} = t)\mathbf{P}(\mathrm{T} = t) \\ &= \frac{1}{\binom{n}{m}} \mathbf{P}(\mathrm{X} = a).\end{aligned}$$

c) Par définition, on a $\theta^*(\mathrm{X}) = \mathbf{E}(\theta(\mathrm{X}) \mid f(\mathrm{X}))$. D'après la première question de l'exercice 0.5.7, on a donc

$$\mathbf{E}(\theta^*(\mathrm{X})) = \mathbf{E}(\mathbf{E}(\theta(\mathrm{X}) \mid f(\mathrm{X})) = \mathbf{E}(\theta(\mathrm{X})).$$

On peut aussi refaire l'argument : pour toute valeur k de f, l'estimateur $\theta^*(\mathrm{X})$ est constant conditionnellement à l'événement $f(\mathrm{X}) = k$, de valeur $\mathbf{E}(\theta(\mathrm{X}) \mid f(\mathrm{X}) = k)$; par suite, on a

$$\mathbf{E}(\theta^*(\mathrm{X}) \mid f(\mathrm{X}) = k) = \mathbf{E}(\theta(\mathrm{X}) \mid f(\mathrm{X}) = k).$$

L'égalité des espérances en résulte.

D'autre part, en appliquant la seconde question de l'exercice 0.5.7 aux couples $(\theta(\mathrm{X}) - \mathrm{T}, f(\mathrm{X}))$ et $(\theta^*(\mathrm{X}) - \mathrm{T}, f(\mathrm{X}))$, on obtient

$$\begin{aligned}\mathbf{V}(\theta(\mathrm{X}) - \mathrm{T}) - \mathbf{V}(\theta^*(\mathrm{X})) = \mathbf{V}(\mathbf{E}(\theta(\mathrm{X}) - \mathrm{T} \mid f(\mathrm{X})) - \mathbf{V}(\mathbf{E}(\theta^*(\mathrm{X}) - \mathrm{T} \mid f(\mathrm{X}))) \\ + \mathbf{E}(\mathbf{V}(\theta(\mathrm{X}) - \mathrm{T} \mid f(\mathrm{X})) - \mathbf{E}(\mathbf{V}(\theta^*(\mathrm{X}) - \mathrm{T} \mid f(\mathrm{X}))).\end{aligned}$$

Les deux variables aléatoires $\mathbf{E}(\theta(\mathrm{X}) - \mathrm{T} \mid f(\mathrm{X}))$ et $\mathbf{E}(\theta^*(\mathrm{X}) - \mathrm{T} \mid f(\mathrm{X}))$ sont égales à $\theta^*(\mathrm{X}) - \mathbf{E}(\mathrm{T} \mid f(\mathrm{X}))$, par définition de $\theta^*(\mathrm{X})$, donc les deux premiers termes s'annulent. Les deux suivants sont des espérances, on considère d'abord une valeur donnée, k, de $f(\mathrm{X})$ et on étudie

$$\begin{aligned}\mathbf{V}(\theta(\mathrm{X}) - \mathrm{T} \mid f(\mathrm{X}) = k) - \mathbf{V}(\theta^*(\mathrm{X}) - \mathrm{T} \mid f(\mathrm{X}) = k) \\ = \mathbf{E}((\theta(\mathrm{X}) - \mathrm{T})^2 \mid f(\mathrm{X}) = k) - \mathbf{E}((\theta^*(\mathrm{X}) - \mathrm{T})^2 \mid f(\mathrm{X}) = k)\end{aligned}$$

car, en restriction à l'évènement $f(\mathrm{X}) = k$, on a

$$\begin{aligned}\mathbf{E}(\theta(\mathrm{X}) - \mathrm{T} \mid f(\mathrm{X}) = k) &= \theta^*(\mathrm{X}) - \mathbf{E}(\mathrm{T} \mid f(\mathrm{X}) = k) \\ &= \mathbf{E}(\theta^*(\mathrm{X}) - \mathrm{T} \mid f(\mathrm{X}) = k).\end{aligned}$$

En développant, on obtient

$$\mathbf{E}(\theta(\mathrm{X})^2 - \theta^*(\mathrm{X})^2 \mid f(\mathrm{X}) = k) + 2\mathbf{E}(\mathrm{T} \cdot (\theta^*(\mathrm{X}) - \theta(\mathrm{X})) \mid f(\mathrm{X}) = k).$$

L'hypothèse que f est une statistique suffisante pour T entraîne que le dernier terme est nul : conditionnées à l'évèneùent $f(\mathrm{X}) = k$, les variables aléatoires X et T sont indépendantes, de sorte que

$$\begin{aligned}&\mathbf{E}(\mathrm{T} \cdot (\theta^*(\mathrm{X}) - \theta(\mathrm{X})) \mid f(\mathrm{X}) = k) \\ &\qquad = \mathbf{E}(\mathrm{T} \mid f(\mathrm{X}) = k)\mathbf{E}(\theta^*(\mathrm{X}) - \theta(\mathrm{X}) \mid f(\mathrm{X}) = k) = 0,\end{aligned}$$

par définition de $\theta^*(\mathrm{X})$. De plus,

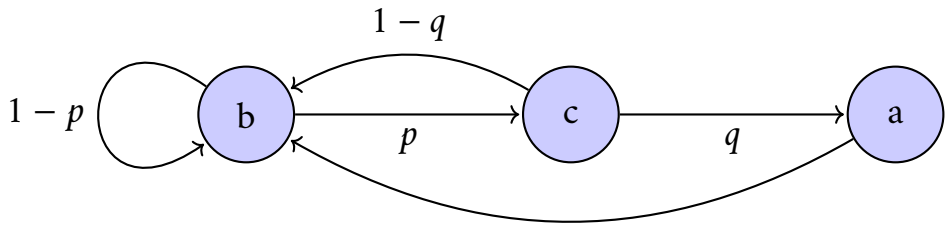
$$\mathbf{E}(\theta(\mathrm{X})^2 - \theta^*(\mathrm{X})^2 \mid f(\mathrm{X}) = k) = \mathbf{V}(\theta(\mathrm{X}) \mid f(\mathrm{X}) = k),$$

si bien que

$$\mathbf{E}(\mathbf{V}(\theta(\mathrm{X}) - \mathrm{T} \mid f(\mathrm{X})) - \mathbf{E}(\mathbf{V}(\theta^*(\mathrm{X}) - \mathrm{T} \mid f(\mathrm{X}))) = \mathbf{V}(\theta(\mathrm{X}) \mid f(\mathrm{X})).$$

Cela démontre la relation demandée.

Solution de l'exercice (*1.6.17*). — *a*) Les trois états représentent la position de l'étudiante, *b* pour bibliothèque, *c* pour café, et *a* lorsqu'elle prend l'air. Soit X_n son état au « temps » n. Selon l'histoire en tête de l'exercice, lorsque l'étudiante est à la bibliothèque, elle part prend un café avec probabilité p, on a ainsi $\mathbf{P}(\mathrm{X}_{n+1} = \mathrm{c} \mid \mathrm{X}_n = \mathrm{b}) = p$, et $\mathbf{P}(\mathrm{X}_{n+1} = \mathrm{b} \mid \mathrm{X}_n = \mathrm{b}) = 1 - p$. Lorsqu'elle prend un café, elle retourne à la bibliothèque avec probabilité $1 - q$: $\mathbf{P}(\mathrm{X}_{n+1} = \mathrm{b} \mid \mathrm{X}_n = \mathrm{c}) = 1 - q$, et part prendre l'air avec probabilité q : $\mathbf{P}(\mathrm{X}_{n+1} = \mathrm{a} \mid \mathrm{X}_n = \mathrm{c}) = q$. Lorsqu'elle a pris l'air, elle retourne travailler à la bibliothèque : $\mathbf{P}(\mathrm{X}_{n+1} = \mathrm{b} \mid \mathrm{X}_n = \mathrm{a}) = 1$.



b) La matrice de transitions de cette chaîne de Markov est donnée par

$$\mathrm{P} = \begin{array}{c} \\ \mathrm{a} \\ \mathrm{b} \\ \mathrm{c} \end{array} \begin{array}{c} \begin{array}{ccc} \mathrm{a} & \mathrm{b} & \mathrm{c} \end{array} \\ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1-p & p \\ q & 1-q & 0 \end{pmatrix} \end{array}$$

On constate que la somme des coefficients de chaque ligne est égale à 1 ; cette matrice est donc stochastique.

c) Une loi stationnaire pour cette chaîne de Markov est donnée par un vecteur-ligne $\mathrm{M} = (a\, b\, c)$ à coefficients positifs, de somme 1, tel que $\mathrm{M}\cdot\mathrm{P} = \mathrm{M}$. Explicitons d'abord ce système linéaire ; on obtient :

$$qc = a, \quad a + (1-p)b + (1-q)c = b, \quad pb = c.$$

On a alors $a = qc = pqb$ et $c = pb$, et la dernière relation

$$pqb + (1-p)b + p(1-q)b = b$$

est automatiquement vérifiée. La relation $a+b+c = 1$ s'écrit alors $(pq+1+p)b = 1$, d'où $b = 1/(1+p+pq)$. Il y a donc une unique loi stationnaire, donnée par le vecteur-ligne

$$\left(\frac{pq}{1+p+pq} \; \frac{1}{1+p+pq} \; \frac{p}{1+p+pq} \right).$$

d) Un théorème du cours donne l'entropie d'une chaîne de Markov homogène stationnaire : c'est la moyenne, pour la loi stationnaire, des entropies des lignes de sa matrice de transitions. Les entropies des lignes valent :

$$\begin{aligned} \mathrm{H_a} &= 0 \\ \mathrm{H_b} &= -(1-p)\log(1-p) - p\log(p) = h(p) \\ \mathrm{H_c} &= -q\log(q) - (1-q)\log(1-q) = h(q). \end{aligned}$$

(On a noté $h(p)$ l'entropie d'un processus de Bernoulli de paramètre p.) Alors,

$$\mathrm{H} = a\mathrm{H_a} + b\mathrm{H_b} + c\mathrm{H_c} = \frac{h(p) + ph(q)}{1+p+pq}.$$

e) D'après un théorème de cours, ce calcul reste valable pour toute loi initiale si cette chaîne de Markov est irréductible apériodique. Le cycle $\mathrm{b} \to \mathrm{c} \to \mathrm{a} \to \mathrm{b}$ entraîne qu'on peut atteindre tout état depuis n'importe quel autre. Cette chaîne est donc irréductible. Par ailleurs, il y a un cycle $\mathrm{b} \to \mathrm{b}$ de longueur 1, de sorte

que les pgcd des longueurs des cycles en chaque état sont égaux à 1. Ainsi, la chaîne est apériodique.

Solution de l'exercice (1.6.18). — *a*) Considérons le carquois dont les sommets sont les 64 cases de l'échiquier et dont les flèches relient une case à chacune des cases voisines, qui sont les cases accessibles au roi en un déplacement. Ce graphe est fortement connexe ; il est aussi apériodique car on peut aller d'une case à elle-même en 2 étapes (aller-retour), mais aussi en 3 étapes (droite, haut, diagonale). Ainsi, (X_n) est une chaîne de Markov primitive.

b) Comme cette chaîne de Markov est primitive, elle possède une unique loi stationnaire. A priori, il faut chercher un vecteur à 64 composantes, mais l'énoncé suggère que ce vecteur n'aura que trois composantes distinctes, qui dépendent juste de la position de la case, suivant que c'est un coin, un bord ou une case intérieur. On écrit les équations pour ces trois nombres réels c, b, i. Tout d'abord, la somme des probabilités est 1 ; comme il y a 4 coins, 24 cases de bord et 36 cases intérieures, on obtient

(1.7.18.1) $$4c + 24b + 36i = 1.$$

Une case de coin a deux cases de bord voisines qui ont elles-mêmes 5 voisins, et une case intérieure voisine qui a 8 voisins ; la relation de stationnarité en une case de coin s'écrit donc :

(1.7.18.2) $$c = 2\frac{1}{5}b + \frac{1}{8}i.$$

Pour les cases de bord, il y a deux cas : celles jouxtant un coin et les autres ; cela donne les deux relations

(1.7.18.3) $$b = \frac{1}{3}c + 2\frac{1}{5}b + 2\frac{1}{8}i \quad \text{et} \quad b = 2\frac{1}{5}b + 3\frac{1}{8}i.$$

Il y a quatre cas pour les cases intérieures : celles qui ne jouxtent pas le bord, celles qui jouxtent le bord mais pas un coin, et celles qui jouxtent un coin ; cela donne les trois relations

(1.7.18.4) $$i = 8\frac{1}{8}i, \qquad i = 3\frac{1}{5}b + 5\frac{1}{8}i, \quad \text{et} \quad i = \frac{1}{3}c + 4\frac{1}{5}b + 3\frac{1}{8}i.$$

Trois inconnues, sept équations, cela semble un peu miraculeux que ce système ait une solution. Par élimination, on obtient immédiatement

(1.7.18.5) $$\frac{1}{8}i = \frac{1}{5}b = \frac{1}{3}c$$

puis, en reportant cette valeur commune t dans l'équation (1.7.18.1),

$$4 \cdot 3t + 24 \cdot 5t + 36 \cdot 8t = 1,$$

d'où $t = 1/420$ puis

(1.7.18.6) $$c = \frac{3}{420} = \frac{1}{140}, \quad b = \frac{5}{420} = \frac{1}{84}, \quad i = \frac{8}{420} = \frac{2}{105}.$$

c) Le taux d'entropie du processus aléatoire correspondant est donné par la proposition 1.5.3 : $\mathrm{H}(\mathrm{X}) = \sum_a \mu_a \mathrm{H}(p_{a,b})$, où a parcourt l'ensemble des cases, μ_a est la probabilité que le roi sur sur la case a pour la loi stationnaire, valeur et $p_{a,b} = \mathbf{P}(\mathrm{X}_{n+1} = b \mid \mathrm{X}_n = a)$. Il y a trois cas, suivant que a est un coin, un bord ou une case intérieure :

– Si a est un coin, $\mu_a = 1/140$ et le vecteur $p_{a,b}$ vaut $(1/3, 1/3, 1/3, 0, \dots)$, de sorte que $\mathrm{H}((p_{a,b})) = \log(3)$;

– Si a est un bord, $\mu_a = 1/84$ et le vecteur $p_{a,b}$ vaut $(1/5, 1/5, 1/5, 1/5, 1/5, 0, \dots)$, de sorte que $\mathrm{H}((p_{a,b})) = \log(5)$;

– Enfin, si a est une case intérieure, $\mu_a = 2/105$ et le vecteur $p_{a,b}$ vaut $(1/8, \dots, 1/8, 0, \dots)$, de sorte que $\mathrm{H}((p_{a,b})) = \log(8)$.

On obtient

(1.7.18.7) $$\mathrm{H}(\mathrm{X}) = 4 \cdot \frac{1}{140}\log(3) + 24 \cdot \frac{1}{84}\log(5) + 36 \cdot \frac{2}{105}\log(8) \approx 1{,}917\dots$$

Remarque : Avec un logiciel tel que SageMath, on peut résoudre l'exercice de façon plus mécanique : on commence par construire la matrice `MKing` de probabilités de transitions.

```
# Trois fonctions pour gérer les coordonnées
def n2xy(n):
    return (n%8, n//8)
def xy2n(x,y):
    return x+y*8
def valid(x,y):
    return (x >= 0 and y >= 0 and x < 8 and y <8)
# Déplacements du roi
King=[]
for e in [-1,0,1]:
    for f in [-1,0,1]:
        King = King +[(e,f)]
King.remove((0,0))
# Construction de la matrice de transitions pour le roi
MKing = []
```

```
for n in range(64):
    MKing.append([0]*64)
    x,y=n2xy(n)
    Kxy = [].copy()
    for dx, dy in King:
        if valid(x+dx,y+dy):
            Kxy.append (xy2n(x+dx,y+dy))
    for d in Kxy:
        MKing[-1][d] = 1/len(Kxy)
MKing=matrix(QQ,MKing)
```

La commande

```
evKing = MKing.eigenvalues()
```

calcule les valeurs propres de la matrice `MKing` ; les quatre premières sont $\left[1, -\frac{1}{5}, -0.4910211476797844?, -0.3316809492706161?\right]$. En particulier, 1 est bien la plus grande valeur propre de cette matrice stochastique primitive ; on calcule alors le vecteur propre à gauche normalisé correspondant :

```
# Calcul du vecteur propre pour la valeur propre 1
EVKing = MKing.eigenvectors_left()[0][1][0]
EVKing = EVKing/sum(EVKing)
```

Ses premières coordonnées sont $\left(\frac{1}{140}, \frac{1}{84}, \frac{1}{84}, \frac{1}{84}, \frac{1}{84}, \frac{1}{84}, \frac{1}{84}, \frac{1}{140}, \frac{1}{84}, \frac{2}{105}\right)$. Enfin, on calcule le taux d'entropie (la fonction `H` calcule l'entropie de Shannon d'un vecteur ligne) :

```
H = lambda p : sum(map(lambda x: 0 if x <= 0 else -x*log(x),p))
HKing = RR(sum([EVKing[i]*H(MKing[i]) for i in range(len(EVKing))]))
```

et on retrouve la valeur 1.91713109752358 calculée dans l'exercice.

CHAPITRE 2

CODAGE

Nous abordons maintenant les deux contributions fondamentales de Shannon (1948) à la théorie de l'information en abordant la question du codage, c'est-à-dire, de la façon optimale de transmettre un signal, un « message ».

On cherche d'abord à minimiser le temps de diffusion, ce qui recoupe alors la question de la *compression* des fichiers : comment les coder de sorte à ce qu'ils occupent une place aussi petite que possible, et peut-on préciser jusqu'à quel point on peut les comprimer ? Apparue au début des transmissions électriques, il s'agissait alors de faire passer plusieurs signaux télégraphiques sur une même ligne, cette question est devenue fondamentale à l'ère numérique : les formats ePub (pour le texte), Flac, OggVorbis ou MP3 (pour le son), Jpeg ou DjVu (pour l'image) cherchent tous à tirer partie du type d'information enregistrée pour le faire de façon efficace. En revanche, nous n'aborderons pas la question, également importante en pratique, notamment pour les applications en temps réel, de la facilité ou de la rapidité du codage et du décodage.

Nous présentons l'*interprétation statistique* de l'entropie : dans certains processus stochastiques, tout se passe plus ou moins comme si les variables aléatoires étaient tirées uniformément parmi une partie de l'espace des valeurs a priori possibles. Cette interprétation est d'ailleurs à la base des démonstrations de Shannon dans son article, c'est cependant un point où ses arguments manquent un peu de rigueur, faute de quantifier ce « comme si ».

Un autre aspect du codage abordé par Shannon (1948) est de permettre de tenir compte de la possibilité d'interférences, et donc d'erreurs, au cours de la transmission, liées au caractère physique du canal de transmission. Nous présentons le formalisme d'un canal sans mémoire : c'est une modélisation des canaux de transmission physiques qui considère que les erreurs successives de transmission

sont indépendantes les unes des autres, et suivent une loi qui dépend uniquement des symboles transmis. Cela exclut par exemple des phénomènes de saturation.

La *capacité* de transmission d'un tel canal est définie en termes d'entropie, plus exactement de l'information mutuelle que peuvent posséder le signal émis et le signal reçu. Dans un canal sans mémoire, la probabilité d'une erreur ne peut pas être totalement annulée, et le théorème remarquable de Shannon est que l'on peut la rendre aussi petite que voulue, tant que l'on ne cherche pas à transmettre plus d'information que la capacité de transmission du canal. Pour la preuve de ce théorème, nous nous écartons des arguments de Shannon et reprenons plutôt ceux, plus précis, de Wolfowitz (1958). Un aspect commun à ces deux preuves est de ne pas chercher à construire explicitement un procédé de codage/décodage, mais à montrer qu'un procédé de codage choisi au hasard convient. C'est, en même temps que des travaux d'Erdős, l'apparition de la *méthode probabiliste* en mathématiques, méthode dont le livre de Alon & Spencer (2008) témoigne de la richesse.

2.1. Codes

2.1.1. Alphabets et mots. — Soit A un ensemble. On considère les éléments de A comme les lettres d'un *alphabet* et on considère les mots que l'on peut écrire avec ces symboles. Par définition, un *mot* est une suite finie $(a_1, \dots, a_n)$ d'éléments de A ; l'entier n est la longueur de ce mot. On notera A^* l'ensemble des mots écrits dans l'alphabet A ; c'est la réunion, lorsque l'entier n varie, des ensembles A^n des mots de longueur n.

Il y a un seul mot de longueur 0, c'est le mot vide, parfois noté ε. L'ensemble A^* est muni d'une loi interne de concaténation. Si $a = (a_1, \dots, a_n)$ et $b = (b_1, \dots, b_m)$ sont des mots, le mot ab est donné par la suite $(a_1, \dots, a_n, b_1, \dots, b_m)$. Sa longueur est la somme des longueurs des mots a et b. Cette loi interne est associative ; le mot vide est son un élément neutre.

On notera $\ell(a)$ la longueur du mot a.

2.1.2. — Un code C est la donnée d'un second alphabet B et d'une application, également notée C, de A dans B^*, telle que $\ell(C(a)) > 0$ pour tout a. Par cette application, les symboles de A sont représentés par des mots non vides dans l'alphabet B.

Un exemple représentatif consisterait à prendre pour A un ensemble de symboles assez vaste contenant, par exemple, les lettres de l'alphabet latin et les symboles de ponctuation, et pour C l'application qui à un tel symbole associe son *code* dans le système ASCII.

2.1.3. — Soit C un code sur l'alphabet A. En pratique, on ne code pas uniquement des symboles de l'alphabet A mais des mots dans cet alphabet : si $(a_1, \dots, a_n)$ est un mot, son code est le mot concaténé $\mathrm{C}(a_1) \dots \mathrm{C}(a_n)$. On notera C^*, ou parfois encore C, l'application de A^* dans B^* ainsi définie. Elle vérifie $\mathrm{C}^*(ab) = \mathrm{C}(a)\mathrm{C}(b)$ pour tous a, b dans A^*.

On dit que le code C est *uniquement décodable* si cette application C^* est injective, c'est-à-dire si deux mots distincts ont des codes distincts.

2.1.4. Codes préfixes. — On dit qu'un code C sur un alphabet A est *préfixe* si, pour tous $a, b \in \mathrm{A}$ tels que $a \neq b$, aucun des deux mots $\mathrm{C}(a)$, $\mathrm{C}(b)$ n'est le début de l'autre.

Démontrons qu'un tel code est uniquement décodable. Soit en effet $a = (a_1, \dots, a_n)$ et $b = (b_1, \dots, b_m)$ des mots dans l'alphabet A tels que $\mathrm{C}^*(a) = \mathrm{C}^*(b)$, c'est-à-dire $\mathrm{C}(a_1) \dots \mathrm{C}(a_n) = \mathrm{C}(b_1) \dots \mathrm{C}(b_m)$; démontrons que $a = b$.

Si $a = \varepsilon$, alors $\mathrm{C}(a) = \varepsilon$, donc les mots $\mathrm{C}(b_1), \dots, \mathrm{C}(b_m)$ sont vides, ce qui impose $m = 0$. Ainsi $a = \varepsilon = b$. De même, si $b = \varepsilon$, alors $a = \varepsilon$.

Supposons maintenant $n \geqslant 1$, d'où $m \geqslant 1$ d'après ce qui précède. Posons $p = \ell(a_1)$ et supposons, quitte à échanger a et b, que $p \leqslant \ell(b_1)$. Par définition des mots $\mathrm{C}(a)$ et $\mathrm{C}(b)$, le mot de B^* formé des p premiers symboles de $\mathrm{C}(a)$ est égal à $\mathrm{C}(a_1)$. Comme $\mathrm{C}(a_1)\mathrm{C}(a_2) \dots \mathrm{C}(a_n) = \mathrm{C}(a) = \mathrm{C}(b) = \mathrm{C}(b_1) \dots \mathrm{C}(b_m)$ et $\ell(b_1) \geqslant p$, c'est aussi le mot formé des p premiers symboles de $\mathrm{C}(b_1)$. Par suite, $\mathrm{C}(a_1)$ est le début du mot $\mathrm{C}(b_1)$. Puisque C est un code préfixe, on a donc $a_1 = b_1$. Les mots formés à partir de $\mathrm{C}(a)$ et $\mathrm{C}(b)$ en enlevant les p premiers symboles sont aussi égaux ; on a donc $\mathrm{C}(a_2) \dots \mathrm{C}(a_n) = \mathrm{C}(b_2) \dots \mathrm{C}(b_m)$. Par récurrence, cela entraîne $m = n$ et $a_2 = b_2, \dots, a_n = b_n$.

Nous avons ainsi démontré que $a = b$.

Exemple **(2.1.5)**. — Supposons $\mathrm{A} = \{\mathrm{a}, \mathrm{b}, \mathrm{c}\}$ et $\mathrm{B} = \{0, 1\}$. Le code C tel que $\mathrm{C}(\mathrm{a}) = 00$, $\mathrm{C}(\mathrm{b}) = 01$ et $\mathrm{C}(\mathrm{c}) = 1$ est un code préfixe, puisqu'aucun des trois mots 00, 01 et 1 n'est le début d'un autre. Expliquons comment décoder le mot 0010001. Si c'est le code d'un mot m, ce mot m n'est pas vide puisque seul le

mot vide a pour codage un mot vide ; soit alors x le premier symbole de m. Par définition de l'application C^*, le mot 0010001 commence par $C(x)$; on voit que seul $x = a$ convient, si bien que le premier symbole de m doit être a. Si $m = am'$, la relation $C^*(m) = 0010001 = C^*(am') = C(a)C^*(m') = 00C^*(m')$ entraîne que $C^*(m') = 10001$. De même, on trouve que m' n'est pas le mot vide et commence par c ; en écrivant $m' = cm''$, il vient de même $C^*(m'') = 0001$. Par le même raisonnement, on obtient $m'' = ab$, d'où $m = acab$.

Cet argument permet plus généralement de constater qu'un mot dans B^* n'appartient pas à l'image de C^*. Cherchons par exemple un mot m tel que $C^*(m) = 100010$. Ce mot doit débuter par cab, et si on l'écrit $m = cabm'$, pour $m' \in A^*$, on a $C(m') = 0$. Cet mot m' ne peut pas être vide ; il débute donc par l'un des mots $C(a), C(b), C(c)$, ce qui est absurde.

Remarque **(2.1.6)**. — On dit également qu'un code préfixe est *instantanément décodable*. En effet, si $a \in A^*$, il n'est pas besoin de parcourir tout le mot $C^*(a)$ pour déterminer le premier symbole de a, il suffit de reconnaître, en tête de $C^*(a)$, l'un des mots $C(x)$, pour $x \in A$. Alors, x est le premier symbole de a, on peut écrire $a = xa'$, pour $a' \in A^*$, et il reste à décoder le mot $C^*(a')$ obtenu en enlevant de la tête de $C^*(a)$ le mot $C(x)$.

2.2. L'inégalité de Kraft–McMillan

Proposition **(2.2.1)** (Kraft, McMillan). — *Soit* A *un ensemble et soit* C *un code sur* A *à valeurs dans les mots sur un alphabet fini* B. *Posons* $D = \mathrm{Card}(B)$. *Si le code* C *est uniquement décodable, on a l'inégalité*

$$\sum_{a \in A} D^{-\ell(C(a))} \leqslant 1.$$

Démonstration. — Pour prouver l'inégalité, on peut supposer que l'ensemble A est fini. Soit N un entier tel que $N \geqslant \ell(C(a))$ pour tout $a \in A$.

Soit k un entier $\geqslant 1$. On a

$$\left(\sum_{a \in A} D^{-\ell(C(a))}\right)^k = \sum_{(a_1,\dots,a_k) \in A^k} D^{-\ell(C(a_1))} \dots D^{-\ell(C(a_k))} = \sum_{a \in A^k} D^{-\ell(C(a))}.$$

Pour tout entier m, soit c_m le nombre d'éléments $a \in A^k$ tels que $C(a)$ soit de longueur m. Par hypothèse, l'application de A^k dans B^* donnée par $(a_1, \dots, a_k) \mapsto C(a_1) \dots C(a_k)$ est injective. Ainsi, c_m est le nombre de mots

de B^m de la forme $\mathrm{C}(a)$, pour $a \in \mathrm{A}^k$, si bien que $c_m \leqslant \mathrm{D}^m$. On a aussi $c_m = 0$ si $m > k\mathrm{N}$. Alors,

$$\sum_{a\in\mathrm{A}^k} \mathrm{D}^{-\ell(\mathrm{C}(a))} = \sum_m c_m \mathrm{D}^{-m} \leqslant \sum_{m=1}^{k\mathrm{N}} \mathrm{D}^m \mathrm{D}^{-m} = k\mathrm{N}.$$

Par suite,

$$\sum_{a\in\mathrm{A}} \mathrm{D}^{-\ell(\mathrm{C}(a))} \leqslant (k\mathrm{N})^{1/k}.$$

Lorsqu'on fait tendre k vers $+\infty$, on obtient l'inégalité voulue. □

Théorème **(2.2.2)** (Shannon). — *Soit* X *une variable aléatoire discrète à valeurs dans un ensemble* A*. Soit* C *un code sur un alphabet* A*, à valeurs dans un alphabet fini* B *de cardinal* $\mathrm{D} \geqslant 2$*. Si* C *est uniquement décodable, la longueur moyenne de* $\mathrm{C}(\mathrm{X})$ *vérifie l'inégalité*

$$\mathbf{E}(\ell(\mathrm{C}(\mathrm{X}))) \geqslant \mathrm{H}_\mathrm{D}(\mathrm{X}),$$

où $\mathrm{H}_\mathrm{D}(\mathrm{X})$ *est l'entropie en base* D *de* X*. Il y a égalité si et seulement si* $\ell(\mathrm{C}(a)) = -\log_\mathrm{D}(\mathbf{P}(\mathrm{X} = a))$ *pour tout* $a \in \mathrm{A}$ *tel que* $\mathbf{P}(\mathrm{X} = a) > 0$*.*

Démonstration. — Déduisons l'inégalité de Shannon de l'inégalité de Kraft–McMillan. Par définition de la longueur moyenne de $\mathrm{C}(\mathrm{X})$ et de l'entropie de X, on a

$$\begin{aligned}\mathbf{E}(\ell(\mathrm{C}(\mathrm{X}))) - \mathrm{H}_\mathrm{D}(\mathrm{X}) &= \sum_{a\in\mathrm{A}} \mathbf{P}(\mathrm{X} = a)\ell(\mathrm{C}(a)) + \sum_{a\in\mathrm{A}} \mathbf{P}(\mathrm{X} = a)\log_\mathrm{D}(\mathbf{P}(\mathrm{X} = a)) \\ &= -\sum_{a\in\mathrm{A}} \mathbf{P}(\mathrm{X} = a)\log_\mathrm{D}\left(\frac{\mathrm{D}^{-\ell(\mathrm{C}(a))}}{\mathbf{P}(\mathrm{X} = a)}\right).\end{aligned}$$

Comme la fonction logarithme est concave, on a

$$\begin{aligned}\sum_{a\in\mathrm{A}} \mathbf{P}(\mathrm{X} = a)\log_\mathrm{D}\left(\frac{\mathrm{D}^{-\ell(\mathrm{C}(a))}}{\mathbf{P}(\mathrm{X} = a)}\right) &\leqslant \log_\mathrm{D}\left(\sum_{a\in\mathrm{A}} \mathbf{P}(\mathrm{X} = a)\frac{\mathrm{D}^{-\ell(\mathrm{C}(a))}}{\mathbf{P}(\mathrm{X} = a)}\right) \\ &= \log_\mathrm{D}\left(\sum_{a\in\mathrm{A}} \mathrm{D}^{-\ell(\mathrm{C}(a))}\right).\end{aligned}$$

D'après l'inégalité de Kraft, l'argument du logarithme est $\leqslant 1$; puisque la fonction logarithme est croissante, on a donc

$$\sum_{a\in\mathrm{A}} \mathbf{P}(\mathrm{X} = a)\log_\mathrm{D}\left(\frac{\mathrm{D}^{-\ell(\mathrm{C}(a))}}{\mathbf{P}(\mathrm{X} = a)}\right) \leqslant 0.$$

Ainsi, $\mathbf{E}(\ell(\mathrm{C}(\mathrm{X}))) - \mathrm{H}_{\mathrm{D}}(\mathrm{X}) \geqslant 0$, d'où l'inégalité de Shannon. La fonction logarithme est strictement concave et strictement croissante. Pour qu'il y ait égalité, il faut donc, et il suffit, d'une part que $\sum \mathrm{D}^{-\ell(\mathrm{C}(a))} = 1$, et d'autre part que tous les termes $\mathrm{D}^{-\ell(\mathrm{C}(a))}/\mathbf{P}(\mathrm{X} = a)$, pour $a \in \mathrm{A}$ tel que $\mathbf{P}(\mathrm{X} = a) > 0$, soient égaux. Puisque $\sum \mathbf{P}(\mathrm{X} = a) = 1$, cela signifie que $\mathrm{D}^{-\ell(\mathrm{C}(a))} = \mathbf{P}(\mathrm{X} = a)$ pour tout a tel que $\mathbf{P}(\mathrm{X} = a) > 0$, autrement dit, $\ell(\mathrm{C}(a)) = -\log_{\mathrm{D}}(\mathbf{P}(\mathrm{X} = a))$ pour tout a tel que $\mathbf{P}(\mathrm{X} = a) > 0$. □

2.2.3. Codes efficaces. — Soit A un alphabet et soit p une loi de probabilité sur A. Soit B un alphabet fini de cardinal $\mathrm{D} \geqslant 2$.

D'après l'inégalité de Shannon, on a $\mathbf{E}(\ell(\mathrm{C}(\mathrm{X}))) \geqslant \mathrm{H}_{\mathrm{D}}(\mathrm{X})$, pour toute variable aléatoire X à valeurs dans A : l'entropie fournit une limite irrémédiable à la compression d'un message. Nous allons maintenant voir que cette limite peut essentiellement être atteinte, qui plus est, par un code préfixe ! Nous commençons par une réciproque à l'inégalité de Kraft-McMillan.

Proposition **(2.2.4)**. — *Soit* A *un ensemble, soit* D *un entier* $\geqslant 1$ *et soit* $\ell : \mathrm{A} \to \mathbf{N}^*$ *une application telle que l'inégalité*

$$\sum_{a \in \mathrm{A}} \mathrm{D}^{-\ell(a)} \leqslant 1$$

soit vérifiée. Il existe un code préfixe C *sur* A *à valeurs dans un alphabet de cardinal* D *tel que* $\ell(\mathrm{C}(a)) = \ell(a)$ *pour tout* $a \in \mathrm{A}$.

Démonstration. — Numérotons les éléments de A en une suite $a_1, a_2, \ldots$, de sorte que $\ell(a_1) \leqslant \ell(a_2) \leqslant \ldots$. C'est évidemment possible lorsque l'ensemble A est fini. Lorsqu'il est infini, on observe que pour tout entier n, l'ensemble des $a \in \mathrm{A}$ tels que $\ell(a) = n$ est fini, car sinon la somme $\sum_a \mathrm{D}^{-\ell(a)}$ serait infinie. Il suffit alors de numéroter d'abord les éléments a de A tels que $\ell(a) = 1$, puis ceux tels que $\ell(a) = 2$, etc.

On définit alors une suite strictement croissante de nombres rationnels en posant

$$z_n = \sum_{m<n} \mathrm{D}^{-\ell(a_m)},$$

pour tout entier n tel que $n \leqslant \mathrm{Card}(\mathrm{A})$. Puisque $\sum_{a \in \mathrm{A}} \mathrm{D}^{-\ell(a)} \leqslant 1$, on a $z_n \leqslant 1 - \mathrm{D}^{-\ell(a_n)} < 1$ pour tout entier $n \leqslant \mathrm{Card}(\mathrm{A})$. Considérons le développement en base D de z_n : il est de la forme $z_n = 0{,}y_1 y_2 \ldots y_p$, où l'entier p vérifie $p \leqslant \ell(a_{n-1})$.

Associons alors au symbole a_n le code $C(a_n) = y_1 \dots y_p 0 \dots 0$ dans l'alphabet $\{0; 1; \dots; D-1\}$, complété par $\ell(a_n) - p$ symboles 0 de sorte que $\ell(C(a_n)) = \ell(a_n)$.

Soit m, n des entiers tels que $m < n \leqslant \mathrm{Card}(A)$. On a

$$z_n - z_m = \sum_{q=m}^{n-1} D^{-\ell(a_q)} \geqslant D^{-\ell(a_m)}.$$

Par suite, les développements en base D de z_m et z_n diffèrent au moins par le $\ell(a_m)$-ième chiffre, de sorte que $C(a_m)$ n'est pas préfixe de $C(a_n)$. Mais $C(a_n)$ n'est pas non plus préfixe de $C(a_m)$: c'est évident si $\ell(a_n) > \ell(a_m)$, et dans le cas où $\ell(a_m) = \ell(a_n)$, cela signifierait que $C(a_m) = C(a_n)$.

L'application $C : A \to \{0; \dots; D-1\}^*$ est un code préfixe tel que $\ell(C(a)) = \ell(a)$ pour tout a. □

Exemple **(2.2.5)**. — Supposons que $A = \{a, b, c, d, e\}$ et supposons que l'on ait $\ell(a) = \ell(b) = 1$, $\ell(c) = 2$, $\ell(d) = \ell(e) = 3$; on numérote A par $a_1 = a, a_2 = b, \dots, a_5 = e$. Prenons $D = 3$. Les nombres réels $z_1, \dots, z_5$ construits par la preuve de la proposition sont (en base 3) $z_1 = 0, z_2 = 0{,}1, z_3 = 0{,}2, z_4 = 0{,}21$ et $z_5 = 0{,}211$. On pose alors $C(a) = 0$, $C(b) = 1$, $C(c) = 20$, $C(d) = 210$ et $C(e) = 211$.

Théorème **(2.2.6)** (Shannon). — *Soit* X *une variable aléatoire discrète à valeurs dans un alphabet* A*; on suppose que* $\mathbf{P}(X = a) > 0$ *pour tout* $a \in A$. *Soit* B *un ensemble fini de cardinal* $D \geqslant 2$. *Il existe un code préfixe* C *sur* A, *à valeurs dans* B, *tel que*

$$H_D(X) \leqslant \mathbf{E}(\ell(C(X))) < H_D(X) + 1.$$

Pour qu'il existe un tel code C *vérifiant l'égalité* $\mathbf{E}(\ell(C(X))) = H_D(X)$, *il faut et il suffit que pour tout élément* $a \in A$, $\mathbf{P}(X = a)$ *soit de la forme* D^{-m} *pour un entier* $m \geqslant 0$*; on a alors* $\ell(C(a)) = -\log_D(\mathbf{P}(X = a))$.

Démonstration. — Pour tout $a \in A$, posons $\lambda(a) = \lceil -\log_D(\mathbf{P}(X = a)) \rceil$, le plus petit entier supérieur ou égal à $\log_D(\mathbf{P}(X = a))$, de sorte que $D^{-\lambda(a)} \leqslant \mathbf{P}(X = a)$. On a donc $\sum_{a \in A} D^{-\lambda(a)} \leqslant \sum_{a \in A} \mathbf{P}(X = a) = 1$. D'après la proposition 2.2.4, il existe ainsi un code préfixe $C : A \to \{0; 1; \dots, D-1\}^*$ tel que $\ell(C(a)) = \lambda(a)$ pour tout $a \in A$. Démontrons que ce code vérifie la conclusion du théorème.

L'inégalité $\mathrm{H_D(X)} \leqslant \mathbf{E}(\ell(\mathrm{C(X)}))$ est un cas particulier du théorème 2.2.2. D'autre part, on a

$$\begin{aligned}\mathbf{E}(\ell(\mathrm{C(X)})) &= \sum_{a\in\mathrm{A}} \mathbf{P}(\mathrm{X}=a)\ell(\mathrm{C}(a)) = \sum_{a\in\mathrm{A}} \mathbf{P}(\mathrm{X}=a)\lceil \log_{\mathrm{D}}(\mathbf{P}(\mathrm{X}=a))\rceil \\ &< \sum_{a\in\mathrm{A}} \mathbf{P}(\mathrm{X}=a)\left(\log_{\mathrm{D}}(\mathbf{P}(\mathrm{X}=a))+1\right) \\ &= \mathrm{H_D(X)} + \sum_{a\in\mathrm{A}} \mathbf{P}(\mathrm{X}=a) = \mathrm{H_D(X)}+1.\end{aligned}$$

Cela conclut la démonstration.

La dernière assertion résulte de cela et du théorème 2.2.2 : d'après ce théorème, le cas d'égalité se produit si et seulement si $\ell(\mathrm{C}(a)) = -\log_{\mathrm{D}}(\mathbf{P}(\mathrm{X}=a))$ pour tout $a \in \mathrm{A}$. D'autre part, si $\mathbf{P}(\mathrm{X}=a)$ est de la forme D^{-m}, on a $\lambda(a) = -\log_{\mathrm{D}}(\mathbf{P}(\mathrm{X}=a))$ et le code construit vérifie $\mathbf{E}(\ell(\mathrm{C(X)}) = \mathrm{H_D(X)}$. □

2.3. Codes optimaux

2.3.1. — Bien que sa longueur moyenne soit proche de l'optimum (limité par l'entropie), le code préfixe construit par la méthode de la preuve du théorème 2.2.6 n'est pas toujours optimal. Par exemple, lorsque X suit une loi de Bernoulli de paramètre $p \in]0;1[$ et que l'alphabet-but a deux symboles, les mots codés ont longueur $\lceil -\log_2(p)\rceil$ et $\lceil -\log_2(1-p)\rceil$, alors qu'on pourrait se contenter de recopier X ! Ce code trivial a longueur moyenne 1, alors que la longueur moyenne du code proposé par Shannon est égale à $\mathrm{S}(p) = p\lceil -\log_2(p)\rceil + (1-p)\lceil -\log_2(1-p)\rceil$; il n'y a égalité que si $p = 1/2$, qui est d'ailleurs le seul cas où les probabilités p et $1-p$ sont toutes deux de la forme 2^{-m}. En fait, lorsque $2^{-m-1} \leqslant p < 2^{-m}$, avec $m \geqslant 1$, on a $\lceil -\log_2(p)\rceil = m+1$, tandis que $1-p > 1/2$, de sorte que $\lceil -\log_2(1-p)\rceil = 1$. Alors, $\mathrm{S}(p) = p(m+1)+(1-p) = mp+1 < 1+m/2^m < 1{,}5$. Et lorsque $p \to 1/2$ par valeurs inférieures, $\mathrm{S}(p)$ converge vers 1,5.

Définition **(2.3.2)**. — *Soit* C *un code uniquement décodable sur un alphabet* A *à valeurs dans un un alphabet* B. *Soit* p *une loi de probabilité sur* A *telle que* $p(a) > 0$ *pour tout* $a \in \mathrm{A}$. *On dit que* C *est optimal (par rapport à* p*) si le code* C *minimise l'expression* $\sum_{a\in\mathrm{A}} p(a)\ell(\mathrm{C}(a))$ *parmi tous les codes uniquement décodables à valeurs dans l'alphabet* B.

L'expression $\ell_p(\mathrm{C}) = \sum_{a\in\mathrm{A}} p(a)\ell(\mathrm{C}(a))$ est la valeur moyenne du code d'un symbole de A, lorsque ces symboles sont pris avec la loi p.

Lemme **(2.3.3)**. — *Soit* A *un alphabet fini et soit p une loi de probabilité sur* A *telle que $p(a) > 0$ pour tout $a \in \mathrm{A}$. Soit* B *un alphabet fini*

a) *Il existe un code préfixe sur* A *à valeurs dans* B *qui est optimal.*

b) *Si* C *est un code optimal, et si a, b sont des éléments de* A *tels que $p(a) < p(b)$, alors $\ell(\mathrm{C}(a)) \geqslant \ell(\mathrm{C}(b))$ — les symboles moins probables ont des codes plus longs ;*

c) *Si* C *est un code préfixe qui est optimal, alors pour chaque symbole $a \in \mathrm{A}$ tel que* $\mathrm{C}(a)$ *soit de longueur maximale, il existe $b \in \mathrm{A}$ tel que* $\mathrm{C}(b)$ *soit de même longueur que* $\mathrm{C}(a)$ *et en diffère uniquement par le dernier symbole.*

Démonstration. — a) Les éléments $a \in \mathrm{A}$ tels que $p(a) = 0$ n'interviennent pas dans la définition de la longueur moyenne d'un code ; quitte à remplacer A par l'ensemble des éléments a tels que $p(a) > 0$, on suppose que $p(a) > 0$ pour tout $a \in \mathrm{A}$.

Soit C_1 un code uniquement décodable et soit C un autre code uniquement décodable tel que $\ell_p(\mathrm{C}) \leqslant \ell_p(\mathrm{C}_1)$. On a en particulier $p(a)\ell(\mathrm{C}(a)) < \ell_p(\mathrm{C}_1)$ pour tout $a \in \mathrm{A}$, donc $\ell(\mathrm{C}(a)) < \ell_p(\mathrm{C}_1)/p(a)$. Ainsi, le code C est une application de A dans l'ensemble fini des mots de longueurs $< \ell_p(\mathrm{C}_1)/\inf(p)$. L'ensemble de ces applications étant fini, il n'y a qu'un nombre fini de codes uniquement décodables de longueur moyenne inférieure ou égale à celle de C_1. On trouvera dans cet ensemble fini un code uniquement décodable de longueur moyenne minimale, c'est-à-dire optimal.

Soit alors C un code optimal. Les longueurs $\ell(\mathrm{C}(a))$ vérifient l'inégalité de Kraft $\sum \mathrm{D}^{-\ell(\mathrm{C}(a))} \leqslant 1$. Il existe alors un code *préfixe* C′ tel que $\ell(\mathrm{C}'(a)) = \ell(\mathrm{C}(a))$ pour tout $a \in \mathrm{A}$. Le code C′ a même longueur moyenne que C, donc est un code optimal.

b) Soit C un code optimal et soit a, b des éléments de A tels que $p(a) < p(b)$ et $\ell(\mathrm{C}(a)) < \ell(\mathrm{C}(b))$. Considérons le code C′ qui coïncide avec C sur $\mathrm{A} - \{a, b\}$

mais qui échange les codes de a et b : $\mathrm{C}'(a) = \mathrm{C}(b)$ et $\mathrm{C}'(b) = \mathrm{C}(a)$. On a

$$\begin{aligned}\ell_p(\mathrm{C}) - \ell_p(\mathrm{C}') &= \sum_{x\in\mathrm{A}} p(x)\ell(\mathrm{C}(x)) - \sum_{x\in\mathrm{A}} \ell(\mathrm{C}'(x)) \\ &= p(a)\ell(\mathrm{C}(a)) + p(b)\ell(\mathrm{C}(b)) - p(a)\ell(\mathrm{C}'(a)) - p(b)\ell(\mathrm{C}'(b)) \\ &= p(a)\ell(\mathrm{C}(a)) + p(b)\ell(\mathrm{C}(b)) - p(a)\ell(\mathrm{C}(b)) - p(b)\ell(\mathrm{C}(a)) \\ &= (p(a) - p(b))(\ell(\mathrm{C}(a)) - \ell(\mathrm{C}(b))) \\ &> 0.\end{aligned}$$

Cela contredit l'hypothèse que C est un code optimal.

c) Soit C un code préfixe optimal. Soit a un élément de A dont le code est de longueur maximale ; écrivons $\mathrm{C}(a) = mx$, où $m \in \mathrm{B}^*$ et $x \in \mathrm{B}$. Supposons que m n'est pas préfixe d'un mot de code. Soit alors C′ le code qui coïncide avec C sur $\mathrm{A} - \{a\}$ et tel que $\mathrm{C}'(a) = m$. C'est encore un code préfixe : $\mathrm{C}'(a)$ n'est pas hypothèse pas préfixe d'un autre mot, et un autre mot, disons $\mathrm{C}'(b) = \mathrm{C}(b)$, ne peut être préfixe de $\mathrm{C}'(a)$, puisqu'il serait alors préfixe de $\mathrm{C}(a)$. En particulier, le code C′ est uniquement décodable, mais sa longueur moyenne est strictement plus petite que celle de C, ce qui contredit l'hypothèse que C est optimal. Donc m est préfixe d'un autre mot de code, disons $\mathrm{C}(b)$; écrivons $\mathrm{C}(b) = mp$, avec $p \in \mathrm{B}^*$. Comme $\mathrm{C}(a) = mx$ est de longueur maximale, égale à $\ell(m) + 1$, on a $\ell(p) = \ell(\mathrm{C}(b)) - \ell(m) \leqslant \ell(\mathrm{C}(a)) - \ell(m) = 1$, c'est-à-dire que p est soit le mot vide, soit réduit à un seul symbole. Si p est vide, $\mathrm{C}(b) = m$ est préfixe de $\mathrm{C}(a) = mx$, ce qui contredit l'hypothèse que C est un code préfixe. Il existe donc $y \in \mathrm{B}$ tel que $p = (y)$. Les mots $\mathrm{C}(a) = mx$ et $\mathrm{C}(b) = my$ diffèrent donc uniquement par leur dernier symbole. □

2.3.4. Code de Huffman. — Soit A un ensemble fini et soit $(p(a))_{a\in\mathrm{A}}$ une loi de probabilité sur A telle que $p(a) > 0$ pour tout $a \in \mathrm{A}$. Lorsque l'alphabet d'arrivée B est $\{0, 1\}$, le *code de Huffman* (relativement à la loi p) est construit de la façon suivante par récurrence sur le cardinal de A.

Si $\mathrm{Card}(\mathrm{A}) = 2$, le code H associe aux deux symboles de A les mots 0 et 1, tous deux de longueur 1. Supposons $\mathrm{Card}(\mathrm{A}) > 2$ et soit a, b deux éléments de A minimisant p : explicitement, on a $p(a), p(b) \leqslant \inf_{c\neq a,b} p(c)$. Soit A′ la réunion de l'ensemble $\mathrm{A} - \{a, b\}$ et d'un élément auxiliaire noté ab ; on définit une loi de probabilité sur A′ par $p'(c) = p(c)$ si $c \in \mathrm{A} - \{a, b\}$, et $p(ab) = p(a) + p(b)$. Soit H′ un code de Huffman (pour la loi p' sur l'alphabet A′. Le code H_p associe à un

symbole $c \in A - \{a, b\}$ le mot $H'(c)$; si $m = H'(ab)$ est le code du symbole ab pour H', on pose aussi $H(a) = m0$ et $H(b) = m1$.

Exemple **(2.3.5)**. — Supposons $A = a, b, c, d, e$, avec les probabilités données par le tableau

a	b	c	d	e
0,25	0,25	0,20	0,15	0,15

La méthode commence par combiner d et e et leur associer la probabilité $p'(de) = 0,30$, les autres symboles étant a, b, c, avec leurs probabilités initiales, d'où le tableau

a	b	c	de
0,25	0,25	0,20	0,30

Puis elle combine, disons a et c et leur associe la probabilité $p''(ac) = 0,45$, les autres symboles étant b, de de probabilités 0,25 et 0,30 :

ac	b	de
0,45	0,25	0,30

Ensuite, elle combine b et de, d'où les deux symboles bde et ac, avec probabilités 0, 55 et 0,45.

ac	bde
0,45	0,55

On parcourt maintenant le chemin en sens inverse. À la dernière étape, on code ac par 0, bde par 1. À l'avant dernière, on code ac par 0, b par 10 et de par 11. Puis on code c par 00, a par 01, b par 10 et de par 11. Finalement, le code obtenu est

a	b	c	d	e
01	10	00	110	111

L'entropie (en base 2) d'une variable aléatoire X de loi p est égale à

$$H_2(X) = -2 \cdot 0,25 \log_2(0,25) - 0,20 \log_2(0,20) - 2 \cdot 0,15 \log_2(0,15) \approx 2,285.$$

La longueur moyenne du code ci-dessus est alors

$$\mathbf{E}(\ell_H(X)) = (2 \cdot 0,25 + 0,20) \cdot 2 + (2 \cdot 0,15) \cdot 3 = 2,3.$$

Pour comparaison, les longueurs du code construit par la méthode de Shannon sont 2, 2, 3, 3, 3, de sorte que sa longueur moyenne est

$$\mathbf{E}(\ell_S(X)) = (2 \cdot 0,25) \cdot 2 + (0,20) + 2 \cdot 0,15) \cdot 3 = 2,5.$$

Voici d'ailleurs un tel code :

a	b	c	d	e
00	01	100	101	110

Proposition **(2.3.6)** (D. Huffman, 1952). — *Soit* A *un ensemble fini et soit p une loi de probabilité sur* A*. Tout code de Huffman relativement à la loi p sur* A *est un code préfixe et est optimal (relativement à la loi p).*

Démonstration. — Soit H un code de Huffman relativement à la loi p sur A. Prouvons par récurrence sur le cardinal de A que ce code H est un code préfixe. C'est évident si $\mathrm{Card}(A) \leqslant 2$; supposons maintenant $\mathrm{Card}(A) \geqslant 3$. Reprenons les notations de la construction : a, b sont deux éléments de A de probabilités minimales, l'ensemble A′ est la réunion de $A - \{a, b\}$ et d'un symbole ab, et la loi de probabilité p' sur A′ attache à tout $c \neq a, b$ la probabilité qu'il avait pour p, et à ab la somme des probabilités de a et b.

Par récurrence, le code H′ associé à A′ et à la loi p' est un code préfixe. Les mots de H sont les $H(c) = H'(c)$, pour $c \neq a, b$, et les deux mots $H(a) = H'(ab)0$ et $H(b) = H'(ab)1$. Par récurrence, $H(c)$ et $H(c')$ ne sont pas préfixes l'un de l'autre si c, c' sont des éléments distincts, distincts de a, b. Les mots $H(a) = H'(ab)0$ et $H(b) = H'(ab)1$ ne sont pas préfixes l'un de l'autre, puisqu'ils ont même longueur et sont distincts. Pour $c \neq a, b$, le mot $H(c) = H'(c)$ n'est pas préfixe du mot $H'(ab)$, par l'hypothèse de récurrence. S'il est préfixe de l'un des mots $H'(ab)0$ ou $H'(ab)1$, c'est qu'il leur est égal, mais alors $H'(ab)$ est préfixe de $H'(c)$, une contradiction. Enfin, si $H(a) = H'(ab)0$ est préfixe de $H(c)$, pour $c \neq a, b$, alors $H'(ab)$ est préfixe de $H'(c) = H(c)$, une contradiction également. De même, $H(b)$ n'est pas préfixe de $H(c)$, pour aucun $c \neq a, b$. Cela prouve que le code H est un code préfixe.

Démontrons maintenant que le code H est optimal relativement à la loi p. Soit C un code binaire uniquement décodable optimal; par définition, la longueur moyenne de C est inférieure à celle de H, c'est-à-dire que l'on a

$$\sum_{x \in A} p(x)\ell(C(x)) \leqslant \sum_{x \in A} p(x)\ell(H(x)).$$

Démontrons que l'on a en fait égalité, ce qui prouvera que H est optimal.

On peut déjà supposer que C est un code préfixe.

Soit $x \in \mathrm{A}$ un élément tel que $\mathrm{C}(x)$ soit de longueur maximale. Si l'on échange $\mathrm{C}(a)$ et $\mathrm{C}(x)$, on obtient un code C_1 dont la longueur moyenne vérifie

$$\begin{aligned}\ell_p(\mathrm{C}_1) - \ell_p(\mathrm{C}) &= p(a)\ell(\mathrm{C}(x)) + p(x)\ell(\mathrm{C}(a)) - p(a)\ell(\mathrm{C}(a)) - p(x)\ell(\mathrm{C}(x)) \\ &= (p(a) - p(x))(\ell(\mathrm{C}(x)) - \ell(\mathrm{C}(a))) \\ &\leqslant 0\end{aligned}$$

puisque $p(a)$ est minimal. Le nouveau code est donc de longueur moyenne inférieure ou égale à celle du code C, donc égale puisque le code C était supposé optimal. C'est aussi un code préfixe. On peut donc supposer que $\mathrm{C}(a)$ est de longueur maximale.

Puisque le code C est un code préfixe optimal, il existe un symbole $y \neq a$ tels que $\mathrm{C}(a)$ et $\mathrm{C}(y)$ ne diffèrent que par leur dernier symbole. Si l'on échange $\mathrm{C}(b)$ et $\mathrm{C}(y)$, on obtient un code C_2 dont la longueur moyenne vérifie

$$\begin{aligned}\ell_p(\mathrm{C}_2) - \ell_p(\mathrm{C}) &= p(b)\ell(\mathrm{C}(y)) + p(y)\ell(\mathrm{C}(b)) - p(b)\ell(\mathrm{C}(b)) - p(y)\ell(\mathrm{C}(y)) \\ &= (p(b) - p(y))(\ell(\mathrm{C}(y)) - \ell(\mathrm{C}(b))) \\ &\leqslant 0\end{aligned}$$

puisque $p(b) \leqslant p(y)$ et $\ell(\mathrm{C}(y)) = \ell(\mathrm{C}(a)) \geqslant \ell(\mathrm{C}(b))$. De même, le code C_2 est de longueur moyenne inférieure ou égale à celle du code C, donc égale, puisque C est optimal. On peut donc remplacer C par C_2, ce qui permet de supposer que $\mathrm{C}(b)$ diffère de $\mathrm{C}(a)$ par son dernier symbole uniquement.

Quitte à échanger $\mathrm{C}(a)$ et $\mathrm{C}(b)$, on suppose aussi que $\mathrm{C}(a)$ se termine par 0 et $\mathrm{C}(b)$ se termine par 1.

Le codage de Huffman a introduit l'alphabet $\mathrm{A}' = \mathrm{A} - \{a, b\} \cup \{ab\}$, muni de la loi de probabilité p' qui coïncide avec p sur $\mathrm{A} - \{a, b\}$et telle que $p'(ab) = p(a) + p(b)$. Définissons un code C′ sur cet alphabet en posant $\mathrm{C}'(x) = \mathrm{C}(x)$ si $x \in \mathrm{A} - \{a, b\}$, et en prenant pour $\mathrm{C}'(ab)$ le mot déduit de $\mathrm{C}(a)$ (ou de $\mathrm{C}(b)$) en enlevant le dernier symbole. C'est un code préfixe : En effet, si x, y sont des éléments distincts de $\mathrm{A} - \{a, b\}$, on a $\mathrm{C}'(x) = \mathrm{C}(x)$ et $\mathrm{C}'(y) = \mathrm{C}(y)$, et C est un code préfixe, donc $\mathrm{C}'(x)$ n'est pas préfixe de $\mathrm{C}'(y)$ puisque C. Si $x \in \mathrm{A} - \{a, b\}$, alors $\mathrm{C}'(x) = \mathrm{C}(x)$ n'est pas préfixe de $\mathrm{C}'(ab)$, car sinon $\mathrm{C}(x)$ serait préfixe de $\mathrm{C}(a)$ puisque $\mathrm{C}'(a)$ est préfixe de $\mathrm{C}(a)$; comme $\mathrm{C}(a)$ est un mot de longueur maximale et $\mathrm{C}'(ab)$ est un préfixe strict de $\mathrm{C}(a)$, le mot $\mathrm{C}'(ab)$ est strictement plus court que $\mathrm{C}'(x) = \mathrm{C}(x)$,

donc n'en est pas préfixe. La longueur moyenne du code C′ (relativement à la loi p') est donnée par

$$\begin{aligned}\ell_{p'}(\mathrm{C}') &= \sum_{x\neq a,b} p'(x)\ell(\mathrm{C}'(x)) + p'(ab)\ell(\mathrm{C}'(ab)) \\ &= \sum_{x\neq a,b} p(x)\ell(\mathrm{C}(x)) + (p(a)+p(b))(\ell(\mathrm{C}(a)-1) \\ &= \ell_p(\mathrm{C}) - (p(a)+p(b)),\end{aligned}$$

car $\ell(\mathrm{C}(a)) = \ell(\mathrm{C}(b))$. Le même calcul pour le code de Huffman H′ démontre que H′ est de longueur moyenne

$$\ell_p(\mathrm{H}) - (p(a)+p(b))$$

relativement à la loi p'. Par récurrence, le code de Huffman H′ est optimal relativement à la loi p', de sorte que $\ell_{p'}(\mathrm{C}') \geqslant \ell_{p'}(\mathrm{H}')$. On a donc $\ell_p(\mathrm{C}) \geqslant \ell_p(\mathrm{H})$, d'où l'égalité, comme il fallait démontrer. □

2.4. Loi des grands nombres et compression

Dans son article originel, Shannon (1948) utilisait une autre description de l'entropie, liée à la loi des grands nombres en théorie des probabilités.

Commençons par rappeler deux inégalités importantes.

Proposition **(2.4.1)**. — *Soit* X *une variable aléatoire possédant une espérance.*

a) *Pour tout nombre réel* $t > 0$*, on a l'*inégalité de Markov :

$$\mathbf{P}(|\mathrm{X}| > t) \leqslant \mathbf{E}(|\mathrm{X}|)/t.$$

b) *Supposons, de plus, que* X *possède une variance* V(X)*. Alors, pour tout nombre réel* $t > 0$*, on a l'*inégalité de Bienaymé–Tchebitcheff :

$$\mathbf{P}(|\mathrm{X} - \mathbf{E}(\mathrm{X})| > t) \leqslant \mathrm{V}(\mathrm{X})/t^2.$$

Démonstration. — a) Soit A l'ensemble des éléments ω de l'univers tels que $|\mathrm{X}(\omega)| > t$; il s'agit de majorer $\mathbf{P}(\mathrm{A})$. Observons que sur A, la variable aléatoire $|\mathrm{X}|/t$ est supérieure à 1 ; sur son complémentaire $\complement\mathrm{A}$, elle est positive ou nulle. On a donc $\mathbf{E}(|\mathrm{X}|/t) \geqslant 1\cdot\mathbf{P}(\mathrm{A}) + 0\cdot\mathbf{P}(\complement\mathrm{A})$. Comme $\mathbf{E}(|\mathrm{X}|/t) = \mathbf{E}(|\mathrm{X}|)/t$, l'inégalité de Markov en résulte.

b) On considère maintenant la variable aléatoire $Y = X - \mathbf{E}(X)$. Comme X a une variance, Y^2 possède une espérance, égale à $V(X)$ par définition. Appliquons donc à Y^2 l'inégalité de Markov : on trouve $\mathbf{P}(Y^2 > t^2) \leqslant \mathbf{E}(Y^2)/t^2 = V(X)/t^2$. Puisque $Y^2 > t^2$ équivaut à $|X - \mathbf{E}(X)| > t$, cela prouve l'inégalité de Bienaymé–Tchebitcheff. □

Nous utiliserons directement ces inégalités, mais il est intéressant d'en déduire tout de suite la *loi des grands nombres*.

Théorème **(2.4.2)** (Loi faible des grands nombres). — *Soit* (X_n) *une suite de variables indépendantes et identiquement distribuées, d'espérance finie. Pour tout* $n \geqslant 1$, *on pose* $S_n = (X_1 + \cdots + X_n)/n$. *Pour tout nombre réel* $t > 0$, *on a*

$$\mathbf{P}(|S_n - \mathbf{E}(X_1)| > t) \to 0$$

quand n tend vers $+\infty$.

Dans le langage de la théorie des probabilités, on dit que S_n *converge en probabilité vers* $\mathbf{E}(X_1)$.

Démonstration. — Comme toutes les X_n ont même loi, elles ont même espérance, en remplaçant X_n par $X_n - \mathbf{E}(X_1)$, on remplace S_n par $S_n - \mathbf{E}(X_1)$. Il suffit alors de démontrer que $\mathbf{P}(|S_n| > t)$ tend vers 0 sous l'hypothèse $\mathbf{E}(X_1) = 0$.

Commençons par démontrer une majoration précise de cette probabilité sous l'hypothèse supplémentaire que les variables aléatoires X_n sont de variance finie. Dans ce cas, S_n est de variance

$$V(S_n) = \mathbf{E}(S_n^2) = \frac{1}{n^2}\mathbf{E}((X_1 + \cdots + X_n)^2) = \frac{1}{n^2}\sum_{i,j}\mathbf{E}(X_iX_j).$$

Pour $i \neq j$, l'indépendance de X_i et X_j entraîne $\mathbf{E}(X_iX_j) = \mathbf{E}(X_i)\mathbf{E}(X_j) = 0$; pour $i = j$, on a $\mathbf{E}(X_i^2) = V(X_i) = V(X_1)$ puisque les X_i ont même loi, donc même variance. Ainsi, $V(S_n) = V(X_1)/n$. (Plus généralement, la variance d'une somme de variables aléatoires indépendantes est la somme de leurs variances.) Appliquons maintenant l'inégalité de Bienaymé–Tchebitcheff : pour tout nombre réel $t > 0$, on a

$$\mathbf{P}(|S_n| > t) \leqslant \mathbf{E}((S_n/t)^2) \leqslant V(S_n)/t^2.$$

Par suite, $\mathbf{P}(|S_n| > t) \leqslant V(X_1)/nt^2$, d'où le résultat voulu.

Le cas général est plus difficile et se démontre par une méthode classique de troncation. Introduisons un paramètre $\delta > 0$ et posons $X'_k = X_k$ si $|X_k| \leqslant \delta n$, et $X'_k = 0$ sinon; posons aussi

$X''_k = X_k - X'_k$. On va majorer les probabilités

$$\mathbf{P}(|X'_1 + \cdots + X'_n| > nt/2) \qquad \text{et} \qquad \mathbf{P}(|X''_1 + \cdots + X''_n| > nt/2).$$

La somme de ces probabilités fournira une majoration de $\mathbf{P}(|X_1 + \cdots + X_n| > nt)$ qui sera arbitrairement petite pour tout n assez grand. L'idée sous-jacente à cette méthode est que les X'_k sont majorées, donc de variance finie, et seront justiciables du premier cas, tandis que les X''_k seront rares, car X''_k est nulle lorsque X_k n'est pas trop grande.

Tout d'abord, les $|X'_j|$ sont de même loi, mutuellement indépendantes, et majorées par δn. Elles ont donc une variance commune, laquelle vérifie

$$V(X'_j) = V(X'_1) \leqslant \mathbf{E}((X'_1)^2) \leqslant \delta \mathbf{E}(|X'_1|)n \leqslant \delta \mathbf{E}(|X_1|)n.$$

Par suite,

$$V(X'_1 + \cdots + X'_n) = nV(X'_1) \leqslant \delta \mathbf{E}(|X_1|)n^2.$$

On a aussi

$$\mathbf{E}(X'_1 + \cdots + X'_n)^2 = \mathbf{E}(X'_1)^2 n^2.$$

Lorsque n tend vers l'infini, X'_1 tend vers X_1 presque sûrement, tout en étant majorée en valeur absolue par $|X_1|$; le théorème de convergence dominée entraîne donc que $\mathbf{E}(X'_1)$ tend vers $\mathbf{E}(X_1) = 0$. En particulier, pour n assez grand, $\mathbf{E}(X'_1 + \cdots + X'_n)^2 \leqslant \delta n^2$, et

$$\mathbf{E}((X'_1 + \cdots + X'_n)^2) \leqslant 2\delta \mathbf{E}(|X_1|)n^2.$$

L'inégalité de Bienaymé–Tchebitcheff entraîne alors que

$$\mathbf{P}(|X'_1 + \cdots + X'_n| > nt/2) \leqslant 8\delta \mathbf{E}(|X_1|)t^{-2} \tag{2.4.2.1}$$

pour tout entier n assez grand. Fixons un nombre réel $\varepsilon > 0$ et choisissons δ de sorte que

$$8\delta \mathbf{E}(|X_1|)t^{-2} < \varepsilon/2.$$

On retient alors de l'inégalité (2.4.2.1) que pour tout n assez grand, on a $\mathbf{P}(|X'_1 + \cdots + X'_n|) \leqslant \varepsilon/2$.

Par ailleurs,

$$\mathbf{P}(|X''_1 + \cdots + X''_n| > nt/2) \leqslant \mathbf{P}(X''_1 + \cdots + X''_n \neq 0) \leqslant n\mathbf{P}(X''_1 \neq 0),$$

puisque les X''_j sont de même loi. Or,

$$\mathbf{P}(X''_1 \neq 0) = \mathbf{P}(|X''_1| > \delta n) \leqslant \mathbf{E}(|X''_1|/\delta n) = \mathbf{E}(|X''_1|)\delta^{-1}n^{-1},$$

d'où l'inégalité

$$\mathbf{P}(|X''_1 + \cdots + X''_n| > nt/2) \leqslant \mathbf{E}(|X''_1|)\delta^{-1}. \tag{2.4.2.2}$$

Quand n tend vers $+\infty$, X''_1 tend presque partout vers 0, et l'on a $|X''_1| \leqslant |X_1|$, de sorte que $\mathbf{E}(|X''_1|)$ tend vers 0. Alors, pour n assez grand, l'inégalité (2.4.2.2) assure que $\mathbf{P}(|X''_1 + \cdots + X''_n| > nt/2) < \varepsilon/2$.

En combinant ces deux majorations, on en déduit que pour tout n assez grand, l'évènement $\{|X_1 + \cdots + X_n| > nt\}$ est de probabilité $< \varepsilon$, ce qui conclut la démonstration. □

Théorème **(2.4.3)** (Shannon). — *Soit* (X_n) *une suite de variables aléatoires prenant leurs valeurs dans un ensemble fini* A*, indépendantes et de même loi* p*; posons* $c = \sum_{a,b\in A} p_a p_b (\log(p_a/p_b))^2$*. Pour tout entier* $n \geqslant 1$*, munissons l'ensemble* A^n *de la loi produit. Soit* ε *un nombre réel* > 0 *et soit* A_ε^n *l'ensemble des* $(a_1, \ldots, a_n)$ *tels que*

$$e^{-n(H(X_1)+\varepsilon)} \leqslant \mathbf{P}(X_1 = a_1, \ldots, X_n = a_n) \leqslant e^{-n(H(X_1)-\varepsilon)}.$$

On a

$$\mathbf{P}(A_\varepsilon^n) > 1 - \frac{c}{2n\varepsilon^2},$$

et

$$(1 - \frac{c}{2n\varepsilon^2}) e^{n(H(X_1)-\varepsilon)} \leqslant \mathrm{Card}(A_\varepsilon^n) \leqslant e^{n(H(X_1)+\varepsilon)}.$$

Reformulons un peu cet énoncé : $1 - \mathbf{P}(A_\varepsilon^n)$ est la probabilité du complémentaire de A_ε^n, et est majorée par $c/2n\varepsilon^2$; lorsque n est grand, elle est arbitrairement petite. Autrement dit, lorsque n est grand, la plupart des tirages $(a_1, \ldots, a_n)$ ont une probabilité voisine de $e^{-nH(X_1)}$, et il y a environ $e^{nH(X_1)}$ tels tirages. Autrement dit encore, lorsqu'on effectue un grand nombre n de tirages, tout se passe comme si l'on avait effectué un tirage au sort équitable parmi $e^{nH(X_1)}$ valeurs — c'est l'*interprétation statistique* de l'entropie.

Démonstration. — Quitte à modifier l'univers en lui enlevant un ensemble de probabilité 0, puis l'ensemble A par l'ensemble des valeurs des X_k, on suppose que $\mathbf{P}(X_k = a) > 0$ pour tout $a \in A$ et tout $k \in \{1, \ldots, n\}$. Soit alors $\varphi : A \to \mathbf{R}$ l'application définie par $\varphi(a) = -\log(\mathbf{P}(X_1 = a))$.

Comme les X_k sont indépendantes et de même loi, on a

$$\begin{aligned}\mathbf{P}(X_1 = a_1, \ldots, X_n = a_n) &= \mathbf{P}(X_1 = a_1) \ldots \mathbf{P}(X_n = a_n) \\ &= \mathbf{P}(X_1 = a_1) \ldots \mathbf{P}(X_1 = a_n),\end{aligned}$$

soit encore

$$-\frac{1}{n} \log(\mathbf{P}(X_1 = a_1, \ldots, X_n = a_n)) = -\frac{1}{n} \sum_{k=1}^{n} \log(\mathbf{P}(X_1 = a_k)) = \frac{1}{n} \sum_{k=1}^{n} \varphi(a_k).$$

On munit l'ensemble A de la loi de X_1 ; quitte à le remplacer par l'ensemble des $a \in A$ tels que $\mathbf{P}(X_1 = a) > 0$, on suppose que $\mathbf{P}(X_1 = a) > 0$ pour tout $a \in A$. On munit alors l'ensemble A^n de la loi produit. On a $\mathbf{P}(a_1, \ldots, a_n) = \prod_{k=1}^n \mathbf{P}(X_1 = a_k)$. Sur cet espace probabilisé A^n, on pose $U_k(a_1, \ldots, a_n) = \varphi(a_k)$.

Les variables aléatoires $\mathrm{U}_1, \ldots, \mathrm{U}_n$ sont indépendantes. Elles ont même loi : pour tout $a \in \mathrm{A}$, on a

$$\mathbf{P}(\mathrm{U}_k = \varphi(a)) = \mathbf{P}(\mathrm{X}_1 = a),$$

et $\mathbf{P}(\mathrm{U}_k = t) = 0$ si $t \notin \varphi(\mathrm{A})$. Elles sont d'espérance et de variance finies car elles ne prennent qu'un nombre fini de valeurs. De plus, on a

$$\mathrm{H}(\mathrm{X}_1) = -\sum_{a \in \mathrm{A}} \mathbf{P}(\mathrm{X}_1 = a) \log(\mathbf{P}(\mathrm{X}_1) = a)) = \mathbf{E}(\mathrm{U}_1).$$

D'après l'inégalité de Bienaymé–Tchebitcheff, on a

$$\mathbf{P}\left(|\mathrm{H}(\mathrm{X}_1) - \frac{1}{n}\sum_{k=1}^{n} \mathrm{U}_k| > \varepsilon\right) < \mathrm{V}(\mathrm{U}_1)/n\varepsilon^2.$$

On a

$$\frac{1}{n}\sum_{k=1}^{n} \mathrm{U}_k(a_1, \ldots, a_n) = -\frac{1}{n}\log(\mathbf{P}(\mathrm{X}_1 = a_1, \mathrm{X}_2 = a_2, \ldots, \mathrm{X}_n = a_n)).$$

Il reste à calculer la variance $\mathrm{V}(\mathrm{U}_1)$ de U_1. Par définition, on a

$$\mathrm{V}(\mathrm{U}_1) = \mathbf{E}((\mathrm{U}_1 - \mathbf{E}(\mathrm{U}_1))^2) = \mathbf{E}(\mathrm{U}_1^2) - \mathbf{E}(\mathrm{U}_1)^2,$$

de sorte que

$$\begin{aligned}
\mathrm{V}(\mathrm{U}_1) &= \sum_{a \in \mathrm{A}} \mathbf{P}(\mathrm{X}_1 = a) \log(\mathbf{P}(\mathrm{X}_1 = a))^2 \\
&\qquad - \sum_{a,b \in \mathrm{A}} \mathbf{P}(\mathrm{X}_1 = a)\mathbf{P}(\mathrm{X}_1 = b) \log(\mathbf{P}(\mathrm{X}_1) = a) \log(\mathbf{P}(\mathrm{X}_1 = b) \\
&= \sum_{a,b \in \mathrm{A}} p_a p_b \left(\log(p_a)^2 - \log(p_a)\log(p_b)\right) \\
&= \sum_{a,b \in \mathrm{A}} p_a p_b \log(p_a)\log(p_a/p_b).
\end{aligned}$$

Par symétrie, on a aussi

$$\mathrm{V}(\mathrm{U}_1) = \sum_{a,b \in \mathrm{A}} p_a p_b \log(p_b)\log(p_b/p_a),$$

d'où, en additionant ces deux formules, l'égalité

$$2\mathrm{V}(\mathrm{U}_1) = \sum_{a,b \in \mathrm{A}} p_a p_b \log(p_b/p_a)^2 = c.$$

Cela conclut la preuve de la première inégalité.

Ensuite, en utilisant la majoration de $\mathbf{P}(X_1 = a_1, \dots, X_n = a_n)$ pour $(a_1, \dots, a_n) \in A_\varepsilon^n$,

$$1 \geqslant \mathbf{P}(A_\varepsilon^n) \geqslant \mathrm{Card}(A_\varepsilon^n) e^{-n(H(X_1)+\varepsilon)},$$

d'où la majoration donnée pour $\mathrm{Card}(A_\varepsilon^n)$. En utilisant la minoration analogue, on obtient aussi

$$1 - \frac{c}{2n\varepsilon^2} \leqslant \mathbf{P}(A_\varepsilon^n) \leqslant \mathrm{Card}(A_\varepsilon^n) e^{-n(H(X_1)-\varepsilon)},$$

ce qui donne la minoration de $\mathrm{Card}(A_\varepsilon^n)$. □

2.4.4. — Comment Shannon en déduit-il la possibilité de comprimer un signal (dans la limite permise par l'entropie) ? Fixons un paramètre ε et considérons l'« ensemble typique » A_ε^n de A^n défini dans le théorème 2.4.3. Il est de cardinal au plus $2^{n(H_2(X_1)+\varepsilon)}$; donc on numérotant ses éléments, chacun ne requiert que $\lceil n(H_2(X_1) + \varepsilon) \rceil$ bits. Les autres vont chacun requérir $\mathrm{Card}(A)^n$ symboles, soit $n \log_2(\mathrm{Card}(A))$ bits, mais n'apparaissent qu'avec une probabilité faible, majorée par $c/2n\varepsilon^2$. Ainsi, la longueur moyenne du code d'une suite de n symboles est majorée par

$$\lceil n(H_2(X_1) + \varepsilon) \rceil + \frac{c}{2n\varepsilon^2} n \log_2(\mathrm{Card}(A)).$$

Lorsqu'on la divise par n, on obtient

$$\frac{1}{n} \lceil n(H_2(X_1) + \varepsilon) \rceil + \frac{c}{2n\varepsilon^2} \log_2(\mathrm{Card}(A)),$$

quantité majorée par $H_2(X_1) + 1$ lorsque n est assez grand.

2.4.5. — L'information mutuelle, comme l'entropie, dispose d'une interprétation statistique. Soit A et B des ensembles finis, soit $C = A \times B$ l'ensemble produit et soit $Z_1 = (X_1, Y_1), \dots, Z_n = (X_n, Y_n)$ des variables aléatoires indépendantes et de même loi à valeurs dans C. Posons enfin $X = (X_1, \dots, X_n)$, $Y = (Y_1, \dots, Y_n)$ et $Z = (Z_1, \dots, Z_n) = (X, Y)$ si l'on identifie l'élément (a, b) de $A^n \times B^n$ avec l'élément $((a_1, b_1), \dots, (a_n, b_n))$ de C^n. On pose $c(Z) = \sum_{a,b \in C} \mathbf{P}(Z_1 = a)\mathbf{P}(Z_1 = b) \log(\mathbf{P}(Z_1 = a)/\mathbf{P}(Z_1 = b))^2$ et on définit $c(X)$ et $c(Y)$ de manière analogue.

Soit ε un nombre réel > 0 ; définissons une partie C_ε^n de C^n par : C_ε^n est l'ensemble des $(a, b) \in C_\varepsilon^n$ tels que

$$e^{-n(H(X_1)+\varepsilon)} \leqslant \mathbf{P}(X = a) \leqslant e^{-n(H(X_1)-\varepsilon)}$$
$$e^{-n(H(Y_1)+\varepsilon)} \leqslant \mathbf{P}(Y = b) \leqslant e^{-n(H(Y_1)-\varepsilon)}$$
$$e^{-n(H(X_1,Y_1)+\varepsilon)} \leqslant \mathbf{P}(X = a, Y = b) \leqslant e^{-n(H(X_1,Y_1)-\varepsilon)}.$$

Théorème **(2.4.6)**. — *On a*

$$\mathbf{P}(Z \in C_\varepsilon^n) \geqslant 1 - \frac{c(X) + c(Y) + c(Z)}{2n\varepsilon^2}$$

et

$$\mathrm{Card}(C_\varepsilon^n) \leqslant e^{n(H(X,Y)+\varepsilon)}.$$

Enfin, si $X'_1, \ldots, X'_n$ d'une part, $Y'_1, \ldots, Y'_n$ d'autre part, sont des variables aléatoires de mêmes lois que $X_1, \ldots, X_n$ et $Y_1, \ldots, Y_n$, mais indépendantes, alors

$$(1 - \frac{c(X) + c(Y) + c(Z)}{2n\varepsilon^2})e^{-n(I(X,Y)+3\varepsilon)} \leqslant \mathbf{P}((X', Y')) \in C_\varepsilon^n) \leqslant e^{-n(I(X,Y)-3\varepsilon)}.$$

Démonstration. — On munit l'ensemble C^n de la loi de Z. Soit $\varphi_Z : C \to \mathbf{R}_+$ la variable aléatoire définie par $\varphi_Z(c) = -\log(\mathbf{P}(Z = c))$ si $\mathbf{P}(Z = c) > 0$, et $\varphi_Z(c) = 0$ sinon. Définissons $\varphi_X : A \to \mathbf{R}_+$ et $\varphi_Y : B \to \mathbf{R}_+$ de façon analogue. Comme dans la démonstration du théorème ..., on prouve que

$$\mathbf{P}(\complement C_\varepsilon^n) < \frac{c(X)}{2n\varepsilon^2} + \frac{c(Y)}{2n\varepsilon^2} + \frac{c(Z)}{2n\varepsilon^2},$$

d'où la minoration voulue pour $\mathbf{P}(C_\varepsilon^n)$. On prouve aussi, par le même argument que

$$\left(1 - \frac{c(X) + c(Y) + c(Z)}{2n\varepsilon^2}\right) e^{n(H(X_1,Y_1)-\varepsilon)} \leqslant \mathrm{Card}(C_\varepsilon^n) \leqslant e^{n(H(X_1,Y_1)+\varepsilon)}.$$

Considérons alors des variables aléatoires X', Y', indépendantes et de mêmes lois que X, Y, et posons $Z' = (X', Y')$. On a

$$\begin{aligned}\mathbf{P}(Z' \in C_\varepsilon^n) &= \sum_{(a,b)\in C_\varepsilon^n} \mathbf{P}(Z' = (a, b)) \\ &= \sum_{(a,b)\in C_\varepsilon^n} \mathbf{P}(X' = a)\mathbf{P}(Y' = b) \\ &= \sum_{(a,b)\in C_\varepsilon^n} \mathbf{P}(X = a)\mathbf{P}(Y = b).\end{aligned}$$

Par définition de C_ε^n et la majoration de $\mathrm{Card}(\mathrm{C}_\varepsilon^n)$, on a donc

$$\begin{aligned}\mathbf{P}(\mathrm{Z}' \in \mathrm{C}_\varepsilon^n) &\leqslant \mathrm{Card}(\mathrm{C}_\varepsilon^n) e^{-n(\mathrm{H}(\mathrm{X}_1)-\varepsilon)} e^{-n(\mathrm{H}(\mathrm{Y}_1)-\varepsilon)} \\ &\leqslant e^{-n(\mathrm{H}(\mathrm{X}_1)+\mathrm{H}(\mathrm{Y}_1)-\mathrm{H}(\mathrm{X}_1,\mathrm{Y}_1)-3\varepsilon)} \\ &= e^{-n(\mathrm{I}(\mathrm{X}_1,\mathrm{Y}_1)-3\varepsilon)}.\end{aligned}$$

La preuve de la minoration est analogue :

$$\begin{aligned}\mathbf{P}(\mathrm{Z}' \in \mathrm{C}_\varepsilon^n) &\geqslant \mathrm{Card}(\mathrm{C}_\varepsilon^n) e^{-n(\mathrm{H}(\mathrm{X}_1)+\varepsilon)} e^{-n(\mathrm{H}(\mathrm{Y}_1)+\varepsilon)} \\ &\geqslant \left(1 - \frac{c(\mathrm{X}) + c(\mathrm{Y}) + c(\mathrm{Z})}{2n\varepsilon^2}\right) e^{-n(\mathrm{H}(\mathrm{X}_1)+\mathrm{H}(\mathrm{Y}_1)-\mathrm{H}(\mathrm{X}_1,\mathrm{Y}_1)+3\varepsilon)} \\ &= \left(1 - \frac{c(\mathrm{X}) + c(\mathrm{Y}) + c(\mathrm{Z})}{2n\varepsilon^2}\right) e^{-n(\mathrm{I}(\mathrm{X}_1,\mathrm{Y}_1)+3\varepsilon)}.\end{aligned}$$

Ceci conclut la preuve du théorème. □

2.5. Capacité de transmission d'un canal

Les deux thèmes étudiés jusqu'à présent — entropie d'une variable aléatoire et codage — concernaient uniquement les deux premières étapes du diagramme de communication présenté dans l'introduction. Nous allons maintenant faire intervenir la troisième : le canal de transmission et, en particulier, le problème du *bruit* à cause duquel un symbole reçu ne coïncide pas forcément avec le symbole émis.

Définition **(2.5.1)**. — *Soit* A *et* B *des alphabets. Un* canal de transmission sans mémoire *de l'alphabet* A *à l'alphabet* B *est donné par une famille* $(p(\cdot \mid a))$ *de lois de probabilités sur* B*, indexée par l'ensemble* A*.*

Pour $a \in \mathrm{A}$ et $b \in \mathrm{B}$, $p(b \mid a)$ est la probabilité que le canal transmette le symbole b sachant que le symbole émis était a. La matrice $(p(b \mid a))$ de type $\mathrm{A} \times \mathrm{B}$ est la *matrice de probabilités de transmission* du canal : ses lignes, indexées par les éléments a de A, sont les lois $p(\cdot \mid a)$. En particulier, les coefficients de cette matrice sont positifs ou nuls et la somme des coefficients de chaque ligne est égale à 1.

Le fait que le canal soit *sans mémoire* signifie que, pour ce modèle de bruit, la transmission des symboles d'un mot $(a_1, \ldots, a_n)$ est faite symbole par symbole,

de façon certes aléatoire, mais indépendante. Autrement dit, la probabilité que le mot $(a_1, \dots, a_n)$ soit transmis en $(b_1, \dots, b_n)$ est donnée par

$$\mathbf{P}(\mathrm{Y} = b_1 \dots b_n \mid \mathrm{X} = a_1 \dots a_n) = p(b_1 \mid a_1) \dots p(b_n \mid a_n).$$

Définition **(2.5.2)**. — *Soit* C *un canal de matrice de probabilités de transmission* $(p(b \mid a))$. *On appelle* capacité de transmission *de ce canal l'expression*

$$\mathrm{I}(\mathrm{C}) = \sup \mathrm{I}(\mathrm{X}, \mathrm{Y})$$

où X *parcourt l'ensemble des variables aléatoires sur* A *et* Y *parcourt l'ensemble des variables aléatoires sur* B *telles que* $\mathbf{P}(\mathrm{Y} = b \mid \mathrm{X} = a) = p(b \mid a)$ *pour tout* $a \in \mathrm{A}$ *et tout* $b \in \mathrm{B}$.

Dans la suite, on notera $\mathrm{X} \sim_{\mathrm{C}} \mathrm{Y}$ pour signifier que X et Y sont des variables aléatoires telles que $\mathbf{P}(\mathrm{Y} = b \mid \mathrm{X} = a) = p(b \mid a)$ pour tout $a \in \mathrm{A}$ et tout $b \in \mathrm{B}$.

Rappelons que l'on a

$$\mathrm{I}(\mathrm{X}, \mathrm{Y}) = \mathrm{H}(\mathrm{X}) + \mathrm{H}(\mathrm{Y}) - \mathrm{H}(\mathrm{X}, \mathrm{Y}) = \mathrm{H}(\mathrm{Y}) - \mathrm{H}(\mathrm{Y} \mid \mathrm{X}) = \mathrm{H}(\mathrm{X}) - \mathrm{H}(\mathrm{X} \mid \mathrm{Y}).$$

Pour tout couple (X, Y), on a $0 \leqslant \mathrm{I}(\mathrm{X}, \mathrm{Y}) \leqslant \max(\log(\mathrm{Card}(\mathrm{A})), \log(\mathrm{Card}(\mathrm{B})))$, de sorte que

$$0 \leqslant \mathrm{I}(\mathrm{C}) \leqslant \max(\log(\mathrm{Card}(\mathrm{A})), \log(\mathrm{Card}(\mathrm{B}))).$$

Expliquons tout d'abord cette définition en reprenant, comme Shannon (1948, §12), le cas où il n'y a que deux symboles 0 et 1 à transmettre « *à un débit de 1000 symboles par seconde avec les probabilités* $p_0 = p_1 = 1/2$. *Ainsi,* continue Shannon, *notre source produit de l'information avec un débit de 1000 bits par seconde. Lors de la transmission, le bruit introduit des erreurs, de sorte que, en moyenne, un symbole sur 100 est reçu incorrectement(0 pour 1, ou 1 pour 0). Quel est le débit d'information transmis? Certainement moins de 1000 bits par seconde puisque 1% environ des symboles reçus sont incorrects. Notre première réaction pourrait être de dire que ce débit est de 990 bits par seconde, par simple soustraction du nombre d'erreurs prévues. Cela n'est pas satisfaisant, puisqu'on ne tient pas compte du fait que le destinataire ne sait pas où se trouvent les erreurs. Prenons le cas extrême où le bruit est si grand que les symboles reçus sont entièrement indépendants des symboles transmis. La probabilité de recevoir 1 est* $1/2$ *quel que soit ce qui est transmis, et de même pour 0. Alors, environ la moitié des symboles reçus sont corrects, du seul fait du hasard, et on pourrait de la même façon dire que le système transmet 500 bits par seconde, alors qu'aucune information n'est transmise en réalité.* »

Shannon continue : « *La correction adéquate à appliquer à la quantité d'information transmise est évidemment la quantité de cette information qui est manquante dans le signal reçu, ou, ce qui revient au même, l'incertitude lors de la réception du signal sur ce qui a été réellement émis. Vu notre discussion antérieure, il semble raisonnable d'utiliser l'entropie conditionnelle du message connaissant le signal reçu comme mesure de cette information manquante.* »

C'est ce que dit la troisième égalité dans la formule précédente : on obtient l'information mutuelle $\mathrm{I}(\mathrm{X}, \mathrm{Y})$ en partant de la quantité d'information dans le message envoyé X, mesurée par son entropie $\mathrm{H}(\mathrm{X})$, et en lui soustrayant l'incertitude $\mathrm{H}(\mathrm{X} \mid \mathrm{Y})$ que mesure l'entropie de X conditionnellement à Y. La seconde égalité présente cette quantité comme la quantité d'information $\mathrm{H}(\mathrm{Y})$ du message reçu minorée du bruit que mesure l'entropie conditionnelle $\mathrm{H}(\mathrm{Y} \mid \mathrm{X})$.

Le fait de prendre la borne supérieure sur toutes les lois possibles sur les symboles X reflète la possibilité pour l'émetteur d'*adapter* la façon dont il écrit le message pour tenir compte des problèmes du canal. Par exemple, si tous les symboles étaient envoyés sans erreur, sauf un qui était systématiquement corrompu, il serait malin d'utiliser un codage qui permette de ne jamais l'utiliser.

Continuons avec quelques exemples de capacité de transmission.

Exemple **(2.5.3)**. — a) Prenons pour alphabets $\mathrm{A} = \mathrm{B} = \{0, 1\}$; soit p un élément de $[0; 1]$. Le canal avec bruit de paramètre p transmet le mauvais symbole avec probabilité p. Lorsque $p = 0$, ce canal retransmet exactement le symbol émis : on parle de canal *sans bruit.* Lorsque $p = 1/2$, ce canal envoie chaque symbole avec probabilité $1/2$, indépendamment du symbole émis ; on comprend bien, et on verra, qu'un tel canal n'est pas très utile.

Sa matrice de probabilités de transmission est donc

$$\begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}.$$

Soit X et Y des variables aléatoires sur A et B respectivement telles que $\mathrm{X} \sim_{\mathrm{C}} \mathrm{Y}$, c'est-à-dire, $\mathbf{P}(\mathrm{Y} = b \mid \mathrm{X} = a) = p(b \mid a)$ pour $a \in \mathrm{A}$ et $b \in \mathrm{B}$. Notons $u = \mathbf{P}(\mathrm{X} = 0)$; on a donc $\mathbf{P}(\mathrm{X} = 1) = 1 - u$, puis

$$\begin{aligned} \mathrm{H}(\mathrm{Y} \mid \mathrm{X}) &= u\mathrm{H}(\mathrm{Y} \mid \mathrm{X} = 0) + (1-u)\mathrm{H}(\mathrm{Y} \mid \mathrm{X} = 1) \\ &= uh(p) + (1-u)h(1-p) = h(p). \end{aligned}$$

D'autre part, Y étant une variable aléatoire binaire, on a $\mathrm{H}(\mathrm{Y}) \leqslant \log(2)$. Par suite,

$$\mathrm{I}(\mathrm{X},\mathrm{Y}) \leqslant \log(2) - h(p).$$

Lorsque X suit une loi uniforme ($u = 1/2$), il en est de même de la loi Y — on peut le justifier par symétrie des probabilités, ou bien faire le calcul. Cela montre que la capacité de ce canal est $\log(2) - h(p)$. À ce stade, il est vraiment plus pratique de fixer à 2 la base des logarithmes, ce qui mesure les entropies en *bits*. Alors, la capacité du canal symétrique à bruit est $1 - h(p)$.

Lorsque $p = 0$, la capacité de ce canal est 1 ; lorsque $p = 1/2$, elle est nulle. Lorsque $p = 1$, on trouve encore $\mathrm{I}(\mathrm{C}) = 1$: ce canal modifie *systématiquement* le symbole reçu — il n'y a en fait pas de perte d'information !

b) Une variante du canal précédent utilise l'alphabet $\mathrm{A} = \{0, 1\}$ mais a pour but l'alphabet $\mathrm{B} = \{0, 1, e\}$, où e est un symbole auxiliaire indiquant une erreur de transmission, commise avec probabilité q, tandis que la probabilité de transmettre un symbole erroné est $(1 - q)p$. On a $p(1 \mid 0) = p(0 \mid 0) = (1 - q)q$ et $p(e \mid 1) = p(e \mid 0) = q$. La matrice de probabilités de transmission de ce canal est

$$\begin{pmatrix} (1-q)(1-p) & (1-q)p & q \\ (1-q)p & (1-q)(1-p) & q \end{pmatrix}.$$

Notons encore $\mathbf{P}(\mathrm{X} = 0) = u$. Alors, en posant $t = u(1 - p) + (1 - u)p$, on a

$$\begin{aligned} \mathbf{P}(\mathrm{Y} = 0) &= u(1-q)(1-p) + (1-u)(1-q)p = (1-q)t, \\ \mathbf{P}(\mathrm{Y} = 1) &= (1-u)(1-q)(1-p) + u(1-q)p = (1-q)(1-t) \\ \mathbf{P}(\mathrm{Y} = e) &= q. \end{aligned}$$

Soit E la variable aléatoire qui vaut 1 si $\mathrm{Y} = e$ et 0 sinon. Puisque E est conséquence de Y, on a $\mathrm{H}(\mathrm{Y}) = \mathrm{H}(\mathrm{Y}, \mathrm{E})$; alors,

$$\mathrm{H}(\mathrm{Y}) = \mathrm{H}(\mathrm{Y}, \mathrm{E}) = \mathrm{H}(\mathrm{E}) + \mathrm{H}(\mathrm{Y} \mid \mathrm{E}).$$

D'autre part, $\mathbf{P}(\mathrm{E} = 1) = q$ et $\mathbf{P}(\mathrm{E} = 0) = 1 - q$, de sorte que $\mathrm{H}(\mathrm{E}) = h(q)$. De plus, conditionnée à l'évènement $\mathrm{Y} = e$, la variable aléatoire Y est certaine, donc d'entropie nulle ; conditionnée à l'évènement complémentaire, elle a pour loi une loi de Bernoulli de paramètre t, de sorte que

$$\mathrm{H}(\mathrm{Y} \mid \mathrm{E}) = q\mathrm{H}(\mathrm{Y} \mid \mathrm{Y} = e) + (1-q)\mathrm{H}(\mathrm{Y} \mid \mathrm{Y} \neq e) = (1-q)h(t),$$

de sorte que

$$\mathrm{H}(\mathrm{Y}) = h(q) + (1-q)h(t).$$

On applique un argument similaire pour le terme $\mathrm{H}(\mathrm{Y} \mid \mathrm{X})$. On a tout d'abord

$$\mathrm{H}(\mathrm{Y} \mid \mathrm{X}) = \mathrm{H}(\mathrm{Y}, \mathrm{E} \mid \mathrm{X}) = \mathrm{H}(\mathrm{E} \mid \mathrm{X}) + \mathrm{H}(\mathrm{Y} \mid \mathrm{E}, \mathrm{X}).$$

Le premier terme est de nouveau égal à $h(q)$. Conditionnée à l'évènement $\mathrm{Y} = e$, de probabilité q, la variable aléatoire Y est certaine ; conditionnée à l'évènement $(\mathrm{E} = 0) \cap (\mathrm{X} = 0)$, de probabilité $(1-q)u$, elle se comporte comme une loi de Bernoulli de paramètre p, de même que conditionnée à l'événément $(\mathrm{E} = 0) \cap (\mathrm{X} = 1)$ qui est de probabilité $(1-q)(1-u)$. Ainsi,

$$\begin{aligned}\mathrm{H}(\mathrm{Y} \mid \mathrm{E}, \mathrm{X}) &= q\mathrm{H}(\mathrm{Y} \mid \mathrm{E} = 1) + (1-q)u\mathrm{H}(\mathrm{Y} \mid \mathrm{E} = 0, \mathrm{X} = 0) \\ &\qquad + (1-q)(1-u)\mathrm{H}(\mathrm{Y} \mid \mathrm{E} = 0, \mathrm{X} = 1) \\ &= q \cdot 0 + (1-q)u \cdot h(p) + (1-q)(1-u) \cdot h(p) \\ &= (1-q)h(p).\end{aligned}$$

On a donc

$$\mathrm{H}(\mathrm{Y} \mid \mathrm{X}) = h(q) + (1-q)h(p).$$

Finalement,

$$\mathrm{I}(\mathrm{X}, \mathrm{Y}) = (1-q)(h(t) - h(p)).$$

Cette expression est maximale lorsque $h(t)$ est maximale. Lorsque la base des logarithmes est 2, on a $h(t) \leqslant 1$, de sorte que $\mathrm{I}(\mathrm{X}, \mathrm{Y}) \leqslant (1-q)(1-h(p))$. On a aussi $h(t) = 1$ pour $t = 1/2$. Or, rappelons que $t = u(1-p) + (1-u)p$; on constate que pour $u = 1/2$, on a également $t = 1/2$, d'où

$$\mathrm{I}(\mathrm{C}) = (1-q)(1-h(p)) \text{ bits.}$$

(Si on n'avait pas su faire cette constatation, il restait à calculer u en fonction de t : on trouve $u = (t-p)/(1-2p) = 1/2$ si $t = 1/2$.)

c) Un canal est dit *faiblement symétrique* si les lignes de sa matrice de probabilités de transmission diffèrent uniquement l'une de l'autre par des permutations et si la somme des coefficients de chaque colonne est constante. On parle de canal *symétrique* si, de plus, les colonnes de sa matrice de probabilités de transmission diffèrent par permutations l'une de l'autre ; c'est le cas du canal avec bruit de l'exemple *a*). Une façon d'obtenir un canal symétrique consiste à prendre pour alphabets $\mathrm{A} = \mathrm{B} = \mathbf{Z}/d\mathbf{Z}$ et à poser $p(b \mid a) = q(b-a)$, où q est une loi de probabilité sur A. On peut bien sûr remplacer $\mathbf{Z}/d\mathbf{Z}$ par un groupe fini arbitraire. En revanche, sauf si $p = 1/3$, le canal de l'exemple *b*) n'est pas faiblement symétrique.

Soit C un canal faiblement symétrique et soit X, Y des variables aléatoires sur A, B respectivement, liées par la condition $\mathbf{P}(\mathrm{Y} = b \mid \mathrm{X} = a) = p(b \mid a)$. Pour tout $a \in \mathrm{A}$, on a

$$\mathrm{H}(\mathrm{Y} \mid \mathrm{X} = a) = -\sum_b p(b \mid a) \log(p(b \mid a)),$$

et cette expression est indépendante de a par la condition de symétrie des lignes de la matrice de probabilités de transmission du canal. D'autre part,

$$\mathrm{H}(\mathrm{Y}) \leqslant \log(\mathrm{Card}(\mathrm{B})).$$

Lorsque la loi de X est uniforme, la condition sur la somme des coefficients de chaque colonne entraîne que la loi de Y est également uniforme : pour tout $b \in \mathrm{B}$, on a en effet

$$\mathbf{P}(\mathrm{Y} = b) = \sum_{a \in \mathrm{A}} \mathbf{P}(\mathrm{Y} = b \mid \mathrm{X} = a)\mathbf{P}(\mathrm{X} = a) = \frac{1}{\mathrm{Card}(\mathrm{A})} \sum_{a \in \mathrm{A}} p(b \mid a),$$

expression indépendante de b. Dans ce cas, on a donc $\mathrm{H}(\mathrm{Y}) = \log(\mathrm{Card}(\mathrm{B}))$.

Puique $\mathrm{I}(\mathrm{X}, \mathrm{Y}) = \mathrm{H}(\mathrm{Y}) - \mathrm{H}(\mathrm{Y} \mid \mathrm{X})$, ce qui précède entraîne ainsi la formule

$$\mathrm{I}(\mathrm{C}) = \log(\mathrm{Card}(\mathrm{B})) - \mathrm{H}(\mathrm{Y} \mid \mathrm{X} = a),$$

où a est un élément quelconque de A.

d) Considérons un canal C d'un alphabet A à un alphabet B, soit n un entier $\geqslant 2$ et définissons un canal C^n de l'alphabet A^n à l'alphabet B^n de probabilités de transmission d'un canal sans mémoire : $p(b \mid a) = \prod_{i=1}^n p(b_i \mid a_i)$, pour $a = (a_1, \ldots, a_n) \in \mathrm{A}^n$ et $b = (b_1, \ldots, b_n) \in \mathrm{B}^n$. Démontrons que $\mathrm{I}(\mathrm{C}^n) = n\mathrm{I}(\mathrm{C})$.

Soit $\mathrm{X} = (\mathrm{X}_1, \ldots, \mathrm{X}_n)$ et $\mathrm{Y} = (\mathrm{Y}_1, \ldots, \mathrm{Y}_n)$ des variables aléatoires à valeurs dans A^n et B^n respectivement vérifiant $\mathbf{P}(\mathrm{Y} = b \mid \mathrm{X} = a) = p(b \mid a)$ pour $a \in \mathrm{A}^n$ et $b \in \mathrm{B}^n$. On a

$$\mathrm{I}(\mathrm{X}, \mathrm{Y}) = \mathrm{H}(\mathrm{Y}) - \mathrm{H}(\mathrm{Y} \mid \mathrm{X}).$$

Le premier terme se calcule par récurrence :

$$\begin{aligned} \mathrm{H}(\mathrm{Y}) &= \mathrm{H}(\mathrm{Y}_1) + \mathrm{H}(\mathrm{Y}_2 \mid \mathrm{Y}_1) + \cdots + \mathrm{H}(\mathrm{Y}_n \mid \mathrm{Y}_1, \ldots, \mathrm{Y}_{n-1}) \\ &\leqslant \mathrm{H}(\mathrm{Y}_1) + \mathrm{H}(\mathrm{Y}_2) + \cdots + \mathrm{H}(\mathrm{Y}_n), \end{aligned}$$

puisque l'entropie diminue par conditionnement ; on a même égalité lorsque les X_i sont indépendantes. Encore par récurrence, on a

$$\mathrm{H}(\mathrm{Y} \mid \mathrm{X}) = \mathrm{H}(\mathrm{Y}_1 \mid \mathrm{X}) + \mathrm{H}(\mathrm{Y}_2 \mid \mathrm{Y}_1, \mathrm{X}) + \cdots + \mathrm{H}(\mathrm{Y}_n \mid \mathrm{Y}_1, \ldots, \mathrm{Y}_{n-1}, \mathrm{X}).$$

Soit $p \in \{1, \dots, n\}$. Par définition du canal C^n, la variable aléatoire Y_p est indépendante des Y_i et des X_i (pour $i \neq p$) conditionnellement à X_p ; ainsi,

$$H(Y_p \mid Y_1, \dots, Y_{p-1}, X) = H(Y_p \mid X_p).$$

Ainsi, on a

$$I(X, Y) \leqslant \sum_{p=1}^{n} H(Y_p) - \sum_{p=1}^{n} H(Y_p \mid X_p) = \sum_{p=1}^{n} I(X_p, Y_p),$$

avec égalité si les X_p sont indépendantes.

On obtient donc d'une part l'inégalité $I(X, Y) \leqslant nI(C)$, d'où $I(C^n) \leqslant nI(C)$. D'autre part, si les X_p sont indépendantes et vérifient $I(X_p, Y_p) = I(C)$, on obtient $I(X, Y) = nI(C)$. Finalement, $I(C^n) = nI(C)$.

2.6. Codage adapté à un canal avec bruit

2.6.1. — À moins qu'il ne soit en fait *sans* bruit, il n'est pas possible de transmettre, dans un canal avec bruit, un message avec certitude. Le théorème de Shannon (1948) que nous allons maintenant démontrer affirme que c'est toutefois possible de le transmettre de sorte que la probabilité d'erreur soit aussi petite que désirée, et que la vitesse de transmission n'est alors limitée que par la capacité du canal sans mémoire.

Considérons un canal de transmission C d'un alphabet A à un alphabet B ; pour fixer les idées, on peut imaginer que $A = B = \{0; 1\}$ et que C est le canal binaire avec bruit qui transmet le bon symbole avec une probabilité p. Les messages qu'on veut envoyer (un texte, une vidéo, un fichier de musique…) ont leur structure naturelle, ce sont par exemples de fichiers au format *Markdown*, *H.264*, *Flac*…) et le système de transmission n'en dépendra essentiellement pas.

Pour cela, la source est disposée à sectionner son fichier en blocs d'une taille appropriée ; chaque bloc sera *codé* en un mot dans l'alphabet A, lequel est transmis dans le canal. Le mot reçu est *décodé* par le récepteur et le destinataire reconstruit un fichier bloc par bloc. Comme on le verra, l'efficacité du système reposera sur le fait que l'on s'autorise à transmettre au canal des mots d'une longueur n assez grande.

Définition **(2.6.2)**. — *Soit* C *un canal de transmission d'un alphabet* A *à un alphabet* B. *Soit* M *un ensemble fini ; un code* Φ *de longueur* n *sur* M *pour le canal* C *est la donnée de deux applications* $f_\Phi : M \to A^n$ *et* $g_\Phi : B^n \to M$.

Reprenons : l'émetteur code son fichier en une suite de mots de longueur n dans l'alphabet A qui sont envoyés dans le canal ; ces mots sont de la forme $\alpha = f_\Phi(m)$, où m est un « bloc » ; le récepteur reçoit un mot β de longueur n dans l'alphabet B qu'il décode au moyen de la fonction g_Φ pour reconstruire un bloc $g_\Phi(\beta)$. Si tout s'est bien passé, on a $g_\Phi(\beta) = m$; sinon, il y a eu une erreur de transmission et le but sera d'en limiter la probabilité.

L'ensemble M qui est sous-jacent à cette description n'a aucune importance : il n'intervient que par les applications f_Φ et g_Φ, et n'importe quel ensemble de même cardinal pourrait convenir.

Le *taux de transmission* d'un tel code est le quotient

$$\tau(\Phi) = \frac{\log(\mathrm{Card}(\mathrm{M}))}{n}.$$

C'est la quantité d'information que ce système prétend transmettre, rapportée au nombre de symboles utilisés.

La probabilité d'erreur lorsqu'on transmet un bloc $m \in \mathrm{M}$ est donnée par

$$\lambda_m(\Phi) = \mathbf{P}(g_\Phi(\mathrm{Y}) \neq m \mid \mathrm{X} = f_\Phi(m)),$$

où X et Y sont des variables aléatoires à valeurs dans A^n et B^n liées par les probabilités de transmission définies par le canal C. Comme il s'agit d'un canal sans mémoire, on a, si $f_\Phi(m) = a_1 \dots a_n$,

$$\lambda_m(\Phi) = \sum_{\substack{b \in \mathrm{B}^n \\ g_\Phi(b) \neq m}} \mathbf{P}(\mathrm{Y} = b \mid \mathrm{X} = f_\Phi(m)) = \sum_{\substack{b=(b_1,\dots,b_n) \in \mathrm{B}^n \\ g_\Phi(b) \neq m}} \prod_{i=1}^{n} p(b_i \mid a_i).$$

Cela montre que ces probabilités d'erreur ne dépendent que des probabilités de transmission du canal C et pas du choix de variables aléatoires X et Y adaptées au canal.

On définit aussi la probabilité d'erreur *maximale* :

$$\lambda_{\max}(\Phi) = \sup_{m \in \mathrm{M}} \lambda_m(\Phi)$$

et la probabilité d'erreur *moyenne* :

$$\lambda_{\mathrm{moy}}(\Phi) = \frac{1}{\mathrm{Card}(\mathrm{M})} \sum_{m \in \mathrm{M}} \lambda_m(\Phi).$$

Définition **(2.6.3)**. — *Soit* C *un canal de transmission d'un alphabet* A *à un alphabet* B. *On dit qu'un nombre réel* ρ *est un taux de transmission* atteignable *par*

le canal C *s'il existe, pour tout nombre réel* $\varepsilon > 0$ *et tout entier* n *assez grand, un ensemble fini* M *et un code* Φ *de longueur* n *sur* M *de taux de transmission* $\geqslant \rho$ *et de probabilité d'erreur maximale* $\leqslant \varepsilon$.

Le théorème de Shannon (1948) fait le lien entre la capacité de de transmission d'un canal avec bruit, au sens de la définition 2.5.2 et la possibilité de transmettre des messages dans ce canal avec une erreur aussi petite que voulue.

Théorème **(2.6.4)** (Shannon). — *Soit* C *un canal de transmission d'un alphabet* A *à un alphabet* B. *Tout taux de transmission atteignable par le canal* C *est inférieur ou égal à* $\mathrm{I}(\mathrm{C})$ *; inversement, tout nombre réel* $\rho < \mathrm{I}(\mathrm{C})$ *est un taux de transmission atteignable par le canal* C.

Proposition **(2.6.5)** (Inégalité de Fano). — *Soit* X, Z *des variables aléatoires discrètes à valeurs dans un ensemble fini* A. *Posons* $\varepsilon = \mathbf{P}(\mathrm{X} \neq \mathrm{Z})$ *; alors,*

$$\mathrm{H}(\mathrm{X} \mid \mathrm{Z}) \leqslant h(\varepsilon) + \varepsilon \log(\mathrm{Card}(\mathrm{A}) - 1).$$

Démonstration. — Soit U la variable aléatoire qui vaut 1 si $\mathrm{Z} = \mathrm{X}$ et 0 sinon. Par conditionnement par rapport à X, on a

$$\mathrm{H}(\mathrm{X} \mid \mathrm{Z}) = \mathrm{H}(\mathrm{X}, \mathrm{U} \mid \mathrm{Z}) - \mathrm{H}(\mathrm{U} \mid \mathrm{X}, \mathrm{Z}).$$

Comme U est certaine conditionnée à (X, Z), on a $\mathrm{H}(\mathrm{U} \mid \mathrm{X}, \mathrm{Z}) = 0$, de sorte que

$$\mathrm{H}(\mathrm{X} \mid \mathrm{Z}) = \mathrm{H}(\mathrm{X}, \mathrm{U} \mid \mathrm{Z}).$$

Par conditionnement par rapport à U, on a également

$$\mathrm{H}(\mathrm{X}, \mathrm{U} \mid \mathrm{Z}) = \mathrm{H}(\mathrm{U} \mid \mathrm{Z}) + \mathrm{H}(\mathrm{X} \mid \mathrm{U}, \mathrm{Z}).$$

L'entropie décroit par conditionnement, donc

$$\mathrm{H}(\mathrm{U} \mid \mathrm{Z}) \leqslant \mathrm{H}(\mathrm{U}) = h(\varepsilon),$$

puisque U suit une loi de Bernoulli de paramètre ε. Par définition de l'entropie conditionnelle, on a aussi

$$\mathrm{H}(\mathrm{X} \mid \mathrm{U}, \mathrm{Z}) = (1 - \varepsilon)\mathrm{H}(\mathrm{X} \mid \mathrm{Z}, \mathrm{U} = 1) + \varepsilon \mathrm{H}(\mathrm{X} \mid \mathrm{Z}, \mathrm{U} = 0).$$

Le premier terme est nul, car si $\mathrm{U} = 1$, $\mathrm{X} = \mathrm{Z}$ est certaine conditionnellement à Z. Dans le second terme, le facteur $\mathrm{H}(\mathrm{X} \mid \mathrm{Z}, \mathrm{U} = 0)$ est majoré par l'entropie d'une variable aléatoire à valeurs dans A, donc est au plus égal à l'entropie $\log(\mathrm{Card}(\mathrm{A}))$ d'une loi uniforme sur A. En fait, conditionné à l'évènement $\mathrm{U} = 0$, c'est-à-dire

$X \neq Z$, cette variable aléatoire évite une valeur, donc son entropie est majorée par $\log(\mathrm{Card}(A) - 1)$. Reprenant ces in·égalités, on a donc

$$H(X \mid Z) = H(X, U \mid Z) = H(U \mid Z) + H(X \mid U, Z) \leqslant h(\varepsilon) + \varepsilon \log(\mathrm{Card}(A) - 1),$$

d'où la proposition. □

2.6.6. — Commençons par démontrer que tout taux de transmission atteignable est $\leqslant I(C)$.

Soit donc Φ un code de longueur n sur un ensemble M pour le canal C ; soit f et g les applications de codage et de décodage. Soit W une variable aléatoire à valeurs dans M, de loi uniforme ; son entropie est $\log(\mathrm{Card}(M))$. Alors $X = f(W)$ est une variable aléatoire à valeurs dans A^n, transmise par le canal, et le mot Y reçu à l'autre extrémité du canal est une variable aléatoire à valeurs dans B^n. Le symbole décodé est alors $W' = g(Y)$, qu'il faut comparer à W. Posons $\varepsilon = \mathbf{P}(W \neq W')$. La variable aléatoire W est uniforme dans l'ensemble M, donc $H(W) = \log(\mathrm{Card}(M))$. L'inégalité de Fano appliquée aux variables W, W' entraîne aussi $H(W \mid W') \leqslant h(\varepsilon) + \varepsilon \log(\mathrm{Card}(M))$. En écrivant l'égalité

$$H(W) = H(W \mid W') + I(W, W'),$$

on obtient donc

$$\log(\mathrm{Card}(M)) \leqslant h(\varepsilon) + \varepsilon \log(\mathrm{Card}(M)) + I(W, W'),$$

d'où

$$(1 - \varepsilon) \log(\mathrm{Card}(M)) \leqslant h(\varepsilon) + I(W, W').$$

Dans la chaîne de variables aléatoires $W \to X \to Y \to W'$, les variables aléatoires W et Y sont conditionnellement indépendantes relativement à X (le canal ne connaît pas le mot W d'où est issu X), et W et W' sont conditionnellement indépendantes relativement à Y (car W' est certaine conditionnellement à Y). D'après le théorème 1.3.11, on a donc

$$I(W, W') \leqslant I(W, Y) = I(Y, W) \leqslant I(Y, X) = I(X, Y).$$

La transmission de X en Y correspond au canal répété C^n de l'exemple 2.5.3, *d*), dont la capacité de transmission est $I(C^n) = nI(C)$; on a donc $I(X, Y) \leqslant nI(C)$. Par suite, on a l'inégalité $I(W, W') \leqslant nI(C)$.

On a donc

$$(1 - \varepsilon) \log(\mathrm{Card}(M)) \leqslant h(\varepsilon) + nI(C),$$

d'où l'inégalité

$$\tau(\Phi) = \frac{\log(\mathrm{Card}(\mathrm{M}))}{n} \leqslant \frac{\mathrm{I}(\mathrm{C}) + h(\varepsilon)/n}{1-\varepsilon}.$$

Appliquons cette inégalité à des codes de longueur arbitrairement grande (n tend vers $+\infty$) et dont la probabilité d'erreur est arbitrairement petite (ε tend vers 0, donc $h(\varepsilon)$ tend vers 0); le membre de droite de l'inégalité précédente tend vers $\mathrm{I}(\mathrm{C})$, donc a limite supérieure des taux de transmission $\tau(\Phi)$ sera au plus égale à $\mathrm{I}(\mathrm{C})$.

Cela prouve que tout taux de transmission atteignable par le canal C est inférieur ou égal à $\mathrm{I}(\mathrm{C})$.
(1)

2.6.7. — Démontrons maintenant la partie « positive » du théorème de Shannon, c'est-à-dire que tout nombre réel ρ tel que $\rho < \mathrm{I}(\mathrm{C})$ est atteignable. On fixe un entier $n \geqslant 1$ et un nombre réel $\alpha > 0$. Il s'agit de prouver qu'il existe, pourvu que n soit assez grand, un code de longueur n sur un ensemble M_Φ de cardinal $\lceil \exp(n\rho) \rceil$ qui est adapté au canal C dont la probabilité maximale d'erreur est au plus α. On va commencer par prouver qu'il existe un tel code dont la probabilité moyenne d'erreur est petite, on verra ensuite comment en déduire un code de même longueur et probabilité maximale d'erreur au plus double, et de taux de transmission un peu plus faible.

La méthode suivie par Shannon (1948), et peu modifiée depuis, consiste, non pas à construire explicitement un code adapté au canal C, mais à évaluer l'espérance de la probabilité d'erreur lorsque le code Φ est choisi *aléatoirement*. Comme cette espérance sera petite, l'un au moins des codes considérés aura une probabilité d'erreur petite.

Précisons : n sera un entier assez grand, M sera un ensemble non précisé de cardinal $\lceil e^{n\rho} \rceil$, et ce qui est aléatoire c'est la fonction de codage $f_\Phi : \mathrm{M} \to \mathrm{A}^n$, choisie parmi les applications de M dans A^n. Ainsi, pour tout $m \in \mathrm{M}$, $f_\Phi(m)$ est une variable aléatoire sur A^n ; on suppose que ces variables aléatoires sont indépendantes et ont toutes pour loi la loi π sur A^n, produit d'une loi sur A qui réalise la capacité du canal C. (Rappelons que $\mathrm{I}(\mathrm{C})$ est la borne supérieure, pour toutes les lois sur A, de l'information mutuelle $\mathrm{I}(\mathrm{X}, \mathrm{Y})$, où X et Y sont des

(1) Ajouter une remarque ou une preuve de la réciproque forte : si le taux de transmission du code est strictement supérieure à la capacité du canal, la probabilité d'erreur tend exponentiellement vite vers 1.

variables aléatoires à valeurs dans A et B respectivement, liées par la relation $\mathbf{P}(\mathrm{Y} = b \mid \mathrm{X} = a) = p(b \mid a)$, $p(\cdot \mid \cdot)$ désignant la probabilité de transmission du canal C. Comme A et B sont finis, cette borne supérieure est réalisée par une loi ; si elle ne l'avait pas été, on aurait choisi une loi qui l'approche.)

La fonction de décodage g_Φ n'est pas aléatoire — ce serait absurde ! — mais est définie par la stratégie de la « correction typique ». Bien qu'elle ne soit pas explicite, cette stratégie a l'avantage de permettre une évaluation relativement simple de la probabilité d'erreur. Dans $\mathrm{C}^n = \mathrm{A}^n \times \mathrm{B}^n$, considérons l'ensemble typique C^n_ε adapté à un paramètre $\varepsilon > 0$, tel que défini dans le théorème 2.4.3 pour l'entropie, et dans le paragraphe 2.4.5 pour l'information mutuelle. Par définition, la fonction de décodage g_Φ appliquera un élément $b \in \mathrm{B}^n$ sur un élément $m \in \mathrm{M}$ tel que $(f_\Phi(m), b) \in \mathrm{C}^n_\varepsilon$, s'il existe un tel élément et un seul, et appliquera b sur un élément de M non précisé sinon.

Rappelons la définition de l'ensemble typique : pour $a \in \mathrm{A}^n$ et $b \in \mathrm{B}^n$, le couple (a, b) appartient à C^n_ε si et seulement si $\mathbf{P}(\mathrm{X} = a, \mathrm{Y} = b)$ est de l'ordre de $e^{-n\mathrm{H}(\mathrm{X},\mathrm{Y})}$, $\mathbf{P}(\mathrm{X} = a)$ est de l'ordre de $e^{-n\mathrm{H}(\mathrm{X})}$ et $\mathbf{P}(\mathrm{Y} = b)$ est de l'ordre de $e^{-n\mathrm{H}(\mathrm{Y})}$; la formulation précise de l'expression « de l'ordre de » fait bien sûr intervenir ε, mais je ne l'explicite pas tout de suite. La notation $\mathbf{P}(\mathrm{X} = a, \mathrm{Y} = b)$ est un raccourci pour la probabilité que le canal C reçoive le mot de longueur n et transmette le mot b :

$$\mathbf{P}(\mathrm{X} = a, \mathrm{Y} = b) = \mathbf{P}(\mathrm{X} = a)\mathbf{P}(\mathrm{Y} = b \mid \mathrm{X} = a) = \prod_{j=1}^{n} \mathbf{P}(\mathrm{X} = a_j).$$

On choisit aussi aléatoirement le bloc qui est transmis, au moyen d'une variable aléatoire W uniforme dans M, indépendante du code Φ. Le mot transmis dans le canal est $\mathrm{X} = f_\Phi(\mathrm{W})$, celui qui est reçu est Y, et le bloc décodé est $\mathrm{W}' = g_\Phi(\mathrm{Y})$.

Il s'agit pour commencer de montrer que la probabilité que $\mathrm{W}' \neq \mathrm{W}$ est petite. On notera U la variable aléatoire qui vaut 1 lorsque $\mathrm{W}' \neq \mathrm{W}$ et 0 sinon ; on a $\mathbf{P}(\mathrm{W}' \neq \mathrm{W}) = \mathbf{E}(\mathrm{U})$.

Proposition **(2.6.8)**. — *Soit $\alpha > 0$. Il existe $\varepsilon > 0$ tel que, dès que n est assez grand, on a $\mathbf{P}(\mathrm{W}' \neq \mathrm{W}) \leqslant \alpha$.*

Démonstration. — Puisque $\mathbf{P}(\mathrm{W} = m) = 1/\mathrm{Card}(\mathrm{M})$ pour tout $m \in \mathrm{M}$, on a

$$\begin{aligned}\mathbf{P}(\mathrm{W}' \neq \mathrm{W}) &= \sum_{m\in\mathrm{M}} \mathbf{P}(\mathrm{W} = m)\mathbf{P}(\mathrm{W}' \neq \mathrm{W} \mid \mathrm{W} = m)\\ &= \frac{1}{\mathrm{Card}(\mathrm{M})} \sum_{m\in\mathrm{M}} \mathbf{P}(\mathrm{W}' \neq \mathrm{W} \mid \mathrm{W} = m).\end{aligned}$$

Fixons un élément $m \in \mathrm{M}$ et conditionnons la situation à $\mathrm{W} = m$; on a erreur lorsque, soit $(f_\Phi(m), \mathrm{Y})$ n'appartient pas à C_ε^n (évènement E ; rappelons que $\mathrm{X} = f_\Phi(\mathrm{W})$), soit il existe $m' \neq m$ tel que $(f_\Phi(m'), \mathrm{Y})$ appartient à C_ε^n (évènement $\mathrm{E}_{m'}$), de sorte que

$$\mathbf{P}(\mathrm{W}' \neq \mathrm{W} \mid \mathrm{W} = m) \leqslant \mathbf{P}(\mathrm{E} \mid \mathrm{W} = m) + \sum_{m'\neq m} \mathbf{P}(\mathrm{E}_{m'} \mid \mathrm{W} = m).$$

Alors,

$$\mathbf{P}(\mathrm{W}' \neq \mathrm{W}) \leqslant \mathbf{P}((\mathrm{X}, \mathrm{Y}) \notin \mathrm{C}_\varepsilon^n) + \frac{1}{\mathrm{Card}(\mathrm{M})} \sum_{m\neq m'} \mathbf{P}((f_\Phi(m'), \mathrm{Y}) \in \mathrm{C}_\varepsilon^n \mid \mathrm{X} = f_\Phi(m)).$$

Introduisons une variable aléatoire X' à valeurs dans A^n, de même loi que X mais indépendante de X ; par définition d'un canal sans mémoire, les variables aléatoires X' et Y sont indépendantes. Soit $m' \in \mathrm{M}$ tel que $m' \neq m$; la variable aléatoire $f_\Phi(m')$ a même loi que X et se comporte comme X', de sorte que que le couple $(f_\Phi(m'), \mathrm{Y})$ a même loi que $(\mathrm{X}', \mathrm{Y})$. Ainsi,

$$\begin{aligned}&\frac{1}{\mathrm{Card}(\mathrm{M})} \sum_{m\neq m'} \mathbf{P}((f_\Phi(m'), \mathrm{Y}) \in \mathrm{C}_\varepsilon^n \mid \mathrm{X} = f_\Phi(m))\\ &\qquad\qquad \leqslant \mathrm{Card}(\mathrm{M})\mathbf{P}((\mathrm{X}', \mathrm{Y}) \in \mathrm{C}_\varepsilon^n \mid \mathrm{X} = f_\Phi(m)),\end{aligned}$$

de sorte que

$$\mathbf{P}(\mathrm{W}' \neq \mathrm{W}) \leqslant \mathbf{P}((\mathrm{X}, \mathrm{Y}) \notin \mathrm{C}_\varepsilon^n) + \mathbf{P}((\mathrm{X}', \mathrm{Y}) \in \mathrm{C}_\varepsilon^n).$$

Définissons $c(\mathrm{X})$, $c(\mathrm{Y})$ et $c(\mathrm{X}, \mathrm{Y})$ comme dans le paragraphe 2.4.5 ; compte tenu de l'interprétation statistique de l'entropie (théorème 2.4.3) et de l'information mutuelle le premier terme est donc majoré par $(c(\mathrm{X}) + c(\mathrm{Y}) + c(\mathrm{X}, \mathrm{Y}))/2n\varepsilon^2$, et le second est majoré par

$$\mathrm{Card}(\mathrm{M})e^{-n(\mathrm{I}(\mathrm{X}_1,\mathrm{Y}_1))-3\varepsilon)} = \lceil e^{n\rho} \rceil e^{-n(\mathrm{I}(\mathrm{C})-3\varepsilon)} \sim e^{n(\rho-\mathrm{I}(\mathrm{C})+3\varepsilon)}.$$

Comme $\rho < \mathrm{I}(\mathrm{C})$, il existe $\varepsilon > 0$ tel que $\rho - \mathrm{I}(\mathrm{C}) + 3\varepsilon < 0$. Quand n tend vers $+\infty$, la majoration que nous avons obtenue pour $\mathbf{P}(\mathrm{W}' \neq \mathrm{W})$ tend alors vers 0 ; pour n assez grand, on a donc $\mathbf{P}(\mathrm{W}' \neq \mathrm{W}) < \alpha$. □

Corollaire **(2.6.9)**. — *Soit* C *un canal sans mémoire. Soit* $\alpha > 0$. *Pour tout nombre réel* $\rho < \mathrm{I}(\mathrm{C})$ *et tout entier* n *assez grand, il existe un code* Φ *de longueur* n *adapté au canal* C *dont le taux de transmission est au moins* ρ *et dont la probabilité d'erreur moyenne* $\lambda_{\mathrm{moy}}(\Phi)$ *est inférieure à* α.

Démonstration. — Choisissons n assez grand de sorte que $\mathbf{P}(\mathrm{W}' \neq \mathrm{W}) < \alpha$ (proposition 2.6.8). En conditionnant sur tous les codes possibles, on a

$$\mathbf{P}(\mathrm{W}' \neq \mathrm{W}) = \frac{1}{\mathrm{Card}(\{\Phi\})} \sum_{\Phi} \mathbf{P}(\mathrm{W}' \neq \mathrm{W} \mid f = f_\Phi).$$

Par suite, il existe Φ tel que $\mathbf{P}(\mathrm{W}' \neq \mathrm{W} \mid f = f_\Phi) < \alpha$. Par ailleurs, comme la variable aléatoire W est indépendante de Φ et uniforme dans M, on a

$$\mathbf{P}(\mathrm{W}' \neq \mathrm{W} \mid f = f_\Phi) = \frac{1}{\mathrm{Card}(\mathrm{M})} \sum_{m \in \mathrm{M}} \mathbf{P}(\mathrm{W}' \neq \mathrm{W} \mid f = f_\Phi, \mathrm{W} = m).$$

Par définition, $\mathbf{P}(\mathrm{W}' \neq \mathrm{W} \mid f = f_\Phi, \mathrm{W} = m) = \lambda_m(\Phi)$, la probabilité d'erreur de transmission lorsque le bloc m est transmis dans le canal C au moyen du code Φ. Ainsi,

$$\lambda_{\mathrm{moy}}(\Phi) = \mathbf{P}(\mathrm{W}' \neq \mathrm{W} \mid f = f_\Phi) < \alpha.$$

Enfin, le taux de transmission du code Φ vérifie

$$\tau(\Phi) = \frac{\log(\mathrm{Card}(\Phi))}{n} \geqslant \rho,$$

ce qui conclut la démonstration du corollaire. □

Lemme **(2.6.10)**. — *Soit* Φ *un code de longueur* n *adapté à un canal sans mémoire* C. *Il existe un code* Φ' *de même longueur tel que*

$$\tau(\Phi') \geqslant \tau(\Phi) - \frac{\log(2)}{n} \quad \textit{et} \quad \lambda_{\max}(\Phi') \leqslant 2\lambda_{\mathrm{moy}}(\Phi).$$

Démonstration. — Soit M le domaine du code Φ, soit f sa fonction de codage et g sa fonction de décodage.

Soit M′ l'ensemble des éléments $m \in \mathrm{M}$ tels que $\lambda_m(\Phi) \leqslant 2\lambda_{\mathrm{moy}}(\Phi)$. Appliquons l'inégalité de Markov (proposition 2.4.1) à la fonction $m \mapsto \lambda_m(\Phi)$ sur l'univers M muni de la mesure de probabilité uniforme ; son espérance est $\lambda_{\mathrm{moy}}(\Phi)$. On a donc

$$\mathbf{P}(\lambda_m(\Phi) > 2\lambda_{\mathrm{moy}}(\Phi)) \leqslant \frac{1}{2},$$

c'est-à-dire $\mathrm{Card}(\mathrm{M} - \mathrm{M}') \leqslant \frac{1}{2}\mathrm{Card}(\mathrm{M})$, soit encore $\mathrm{Card}(\mathrm{M}') \geqslant \frac{1}{2}\mathrm{Card}(\mathrm{M})$.

Soit $f' : \mathrm{M}' \longrightarrow \mathrm{A}^n$ la restriction à M' de la fonction de codage f. On choisit une fonction $g' : \mathrm{B}^n \longrightarrow \mathrm{M}'$ telle que $g'(b) = g(b)$ si $g(b) \in \mathrm{M}'$. Alors, (f', g') est un code Φ' sur l'ensemble M' adapté au canal C. Pour $m \in \mathrm{M}'$, on a

$$\begin{aligned}\lambda_m(\Phi') &= \mathbf{P}(g'(\mathrm{Y}) \neq m \mid \mathrm{X} = f'(m)) \\ &\leqslant \mathbf{P}(g(\mathrm{Y}) \neq m \mid \mathrm{X} = f_\Phi(m)) \\ &= \lambda_m(\Phi) \leqslant 2\lambda_{\mathrm{moy}}(\Phi),\end{aligned}$$

donc $\lambda_{\max}(\Phi') \leqslant 2\lambda_{\mathrm{moy}}(\Phi)$. Enfin, le taux de transmission de ce code Φ' vérifie

$$\tau(\Phi') = \frac{\log(\mathrm{Card}(\mathrm{M}'))}{n} \geqslant \frac{\log(\mathrm{Card}(\mathrm{M})) - \log(2)}{n} \geqslant \tau(\Phi) - \frac{\log(2)}{n}.$$

□

2.6.11. Conclusion de la démonstration du théorème 2.6.4. — Rappelons qu'il s'agit de prouver qu'il existe, pour tout nombre réel ρ tel que $\rho < \mathrm{I}(\mathrm{C})$, tout nombre réel $\alpha > 0$ et tout entier n assez grand, un code de longueur n adapté au canal C, de taux de transmission au moins ρ et de probabilité d'erreur maximale au plus α. Soit ρ' un nombre réel tel que $\rho < \rho' < \mathrm{I}(\mathrm{C})$. D'après le corollaire 2.6.9, il existe, pour tout entier n assez grand, un code Φ de longueur n adapté au canal C, de taux de transmission $\geqslant \rho'$ et de probabilité d'erreur moyenne $< \alpha/2$. Soit Φ' un code tel que construit dans le lemme 2.6.10. Son taux de transmission est au moins égal à $\rho' - \frac{\log(2)}{n}$, donc $\tau(\Phi') \geqslant \rho$ si n est assez grand, précisément, si $n \geqslant \log(2)/(\rho' - \rho)$, et sa probabilité d'erreur maximale est au plus α. Le théorème est ainsi démontré.

(2)

2.7. Exercices

Exercice **(2.7.1).** — On considère un code binaire sur un ensemble à deux éléments tel que les deux mots codés sont 0 et 01.

a) S'agit-il d'un code préfixe ?

b) Démontrer que ce code est uniquement décodable.

(2) Ajouter une discussion 1) sur la méthode probabiliste ; 2) sur les codes correcteurs d'erreur.

Exercice **(2.7.2)**. — Soit (X_n) un processus stationnaire prenant ses valeurs dans un ensemble A fini. Pour tout entier n, on considère la variable aléatoire $Y_n = (X_1, \dots, X_n)$ à valeurs dans A^n.

a) Lorsque de plus les X_n sont indépendantes, rappeler quelle est la loi de Y_n et son entropie.

b) Soit C_n un code sur A^n, à valeurs dans un alphabet de cardinal D, qui est optimal relativement à la loi de Y_n. On pose

$$L_n = \mathbf{E}(\ell(C_n(Y)))/n.$$

En appliquant le théorème de Shannon à la variable Y_n, démontrer que L_n converge vers le taux d'entropie du processus (X_n).

Exercice **(2.7.3)**. — On considère l'alphabet $A = \{a, b, c, d, e, f, g\}$ avec les probabilités respectives :

a	b	c	d	e	f	g
0,49	0,26	0,12	0,04	0,04	0,03	0,02

a) Calculer l'entropie d'une variable aléatoire ayant une telle loi.

b) Construire un code par la méthode de Shannon (c'est-à-dire qu'un symbole $x \in A$ est codé par un mot de longueur $\lceil -\log(p(x)) \rceil$, où $p(x)$ est sa probabilité). Quelle est la longueur moyenne d'un tel code ?

c) Construire, par la méthode de Huffman, un code binaire optimal. Quelle est sa longueur moyenne ?

d) Coder le mot *bagage*.

e) Décoder le message 111110111101111011101.

Exercice **(2.7.4)**. — On considère une variable aléatoire X sur un alphabet fini A, de loi de probabilité p. Pour calculer un code binaire optimal relativement à cette loi, on doit connaître la loi p. Supposons qu'on n'en connaisse qu'une approximation q, qu'on utilise comme code C un code binaire C construit à la Shannon, relativement à la loi q ; en particulier, on a $\ell(C(a)) = \lceil -\log_2(q(a)) \rceil$.

a) On suppose que q est *dyadique*, c'est-à-dire que pour tout a, $q(a)$ est de la forme $1/2^n$, pour un certain entier n. Démontrer que C est un code optimal relativement à la loi q. Quelle est la longueur moyenne $\mathbf{E}(\ell(C(X)))$ d'un mot de code ?

b) Dans le cas général, démontrer l'encadrement de cette longueur moyenne :

$$\mathrm{H}(\mathrm{X}) + \mathrm{D}(p \mid q) \leqslant \mathbf{E}(\ell(\mathrm{C}(\mathrm{X}))) < \mathrm{H}(\mathrm{X}) + \mathrm{D}(p \mid q) + 1.$$

Exercice **(2.7.5)**. — On considère une variable aléatoire X à valeurs dans un alphabet $\mathrm{A} = \{\mathrm{a}, \mathrm{b}, \mathrm{c}, \mathrm{d}\}$. Dans le tableau suivant, on indique la loi de X, ainsi que deux codes binaires sur cet alphabet.

X	p_{X}	code I	code II
a	0,4	1	1
b	0,3	01	10
c	0,2	001	100
d	0,1	0001	1000

Pour chacun de ces deux codes, répondez aux quatre questions suivantes :

a) S'agit-il d'un code préfixe ? S'agit-il d'un code uniquement décodable ?

b) On considère les deux variables aléatoires (à valeurs vrai/faux) U = « X = a » et V = « le premier symbole du mot de code est 1 ». Quelle est leur information mutuelle $\mathrm{I}(\mathrm{U}, \mathrm{V})$?

c) Quelle est la longueur moyenne d'un mot de code ? Que dit le théorème de Shannon dans ce contexte ?

d) Construire un code binaire optimal pour la variable aléatoire X. Quelle est la longueur moyenne d'un mot de code ?

Exercice **(2.7.6)**. — *a*) Soit X une variable aléatoire bornée. Prouver que l'on a $\mathbf{P}(\mathrm{X} \geqslant a) \leqslant \mathbf{E}(e^{t\mathrm{X}})e^{-ta}$ pour tous $a \in \mathbf{R}$ et $t > 0$. (*Inégalité de Chernoff*)

Soit $(\mathrm{X}_k)_{1 \leqslant k \leqslant n}$ une suite indépendante de variables aléatoires, obéissant toutes à la loi de Bernoulli de paramètre p. On pose $\mathrm{S} = (\mathrm{X}_1 + \cdots + \mathrm{X}_n)/n$.

b) Pour $t > 0$, calculer $\mathbf{E}(e^{t\mathrm{S}})$.

c) Calculer la divergence $\mathrm{D}(q \mid p)$ d'une variable de Bernoulli de paramètre q par rapport à une variable de Bernoulli de paramètre p.

d) Soit $q \in [0; 1]$ tel que $q > p$. Démontrer que l'on a $\mathbf{P}(\mathrm{S} \geqslant q) \leqslant e^{-n\mathrm{D}(p|q)}$.

e) Soit $q \in [0; 1]$ tel que $q < p$. Démontrer que l'on a $\mathbf{P}(\mathrm{S} \leqslant q) \leqslant e^{-n\mathrm{D}(p|q)}$.

Exercice **(2.7.7)**. — Soit d un entier $\geqslant 3$; on considère un canal avec bruit sans mémoire C dont les alphabets sont tous deux égaux au groupe fini $\mathrm{A} = \mathbf{Z}/d\mathbf{Z}$, avec

probabilités de transmission $p(a+1 \mid a) = p(a-1 \mid a) = p$ et $p(a \mid a) = 1-2p$, où p est un nombre réel tel que $0 \leqslant p \leqslant 1/2$.

Quelle est la capacité de ce canal ? Déterminer une loi d'une variable aléatoire X sur A telle que $\mathrm{I}(\mathrm{C}) = \mathrm{I}(\mathrm{X}, \mathrm{Y})$, où $\mathbf{P}(\mathrm{Y} = b \mid \mathrm{X} = a) = p(b \mid a)$.

Exercice **(2.7.8)**. — Soit p un nombre réel tel que $0 \leqslant p \leqslant 1$. Calculer la capacité du canal avec bruit sans mémoire de matrice de probabilités de transmission

$$\begin{pmatrix} 1 & 0 \\ p & 1-p \end{pmatrix},$$

ainsi que les lois sur la source qui permettent d'atteindre cette capacité. Étudier la variation de cette capacité avec p ; interpréter en particulier les cas $p = 1/2$, $p = 1$, $p = 0$.

Exercice **(2.7.9)**. — Soit C′ et C″ des canaux. On suppose que l'alphabet d'entrée de C″ est égal à l'alphabet de sortie de C′ et on considère le canal C obtenu en concaténant les deux canaux C′ puis C″.

a) Calculer la matrice de probabilités de transmissions de C en fonction de celles de C′ et C″.

b) Démontrer que la capacité de transmission du canal C vérifie

$$\mathrm{I}(\mathrm{C}) \leqslant \inf(\mathrm{I}(\mathrm{C}'), \mathrm{I}(\mathrm{C}'')).$$

c) On « empile » ainsi une suite de n canaux symétriques binaires C de paramètre p (c'est-à-dire que $p(1 \mid 0) = p(0 \mid 1) = p$). Démontrer que le canal C_n obtenu se comporte comme un canal symétrique binaire de paramètre $(1-(1-2p)^n)/2$. Que se passe-t-il quand $n \longrightarrow +\infty$. Comparer avec le théorème de Shannon.

Exercice **(2.7.10)**. — Soit C′ et C″ des canaux, d'alphabets d'entrée A′ et A″, et d'alphabets de sortie B′ et B″. On considère le canal $\mathrm{C} = \mathrm{C}' \times \mathrm{C}''$ sur l'alphabet d'entrée $\mathrm{A} = \mathrm{A}' \times \mathrm{A}''$ et l'alphabet de sortie $\mathrm{B} = \mathrm{B}' \times \mathrm{B}''$, avec probabilités de transmission

$$p((b', b'') \mid (a', a'')) = p(b' \mid a')p(b'' \mid a'').$$

a) Soit $\mathrm{X}', \mathrm{X}'', \mathrm{Y}', \mathrm{Y}''$ des variables aléatoires à valeurs dans $\mathrm{A}', \mathrm{A}'', \mathrm{B}', \mathrm{B}''$; on pose $\mathrm{X} = (\mathrm{X}', \mathrm{X}'')$ et $\mathrm{Y} = (\mathrm{Y}', \mathrm{Y}'')$ et l'on suppose que l'on a $\mathrm{X} \sim_{\mathrm{C}} \mathrm{Y}$. Démontrer que l'on a $\mathrm{X}' \sim_{\mathrm{C}'} \mathrm{Y}'$ et $\mathrm{X}'' \sim_{\mathrm{C}''} \mathrm{Y}''$.

b) Démontrer aussi que l'on a $\mathrm{X}'' \perp_{\mathrm{X}'} \mathrm{Y}'$ et $\mathrm{Y}'' \perp_{\mathrm{X}''} \mathrm{X}'$.

c) Démontrer que la capacité du canal C est donnée par $\mathrm{I}(\mathrm{C}) = \mathrm{I}(\mathrm{C}') + \mathrm{I}(\mathrm{C}'')$. Préciser également une loi sur A qui réalise cette capacité.

Exercice **(2.7.11)**. — Soit C′ et C″ des canaux, d'alphabets d'entrée A′ et A″, et d'alphabets de sortie B′ et B″. On suppose que les ensembles A′ et A″ d'une part, B′ et B″ d'autre part, sont disjoints, et l'on note $\mathrm{A} = \mathrm{A}' \cup \mathrm{A}''$ et $\mathrm{B} = \mathrm{B}' \cup \mathrm{B}''$. On considère le canal C sur l'alphabet d'entrée A à valeurs dans l'alphabet B qui a les probabilités de transmission : $p_{\mathrm{C}}(b \mid a) = p_{\mathrm{C}'}(b \mid a)$ si $a \in \mathrm{A}'$ et $b \in \mathrm{B}'$, et $p_{\mathrm{C}}(b \mid a) = p_{\mathrm{C}''}(b \mid a)$ si $a \in \mathrm{A}''$ et $b \in \mathrm{B}''$.

a) Expliquer que $p(b \mid a) = 0$ si $b \in \mathrm{B}'$ et $a \in \mathrm{A}''$, ou si $b \in \mathrm{B}''$ et $a \in \mathrm{A}'$.

b) Démontrer que la capacité de C vérifie

$$e^{\mathrm{I}(\mathrm{C})} = e^{\mathrm{I}(\mathrm{C}')} + e^{\mathrm{I}(\mathrm{C}'')}.$$

Pour quelles lois de probabilité sur A est-elle atteinte ?

Exercice **(2.7.12)**. — On considère un canal C sur des alphabets A et B, mais tels que l'utilisation d'un symbole $a \in \mathrm{A}$ ait un « coût » $c(a) \geqslant 0$. La fonction capacité–coût de ce canal est définie par

$$\mathrm{I}(\mathrm{C}, \gamma) = \sup\{\mathrm{I}(\mathrm{X}, \mathrm{Y}) \,;\, \mathrm{X} \sim_{\mathrm{C}} \mathrm{Y} \text{ et } \mathbf{E}(c(\mathrm{X})) \leqslant \gamma\}.$$

a) Calculer cette fonction lorsque C est un canal symétrique binaire de paramètre p.

b) Plus généralement, la calculer lorsque C est un canal sur l'alphabet $\{1, \dots, d\}$ (de cardinal d) de matrice de probabilités de transmission

$$\begin{pmatrix} q & p & \dots & p \\ p & q & \dots & p \\ \vdots & \vdots & \ddots & \vdots \\ p & p & \dots & q \end{pmatrix}$$

où p est un nombre réel tel que $0 \leqslant p \leqslant 1/(d-1)$ et $q = 1 - (d-1)p$.

2.8. Solutions des exercices

Solution de l'exercice (2.7.1). — *a*) Comme le mot o est préfixe du mot o1, ce n'est pas un code préfixe.

b) Soit $a = a_1 \dots a_m$ et $b = b_1 \dots b_n$ des mots ayant même code. Démontrons qu'ils sont égaux par récurrence sur leur longueur. Si l'un des deux est vide, l'autre aussi. Supposons donc qu'ils ne soient pas vides ; on écrit alors $a = a_1 a'$ et $b = b_1 b'$, de sorte que le code de a est $\mathrm{C}(a_1)\mathrm{C}(a')$ et celui de b est $\mathrm{C}(b_1)\mathrm{C}(b')$. Si $a_1 = b_1$, alors a' et b' ont même code ; par récurrence, $a' = b'$ donc $a = b$. Supposons donc $a_1 \neq b_1$ et, pour fixer les idées, que le code de a_1 soit 0 tandis que celui de b_1 est 01. On a dans ce cas $0\mathrm{C}(a') = 01\mathrm{C}(b')$, donc $\mathrm{C}(a') = 1\mathrm{C}(b')$; cela signifie que le code de a_2 débute par un 1, ce qui est absurde.

Une démonstration plus simple consisterait à lire les mots de droite à gauche. Cela revient à considérer que les codes des deux symboles sont 0 et 10 ; ce code renversé est un code préfixe, donc est uniquement décodable. Ainsi, le code initial est uniquement décodable.

Solution de l'exercice (2.7.2). — *a*) Par définition de l'indépendance, pour tout $(a_1, \dots, a_n) \in \mathrm{A}^n$, on a

$$\mathrm{P}(\mathrm{Y}_n = (a_1, \dots, a_n)) = \mathbf{P}(\mathrm{X}_1 = a_1) \dots \mathbf{P}(\mathrm{X}_n = a_n).$$

Comme le processus (X_n) est stationnaire, les X_n ont toute même loi, celle de X_1, et l'on a

$$\mathrm{P}(\mathrm{Y}_n = (a_1, \dots, a_n)) = \mathbf{P}(\mathrm{X}_1 = a_1) \dots \mathbf{P}(\mathrm{X}_1 = a_n).$$

L'entropie de Y_n est alors $n\mathrm{H}(\mathrm{X}_1)$.

b) Le théorème de Shannon affirme que

$$\mathrm{H}_\mathrm{D}(\mathrm{Y}_n) \leqslant \mathbf{E}(\ell(\mathrm{C}_n(\mathrm{Y}_n))) < \mathrm{H}_\mathrm{D}(\mathrm{Y}_n) + 1.$$

Autrement dit,

$$\frac{1}{n}\mathrm{H}_\mathrm{D}(\mathrm{Y}_n) \leqslant \mathrm{L}_n < \frac{1}{n}\mathrm{H}_\mathrm{D}(\mathrm{Y}_n) + \frac{1}{n}.$$

Quand $n \longrightarrow +\infty$, les membres de droite et de gauche de cette inégalité tendent vers le taux d'entropie $\mathrm{H}(\mathrm{X})$ du processus (X_n). Par le théorème d'encadrement, on en déduit que L_n converge vers ce taux d'entropie.

Solution de l'exercice (2.7.3). — *a*) Il suffit d'appliquer la formule $\mathrm{H}(\mathrm{X}) = -\sum p(a) \log(p(a))$. Par exemple, en utilisant SageMath :

```
h2 = lambda p:-p*log(p,2)
H2 = lambda p: sum (map(h2,p))
p = [0.49, 0.26, 0.12, 0.04, 0.04, 0.03, 0.02]
```

L'entropie en base 2 de cette variable aléatoire est donc 2.01278966433342.

b) On complète le tableau en indiquant la longueur d'un symbole tel que proposé par la méthode de Shannon.

a	b	c	d	e	f	g
0,49	0,26	0,12	0,04	0,04	0,03	0,02
2	2	4	5	5	6	6

On ajoute ensuite successivement les entiers $2^{-\ell}$ et on isole ensuite la partie convenable du développement binaire.

a	2	0.	00
b	2	0.01	01
c	4	0.10	1000
d	5	0.1001	10010
e	5	0.10011	10011
f	6	0.10100	101000
g	6	0.101001	101001

```
lS = lambda p:ceil(-ln(p)/ln(2.0))
pS = list(map(lS,p))
lpS = sum (pS[i]*p[i] for i in range(len(p)))
```

La longueur moyenne de ce code est donc $0{,}49 \times 2 + 0{,}226 \times 2 + \cdots = 2.68000000000000$.

c) La méthode de Huffman part du tableau de probabilités initial

a	b	c	d	e	f	g
0,49	0,26	0,12	0,04	0,04	0,03	0,02

et combine les deux lettres de probabilité minimale. Ce sont ici f et g, la somme de leurs probabilités est 0,04, et on obtient :

a	b	c	d	e	fg
0,49	0,26	0,12	0,04	0,04	0,05

On poursuit le processus : on combine maintenant d et e :

a	b	c	de	fg
0,49	0,26	0,12	0,08	0,05

Puis les groupes de et fg :

a	b	c	defg
0,49	0,26	0,12	0,13

Ensuite le symbole c et le groupe defg :

a	b	cdefg
0,49	0,26	0,25

Puis le symbole b et le groupe cdefg :

a	bcdefg
0,49	0,51

À ce moment, on code a par 0, bcdefg par 1 ; b par 10 et cdefg par 11 ; c par 110 et defg par 111 ; de par 1110 et fg par 1111 ; d par 11100 et e par 11101, f par 11110 et g par 11111, d'où le code et les longueurs :

a	b	c	d	e	f	g
0,49	0,26	0,12	0,04	0,04	0,03	0,02
0	10	110	11100	11101	11110	11111
1	2	3	5	5	5	5

Les commandes SageMath

```
pH = [1,2,3,5,5,5,5,5]
lpH = sum (pH[i]*p[i] for i in range(len(p)))
```

calculent la longueur moyenne de ce code ; on obtient 2.02000000000000.

Solution de l'exercice (2.7.4). — *a*) Si $q(a) = 1/2^n$, on a $\log_2(q(a)) = -n$ et $\ell(\mathrm{C}(a)) = n$. Ainsi,

$$\mathbf{E}_q(\ell(\mathrm{C}(a)) = \sum_a \big(-q(a)\log_2(q(a))\big) = \mathrm{H}_2(q).$$

Compte tenu de l'inégalité de Shannon, le code C est optimal relativement à la loi q. La longueur moyenne d'un mot de code est

$$\mathbf{E}(\ell(\mathrm{C}(\mathrm{X})) = \sum_a p(a)\ell(\mathrm{C}(a)) = -\sum_a p(a)\log_2(q(a)).$$

On devine une divergence $\mathrm{D}(p \mid q)$; introduisons donc $\log_2(p(a))$. Ainsi,

$$\mathbf{E}(\ell(\mathrm{C}(\mathrm{X}))) = -\sum_a p(a)\log_2\Big(\frac{q(a)}{p(a)}\Big) - \sum_a p(a)\log_2(p(a)) = \mathrm{D}(p \mid q) + \mathrm{H}(p).$$

La divergence $\mathrm{D}(p \mid q)$ de q par rapport à p mesure ainsi exactement combien la longueur moyenne d'un mot de code dépasse dépasse la borne de Shannon.

b) On reprend le même calcul en utilisant l'encadrement

$$-\log_2(q(a)) \leqslant \ell(\mathrm{C}(a)) < 1 - \log_2(q(a)).$$

Ainsi,

$$\mathbf{E}(\ell(\mathrm{C}(\mathrm{X}))) = \sum_a p(a)\ell(\mathrm{C}(a)) \geqslant -\sum_a p(a)\log_2 q(a) = \mathrm{D}(p \mid q) + \mathrm{H}(p).$$

De même,

$$\begin{aligned}\mathbf{E}(\ell(\mathrm{C}(\mathrm{X}))) &= \sum_a p(a)\ell(\mathrm{C}(a)) \\ &\leqslant \sum_a p(a) + \mathrm{D}(p \mid q) + \mathrm{H}(p) = 1 + \mathrm{D}(p \mid q) + \mathrm{H}(p).\end{aligned}$$

Comme $\sum p(a) = 1$, il y a au mois un symbole pour lequel $p(a) > 0$; alors $\ell(\mathrm{C}(a)) < 1 - \log_2(q(a))$ et la majoration finale est stricte.

Solution de l'exercice (*2.7.5*). — *a*) Le code I est préfixe, mais pas le code II.

Les deux codes sont uniquement décodables. Pour le code I, c'est parce que c'est un code préfixe. Pour le code II, on peut par exemple observer qu'il est obtenu par renversement à partir du code I ; pour décoder un texte, il suffit de le renverser, de le décoder avec le code I, et de renverser de nouveau le message obtenu.

b) Notons U et V ces deux variables aléatoires. Par définition,

$$\mathrm{I}(\mathrm{U},\mathrm{V}) = \mathrm{H}(\mathrm{U}) + \mathrm{H}(\mathrm{V}) - \mathrm{H}(\mathrm{U},\mathrm{V}) = \mathrm{H}(\mathrm{V}) - \mathrm{H}(\mathrm{V} \mid \mathrm{U}).$$

On a $\mathbf{P}(\mathrm{U} = \text{vrai}) = 0{,}4$ et $\mathbf{P}(\mathrm{U} = \text{faux}) = 0{,}6$. Par suite, $\mathrm{H}(\mathrm{U}) = -0{,}4\log(0{,}4) - 0{,}6\log(0{,}6) \approx 0{,}971$.

Considérons d'abord le code I. Dans ce cas, $\mathrm{V} = \mathrm{U}$ puisque le mot de code commence par 1 exactement quand la lettre est a. Alors, $\mathrm{I}(\mathrm{U},\mathrm{V}) = \mathrm{H}(\mathrm{U}) \approx 0{,}971$.

Considérons maintenant le code II. On a $\mathbf{P}(\mathrm{V} = \text{vrai}) = 1$: la variable V est donc certaine, donc est indépendante de U si bien que $\mathrm{I}(\mathrm{U},\mathrm{V}) = 0$.

c) Les codes I et II ont même longueur. On a

$$\begin{aligned}\mathbf{E}(\ell(C(X))) &= \mathbf{P}(X = a)\ell(C(a)) + \cdots + \mathbf{P}(X = d)\ell(C(d)) \\ &= 0{,}4 \cdot 1 + 0{,}3 \cdot 2 + 0{,}2 \cdot 3 + 0{,}1 \cdot 4 \\ &= 2.\end{aligned}$$

Le théorème de Shannon affirme que l'on a toujours $\mathbf{E}(\ell(C(X))) \geqslant H_2(X)$ (entropie de X en base 2), et qu'il existe un code de longueur moyenne au plus $1 + H_2(X)$. Or, l'entropie de X est égale à

$$H_2(X) = -0{,}4 \log_2(0{,}4) - \cdot - 0{,}1 \log_2(0{,}1) \approx 1{,}846.$$

La longueur moyenne trouvée est dans l'encadrement donné par le théorème de Shannon.

d) Construisons un code optimal à la Huffman pour la variable X. On part de l'ensemble $A = \{a, b, c, d\}$ et des probabilités données par le tableau

a	b	c	d
0,4	0,3	0,2	0,1

On combine d'abord les deux symboles c et d pour leur associer le symbole cd de probabilité 0,3. On obtient donc le tableau

a	b	cd
0,4	0,3	0,3

On combine ensuite les deux symboles b et cd pour leur associer le symbole cd de probabilité 0,6. On obtient ainsi le tableau

a	bcd
0,4	0,6

On parcourt ceci en sens inverse : on code a par 0, bcd par 1. Puis b par 10 et cd par 11. Puis c par 110 et d par 111, d'où le code

X	p_X	code III
a	0,4	0
b	0,3	10
c	0,2	110
d	0,1	111

Sa longueur moyenne est

$$\mathbf{E}(\ell(\mathrm{C_{III}}(\mathrm{X}))) = 0{,}4 \cdot 1 + 0{,}3 \cdot 2 + 0{,}2 \cdot 3 + 0{,}1 \cdot 3 = 1{,}9,$$

très proche de l'entropie trouvée dans la question précédente.

Solution de l'exercice (2.7.6). — *a*) Comme la fonction exponentielle est strictement croissante et $t > 0$, on a

$$\mathbf{P}(\mathrm{X} \geqslant a) = \mathbf{P}(t\mathrm{X} \geqslant ta) = \mathbf{P}(e^{t\mathrm{X}} \geqslant e^{ta}) \leqslant \mathbf{E}(e^{t\mathrm{X}})e^{-ta}$$

en appliquant l'inégalité de Markov à la variable aléatoire $e^{t\mathrm{X}}$.

Remarque : Le domaine d'application de l'inégalité de Chernoff est plus restreint que celui de l'inégalité de Markov (qui n'exige que l'existence de l'espérance de S) ou que celui de l'inégalité de Bienaymé–Tchebitcheff (qui demande l'existence de la variance), mais elle fournit une information bien plus fine.

b) Pour $k \in \{0, \dots, n\}$, on a $\mathbf{P}(\mathrm{S} = k/n) = \binom{n}{k} p^k (1-p)^{n-k}$, la probabilité que parmi $\mathrm{X}_1, \dots, \mathrm{X}_n$, on obtienne exactement k fois la valeur 1. On a $\mathbf{P}(\mathrm{S} = x) = 0$ si x n'est pas de cette forme. Ainsi,

$$\mathbf{E}(e^{t\mathrm{S}}) = \sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k} e^{tk/n} = \big((1-p) + pe^{t/n}\big)^n,$$

en appliquant la formule du binôme.

c) On a

$$\begin{aligned} \mathrm{D}(p \mid q) &= q \log\Big(\frac{q}{p}\Big) + (1-q) \log\Big(\frac{1-q}{1-p}\Big) \\ &= q \log(q) + (1-q)\log(1-q) - q\log(p) - (1-q)\log(1-p). \end{aligned}$$

d) On écrit $\mathbf{E}(e^{t\mathrm{S}})e^{-tq} = f(t/n)^n$, où

$$f(x) = ((1-p) + pe^x)e^{-qx} = (1-p)e^{-qx} + pe^{(1-q)x}.$$

Si $q > 1$, la fonction f est strictement décroissante sur $\mathbf{R}$, et tend vers 0 à l'infini ; on a donc $\inf_t \mathbf{E}(e^{t\mathrm{S}})e^{-tq} = 0$ dans ce cas. L'inégalité de Chernoff entraîne $\mathbf{P}(\mathrm{S} \geqslant q) = 0$, une évidence puisque S prend ses valeurs dans $[0; 1]$. Si $q = 1$, on obtient une inégalité sans intérêt $\mathbf{P}(\mathrm{S} \geqslant 1) \leqslant p$. Si $q \leqslant 0$, la fonction f est strictement croissante sur $\mathbf{R}$, d'où $\inf_{x>0} f(x) = 1$, et l'on obtient $\mathbf{P}(\mathrm{S} \geqslant q) \leqslant 1$, une inégalité également sans intérêt.

On suppose maintenant $0 < q < 1$. La fonction f est de classe $\mathscr{C}^\infty$, sa dérivée est donnée par

$$f'(x) = -(1-p)qe^{-qx} + p(1-q)e^{(1-q)x}.$$

On en déduit que f est strictement décroissante sur $]-\infty;\xi]$ et strictement croissante sur $[\xi;+\infty[$, où ξ est défini par

$$e^{\xi} = \frac{1-p}{p}\frac{q}{1-q}.$$

On a donc

$$\begin{aligned} f(\xi) &= ((1-p) + pe^{\xi})e^{-q\xi} \\ &= (1-p)\big(1 + \frac{q}{1-q}\big)p^q(1-p)^{-q}q^{-q}(1-q)^q \\ &= (1-p)^{1-q}p^q/q^q(1-q)^{1-q} \\ &= \exp(-\mathrm{D}(q \mid p)). \end{aligned}$$

Comme $q > p$, on a $1/p > 1/q$, puis $1/p - 1 > 1/q - 1$ et $(1-p)/p > (1-q)/q$; autrement dit, $\xi > 0$. Ainsi, l'inégalité de Chernoff s'applique et fournit

$$\mathbf{P}(\mathrm{S} \geqslant q) \leqslant \mathbf{E}(e^{n\xi \mathrm{S}})e^{-n\xi q} = \exp(-n\mathrm{D}(q \mid p)).$$

Puisque $q > p$, on a $\mathrm{D}(q \mid p) > 0$ et cela fournit une décroissance exponentielle de $\mathbf{P}(\mathrm{S} \geqslant q)$.

e) Posons $\mathrm{X}'_k = 1 - \mathrm{X}_k$; c'est une variable aléatoire de Bernoulli de paramètre $1-p$. La suite $(\mathrm{X}'_1, \dots, \mathrm{X}'_n)$ est indépendante. Si $\mathrm{S}' = (\mathrm{X}'_1 + \cdots + \mathrm{X}'_n)/n$, on a $\mathrm{S}' = 1 - \mathrm{S}$ et la question précédente entraîne $\mathbf{P}(\mathrm{S}' \geqslant 1-q) \leqslant \exp(-n\mathrm{D}(1-q \mid 1-p))$. Par conséquent,

$$\mathbf{P}(\mathrm{S} \leqslant q) \leqslant \exp(-n\mathrm{D}(1-q \mid 1-p)) = \exp(-n\mathrm{D}(q \mid p)).$$

Solution de l'exercice (2.7.7). — *a*) Un tel canal est symétrique. Pour tout $a \in \mathrm{A}$, on a

$$\mathrm{H}(\mathrm{Y} \mid \mathrm{X} = a) = -2p\log(p) - (1-2p)\log(1-2p).$$

Alors, la formule du cours donne

$$\mathrm{I}(\mathrm{C}) = \log(d) + 2p\log(p) + (1-2p)\log(1-2p).$$

b) Soit X et Y des variables aléatoires à valeurs dans A telles que $\mathbf{P}(Y = b \mid X = a) = p(b \mid a)$ pour tous a, b. Soit $u = (u_a)$ la loi de A. On a $I(X, Y) = H(Y) - H(X \mid Y)$. L'expression $H(X \mid Y)$ est égale à $-2p\log(p) - (1-2p)\log(1-2p)$, tandis que $H(Y)$ est majoré par $\log(d)$, avec égalité si et seulement si la loi de Y est uniforme, c'est-à-dire $\mathbf{P}(Y = b) = 1/d$ pour tout b. On a

$$\mathbf{P}(Y = b) = (1 - 2p)u_b + pu_{b-1} + pu_{b+1}.$$

Si la loi de X est elle-même uniforme, on a $u_b = 1/d$ pour tout b, d'où $\mathbf{P}(Y = b) = 1/d$ pour tout b, si bien que la loi de Y est uniforme. (Il peut y avoir des lois non uniformes sur X qui rendent la loi de Y uniforme ; c'est par exemple le cas si $d = 8$ et $p = 1/4$.)

Solution de l'exercice (2.7.8). — Soit X et Y des variables aléatoires liées par les probabilités de transmission de ce canal : $\mathbf{P}(Y = 0 \mid X = 0) = 1$ et $\mathbf{P}(Y = 0 \mid X = 1) = p$. Soit $u = \mathbf{P}(X = 1)$; on a donc

$$\mathbf{P}(Y = 1) = \mathbf{P}(X = 0)\mathbf{P}(Y = 1 \mid X = 0) + \mathbf{P}(X = 1)\mathbf{P}(Y = 1 \mid X = 1) = u(1 - p)$$

et

$$P(Y = 0) = 1 - u(1 - p).$$

Alors,

$$H(Y) = -(1 - u(1 - p)))\log(1 - u(1 - p)) - u(1 - p)\log(u(1 - p))$$

tandis que

$$\begin{aligned} H(Y \mid X) &= \mathbf{P}(X = 0)H(Y \mid X = 0) + \mathbf{P}(X = 1)H(Y \mid X = 1) \\ &= (1 - u) \cdot 0 + u(-p\log(p) - (1 - p)\log(1 - p)) \\ &= -up\log(p) - u(1 - p)\log(1 - p). \end{aligned}$$

Ainsi,

$$\begin{aligned} I(X, Y) &= H(Y) - H(Y \mid X) \\ &= -(1 - u(1 - p)))\log(1 - u(1 - p)) - u(1 - p)\log(u(1 - p)) \\ &\qquad + up\log(p) + u(1 - p)\log(1 - p) \\ &= -(1 - u(1 - p)))\log(1 - u(1 - p)) - u(1 - p)\log(u) + up\log(p) \end{aligned}$$

Étudions cette fonction $u \mapsto \mathrm{F}(u)$ lorsque u varie. Pour simplifier, on suppose pour le moment $0 < p < 1$. On calcule

$$\begin{aligned}\mathrm{F}'(u) &= (1-p)\log(1-u(1-p)) + p\log(p) - (1-p)\log(u)\\ &= (1-p)\log\left(\frac{1}{u} - (1-p)\right) + p\log(p)\end{aligned}$$

ce qui prouve la fonction F' est strictement décroissante sur $[0,1]$. On a aussi $\mathrm{F}'(0^+) = +\infty$ et $\mathrm{F}'(1) = \log(p) < 0$. Par suite, il existe un unique nombre réel $u_p \in]0;1[$ tel que $\mathrm{F}'(u) = 0$; la fonction F est strictement croissante sur $[0;u_p]$ et strictement décroissante sur $[u_p;0]$, et l'on a $\mathrm{I}(\mathrm{C}) = \mathrm{F}(u_p,p)$. On peut en fait calculer u_p explicitement : on trouve

$$\frac{1}{u_p} = (1-p) + \exp(-\frac{p}{1-p}\log(p)).$$

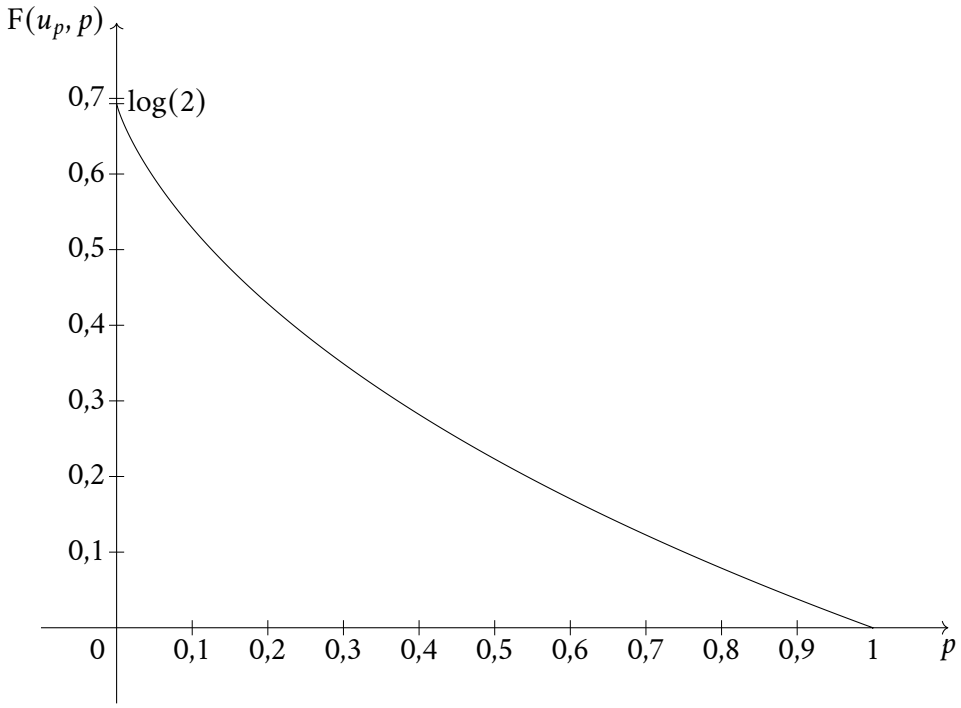


FIGURE 2.8.8.1. Graphe de la fonction $\mathrm{F}(u_p,p)$

On vérifie que la capacité du canal est décroissante avec p. Elle tend vers $\log(2)$ en 0 (le canal tend vers un canal *sans* bruit !), et vers 0 en 1 (le canal ne transmet que des 0).

Solution de l'exercice (2.7.9). — *a*) On suppose que les canaux C′ et C″ sont indépendants. Notons A l'alphabet d'entrée du canal C′, A′ son alphabet de sortie, qui

est l'alphabet d'entrée du canal C″, et B l'alphabet de sortie de C″. Alors, pour tout $a \in A$ et tout $b \in B$, on a

$$p_C(a \mid b) = \sum_{a'} p_{C'}(a \mid a') p_{C''}(a' \mid b).$$

La matrice de probabilités de transmissions du canal C est le produit des matrices de probabilités de transmissions des deux canaux C′ et C″.

b) Soit X, Z des variables aléatoires discrètes à valeurs dans A, B telles que $X \sim_C Z$. On introduit une variable aléatoire Y intermédiaire entre X et Z, le résultat de X après passage dans le canal C′, et qui fournira Z après passage dans le canal C″. On a donc $X \sim_{C'} Y$ et $Y \sim_{C''} Z$. Par définition, $I(X, Y) \leqslant I(C')$ et $I(Y, Z) \leqslant I(C'')$.

Le but est de majorer $I(X, Z)$. On remarque que X et Z sont conditionnellement indépendantes relativement à Y : le canal sans mémoire C″ reçoit Y et renvoie Z ; connaître X, la source du canal C′, n'apporte aucune information sur Z. D'après l'inégalité du traitement de données (th. 1.3.11), on a donc $I(X, Z) \leqslant I(X, Y) = I(C')$. Comme on l'a vu dans la démonstration de ce théorème, cette inégalité provient des relations

$$I(X, (Y, Z)) = I(X, Z \mid Y) + I(X, Y) = I(X, Y \mid Z) + I(X, Z),$$

de la nullité de $I(X, Z \mid Y)$ (car $X \perp_Y Z$) et de la positivité de $I(X, Y \mid Z)$. Par symétrie, on a aussi

$$I((X, Y), Z) = I(X, Z \mid Y) + I(Y, Z) = I(Y, Z \mid X) + I(X, Z),$$

ce qui entraîne

$$I(X, Z) = I(Y, Z) - I(Y, Z \mid X) \leqslant I(Y, Z).$$

En particulier, $I(C) \leqslant \inf(I(C'), I(C''))$: le canal C ne peut pas faire mieux que ce que fait chacun des deux canaux C′ et C″.

c) Soit A la matrice de probabilités de transmission du code C :

$$A = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}.$$

La matrice de probabilités de transmission du code C_n est la puissance A^n de A. On démontre que A^n est la matrice de probabilités de transmission d'un canal

symétrique binaire de paramètre $p_n = (1-(1-2p)^n)/2$: on a

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

On peut vérifier cela par récurrence, ou bien observer que A^n est symétrique (c'est la puissance d'une matrice symétrique) et que $PA^nP = A^n$, où $P = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Pour calculer la valeur du nombre réel p_n, on note que

$$\det(A^n) = \det(A)^n = \left((1-p)^2 - p^2\right)^n = (1-2p)^n = 1-2p_n.$$

On a donc $p_n = (1-(1-2p)^n)/2$, comme annoncé.

On suppose $0 < p < 1$; quand n tend vers l'infini, on a $(1-2p)^n \to 0$ et $p_n \to 1/2$. La capacité du canal C_n, égale à $\log(2) - h(p_n)$, tend donc vers $\log(2) - h(1/2) = 0$.

Solution de l'exercice (*2.7.10*). — *a*) Supposons que les variables aléatoires $\mathrm{X} = (\mathrm{X}', \mathrm{X}'')$ et $\mathrm{Y} = (\mathrm{Y}', \mathrm{Y}'')$ sont liées par le canal C, c'est-à-dire telles que

$$\mathbf{P}(\mathrm{Y} = (b', b'') \mid \mathrm{X} = (a', a'')) = p(b' \mid a')p(b'' \mid a'').$$

Par conséquent,

$$\begin{aligned}
\mathbf{P}(\mathrm{Y}' = b' \mid \mathrm{X}' = a') &= \sum_{b'' \in \mathrm{B}''} \mathbf{P}(\mathrm{Y}' = b', \mathrm{Y}'' = b'' \mid \mathrm{X}' = a') \\
&= \sum_{b'' \in \mathrm{B}''} \mathbf{P}(\mathrm{X}' = a')^{-1} \mathbf{P}(\mathrm{Y}' = b', \mathrm{Y}'' = b'', \mathrm{X}' = a') \\
&= \mathbf{P}(\mathrm{X}' = a')^{-1} \times \\
&\qquad \times \sum_{b'' \in \mathrm{B}''} \sum_{a'' \in \mathrm{A}''} \mathbf{P}(\mathrm{Y}' = b', \mathrm{Y}'' = b'', \mathrm{X}' = a', \mathrm{X}'' = a'') \\
&= \mathbf{P}(\mathrm{X}' = a')^{-1} \sum_{a'' \in \mathrm{A}''} \mathbf{P}(\mathrm{X}' = a', \mathrm{X}'' = a'') \times \\
&\qquad \times \sum_{b'' \in \mathrm{B}''} \mathbf{P}(\mathrm{Y}' = b', \mathrm{Y}'' = b'' \mid \mathrm{X}' = a', \mathrm{X}'' = a'') \\
&= \mathbf{P}(\mathrm{X}' = a')^{-1} \sum_{a'' \in \mathrm{A}''} \mathbf{P}(\mathrm{X}' = a', \mathrm{X}'' = a'') \times \\
&\qquad \times \sum_{b'' \in \mathrm{B}''} p(b' \mid a') p(b'' \mid a'') \\
&= \mathbf{P}(\mathrm{X}' = a')^{-1} \sum_{a'' \in \mathrm{A}''} \mathbf{P}(\mathrm{X}' = a', \mathrm{X}'' = a'') p(b' \mid a') \\
&= p(b' \mid a').
\end{aligned}$$

Cela signifie que les variables aléatoires X' et Y' sont liées par le canal C', et $\mathrm{I}(\mathrm{X}', \mathrm{Y}') \leqslant \mathrm{I}(\mathrm{C}')$. De même, les variables aléatoires X'' et Y'' sont liées par le canal C'' et $\mathrm{I}(\mathrm{X}'', \mathrm{Y}'') \leqslant \mathrm{I}(\mathrm{C}'')$.

b) Intuitivement, connaissant Y', la connaissance de X'' ne fournit aucune information concernant X'. De fait, pour $a' \in \mathrm{A}'$, $b' \in \mathrm{B}'$ et $a'' \in \mathrm{A}''$, on a

$$\begin{aligned}
&\mathbf{P}(\mathrm{Y}' = b', \mathrm{X}'' = a'' \mid \mathrm{X}' = a') \\
&\qquad = \mathbf{P}(\mathrm{X}'' = a'' \mid \mathrm{X}' = a') \mathbf{P}(\mathrm{Y}' = b' \mid \mathrm{X}' = a', \mathrm{X}'' = a'') \\
&\qquad = \mathbf{P}(\mathrm{X}'' = a'' \mid \mathrm{X}' = a') \sum_{b'' \in \mathrm{B}''} \mathbf{P}(\mathrm{Y}' = b', \mathrm{Y}'' = b'' \mid \mathrm{X}' = a', \mathrm{X}'' = a'') \\
&\qquad = \mathbf{P}(\mathrm{X}'' = a'' \mid \mathrm{X}' = a') \sum_{b'' \in \mathrm{B}''} p(b' \mid a') p(b'' \mid a'') \\
&\qquad = \mathbf{P}(\mathrm{X}'' = a'' \mid \mathrm{X}' = a') p(b' \mid a') \\
&\qquad = \mathbf{P}(\mathrm{X}'' = a'') \mathbf{P}(\mathrm{Y}' = b' \mid \mathrm{X}' = a'),
\end{aligned}$$

ce qui prouve que Y' et X'' sont conditionnellement indépendantes relativement à X'. La démonstration de l'autre indépendance conditionnelle est identique, par symétrie.

c) Remarquons que

$$I(X, Y) = I((X', X''), (Y', Y'')) = H(Y', Y'') - H(Y', Y'' \mid X', X'').$$

La formule

$$\mathbf{P}(Y' = b', Y'' = b'' \mid X' = a', X'' = a'') = p(b' \mid a')p(b'' \mid a'')$$

entraîne que les variables Y' et Y'' sont conditionnellement indépendantes relativement à X', X'' ; par suite,

$$H(Y', Y'' \mid X', X'') = H(Y' \mid X', X'') + H(Y'' \mid X', X'').$$

Comme Y' et X'' sont conditionnellement indépendantes relativement à X', on a également

$$H(Y' \mid X', X'') = H(Y', X'' \mid X') - H(X'' \mid X') = H(Y' \mid X').$$

De même, on a

$$H(Y'' \mid X', X'') = H(Y'' \mid X'').$$

Ainsi,

$$\begin{aligned} I(X, Y) &= H(Y', Y'') - H(Y' \mid X') - H(Y'' \mid X'') \\ &= H(Y') + H(Y'') - I(Y', Y'') - H(Y' \mid X') - H(Y'' \mid X'') \\ &= I(X', Y') + I(X'', Y'') - I(Y', Y''). \end{aligned}$$

Le premier terme est majoré par $I(C')$, le second par $I(C'')$; le troisième est positif, et est nul si et seulement si Y' et Y'' sont indépendantes. Cela démontre que $I(X, Y) \leqslant I(C') + I(C'')$, avec égalité si et seulement si Y' et Y'' sont indépendantes. En particulier, $I(C) \leqslant I(C') + I(C'')$.

Supposons maintenant que X' et X'' sont indépendantes et que leurs lois soient telles que $I(X', Y') = I(C')$ et $I(X'', Y'') = I(C'')$. Alors, Y' et Y'' sont indépendantes :

$$\begin{aligned}\mathbf{P}(Y' = b', Y'' = b'') &= \sum_{a' \in A'} \sum_{a'' \in A''} \mathbf{P}(X' = a', X'' = a'') \times \\ &\qquad \times \mathbf{P}(Y' = b', Y'' = b'' \mid X' = a', X'' = a'') \\ &= \sum_{a' \in A'} \sum_{a'' \in A''} \mathbf{P}(X' = a') \mathbf{P}(X'' = a'') p(b' \mid a') p(b'' \mid a'') \\ &= \sum_{a' \in A'} \mathbf{P}(X' = a') p(b' \mid a') \sum_{a'' \in A''} \mathbf{P}(X'' = a'') p(b'' \mid a'') \\ &= \mathbf{P}(Y' = b') \mathbf{P}(Y'' = b'').\end{aligned}$$

On a donc $I(X, Y) = I(X', Y') + I(X'', Y'') = I(C') + I(C'')$. Cela démontre que la capacité du canal C est égale à $I(C') + I(C'')$, et que la loi sur $A' \times A''$ produit des lois sur A' et A'' qui réalisent $I(C')$ et $I(C'')$ réalise cette capacité.

Solution de l'exercice (2.7.11). — *a*) Soit $a \in A''$ et $b \in B'$. La somme des probabilités conditionnelles $p_C(x \mid a)$ est égale à 1 ; on a donc

$$p_C(b \mid a) = 1 - \sum_{x \in B' \cup B'' - \{b\}} p_c(x \mid a) = 1 - \sum_{x \in B' - \{b\}} p_c(b \mid a) - \sum_{x \in B''} p_C(x \mid a).$$

Tous les termes $p_C(x \mid a)$ sont positifs ou nuls ; par ailleurs, $\sum_{x \in B''} p_C(x \mid a) = 1$. On obtient donc $p_C(b \mid a) \leqslant 0$, d'où $p_C(b \mid a) = 0$.

Un raisonnement symétrique démontre que $p_C(b \mid a) = 0$ si $b \in B''$ et $a \in A'$.

b) Soit X, Y des variables aléatoires à valeurs dans A et B respectivement, liées par le canal C : $\mathbf{P}(Y = b \mid X = a) = p_C(b \mid a)$. Soit U la variable aléatoire qui vaut 1 si $X \in A'$ et 0 si $X \in A''$. Lorsque $U = 1$, on a également $Y \in B'$; lorsque $U = 0$, on a $Y \in B''$. Posons $p = \mathbf{P}(U = 1)$. On calcule $I(X, Y)$ par conditionnement. Comme U est certaine conditionnellement à X ou Y, on a

$$\begin{aligned}I(X, Y) &= H(X) + H(Y) - H(X, Y) \\ &= H(X, U) + H(Y, U) - H(X, Y, U) \\ &= H(U) + H(X \mid U) + H(Y \mid U) - H(X, Y \mid U) \\ &= H(U) + I(X, Y \mid U).\end{aligned}$$

Par ailleurs,

$$I(X, Y \mid U) = \mathbf{P}(U = 0) I(X, Y \mid U = 0) + \mathbf{P}(U = 1) I(X, Y \mid U = 1).$$

Une fois conditionné à l'évènement $U = 0$, le couple (X, Y) se comporte comme un couple de variables aléatoires liées par le canal C' ; on a donc $I(X, Y \mid U = 0) \leqslant I(C'')$. De même, $I(X, Y \mid U = 1) \leqslant I(C')$. Par suite,

$$I(X, Y) \leqslant (1 - p)(I(C'') - \log(1 - p) + p(I(C') - \log(p)).$$

Notons $f(p)$ le membre de droite de cette inégalité. C'est une fonction continue de $p \in [0; 1]$, strictement concave (car somme de la fonction strictement concave $h(p)$ et d'une fonction affine) ; elle vaut $I(C'')$ en $p = 0$ et $I(C')$ en $p = 1$. Elle atteint son maximum en un unique point $p \in [0; 1]$. Plus précisément, f est dérivable sur l'intervalle $]0; 1[$ et sa dérivée est donnée par

$$\begin{aligned} f'(p) &= I(C') - \log(p) - 1 - I(C'') + \log(1 - p) + 1 \\ &= I(C') - I(C'') - \log(p) + \log(1 - p). \end{aligned}$$

La fonction $p \mapsto -\log(p) + \log(1 - p)$ est strictement décroissante, car sa dérivée, donnée par $p \mapsto -1/p - 1/(1 - p)$, est strictement négative. Par ailleurs, f' tend vers $+\infty$ en 0 et vers $-\infty$ en 1 ; il existe donc un unique nombre réel p tel que $f'(p) = 0$; la fonction f est alors strictement croissante sur $[0; p]$ et strictement décroissante sur $[p; 1]$, et l'on a $\sup(f) = f(p)$. La relation $f'(p) = 0$ entraîne $\log(1/p - 1) = I(C'') - I(C')$, donc $1/p - 1 = e^{I(C'')}/e^{I(C')}$ et

$$p = \frac{e^{I(C')}}{e^{I(C')} + e^{I(C'')}}.$$

Pour simplifier les notations, posons $\gamma' = e^{I(C')}$ et $\gamma'' = e^{I(C'')}$; on a alors

$$I(C') - \log(p) = \log(\gamma') - \log\Big(\frac{\gamma'}{\gamma' + \gamma''}\Big) = \log(\gamma' + \gamma'')$$

et, par symétrie,

$$I(C'') - \log(1 - p) = \log(\gamma' + \gamma'').$$

Ainsi,

$$\begin{aligned} f(p) &= p(I(C') - \log(p)) + (1 - p)(I(C'') - \log(1 - p)) \\ &= p \log(\gamma' + \gamma'') + (1 - p) \log(\gamma' + \gamma'') \\ &= \log(\gamma' + \gamma''). \end{aligned}$$

On a donc $I(X, Y) \leqslant \log(\gamma' + \gamma'')$, soit encore

$$e^{I(C)} \leqslant e^{I(C')} + e^{I(C'')}.$$

Pour démontrer qu'il y a égalité, choisissons des variables aléatoires X' et X'', à valeurs dans A' et A'' respectivement, qui réalisent les capacités $I(C')$ et $I(C'')$ et qui sont indépendantes. Soit U une variable de Bernoulli de paramètre p (c'est-à-dire que $\mathbf{P}(U = 1) = p$ et $\mathbf{P}(U = 1) = 1 - p$, indépendante du couple (X', X''). Définissons une variable aléatoire X par : $X = X'$ si $U = 1$, et $X = X''$ si $U = 0$; définissons également Y de sorte que $X \sim_C Y$. Les calculs précédents démontrent que $I(X, Y) = f(p) = \log(e^{I(C')} + e^{I(C'')})$. Par suite, $I(C) = \log(e^{I(C')} + e^{I(C'')})$ et la loi de la variable X réalise cette capacité.

Solution de l'exercice (2.7.12). — *a*) On suppose que le symbole 0 a coût c_0 et que le symbole 1 a coût c_1 ; par hypothèse, on a $p(1 \sim 0) = p(0 \sim 1) = p$. Soit (X, Y) un couple de variables aléatoires telles que $X \sim_C Y$. Notons $u = \mathbf{P}(X = 0)$ et $v = \mathbf{P}(Y = 0)$; comme on a vu dans le calcul de la capacité d'un canal symétrique binaire, on a $H(Y \mid X) = h(p)$. On a aussi $v = (1 - p)\mathbf{P}(X = 0) + p\mathbf{P}(X = 1) = (1 - p)u + p(1 - u) = u + p - 2up$, de sorte que

$$I(X, Y) = h(u(1 - 2p) + p) - h(p),$$

expression qu'il faut maximiser. Pour simplifier, on suppose $p \leqslant 1/2$; la fonction $u \mapsto u(1-2p)+p$ est alors affine croissante, d'image $[p; 1-p]$ lorsque $u \in [0; 1]$, et $I(X, Y)$ est maximal lorsque $u = 1/2$, c'est-à-dire quand X est uniforme, et alors Y est uniforme. Dans ce cas, on trouve $I(X, Y) = 1 - h(p)$, la capacité du canal symétrique binaire C.

Il faut cependant prendre en compte la condition de coût. On a $\mathbf{E}(c(X)) = uc_0+(1-u)c_1$, de sorte que la condition $\mathbf{E}(c(X)) \leqslant \gamma$ équivaut à $(c_0-c_1)u \leqslant \gamma-c_1$.

Si $u = 1/2$ satisfait cette condition, c'est-à-dire si $(c_0+c_1)/2 \leqslant \gamma$, alors $I(C, \gamma) = 1 - h(p)$ pour $\gamma \geqslant (c_0 + c_1)/2$. C'est notamment le cas lorsque c_0, c_1 sont tous deux $\leqslant \gamma$.

À l'inverse, si $\gamma < \sup(c_0, c_1)1$, aucune loi sur X ne convient : la condition de coût ne peut pas être satisfaite puisque le coût de chaque symbole est supérieur au coût autorisé. La borne supérieure qui définit $I(C, \gamma)$ est prise dans $\mathbf{R}_+$, ce qui donne $I(C, \gamma) = 0$.

Supposons maintenant que $(c_0 + c_1)/2 > \gamma$ mais que $\inf(c_0, c_1) \leqslant \gamma$. Il y a deux cas, suivant que $c_0 < c_1$ ou $c_1 < c_0$. Supposons d'abord $c_0 < c_1$. La condition $\mathbf{E}(c(X)) \leqslant \gamma$ devient $u \leqslant (c_1 - \gamma)/(c_1 - c_0)$, cette expression étant $< 1/2$ par

hypothèse. C'est la valeur de u pour laquelle $\mathrm{I}(\mathrm{X},\mathrm{Y})$ est maximale. Cela donne

$$\mathrm{I}(\mathrm{C},\gamma) = h\big(\frac{c_1-\gamma}{c_1-c_0}(1-p) + \frac{\gamma-c_0}{c_1-c_0}p\big) - h(p).$$

Si $c_0 > c_1$, la condition $\mathbf{E}(c(\mathrm{X})) \leqslant \gamma$ devient $u \geqslant (\gamma - c_1)/(c_0 - c_1)$, cette expression étant $> 1/2$ par hypothèse. C'est la valeur de u pour laquelle $\mathrm{I}(\mathrm{X},\mathrm{Y})$ est maximale. Cela donne la même formule pour $\mathrm{I}(\mathrm{C},\gamma)$.

b) Les calculs sont tout à fait analogues. Par symétrie, on obtient

$$\mathrm{H}(\mathrm{Y} \mid \mathrm{X}) = h(q,p,\dots,p) = -q\log(q) - (d-1)p\log(p).$$

Si $u_j = \mathbf{P}(\mathrm{X}=j)$ et $v_j = \mathbf{P}(\mathrm{Y}=j)$, on a

$$v_j = q\mathbf{P}(\mathrm{X}=j) + \sum_{k\neq j} p\mathbf{P}(\mathrm{X}=k) = qu_j + p(1-u_j)$$

de sorte que

$$\mathrm{H}(\mathrm{Y}) = -\sum_{j=1}^{d} v_j\log(v_j) = \sum_{j=1}^{d}\lambda(p+(1-dp)u_j),$$

où $\lambda(x) = -x\log(x)$. On a ainsi la formule

$$\mathrm{I}(\mathrm{X},\mathrm{Y}) = \mathrm{H}(\mathrm{Y}) - \mathrm{H}(\mathrm{Y}\mid\mathrm{X}) = \sum_{j=1}^{d}\lambda(p+(1-dp)u_j) + q\log(q) + (d-1)p\log(p),$$

expression qui est maximale lorsque X est uniforme ($u_j = 1/d$ pour tout j), de sorte que Y est encore uniforme, $\mathrm{H}(\mathrm{Y}) = \log(d)$, et

$$\mathrm{I}(\mathrm{C}) = \log(d) + q\log(q) + (d-1)p\log(p).$$

Prenons maintenant en compte le coût des symboles. Si c_j est le coût du symbole j, on a aussi

$$\mathbf{E}(c(\mathrm{X})) = \sum_{j=1}^{d} c_j u_j.$$

Dans le cas où $(\sum_{j=1}^{d} c_j)/d \leqslant \gamma$, la solution $u_j = 1/d$ est admissible et on obtient

$$\mathrm{I}(\mathrm{C},\gamma) = \mathrm{I}(\mathrm{C}).$$

À l'inverse, si $c_j > \gamma$ pour tout j, il n'y a pas de possibilité de respecter la condition et on obtient $\mathrm{I}(\mathrm{C},\gamma) = 0$.

Reste à traiter le cas intermédiaire, quand $\inf(c_j) \leqslant \gamma < (\sum c_j)/d$, et il ne semble pas aisé de donner une formule explicite. La question revient à maximaliser une fonction concave

$$(u_1, \dots, u_d) \mapsto \sum_{j=1}^{d} \lambda(p + (1 - dp)u_j)$$

sur le polytope convexe compact de $\mathbf{R}^d$ défini par les relations

$$u_1, \dots, u_d \geqslant 0, \quad \sum_{j=1}^{d} u_j = 1, \quad \sum_{j=1}^{d} c_j u_j \leqslant \gamma.$$

On sait que ce maximum est atteint sur un sous-ensemble convexe et compact Λ de ce polytope. On verra a posteriori qu'on peut négliger les conditions de positiver sur les u_j, et le théorème des extrémas liés affirme que pour $u \in \Lambda$, le vecteur $(1-dp)(\lambda'(p+(1-dp)u_1), \dots, \lambda'(p+(1-dp)u_d))$ est multiple du vecteur $(1, \dots, 1)$ si $\sum c_j u_j < \gamma$, et est combinaison linéaire des vecteurs $(1, \dots, 1)$ et $(c_1, \dots, c_d)$ sinon. Le premier cas entraîne que tous les u_j sont égaux, puis que $u_j = 1/d$ pour tout j, ce qui est impossible en raison de l'hypothèse $(\sum c_j)/d > \gamma$. Il existe donc $a, b \in \mathbf{R}$ tels que $\lambda'(u_j) = a + bc_j$ pour tout j. Comme $\lambda'(x) = -1 - \log(x)$, on modifie les notations et on écrit

$$-\log(p + (1 - dp)u_j) = a + bc_j.$$

Cela donne $p + (1 - dp)u_j = e^{-a}e^{-bc_j}$ puis

$$u_j = \frac{1}{1 - dp} e^{-a} e^{-bc_j} - \frac{p}{1 - dp}.$$

Posons $\mathrm{F}(b) = \sum_{j=1}^{d} e^{-bc_j}$. La condition $\sum u_j = 1$ entraîne

$$e^{-a}\mathrm{F}(b) = 1,$$

d'où

(2.8.12.1)
$$u_j = \frac{1}{(1 - dp)\mathrm{F}(b)} e^{-bc_j} - \frac{p}{1 - dp}.$$

La condition $\sum c_j u_j = \gamma$ devient alors

$$\frac{1}{(1 - dp)\mathrm{F}(b)} \sum c_j e^{-bc_j} = \gamma + \frac{p}{1 - dp} \sum c_j,$$

d'où

(2.8.12.2) $$(1-dp)\gamma + dp\overline{\gamma} = -\frac{\mathrm{F}'(b)}{\mathrm{F}(b)}.$$

On a posé $\overline{\gamma} = (\sum c_j)/d$, le coût qu'il faudrait autoriser pour utiliser la loi uniforme sur X. Il reste à observer que la fonction $b \mapsto -\mathrm{F}'(b)/\mathrm{F}(b)$ est strictement croissante : sa dérivée est $(\mathrm{F}'^2 - \mathrm{F}\mathrm{F}'')/\mathrm{F}^2$; le numérateur est

$$(\sum c_j e^{-bc_j})^2 - (\sum e^{-bc_j})(\sum c_j^2 e^{-bc_j}),$$

donc est positif d'après l'inégalité de Cauchy–Schwarz ; il ne s'annule que si les c_j sont tous égaux, ce qui n'est pas le cas puisque $\inf(c_j) \leqslant \gamma < \overline{\gamma}$. Quand $b \to 0$, $-\mathrm{F}'(b)/\mathrm{F}(b)$ tend vers $(\sum c_j)/d = \overline{\gamma}$; quand $b \to +\infty$, $-\mathrm{F}'(b)/\mathrm{F}(b)$ tend vers $\inf(c_j)$. Comme $\inf(c_j) \leqslant \gamma < (1-dp)\gamma + dp\overline{\gamma} < \overline{\gamma}$, il existe un unique nombre réel $b \in \mathbf{R}_+^*$ tel que l'équation (2.8.12.2) soit vérifiée. Les relations (2.8.12.1) fournissent alors les u_j.

CHAPITRE 3

ÉCHANTILLONAGE

Ce dernier chapitre aborde un autre aspect de l'œuvre de Shannon en théorie de l'information, le théorème d'échantillonage qui garantit la possibilité de ne conserver d'un signal que des valeurs successives, régulièrement espacées, pourvu que la fréquence d'échantillonage soit au moins le double des fréquences qui « apparaissent » dans le signal.

C'est par la théorie des séries de Fourier et de la transformation de Fourier qu'on donne un sens mathématique rigoureux à cette expression. De manière imagée, cette théorie est un miroir entre une présentation d'un signal selon le temps (quelle amplitude à quel moment ?) et une présentation selon les fréquences (quels sons élémentaires ?). L'efficacité que procure la combinaison de ces deux points de vue justifie l'importance de la théorie de Fourier dans tous les domaines des mathématiques, aussi bien « purs » qu'« appliqués ».

Les séries de Fourier s'intéressent au signaux périodiques, qu'on peut reconstruire en combinant des signaux de fréquences multiples de la fréquence fondamentale. La transformation de Fourier traite le cas des signaux plus généraux ; s'il faudra faire ici l'hypothèse que leur « énergie » est finie, la théorie des distributions tempérées permettrait de s'en affranchir.

Si le cadre des deux premiers chapitres était celui de la théorie des probabilités, celui de ce troisième chapitre relève plutôt de l'analyse. Pour ne pas présupposer la connaissance de la théorie de Lebesgue (espaces L^p, etc.), nous avons fait le choix de ne pas toujours donner des démonstrations complètes.

Nous pouvons alors démontrer le théorème d'échantillonage, ainsi que faire le lien avec la formule de Poisson.

Un dernier paragraphe aborde le *principe d'incertitude* : un signal ne peut pas être simultanément trop localisé en temps et en fréquence. Fameux dans le contexte

de la mécanique quantique, nous verrons que le principe d'incertitude s'incarne aussi en théorie de l'information.

3.1. Signaux continus et signaux discrets

Considérons un signal ; ce peut être le chant d'une artiste, représenté par exemple par la pression d'air exercée au cours du temps sur un microphone, ou un signal visuel, tel une image à photographier, alors représentée par la luminosité émise par chaque point de la scène. *Échantillonner* ce signal, c'est le mesurer à divers instants, ou à divers lieux, souvent régulièrement espacés ; cela transforme ainsi un signal continu (une fonction du temps) en un signal discret (une suite de valeurs). La question de l'échantillonnage est apparue très tôt en théorie de la communication. Les ingénieurs l'ont par exemple utilisée dès le milieu du XIX^{e} siècle pour faire passer plusieurs signaux sur un même canal. Elle est aujourd'hui fondamentale pour le traitement numérique du signal puisque les ordinateurs ne manipulent qu'une quantité finie d'information.

D'ailleurs, les ordinateurs doivent faire plus qu'échantillonner : ils doivent également *quantifier* le signal c'est-à-dire transformer une valeur continue (la pression, une tension électrique) en une valeur discrète, que l'on peut représenter sur 8 bits ou 16 bits, par exemple...). C'est cette combinaison échantillonnage/quantification, et la reconstruction ultérieure du signal, qui est au cœur de l'ingéniérie du traitement du signal.

Comme l'indique son titre, nous nous contenterons dans ce chapitre de la question de l'échantillonnage en démontrant que l'*on peut reconstruire un signal échantillonné s'il ne contenait pas de fréquences supérieures à la moitié de la fréquence d'échantillonnage.* Dit autrement, si l'on échantillonne un signal à une fréquence au moins deux fois supérieure à celles qu'il contient, on pourra le reconstruire exactement, au moins théoriquement. Ce théorème mathématique est le plus souvent attribué à Shannon, car il apparaît semble-t-il, pour la première fois dans Shannon (1949). Cependant, Shannon y insiste que ce résultat était *common knowledge in the communication art ;* l'idée de l'échantillonnage à une fréquence double était également bien connue de H. Nyquist. C'est pourquoi on trouve aussi l'appellation *théorème de Nyquist–Shannon*.

La preuve de ce théorème repose sur la théorie des séries et de la transformation de Fourier qui permet de décomposer tout signal en une combinaison de signaux trigonométriques « purs ». C'est aussi cette théorie qui fournira une définition

précise de l'ensemble des *fréquences* qui apparaissent dans un signal donné — ce sera le support de sa transformée de Fourier.

La considération d'un tel signal trigonométrique pur explique déjà la nécessité de l'échantillonnage à la fréquence de Nyquist. Si la fonction F définie par $\mathrm{F}(t) = \sin(\omega t)$ (de période $2\pi/\omega$, de fréquence $f = \omega/2\pi$) est échantillonnée à la fréquence double ω/π, on obtient les données $\mathrm{F}(n\pi/\omega) = \sin(n\pi) = 0$. On ne peut donc distinguer le signal F du signal nul !

Nous pouvons aussi expliquer tout de suite la façon dont ce théorème, appliqué aux signaux sonores, intervient dans la vie de tous les jours.

Les sons simples que nous percevons, ceux d'une voix chantée, d'un instrument de musique, etc., ont une *fréquence fondamentale* f_1, qui détermine la note (do, ré,…) que nous attribuerons à ce son. Lorsque cette fréquence fondamentale est doublée, nous entendons la « même » note, à l'octave supérieur, et ce qui fait la richesse de ces sons est qu'ils « contiennent » des *harmoniques*, c'est-à-dire des fréquences multiples $f_2 = 2f_1$, $f_3 = 3f_1$,…, de la fréquence fondamentale. C'est notre perception du son qui unifie toutes ces signaux en un son unique. Au subtilités (fondamentales) des gammes près, lorsque la fréquence fondamentale f_1 correspond à un do, les harmoniques suivantes correspondent, $f_2 = 2f_1$ au do de l'octave supérieur, $f_3 = 3f_1$ au sol de cet octable, $f_4 = 4f_1$ au do de l'octave encore supérieur, puis $f_5 = 5f_1$ au mi de cet octave et $f_6 = 6f_1$ au sol de cet octave, un octave plus haut que la troisième harmonique $f_3 = 3f_1$. On devine là d'où provient l'impression de solidité que procure l'accord « parfait » (do-mi-sol, par exemple) en harmonie classique.

Nous avons indiqué figure 3.1.0.1 le spectre des fréquences fondamentales (arrondies au Hz le plus proche) de quelques instruments de musique. Elle ne tient pas compte des harmoniques qui, nous l'avons dit, sont responsables de la nature du son ; disons que les 10 premières harmoniques ont une importance. Cette figure tient encore moins compte des fréquences *anharmoniques* qui existent également, mais dans une proportion bien plus faible. (Dans certains instruments, tels les toms d'une batterie, les fréquences anharmoniques sont très présentes, si bien qu'on peut difficilement leur attribuer une note, mais la façon dont l'instrument est joué, la baguette utilisée par exemple, influe beaucoup sur le son et même sur sa hauteur.)

La perception des sons dépend ensuite du fonctionnement de notre oreille, du tympan qui transforme les oscillations de la pression de l'air en vibrations

piano		27,5 Hz	4 186 Hz
saxophone	soprano	233 Hz	1480 Hz
	alto	139 Hz	831 Hz
	ténor	104 Hz	659 Hz
	baryton	65 Hz	440 Hz
batterie –	cymbales	200 Hz	10 000 Hz
	caisse claire	240 Hz	6 000 Hz
	toms	120 Hz	5 000 Hz
	grosse caisse	60 Hz	4 000 Hz
voix –	soprano	261 Hz	1 047 Hz
	ténor	123 Hz	440 Hz
	basse	82 Hz	300 Hz
violon		196 Hz	2 794 Hz

FIGURE 3.1.0.1. Domaines de fréquences de quelques instruments de musique

mécaniques qu'il transmet à la cochlée, un petit os en forme de limaçon rempli d'un liquide où des milliers de cellules ciliées réagissent aux diverses fréquences du son et les transforment en signal nerveux. Ainsi, l'oreille humaine est sensible aux signaux de fréquences variant de 20 Hz à 20 000 Hz ; selon la page WIKIPEDIA (2005), des conditions idéales permettent d'observer une sensibilité plus large, de 12 Hz à 28 000 Hz, et la partie où l'audition est le plus efficace est entre 2 000 et 5 000 Hz.

En conclusion, pour les applications aux signaux sonores, on peut prendre pour fréquence de Nyquist toute fréquence supérieure à 40 000 Hz. Celle choisie par la norme Audio-CD est 44,1 kHz permet donc, en théorie, de recréer tout le spectre audible d'un signal. Si l'on se contente d'un signal de moindre qualité, on peut bien sûr échantillonner à une fréquence plus basse, par exemple 8 000 Hz pour des téléphones basiques ou le protocole VoIP (*Voice over IP*).

Pour terminer cette introduction technologique, rappelons qu'en plus d'être échantillonnés, les signaux doivent être quantifiés. La norme Audio-CD, par exemple, les code sur 16 bits (2 octets), d'où, en principe, pour un signal stéréo, une quantité d'information de 176 kO par seconde. En fait, selon cette norme, 6 échantillons sont regroupés en un *frame* de 192 bits (24 octets), auquel s'ajoutent

8 octets de code correcteur d'erreur et un octet de contrôle (*subcode*) ; finalement, ce sont 33 octets pour 6 échantillons, d'où une quantité d'information de 242 kO par seconde. La durée d'un CD musical est ainsi de l'ordre d'une heure. L'utilisation d'algorithmes de compression permet d'y stocker un signal plus long ; c'est ainsi que certains CDs contiennent, non pas, un signal comme décrit ci-dessus, mais des fichiers compressés selon la norme MP3.

La plus grande partie de ce chapitre est consacrée à rappeler la théorie des séries de Fourier et de la transformation de Fourier. Même si ce sont deux exemples d'une théorie qui les englobe, l'analyse harmonique sur les groupes abéliens localement compacts, la tradition pédagogique et leur importance pratique conduit à les présenter successivement.

3.2. Série de Fourier d'une fonction périodique

3.2.1. — La théorie des *séries de Fourier* permet l'analyse fréquentielle des fonctions périodiques. Elle repose sur l'observation qu'une fonction trigonométrique $t \mapsto \exp(i\omega t)$ est de période T si et seulement si ω est un multiple entier de $2\pi/\mathrm{T}$, et sur l'idée que « toute » fonction de période T est, en un sens qu'il faudra préciser, *somme* de telles fonctions trigonométriques.

La seule hypothèse que doit vérifier une fonction f sur $\mathbf{R}$ pour que l'on puisse envisager sa série de Fourier est d'être *localement intégrable* au sens de la théorie de Lebesgue, ce qui permettra de calculer son intégrale sur tout intervalle borné. Un cadre plus restrictif, mais souvent suffisant, est celui des *fonctions continues par morceaux*.

3.2.2. — Soit k un entier $\geqslant 0$. On dit qu'une fonction f définie sur un intervalle compact $[a, b]$ de $\mathbf{R}$ est de *classe $\mathscr{C}^k$ par morceaux* s'il existe une suite finie croissante $(a_0, a_1, \ldots, a_n)$ de nombres réels telle que $a_0 = a$, $a_n = b$, et telle que pour tout entier $p \in \{1, \ldots, n\}$, la fonction f soit de classe $\mathscr{C}^k$ sur $]a_{p-1}, a_p[$ et ait, ainsi que toutes ses dérivées d'ordres $\leqslant k$, une limite à droite en a_{p-1} et une limite à gauche en a_p.

Si f est définie sur un intervalle arbitraire de $\mathbf{R}$, on dit qu'elle est de classe $\mathscr{C}^k$ par morceaux si c'est le cas de sa restriction à tout intervalle compact contenu dans son intervalle de définition.

Si f est une fonction de classe $\mathscr{C}^k$ par morceaux, on notera abusivement $f^{(k)}$ sa dérivée k-ième ; elle est définie seulement presque partout, plus précisément sauf sur un ensemble dont la trace sur tout intervalle compact est finie.

Lemme **(3.2.3)**. — a) *Soit $f : [a;b] \to \mathbf{C}$ une fonction de classe $\mathscr{C}^1$ par morceaux et continue. On a*

$$\int_a^b f'(t)\,dt = f(b) - f(a).$$

b) *Soit $u, v : [a;b] \to \mathbf{C}$ des fonctions de classe $\mathscr{C}^1$ par morceaux et continues. On a la formule d'intégration par parties :*

$$\int_a^b u'(t)v(t)\,dt = [u(t)v(t)]_a^b - \int_a^b u(t)v'(t)\,dt.$$

Démonstration. — *a*) Soit $(a_0, \ldots, a_n)$ une suite finie, croissante, telle que $a = a_0$, $b = a_n$, et telle que f soit de classe $\mathscr{C}^1$ sur chaque intervalle $]a_{k-1}, a_k[$. Si x et y sont des éléments de $]a_{k-1}, a_k[$ tels que $a_{k-1} < x \leqslant y < a_k$, on a

$$\int_x^y f'(t)\,dt = f(y) - f(x),$$

par la formule fondamentale du calcul différentiel et intégral. Lorsqu'on fait tendre x vers a_{k-1} par valeurs supérieures et y vers a_k par valeurs inférieures, $f(x)$ tend vers $f(a_{k-1})$ et $f(y)$ tend vers $f(a_k)$, parce que f est continue. On obtient alors

$$\int_{a_{k-1}}^{a_k} f'(t)\,dt = f(a_k) - f(a_{k-1}).$$

Finalement, on a

$$\int_a^b f'(t)\,dt = \sum_{k=1}^n \int_{a_{k-1}}^{a_k} f'(t)\,dt = \sum_{k=1}^n (f(a_k) - f(a_{k-1})) = f(b) - f(a).$$

b) La preuve de la seconde formule est analogue. Plus simplement, on peut observer que la fonction f définie par $f(t) = u(t)v(t)$ est également de classe $\mathscr{C}^1$ par morceaux et continue, et que l'on a $f'(t) = u'(t)v(t) + u(t)v'(t)$ pour tout $t \in [a;b]$, sauf pour un nombre fini d'exceptions. En appliquant la formule *a*) à cette fonction f, on retrouve la formule *b*). □

Définition **(3.2.4)**. — *Soit* $f : \mathbf{R} \to \mathbf{C}$ *une fonction localement intégrable, de période* $\mathrm{T} > 0$. *Ses* coefficients de Fourier *sont les nombres complexes :*

$$\textbf{(3.2.4.1)} \qquad a_n(f) = \frac{2}{\mathrm{T}} \int_0^{\mathrm{T}} f(t) \cos(2\pi nt/\mathrm{T})\, dt,$$

$$\textbf{(3.2.4.2)} \qquad b_n(f) = \frac{2}{\mathrm{T}} \int_0^{\mathrm{T}} f(t) \sin(2\pi nt/\mathrm{T})\, dt,$$

$$\textbf{(3.2.4.3)} \qquad c_n(f) = \frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} f(t) e^{-2i\pi nt/\mathrm{T}}\, dt,$$

pour $n \in \mathbf{Z}$.

Comme les fonctions intégrées sur de période T, on peut en fait intégrer sur n'importe quel intervalle de longueur T ; en particulier, il est parfois utile de considérer l'intervalle $[-\mathrm{T}/2; \mathrm{T}/2]$.

Ces coefficients ne sont pas indépendants. La parité de la fonction cosinus et l'imparité de la fonction sinus entraînent que l'on a $a_{-n}(f) = a_n(f)$ et $b_{-n}(f) = -b_n(f)$ pour tout entier n ; en particulier, $b_0(f) = 0$. De même, en décomposant l'exponentielle complexe

$$e^{-2i\pi nt/\mathrm{T}} = \cos(2\pi nt/\mathrm{T}) - i \sin(2\pi nt/\mathrm{T}),$$

on obtient les formules

$$\textbf{(3.2.4.4)} \quad c_n(f) = \frac{1}{2}(a_n(f) - ib_n(f)) \qquad \text{et} \qquad c_{-n}(f) = \frac{1}{2}(a_n(f) + ib_n(f)),$$

que l'on peut inverser en

$$\textbf{(3.2.4.5)} \qquad a_n(f) = c_n(f) + c_{-n}(f) \qquad \text{et} \qquad b_n(f) = i(c_n(f) - c_{-n}(f)).$$

Ainsi, dans la pratique, il suffira de travailler avec les coefficients c_n ; Ils sont linéaires en f :

$$c_n(\lambda f) = \lambda c_n(f), \qquad c_n(f + g) = c_n(f) + c_n(g),$$

et de même pour les coefficients a_n et b_n.

Les fonctions cosinus et sinus sont à valeurs réelles, tandis que la conjugaison complexe change $e^{-2i\pi nt/\mathrm{T}}$ en $e^{2i\pi nt/\mathrm{T}}$. Par suite, on a aussi

$$a_n(\overline{f}) = \overline{a_n(f)}, \qquad b_n(\overline{f}) = \overline{b_n(f)}, \qquad c_n(\overline{f}) = \overline{c_{-n}(f)}.$$

Notons $\check{f}$ la fonction $t \mapsto f(-t)$; elle est également de période T. En faisant le changement de variables $t' = -t$ dans l'intégrale qui définit ses coefficients de Fourier, on trouve

$$a_n(\check{f}) = a_n(f), \qquad b_n(\check{f}) = -b_n(f), \qquad c_n(\check{f}) = c_{-n}(f).$$

En particulier, si f est paire ($\check{f} = f$), ses coefficients b_n sont nuls, tandis que si f est impaire ($\check{f} = -f$), ses coefficients a_n sont nuls.

3.2.5. — Soit encore une fonction f, définie sur $\mathbf{R}$, localement intégrable et de période T. Sa *série de Fourier* est la série (illimitée dans les deux directions)

$$\sum_{n\in\mathbf{Z}} c_n(f)e^{2\pi int/\mathrm{T}}. \tag{3.2.5.1}$$

Sa série de Fourier « réelle » est la série

$$\frac{1}{2}a_0(f) + \sum_{n=1}^{\infty} \left(a_n(f)\cos(2\pi nt/\mathrm{T}) + b_n(f)\sin(2\pi nt/\mathrm{T})\right). \tag{3.2.5.2}$$

Notons qu'elles dépendent de t : ce ce sont des séries de fonctions. À ce stade là du cours, on n'affirme pas encore que ces séries convergent, ce n'est d'ailleurs pas toujours le cas, et encore moins qu'elles convergent vers $f(t)$.

Pour tout entier $n \geqslant 0$, on notera

$$\mathrm{S}_n(f)(t) = \sum_{p=-n}^{n} c_p(f)e^{2\pi ipt/\mathrm{T}}. \tag{3.2.5.3}$$

Si l'on exprime les coefficients c_p en fonction de a_p et b_p, on obtient l'égalité

$$\mathrm{S}_n(f) = \frac{1}{2}a_0(f) + \sum_{p=1}^{n} \left(a_p(f)\cos(2\pi pt/\mathrm{T}) + b_p(f)\sin(2\pi pt/\mathrm{T})\right), \tag{3.2.5.4}$$

qui justifie la définition (3.2.5.2) de la série de Fourier réelle de la fonction f. En effet, on a :

$$\begin{aligned}
\mathrm{S}_n(f)(t) &= c_0(f) + \sum_{p=1}^{n} \big(c_p(f)(\cos(2\pi pt/\mathrm{T}) + i\sin(2\pi pt/\mathrm{T})) \\
&\qquad + c_{-p}(f)(\cos(2\pi pt/\mathrm{T}) - i\sin(2\pi pt/\mathrm{T}))\big) \\
&= \frac{1}{2}a_0(f) + \sum_{p=1}^{n} \big((c_p(f) + c_{-p}(f))\cos(2\pi pt/\mathrm{T}) \\
&\qquad + i(c_p(f) - c_{-p}(f))\sin(2\pi pt/\mathrm{T})\big) \\
&= \frac{1}{2}a_0(f) + \sum_{p=1}^{n} \big(a_p(f)\cos(2\pi pt/\mathrm{T}) + b_p(f)\sin(2\pi t/\mathrm{T})\big)\,.
\end{aligned}$$

Exemple **(3.2.6)**. — On dit que f est un *polynôme trigonométrique* si c'est une combinaison linéaire (finie) de fonctions de la forme $t \mapsto e^{2i\pi pt/\mathrm{T}}$, autrement dit s'il existe un entier $\mathrm{N} \geqslant 0$ et une famille $(c_p)_{-\mathrm{N}\leqslant p\leqslant \mathrm{N}}$ de nombres complexes telle que

$$f(t) = \sum_{p=-\mathrm{N}}^{\mathrm{N}} c_p e^{2i\pi pt/\mathrm{T}}.$$

En décomposant l'exponentielle en cosinus et sinus, cela revient aussi à l'existence de deux familles $(a_p)_{0\leqslant p\leqslant \mathrm{N}}$ et $(b_p)_{1\leqslant p\leqslant \mathrm{N}}$ de nombres complexes tels que

$$f(t) = \frac{1}{2}a_0 + \sum_{p=1}^{\mathrm{N}} a_p\cos(2\pi pt/\mathrm{T}) + b_p\sin(2\pi pt/\mathrm{T}),$$

les a_p, b_p et c_p étant reliés par les formules $a_0 = 2c_0$, $a_p = c_p + c_{-p}$ et $b_p = i(c_p - c_{-p})$ pour $p \in \{1,\dots,\mathrm{N}\}$ dans un sens, et $c_0 = \frac{1}{2}a_0$, $c_p = \frac{1}{2}(a_p - ib_p)$ et $c_{-p} = \frac{1}{2}(a_p - ib_p)$ pour $p \in \{1,\dots,n\}$ dans l'autre sens.

Ses coefficients de Fourier vérifient précisément $c_n(f) = c_n$, si $|n| \leqslant \mathrm{N}$, $a_n(f) = a_n$ si $0 \leqslant n \leqslant \mathrm{N}$, $b_n(f) = b_n$ si $1 \leqslant n \leqslant \mathrm{N}$, et tous ses autres coefficients sont nuls. Pour le démontrer, il suffit, par linéarité, de traiter le cas où $f(t) = e^{2i\pi pt/\mathrm{T}}$. Dans ce cas, on a

$$c_n(f) = \frac{1}{\mathrm{T}}\int_0^{\mathrm{T}} e^{2i\pi pt/\mathrm{T}}e^{-2i\pi nt/\mathrm{T}}\,dt = \frac{1}{\mathrm{T}}\int_0^{\mathrm{T}} e^{2i\pi(p-n)t/\mathrm{T}}\,dt.$$

Lorsque $n = p$, on obtient

$$c_p(f) = \frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} 1 \, dt = 1,$$

tandis que si $n \neq p$, on a

$$c_n(f) = \frac{1}{\mathrm{T}} \left[\frac{\mathrm{T}}{2i\pi(p-n)} e^{2i\pi(p-n)t/\mathrm{T}} \right]_0^{\mathrm{T}} = 0.$$

Les formules pour $a_n(f)$ et $b_n(f)$ s'en déduisent.

On observe alors que pour tout entier n tel que $n \geqslant \mathrm{N}$, on a $\mathrm{S}_n(f)(t) = f(t)$.

Exemple **(3.2.7)**. — Supposons que f soit une fonction de classe $\mathscr{C}^1$ sur $\mathbf{R}$, de période T. Dans ce cas, sa dérivée f' est une fonction continue, également de période T, donc dispose de coefficients de Fourier. Montrons comment on peut, par intégration par parties, les calculer en fonction de ceux de f. En effet, pour tout entier n, on a

$$\begin{aligned} c_n(f') &= \frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} f'(t) e^{-2\pi int/\mathrm{T}} \, dt \\ &= \frac{1}{\mathrm{T}} \left[f(t) e^{-2\pi int/\mathrm{T}} \right]_0^{\mathrm{T}} - \frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} f(t)(-2\pi in/\mathrm{T}) e^{-2\pi int/\mathrm{T}} \, dt \\ &= \frac{2\pi in}{\mathrm{T}} \frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} f(t) e^{-2\pi int/\mathrm{T}} \, dt \\ &= \frac{2\pi in}{\mathrm{T}} c_n(f). \end{aligned} \tag{3.2.7.1}$$

Pour les coefficients de Fourier a_n et b_n, on obtient alors

$$a_n(f') = -\frac{2\pi n}{\mathrm{T}} b_n(f) \qquad \text{et} \qquad b_n(f') = \frac{2\pi n}{\mathrm{T}} a_n(f). \tag{3.2.7.2}$$

Ces formules valent, en fait, sous l'hypothèse un peu plus générale que f est de classe $\mathscr{C}^1$ par morceaux et continue, et se démontrent par le même raisonnement, grâce à la formule d'intégration par parties pour les fonctions de classe $\mathscr{C}^1$ par morceaux et continues.

3.3. Les principaux théorèmes de la théorie des séries de Fourier

Proposition **(3.3.1)** (Relation de Bessel). — *Soit f une fonction localement intégrable, périodique de période* $\mathrm{T} > 0$. *Pour tout entier $n \geqslant 0$, on a*

$$\frac{1}{\mathrm{T}}\int_0^{\mathrm{T}} |f(t) - \mathrm{S}_n(f)(t)|^2\, dt = \frac{1}{\mathrm{T}}\int_0^{\mathrm{T}} |f(t)|^2\, dt - \sum_{k=-n}^{n} |c_k(f)|^2.$$

Démonstration. — Pour démontrer cette relation, on calcule l'intégrale

$$\frac{1}{\mathrm{T}}\int_0^{\mathrm{T}} |f(t) - \mathrm{S}_n(f)(t)|^2\, dt.$$

Pour $t \in \mathbf{R}$, on a

$$\begin{aligned}
|f(t) - \mathrm{S}_n(f)(t)|^2 &= |f(t) - \sum_{k=-n}^{n} c_k(f) e^{2i\pi kt/\mathrm{T}}|^2 \\
&= \overline{f(t)}\mathrm{S}_n(f)(t) - \sum_{k=-n}^{n} f(t)\overline{c_k(f)} e^{-2i\pi kt/\mathrm{T}} \\
&\quad - \sum_{k=-n}^{n} \overline{f(t)} c_k(f) e^{2i\pi kt/\mathrm{T}} \\
&\quad + \sum_{k,\ell=-n^n} c_k(f)\overline{c_\ell(f)} e^{2i\pi(k-\ell)t/\mathrm{T}}.
\end{aligned}$$

Intégrons cette relation sur l'intervalle $[0;\mathrm{T}]$; on obtient que $\int_0^{\mathrm{T}} |f(t) - \mathrm{S}_n(f)(t)|^2\, dt$ est la somme de quatre termes : le premier est $\int_0^{\mathrm{T}} |f(t)|^2\, dt$; le second est

$$-\sum_{k=-n}^{n} \overline{c_k(f)} \int_0^{\mathrm{T}} f(t) e^{-2i\pi kt/\mathrm{T}}\, dt = -\sum_{k=-n}^{n} \overline{c_k(f)} \cdot \mathrm{T} c_k(f) = -\mathrm{T}\sum_{k=-n}^{n} |c_k(f)|^2.$$

Le troisième est le conjugué du précédent, donc est également égal à $-\mathrm{T}\sum_{k=-n}^{n} |c_k(f)|^2$. Enfin, le dernier vaut

$$\sum_{k,\ell=-n}^{n} c_k(f)\overline{c_\ell(f)} \int_0^{\mathrm{T}} e^{2i\pi(k-\ell)t/\mathrm{T}}\, dt = \mathrm{T}\sum_{k=-n}^{n} |c_k(f)|^2$$

puisque $\int_0^{\mathrm{T}} e^{2i\pi mt/\mathrm{T}}\, dt = 0$ si $m \neq 0$. Ainsi,

$$\frac{1}{\mathrm{T}}\int_0^{\mathrm{T}} |f(t) - \mathrm{S}_n(f)(t)|^2\, dt = \frac{1}{\mathrm{T}}|f(t)|^2\, dt - \sum_{k=-n}^{n} |c_k(f)|^2,$$

comme il fallait démontrer. □

Corollaire **(3.3.2)** (Inégalité de Bessel). — *Soit f une fonction localement intégrable, de période $\mathrm{T} > 0$.*

$$\frac{1}{4}|a_0(f)|^2 + \frac{1}{2}\sum_{n=1}^{\infty}(|a_n(f)|^2 + |b_n(f)|^2) = \sum_{n\in\mathbf{Z}}|c_n(f)|^2 \leqslant \frac{1}{\mathrm{T}}\int_0^{\mathrm{T}}|f(t)|^2\,dt.$$

On démontrera plus loin le théorème de Parseval (théorème 3.3.8) selon lequel l'inégalité est en fait une égalité.

Démonstration. — On $\frac{1}{4}|a_0(f)|^2 = |c_0(f)|^2$ et $\frac{1}{2}(|a_n(f)|^2 + |b_n(f)|^2) = |c_n(f)|^2 + |c_{-n}(f)|^2$ pour tout entier $n \geqslant 1$. Cela entraîne l'égalité de gauche.

On déduit alors de la relation de Bessel l'inégalité

$$\sum_{k=-n}^{n}|c_k(f)|^2 \leqslant \frac{1}{\mathrm{T}}|f(t)|^2\,dt,$$

valable pour tout entier $n \geqslant 0$. L'inégalité de Bessel s'en déduit en faisant tendre n vers $+\infty$. □

Puisque le terme général d'une série convergente tend vers 0, on en déduit :

Corollaire **(3.3.3)**. — *Soit f une fonction localement intégrable, de période $\mathrm{T} > 0$. On a $\lim_{n\to\pm\infty} c_n(f) = 0$.*

Proposition **(3.3.4)**. — *Soit f une fonction continue, de période $\mathrm{T} > 0$. Si tous les coefficients de Fourier sont nuls, alors $f = 0$.*

Démonstration. — Quitte à considérer la fonction $t \mapsto f(2\pi t/\mathrm{T})$, on se ramène au cas où $\mathrm{T} = 2\pi$. Raisonnons par l'absurde. Supposons que f ne soit pas nulle et soit $u \in \mathbf{R}$ tel que $f(u) \neq 0$; quitte à changer f en la fonction $t \mapsto f(t-u)/f(u)$, on suppose même $u = 0$ et $f(0) = 1$. Comme f est continue, il existe des nombres réels $m > 0$ et $h \in [0;\pi/2]$ tels que $f(t) \geqslant m$ pour tout $t \in [u-h;u+h]$.

Pour tout entier $n \geqslant 0$, posons $\mathrm{T}_n(t) = (1 + \cos(t) - \cos(h))^n$; en écrivant

$$1 + \cos(t) - \cos(h) = (1 - \cos(h)) + \frac{1}{2}e^{it} + \frac{1}{2}e^{-it},$$

on représente $\mathrm{T}_n(t)$ sous la forme d'un polynôme trigonométrique : il existe des nombres réels m_k, pour $k \in \{-n, 1-n, \ldots, 0, 1, \ldots, n\}$, tels que $\mathrm{T}_n(t) =$

$\sum_{k=-n}^{n} m_k e^{ikt}$ pour tout $t \in \mathbf{R}$. Alors,

$$\int_{-\pi}^{\pi} \mathrm{T}_n(t) f(t)\, dt = \sum_{k=-n}^{n} m_k \int_{-\pi}^{+\pi} e^{ikt} f(t)\, dt = \sum_{k=-n}^{n} m_k 2\pi c_{-k}(f) = 0.$$

Pour $t \in [-h; h]$, on a $\cos(t) \geqslant \cos(h)$, de sorte que $1 + \cos(t) - \cos(h) \geqslant 1$ puis $\mathrm{T}_n(t) \geqslant 1$. Si $t \in [-h/2; h/2]$, on a même

$$1 + \cos(t) - \cos(h) \geqslant 1 + \cos(h/2) - \cos(h) > 0.$$

En revanche, si $t \in [-\pi; \pi]$ mais $t \notin [-h; h]$, on a $-1 \leqslant \cos(t) \leqslant \cos(h)$ donc $-1 \leqslant 1 + \cos(t) - cos(h) \leqslant 1$ et $|\mathrm{T}_n(t)| \leqslant 1$. Il en résulte une inégalité

$$\begin{aligned} \left|\int_{-\pi}^{\pi} \mathrm{T}_n(t) f(t)\, dt\right| &\geqslant m \int_{-h}^{h} (1 + \cos(t) - \cos(h))^n\, dt - \int_{-\pi}^{\pi} |f(t)|\, dt \\ &\geqslant mh(1 + \cos(h/2) - \cos(h))^n - \int_{-\pi}^{\pi} |f(t)|\, dt. \end{aligned}$$

Cette expression tend vers $+\infty$ lorsque n tend vers $+\infty$, alors que le membre de gauche est nul. C'est une contradiction. □

Corollaire **(3.3.5)**. — *Soit f une fonction continue par morceaux, de période $\mathrm{T} > 0$. Si tous les coefficients de Fourier de f sont nuls, alors $f \equiv 0$ sauf en un nombre fini de points de $[0; \mathrm{T}]$.*

Une variante de ce corollaire vaut lorsque f est seulement supposée localement intégrable ; la conclusion est alors que f est nulle presque partout.

Démonstration. — Soit $g : \mathbf{R} \to \mathbf{R}$ la fonction définie par $g(t) = \int_0^t f(s)\, ds$. Pour $t \in \mathbf{R}$, on a

$$g(t + \mathrm{T}) - g(t) = \int_t^{t+\mathrm{T}} f(s)\, ds = \int_0^{\mathrm{T}} f(s)\, ds = \mathrm{T} \cdot c_0(f) = 0.$$

Ainsi, g est périodique, de période T ; elle est également continue. Ses coefficients de Fourier sont donnés par

$$c_n(g) = \frac{\mathrm{T}}{2\pi i n} c_n(f) = 0$$

si $n \in \mathbf{Z} - \{0\}$. Par conséquent, la fonction g^* définie par $g^*(t) = g(t) - c_0(g)$, est continue et tous ses coefficients de Fourier sont nuls. D'après le théorème précédent, on a $g^* \equiv 0$, donc g est constante, puis nulle puisque $g(0) = 0$.

Étant définie comme l'intégrale de f, la fonction g en est « presque » une primitive. Précisément, elle est dérivable en tout point t où f est continue, de dérivée

$g'(t) = f(t)$. Par suite, f est nulle en tout point où elle est continue. Puisqu'elle est continue par morceaux, seuls un nombre fini de points de $[0; \mathrm{T}]$ y échappent, d'où le corollaire. □

Corollaire **(3.3.6)**. — *Soit f une fonction continue ; si la série de Fourier de f converge uniformément vers une fonction g, alors $f = g$.*

Démonstration. — Une limite uniforme de fonctions continues est continue ; par suite, g est continue. Démontrons que $c_n(g) = c_n(f)$ pour tout $n \in \mathbf{Z}$. Pour tout entier $m \geqslant n$, on a en effet

$$c_n(f) = \frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} \mathrm{S}_m(f)(t) e^{-int}\, dt.$$

Puisque $(\mathrm{S}_m(f))_m$ converge uniformément vers g, on a donc

$$\frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} \mathrm{S}_m(f)(t) e^{-int}\, dt \to \frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} g(t) e^{-int}\, dt = c_n(g).$$

Cela prouve que $c_n(f) = c_n(g)$. Par suite, la fonction continue $f - g$ vérifie $c_n(f - g) = c_n(f) - c_n(g) = 0$ pour tout $n \in \mathbf{Z}$. D'après le théorème, on a donc $f - g \equiv 0$, d'où $g = f$. □

Corollaire **(3.3.7)**. — *Soit f une fonction de classe $\mathscr{C}^1$ par morceaux et continue, de période $\mathrm{T} > 0$. La série de Fourier de f converge uniformément vers f.*

Démonstration. — Lorsque f est de classe $\mathscr{C}^2$ par morceaux et f, f' sont continues, on peut utiliser l'exemple 3.2.7 pour évaluer ses coefficients de Fourier : on a, pour tout entier $n \in \mathbf{Z}$ tel que $n \neq 0$,

$$c_n(f) = \frac{\mathrm{T}}{2\pi i n} c_n(f') = \frac{\mathrm{T}^2}{-4\pi^2 n^2} c_n(f'').$$

Les coefficients de Fourier de f'' sont bornés par $\sup(|f''|)$. Cela entraîne l'existence d'un nombre réel $\mathrm{A} > 0$ tel que $|c_n(f)| \leqslant \mathrm{A}/n^2$ pour tout entier $n \in \mathbf{Z} - \{0\}$. De cette majoration uniforme, et de la convergence de la série de Riemann $\sum 1/n^2$, on en déduit que la série de Fourier de f,

$$\mathrm{S}_n(f)(t) = \sum_{k=-n}^{n} c_k(f) e^{ikt}$$

converge *normalement*, et en particulier uniformément. D'après le corollaire précédent, sa limite est f.

Lorsque f est seulement de classe $\mathscr{C}^1$ par morceaux et continue, on raisonne un peu différemment. Si n et m sont des entiers tels que $n > m \geqslant 0$, et $t \in \mathbf{R}$, on a

$$\begin{aligned}
|\mathrm{S}_n(f)(t) - \mathrm{S}_m(f)(t)| &= \Big| \sum_{m+1\leqslant|k|\leqslant n} c_k(f) e^{2i\pi kt/\mathrm{T}} \Big| \\
&\leqslant \sum_{m+1\leqslant|k|\leqslant n} |c_k(f)| \\
&\leqslant \sum_{m+1\leqslant|k|\leqslant n} |c_k(f')| \frac{\mathrm{T}}{2\pi|k|} \\
&\leqslant \frac{\mathrm{T}}{2\pi} \left(\sum_{m+1\leqslant|k|\leqslant n} |c_k(f')|^2 \right)^{1/2} \left(\sum_{m+1\leqslant|k|\leqslant n} \frac{1}{k^2} \right)^{1/2} \\
&\leqslant \frac{\mathrm{T}}{2\pi} \left(\sum_{|k|\geqslant n} |c_k(f')|^2 \right)^{1/2} \left(2 \sum_{k=1}^{\infty} \frac{1}{k^2} \right)^{1/2},
\end{aligned}$$

où l'on a utilisé l'inégalité de Cauchy–Schwarz. Puisque la série de terme général $|c_k(f')|^2$ converge (inégalité de Bessel), cette majoration garantit que la suite $(\mathrm{S}_n(f))$ vérifie le critère de Cauchy pour la convergence uniforme. Elle converge donc uniformément et, d'après le corollaire précédent, sa limite est f. □

Théorème **(3.3.8)** (Formule de Parseval). — *Soit f une fonction continue par morceaux, de période $\mathrm{T} > 0$. On a*

$$\frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} |f(t)|^2 \, dt = \frac{1}{4}|a_0(f)|^2 + \frac{1}{2} \sum_{n=1}^{\infty} (|a_n(f)|^2 + |b_n(f)|^2) = \sum_{n\in\mathbf{Z}} |c_n(f)|^2.$$

En fait, la formule est valable également pour des fonctions qui ne sont pas continues par morceaux mais seulement localement de carré intégrable au sens de Lebesgue, ce qui suffit à définir à la fois le membre de gauche, et qui entraîne que l'on peut également définir ses coefficients de Fourier.

Compte tenu de la relation de Bessel, ce que démontre la formule de Parseval c'est la limite

$$\lim_{n\to+\infty} \frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} |f(t) - \mathrm{S}_n(f)(t)|^2 \, dt = 0 \ :$$

la série de Fourier de f converge « en moyenne quadratique » vers f.

La démonstration repose sur un énoncé d'approximation.

Lemme **(3.3.9)**. — *Soit f une fonction continue par morceaux, de période* $\mathrm{T} > 0$*. Pour tout nombre réel ε tel que $\varepsilon > 0$, il existe une fonction g de classe $\mathscr{C}^1$ par morceaux, continue, de période* T*, telle que*

$$\frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} |f(t) - g(t)|^2 \, dt \leqslant \varepsilon.$$

Démonstration. — Soit α un nombre réel strictement positif qui sera choisi ultérieurement.

Soit $(a_0, \ldots, a_n)$ une suite strictement croissante de nombres réels telle que $a_0 = 0$, $a_n = \mathrm{T}$, et telle que sur chaque intervalle $]a_{k-1}; a_k[$, la fonction f soit la restriction d'une fonction continue f_k sur $[a_{k-1}; a_k]$. Comme cet intervalle est fermé et borné, la fonction f_k est uniformément continue et il existe un nombre réel $h > 0$ tel que $|f_k(t) - f_k(s)| \leqslant \alpha$ si $|t - s| \leqslant h$. On considère alors une subdivision de l'intervalle $[a_{k-1}; a_k]$ en m_k intervalles de longueur $\leqslant h$: $(b_{k,0}, b_{k,1}, \ldots, b_{k,m_k})$. Soit g_k l'unique fonction continue sur $[a_{k-1}; a_k]$ qui est affine sur chaque sous-intervalle $[b_{k,p-1}; b_{k,p}]$, qui coïncide avec f aux points $b_{k,1}, \ldots, b_{k,p-1}$, avec $\frac{1}{2}(f_k(a_k) + f_{k+1}(a_k))$ en a_k et avec $\frac{1}{2}(f_k(a_{k-1}) + f_{k-1}(a_{k-1}))$ en a_{k-1}, en adaptant ces formules pour $k = 1$ et $k = n$: $g_1(a_0) = f_1(a_0)$ et $g_n(a_n) = f_n(a_n)$. Soit M un majorant de $|f|$. Si t appartient à un intervalle de la forme $[b_{k,p-1}, b_{k,p}]$, où $0 < p-1 < p < m_k$, on a $|g_k(t) - f(t)| \leqslant \alpha$. Si t appartient à un intervalle de la forme $[b_{k,0}; b_{k,1}]$, ou à un intervalle de la forme $[b_{k,m_k-1}; b_{k,m_k}]$, on a seulement $|f_k(t) - f(t)| \leqslant \mathrm{M}$. Soit g l'unique fonction sur $[0; \mathrm{T}]$ telle que $g(t) = g_k(t)$ si $t \in [a_{k-1}; a_k]$. On a

$$\frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} |g(t) - f(t)|^2 \, dt \leqslant \alpha^2 + \frac{1}{\mathrm{T}} 2h\mathrm{M}^2.$$

En choisissant $\alpha = \varepsilon/2$ et h assez petit pour que $h \leqslant \mathrm{T}\varepsilon/4\mathrm{M}^2$, on obtient l'inégalité voulue. □

Démonstration de l'égalité de Parseval. — Pour une fonction f, de période T, disons continue par morceaux, notons

$$\|f\|_2 = \left(\frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} |f(t)|^2 \, dt \right).$$

C'est une seminorme sur l'espace des fonctions périodiques de période T : elle vérifie $\|af\|_2 = |a| \, \|f\|_2$ pour tout $a \in \mathbf{C}$ et toute fonction T-périodique f (homogénéité), et $\|f + g\| \leqslant \|f\| + \|g\|$ (inégalité triangulaire). Ce n'est pas tout à fait

une norme car les fonctions continues par morceaux f qui sont nulles sauf en un nombre fini de points (sur une période) vérifient $\|f\|_2 = 0$, mais ce sont les seules.

Pour une telle fonction f, notons aussi

$$\|c(f)\|_2 = \left(\sum_{k\in\mathbf{Z}} |c_k(f)|^2\right)^{1/2}.$$

C'est également une seminorme (homogénéité et inégalité triangulaire) ; si $\|c(f)\|_2 = 0$, alors $c_k(f) = 0$ pour tout $k \in \mathbf{Z}$ et cela entraîne que f est nulle sauf un nombre fini de points (sur une période).

L'inégalité de Bessel affirme que $\|c(f)\|_2 \leqslant \|f\|_2$ pour toute fonction f, de période T, continue par morceaux ; la formule de Parseval précise que l'on a égalité : $\|c(f)\|_2 = \|f\|_2$. Nous allons la démontrer en approchant f par une fonction g de classe $\mathscr{C}^1$ par morceaux et continue. Soit ε un nombre réel strictement positif ; d'après le lemme 3.3.9, il existe une fonction g de classe $\mathscr{C}^1$ par morceaux, continue, telle que $\|f - g\|_2 \leqslant \varepsilon$; l'inégalité triangulaire entraîne alors

$$\|g\|_2 \geqslant \|f\|_2 - \varepsilon.$$

D'après l'inégalité de Bessel, on a $\|c(f-g)\|_2 \leqslant \|f-g\|_2 \leqslant \varepsilon$. Puisque $c_k(f) = c_k(f-g) + c_k(g)$ pour tout entier k, on déduit de l'inégalité triangulaire que

$$\|c(f)\|_2 \geqslant \|c(g)\|_2 - \|c(f-g)\|_2 \geqslant \|c(g)\|_2 - \varepsilon.$$

Comme la suite de fonctions $(\mathrm{S}_n(g))$ converge uniformément vers g, il existe un entier N tel que $|g(t) - \mathrm{S}_n(g)(t)| \leqslant \varepsilon$ pour tout $t \in \mathbf{R}$ et tout entier n tel que $n \geqslant \mathrm{N}$. Pour de tels entiers n, on a donc

$$\|g - \mathrm{S}_n(g)\|_2 = \left(\frac{1}{\mathrm{T}}\int_0^{\mathrm{T}} |g(t) - \mathrm{S}_n(g)(t)|^2\, dt\right)^{1/2} \leqslant \varepsilon,$$

et l'inégalité de Bessel entraîne alors :

$$\sum_{|k|\leqslant n} |c_k(g)|^2 \geqslant \frac{1}{\mathrm{T}}\int_0^{\mathrm{T}} |g(t)|^2\, dt - \varepsilon^2.$$

Faisant tendre n vers l'infini, on obtient

$$\|c(g)\|_2^2 \geqslant \|g\|_2^2 - \varepsilon^2.$$

Finalement,

$$\|c(f)\|_2 \geqslant \|c(g)\|_2 - \varepsilon \geqslant \left(\|g\|_2^2 - \varepsilon^2\right)^{1/2} \geqslant \left((\|f\|_2 - \varepsilon)^2 - \varepsilon^2\right)^{1/2}.$$

Lorsqu'on fait tendre ε vers 0, on obtient l'inégalité $\|c(f)\|_2 \geqslant \|f\|_2$, ce qui conclut la démonstration de l'égalité de Parseval. □

3.4. Convolution et théorème de Dirichlet

On expose dans ce paragraphe une autre approche des séries de Fourier et de leur convergence.

3.4.1. — Soit f une fonction continue par morceaux sur $\mathbf{R}$. On note f^* la fonction définie sur $\mathbf{R}$ par la formule

$$f^*(t) = \frac{1}{2}\big(f(t^-) + f(t^+)\big),$$

où $f(t^+)$ et $f(t^-)$ désignent les limites à droite et à gauche de f en t. On dit que c'est la *régularisée* de f au sens de Dirichlet.

Si I est un intervalle ouvert tel que $f|_{\mathrm{I}}$ est continue, alors $f^* = f$ sur I. Par suite, la trace de l'ensemble des points où f et f^* diffèrent rencontre tout intervalle compact en un ensemble fini.

Théorème **(3.4.2)**. — *Soit* $f : \mathbf{R} \to \mathbf{C}$ *une fonction de classe* $\mathscr{C}^1$ *par morceaux, de période* T. *Pour tout* $x \in \mathbf{R}$, *on a*

$$\mathrm{S}_n(f)(x) \to f^*(x).$$

3.4.3. — La preuve commence par récrire $\mathrm{S}_n(f)(x)$ sous la forme d'une intégrale. En effet, on a

$$\begin{aligned}
\mathrm{S}_n(f)(x) &= \sum_{p=-n}^{n} c_p(f) e^{2\pi i p x/\mathrm{T}} \\
&= \sum_{p=-n}^{n} \left(\frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} f(t) e^{-2\pi i p t/\mathrm{T}}\, dt \right) e^{2\pi i p x/\mathrm{T}} \\
&= \frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} f(t) \sum_{p=-n}^{n} e^{2\pi i p(x-t)/\mathrm{T}}\, dt.
\end{aligned}$$

Posons ainsi, pour tout $u \in \mathbf{R}$,

(3.4.3.1) $$\mathrm{D}_n(u) = \frac{1}{\mathrm{T}} \sum_{p=-n}^{n} e^{2\pi i p u/\mathrm{T}} ;$$

la fonction D_n est un polynôme trigonométrique qu'on appelle *noyau de Dirichlet*. Par définition, on a

$$\mathrm{S}_n(f)(x) = \int_0^{\mathrm{T}} f(t)\mathrm{D}_n(x-t)\,dt. \tag{3.4.3.2}$$

Le changement de variables $t' = x - t$ et la périodicité de f et de D_n permettent de récrire

$$\mathrm{S}_n(f)(x) = \int_{x-\mathrm{T}}^{x} f(x-u)\mathrm{D}_n(u)\,du = \int_{-\mathrm{T}/2}^{\mathrm{T}/2} f(x-u)\mathrm{D}_n(u)\,du. \tag{3.4.3.3}$$

Lemme **(3.4.4)**. — *Soit n un entier naturel.*

a) *On a $\int_0^{\mathrm{T}} \mathrm{D}_n(u)\,du = 1$.*

b) *Soit $u \in \mathbf{R}$. Si $u \in \mathrm{T}\mathbf{Z}$, on a $\mathrm{D}_n(u) = 2n+1$; sinon, on a*

$$\mathrm{D}_n(u) = \frac{1}{\mathrm{T}}\frac{\sin(\pi(2n+1)u/\mathrm{T})}{\sin(\pi u/\mathrm{T})}.$$

Démonstration. — La première relation est immédiate. Démontrons la seconde. On part de la définition de $\mathrm{D}_n(u)$:

$$\mathrm{D}_n(u) = \frac{1}{\mathrm{T}}\sum_{p=-n}^{n} e^{2\pi i p u/\mathrm{T}} = \frac{1}{\mathrm{T}} e^{-2\pi i n u/\mathrm{T}} \sum_{p=0}^{2n} e^{2\pi i p u/\mathrm{T}}.$$

La somme qui apparaît est la somme des $(2n+1)$ premiers termes d'une suite géométrique de raison $e^{2\pi i u/\mathrm{T}}$. Si $u \in \mathrm{T}\mathbf{Z}$, ils sont tous égaux à 1, d'où $\mathrm{D}_n(u) = 2n+1$. Sinon, on a $e^{2\pi i u/\mathrm{T}} \neq 1$, de sorte que

$$\begin{aligned}
\mathrm{D}_n(u) &= \frac{1}{\mathrm{T}} e^{-2\pi i n u/\mathrm{T}} \frac{1 - e^{2\pi i(2n+1)u/\mathrm{T}}}{1 - e^{2\pi i u/\mathrm{T}}} \\
&= \frac{1}{\mathrm{T}} e^{-2\pi i n u/\mathrm{T}} \frac{e^{\pi i(2n+1)u/\mathrm{T}}(-2i\sin(\pi(2n+1)u/\mathrm{T}))}{e^{\pi i u/\mathrm{T}}(-2i\sin(piu/\mathrm{T})} \\
&= \frac{1}{\mathrm{T}} \exp((-2n + (2n+1) - 1)\pi i u/\mathrm{T}) \frac{\sin(\pi(2n+1)u/\mathrm{T})}{\sin(\pi u/\mathrm{T})} \\
&= \frac{1}{\mathrm{T}} \frac{\sin(\pi(2n+1)u/\mathrm{T})}{\sin(\pi u/\mathrm{T})}.
\end{aligned}$$

Le lemme est ainsi démontré. □

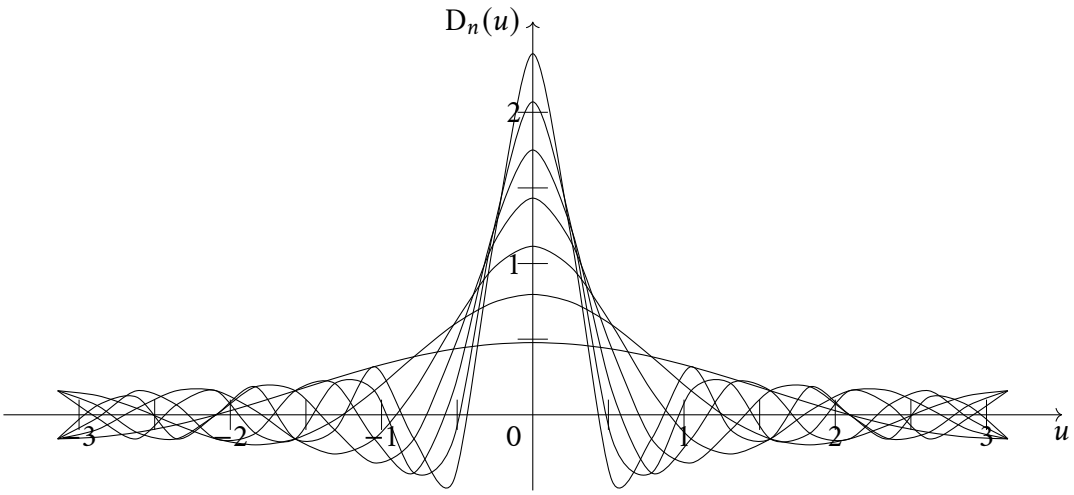


FIGURE 3.4.4.1. Graphe du noyau de Dirichlet ($T = 2\pi$), pour $1 \leqslant n \leqslant 7$

3.4.5. — La représentation graphique du noyau de Dirichlet sur $[-T/2; T/2]$ montre que lorsque n grandit, il se concentre autour de 0 (modulo T). Jointe à la première relation du lemme précédent, cette observation aurait pu être la clé de la démonstration du théorème de Dirichlet si les changements de signe de D_n n'avaient pas comme conséquence que $\frac{1}{T}\int_0^T |D_n(u)|\,du$ tende vers $+\infty$, bien que $\frac{1}{T}\int_0^T D_n(u)\,du$ soit constante, égale à 1.

Reprenons donc plutôt la relation (3.4.3.3). Comme D_n est paire, on a

$$\int_0^{T/2} D_n(u)\,du = \int_{-T/2}^{0} D_n(u)\,du = \frac{1}{2}\int_{-T/2}^{T/2} D_n(u)\,du = \frac{1}{2},$$

de sorte que

$$\begin{aligned} S_n(f)(x) - f^*(x) &= \int_{-T/2}^{T/2} f(x-t)D_n(t)\,dt \\ &\qquad - \int_{-T/2}^{0} f(x^-)D_n(t)\,dt - \int_0^{T/2} f(x^+)D_n(t)\,dt \\ &= \int_0^{T/2} (f(x-t) - f(x^-))D_n(t)\,dt \\ &\qquad + \int_{-T/2}^{0} (f(x-t) - f(x^+))D_n(t)\,dt \\ &= \int_0^{T/2} \big((f(x-t) - f(x^-)) + (f(x+t) - f(x^+))\big)D_n(t)\,dt. \end{aligned}$$

Comme f est de classe $\mathscr{C}^1$ par morceaux, $\frac{f(x-t)-f(x^-)}{t}$ et $\frac{f(x+t)-f(x^+)}{t}$ ont une limite quand t tend vers 0. Autrement dit, il existe une fonction continue g_x sur $[0;\mathrm{T}/2]$ telle que

$$(f(x-t)-f(x^-))+(f(x+t)-f(x^+))=tg_x(t)$$

pour tout $t\in[0;\mathrm{T}/2]$. On écrit alors

$$\mathrm{S}_n(f)(x)-f^*(x)=\int_0^{\mathrm{T}/2} g_x(t)\frac{t}{\mathrm{T}\sin(\pi t/\mathrm{T})}\sin(\pi(2n+1)t/\mathrm{T})\,dt.$$

La fonction définie par $t\mapsto t/\sin(\pi t/\mathrm{T})$ pour $t\in\,]0;\mathrm{T}/2]$ est continue, et a une limite (T/π) en 0 ; elle se prolonge par continuité en une fonction continue sur $[0;\mathrm{T}/2]$. Alors, la fonction h_x sur $[0;\mathrm{T}/2]$ définie par

$$h_x(t)=g_x(t)\frac{t}{\mathrm{T}\sin(\pi t/\mathrm{T})}$$

pour $t\in\,]0;\mathrm{T}/2]$ se prolonge par continuité en 0, et l'on a

$$\mathrm{S}_n(f)(x)-f^*(x)=\int_0^{\mathrm{T}/2} h_x(t)\sin(\pi(2n+1)t/\mathrm{T})\,dt. \tag{3.4.5.1}$$

D'après le lemme ci-dessous (lemme 3.4.6), le membre de droite de cette égalité tend vers 0, on a donc

$$\lim_{x\to\infty}\mathrm{S}_n(f)(x)=f^*(x),$$

et cela conclut la démonstration du théorème de Dirichlet.

Lemme **(3.4.6)** (« Lemme de Riemann–Lebesgue »). — *Soit* $h:\mathbf{R}\to\mathbf{C}$ *une fonction localement intégrable telle que* $\int_{-\infty}^{\infty}|h(t)|\,dt<+\infty$. *On a :*

$$\lim_{\omega\to\pm\infty}\int_{-\infty}^{+\infty}h(t)e^{-i\omega t}\,dt=0.$$

Ce lemme vaut en particulier pour toute fonction continue par morceaux qui est nulle hors d'un intervalle compact de $\mathbf{R}$. Nous allons d'ailleurs essentiellement nous contenter de le prouver dans ce cas particulier.

Démonstration. — Pour alléger l'écriture, posons, pour toute fonction h qui est localement intégrable et telle que $\int_{-\infty}^{\infty}|h(t)|\,dt<+\infty$,

$$\widehat{h}(\omega)=\int_{-\infty}^{\infty}h(t)e^{-i\omega t}\,dt.$$

Supposons tout d'abord que h soit de classe $\mathscr{C}^1$ sur un intervalle compact $[a;b]$, et nulle en dehors. Alors, on peut intégrer par parties dans la définition de $\widehat{h}(\omega)$, d'où :

$$\widehat{h}(\omega) = \left[h(t)\frac{i}{\omega}e^{-i\omega t}\right]_a^b - \frac{i}{\omega}\int_a^b h'(t)e^{-i\omega t}\,dt.$$

Cette expression montre que l'on a

$$|\omega\widehat{h}(\omega)| \leqslant |h(a)| + |h(b)| + \int_a^b |h'(t)|\,dt,$$

si bien que $|\widehat{h}(\omega)| = \mathrm{O}(1/\omega)$. En particulier, $\lim_{\pm\infty}\widehat{h}(\omega) = 0$.

Si h est seulement intégrable, cet argument ne suffit pas car la formule d'intégration par parties ne sera pas valable. On peut, en revanche, l'approcher « en moyenne » par une fonction en escalier, nulle hors d'un intervalle bornée. Expliquons comment faire lorsque h est continue par morceaux. Soit $\varepsilon > 0$; choisissons des nombres réels a et b tels que $a < b$ et tels que les deux intégrales

$$\int_{-\infty}^a |h(t)|\,dt, \qquad \int_b^{+\infty} |h(t)|\,dt$$

soient inférieures à ε.

Choisissons ensuite une suite finie croissante $(a_0,\dots,a_n)$ telle que $a = a_0$ et $a_n = b$, et telle que pour tout $k \in \{1,\dots,n\}$, la fonction h soit continue sur $]a_{k-1},a_k[$ et ait une limite à droite en a_{k-1}, et à gauche en a_k. Notons h_k la fonction continue sur $[a_{k-1},a_k]$ qui coïncide avec h sur l'intervalle ouvert $]a_{k-1},a_k[$. Elle est uniformément continue : il existe donc un nombre réel $\delta > 0$ tel que pour tous $x, y \in [a_{k-1},a_k]$ tels que $|x-y| \leqslant \delta$, on ait $|h_k(x) - h_k(y)| < \varepsilon$. Subdivisons alors l'intervalle $[a_{k-1},a_k]$ en sous-intervalles de longueur $< \delta$ et notons g_k la fonction constante sur l'intérieur de chacun de ces intervalles et qui coïncide avec h_k en leur milieu $b_k = (a_k + a_{k-1})/2$. Sur chacun de ces intervalles I, on a $|g_k(x) - h_k(x)| < \varepsilon$, donc l'intégrale sur I de $|g_k - h_k|$ est majorée par $\varepsilon\,\ell(\mathrm{I})$. Finalement, $\int_{a_{k-1}}^{a_k} |g_k - h_k| < \varepsilon(a_k - a_{k-1})$. Soit g une fonction sur $\mathbf{R}$ qui, pour tout k, coïncide avec g_k sur l'intervalle $]a_{k-1},a_k[$, et est nulle hors de l'intervalle $[a;b]$. C'est une fonction en escalier et l'on a

$$\int_{-\infty}^{\infty} |g-h| = \int_{-\infty}^{a} + \int_a^b + \int_b^{\infty} |g-h| \leqslant \varepsilon(2 + b - a).$$

De cette inégalité, on déduit la majoration

$$|\widehat{g}(\omega) - \widehat{h}(\omega)| = |\int_{-\infty}^{\infty} (g(t) - h(t))e^{-i\omega t}\, dt| \leqslant \int_{-\infty}^{\infty} |g(t) - h(t)|\, dt \leqslant \varepsilon(2 + b - a),$$

pour tout $\omega \in \mathbf{R}$. Par ailleurs, on a

$$\begin{aligned}\widehat{g}(\omega) &= \sum_{k=1}^{n} h(b_k) \int_{a_{k-1}}^{a_k} e^{-i\omega t}\, dt \\ &= \frac{1}{\omega} \sum_{k=1}^{n} ih(b_k)(e^{-i\omega a_k} - e^{-i\omega a_{k-1}}),\end{aligned}$$

formule qui prouve que

$$\lim_{\omega \to \pm\infty} \widehat{g}(\omega) = 0.$$

En particulier, il existe $\mathrm{W} \in \mathbf{R}$ tel que $|\widehat{g}(\omega)| \leqslant \varepsilon$ dès que ω vérifie $|\omega| \geqslant \mathrm{W}$. Pour un tel ω, on a donc $|\widehat{h}(\omega)| \leqslant \varepsilon(3 + b - a)$. La démonstration du lemme de Riemann–Lebesgue est ainsi terminée. □

Remarque **(3.4.7)**. — Dans les cours de Licence, on apprend à « sommer » une série en considérant ses sommes partielles, mais il y a de nombreuses autres procédés. Deux d'entre eux, au moins, sont particulièrement adaptés à la théorie des séries de Fourier.

Pour tout nombre réel r tel que $0 \leqslant r < 1$, posons

$$\mathrm{P}_r(f)(x) = \sum_{k=-\infty}^{\infty} c_k(f) r^{|k|} e^{2\pi i k x/\mathrm{T}}. \tag{3.4.7.1}$$

Comme les coefficients de Fourier de f sont bornés, le facteur supplémentaire $r^{|k|}$ entraîne une majoration des termes de cette série (infinie dans les deux sens) par les termes d'une série géométrique, si bien que cette série converge normalement et sa limite est une fonction continue de x. On peut exprimer $\mathrm{P}_r(f)$ de façon

analogue à la formule (3.4.3.3) :

$$\begin{aligned}\mathrm{P}_r(f)(x) &= \sum_{k=-\infty}^{\infty} \frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} f(t) e^{-2\pi i k t/\mathrm{T}}\, dt r^{|k|} e^{2\pi k x/\mathrm{T}} \\ &= \int_0^{\mathrm{T}} f(t) \frac{1}{\mathrm{T}} \sum_{k=-\infty}^{\infty} r^{|k|} e^{2\pi i k(x-t)/\mathrm{T}}\, dt \\ &= \int_0^{\mathrm{T}} f(t) \mathrm{K}_r(x-t)\, dt,\end{aligned}$$

où la fonction K_r, *noyau de Poisson*, est défini par

$$\mathrm{K}_r(t) = \frac{1}{\mathrm{T}} \sum_{k=-\infty}^{\infty} r^{|k|} e^{2\pi i k t/\mathrm{T}}.$$

On peut, en fait, calculer précisément K_r :

$$\begin{aligned}\mathrm{K}_r(t) &= 1 + \sum_{k=1}^{\infty} r^k e^{2\pi i k t/\mathrm{T}} + \sum_{k=1}^{\infty} r^k e^{-2\pi i k t/\mathrm{T}} \\ &= 1 + \frac{r e^{2\pi i t/\mathrm{T}}}{1 - r e^{2\pi i t/\mathrm{T}}} + \frac{r e^{-2\pi i t/\mathrm{T}}}{1 - r e^{-2\pi i t/\mathrm{T}}} \\ &= \frac{1 - r^2}{1 - 2r\cos(2\pi t/\mathrm{T}) + r^2}\end{aligned}$$

Cette formule permet de constater que le noyau de Poisson est positif et converge uniformément vers 0 sur tout intervalle $[\delta; \mathrm{T} - \delta]$ lorsque $r \longrightarrow 1^-$; sa définition montre aussi qu'il est pair et d'intégrale 1. Alors, un argument classique démontre que $\mathrm{K}_r(t)(x)$ converge vers la régularisée $f^*(x)$ de f en tout point x tel que f ait des limites à droite et à gauche. Comme dans la preuve du théorème de Dirichlet, on écrit en fait

$$\mathrm{P}_r(f)(x) - f^*(x) = \int_0^{\mathrm{T}/2} \big((f(x-t) - f(x^-)) + (f(x+t) - f(x^+))\big)\, \mathrm{K}_r(t)\, dt.$$

Soit ε un nombre réel > 0. Il existe un nombre réel $\delta > 0$ tel que si $0 < t < \delta$, on ait $|f(x-t) - f(x^-)| \leqslant \varepsilon$ et $|f(x+t) - f(x^+)| \leqslant \varepsilon$. Comme $\mathrm{K}_r(t)$ est positif, la partie de l'intégrale précédente pour $t \in [0; \delta]$ est majorée par

$$\int_0^{\delta} 2\varepsilon \mathrm{K}_r(t)\, dt \leqslant 2\varepsilon \int_0^{\mathrm{T}/2} \mathrm{K}_r(t)\, dt = \varepsilon.$$

Si M est un majorant de $|f|$, le reste de l'intégrale est majoré par

$$4M \int_{\delta}^{T/2} K_r(t)\, dt,$$

expression qui tend vers 0 quand $r \to 1^-$ puisque $K_r(t)$ tend uniformément vers 0 sur l'intervalle $[\delta; T/2]$. Ainsi, pour r assez proche de 1, cette intégrale est majorée par ε, et $|P_r(f)(x) - f^*(x)| \leqslant 2\varepsilon$.

Un autre procédé consiste à introduire les moyennes, au sens de Cesáro, des sommes partielles $S_n(f)(x)$, et de poser

(3.4.7.2)
$$T_n(f)(x) = \frac{1}{n+1} \sum_{k=0}^{n} S_n(f)(x).$$

Posons

$$F_n(t) = \frac{1}{n+1} \sum_{k=0}^{n} D_k(t)\,;$$

cette fonction F_n est appelée *noyau de Fejér* et on déduit de l'équation (3.4.3.3) que l'on a

$$T_n(f)(x) = \int_0^T f(t) F_n(x-t)\, dt.$$

Le noyau de Fejér est pair, T-périodique et d'intégrale 1, et un calcul explicite prouve qu'il est positif. Une variante de l'argument précédent entraîne que si f a des limites à droite et à gauche en x, alors $T_n(f)(x)$ converge vers sa régularisée $f^*(x)$.

3.5. Transformation de Fourier

Nous passons maintenant à la « transformation de Fourier », c'est-à-dire l'étude fréquentielle des fonctions définies sur $\mathbf{R}$.

3.5.1. — Soit $f : \mathbf{R} \to \mathbf{C}$ une fonction localement intégrable telle que $\int_{-\infty}^{\infty} |f(t)|\, dt < +\infty$. On définit alors sa *transformée de Fourier* $\widehat{f}$ par la formule

(3.5.1.1)
$$\widehat{f}(y) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i x y}\, dx.$$

Exemple **(3.5.2).** — Soit W un nombre réel $\geqslant 0$ et soit $f : \mathbf{R} \to \mathbf{C}$ la fonction définie par $f(x) = 1$ pour $x \in [-\mathrm{W}; \mathrm{W}]$, et par $f(x) = 0$ sinon. On a, pour $y \neq 0$,

$$\begin{aligned}\widehat{f}(y) &= \int_{-\infty}^{\infty} f(x)e^{-2\pi ixy}\,dx = \int_{-\mathrm{W}}^{\mathrm{W}} e^{-2\pi ixy}\,dx \\ &= \left[\frac{1}{-2\pi iy}e^{-2\pi ixy}\right]_{-\mathrm{W}}^{\mathrm{W}} = \frac{e^{-2\pi i\mathrm{W}y} - e^{2\pi i\mathrm{W}y}}{-2\pi iy} = \frac{\sin(2\pi y\mathrm{W})}{\pi y} \\ &= 2\mathrm{W}\,\mathrm{sinc}(2\pi y\mathrm{W}),\end{aligned}$$

où la fonction sinc, usuellement appelée *sinus cardinal*, est définie par

(3.5.2.1) $$\mathrm{sinc}(y) = \sin(y)/y$$

pour $y \neq 0$, et $\mathrm{sinc}(0) = 1$. Pour $y = 0$, on trouve $\widehat{f}(y) = 2\mathrm{W}$, de sorte que cette formule est encore valable.

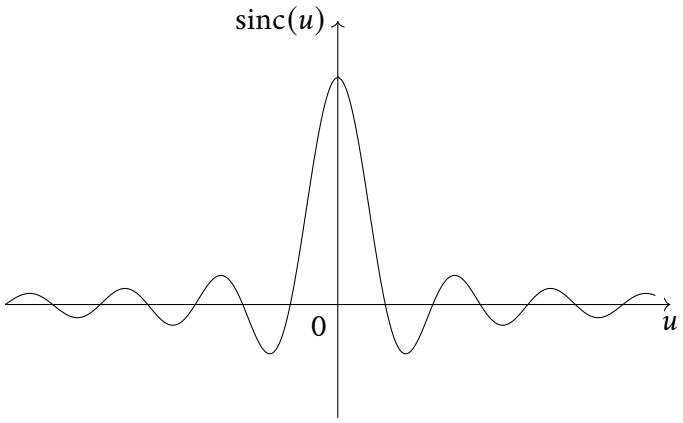


FIGURE 3.5.2.2. Graphe du sinus cardinal

3.5.3. — Les propriétés suivantes se déduisent immédiatement de la définition de la transformée de Fourier. Soit f, g des fonctions localement intégrables de $\mathbf{R}$ dans $\mathbf{C}$ telles que $\int_{-\infty}^{\infty} |f(x)|\,dx < +\infty$, et de même pour g.

a) On $\widehat{f+g}(y) = \widehat{f}(y) + \widehat{g}(y)$ pour tout $y \in \mathbf{R}$.
b) Pour tout $c \in \mathbf{C}$, on a $\widehat{cf}(y) = c\widehat{f}(y)$ pour tout $y \in \mathbf{R}$.

c) Soit $a \in \mathbf{R}^*$ et $b \in \mathbf{R}$; supposons que l'on ait $g(x) = f(ax+b)$ pour tout $x \in \mathbf{R}$. Alors, $a\widehat{g}(ay) = e^{2\pi ib/a}\widehat{f}(y)$ pour tout $y \in \mathbf{R}$. En effet,

$$\begin{aligned}\widehat{g}(y) &= \int_{-\infty}^{\infty} f(ax+b)e^{-2\pi ixy}\,dx \\ &= \int_{-\infty}^{\infty} f(ax+b)e^{-2\pi i(ax+b)(y/a)}e^{2\pi ib/a}\,dx \\ &= \frac{1}{a}e^{2\pi ib/a}\int_{-\infty}^{\infty} f(x)e^{-2\pi ix(y/a)}\,dx \\ &= \frac{1}{a}e^{2\pi ib/a}\widehat{f}(y/a).\end{aligned}$$

d) Supposons que $g(x) = \overline{f(x)}$; alors on a $\widehat{g}(y) = \overline{\widehat{f}(-y)}$ pour tout $y \in \mathbf{R}$.

3.5.4. — Soit f une fonction localement intégrable de $\mathbf{R}$ dans $\mathbf{C}$ telle que $\int_{-\infty}^{\infty}|f| < \infty$.

On a $\widehat{f}(y) \leqslant \int_{-\infty}^{\infty}|f|$ pour tout $y \in \mathbf{R}$ et $\lim_{y\to\pm\infty}\widehat{f}(y) = 0$ (lemme de Riemann–Lebesgue, lemme 3.4.6). Par ailleurs, il découle des théorèmes de continuité des intégrales à paramètre que la fonction $\widehat{f}$ est continue.

Il y a plus généralement une sorte de « correspondance » entre propriétés de décroissance pour f et propriétés de régularité pour $\widehat{f}$ d'une part, et propriété de régularité pour f et propriétés de décroissance pour $\widehat{f}$.

a) Soit p un entier. Si la fonction $x \mapsto x^p f(x)$ est intégrable sur $\mathbf{R}$, on déduit des théorèmes sur la dérivabilité des intégrales à paramètres que $\widehat{f}$ est p-fois continûment dérivable et que

$$\widehat{f}^{(p)}(y) = \int_{-\infty}^{\infty}(-2\pi ix)^p f(x)e^{-2\pi ixy}\,dx = \mathscr{F}((-2\pi ix)^p f)(y).$$

b) Supposons de plus que f soit de classe $\mathscr{C}^1$ par morceaux, continue, et que $\int_{-\infty}^{\infty}|f'| < \infty$. Dans ce cas, f a des limites en $\pm\infty$, nécessairement nulles. On peut alors intégrer par parties dans la définition de $\widehat{f'}$:

$$\begin{aligned}\widehat{f'}(y) &= \int_{-\infty}^{\infty} f'(x)e^{-2\pi ixy}\,dx \\ &= \left[f(x)e^{-2\pi ixy}\right]_{-\infty}^{\infty} + \int_{-\infty}^{\infty} f(x)2\pi iye^{-2\pi ixy}\,dx \\ &= 2\pi iy\widehat{f}(y).\end{aligned}$$

Supposons plus généralement que f est de classe $\mathscr{C}^p$ par morceaux, que $f, \dots, f^{(p-1)}$ sont continues, et que $\int_{-\infty}^{\infty} |f^{(k)}| < \infty$ pour $k \in \{0, \dots, p\}$. Dans ce cas, on a

$$\widehat{f^{(p)}}(y) = (2\pi i y)^p \widehat{f}(y)$$

pour tout $y \in \mathbf{R}$.

On note $\mathscr{S}(\mathbf{R})$ l'ensemble des fonctions de classe $\mathscr{C}^\infty$ de $\mathbf{R}$ dans $\mathbf{R}$ telles que pour tout entier p et tout entier k, la fonction $x \mapsto x^p f^{(k)}(x)$ soit bornée sur $\mathbf{R}$. C'est un sous-espace vectoriel de l'espace des fonctions de $\mathbf{R}$ dans $\mathbf{C}$ qu'on appelle *classe de Schwartz*. Il est stable par multiplication par la fonction x, par dérivation et, d'après les calculs précédents, par transformation de Fourier.

Théorème **(3.5.5)**. — *Soit $f : \mathbf{R} \to \mathbf{C}$ une fonction localement intégrable telle que $\int_{-\infty}^{\infty} |f| < +\infty$.*

a) *Si la fonction $\widehat{f}$ est intégrable sur $\mathbf{R}$, on a la* formule d'inversion de Fourier :

$$f(x) = \int_{-\infty}^{\infty} \widehat{f}(y) e^{2\pi i x y}\, dy$$

pour tout $x \in \mathbf{R}$. Autrement dit, $\widehat{\widehat{f}} = \check{f}$.

b) *La fonction $|f|^2$ est intégrable sur $\mathbf{R}$ si et seulement si $|\widehat{f}|^2$ l'est. Dans ce cas, on a la* formule de Plancherel :

$$\int_{-\infty}^{\infty} |f(x)|^2\, dx = \int_{-\infty}^{\infty} |\widehat{f}(y)|^2\, dy.$$

Démonstration. — On ne va démontrer ce théorème que sous l'hypothèse que f est de classe $\mathscr{C}^1$ par morceaux, continue, et qu'elle est également à support compact, c'est-à-dire qu'il existe un nombre réel T tel que $f(x) = 0$ si $|x| \geqslant \mathrm{T}/2$. Soit f_T la fonction de période T qui coïncide avec f sur l'intervalle $]-\mathrm{T}/2; \mathrm{T}/2]$. Elle est $\mathscr{C}^1$ par morceaux et continue. En particulier, elle est somme de sa série de Fourier. Ses coefficients de Fourier vérifient :

$$c_n(f_\mathrm{T}) = \frac{1}{\mathrm{T}} \int_{-\mathrm{T}/2}^{\mathrm{T}/2} f(t) e^{-2\pi i n t/\mathrm{T}}\, dt = \frac{1}{\mathrm{T}} \int_{-\infty}^{\infty} f(t) e^{-2\pi i n t/\mathrm{T}}\, dt = \frac{1}{\mathrm{T}} \widehat{f}(n/\mathrm{T}).$$

Pour $x \in \mathbf{R}$ tel que $|x| < \mathrm{T}/2$, on a donc

$$f(x) = f_\mathrm{T}(x) = \sum_{n \in \mathbf{Z}} c_n(f) e^{2\pi i n x/\mathrm{T}} = \frac{1}{\mathrm{T}} \sum_{n \in \mathbf{Z}} \widehat{f}(n/\mathrm{T}) e^{2\pi i x n x/\mathrm{T}}.$$

Le membre de droite est l'approximation de l'intégrale $\int_{-\infty}^{\infty} \widehat{f}(y)e^{2\pi ixy}\,dy$ par la méthode des rectangles, appliquée à des rectangles de largeur $1/\mathrm{T}$. Lorsque $\mathrm{T} \longrightarrow +\infty$, cela fournit

$$f(x) = \int_{-\infty}^{\infty} \widehat{f}(y)e^{2\pi ixy}\,dy = \widehat{\widehat{f}}(-x),$$

pour tout $x \in \mathbf{R}$. Cela démontre la formule d'inversion.

La preuve de l'identité de Plancherel est analogue : on a

$$\begin{aligned}\int_{-\infty}^{\infty} |f(x)|^2\,dx &= \int_{-\infty}^{\infty} |f_{\mathrm{T}}(x)|^2\,dx \\ &= \mathrm{T}\sum_{n\in\mathbf{Z}} |c_n(f_{\mathrm{T}})|^2 \\ &= \mathrm{T}\frac{1}{\mathrm{T}^2}\sum_{n\in\mathbf{Z}} |\widehat{f}(n/\mathrm{T})|^2 \\ &= \frac{1}{\mathrm{T}}\sum_{n\in\mathbf{Z}} |\widehat{f}(n/\mathrm{T})|^2,\end{aligned}$$

qui est l'approximation de l'intégrale $\int_{-\infty}^{\infty} |\widehat{f}(y)|^2\,dy$ par la méthode des rectangles, appliquée à des rectangles de largeur $1/\mathrm{T}$. Lorsque $\mathrm{T} \longrightarrow +\infty$, cela fournit

$$\int_{-\infty}^{\infty} |f(x)|^2\,dx = \int_{-\infty}^{\infty} |\widehat{f}(y)|^2\,dy,$$

Cela démontre la formule de Plancherel. □

Exemple **(3.5.6)**. — Reprenons la fonction f de l'exemple 3.5.2, donnée $f(x) = 1$ si $x \in [-\mathrm{W};\mathrm{W}]$, et $f(x) = 0$ sinon ; on a $\int_{\mathbf{R}} |f(x)|^2\,dx = 2\mathrm{W}$. On vu que sa transformée de Fourier est la fonction g donnée par $g(y) = 2\mathrm{W}\sin(2\pi\mathrm{W}y)/2\pi\mathrm{W}y$. Par suite, $\int_{\mathbf{R}} |g(y)|^2\,dy = 1$. Autrement dit,

$$4\mathrm{W}^2 \int_{\mathbf{R}} \left(\frac{\sin(2\pi\mathrm{W}y)}{2\pi\mathrm{W}y}\right)^2 dy = 2\mathrm{W}.$$

En choisissant $\mathrm{W} = 1/2\pi$, on obtient

$$\int_{-\infty}^{\infty} \left(\frac{\sin(y)}{y}\right)^2 = 2\pi.$$

3.6. Le théorème d'échantillonnage

Théorème **(3.6.1)**. — *Soit* $f : \mathbf{R} \to \mathbf{C}$ *une fonction continue telle que* $x^2 f(x)$ *soit borné, lorsque* x *varie. Alors* f *est intégrable sur* $\mathbf{R}$*, et on suppose qu'il existe un nombre réel* W *tel que* $\widehat{f}(y) = 0$ *pour tout* $y \in \mathbf{R}$ *tel que* $|y| \geqslant \mathrm{W}$*. Alors, pour tout* $x \in \mathbf{R}$*, on a la formule,*

$$\textbf{(3.6.1.1)} \qquad f(x) = \sum_{n=-\infty}^{\infty} f\left(\frac{n}{2\mathrm{W}}\right) \operatorname{sinc}\left(x - \frac{n}{2\mathrm{W}}\right).$$

Autrement dit, en échantillonnant le signal donné par f à la fréquence 2W, on peut le reconstituer exactement !

3.6.2. — Selon Shannon (1949), l'idée que l'on puisse reconstruire un signal en l'échantillonnant à une fréquence au moins double de la plus grande fréquence intervenant dans un signal était bien connue des spécialistes de la théorie de la communication — « *common knowledge in the communication art* ». L'apport de cet article est ainsi de donnner une formule explicite pour cette reconstruction. Shannon (1949) admet aussi que cette formule avait déjà été démontrée, sous une forme ou sous une autre, par divers mathématiciens ; citons par exemple E. Whittaker (1915), Oguro (1920), Kotel'nikov (1933). Il insiste cependant que c'est la première fois qu'elle est explicitée dans le contexte de la théorie de la communication.

Cette histoire un peu balbutiante explique peut-être pourquoi ce théorème d'échantillonnage est parfois dénommé *théorème de Nyquist–Shannon*.

3.6.3. Démonstration du théorème d'échantillonnage. — Puisque f est continue, intégrable, et que $\widehat{f}$ est nulle en dehors de l'intervalle borné $[-\mathrm{W}; \mathrm{W}]$, on a la formule d'inversion de Fourier

$$f(x) = \int_{-\mathrm{W}}^{\mathrm{W}} \widehat{f}(y) e^{2\pi i x y}\, dy.$$

En particulier, f est indéfiniment dérivable.

Soit φ la fonction de période W qui coïncide avec $\widehat{f}$ sur $[-\mathrm{W}; \mathrm{W}]$. Comme $\widehat{f}(\mathrm{W}) = \widehat{f}(-\mathrm{W}) = 0$, elle est continue. Calculons ses coefficients de Fourier : pour

$n \in \mathbf{Z}$, on a

$$\begin{aligned} c_n(\varphi) &= \frac{1}{2W}\int_{-W}^{W} \varphi(y)e^{-2\pi iny/2W}\,dy \\ &= \frac{1}{2W}\int_{-\infty}^{\infty} \widehat{f}(y)e^{-2\pi iny/2W}\,dy \\ &= \frac{1}{2W} f(-n/2W). \end{aligned}$$

Le développement en série de Fourier de φ est ainsi

$$\varphi(y) = \sum_{n\in\mathbf{Z}} c_n(\varphi)e^{2\pi iny/2W} = \frac{1}{2W}\sum_{n\in\mathbf{Z}} f(n/2W)e^{-2\pi iny/2W}.$$

Comme $n^2 f(n/2W)$ est borné, cette série converge uniformément. On peut donc la reporter dans la formule d'inversion de Fourier et intégrer terme à terme, ce qui fournit, puisque $\widehat{f}(y) = \varphi(y)$ pour $y \in [-W; W]$ et $\widehat{f}(y) = 0$ sinon,

$$\begin{aligned} f(x) &= \frac{1}{2W}\sum_{n\in\mathbf{Z}} f(n/2W)\int_{-W}^{W} e^{2\pi i(x-n/2W)y}\,dy \\ &= \sum_{n\in\mathbf{Z}} f(n/2W)\,\mathrm{sinc}(x - n/2W), \end{aligned}$$

comme il fallait démontrer.

Proposition **(3.6.4)**. — *Soit $f : \mathbf{R} \to \mathbf{C}$ une fonction intégrable ; on suppose que $\widehat{f}$ est nulle hors d'un intervalle $[-W_0; W_0]$. Soit W un nombre réel tel que $W \geqslant W_0$ et soit $\psi : \mathbf{R} \to \mathbf{C}$ une fonction nulle hors de $[-W; W]$ et identiquement égale à 1 sur l'intervalle $[-W_0; W_0]$. Alors, pour tout $x \in \mathbf{R}$, on a*

$$f(x) = \frac{1}{2W}\sum_{n\in\mathbf{Z}} f(n/2W)\widehat{\psi}(n/2W - x).$$

C'est une formule analogue à la formule de reconstruction (3.6.1.1) que l'on retrouve formellement en prenant $W = W_0$ et pour fonction ψ la fonction indicatrice de $[-W_0; W_0]$. Toutefois, lorsque $W > W_0$ (il y a alors *suréchantillonnage* par rapport à la fréquence de Nyquist $2W_0$), on peut prendre pour ψ une fonction de classe $\mathscr{C}^\infty$. Sa transformée de Fourier $\widehat{\psi}$ décroît alors rapidement à l'infini si bien que la série donnée dans la proposition converge très vite.

Démonstration. — On note encore φ la fonction de période W qui coïncide avec $\widehat{f}$ sur $[-\mathrm{W};\mathrm{W}]$; elle est $\mathscr{C}^1$ par morceaux et ses coefficients de Fourier sont donnés par

$$c_n(\varphi) = f(-n/2\mathrm{W})/2\mathrm{W},$$

comme dans la démonstration du théorème 3.6.1. Pour tout $y \in \mathbf{R}$, on peut alors écrire

$$\widehat{f}(y) = \varphi(y)\psi(y),$$

puisque cette égalité devient $\widehat{f}(y) = \widehat{f}(y)\psi(y)$ si $y \in [-\mathrm{W};\mathrm{W}]$, égalité vraie car $\psi(y) = 1$ si $\widehat{f}(y) \neq 0$, et qu'elle se réduit à $0 = 0$ si $y \notin [-\mathrm{W};\mathrm{W}]$. Ainsi, en écrivant φ comme la somme de sa série de Fourier, on a

$$\widehat{f}(y) = \sum_{n\in\mathbf{Z}} \frac{1}{2\mathrm{W}} f(n/2\mathrm{W}) e^{-2i\pi n y} \psi(y).$$

Appliquons maintenant la formule d'inversion de Fourier à cette égalité ; on trouve

$$f(x) = \sum_{n\in\mathbf{Z}} \frac{1}{2\mathrm{W}} f(-n/2\mathrm{W}) \int_{-\infty}^{\infty} e^{-2i\pi n y/2\mathrm{W}} \psi(y) e^{2i\pi x y}\, dy.$$

Cette dernière intégrale vaut $\widehat{\psi}(-x + n/2\mathrm{W})$, d'où la proposition. □

La démonstration du théorème d'échantillonnage est en fait très proche de celle d'une formule importante en mathématiques, la *formule sommatoire de Poisson*.

Théorème **(3.6.5)** (Formule de Poisson). — *Soit $f : \mathbf{R} \to \mathbf{C}$ une fonction appartenant à la classe de Schwartz. Alors, pour tout nombre réel $a > 0$, on a*

(3.6.5.1)
$$\sum_{m\in\mathbf{Z}} f(am) = \frac{1}{a} \sum_{n\in\mathbf{Z}} \widehat{f}(n/a).$$

Plus généralement, pour tout nombre réel $a > 0$ et tout nombre réel x, on a

(3.6.5.2)
$$\sum_{m\in\mathbf{Z}} f(x + am) = \frac{1}{a} \sum_{n\in\mathbf{Z}} \widehat{f}(n/a) e^{2i\pi n x/a}.$$

L'hypothèse que f appartient à la classe de Schwartz est plus forte que nécessaire ; il suffit par exemple que f soit de classe $\mathscr{C}^1$ et que f et f' décroissent « assez vite » à l'infini, par exemple qu'il existe des nombres réels c, c' tels que $|f(x)| \leqslant c/(1+|x|^2)$ et $|f'(x)| \leqslant c'/(1+|x|^2)$ pour tout x.

Démonstration. — Considérons la série

$$\mathrm{F}(x) = \sum_{m\in\mathbf{Z}} f(x+am).$$

La décroissance de f et de f' entraînent que cette série converge uniformément, de même que sa dérivée terme à terme, lorsque x parcourt un intervalle borné. La fonction F ainsi définie est ainsi de classe $\mathscr{C}^1$ sur $\mathbf{R}$; elle est aussi de période a. Calculons ses coefficients de Fourier : pour tout $n \in \mathbf{Z}$, on a

$$c_n(\mathrm{F}) = \frac{1}{a}\int_0^a \mathrm{F}(x)e^{-2i\pi nx/a}\,dx = \frac{1}{a}\int_0^a \sum_{m\in\mathbf{Z}} f(x+ma)e^{-2i\pi nx/a}\,dx.$$

Par convergence uniforme de la série pour $x \in [0;a]$, on peut intervertir intégration et sommation, d'où

$$\begin{aligned}
c_n(\mathrm{F}) &= \frac{1}{a}\sum_{m\in\mathbf{Z}}\int_0^a f(x+ma)e^{-2i\pi nx/a}\,dx \\
&= \frac{1}{a}\sum_{m\in\mathbf{Z}}\int_{ma}^{(m+1)a} f(x)e^{-2i\pi n(x-ma)/a}\,dx \\
&= \frac{1}{a}\sum_{m\in\mathbf{Z}}\int_{ma}^{(m+1)a} f(x)e^{-2i\pi nx/a}\,dx \\
&= \frac{1}{a}\int_{-\infty}^{\infty} f(x)e^{-2i\pi nx/a}\,dx \\
&= \widehat{f}(n/a).
\end{aligned}$$

Comme F est de classe $\mathscr{C}^1$, elle est somme de sa série de Fourier, d'où la relation :

$$\sum_{m\in\mathbf{Z}} f(x+am) = \frac{1}{a}\sum_{n\in\mathbf{Z}} \widehat{f}(n/a)e^{2i\pi nx/a},$$

pour tout $x \in \mathbf{R}$. En prenant $x = 0$, on obtient l'autre relation. □

3.7. Principe d'incertitude en théorie de l'information

L'inégalité suivante est le prototype des principes d'incertitude.

Proposition **(3.7.1)** (Inégalité de Heisenberg). — *Soit* $f : \mathbf{R} \to \mathbf{C}$ *une fonction localement intégrable telle que* $|f|^2$ *soit intégrable. On a*

$$\left(\int_{-\infty}^{\infty} x^2 |f(x)|^2 \, dx\right)\left(\int_{-\infty}^{\infty} y^2 |\widehat{f}(y)|^2 \, dy\right) \geqslant \frac{1}{16\pi^2}\left(\int_{-\infty}^{\infty} |f(x)|^2 \, dx\right)^2.$$

En mécanique quantique, $|f(x)|^2$ représente la densité de probabilité de présence d'une particule, en fonction de la position x, de même que $|f(y)|^2$ représente la densité de probabilité d'une particule ayant la quantité de mouvement y. Si sa position moyenne et sa quantité moyenne est nulle (le cas général est similaire), le membre de gauche est le produit de la variance de la position par la variance de la quantité de mouvement et l'inégalité de Heisenberg minore ce produit par une constante $(1/16\pi^2)$. On dit ainsi qu'on ne peut connaître précisément la position et la quantité de mouvement d'une particule, et c'est dans ce contexte de mécanique quantique que le physicien allemand Heisenberg (1927) avait énoncé (en 1927) cette inégalité d'incertitude. La démonstration de l'énoncé mathématique est due à Kennard (1927), et celle que nous allons suivre est essentiellement celle de Weyl (1950).

Démonstration. — On ne la démontre que pour f de classe $\mathscr{C}^1$, continue et à support compact. Par intégration par parties, on a

$$\begin{aligned}\int_{-\infty}^{\infty} |f(x)|^2 \, dx &= -\int_{-\infty}^{\infty} x(|f^2|')(x) \, dx \\ &= \int_{-\infty}^{\infty} x(f'(x)\overline{f(x)} + f(x)\overline{f'(x)}) \, dx \\ &\leqslant 2\int_{-\infty}^{\infty} |x||f'(x)||f(x)| \, dx.\end{aligned}$$

Appliquons l'inégalité de Cauchy–Schwarz : on obtient alors

$$\int_{-\infty}^{\infty} |f(x)|^2 \, dx \leqslant 2\left(\int_{-\infty}^{\infty} |x|^2 |f(x)|^2 \, dx\right)^{1/2}\left(\int_{-\infty}^{\infty} |f'(x)|^2 \, dx\right)^{1/2}.$$

D'après la formule de Plancherel, on a ensuite

$$\begin{aligned}\int_{-\infty}^{\infty} |f'(x)|^2\,dx &= \int_{-\infty}^{\infty} |\widehat{f'}(y)|^2\,dy \\ &= \int_{-\infty}^{\infty} |2\pi i y\widehat{f}(y)|^2\,dy \\ &= 4\pi^2 \int_{-\infty}^{\infty} |y|^2|\widehat{f}(y)|^2\,dy.\end{aligned}$$

En combinant ces inégalités, on obtient

$$\begin{aligned}\left(\int_{-\infty}^{\infty} |f(x)|^2\,dx\right)^2 &\leqslant 4\int_{-\infty}^{\infty} |x||f'(x)||f(x)|\,dx \\ &\leqslant 4\left(\int_{-\infty}^{\infty} |x|^2|f(x)|^2\,dx\right)\left(\int_{-\infty}^{\infty} |f'(x)|^2\,dx\right) \\ &\leqslant 4\left(\int_{-\infty}^{\infty} |x|^2|f(x)|^2\,dx\right)\left(4\pi^2\int_{-\infty}^{\infty} |y|^2|\widehat{f}(y)|^2\,dy\right) \\ &\leqslant 16\pi^2\left(\int_{-\infty}^{\infty} |x|^2|f(x)|^2\,dx\right)\left(\int_{-\infty}^{\infty} |y|^2|\widehat{f}(y)|^2\,dy\right),\end{aligned}$$

ce qu'il fallait démontrer. □

3.7.2. — La suite de ce paragraphe est consacrée à des variantes du théorème d'incertitude dans le contexte de la théorie de l'information. Une motivation peut être le théorème d'échantillonnage : il s'applique à des fonctions f dont la transformée de Fourier est à support compact — autrement dit, des signaux dont le spectre est localisé — et le principe d'incertitude affirme que de telles fonctions ne peuvent pas être à support compact : il est impossible pour un signal d'être localisé à la fois en temps et en fréquence. Plus généralement, on a la proposition suivante.

Proposition **(3.7.3)**. — *Soit* $f : \mathbf{R} \to \mathbf{C}$ *une fonction intégrable sur* $\mathbf{R}$*, non identiquement nulle. On suppose qu'il existe un nombre réel* $\mathrm{W} \geqslant 0$ *tel que sa transformée de Fourier s'annule hors de l'intervalle* $[-\mathrm{W}; \mathrm{W}]$*. Alors il n'existe pas d'intervalle* $[u; v]$*, où* $u < v$*, sur lequel* f *soit identiquement nulle.*

Démonstration. — On raisonne par contraposition en considérant une fonction f, intégrable sur $\mathbf{R}$, qui est identiquement nulle sur un tel intervalle $[u; v]$ et dont

la transformée de Fourier est supportée par l'intervalle $[-\mathrm{W}; \mathrm{W}]$; on va prouver qu'en fait, f est identiquement nulle.

La formule d'inversion de Fourier donne, pour tout $x \in [u; v]$, on a

$$f(x) = \int_{-\mathrm{W}}^{\mathrm{W}} \widehat{f}(y) e^{2\pi i x y}\, dy = 0,$$

et de même pour les dérivées de f :

$$\int_{-\mathrm{W}}^{\mathrm{W}} \widehat{f}(y)(2\pi i y)^p e^{2\pi i x y}\, dy = 0,$$

pour tout entier $p \geqslant 0$. Reprenons alors la formule d'inversion de Fourier pour un nombre réel x quelconque :

$$f(x) = \int_{-\mathrm{W}}^{\mathrm{W}} \widehat{f}(y) e^{2\pi i x y}\, dy = \int_{-\mathrm{W}}^{\mathrm{W}} \widehat{f}(y) e^{2\pi i (x-u) y} e^{2\pi i u y}\, dy.$$

Développons l'exponentielle en série :

$$e^{2\pi i (x-u) y} = \sum_{p=0}^{\infty} \frac{1}{p!} (2\pi i y)^p (x-u)^p,$$

de sorte que

$$f(x) = \sum_{p=0}^{\infty} \frac{1}{p!} (x-u)^p \int_{-\mathrm{W}}^{\mathrm{W}} \widehat{f}(y)(2\pi i y)^p e^{2\pi i u y}\, dy = 0.$$

Cela prouve que f est identiquement nulle. □

3.7.4. — Considérons une fonction $f : \mathbf{R} \to \mathbf{C}$ qui est intégrable, de sorte à pouvoir parler de sa transformée de Fourier ; supposons-la normalisée par

$$\int_{-\infty}^{\infty} |f(x)|^2\, dx = 1.$$

D'après la formule de Parseval, on a également

$$\int_{-\infty}^{\infty} |\widehat{f}(y)|^2\, dy = 1.$$

Un thème important de la théorie de l'information consiste à isoler la partie du signal représenté par f qui est située dans un intervalle $[-a; a]$, et à poser

$$\mathrm{U}_a(f) = \int_{-a}^{a} |f(x)|^2\, dx.$$

On a $\mathrm{U}_a(f) \in [0;1]$ et, en quelque sorte, $\mathrm{U}_a(f)$ représente l'énergie du signal qui est localisée dans l'intervalle de temps $[-a;a]$. De même, on peut isoler la partie du signal dont le spectre est situé dans un intervalle $[-b;b]$ et on pose

$$\mathrm{V}_b(f) = \int_{-b}^{b} |\widehat{f}(y)|^2 \, dy \; ;$$

ainsi, on a $\mathrm{V}_b(f) \in [0;1]$ et $\mathrm{V}_b(f)$ représente l'énergie du signal représenté par f qui est localisée dans l'intervalle de fréquences $[-b;b]$. D'après la proposition précédente, on ne peut pas avoir $\mathrm{U}_a(f) = \mathrm{V}_b(f) = 1$.

Théorème **(3.7.5)** (Slepian, Landau, Pollak). — *Il existe un nombre réel $\theta > 0$ tel que pour toute fonction $f \in \mathrm{L}_2$, on ait*

$$\arccos(\sqrt{\mathrm{U}_a(f)}) + \arccos(\sqrt{\mathrm{V}_b(f)}) \geqslant \theta.$$

La démonstration requiert un peu plus d'analyse fonctionnelle que nous ne voulons en mettre en œuvre dans ce cours, et nous nous contentons d'en esquisser les grandes lignes, en renvoyant aux articles Slepian & Pollak (1961); Landau & Pollak (1961) et au livre Dym & McKean (2016) — où les lecteurs et lectrices trouveront d'ailleurs d'autres applications à la théorie de l'information.

Notons L_2 l'espace des fonctions de $\mathbf{R}$ dans $\mathbf{C}$ qui sont de carré intégrable (modulo fonctions nulles presque partout) ; il est muni du produit scalaire défini par $\langle f, g\rangle = \int_{\mathbf{R}} \overline{f}(x) g(x) \, dx$ qui en fait un espace de Hilbert. On notera $\|f\|_2 = (\langle f, f\rangle)^{1/2}$ la norme correspondante, pour $f \in \mathrm{L}_2$. On rappelle aussi l'inégalité de Cauchy–Schwarz : $|\langle f, g\rangle| \leqslant \|f\|_2 \, \|g\|_2$.

Soit A l'application linéaire de troncation en temps : pour toute fonction f,

$$\mathrm{A}(f)(x) = \begin{cases} f(x) & \text{si } |x| \leqslant a, \\ 0 & \text{sinon.} \end{cases}$$

Cette application linéaire est un projecteur ($\mathrm{A} \circ \mathrm{A} = \mathrm{A}$) orthogonal ($\mathrm{A}^* = \mathrm{A}$) et son image est le sous-espace vectoriel fermé V des fonctions de L_2 qui sont nulles (presque partout) hors de $[-a;a]$.

De même, soit B l'application linéaire de troncation en fréquence : pour toute fonction f,

$$\widehat{\mathrm{B}(f)}(y) = \begin{cases} \widehat{f}(y) & \text{si } |y| \leqslant b, \\ 0 & \text{sinon.} \end{cases}$$

Compte tenu de la formule d'inversion de Fourier, on a donc

$$\mathrm{B}(f)(x) = \int_{-b}^{b} \widehat{f}(y) e^{2\pi i x y}\, dy.$$

C'est également un projecteur orthogonal, son image est le sous-espace vectoriel fermé W de L_2 constitué des fonctions dont la transformée de Fourier est nulle (presque partout) hors de $[-b; b]$. Ces fonctions sont très particulières : grâce au fait que le domaine d'intégration est limité à l'intervalle $[-b; b]$, on peut dériver sous le signe somme dans la formule d'inversion de Fourier, de sorte que W est formé de fonctions indéfiniment dérivables. De plus, si $g \in \mathrm{W}$, on a des inégalités, pour tout $k \geqslant 0$,

$$|g^{(k)}(x)| = |\int_{-b}^{b} (2\pi i y)^k \widehat{g}(y) e^{2\pi i x y}\, dy| \leqslant (2\pi b)^k \sqrt{2b}\, \|g\|.$$

Proposition **(3.7.6)**. — *On a* $\|\mathrm{B} \circ \mathrm{A}\| < 1$.

La norme $\|\mathrm{B} \circ \mathrm{A}\|$ de l'application linéaire $\mathrm{B} \circ \mathrm{A}$ est le plus petit nombre réel γ tel que $\|\mathrm{B} \circ \mathrm{A}(f)\| \leqslant \gamma \|f\|$ pour tout $f \in \mathrm{L}_2$. Comme A et B sont des projecteurs orthogonaux, on a $\|\mathrm{B} \circ \mathrm{A}(f)\| \leqslant \|\mathrm{A}(f)\| \leqslant \|f\|$, de sorte que $\gamma \leqslant 1$. Le point crucial est que l'on a $\gamma < 1$.

Géométriquement, cela signifie que les sous-espaces V et W forment un angle au moins $\arccos(\gamma) > 0$. Prenons en effet $f \in \mathrm{V}$ et $g \in \mathrm{W}$. L'angle $\theta(f, g)$ que font ces fonctions dans L_2 apparaît dans l'inégalité de Cauchy–Schwarz :

$$\mathrm{Re}(\langle f, g\rangle) = \cos(\theta(f, g))\, \|f\|\, \|g\|.$$

Puisque $f \in \mathrm{V}$ et $g \in \mathrm{W}$, on a $f = \mathrm{A}(f)$ et $g = \mathrm{B}(g)$, de sorte que

$$\langle f, g\rangle = \langle \mathrm{A}(f), \mathrm{B}(g)\rangle = \langle \mathrm{B} \circ \mathrm{A}(f), g\rangle.$$

D'après l'inégalité de Cauchy–Schwarz, on a donc

$$\mathrm{Re}(\langle f, g\rangle) \leqslant |\langle f, g\rangle| \leqslant |\langle \mathrm{B} \circ \mathrm{A}(f), g\rangle| \leqslant \|\mathrm{B} \circ \mathrm{A}(f)\|\, \|g\| \leqslant \gamma\, \|f\|\, \|g\|,$$

d'où l'inégalité $\cos(\theta(f, g)) \leqslant \gamma$.

Comme premier pas, démontrons que l'angle $\theta(f, g)$ n'est jamais nul — de manière équivalente, on a $\mathrm{V} \cap \mathrm{W} = 0$. En effet, d'après la proposition 3.7.3, seule la fonction nulle est à support compact de même que sa transformée de Fourier.

Du point de vue de la théorie du signal, cette inégalité $\|\mathrm{B} \circ \mathrm{A}(f)\| < 1$ se traduit par le phénomène très concret que si l'on applique successivement une troncation en temps puis une troncation en fréquences — ce que l'on fait automatiquement

lorsqu'on ne considère un signal que pendant une durée limitée puis qu'on n'en perçoit que certaines fréquences — l'énergie du signal obtenu n'est qu'une fraction de celle du signal initial.

Démonstration. — Comme $\mathrm{A}(f) = f$ pour $f \in \mathrm{V}$ et $\|\mathrm{A}\| \leqslant 1$, on a

$$\gamma = \|\mathrm{B} \circ \mathrm{A}\| = \sup_{f \in \mathrm{V}} \frac{\|\mathrm{B}(f)\|}{\|f\|} \|\mathrm{B}|_{\mathrm{V}}\|.$$

De manière symétrique, on a également

$$\gamma = \sup_{g \in \mathrm{W}} \frac{\|\mathrm{A}(g)\|}{\|g\|} = \|\mathrm{A}|_{\mathrm{W}}\|.$$

Soit $g \in \mathrm{W}$. Par inversion de Fourier, on a

$$g(x) = \int_{\mathbf{R}} \widehat{g}(y) e^{2\pi i x y}\, dy = \int_{-b}^{b} \widehat{g_n}(y) e^{2\pi i x y}\, dy,$$

de sorte que

$$\mathrm{A}(g)(x) = \begin{cases} \int_{-b}^{b} \widehat{g_n}(y) e^{2\pi i x y}\, dy & \text{si } |x| \leqslant a, \\ 0 & \text{sinon.} \end{cases}$$

Choisissons une suite (g_n) de fonctions de W telles que $\|g_n\| = 1$ et $\|\mathrm{A}(g_n)\| \to \gamma$. On a vu que les fonctions (g_n) et leurs dérivées sont bornées dans tout intervalle borné. On applique maintenant le théorème d'Ascoli en analyse fonctionnelle. Il garantit que l'on peut extraire de la suite (g_n) une sous-suite qui, sur tout intervalle borné, converge uniformément ainsi que toutes ses dérivées. Notons g la limite de cette suite. Supposons, pour simplifier les notations, que g_n converge uniformément, ainsi que ses dérivées, vers g sur tout intervalle borné.

Comme $\|g_n\| \leqslant 1$, on a

$$\int_{-a}^{a} g(x)^2\, dx = \lim_{n \to +\infty} \int_{-a}^{a} g_n(x)^2\, dx \leqslant 1.$$

Par suite, $\|g\| \leqslant 1$; en particulier, $g \in \mathrm{L}_2$.

En fait, g appartient même au sous-espace W. Considérons en effet une fonction h dans L_2, nulle sur $[-b; b]$. On a donc $h\widehat{g_n} = 0$ pour tout n ; compte tenu de l'égalité de Plancherel, on a donc

$$\langle \widehat{h}, g_n \rangle = \langle h, \widehat{g_n} \rangle = 0.$$

Si $\widehat{h}$ est intégrable sur $\mathbf{R}$, le théorème de convergence dominée de Lebesgue entraîne que le membre de gauche tend vers $\langle \widehat{h}, g \rangle$. On en déduit que $\langle \widehat{h}, g \rangle = 0$,

puis que $\langle h, \widehat{g}\rangle = 0$. Les conditions sur h permettent d'en conclure que $\widehat{g}$ est nulle hors de $[-b; b]$, ce qu'il fallait démontrer.

Comme g_n converge uniformément vers g sur $[-a; a]$, on a $\|\mathrm{A}(g)\| = \lim \|\mathrm{A}(g_n)\| = \gamma$. Comme $\|\mathrm{A}(g)\| \leqslant \gamma \|g\|$, on en déduit que $\|g\| = 1$.

Démontrons enfin que $\mathrm{B} \circ \mathrm{A}(g) = \gamma g$. Soit $h \in \mathrm{W}$. Pour $t \in \mathbf{C}$, l'inégalité $\|\mathrm{A}(g + th)\|^2 \leqslant \gamma \|g + th\|^2$ s'écrit

$$\mathrm{Re}(t(\langle \mathrm{A}g, \mathrm{A}h\rangle - \gamma\langle g, h\rangle)) \leqslant t^2 \left(\|\gamma\| h^2 - \|\mathrm{A}(h)\|^2\right).$$

Pour t proche de 0, elle entraîne l'*égalité* $\langle \mathrm{A}(g), \mathrm{A}(h)\rangle = \gamma\langle g, h\rangle$. On en déduit que pour tout $h \in \mathrm{L}_2$, on a

$$0 = \langle \mathrm{A}(g) - \gamma g, \mathrm{B}(h)\rangle = \langle \mathrm{B} \circ \mathrm{A}(g) - \gamma g, h\rangle,$$

et donc que $\mathrm{B} \circ \mathrm{A}(g) = \gamma g$.

Comme $\|\mathrm{A}(g)\| \leqslant 1$, l'égalité $\gamma = 1$ entraînerait que $\|\mathrm{A}(g)\| = 1$, d'où $\mathrm{A}(g) = g$ et $g \in \mathrm{V}$. Or, on a vu que $\mathrm{V} \cap \mathrm{W} = 0$. ainsi, $\gamma < 1$. □

Démonstration. — Soit $f \in \mathrm{L}_2$ tel que $\|f\| = 1$. Posons $\alpha = \arccos(\sqrt{\mathrm{U}_a(f)})$ et $\beta = \arccos(\sqrt{\mathrm{V}_b(f)})$. Dire que $\|\mathrm{A}(f)\|^2 = \mathrm{U}_a(f) = \cos^2(\alpha)$ signifie que l'angle formé par les vecteurs f et $\mathrm{A}(f)$ (dans $[0; \pi/2]$) est égal à α. De même, l'angle des vecteurs f et $\mathrm{B}(f)$ est égal à β. Par suite, l'angle θ formé par les vecteurs $\mathrm{A}(f)$ et $\mathrm{B}(f)$ est au plus égal à $\alpha + \beta$.

D'autre part, cet angle θ vérifie $\mathrm{Re}(\langle \mathrm{A}(f), \mathrm{B}(f)\rangle) = \cos(\theta) \|\mathrm{A}(f)\| \|\mathrm{B}(f)\| \leqslant \gamma \|\mathrm{A}(f)\| \|\mathrm{B}(f)\|$, de sorte que $\alpha + \beta \geqslant \theta \geqslant \arccos(\gamma)$. Cela conclut la démonstration du théorème. □

Remarque **(3.7.7)**. — En fait, Landau & Pollak (1961) démontrent que l'inégalité du théorème (avec $\theta = \arccos(\|\mathrm{B} \circ \mathrm{A}\|)$) est une condition nécessaire et suffisante pour l'existence de $f \in \mathrm{L}_2$ telle que $\|f\| = 1$ et $\mathrm{U}_a(f), \mathrm{V}_b(f)$ données dans $[0; 1]$, à deux exceptions près : si $\mathrm{U}_a(f) = 0$, on ne peut avoir $\mathrm{V}_b(f) = 1$, et si $\mathrm{U}_a(f) = 1$, on ne peut avoir $\mathrm{V}_b(f) = 0$.

3.8. Exercices

Exercice **(3.8.1)**. — Soit f une fonction 2π-périodique qui vaut -1 sur $]-\pi; 0[$ et 1 sur $]0; \pi[$.

a) Calculer ses coefficients de Fourier.

b) Appliquer le théorème de Dirichlet en 0 ; en $\pi/2$.

c) Appliquer la formule de Parseval.

Exercice **(3.8.2)**. — Soit f la fonction 2π-périodique telle que $f(t) = \pi - |t|$ pour $t \in [-\pi; \pi]$.

a) Calculer ses coefficients de Fourier.

b) Calculer les sommes des séries

$$\sum_{n=0}^{\infty} \frac{1}{(2n+1)^2}, \qquad \sum_{n=1}^{\infty} \frac{1}{n^2}, \qquad \sum_{n=0}^{\infty} \frac{1}{(2n+1)^4}, \qquad \sum_{n=1}^{\infty} \frac{1}{n^4}.$$

Exercice **(3.8.3)**. — Soit f la fonction 2π-périodique telle que $f(t) = t(\pi - |t|)$ pour $t \in [-\pi; \pi]$.

a) Calculer ses coefficients de Fourier.

b) Calculer les sommes des séries

$$\sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)^3}, \qquad \sum_{n=0}^{\infty} \frac{1}{(2n+1)^6}, \qquad \sum_{n=1}^{\infty} \frac{1}{n^6}.$$

Exercice **(3.8.4)**. — Soit a un nombre réel. Soit f une fonction 2π-périodique telle que $f(t) = \cos(at)$ pour $t \in]-\pi; \pi[$.

a) Calculer ses coefficients de Fourier.

b) Démontrer la formule, pour $a \notin \mathbf{Z}$,

$$\pi \operatorname{cotan}(\pi a) = \frac{1}{a} + \sum_{n=1}^{\infty} \frac{2a}{a^2 - n^2}.$$

c) Démontrer la formule

$$\sin(\pi a) = \pi a \prod_{n=1}^{\infty} \left(1 - \frac{a^2}{n^2}\right).$$

Exercice **(3.8.5)**. — Soit p un nombre réel non nul et soit f la fonction 2π-périodique telle que $f(x) = e^{px}$ pour $0 \leqslant x < 2\pi$.

a) Calculer les coefficients de Fourier complexes de f.

b) Calculer $\displaystyle\sum_{n=0}^{\infty} \frac{1}{p^2 + n^2}$.

Exercice **(3.8.6)**. — Soit f, g des fonctions de période T, continues par morceaux. On pose

$$f * g(x) = \frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} f(t) g(x-t)\, dt.$$

a) Démontrer que $f * g$ est périodique de période T ; justifier qu'elle est continue.

b) Démontrer que les coefficients de Fourier de $f * g$ vérifient

$$c_n(f * g) = c_n(f) c_n(g)$$

pour tout $n \in \mathbf{Z}$.

Exercice **(3.8.7)**. — On propose dans cet exercice une autre démonstration de la convergence de séries de Fourier, due à Chernoff (1980) et Redheffer (1984).

Soit f une fonction de $\mathbf{R}$ dans $\mathbf{C}$, T-périodique, localement intégrable. Soit $a \in \mathbf{R}$.

a) On suppose que f est dérivable en a. Soit F la fonction définie par $\mathrm{F}(t) = (f(t) - f(a))/(e^{2i\pi(t-a)/\mathrm{T}} - 1)$. Justifier que F se prolonge en une fonction continue, T-périodique. Relier les coefficients de Fourier de f à ceux de F.

b) Sous les hypothèses de la question précédente, en déduire que la série de Fourier de f converge vers $f(a)$ en c. Pouvez-vous donner des hypothèses un peu plus faibles que la dérivabilité en c qui garantissent le même résultat ?

c) Soit δ un nombre réel tel que $0 < \delta < \mathrm{T}/2$ et soit φ la fonction T-périodique définie pour $t \in [a - \mathrm{T}/2; a + \mathrm{T}/2]$, par $\varphi(t) = -1$ si $a - \delta < t < a$, $\varphi(t) = 1$ si $a < t < a + \delta$, et $\varphi(t) = 0$ sinon. Calculer sa série de Fourier. Justifier qu'elle converge vers 0 en $t = a$.

d) On suppose que f est $\mathscr{C}^1$ par morceaux au voisinage de a. Démontrer que la série de Fourier de f en a converge vers $\frac{1}{2}(f(a^-) + f(a^+))$.

Exercice **(3.8.8)**. — Pour $x \in \mathbf{R}$ et pour tout entier n tel que $n \geqslant 1$, on pose

$$\mathrm{S}_n(x) = \sum_{k=1}^{n} \frac{\sin((2k-1)x)}{2k-1}.$$

a) Démontrer que pour tout $x \in]0; \pi[$, on a $\mathrm{S}_n(x) \longrightarrow \pi/4$.

b) Calculer la dérivée de S_n. En déduire que les extrema relatifs de S_n sur $[0; \pi]$ sont les $m_k = \mathrm{S}_n(k\pi/2n)$, pour k entier tel que $0 \leqslant k \leqslant 2n$, avec un maximum local si k est impair et un minimum local si k est pair.

c) Démontrer que $m_1 \geqslant m_3 \geqslant \cdots \geqslant m_{2\lfloor n/2 \rfloor - 1}$. En déduire que $\sup(\mathrm{S}_n) = m_1$.

d) Démontrer que $\lim_{n\to+\infty} \sup(S_n) = \frac{2}{\pi}\int_0^\pi \sin(t)/t\, dt$. En particulier, on a $\lim_n \sup(S_n) > \sup(\lim_n S_n)$. (*Phénomène de Gibbs*)

Exercice **(3.8.9)**. — Soit $f : \mathbf{R} \to \mathbf{R}$ la fonction définie par $f(x) = e^{-\pi x^2}$. Soit g sa transformée de Fourier.

a) À l'aide de la formule $f'(x) = -2\pi x f(x)$, démontrer que g est solution de l'équation différentielle $g'(y) = -2\pi y g(y)$. En déduire qu'il existe $c \in \mathbf{R}$ tel que $g = cf$.

b) Démontrer que $c^2 = 1$, puis que $c = 1$. En déduire également que $\int_{\mathbf{R}} e^{-\pi x^2}\, dx = 1$.

Exercice **(3.8.10)**. — On pose $f(x) = e^{-|x|}$.

a) Calculer sa transformée de Fourier.

b) Que donne la formule d'inversion de Fourier en 0 ? La vérifier directement. L'égalité de Plancherel ?

Exercice **(3.8.11)**. — Soit f la fonction de $\mathbf{R}$ dans $\mathbf{R}$ donnée par $f(x) = \sup(0, 1 - |x|)$.

a) Calculer sa transformée de Fourier.

b) En déduire l'égalité

$$\int_{-\infty}^{\infty} (\mathrm{sinc}(\pi y))^2\, dy = 1.$$

Exercice **(3.8.12)**. — *a*) Soit f la fonction de $\mathbf{R}$ dans $\mathbf{R}$ définie par $f(x) = 1$ pour $x \in [-1; 1]$ et $f(x) = 0$ sinon. Calculer sa transformée de Fourier

b) Démontrer que l'intégrale suivante converge

$$\int_0^{\infty} \left(\frac{\sin(t)}{t}\right)^2 dt$$

et calculer sa valeur.

c) Démontrer que l'intégrale suivante converge

$$\int_0^{\infty} \frac{\sin(t)}{t}\, dt$$

et calculer sa valeur.(*Écrire l'intégrale entre* 0 *et* T *et intégrer par parties.*)

3.9. Solutions des exercices

Solution de l'exercice (3.8.1). — L'énoncé ne définit pas la fonction f aux multiples de π ; en fixant $f(n\pi) = 0$ pour tout $n \in \mathbf{Z}$, on la prolonge en une fonction continue par morceaux définie sur $\mathbf{R}$, 2π-périodique et impaire. Ses coefficients de Fourier en cosinus sont donc nuls ; calculons ses coefficients de Fourier en sinus. Pour tout $n \in \mathbf{N}^*$, on a ainsi

$$\begin{aligned} b_n(f) &= \frac{2}{2\pi}\int_{-\pi}^{\pi} f(t)\sin(nt)\,dt = \frac{2}{\pi}\int_0^{\pi} f(t)\sin(nt)\,dt \\ &= \frac{2}{\pi}\int_0^{\pi}\sin(nt)\,dt = \frac{2}{\pi}\left[-\frac{1}{n}\cos(nt)\right]_0^{\pi} \\ &= \frac{2}{\pi n}\left(1-\cos(n\pi)\right) = \begin{cases} 0 & \text{si } n \text{ est pair ;} \\ 4/\pi n & \text{sinon.} \end{cases} \end{aligned}$$

a) La fonction f est de classe $\mathscr{C}^1$ par morceaux ; le théorème de Dirichlet s'applique et affirme que pour tout $t \in \mathbf{R}$, la série de Fourier de f en t converge vers la moyenne des limites de f à droite et à gauche en t.

En $t = 0$, la limite à gauche de f est -1, sa limite à droite est 1 ; et la série de Fourier est identiquement nulle cas $\sin(0) = 0$. Le théorème de Dirichlet fournit donc l'égalité $0 = \frac{1}{2}(-1+1) = 0$.

La fonction f est continue en $t = \pi/2$, de valeur 1. Par ailleurs, si $n \in \mathbf{N}$ est impair, on écrit $n = 2p+1$, avec $p \in \mathbf{N}$; on a alors $\sin(n\pi/2) = (-1)^p$ et $b_n(f) = 4/\pi n = 4/(2p+1)\pi$. Le théorème de Dirichlet donne donc

$$\sum_{p=0}^{\infty}\frac{(-1)^p}{2p+1} = \frac{\pi}{4}.$$

b) Le membre de gauche de la formule de Parseval est

$$\frac{1}{2\pi}\int_0^{2\pi}|f(t)|^2\,dt = \frac{1}{2\pi}\int_0^{2\pi}dt = 1.$$

Comme les coefficients de Fourier $a_n(f)$ sont nuls, son membre de droite est

$$\frac{1}{2}\sum_{n=1}^{\infty}|b_n(f)|^2 = \frac{1}{2}\sum_{p=0}^{\infty}\frac{16}{\pi^2(2p+1)^2}.$$

On obtient donc l'égalité

$$\sum_{p=0}^{\infty} \frac{1}{(2p+1)^2} = \frac{\pi^2}{8}.$$

Solution de l'exercice (3.8.2). — *a*) La fonction f est continue, $\mathscr{C}^1$ par morceaux et paire ; on calcule ses coefficients en cosinus. Pour $n \in \mathbf{N}$, on a

$$a_n(f) = \frac{2}{2\pi}\int_{-\pi}^{\pi} f(t)\cos(nt)\,dt = \frac{2}{\pi}\int_0^{\pi} (\pi - t)\cos(nt)\,dt.$$

On intègre par parties mais il faut faire le calcul pour $n = 0$ de façon indépendantes. On a

$$a_0(f) = \frac{2}{\pi}\int_0^{\pi} (\pi - t)\,dt = \frac{2}{\pi}\left[\pi t - \frac{1}{2}t^2\right]_0^{\pi} = \pi.$$

Pour $n \neq 0$, il vient alors

$$\begin{aligned} a_n(f) &= \frac{2}{\pi}\left[(\pi - t)\frac{1}{n}\sin(nt)\right]_0^{\pi} + \frac{2}{\pi n}\int_0^{\pi}\sin(nt)\,dt \\ &= \frac{2}{\pi n}\left[-\frac{1}{n}\cos(nt)\right]_0^{\pi} \\ &= \frac{2}{\pi n^2}(1 - \cos(n\pi)) = \begin{cases} 0 & \text{si } n \text{ est pair ;} \\ 4/\pi n^2 & \text{sinon.} \end{cases} \end{aligned}$$

b) Le théorème de Dirichlet en $t = 0$ fournit

$$\pi = f(0) = \frac{1}{2}\pi + \frac{4}{\pi}\sum_{p=0}^{\infty}\frac{1}{(2p+1)^2}.$$

Par conséquent,

$$\sum_{p=0}^{\infty} \frac{1}{(2p+1)^2} = \frac{\pi^2}{8}.$$

On remarque la que la série $S = \sum_{n=1}^{\infty}\frac{1}{n^2}$ contient la précédente (somme des termes d'indice impair), le reste étant la somme des termes d'indice pair. Si $n = 2m$, on a $1/n^2 = 1/(4m^2)$, de sorte que la somme des termes d'indice pair s'identifie à $S/4$. Cela entraîne la relation

$$S = \frac{\pi^2}{8} + \frac{1}{4}S,$$

d'où $3S/4 = \pi^2/8$ puis

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

La troisième série se calcule en appliquant la formule de Parseval à f. On a d'abord

$$\frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)^2\,dt = \frac{1}{\pi}\int_0^{\pi} (\pi - t)^2\,dt = \frac{1}{\pi}\left[-\frac{1}{3}(\pi - t)^3\right]_0^{\pi} = \frac{\pi^2}{3}.$$

On a donc

$$\frac{\pi^2}{3} = \frac{1}{4}\pi^2 + \frac{1}{2}\sum_{p=0}^{\infty} \frac{16}{\pi^2}\frac{1}{(2p+1)^4},$$

d'où

$$\sum_{p=0}^{\infty} \frac{1}{(2p+1)^4} = \frac{\pi^4}{96}.$$

Enfin, la quatrième série, T, s'identifie, par le même raisonnement que la seconde, à la troisième plus 2^{-4}T. Ainsi, $\frac{15}{16}\mathrm{T} = \frac{\pi^4}{96}$ et

$$\sum_{p=0}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90}.$$

Solution de l'exercice (3.8.3). — *a*) La fonction f est impaire ; ses coefficients de Fourier en cosinus sont donc nuls. Calculons ceux en sinus. Pour tout entier $n \geqslant 1$, on a :

$$b_n(f) = \frac{2}{2\pi}\int_{-\pi}^{\pi} f(t)\sin(nt)\,dt = \frac{2}{\pi}\int_0^{\pi} t(\pi - t)\sin(nt)\,dt.$$

Intégrons par parties ; on obtient

$$\begin{aligned} b_n(f) &= \frac{2}{\pi}\left[-\frac{1}{n}t(\pi - t)\cos(nt)\right]_0^{\pi} + \frac{2}{n\pi}\int_0^{\pi}(\pi - 2t)\cos(nt)\,dt \\ &= \frac{2}{n\pi}\left[\frac{1}{n}(\pi - 2t)\sin(nt)\right]_0^{\pi} - \frac{2}{n^2\pi}\int_0^{\pi}(-2)\sin(nt)\,dt \\ &= \frac{2}{n^2\pi}\left[-2\frac{1}{n}\cos(nt)\right]_0^{\pi} \\ &= \begin{cases} 0 & \text{si } n \text{ est pair ;} \\ 8/n^3\pi & \text{sinon.} \end{cases} \end{aligned}$$

b) La fonction f est $\mathscr{C}^1$ par morceaux et continue. D'après le théorème de Dirichlet, sa série de Fourier converge vers f en tout point. Choisissons $t = \pi/2$; en écrivant un entier impair n sous la forme $n = 2p + 1$, on a $\sin(nt) = (-1)^p$, de sorte qu'on obtient

$$f(\pi/2) = \frac{\pi^2}{4} = \sum_{p=0}^{\infty} \frac{8}{(2p+1)^3\pi}(-1)^p,$$

et finalement :

$$\sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)^3} = \frac{\pi^3}{32}.$$

Appliquons maintenant le théorème de Parseval. On a donc

$$\sum_{p=0}^{\infty} \frac{1}{(2p+1)^6} = \frac{\pi^2}{64} \sum_{n=1}^{\infty} b_n(f)^2 = \frac{\pi}{64} \int_{-\pi}^{\pi} f(t)^2\, dt = \frac{\pi}{32} \int_0^{\pi} \left(t(\pi - t)^2\right)^2\, dt.$$

Calculons alors l'intégrale qui apparaît :

$$\begin{aligned} \int_0^{\pi} t^2(\pi - t)^2\, dt &= \int_0^{\pi} \left(\pi^2 t^2 - 2\pi t^3 + t^4\right)\, dt \\ &= \pi^2 \cdot \frac{1}{3}\pi^3 - 2\pi \cdot \frac{1}{4}\pi^4 + \frac{1}{5}\pi^5 \\ &= \left(\frac{1}{3} - \frac{1}{2} + \frac{1}{5}\right)\pi^5 = \frac{1}{30}\pi^5. \end{aligned}$$

En fin de compte, on a

$$\sum_{p=0}^{\infty} \frac{1}{(2p+1)^6} = \frac{\pi^6}{960}.$$

Pour calculer la somme $\mathrm{S} = \sum_{n=1}^{\infty} \frac{1}{n^6}$, on procède comme dans les exercices précédents, en séparant la somme des termes d'indices impairs et celle des termes d'indices pairs. La contribution des premiers est $\pi^4/960$, ainsi qu'il vient d'être calculé ; en posant $n = 2m$, on voit que celle des seconds est $\mathrm{S}/2^6 = \mathrm{S}/64$. Ainsi,

$$\mathrm{S}\frac{63}{64} = \frac{\pi^6}{960}$$

d'où

$$\mathrm{S} = \frac{64}{63 \cdot 960}\pi^6 = \frac{1}{15 \cdot 63}\pi^6 = \frac{\pi^6}{945}.$$

Solution de l'exercice (3.8.4). — *a*) L'énoncé ne définit pas f en $n\pi$, pour $n \in \mathbf{Z}$, mais si on la prolonge par $f(n\pi) = \cos(\pi a)$, on obtient une fonction continue, de classe $\mathscr{C}^1$ par morceaux, 2π-périodique et paire. Ses coefficients de Fourier en sinus sont nuls ; calculons ceux en cosinus. Le cas où $a = m \in \mathbf{Z}$ est évident : on trouve $a_n(f) = 0$ pour $n \neq m$ et $a_m(f) = 1$. Supposons maintenant que $a \notin \mathbf{Z}$.

Pour $n \in \mathbf{N}$, on a

$$a_n(f) = \frac{2}{2\pi}\int_{-\pi}^{\pi} f(t)\cos(nt)\,dt = \frac{2}{\pi}\int_0^{\pi} \cos(at)\cos(nt)\,dt.$$

Pour évaluer cette intégrale, on « linéarise » le produit de cosinus :

$$\cos(at)\cos(nt) = \frac{1}{2}\left(\cos((n+a)t) + \cos((n-a)t)\right),$$

de sorte que

$$a_n(f) = \frac{1}{\pi}\int_0^{\pi} \cos((n+a)t)\,dt + \frac{1}{2\pi}\int_0^{\pi} \cos((n-a)t)\,dt.$$

Comme a n'est pas entier, on a

$$\begin{aligned}\int_0^{\pi} \cos((n+a)t)\,dt &= \left[\frac{1}{n+a}\sin((n+a)t)\right]_0^{\pi}\\ &= \frac{1}{n+a}\sin((n+a)\pi)\\ &= \frac{\sin(\pi a)}{n+a}(-1)^n.\end{aligned}$$

En appliquant cette formule pour a et $-a$, on trouve

$$a_n(f) = (-1)^n\frac{\sin(\pi a)}{\pi}\left(\frac{1}{n+a} - \frac{1}{n-a}\right) = (-1)^n\frac{\sin(\pi a)}{\pi}\frac{2a}{a^2-n^2}.$$

b) La fonction f étant continue, $\mathscr{C}^1$ par morceaux et 2π-périodique le théorème de Dirichlet entraîne l'égalité

$$\cos(at) = \frac{1}{2}a_0(f) + \sum_{n=1}^{\infty} a_n(f)\cos(nt) = \frac{\sin(\pi a)}{\pi}\left(\frac{1}{a} + \sum_{n=1}^{\infty}\frac{2a}{a^2-n^2}(-1)^n\cos(nt)\right),$$

pour tout $t \in [-\pi;\pi]$. Posons $t = \pi$ et divisons les deux membres par $\sin(\pi a)/\pi$. Cela donne la relation

$$\pi\cot(\pi a) = \frac{1}{a} + \sum_{n=1}^{\infty}\frac{2a}{a^2-n^2},$$

comme demandé.

c) En introduisant le développement limité $\log(1 - a^2/n^2) = \mathrm{O}(1/n^2)$, on démontre que le produit infini du membre de droite converge vers un nombre réel qui n'est nul que si a est pas entier, définit une fonction dérivable de a. De fait, la dérivée logarithmique de la relation demandée est celle de la question précédente. Cela entraîne que la formule indiquée est vraie à un facteur multiplicatif près sur chaque intervalle de la forme $]m; m+1[$. Lorsque a tend vers 0, le développement limité $\sin(\pi a) \sim \pi a$ montre que l'on a l'égalité demandée sur $]-1; 1[$. En fait, le membre de droite est une fonction 2-périodique de a. Plus précisément, les calculs suivant montrent que lorsque a est changé en $a+1$, le membre de droite est changé en son opposé :

$$
\begin{aligned}
&\pi(a+1)\prod_{n=1}^{\infty}\left(1-\frac{(a+1)^2}{n^2}\right)\\
&\qquad=\lim_{\mathrm{N}\to+\infty}\pi(a+1)\prod_{n=1}^{\mathrm{N}}\left(1-\frac{a+1}{n}\right)\left(1+\frac{a+1}{n}\right)\\
&\qquad=\lim_{\mathrm{N}\to+\infty}\pi(a+1)\prod_{n=1}^{\mathrm{N}}\left(\frac{n-1}{n}-\frac{a}{n}\right)\left(\frac{n+1}{n}+\frac{a}{n}\right)\\
&\qquad=\lim_{\mathrm{N}\to+\infty}\pi(a+1)(-a)\prod_{n=2}^{\mathrm{N}}\frac{n-1}{n}\left(1-\frac{a}{n-1}\right)\frac{n+1}{n}\left(1+\frac{a}{n+1}\right)\\
&\qquad=\lim_{\mathrm{N}\to+\infty}-\pi a(a+1)\frac{\mathrm{N}+1}{\mathrm{N}}\prod_{n=1}^{\mathrm{N}-1}\left(1-\frac{a}{n}\right)\prod_{n=2}^{\mathrm{N}+1}\left(1+\frac{a}{n}\right)\\
&\qquad=\lim_{\mathrm{N}\to+\infty}-\pi a\frac{\mathrm{N}+1}{\mathrm{N}}\left(1-\frac{a}{\mathrm{N}}\right)^{-1}\left(1+\frac{a}{\mathrm{N}+1}\right)\prod_{n=1}^{\mathrm{N}}\left(1-\frac{a}{n}\right)\prod_{n=1}^{\mathrm{N}}\left(1+\frac{a}{n}\right)\\
&\qquad=-\pi a\prod_{n=1}^{\infty}\left(1-\frac{a^2}{n^2}\right)
\end{aligned}
$$

Comme la fonction $\sin(\pi a)$ vérifie la même équation fonctionnelle, on en déduit l'égalité pour tout $a \in \mathbf{R}$.

Solution de l'exercice (3.8.5). — *a*) Par définition, on a, pour tout entier $n \in \mathbf{Z}$,

$$\begin{aligned} c_n(f) &= \frac{1}{2\pi}\int_0^{2\pi} f(x)e^{-inx}\,dx = \frac{1}{2\pi}\int_0^{2\pi} e^{px}e^{-inx}\,dx \\ &= \frac{1}{2\pi}\int_0^{2\pi} e^{(p-in)x}\,dx = \frac{1}{2\pi}\left[\frac{1}{p-in}e^{(p-in)x}\right]_0^{2\pi} \\ &= \frac{e^{2\pi p}-1}{2\pi(p-in)} = (p+in)\frac{e^{2\pi p}-1}{2\pi(p^2+n^2)}, \end{aligned}$$

où l'on a utilisé que $p \neq in$ puisque $p \in \mathbf{R}^*$.

b) La série de Fourier de f s'écrit $\mathrm{S}(f)(x) = \sum c_n(f)e^{inx}$. La fonction f est $\mathscr{C}^1$ par morceaux ; elle est continue sur $]0;2\pi[$, tend vers 1 en 0^+ et vers $e^{2\pi}$ en $2\pi^-$, et donc aussi vers $e^{2\pi}$ en 0^-. On peut donc lui appliquer le théorème de Dirichlet en tout point :

$$\mathrm{S_N}(f)(x) = \sum_{n=-\mathrm{N}}^{\mathrm{N}} c_n(f)e^{inx} \xrightarrow[\mathrm{N}\to\infty]{} \frac{1}{2}\left(f(x^-)+f(x^+)\right).$$

Quand $x = 0$, cela donne

$$\lim_{\mathrm{N}\to\infty}\sum_{n=-\mathrm{N}}^{\mathrm{N}}(p+in)\frac{e^{2\pi p}-1}{2\pi(p^2+n^2)} = \frac{1}{2}\left(e^{2\pi p}+1\right).$$

Regroupons les termes symétriques d'indices n et $-n$ dans la somme de $-\mathrm{N}$ à N ; on obtient

$$\begin{aligned} \mathrm{S_N}(f)(0) &= \frac{e^{2\pi p}-1}{2\pi p} + \sum_{n=1}^{\mathrm{N}}\frac{2p(e^{2\pi p}-1)}{2\pi(p^2+n^2)} \\ &= \frac{e^{2\pi p}-1}{2\pi p} + \frac{2p(e^{2\pi p}-1)}{2\pi}\sum_{n=1}^{\mathrm{N}}\frac{1}{p^2+n^2}. \end{aligned}$$

Si l'on pose $\mathrm{S} = \sum_{n=0}^{\infty} 1/(p^2+n^2)$, on trouve ainsi

$$\frac{1}{p} + 2p\left(\mathrm{S} - \frac{1}{p^2}\right) = \pi\frac{e^{2\pi p}+1}{e^{2\pi p}-1} = \pi\,\mathrm{cotanh}(\pi p).$$

Pour finir,

$$\mathrm{S} = \frac{1}{p^2} - \frac{1}{2p} + \frac{\pi}{2}\,\mathrm{cotanh}(\pi p).$$

Solution de l'exercice (3.8.6). — *a*) Comme g est T-périodique, on a

$$f * g(x+\mathrm{T}) = \frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} f(t) g(x+\mathrm{T}-t)\, dt = \frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} f(t) g(x-t)\, dt = f * g(x),$$

ce qui démontre que $f * g$ est T-périodique. Justifions que $f * g$ est continue. Soit G une « primitive » de g, définie par $\mathrm{G}(x) = \int_0^x g(t)\, dt$; comme g est continue par morceaux, la fonction G est continue ; elle admet même des dérivées à droite et à gauche en tout point. On traite d'abord le cas où f est une fonction en escalier, c'est-à-dire qu'on suppose qu'il existe une subdivision $(t_0, \dots, t_n)$ de $[0; \mathrm{T}]$ telle que pour tout $i \in \{1, \dots, n\}$, la restriction de f à l'intervalle ouvert $]t_{i-1}; t_i[$ soit une constante c_i. Alors, on a

$$f * g(x) = \frac{1}{\mathrm{T}} \sum_{i=1}^{n} c_i \int_{t_{i-1}}^{t_i} g(x-t)\, dt = \frac{1}{\mathrm{T}} \sum_{i=1}^{n} c_i (\mathrm{G}(x-t_{i-1}) - \mathrm{G}(x-t_i)),$$

et cette formule indique que $f * g$ est continue (et même dérivable à droite et à gauche en tout point). Dans le cas général, on utilise le fait que f étant continue par morceaux, on peut l'approcher uniformément par une fonction en escalier $\tilde{f}$ Cela approche $f * g$ uniformément par la fonction continue $\tilde{f} * g$, et on en déduit que $f * g$ est continue.

b) Soit $n \in \mathbf{Z}$. On écrit

$$\begin{aligned} c_n(f * g) &= \frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} (f * g)(x) e^{-2i\pi n x/\mathrm{T}}\, dx \\ &= \frac{1}{\mathrm{T}^2} \int_0^{\mathrm{T}} \left(\int_0^{\mathrm{T}} f(t) g(x-t)\, dt \right) e^{-2i\pi n x/\mathrm{T}}\, dx. \end{aligned}$$

Le théorème de Fubini permet d'échanger l'ordre d'intégration des variables et d'écrire :

$$c_n(f * g) = \frac{1}{\mathrm{T}^2} \int_0^{\mathrm{T}} \left(f(t) g(x-t) e^{-2i\pi n x/\mathrm{T}}\, dx \right) dt.$$

Dans l'intégrale intérieure, t est fixe, de sorte qu'elle vaut

$$f(t) \int_0^{\mathrm{T}} g(x-t) e^{-2i\pi n x/\mathrm{T}}\, dx.$$

Faisons le changement de variables $y = x - t$; on obtient

$$f(t) \int_{x-\mathrm{T}}^{x} g(y) e^{-2i\pi n(y+t)/\mathrm{T}}\, dy = f(t) e^{-2i\pi n t/\mathrm{T}} \int_{x-\mathrm{T}}^{x} g(y) e^{-2i\pi n y/\mathrm{T}}\, dy.$$

Dans cette expression apparaît l'intégrale qui définit le coefficient de Fourier $c_n(g)$ (à un facteur T près), mais sur l'intervalle $[x - \mathrm{T}; x]$; comme c'est une période, cette intégrale vaut bien $\mathrm{T}c_n(g)$. On a donc

$$c_n(f * g) = \frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} f(t) e^{-2i\pi nt/\mathrm{T}} c_n(g)\, dt = c_n(f) c_n(g).$$

Solution de l'exercice (*3.8.7*). — *a*) La fonction F est 2π continue en tout point t tel que $t - a$ n'est pas multiple de 2π ; Lorsque t converge vers a, $\mathrm{F}(t)$ converge vers $f'(a)/(2i\pi/\mathrm{T})$ (règle de L'Hôpital !), ce qui prouve que F se prolonge par continuité. Soit $\mathbf{1}$ la fonction constante égale à 1 et ε la fonction donnée par $\varepsilon(t) = e^{2i\pi t/\mathrm{T}}$. La relation $f(t) = f(a) + (e^{2i\pi(t-a)/\mathrm{T}} - 1)\mathrm{F}(t)$ s'écrit alors

$$f = f(a)\mathbf{1} + e^{-2i\pi a/\mathrm{T}} \varepsilon \mathrm{F} - \mathrm{F},$$

d'où la relation

$$c_n(f) = f(a) c_n(\mathbf{1}) + e^{-2i\pi a/\mathrm{T}} c_n(\varepsilon \mathrm{F}) - c_n(\mathrm{F})$$

entre coefficients de Fourier de f et de F. On note que

$$c_n(\varepsilon \mathrm{F}) = \frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} \varepsilon(t) \mathrm{F}(t) e^{-2i\pi nt/\mathrm{T}}\, dt = \frac{1}{\mathrm{T}} \int_0^{\mathrm{T}} \mathrm{F}(t) e^{-2i\pi(n-1)t/\mathrm{T}}\, dt = c_{n-1}(\mathrm{F}).$$

D'autre part, $c_n(\mathbf{1}) = 1$ si $n = 0$ et $c_n(\mathbf{1}) = 0$ sinon, soit $c_n(\mathbf{1}) = \delta_n$ (indicateur de Kronecker). Finalement,

$$c_n(f) = f(a)\delta_n + e^{-2i\pi a/\mathrm{T}} c_{n-1}(\mathrm{F}) - c_n(\mathrm{F}).$$

b) En $t = a$, la série de Fourier s'écrit (on somme de $\mathrm{M} < 0$ à $\mathrm{N} > 0$) :

$$\begin{aligned}
\sum_{n=\mathrm{M}}^{\mathrm{N}} c_n(f) e^{2i\pi nc/\mathrm{T}} &= f(a) + \sum_{n=\mathrm{M}}^{\mathrm{N}} \left(e^{-2i\pi a/\mathrm{T}} c_{n-1}(\mathrm{F}) - c_n(\mathrm{F}) \right) e^{2i\pi nc/\mathrm{T}} \\
&= f(a) + \sum_{n=\mathrm{M}}^{\mathrm{N}} \left(c_{n-1}(\mathrm{F}) e^{2i\pi(n-1)a/\mathrm{T}} - c_n(\mathrm{F}) e^{2i\pi nc/\mathrm{T}} \right) \\
&= f(a) + c_{\mathrm{M}-1}(\mathrm{F}) e^{2i\pi(\mathrm{M}-1)a/\mathrm{T}} - c_{\mathrm{N}}(\mathrm{F}) e^{2i\pi \mathrm{N}c/\mathrm{T}}.
\end{aligned}$$

Comme F est continue, elle est intégrable et ses coefficients de Fourier tendent vers 0 en $\pm\infty$. Il en résulte que lorsque $\mathrm{M} \to -\infty$ et $\mathrm{N} \to +\infty$, on a

$$\lim_{\substack{\mathrm{M}\to-\infty \\ \mathrm{N}\to+\infty}} \sum_{n=\mathrm{M}}^{\mathrm{N}} c_n(f) e^{2i\pi nc/\mathrm{T}} = f(a).$$

La preuve irait de même sous la simple hypothèse que F est intégrable car cette condition (nécessaire pour définir les coefficients de Fourier de F) entraîne que les coefficients de Fourier de F tendent vers 0. L'existence d'une dérivée à droite et à gauche suffirait.

c) On écrit

$$\begin{aligned} c_n(\varphi) &= \frac{1}{\mathrm{T}} \int_{a-\mathrm{T}/2}^{a+\mathrm{T}/2} \varphi(t) e^{-2i\pi nt/\mathrm{T}}\, dt \\ &= \frac{1}{\mathrm{T}} \left(-\int_{a-\delta}^{a} e^{-2i\pi nt/\mathrm{T}}\, dt + \int_{a}^{a+\delta} e^{-2i\pi nt/\mathrm{T}}\, dt \right) \\ &= \frac{1}{\mathrm{T}} e^{-2i\pi na/\mathrm{T}} \left(-\int_{-\delta}^{0} e^{-2i\pi nt/\mathrm{T}}\, dt + \int_{0}^{\delta} e^{-2i\pi nt/\mathrm{T}}\, dt \right) \\ &= \frac{1}{\mathrm{T}} e^{-2i\pi na/\mathrm{T}} 2i \int_{0}^{\delta} \sin(2\pi nt/\mathrm{T})\, dt. \end{aligned}$$

En particulier, $c_0(\varphi) = 0$. Si $n \neq 0$, on obtient alors

$$c_n(\varphi) = \frac{2i}{\mathrm{T}} e^{-2i\pi na/\mathrm{T}} \left[-\frac{\mathrm{T}}{2\pi n} \cos(2\pi nt/\mathrm{T}) \right]_0^{\delta} = \frac{i}{\pi n} e^{-2i\pi na/\mathrm{T}} \left(1 - \cos(2\pi n\delta/\mathrm{T})\right).$$

En $t = a$, la série de Fourier de φ devient

$$\sum_{n\neq 0} \frac{i}{\pi n} (1 - \cos(2\pi n\delta/\mathrm{T})).$$

Lorsqu'on la somme de façon symétrique, les termes d'indice $-n$ et n s'annulent. Par suite, la série de Fourier de φ converge vers 0 en $t = a$. On observe que φ a des limites à droite $\varphi(a^+) = 1$ et à gauche $\varphi(a^-) = -1$ en a, et que 0 est leur moyenne.

d) Considérons la fonction g donnée par $g(t) = f(t) - \frac{1}{2}(f(a^+) - f(a^-))\varphi(t)$. Elle est encore de classe $\mathscr{C}^1$ par morceaux ; quand t tend vers a à droite ou à gauche, elle tend vers $\frac{1}{2}(f(a^+) + f(a^-))$; prolongeons-la par continuité en a. On peut alors appliquer le début de l'exercice à la fonction g, dont la série de Fourier converge vers $g(a)$ en $t = a$. La série de Fourier de f est celle de g plus celle de φ (multipliée par $(f(a^+) - f(a^-))/2$). D'après la question précédente, elle converge vers $g(a)$ en $t = a$. Comme $g(a) = \frac{1}{2}(f(a^+) + f(a^-))$, cela conclut l'exercice.

Solution de l'exercice (3.8.8). — *a*) Considérons la fonction 2π-périodique f telle que $f(0) = f(\pi) = 0$, $f(x) = 1$ pour $0 < x < \pi$ et $f(x) = -1$ pour $-\pi < x < 0$.

Elle est impaire et de classe $\mathscr{C}^1$ par morceaux. Sa série de Fourier en sinus est donnée par

$$\sum_{n=1}^{\infty} b_n(f)\sin(nx),$$

où

$$\begin{aligned} b_n(f) &= \frac{2}{2\pi}\int_{-\pi}^{\pi} f(x)\sin(nx)\,dx \\ &= \frac{2}{\pi}\int_0^{\pi} \sin(nx)\,dx \\ &= \frac{2}{\pi}\left[-\frac{1}{n}\cos(nx)\right]_0^{\pi} \\ &= \begin{cases} 4/\pi n & \text{si } n \text{ est impair;} \\ 0 & \text{sinon.} \end{cases} \end{aligned}$$

Autrement dit, $\mathrm{S}_n(x)$ est la $(2n+1)$-ième somme partielle de la série de Fourier de $\frac{\pi}{4}f$. Soit $x \in]0;\pi[$. Comme f est continue en x, le théorème de Dirichlet entraîne que $\mathrm{S}_n(x)$ converge vers $\frac{4}{\pi}f(x) = 4/\pi$.

b) On a $\mathrm{S}_n'(x) = \sum_{k=1}^{n}\cos((2k-1)x)$. Pour simplifier cette somme, on écrit $\cos((2k-1)x) = \mathrm{Re}(e^{i(2k-1)x})$ de sorte que $\mathrm{S}_n'(x)$ est la partie réelle de

$$\sum_{k=1}^{n} e^{i(2k-1)x} = e^{ix}\frac{e^{2inx}-1}{e^{2ix}-1},$$

comme on le voit en sommant n termes d'une suite géométrique de raison e^{2ix} et de premier terme e^{ix}. Cette expression se simplifie en

$$e^{ix}\frac{e^{inx}(2i\sin(nx))}{e^{ix}(2i\sin(x))} = e^{inx}\frac{\sin(nx)}{\sin(x)}.$$

Par suite,

$$\mathrm{S}_n'(x) = \frac{\cos(nx)\sin(nx)}{\sin(x)} = \frac{\sin(2nx)}{2\sin(x)}.$$

La formule ne vaut que si $e^{2ix} \neq 1$, c'est-à-dire si x n'est pas un multiple entier de π ; dans ce cas, on voit directement que $\mathrm{S}_n'(x) = n$ si $x \equiv 0 \pmod{2\pi}$ et $\mathrm{S}_n'(x) = -n$ si $x \equiv \pi \pmod{2\pi}$.

Comme S_n est 2π-périodique et impaire, on étudie les variations sur $[0;\pi]$. Pour x dans $]0;\pi[$, le dénominateur $2\sin(x)$ est strictement positif. En revanche, $\sin(2nx)$ s'annule en changeant de signe aux points x_k tels que $x_k = k\pi/2n$,

pour $k \in \{0, \dots, 2n\}$. Elle est croissante sur $[0; x_1]$, décroissante sur $[x_1; x_2]$, croissante sur $[x_2; x_3]$, etc.

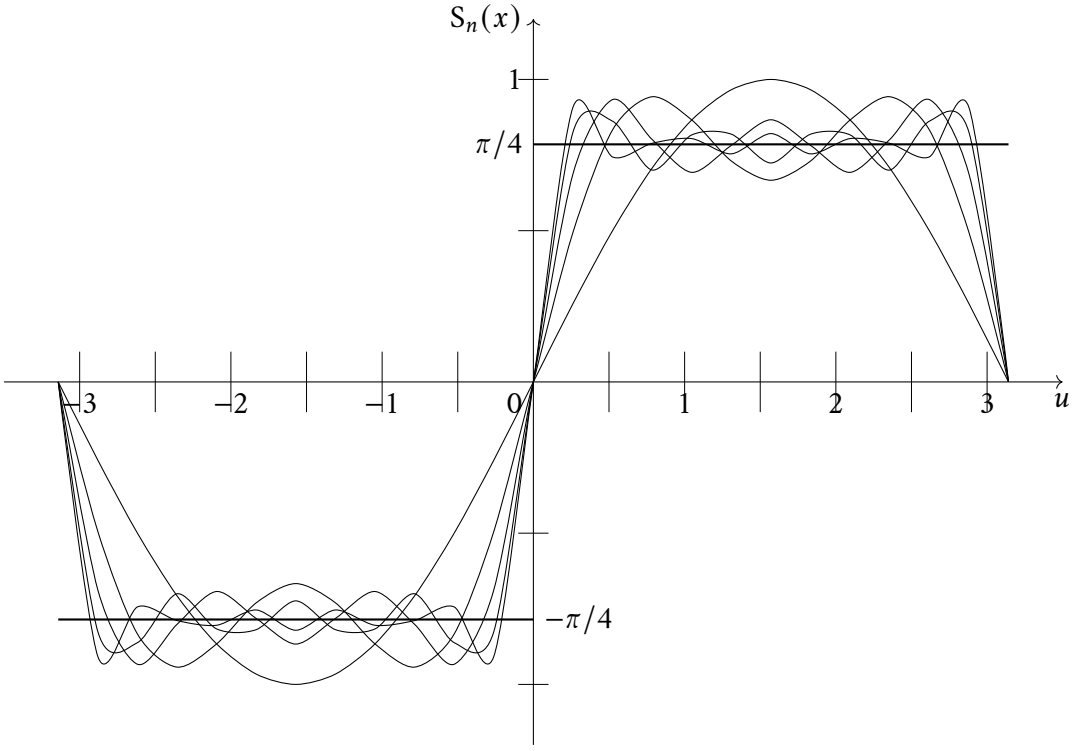


FIGURE 3.9.8.1. Graphe de $S_n(x)$ pour $1 \leqslant n \leqslant 5$

c) Les variations de S_n indiquent que S_n a un maximum local en chaque x_{2k-1}, pour $k \in \{1; \dots; n\}$, de valeur $m_{2k-1} = S_n(x_{2k-1}) = S_n((2k-1)\pi/2n)$. Pour démontrer les inégalités $m_1 \geqslant m_3 \geqslant \dots$, on écrit, pour $k \in \{1; \dots; n-1\}$,

$$m_{2k-1} - m_{2k+1} = S_n(x_{2k-1}) - S_n(x_{2k+1}) = -\int_{x_{2k-1}}^{x_{2k+1}} S_n'(x)\, dx = -\int_{x_{2k-1}}^{x_{2k+1}} \frac{\sin(2nx)}{2\sin(x)}.$$

Faisons le changement de variable $x = t + x_{2k} = t + k\pi/n$; comme $2nx_{2k} = 2k\pi$, il vient $\sin(2nx) = \sin(2nt)$ et

$$\begin{aligned} m_{2k-1} - m_{2k+1} &= -\int_{-\pi/2n}^{\pi/2n} \frac{\sin(2nt)}{2\sin(x)}\, dt \\ &= \int_0^{\pi/2n} \sin(2nt) \left(+\frac{1}{2\sin(x')} - \frac{1}{2\sin(x)} \right) dt, \end{aligned}$$

où $x' = -t + x_{2k}$. Dans l'intervalle considéré, on a $2nt \in [0;\pi]$, de sorte que $\sin(2nt) \geqslant 0$. On a aussi

$$0 \leqslant x_{2k-1} \leqslant x' \leqslant x_{2k} \leqslant x \leqslant x_{2k+1} \leqslant \frac{1}{2}\pi,$$

si bien que $0 \leqslant \sin(x') \leqslant \sin(x)$. On en déduit l'inégalité $m_{2k-1} \geqslant m_{2k+1}$.

d) On note les symétries $f(\pi - x) = f(x)$ et $\mathrm{S}_n(\pi - x) = \mathrm{S}_n(x)$ (car S_n n'a que des coefficients d'ordre impair). D'après la question précédente, le maximum de S_n sur $[0;\pi/2]$ est atteint en x_1 ; sur $[\pi/2;\pi]$, il est alors atteint en x_{2n-1}. Par suite,

$$\sup(\mathrm{S}_n) = m_1 = \mathrm{S}_n(x_1) = \int_0^{x_1} \mathrm{S}_n'(x)\,dx = \int_0^{\pi/2n} \frac{\sin(2nx)}{2\sin(x)}\,dx.$$

Faisons le changement de variables $t = 2nx$; alors

$$\sup(\mathrm{S}_n) = \int_0^{\pi} \frac{\sin(t)}{4n\sin(t/2n)}\,dt.$$

Quand n tend vers l'infini, l'intégrande converge vers $\sin(t)/2t$. La convergence est même uniforme, si bien que

$$\lim_{n\to+\infty} \sup(\mathrm{S}_n) = \frac{1}{2}\int_0^{\pi} \frac{\sin(t)}{t}\,dt \approx 0{,}926.$$

Le *paradoxe*, qu'on devine sur la figure 3.9.8.1 est que cette limite est strictement plus grande que $\sup(f) = \pi/4 \approx 0{,}785$ — le rapport entre ces deux quantités est $\approx 1{,}179$. La fonction f n'étant pas continue ; elle ne peut pas être limite *uniforme* de sa série de Fourier ; il y a même cette espèce de débordement d'environ 9% de l'amplitude de la discontinuité (ici, $f(0^+) - f(0^-) = \pi/22$).

C'est un phénomène général. En effet, considérons une fonction u, disons de classe $\mathscr{C}^1$ par morceaux, 2π-périodique, et supposons qu'elle est discontinue en un point a. On peut alors l'écrire comme la somme d'une fonction continue et d'une combinaison linéaire de fonctions analogue à la fonction f de cet exercice « placées » en chaque discontinuité, dont le rôle est de « supprimer » ladite discontinuité. En fait, la fonction f elle-même ne suffit pas car elle a un saut non seulement en 0, mais aussi en π et on considère plutôt la fonction 2π-périodique g qui vérifie $g(0) = 0$ et $g(t) = \pi - t$ pour $t \in]0;2\pi[$, mais son analyse est un peu plus délicate. Quoi qu'il en soit, la série de Fourier de notre fonction initiale u donne lieu à des débordements locaux en chaque discontinuité, d'environ 9% de l'amplitude de la discontinuité.

Ce phénomène a été découvert par Wilbraham en 1848, il porte aujourd'hui le nom de *phénomène de Gibbs*, du nom du mathématicien qui l'a redécouvert en 1899. Je recommande l'article de Hewitt & Hewitt (1979) pour une présentation détaillée du phénomène et de l'histoire de sa découverte.

Du point de vue de la théorie du signal, il explique des phénomènes de « suroscillation », ou « surélévation » du signal rendu lorsque la source possède des discontinuités.

Solution de l'exercice (3.8.9). — *a*) Par dérivation sous le signe somme, on a

$$\begin{aligned} g'(y) &= \int_{\mathbf{R}} -2i\pi x f(x) e^{-2i\pi xy}\, dx \\ &= i \int_{\mathbf{R}} (-2xf(x)) e^{-2i\pi xy}\, dx \\ &= i \int_{\mathbf{R}} f'(x) e^{-2i\pi xy}\, dx \\ &= i \left[f(x) e^{-2i\pi xy} \right]_{-\infty}^{\infty} - i \int_{\mathbf{R}} f(x)(-2i\pi y) e^{-2i\pi xy}\, dx \\ &= -2\pi y \int_{\mathbf{R}} f(x) e^{-2i\pi xy}\, dx \\ &= -2\pi y g(y). \end{aligned}$$

On peut également partir de la relation $f'(x) = -2\pi x f(x)$ et calculer la transformée de Fourier des deux membres. Concernant le membre de gauche, on sait

$$\widehat{f'}(y) = 2i\pi y \widehat{f}(y) = 2i\pi y g(y),$$

tandis que pour la transformée de Fourier du membre de doite est égale à

$$-i\mathscr{F}(-2i\pi x f(x))(y) = -i\mathscr{F}(f)'(y) = -ig'(y).$$

On retrouve ainsi $g'(y) = -2\pi y g(y)$.

Cette équation différentielle se résoud en

$$g(y) = ce^{-\pi y^2},$$

où c est un nombre réel.

b) Appliquons la transformation de Fourier aux deux membres de l'égalité $g = cf$: le membre de gauche fournit $\widehat{g}(y) = \widehat{\widehat{f}}(x) = f(-x)$, tandis que le membre de droite donne $\widehat{cf}(x) = cg(x) = crf(x)$, d'où l'égalité $c^2 = 1$.

On a aussi $\int_{\mathbf{R}} f(x)\,dx = g(0) = cf(0) = c$. En particulier, $c > 0$; ainsi, $c = 1$ et $\int_{\mathbf{R}} e^{-\pi x^2}\,dx = 1$.

Solution de l'exercice (3.8.10). — *a*) Pour $y \in \mathbf{R}$, on a

$$\begin{aligned}\widehat{f}(y) &= \int_{-\infty}^{\infty} e^{-|x|}e^{-2i\pi xy}\,dx \\ &= \int_0^{\infty} e^{-x(1+2i\pi y)}\,dx + \int_0^{\infty} e^{-x(1-2i\pi y)}\,dx \\ &= \frac{1}{1+2i\pi y} + \frac{1}{1-2i\pi y} \\ &= \frac{2}{1+4\pi^2y^2}.\end{aligned}$$

b) La formule d'inversion de Fourier s'écrit

$$f(x) = e^{-|x|} = \int_{\mathbf{R}} \frac{2}{1+4\pi^2y^2}e^{2i\pi xy}\,dy.$$

En particulier, pour $x = 0$,

$$1 = \int_{-\infty}^{\infty} \frac{2}{1+4\pi^2y^2}\,dy.$$

Comme la dérivée de $\arctan(2\pi y)$ est $2\pi/(1+4\pi^2y^2)$, le membre de droite vaut bien

$$\frac{2}{2\pi}\left[\arctan(2\pi y)\right]_{-\infty}^{\infty} = \frac{2}{2\pi}\left(\frac{\pi}{2} - \frac{-\pi}{2}\right) = 1.$$

Solution de l'exercice (3.8.11). — *a*) On a

$$\begin{aligned}\widehat{f}(y) &= \int_{-\infty}^{\infty} f(x)e^{-2i\pi xy}\,dx = \int_{-1}^{1} (1-|x|)e^{-2i\pi xy}\,dx \\ &= \int_0^1 (1-x)2\cos(2\pi xy)\,dx.\end{aligned}$$

Si $y = 0$, on obtient

$$\widehat{f}(0) = \int_0^1 2(1-x)\,dx = 1.$$

Supposons $y \neq 0$; on intègre alors par parties, d'où

$$\begin{aligned}\widehat{f}(y) &= \left[(1-x)\frac{2}{2\pi y}\sin(2\pi x y)\right]_0^1 + \frac{1}{\pi y}\int_0^1 \sin(2\pi x y)\,dx x \\ &= \frac{1}{\pi y}\left[-\frac{1}{2\pi y}\cos(2\pi y)\right]_0^1 = \frac{1-\cos(2\pi y)}{2\pi^2 y^2} = \frac{\sin^2(\pi y)}{\pi^2 y^2} \\ &= (\operatorname{sinc}(\pi y))^2.\end{aligned}$$

b) La fonction $\widehat{f}$ est continue sur $\mathbf{R}$, elle décroît en $1/y^2$ à l'infini, donc est intégrable. On peut donc appliquer le théorème d'inversion de Fourier :

$$f(0) = 1 = \int_{-\infty}^{\infty} \widehat{f}(y)\,dy,$$

d'où l'égalité demandée.

Solution de l'exercice (*3.8.12*). — *a*) Par définition, on a

$$\widehat{f}(y) = \int_{-\infty}^{\infty} f(x)e^{-2i\pi x y}\,dx = \int_{-1}^{1} e^{-2i\pi x y}\,dx.$$

Si $y = 0$, on obtient $\widehat{f}(0) = 2$. Si $y \neq 0$, on obtient

$$\begin{aligned}\widehat{f}(y) &= \frac{1}{-2i\pi y}\left[e^{-2i\pi x y}\right]_{-1}^{1} \\ &= \frac{1}{-2i\pi y}\left(e^{-2i\pi y} - e^{2i\pi y}\right) \\ &= \frac{1}{-2i\pi y}(-2i\sin(2\pi y) = 2\frac{\sin(2\pi y)}{2\pi y}.\end{aligned}$$

b) Apliquons la formule de Plancherel. On a d'une part

$$\int_{-\infty}^{\infty} |f(x)|^2\,dx = \int_{-1}^{1} dx = 2,$$

et d'autre part,

$$\int_{-\infty}^{\infty} |\widehat{f}(y)|^2\,dy = 4\int_{-\infty}^{\infty}\left(\frac{\sin(2\pi y)}{2\pi y}\right)^2 dy = \frac{2}{\pi}\int_{-\infty}^{\infty}\left(\frac{\sin(t)}{t}\right)^2 dt.$$

Par suite,

$$\int_0^{\infty}\left(\frac{\sin(t)}{t}\right)^2 dt = \frac{1}{2}\int_{-\infty}^{\infty}\left(\frac{\sin(t)}{t}\right)^2 dt = \frac{\pi}{2}.$$

c) La fonction $t \mapsto \sin(t)/t$ est continue sur $\mathbf{R}$; on peut l'intégrer par parties entre 0 et T, en prenant $1 - \cos(t)$ pour primitive de $\sin(t)$.

$$\begin{aligned}\int_0^{\mathrm{T}} \frac{\sin(t)}{t}\,dt &= \left[\frac{1-\cos(t)}{t}\right]_0^{\mathrm{T}} + \int_0^{\mathrm{T}} \frac{1-\cos(t)}{t^2}\,dt \\ &= \frac{1-\cos(\mathrm{T})}{\mathrm{T}} + \int_0^{\mathrm{T}} \frac{2\sin^2(t/2))}{t^2}\,dt \\ &= \frac{1-\cos(\mathrm{T})}{\mathrm{T}} + \int_0^{\mathrm{T}} \frac{\sin^2(t/2))}{t^2/4}\,d(t/2) \\ &= \frac{1-\cos(\mathrm{T})}{\mathrm{T}} + \int_0^{\mathrm{T}/2} \frac{\sin^2(u))}{u^2}\,du.\end{aligned}$$

Lorsque $\mathrm{T} \to +\infty$, le premier terme tend vers 0 et le deuxième vers $\int_0^\infty (\sin(u)/u)^2\,du$. Cela prouve la convergence de l'intégrale proposée et démontre également que l'on a

$$\int_0^{+\infty} \frac{\sin(t)}{t}\,dt = \int_0^{+\infty} \left(\frac{\sin(t)}{t}\right)^2\,dt = \frac{\pi}{2}.$$

BIBLIOGRAPHIE

N. Alon & J. H. Spencer (2008), *The Probabilistic Method*, Wiley-Interscience Series in Discrete Mathematics and Optimization, Wiley, Hoboken, N.J, 3rd ed édition.

P. R. Chernoff (1980), « Pointwise Convergence of Fourier Series ». *The American Mathematical Monthly*, **87** (5), p. 399.

T. M. Cover & J. A. Thomas (2006), *Elements of information theory*, Wiley-Interscience [John Wiley & Sons], Hoboken, NJ, second édition.

H. Dym & H. P. McKean (2016), *Séries et intégrales de Fourier*, Nouvelle bibliothèque mathématique **13**, Cassini, Paris. Translated from the 1972 English original by Éric Kouris.

W. Heisenberg (1927), « Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik ». *Zeitschrift für Physik*, **43** (3), p. 172–198.

E. Hewitt & R. E. Hewitt (1979), « The Gibbs-Wilbraham phenomenon : An episode in fourier analysis ». *Archive for History of Exact Sciences*, **21** (2), p. 129–160.

E. H. Kennard (1927), « Zur Quantenmechanik einfacher Bewegungstypen ». *Zeitschrift für Physik*, **44** (4), p. 326–352.

A. N. Kolmogorov (1956), *Foundation of the Theory of Probability*, Chelsea, New York.

H. J. Landau & H. O. Pollak (1961), « Prolate spheroidal wave functions, fourier analysis and uncertainty — II ». *The Bell System Technical Journal*, **40** (1), p. 65–84.

R. Redheffer (1984), « Convergence of Fourier Series at a Discontinuity ». *SIAM Journal on Mathematical Analysis*, **15** (5), p. 1007–1009.

C. E. Shannon (1948), « A mathematical theory of communication ». *Bell System Tech. J.*, **27**, p. 379–423, 623–656.

C. E. Shannon (1949), « Communication in the presence of noise ». *Proc. I.R.E.*, **37**, p. 10–21.

C. E. Shannon & W. Weaver (2018), *La théorie mathématique de la communication*, Cassini.

D. Slepian & H. O. Pollak (1961), « Prolate spheroidal wave functions, fourier analysis and uncertainty — I ». *The Bell System Technical Journal*, **40** (1), p. 43–63.

H. Weyl (1950), *The Theory of Groups and Quantum Mechanics*, Dover Books on Mathematics, Dover Publ, Mineola, NY, nachdr. édition.

Wikipedia (2005), « Champ auditif — Wikipedia, l'encyclopédie libre ». URL *https://fr.wikipedia.org/w/index.php?title=Champ_auditif*, consulté le 25 juin 2021.

J. Wolfowitz (1958), « The maximum achievable length of an error correcting code ». *Illinois Journal of Mathematics*, **2** (3), p. 454–458.

INDEX