

MATHÉMATIQUES

Combien de fois faut-il battre un jeu de cartes ?

P. Biane

Ce texte est tiré d'un article de D. Bayer et P. Diaconis "Trailing the dovetail shuffle to its lair" *Ann. Appl. Prob.*, **2** (1992), no. 2., p. 294–313.

Je remercie T. Chomette pour sa lecture attentive du texte.

1. Introduction

La méthode la plus utilisée pour battre un paquet de cartes consiste à couper le paquet en deux, puis à mélanger les deux parties en alternant les cartes. J'appellerai ces deux opérations *la coupe* et *le mélange*.

Lorsqu'on suit la méthode rigoureusement, on coupe le paquet en deux parties égales et on alterne exactement les cartes de chaque partie. Si on fait ça avec un paquet de 32 cartes, en prenant soin de laisser toujours la première carte sur le dessus du paquet, on s'aperçoit qu'au bout de 5 battages de cartes, on est revenu dans la position initiale. La règle générale est que la carte en position k arrive en position $2k - 1$ si $k \leq 16$ et en position $2k - 32$ si $k \geq 17$. Par exemple voici les positions successives de la sixième carte : 6, 11, 21, 10, 19, 6. On est bien revenu en position initiale en 5 coups.

Plus généralement, avec un jeu de 2^n cartes, cette méthode permet de revenir dans la position initiale en n battages.

Exercice : démontrer ce résultat ! (Je donne une solution à la fin du texte).

Ce fait est à la base d'un tour de cartes spectaculaire, où le magicien retrouve une carte dans un paquet que tout le monde croit bien mélangé. Évidemment, pour arriver à couper un paquet *exactement* au milieu puis à le « mélanger » parfaitement et cela 5 fois de suite, il faut une dextérité hors du commun, et bien peu de personnes au monde sont capable d'exécuter ce tour.

En général, quand on bat un paquet, après la coupe les deux parties ne sont qu'approximativement égales et lors du mélange les deux paquets n'alternent pas exactement. Heureusement d'ailleurs, car le but de l'opération est que l'on ne puisse pas deviner la position des cartes une fois le paquet battu, même si on la connaissait avant. Cela nous amène à la question principale de l'exposé : combien de fois doit on battre le paquet pour qu'il soit bien mélangé ? L'intérêt de la question est évident, au moins pour les joueurs de cartes ou les patrons de casinos. En effet, si l'on ne bat pas assez les cartes, il reste dans le jeu un peu d'information provenant de la distribution précédente, que certains joueurs pourraient exploiter pour deviner les cartes, comme par exemple dans le tour de magie qui est expliqué plus bas. Évidemment, plus on bat les cartes et plus on lutte contre cet effet, mais d'un autre côté, si l'on bat les cartes pendant trop longtemps, cela ralentit le jeu (et donc diminue les gains du casino !), il est par conséquent utile de savoir à partir de combien de battages le jeu est suffisamment mélangé.

Pour répondre à cette question il faut disposer d'un modèle mathématique qui décrive la façon dont on bat les cartes, puis arriver à en faire une analyse assez précise.

Le modèle dont il sera question ici a été proposé par les mathématiciens Gilbert et Shannon en 1955, et indépendamment par Reeds en 1981, et il a été testé par P. Diaconis qui a vérifié qu'il décrivait de façon réaliste le battage des cartes pratiqué par exemple dans les casinos.

2. Modèle probabiliste

2.1 La coupe

On dispose d'un paquet de n cartes, que l'on commence par couper en deux paquets de j et $n - j$ cartes, le nombre j étant choisi entre 0 et n , avec la loi *binomiale* c'est-à-dire que l'on a une probabilité $\frac{1}{2^n} \frac{n!}{k!(n-k)!}$ que j soit égal à k .

La formule du binôme nous dit que $\sum_{k=0}^n \frac{1}{2^n} \frac{n!}{k!(n-k)!} = 1$ donc la somme des probabilités fait bien 1. Si on trace le graphe de cette probabilité en fonction de k , on observe une courbe "en cloche", dont le maximum se situe en $n/2$, et dont la plus grande partie se trouve concentrée entre $n/2 - \sqrt{n}$ et $n/2 + \sqrt{n}$.

Cela modélise de façon raisonnable ce que peut faire un batteur de carte d'une adresse moyenne en essayant de couper le paquet en deux parties égales. Une autre raison de choisir cette distribution est la suivante : si on choisit une partie de $\{1, \dots, n\}$ au hasard, toutes les parties étant équiprobables, alors la probabilité de tirer une partie à k éléments est $\frac{1}{2^n} \frac{n!}{k!(n-k)!}$. Je donnerai plus bas encore une autre justification pour le choix de cette distribution.

2.2 Le mélange

Ensuite, une fois que le paquet a été coupé, on mélange les deux parties de la façon suivante : supposons qu'il reste a_1 cartes dans le premier paquet et a_2 dans le second, alors on choisit la carte du dessous du premier paquet avec probabilité $\frac{a_1}{a_1 + a_2}$, ou bien celle du second avec probabilité $\frac{a_2}{a_1 + a_2}$, et on continue ainsi, avec $a_1 - 1$ cartes dans le premier et a_2 dans le second, ou bien a_1 dans le premier et $a_2 - 1$ dans le second suivant les cas, jusqu'à épuisement des deux paquets. Là encore ce choix semble raisonnable, car plus l'un des paquets est gros par rapport à l'autre, plus on a de chance de choisir la carte de ce paquet.

2.3 Battages et permutations

On peut interpréter un battage de cartes comme une *permutation* du jeu de cartes. Dans la suite j'appellerai les cartes par des numéros $1, 2, 3, \dots, n$, plutôt que par leurs valeurs faciales habituelles, avec trèfle, pique, etc..., car cela rend les arguments plus aisés à suivre, mais cela ne change rien à la nature des choses. Une permutation peut se représenter sous la forme (ici avec $n = 10$)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 6 & 7 & 1 & 2 & 8 & 3 & 9 & 4 & 10 \end{pmatrix}$$

La première ligne représente l'ordre des cartes avant le battage, et la seconde ligne l'ordre après battage. Pour un jeu de n cartes, il y a $n!$ permutations possibles. Pour un jeu de 52 cartes, on a ainsi $52!$ possibilités, soit :

80658175170943878571660636856403766975289505440883277824000000000000

un nombre gigantesque. Si on voulait écrire tous les ordres possibles d'un jeu de 52 cartes, non seulement cela prendrait des milliards d'années (au bas mot), mais il n'y aurait sans doute pas assez de matière dans l'univers pour le faire. Comme nous le verrons plus loin, un seul battage ne permet de réaliser que 2^n permutations, or ici :

$$2^{52} = 4503599627370496$$

un nombre très grand mais néanmoins beaucoup plus petit que $52!$. Même avec 4 battages, on obtiendra moins de 2^{208} permutations, soit

$$411376139330301510538742295639337626245683966408394965837152256$$

ce qui est toujours beaucoup plus petit que $52!$ (environ 2 millions de fois plus petit).

Il faudra donc nécessairement plus de battages pour espérer obtenir une proportion satisfaisante de toutes les permutations possibles, et une distribution suffisamment aléatoire des cartes. On verra plus bas comment quantifier l'aléa contenu dans le résultat de plusieurs battages de cartes.

3. Répartition des configurations après m battages

3.1 Le théorème

Pour le moment je vais donner une formule explicite pour la probabilité d'obtenir une configuration π du paquet de cartes au bout de m battages. On suppose que dans la configuration initiale les cartes sont dans l'ordre $123\dots n$, alors la configuration π n'est autre que l'ordre des cartes obtenu après m battages. Dans l'énoncé le symbole C_p^q désigne le coefficient du binôme $C_p^q = \frac{p!}{q!(p-q)!}$ si $q \leq p$, et vaut 0 sinon.

Théorème : La probabilité pour que le paquet se trouve dans l'état π après m battages est égale à

$$p_n(\pi) = \frac{1}{2^{mn}} C_{2^m+n-r}^n$$

où r est le nombre de suites montantes dans π .

3. 2 Un joli tour de cartes

3.2.1 Principe du tour

Pour comprendre l'énoncé du théorème il faut savoir ce qu'est une suite montante. Pour l'expliquer je vais décrire un tour de cartes inventé au début du siècle par les magiciens Williams et Jordan. Dans ce tour, le magicien tend un paquet de cartes à un spectateur, puis il tourne le dos au public et il demande au spectateur de battre deux fois le paquet, puis de le couper encore une fois, et de prendre la carte au dessus du paquet. Le spectateur note la valeur de la carte, puis il la remet où il veut dans le paquet et le rebat. Alors le magicien se retourne, étale les cartes devant lui, face dessus, et après les avoir intensément scrutées, désigne la carte que le spectateur avait sortie.

Comment fonctionne le tour ? Le magicien connaît l'ordre des cartes dans le paquet avant le battage, par exemple cet ordre est l'ordre naturel $1, 2, 3, \dots, n$. L'idée de base est que battre trois fois le jeu laisse suffisamment de structures invariantes dans la distribution des cartes, ce qui est vrai si le nombre de cartes est suffisant (en général on prend un jeu de 52 cartes), et que l'on peut retrouver la carte du spectateur en comptant les suites montantes.

3.2.2 Suites montantes

Une suite montante est une sous-suite maximale constituée de nombres successifs. Toute permutation de $\{1, \dots, n\}$ peut être décomposée de façon unique en une juxtaposition de suites montantes, par exemple si on considère la permutation de 16 chiffres

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 14 & 3 & 4 & 15 & 6 & 9 & 10 & 5 & 11 & 1 & 7 & 12 & 2 & 8 & 16 & 13 \end{pmatrix}$$

alors les sous-suites montantes sont : $(1, 2)$, $(3, 4, 5)$, $(6, 7; 8)$, $(9, 10, 11, 12, 13)$ et $(14, 15, 16)$. Pour trouver les suites montantes d'une permutation, on procède comme ceci : on commence par repérer la carte 1. Si la carte 2 est avant 1, alors (1) est une suite montante, sinon on cherche 3. Si 3 est avant 2, alors $(1, 2)$, est une suite montante, sinon on cherche 4, et ainsi de suite jusqu'à épuisement du paquet. Lorsqu'on bat une première fois les cartes qui sont dans la position initiale $123\dots n$, on obtient deux suites montantes $1, 2, \dots, k$ et $k+1, k+2, \dots, n$, où k désigne le numéro de la carte où on a effectué la coupe (sauf dans le cas extrême où on a remis le paquet dans sa position initiale, auquel cas il y a une seule suite montante).

En général, au début, chaque battage multiplie par deux le nombre de suites montantes dans le paquet, donc au bout de 3 battages il y a 8 suites montantes, qui contiennent en moyenne $52/8 = 6,5$ cartes.

3.2.3 Explication du tour

La manipulation du spectateur, qui extrait une carte pour la replacer ailleurs, crée dans la plupart des cas une neuvième suite montante, qui consiste en cette unique carte. Le magicien n'a plus alors qu'à identifier les suites montantes dans le paquet pour trouver la carte recherchée (en fait l'analyse est un peu plus compliquée car on autorise le spectateur à faire une coupe supplémentaire mais j'ignore ici cette complication).

Le tour ne marche pas à tous les coups, c'est facile à voir, car une suite montante contenant une seule carte peut être créée par hasard lors des battages, ce qui peut tromper le magicien, ou bien le spectateur peut remettre la carte qu'il a choisie, à l'endroit où il l'a prise, ce qui détruit le principe du tour. Paradoxalement, en général le spectateur aura tendance, pour essayer d'embrouiller le magicien, à remettre la carte loin de l'endroit où il l'a prise, avec l'effet exactement inverse de celui recherché ! De même, plus il y a de cartes dans le jeu, plus il est rare qu'une suite montante à une seule carte soit créée, et donc plus le tour a de chances de marcher. Une simulation sur ordinateur a montré que, sur un million d'essais, avec un jeu de 52 cartes, le truc permet de deviner la bonne carte dans 84% des cas. Si on s'autorise un second essai en cas d'échec, alors le pourcentage de succès passe à 94%.

3.3 Démonstration du théorème

Voyons maintenant comment on démontre le théorème. Tout d'abord, examinons de plus près ce qui se passe après un seul battage.

Supposons que la coupe ait produit deux tas de j et $n - j$ cartes, numérotées 1 et 2.

Ceci se produit avec la probabilité $\frac{1}{2^n} \frac{n!}{j!(n-j)!}$.

Pour effectuer le mélange on choisit chaque carte successivement dans l'un des deux paquets. Les choix successifs sont notés i_1, i_2, \dots, i_n , où à chaque fois $i_k \in \{1, 2\}$ désigne l'un des deux paquets. La probabilité d'un tel choix est

$$\frac{x_1}{n} \frac{x_2}{n-1} \dots \frac{x_{n-1}}{2} \frac{x_n}{1}$$

où x_k désigne le nombre de cartes qui restent dans le i_k^{eme} paquet à la k^{eme} étape. On voit facilement que les nombres $j, j-1, j-2, \dots, 1$ et $n-j, n-j-1, \dots, 1$ apparaissent chacun une fois au numérateur, donc le produit ne dépend pas de la suite des i_k , et vaut $\frac{j!(n-j)!}{n!}$.

Finalement, tous les résultats possibles avec une coupe au niveau j sont donc équiprobables, de probabilité $\frac{1}{2^n}$.

Ce résultat donne une autre justification au choix de la loi binomiale pour j : il conduit à l'équiprobabilité de tous les choix possibles, indépendamment de la taille des paquets après la coupe.

Il est possible que l'on obtienne la même permutation avec des nombres j_1 et j_2 différents. En fait cela ne peut se produire que si la permutation obtenue est la permutation identique :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \end{pmatrix}$$

et cela peut se produire exactement une fois pour chaque valeur de j . En effet, dans tous les autres cas, les deux suites montantes obtenues à l'issue de ce mélange sont, on l'a vu, de la forme $1, 2, \dots, j$ et $j+1, \dots, n$. C'est-à-dire qu'elles caractérisent l'entier j .

Si nous résumons ce que nous avons obtenu, nous voyons que chaque permutation avec 2 suites montantes peut être réalisée avec probabilité $\frac{1}{2^n}$, alors que la permutation identique, qui a une seule suite montante peut être réalisée une fois pour chaque valeur de j , ce qui fait qu'elle apparaît avec la probabilité $\frac{(n+1)}{2^n}$.

On vérifie bien ainsi le théorème dans le cas $m = 1$: dans ce cas, les seules valeurs possibles de r sont $r = 1$ et $r = 2$.

L'analyse du cas général est un peu plus compliquée. On remarque que l'on peut faire d'abord toutes les coupes avant de faire les mélanges, sans changer la probabilité finale de tirer une permutation donnée. Pour cela, après la première coupe, au lieu de mélanger les deux paquets, recoupons les chacun en deux parties, puis encore les quatre paquets obtenus en deux parties, etc... et cela m fois en tout, de sorte que l'on a obtenu 2^m parties. Rappelons que ces parties peuvent être éventuellement vides ! Alors on mélange ces parties de sorte que chacune des façons de faire le mélange a la même probabilité $\frac{1}{2^{nm}}$ (la démonstration du cas $m = 1$ se transpose telle quelle). On remarque aussi que le nombre de suites montantes après m battages est d'au plus 2^m .

On voit alors que ce procédé donne le même résultat que celui correspondant à faire m battages successifs. Maintenant, pour une permutation donnée, il faut calculer de combien de façons elle peut être réalisée avec ce procédé et multiplier par $\frac{1}{2^{nm}}$ pour obtenir sa probabilité d'apparaître. Quand on a effectué les m coupes on se retrouve avec 2^m paquets, chacun étant constitué de cartes qui se suivent. Cela revient en fait à avoir choisi les $2^m - 1$ positions où se trouvent les coupures entre les 2^m paquets. Supposons que les r suites montantes de la permutation que l'on veut obtenir soient données, par exemple $(1, 2, \dots, k_1); (k_1 + 1, \dots, k_2); \dots; (k_{r-1} + 1, \dots, n)$, alors nécessairement, on doit avoir coupé les paquets entre k_j et k_{j+1} . Cela fait $r - 1$ coupes qui sont déterminées. Il reste alors $2^m - r$ coupes à effectuer, et on peut les faire où l'on veut dans $n + 1$ positions. Une fois cela fait, on pourra retrouver la permutation voulue au moment du mélange, d'une seule façon. Cela fait en tout $C_{2^m+n-r}^m$ possibilités, d'après le

Lemme : Il y a C_{p+q-1}^{p-1} façons de placer q objets dans p cases (les objets sont indistinguables, et on peut en mettre plusieurs dans chaque case).

La démonstration du lemme est simple : si j'appelle a_1, a_2, \dots, a_p le nombre d'objets dans les cases $1, 2, \dots, p$, alors $\{a_1 + 1, a_1 + a_2 + 2, \dots, a_1 + \dots + a_{p-1} + p - 1\}$ forme un sous-ensemble à $p - 1$ éléments de $\{1, 2, 3, \dots, p + q - 1\}$. Nous avons q objets au total, donc $a_1 + \dots + a_p = q$, c'est-à-dire $a_p = q - (a_1 + \dots + a_{p-1})$, et la connaissance des entiers a_1, \dots, a_{p-1} caractérise le placement des objets. On obtient ainsi une bijection entre les façons de placer q objets dans p cases et les sous-ensembles à $p - 1$ éléments de $\{1, 2, 3, \dots, p + q - 1\}$, dont le nombre est C_{p+q-1}^{p-1} .

4. Vers une répartition homogène

Une fois le théorème démontré, comment résoudre notre problème initial ? On voit que, lorsque m tend vers l'infini, alors $\frac{C_{2^m+n-r}^n}{2^{nm}}$ tend vers $1/n!$, *i.e.* toutes les répartitions deviennent équiprobables, ce qui correspond bien à l'idée intuitive que plus l'on bat les cartes, plus le paquet devient aléatoire. Il faut maintenant quantifier cette intuition. Une manière de le faire consiste à introduire la quantité

$$Q_m = \frac{1}{2} \sum_{\pi} \left| p_m(\pi) - \frac{1}{n!} \right|$$

qui mesure la distance entre la probabilité uniforme et la probabilité réalisée par m battages de cartes. Cette quantité est toujours comprise entre 0 et 1. Si elle est proche de 1, cela signifie que les probabilités p_m se concentrent sur un petit nombre de configurations. Plus cette quantité est petite, plus la répartition est "aléatoire". En utilisant le théorème 1, on voit que

$$Q_m = \frac{1}{2} \sum_r A_{n,r} \left| \frac{C_{2^m+n-r}^n}{2^{nm}} - \frac{1}{n!} \right|$$

où $A_{n,r}$ désigne le nombre permutations avec r suites montantes. On ne connaît pas d'expression explicite simple de ces nombres, mais on connaît des algorithmes permettant de les calculer, et des formules approchées lorsque n est grand. À l'aide de cela, Bayer et Diaconis ont montré que, si $m = \frac{3}{2} \log_2 n + x$, alors

$$Q_m = \sqrt{\frac{2}{\pi}} \int_0^{\frac{2-x}{4\sqrt{3}}} e^{-t^2/2} dt + r_n \quad (*)$$

où r_n est un reste qui tend vers 0 quand n tend vers l'infini. On voit que Q_m est proche de 1 lorsque $x \ll 0$ et proche de 0 lorsque $x \gg 0$ (on peut donner des valeurs numériques précises, par exemple en regardant dans une table de la loi de Gauss). La conclusion est qu'il faut environ un peu plus que $\frac{3}{2} \log_2 n$ battages pour bien mélanger un jeu de n cartes. Lorsque $n = 52$, ce qui est le cas le plus fréquent dans les applications, on peut calculer précisément Q_m en fonction de m et on obtient les valeurs (avec 3 décimales)

$$\begin{aligned} Q_1 &= 1.000, Q_2 = 1.000, Q_3 = 1.000, Q_4 = 1.000, Q_5 = 0.924, \\ Q_6 &= 0.614, Q_7 = 0.334, Q_8 = 0.167, Q_9 = 0.085, Q_{10} = 0.043 \end{aligned}$$

On voit que la distance reste pratiquement à son maximum jusqu'à 5 battages, puis elle se met à décroître rapidement, et en pratique, avec 8 battages on obtient un brassage des cartes suffisant pour que la donnée de la distribution avant battage

soit inutilisable par les joueurs. Notez que les valeurs de Q_7, Q_8, Q_9, Q_{10} forment approximativement une suite géométrique de raison $1/2$, ce qui est en accord avec la formule approchée (*).

A. Annexe : solution de l'exercice

Je termine en donnant une solution à l'exercice. On numérote les cartes de 0 à $2^n - 1$, et on écrit leur numéro en notation binaire, chaque numéro est donc une suite de n chiffres égaux à 0 ou 1. On vérifie facilement que la transformation de "battage parfait" consiste à faire une *permutation circulaire* de ces n chiffres, par exemple si on prend la sixième carte d'un jeu de 64 cartes, on écrit 5 en binaire (on a commencé par 0!), soit 000101, et les positions successives seront, en notation binaire, 001010, 010100, 101000, 010001, 100010 et enfin 000101. Il est clair qu'avec une permutation circulaire, on revient sur ses pas en n étapes, et l'exercice est résolu.

Philippe Biane

Département de Mathématiques et Applications
École Normale Supérieure de Paris

Une version mesurable du théorème de Stone-Weierstrass

Y. Coudène

1. Introduction

Le but de cette note est de présenter un résultat d'approximation analogue au théorème de Stone-Weierstrass, dans le cadre des espaces L^p . Rappelons l'énoncé de ce théorème (cf p.ex [Du66] chap.12) :

Soit X un espace topologique et $f_i : X \rightarrow \mathbb{R}$ une famille de fonctions de $C(X)$ qui sépare les points :

$$\forall x, y \in X, x \neq y, \exists i \text{ tq } f_i(x) \neq f_i(y).$$

Alors l'algèbre engendrée par les fonctions f_i est dense dans $C(X)$ pour la topologie compacte-ouverte.

La topologie compacte-ouverte coïncide avec la topologie de la convergence uniforme lorsque X est compact.

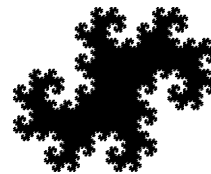
Le théorème de Stone-Weierstrass peut être utilisé pour démontrer que les polynômes trigonométriques sont denses dans $L^2([0, 1], dx)$, ou encore que les fonctions $x \mapsto e^{2\pi i n x}$ forment une base hilbertienne de $L^2([0, 1], dx)$. Cet espace admet également des bases constituées de fonctions qui ne sont pas continues ; la plus simple est la base de Haar, définie comme suit :

$$f_0 = \mathbf{1}, \quad f_{k,n} = 2^{n/2} \left(\mathbf{1}_{\left[\frac{2k}{2^{n+1}}, \frac{2k+1}{2^{n+1}}\right]} - \mathbf{1}_{\left[\frac{2k+1}{2^{n+1}}, \frac{2k+2}{2^{n+1}}\right]} \right), \quad k = 0..2^n - 1, \quad n \in \mathbf{N}.$$

Cette famille de fonctions possède plusieurs propriétés intéressantes : ses éléments ne prennent qu'un nombre fini de valeurs et satisfont une certaine invariance d'échelle :

$f_{k,n+1}(x) = \sqrt{2} f_{k,n}(2x)$. Elle est donc facile à implémenter sur machine.

En dimension supérieure, il est possible de construire des fonctions satisfaisant des conditions semblables. Les intervalles sont remplacés par des ensembles possédant des propriétés d'autosimilarités, comme dans l'exemple ci-contre. Ces constructions interviennent en traitement d'images [KV95].



Revenons à la base de Haar : cette famille orthonormée de $L^2([0, 1], dx)$ sépare les points ; on peut vérifier que le sous-espace vectoriel et l'algèbre qu'elle engendre coïncident. A partir de ces deux propriétés, peut-on en déduire que cette famille forme une base hilbertienne de L^2 ? Autrement dit, peut-on formuler une version du théorème de Stone-Weierstrass valide dans les espaces L^p ?

C'est le but de la première partie de cet article. On présente ensuite une correspondance entre σ -algèbres et partitions, due à V. A. Rokhlin ; cette correspondance permet d'obtenir des théorèmes d'approximation plus précis.

2. Approximation dans les espaces L^p

Afin de donner une preuve élémentaire, on se place sur l'espace $[0, 1]$, qui est muni d'une mesure de probabilité borélienne μ .

Rappelons que pour $p \geq 1$, les espaces L^p sont des espaces de Banach pour la norme $\|f\|_p = (\int |f|^p)^{1/p}$. Pour $p \in]0, 1[$, ce sont des espaces métriques complets pour la distance $d(f, g) = \int (|f - g|^p)$; ils ne sont plus localement convexes ([WRu73]1.47). En particulier, leur dual topologique est restreint à $\{0\}$, si μ est non-atomique. Pour $p = 0$, L^0 est l'espace des fonctions mesurables, muni de la convergence en probabilité ; c'est un espace métrique complet. Là encore, les seuls ouverts convexes sont $\{0\}$ et L^0 ([Fed69] 2.3.8).

Théorème 1. *Soit $p \in [0, \infty[$, μ une mesure de probabilité borélienne sur l'intervalle $[0, 1]$, et $f_n : [0, 1] \rightarrow \mathbf{R}$ une suite de fonctions μ -mesurables bornées qui sépare les points :*

$$\forall x, y \in X, x \neq y, \exists n \in \mathbf{N} \text{ tq } f_n(x) \neq f_n(y).$$

Alors l'algèbre engendrée par les fonctions f_n et les constantes, est dense dans $L^p([0, 1], \mu)$.

Remarques :

- Il faut que la famille de fonctions f_n soit dénombrable. La famille des fonctions indicatrices des singletons sépare les points mais n'engendre pas L^p .
- Les fonctions f_n sont supposées bornées afin que l'algèbre qu'elles engendrent soit bien incluse dans L^p . Lorsque $p = 0$, cette condition est superflue.
- Il est possible de démontrer ce théorème à l'aide du théorème de Krein-Milman, portant sur les points extrémaux des compacts convexes ; cf [WRu73]5.7 pour une preuve dans le cadre topologique.

Preuve :

La démonstration comporte trois étapes : On commence par se ramener au cas où les f_n sont des fonctions indicatrices d'ensembles mesurables B_n . La propriété de séparation permet d'obtenir une injection de $[0, 1]$ dans $\{0, 1\}^{\mathbf{N}}$, qui envoie les ensembles B_n sur les cylindres. Comme les cylindres engendrent la tribu des boréliens, il suffit de vérifier que cette injection est un plongement pour terminer la preuve.

Le lemme suivant est un résultat classique en théorie des probabilités.

Lemme 1. *Soit $n \in \mathbf{N}$, et $a, b \in \mathbf{R}$. Alors la fonction indicatrice de l'ensemble $f_n^{-1}(]a, b[)$ est dans l'adhérence de l'algèbre engendrée par f_n et les constantes.*

Preuve :

Posons $f = f_n$; soit C une constante positive telle que $|f| \leq C$. Sur l'intervalle $[-C, C]$, on peut trouver une suite uniformément bornée de polynômes P_k , qui converge simplement vers $\mathbf{1}_{]a, b[}$. Pour cela, il suffit d'approcher de manière croissante la fonction $\mathbf{1}_{]a, b[}$ par des fonctions continues, par exemple $g_j(x) = \min(1, jd(x,]a, b[))$ puis d'approcher ces fonctions g_j par des polynômes uniformément bornés par 2; la suite P_k est obtenue par extraction diagonale.

On a alors $P_k \circ f \rightarrow \mathbf{1}_{]a, b[} \circ f$ simplement, et $|P_k \circ f(x)| \leq 2, \forall x \in [0, 1]$. Le théorème de convergence dominée montre donc que les éléments $P_k \circ f$ de l'algèbre engendrée par f tendent vers $\mathbf{1}_{f^{-1}(]a, b[)}$ lorsque k tend vers l'infini. La domination uniforme est inutile lorsque $p = 0$, car la convergence presque partout implique la convergence en probabilité. †

Revenons à la preuve du théorème. Les ensembles $f_n^{-1}(]a, b[)$, avec a, b rationnels, sont en nombre dénombrable; mettons les sous la forme d'une suite $\{B_k\}$. L'algèbre engendrée par les $\mathbf{1}_{B_k}$ est contenue dans l'adhérence de l'algèbre engendrée par les f_n , il suffit donc de démontrer qu'elle est dense dans L^p , ou encore que les B_k , et les ensembles négligeables, engendrent la tribu des ensembles μ -mesurables.

La famille $\{\mathbf{1}_{B_k}\}$ sépare les points; par conséquent, on obtient une injection :

$$\begin{aligned} \Phi : [0, 1] &\rightarrow \{0, 1\}^{\mathbf{N}} \\ x &\rightarrow \{\mathbf{1}_{B_k}(x)\}_{k \in \mathbf{N}} \end{aligned}$$

Notons \tilde{B}_k l'ensemble des points de $\{0, 1\}^{\mathbf{N}}$ dont la $k^{ième}$ coordonnée est égale à 1. Les \tilde{B}_k engendrent la tribu des boréliens de $\{0, 1\}^{\mathbf{N}}$. L'égalité $\varphi^{-1}(\tilde{B}_k) = B_k$ montre que les B_k engendrent l'image réciproque de la tribu des boréliens de $\{0, 1\}^{\mathbf{N}}$. Il suffit donc de montrer que l'image réciproque de la tribu des ensembles $\varphi_*\mu$ -mesurables contient la tribu des ensembles μ -mesurables.

L'application φ étant injective, on a, pour tout $A \subset X$, $A = \varphi^{-1}(\varphi(A))$. Il suffit donc de montrer que l'image d'un ensemble μ -mesurable est $\varphi_*\mu$ -mesurable. Quitte à réaliser $\{0, 1\}^{\mathbf{N}}$ comme un compact de \mathbf{R} , on peut considérer que φ est à valeurs réelles. Le lemme suivant termine la démonstration du théorème :

Lemme 2. *Soit μ une mesure de probabilité borélienne sur l'intervalle $[0, 1]$, et soit $\varphi : [0, 1] \rightarrow \mathbf{R}$ une application injective μ -mesurable (l'image réciproque d'un borélien est mesurable). Alors l'image d'un ensemble μ -mesurable est $\varphi_*\mu$ -mesurable.*

Preuve :

Soit $A \subset [0, 1]$ un ensemble μ -mesurable. Pour tout $j \in \mathbf{N}^*$, on peut trouver un compact $K_j \subset A$, de mesure supérieure à $\mu(A) - 1/j$, sur lequel l'application φ est continue. C'est une conséquence de la densité des fonctions continues, au sens de la convergence presque partout, et du théorème d'Egorov : si φ_n est une suite de fonctions mesurables qui convergent presque partout, elle converge uniformément sur des compacts de mesure arbitrairement proche de 1.

On peut supposer les K_j croissants pour l'inclusion; notons A_0 l'union des K_j . L'image d'un compact par une application continue est un compact, si bien que $\varphi(K_j)$

est compact. L'ensemble $\varphi(A_0)$ est donc borélien. De la même façon, on peut trouver un ensemble borélien $A_1 \subset A^c$ tel que $\mu(A^c - A_1) = 0$ et $\varphi(A_1)$ est borélien. L'application φ étant injective, on a les égalités :

$$\varphi^{-1}\varphi(A) = A, \quad \varphi(A) \cap \varphi(A^c) = \emptyset.$$

Les inclusions $A_0 \subset \varphi^{-1}\varphi(A_0) \subset \varphi^{-1}\varphi(A) = A$ montrent que $\varphi_*\mu(\varphi A_0) = \mu(A)$. De même, $\varphi_*\mu(\varphi A_1) = \mu(A^c)$, si bien que l'ensemble $\varphi(A_0) \amalg \varphi(A_1)$ est de $\varphi_*\mu$ -mesure totale.

Enfin, les inclusions $\varphi(A) \subset \varphi(A^c)^c \subset \varphi(A_1)^c$ impliquent la relation suivante : $\varphi(A) - \varphi(A_0) \subset \varphi(A_1)^c \cap \varphi(A_0)^c$. Ce dernier ensemble est négligeable, donc l'image de A est $\varphi_*\mu$ -mesurable. †

L'énoncé du théorème étant de nature mesurable, il reste encore vrai sur tous les espaces probabilisés isomorphes à $[0, 1]$. La preuve qui vient d'être donnée se généralise immédiatement, lorsque $[0, 1]$ est remplacé par un borélien d'un espace métrique séparable complet ; ceci afin d'assurer la régularité de la mesure de probabilité borélienne μ .

Il n'existe, à notre connaissance, aucun ouvrage mentionnant ce résultat d'approximation. Cela ne signifie pas pour autant qu'il est nouveau : dans [Ro52], V. A. Rokhlin démontre qu'une famille dénombrable d'ensembles mesurables séparant les points engendre la tribu des ensembles mesurables. Ce résultat est parfois mentionné dans les livres de théorie de la mesure [Co80] [DRu90]. Il est obtenu comme corollaire des théorèmes de structure des ensembles analytiques.

3. Correspondance de Rokhlin

Que se passe-t-il lorsque les fonctions f_n ne séparent plus les points ? Peut-on encore caractériser les fonctions qui appartiennent à l'adhérence de l'algèbre engendrée par les f_n ? La réponse se trouve dans un article de V. A. Rokhlin [Ro52], qui met en correspondance les sous σ -algèbres de la tribu des ensembles mesurables, et certaines partitions de l'espace considéré.

3.1 Définitions

Définition 1. Une partition ξ de $[0, 1]$ est la donnée d'un ensemble de parties de $[0, 1]$, disjointes deux à deux, recouvrant $[0, 1]$. L'élément de la partition qui contient le point $x \in [0, 1]$ est noté $\xi(x)$.

La partition est dite mesurable s'il existe une famille dénombrable d'ensembles mesurables $\{B_n\}$ qui satisfait : $\forall C_1, C_2 \in \xi, C_1 \neq C_2, \exists n$ tq :

$$C_1 \subset B_n \text{ et } C_2 \subset B_n^c \quad \text{ou} \quad C_1 \subset B_n^c \text{ et } C_2 \subset B_n.$$

On convient d'identifier deux partitions ξ et η s'il existe un ensemble mesurable $\Omega \subset [0, 1]$, de mesure pleine, tel que $\xi(x) \cap \Omega = \eta(x) \cap \Omega, \forall x \in [0, 1]$.

Les éléments d'une partition mesurable sont mesurables. Il suffit de remarquer que les ensembles B_n qui interviennent dans la définition de la partition déterminent complètement cette partition : $\xi(x) = \bigcap_{B_n \ni x} B_n \cap \bigcap_{B_n^c \ni x} B_n^c$.

La σ -algèbre des ensembles μ -mesurables est notée \mathcal{T} . On dira qu'une sous σ -algèbre \mathcal{A} de \mathcal{T} est complète si elle contient les ensembles μ -mesurables négligeables relativement à la mesure μ . Il s'agit d'une complétion relative. Toute sous σ -algèbre $\mathcal{A} \subset \mathcal{T}$ admet une complétion unique : c'est la σ -algèbre engendrée par \mathcal{A} et les ensembles μ -négligeables. De manière équivalente, c'est l'ensemble des parties $\hat{A} \in \mathcal{T}$ pour lesquelles il existe un ensemble $\Omega \in \mathcal{T}$ de mesure pleine, et un ensemble $A \in \mathcal{A}$ satisfaisant : $\hat{A} \cap \Omega = A \cap \Omega$.

On dira qu'une σ -algèbre complète $\mathcal{A} \subset \mathcal{T}$ est *séparable* si c'est la complétion d'une σ -algèbre engendrée par une famille dénombrable de parties.

Lemme 3. *Toute σ -algèbre complète $\mathcal{A} \subset \mathcal{T}$ est séparable.*

Preuve :

L'espace $L^1([0, 1], \mathcal{T}, \mu)$ est séparable. Toute partie d'un espace métrique séparable étant séparable, l'ensemble $\{\mathbf{1}_A \mid A \in \mathcal{A}\}$ est séparable pour la norme L^1 . Soit $\{\mathbf{1}_{A_n}\}$ une partie dénombrable dense ; montrons que les A_n engendrent \mathcal{A} . Pour tout $A \in \mathcal{A}$, on peut trouver une suite n_k telle que $\mathbf{1}_{A_{n_k}}$ converge presque partout vers $\mathbf{1}_A$. La différence symétrique de A et de $\lim A_{n_k}$ est donc de mesure nulle ; l'ensemble A est dans la complétion de la σ -algèbre engendrée par les A_n . †

3.2 Partitions et σ -algèbres

Les algèbres de fonctions considérées dans la suite sont supposées unitaires : elles contiennent les constantes.

Correspondance [Ro52] *Il existe une bijection entre :*

- les partitions mesurables de $[0, 1]$;
- les sous σ -algèbres complètes de \mathcal{T} ;
- les sous-algèbres fermées de $L^0([0, 1], \mathcal{T}, \mu)$.

Cette correspondance est définie comme suit :

A la partition ξ , on associe la complétion de la σ -algèbre $\{A \in \mathcal{T} \mid A = \cup_{x \in A} \xi(x)\}$. Cette complétion est notée $\hat{\xi}$; elle est composée des ensembles mesurables saturés par ξ .

Soit \mathcal{A} une sous σ -algèbre, $\{B_n\}$ un ensemble dénombrable de parties tels que \mathcal{A} soit engendré par les B_n et les ensembles négligeables. On associe à \mathcal{A} la partition $\xi_{\mathcal{A}}$ dont les atomes sont donnés par $\xi_{\mathcal{A}}(x) = \bigcap_{B_n \ni x} B_n \bigcap_{B_n^c \ni x} B_n^c$.

Lemme 4. *La définition de la partition $\xi_{\mathcal{A}}$ ne dépend pas du choix des B_n .*

Preuve :

Soit B_n un ensemble de parties et $\langle B_n \rangle$ la σ -algèbre engendrée. On a l'égalité :

$$\bigcap_{B_n \ni x} B_n \bigcap_{B_n^c \ni x} B_n^c = \bigcap_{A \in \langle B_n \rangle} A$$

Pour voir cela, on remarque que $\langle B_n \rangle_{x,y} = \{A \in \langle B_n \rangle \mid x \in A \leftrightarrow y \in A\}$ est une σ -algèbre qui contient les ensembles B_n , si $x \in B_n \leftrightarrow y \in B_n, \forall n$.

Soit B_n et B'_n deux familles dénombrables dont \mathcal{A} est la complétion. Pour chaque n , il existe des ensembles $A_n^1, A_n^2 \in \langle B_n \rangle$ tel que $A_n^1 \subset B'_n \subset A_n^2$ et $\mu(A_n^2 - A_n^1) = 0$. De la même façon, il existe des ensembles $A_n'^1, A_n'^2 \in \langle B'_n \rangle$ tel que $A_n'^1 \subset B_n \subset A_n'^2$ et $\mu(A_n'^2 - A_n'^1) = 0$. Les partitions associées aux B_n et aux B'_n coïncident sur $\Omega = (\cup A_n^2 - A_n^1)^c \cap (\cup A_n'^2 - A_n'^1)^c$. †

La correspondance entre partitions et σ -algèbres est maintenant une conséquence du lemme suivant :

Lemme 5. *Soit ξ une partition mesurable de $[0, 1]$ et B_n les ensembles qui interviennent dans sa définition. Alors la σ -algèbre $\hat{\xi}$ est engendrée par les B_n et les ensembles négligeables.*

Preuve :

Soit $\varphi : [0, 1] \rightarrow \{0, 1\}^{\mathbb{N}}$ la fonction définie par $\varphi(x) = \{\mathbf{1}_{B_n}(x)\}$. L'image réciproque de la σ -algèbre des ensembles $\varphi_*\mu$ -mesurables est contenue dans la σ -algèbre engendrée par les B_n et les ensembles négligeables. Il s'agit donc de montrer qu'elle contient la σ -algèbre $\{A \in \mathcal{T} \mid A = \cup_{x \in A} \xi(x)\}$.

Considérons un ensemble $A \in \mathcal{T}$; on a l'égalité $\varphi^{-1}\varphi(A) = \cup_{x \in A} \xi(x)$. Par conséquent, si $A = \cup_{x \in A} \xi(x)$, on obtient :

$$\varphi^{-1}\varphi(A) = A, \quad \varphi(A) \cap \varphi(A^c) = \emptyset.$$

La preuve du second lemme montre que $\varphi(A)$ est $\varphi_*\mu$ -mesurable, ce qui termine la démonstration. †

La correspondance entre sous σ -algèbres complètes de \mathcal{T} et sous-algèbres fermées de L^0 dérive du premier lemme. Elle est donnée par :

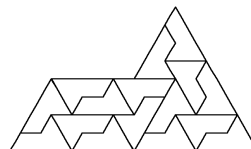
$$\begin{array}{ccc} \mathcal{A} & \longrightarrow & L^0([0, 1], \mathcal{A}, \mu) \\ \{A \in \mathcal{T} \mid \mathbf{1}_A \in \mathcal{A}^0\} & \longleftarrow & \mathcal{A}^0 \end{array}$$

Remarques :

- En général, la σ -algèbre associée à une partition ξ n'est pas la σ -algèbre engendrée par les éléments de la partition. Par exemple, la σ -algèbre associée à la partition en points est égale à \mathcal{T} , tandis que la σ -algèbre engendrée par les singletons ne contient que les ensembles négligeables et leurs complémentaires.
- On peut associer à une partition ξ un facteur $\pi : [0, 1] \rightarrow [0, 1]/\xi$; V. A. Rokhlin démontre que tous les facteurs sont de cette forme.
- Soit T une transformation de $[0, 1]$ qui préserve la mesure. La partition en orbites est mesurable si et seulement si T est intégrable du point de vue de la mesure : il existe une fonction mesurable dont les lignes de niveau coïncident avec les orbites de T . A l'opposé, si T est ergodique, toute partition mesurable qui contient la partition en orbites est grossière.

Illustrons cette correspondance sur un exemple : on cherche à construire sur \mathbf{R}^2 une base d'ondelettes, c'est-à-dire une base hilbertienne de L^2 satisfaisant des propriétés d'échelle. Pour cela, on se donne un pavage autosimilaire du plan.

Celui-ci est par exemple défini par la donnée d'une tuile de référence, disons un borélien d'intérieur non vide, et par une partition de cette tuile en un nombre fini de sous-ensembles qui peuvent être superposés à la tuile de référence à l'aide d'homothéties, rotations et translations.



En répétant ce procédé, on obtient une suite de partitions emboîtées, formées de tuiles dont le diamètre tend vers zéro. Considérons la famille \mathcal{F} des fonctions indicatrice de toutes les tuiles obtenues par ce procédé. C'est une famille dénombrable qui sépare les points. L'algèbre engendrée par \mathcal{F} est donc dense dans L^2 .

Remarquons maintenant que l'algèbre engendrée par les fonctions indicatrice des éléments d'une partition coïncide avec l'espace vectoriel engendré par ces fonctions. Par conséquent, l'espace vectoriel engendré par \mathcal{F} est dense dans L^2 . Il suffit d'appliquer un procédé d'orthonormalisation pour obtenir une base hilbertienne.

3.3 Approximation et partitions

Le théorème suivant est une conséquence immédiate de la correspondance qui vient d'être décrite :

Théorème 2. *Soit A^0 une sous-algèbre fermée de $L^0([0, 1], \mathcal{T}, \mu)$, contenant les constantes. Soit $f_n \in A^0$, $n \in \mathbf{N}$ une suite de (représentants de) fonctions mesurables qui engendrent A^0 . On définit une relation d'équivalence sur $[0, 1]$ comme suit :*

$$x \sim y \leftrightarrow f_n(x) = f_n(y), \forall n \in \mathbf{N}.$$

Cette relation ne dépend pas de la suite f_n , à un ensemble de mesure nulle près.

Une fonction $f \in L^0$ appartient à A^0 si et seulement si il existe un ensemble Ω de mesure pleine tel que la restriction de f à Ω est constante sur les classes d'équivalence de la relation \sim .

En d'autres termes, la projection $\pi : X \rightarrow X/\sim$ induit un isomorphisme de $L^0(X/\sim, \pi_*\mathcal{T}, \pi_*\mu)$ sur A^0 ; on a noté : $\pi_*\mathcal{T} = \{A \subset X/\sim \mid \pi^{-1}A \in \mathcal{T}\}$. Il est possible de donner un énoncé similaire pour les espaces L^p . Ces espaces ne sont pas des algèbres lorsque $p \neq 0$, si bien que le parallèle avec le théorème de Stone-Weierstrass est moins frappant. Afin de faire ressortir ce parallèle lorsque $p = 0$, on introduit les définitions suivantes :

Définition 2. *Un espace probabilisé (X, \mathcal{S}, ν) est un espace de Lebesgue s'il est isomorphe à $([0, 1], \mathcal{T}, \mu)$, où μ est une mesure borélienne sur $[0, 1]$ et \mathcal{T} est la complétion de la σ -algèbre des boréliens relativement à la mesure μ .*

On dit qu'une sous-algèbre de $L^0(X, \mathcal{S}, \nu)$ sépare les points s'il existe une suite de (représentants de) fonctions f_n de cette sous-algèbre et un ensemble mesurable Ω de mesure pleine tel que : $\forall x, y \in \Omega, x \neq y, \exists n \in \mathbf{N}, \text{ tq } f_n(x) \neq f_n(y)$.

Le résultat suivant est une reformulation du théorème 1. C'est aussi un corollaire du théorème 2.

Théorème 3. *Soit (X, \mathcal{S}, ν) un espace de Lebesgue, et A^0 une sous-algèbre de l'algèbre $L^0(X, \mathcal{S}, \mu)$, contenant les constantes. Alors l'algèbre A^0 sépare les points si et seulement si elle est dense dans L^0 .*

4. Conclusion

La notion de partition mesurable joue un rôle important en théorie ergodique. Elle intervient dans les problèmes de désintégration de mesures et dans les calculs d'entropie. Nous espérons avoir montré que cette notion peut être présentée à un niveau élémentaire, et que son intérêt ne se restreint pas au seul domaine de la théorie ergodique.

Yves Coudène
École Normale Supérieure de Paris
Mél : coudene@dma.ens.fr

Références

- [Co80] Cohn, Donald L. Measure theory. Birkhauser, Boston, Mass., 1980.
- [Du66] Dugundji, James. Topology. Allyn and Bacon, Inc., Boston, Mass. 1966.
- [Fed69] Federer, Herbert. Geometric measure theory. Die Grundlehren der mathematischen Wissenschaften, Band 153 Springer-Verlag New York Inc., New York 1969.
- [KV95] Kovacevic, J. Vetterli, M. Wavelets and subband coding, Prentice Hall, Signal Processing Series, 1995. <http://cm.bell-labs.com/who/jelena/TwinDragon>
- [Ro52] Rokhlin, V. A. On the fundamental ideas of measure theory. Amer. Math. Soc. Translation 1952, (1952). no. 71, 55 pp.
- [WRu73] Rudin, Walter. Functional analysis. McGraw-Hill Series in Higher Mathematics. McGraw-Hill Book Co., New York-Dusseldorf-Johannesburg, 1973.
- [DRu90] Rudolph, Daniel J. Fundamentals of measurable dynamics. Ergodic theory on Lebesgue spaces. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1990.