De la manière de battre les cartes en Amérique.

C'est trop super (quand on a compris) !

Un paquet de cartes est un ensemble fini $\mathscr{C} = \{1, \ldots, n\}$ muni d'une relation d'ordre total $\prec$ (où $i \prec j$ signifie que la carte i est au dessus de la carte j). L'ensemble des relations d'ordre totales sur $\mathscr{C}$ est en bijection[1] avec l'ensemble $\mathfrak{S}_n$ des permutations de $\mathscr{C}$: par exemple si $X \in \mathfrak{S}_n$, on définit l'ordre $\prec$ par : $X(1) \prec \ldots \prec X(n)$. Un paquet de cartes est donc aussi une permutation de $\mathscr{C}$. Un mélange du paquet est l'action par composition d'une permutation de $\mathscr{C}$ sur le paquet : par exemple, si $\sigma \in \mathfrak{S}_n$, le paquet $X(1) \prec \ldots \prec X(n)$ devient le paquet $\sigma \circ X(1) \prec \ldots \prec \sigma \circ X(n)$.[2]

Dans la suite, un paquet X est une variable aléatoire à valeurs dans $\mathfrak{S}_n$. Il est dit *bien mélangé* lorsque X suit la loi uniforme sur $\mathfrak{S}_n$, notée π. On s'intéresse à des mélanges successifs du paquet, modélisés par la chaîne de Markov $(X_k)_{k \in \mathbf{N}}$:

$$X_{k+1} = f(X_k, A_k), \quad X_0 = id$$

où les $(A_k)_{k \in \mathbf{N}^*}$ sont des variables aléatoires indépendantes à valeurs dans un certaine espace et qui suivent une loi donnée Q appelée *loi du mélange* (c'est la manière choisie de battre les cartes). On note μ_n la loi de X_n.

Problème. *La loi de $(X_k)_k$ converge-t-elle vers la loi uniforme π ? Dans quel sens ? Et à quelle vitesse ?*

On quantifie la convergence à l'aide de la :

Définition. On appelle *distance de variation totale* entre deux lois Q_1 et Q_2 sur $\mathfrak{S}_n$ la quantité :

$$d_v(Q_1, Q_2) := \max_{S \subset \mathfrak{S}_n} |Q_1(S) - Q_2(S)| = \frac{1}{2} \sum_{\sigma \in \mathfrak{S}_n} \big|Q_1(\{\sigma\}) - Q_2(\{\sigma\})\big|$$

On peut montrer que cette distance métrise la convergence en loi.

Le *mélange américain* consiste à couper aléatoirement le paquet en deux et à insérer les cartes du premier paquet aléatoirement au sein du second en gardant l'ordre relatif des paquets. Une façon équivalente voir les choses est de considérer le *mélange inverse* : on choisit aléatoirement k cartes que l'on place au dessus du paquet en gardant l'ordre relatif. Dit autrement : on se donne une partie $\mathcal{A} = \{i_1, \ldots, i_k\} \subset \{1, \ldots, n\}$ et on place les cartes en positions $i_1, \ldots, i_k$ au dessus du paquet en gardant l'ordre relatif. Par exemple si $\mathcal{A} = \{1, 3\}$ et $n = 4$, le paquet $2 \prec 4 \prec 1 \prec 3$ devient le paquet $2 \prec 1 \prec 4 \prec 3$ et la permutation associé par le mélange inverse est :

$$\pi_0 = \begin{pmatrix} 2 & 4 & 1 & 3 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

[1] Il y a plein de bijections, on prendra celle explicitée ci-après.

[2] Il n'est pas utile de noter différemment la relation d'ordre pour au moins deux raisons : d'abord parce que sa définition est contenue dans l'écriture ci-dessus et aussi parce que $\prec$ pourra garder de fait sa signification concrète tout au long du texte. En cas de réel besoin, on notera $\prec_\sigma$ l'ordre induit par la permutation σ mais génériquement, un paquet sera toujours noté $X(1) \prec \ldots \prec X(n)$.

elle dépend du paquet :

$$X = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \quad \text{qui devient} \quad \pi_0 \circ X = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

C'est complètement tordu mais c'est très pratique parce qu'il suffit d'écrire que le paquet $X(1) \prec \ldots \prec X(n)$ devient le paquet $\pi_0 \circ X(1) \prec \ldots \prec \pi_0 \circ X(n)$ et en fait on n'a pas du tout besoin de savoir comment s'écrit π_0 : étant donné un paquet X et une partie $\mathcal{A}$ on peut en déduire le nouveau paquet[3] : on vient de définir le f de la chaîne de Markov.

Remarquons que tirer une variable aléatoire $\mathscr{A}$ à valeurs dans $\mathcal{P}(\{1\ldots,n\})$ suivant la loi uniforme revient à tirer une variable aléatoire π_0 à valeurs dans $\mathfrak{S}_n$ (associée par le mélange inverse) qui suit la loi :

$$Q(\{\sigma\}) := \begin{cases} \frac{n+1}{2^n} & \text{si } \sigma = id \\ \frac{1}{2^n} & \text{si } \sigma \in H \setminus \{id\} \\ 0 & \text{sinon.} \end{cases}$$

où H est l'ensemble des permutations σ comportant au plus une décroissance ($X(C_i) \prec X(C_j)$ et $X(C_j) \prec_\sigma X(C_i)$). En effet, le choix des parties de la forme $\{1,\ldots,j\}$ conduisent à l'identité. C'est néanmoins très inutile d'écrire cela.

Théorème. *Après avoir effectués k mélanges à l'américaine sur un jeu de n cartes, la distance de variation totale vérifie :*

$$d_v(\mu_k,\pi) \leq 1 - \prod_{i=1}^{n-1} \left(1 - \frac{i}{2^k}\right).$$

Preuve. Avec les notations précédentes, notons $(\mathscr{A}_k)_{k\in\mathbf{N}^*}$ une suite de variables aléatoires indépendantes à valeurs dans $\mathcal{P}(\{1,\ldots,n\})$ et suivant la loi uniforme. Soit $(\pi_k)_k$ la suite des permutations associée par le mélange inverse et $X_k = \pi_k \circ X_{k-1}$ le paquet à l'instant k. Soit $i \in \{1,\ldots,n\}$. Pour tout $k \in \mathbf{N}^*$, on pose $b_k^{(i)} = \mathbf{1}_{i\in\mathcal{A}_k^c}$: puisque les $\mathscr{A}_k$ suivent la loi uniforme et sont indépendantes, les $(b_k^{(i)})_k$ sont des variables aléatoires de Bernoulli indépendantes de paramètre $1/2$. On note enfin $b^{(k)}(i) = b_k^{(i)} \ldots b_1^{(i)}$ le nombre binaire aléatoire construit par concaténation[4] Soit T le plus petit instant où tous les nombres $b^{(k)}(1),\ldots,b^{(k)}(n)$ sont distincts. À l'instant T le paquet est bien mélangé au sens défini précédemment. En effet, à cet instant (mais pas avant), les $b^{(T)}(i)$ définissent un ordre total sur $\mathscr{C}$ et comme toutes les variables aléatoires sont indépendantes et suivent une loi uniforme, l'ordre construit suit aussi une loi uniforme. Or, on a pour tout $\mathfrak{P} \subset \mathfrak{S}_n$:

$$\begin{aligned} \mu_k(\mathfrak{P}) &= \mathbf{P}(X_k \in \mathfrak{P}) = \mathbf{P}(X_k \in \mathfrak{P}, T \leq k) + \mathbf{P}(X_k \in \mathfrak{P}, T > k) \\ &\leq \sum_{j=0}^{k} \mathbf{P}(X_k \in \mathfrak{P}, T = j) + \mathbf{P}(T > k) \\ &\leq \sum_{j=0}^{k} \pi(\mathfrak{P})\mathbf{P}(T = j) + \mathbf{P}(T > k) \\ &\leq \pi(\mathfrak{P}) + \mathbf{P}(T > k) \end{aligned}$$

[3]On pourrait l'écrire mais bon…

[4]Interprétation : on attribue 0 aux cartes que l'on place au dessus, 1 aux autres. On garde en mémoire l'histoire de chaque carte. Un schéma s'imposerait, si ça ne demandait pas tant de prouesses techniques.

où π est on le rappelle la loi uniforme sur $\mathfrak{S}_n$. En faisant pareil avec $\mathfrak{P}^c$, on trouve :

$$\forall \mathfrak{P} \subset \mathfrak{S}_n, \ |\mu_k(\mathfrak{P}) - \pi(\mathfrak{P})| \leq \mathbf{P}(T > k) \Longrightarrow d_v(\mu_n, \pi) \leq \mathbf{P}(T > k).$$

Il y a 2^k possibilités pour le nombre associé à une carte. Comme les $b^{(k)}(i)$ sont indépendants et uniformément distribués, la probabilité que tous les $b^{(k)}(i)$ soient différents au k-ème mélange vaut :

$$\frac{2^k(2^k-1)\dots(2^k-(n-1))}{(2^k)^n} = \prod_{i=1}^{n-1}\left(1-\frac{i}{2^k}\right)$$

(c'est le "paradoxe des anniversaires"). Alors :

$$\mathbf{P}(T > k) = 1 - \prod_{i=1}^{n-1}\left(1-\frac{i}{2^k}\right)$$

□

Remarquons, qu'à n fixé,

$$d_v(\mu_k, \pi) \underset{k\to+\infty}{\sim} \frac{n-1}{2^k}.$$

Mais comme ça va très très vite, il convient de s'interroger sur le sens de l'infini.

Quelques remarques complémentaires

Toutes les remarques intéressantes (et il y en a) sont à retrouver chez Grégoire Clarté (et dans un texte de modélisation option A sur le sujet).

Référence. M. Aigner, G. Ziegler, *Raisonnements divins*

Adapté d'un travail remarquable de l'inénarrable Grégoire Clarté.

105 Groupe des permutations d'un ensemble fini. Applications. *(heureusement que c'était une impasse)*
190 Méthodes combinatoires, problèmes de dénombrement.
262 Modes de convergence d'une suite de variables aléatoires. Exemples et applications.
264 Variables aléatoires discrètes. Exemples et applications.