22 - EXISTENCE D'UNE VARIABLE ALÉATOIRE RÉELLE DE LOI DONNÉE

MISE À JOUR DU 17/10/2012 : AJOUT DU § D

www.daniel-saada.eu

Est rigoureuse toute démonstration, qui, chez tout lecteur suffisamment instruit et préparé, suscite un état d'évidence qui entraîne l'adhésion.

[**René Thom**]

La loi d'une variable aléatoire réelle X sur $(\Omega,\mathcal{T},p)$ est une probabilité q sur $(\mathbb{R},\mathcal{B}^1)$: réciproquement, q étant donnée sur $(\mathbb{R},\mathcal{B}^1)$, existe-t-il X de loi q ? En particulier, existe-t-il sur $(\Omega,\mathcal{T},p)$ une loi uniforme (continue car nous supposerons $card\,\Omega > \aleph_0$) ? À ces questions, nous apportons les réponses suivantes :

Pour que X existe pour toute q, il faut et il suffit qu'existe sur $(\Omega,\mathcal{T},p)$ une loi uniforme U ;
pour qu'il existe sur $(\Omega,\mathcal{T},p)$ une loi uniforme U, il faut et il suffit que p soit sans atome sur $(\Omega,\mathcal{T})$.

On peut évidemment supposer sans perte de généralité que $U(\Omega)=]0,1[$ ou $U(\Omega)=[0,1]$; nous démontrerons *in fine* qu'il existe en fait sur Ω une infinité dénombrable de lois uniformes indépendantes.

A) L'existence de U équivaut à p est sans atome

1) *Une première condition nécessaire et suffisante pour que U existe*

Lorsque U existe, la famille des événements $E_t=(U\le t)$ est croissante en t pour l'inclusion et $p(E_t)=t$ pour tout t. Réciproquement, supposons l'existence, dans la tribu, d'une famille croissante $(E_t)_{t\in]0,1[}$ telle que $p(E_t)=t$ pour tout t. En posant $E_1=\Omega$, l'ensemble des réels u tels que $\omega\in E_u$ n'est vide pour aucun ω de Ω. On définit alors la fonction U par

$$U(\omega)=\inf\{u\in[0,1]:\omega\in E_u\}.$$

Par définition de $U(\omega)$ et en raison de la croissance par inclusion des E_u, $U(\omega)<u$ implique $\omega\in E_u$, aussi l'événement $(U<\lambda)$ est-il inclus dans E_λ. D'autre part, $\omega\in E_u$ et $u<\lambda$ entraînent $U(\omega)<\lambda$, d'où $\bigcup_{u\in]0,\lambda[}E_u\subset(U<\lambda)$. Enfin, comme $U(\omega)<\lambda$ signifie $U(\omega)=u_0<\lambda$, on a $\omega\in E_u$ dès que $u\in]u_0,\lambda[$ et donc $(U<\lambda)\subset\bigcup_{u\in]0,\lambda[}E_u$. En conséquence : $(U<\lambda)=\bigcup_{u\in]0,\lambda[}E_u\subset E_\lambda$.

a) U est une variable aléatoire sur $(\Omega,\mathcal{T})$

Il faut prouver que l'image réciproque par U d'un intervalle de $\mathbb{R}$ est élément de $\mathcal{T}$. Or, par croissance et densité,

$$(U<\lambda)=\bigcup_{u\in]0,\lambda[}E_u=\Big\{\bigcup E_r : r\in[0,\lambda[\cap\mathbb{Q}\Big\},$$

et donc $(U<\lambda)$ est dans la tribu. Et alors, $(U\le\lambda)\in\mathcal{T}$ puisque $(U\le\lambda)=\bigcap_n(U<\lambda+1/n)$. On fera de même pour les autres types d'intervalles de $\mathbb{R}$.

b) U est uniforme sur $[0,1]$: $p(U\le t)=t$

La double inclusion $E_u\subset(U<\lambda)\subset E_\lambda$, valable quand $u<\lambda$, donne $u\le p(U<\lambda)\le\lambda$ puis $p(U<\lambda)=\lambda$; on en déduit $p(U\le\lambda)=\lim_n p(U<\lambda+1/n)=\lambda$.

Complément : exemple d'une chaîne E_t

Supposons qu'il existe une probabilité *p* sur $(\mathbb{R}^n, \mathcal{B}^n)$ pour laquelle toutes les sphères de centre 0 sont négligeables, y compris $\{0\}$ (il en est ainsi quand $n=1$ et p est diffuse). Posons $F(r) = p(B(0,r)) = p(B'(0,r))$:

F est croissante et continue sur $\mathbb{R}^+$, à valeurs dans $[0,1]$.

La limite de F en $+\infty$, qui existe, est $p(\mathbb{R}^n)=1$ et $F(0)=p\{0\}=0$. Il en résulte que F est une surjection de $]0,+\infty[$ sur $]0,1[$. Il existe alors une fonction G de $]0,1[$ dans $]0,+\infty[$ telle que $FoG = id$ (axiome du choix).

Posons $E_t = B\big(0, G(t)\big)$ pour $t \in]0,1[$: les E_t sont croissants, appartiennent à $\mathcal{B}^n$ et $p(E_t) = F\big(G(t)\big) = t$.

2) *Il faut et il suffit que* p *soit sans atome sur* $(\Omega, \mathcal{T})$

Rappelons que « p est sans atome » signifie que si A de la tribu n'est pas négligeable pour p, il existe $B \subset A$ tel que $0 < p(B) < p(A)$[1]. Dans ce cas, on démontre qu'il existe une chaîne croissante d'événements $(E_t)_{t\in[0,1]}$ telle que $p(E_t) = t$ pour tout t (mon ouvrage, pages 270 et suivantes, chapitre **17** ; il y est démontré que toute probabilité diffuse sur $\mathbb{R}^n$ muni de sa tribu borélienne est sans atome).

Nous prouvons la réciproque (démonstration de Alain Rémondière).

On raisonne par l'absurde en supposant que la tribu contient une chaîne croissante d'événements $\big(E(t)\big)_{t\in[0,1]}$ telle que $p\big(E(t)\big) = t$ et que p a un atome A dans la tribu : $p(A)>0$, $B \subset A$ impliquant $p(B)=0$ ou $p(B)=p(A)$.

On pose $A(t) = A \cap E(t)$: comme $p\big(A(t)\big)=0$ ou $p(A)$ pour tout t, on introduit

$$I = \big\{t \in [0,1] : p\big(A(t)\big) = 0\big\} \ , \ J = \big\{t \in [0,1] : p\big(A(t)\big) = p(A)\big\}.$$

I et J sont des intervalles, non vides, disjoints, de somme $[0,1]$, aussi $\sup I = \inf J$. On pose $t_0 = \sup I = \inf J$, $t_0 \in]0,1]$ car $t \in J$ implique $t \geq p(A)$ en vertu de l'inégalité $p\big(A(t)\big) \leq t$.

On suppose $t_0 < 1$: à partir d'un certain rang n_0, $t_0 - 1/n_0$ et $t_0 + 1/n_0$ sont entre 0 et 1 et il est donc permis d'envisager les événements $F = \bigcup_{n_0}^{\infty} E(t_0 - 1/n) \subset E(t_0)$ et $G = \bigcap_{n_0}^{\infty} E(t_0 + 1/n) \supset E(t_0)$.

Comme

$$F \cap A = \bigcup_{n_0}^{\infty} A(t_0 - 1/n) \quad \text{et} \quad G \cap A = \bigcap_{n_0}^{\infty} A(t_0 + 1/n)$$

on a, par monotonie, $p(F \cap A) = \lim_n p\big(A(t_0 - 1/n)\big) = 0$ et $p(G \cap A) = \lim_n p\big(A(t_0 + 1/n)\big) = p(A)$.

Mais $p(G - F) = 0$, car pour $n \geq n_0$, $G - F \subset \big(E(t_0 + 1/n) - \big(E(t_0 - 1/n)\big)\big)$ et $p(G-F) \leq 2/n$; on en déduit sans mal que $p(G \cap A) = 0$: c'est la contradiction cherchée car $p(G \cap A)$ vaut aussi $p(A)$.

Reste le cas $t_0 = 1$: $F = \bigcup_2^{\infty} E(1 - 1/n)$ est de probabilité 1 et la décomposition $A = F \cap A + (\Omega - F) \cap A$ donne $p(A) = 0$, ce qui est contradictoire. En conclusion :

---

[1] En conséquence, si le singleton $\{x\}$ appartient à la tribu, $p\big(\{x\}\big) = 0$; si tous les singletons sont dans la tribu, on dit que p est diffuse.

Il existe une loi uniforme sur $(\Omega,\mathcal{T},p)$ si et seulement si la probabilité p est sans atome

Exemple. Sur $[0,1]^n$, muni de sa tribu borélienne et de la mesure de Lebesgue, existent n variables uniformes naturelles, à savoir $(x_1,...,x_n)\to x_i$. Il en résulte que la mesure de Lebesgue n'a pas d'atome sur cet univers. Une démonstration topologique directe de ce fait figure dans mon ouvrage, **p. 269 § 2)**.

B) Si U uniforme sur $]0,1[$ existe, toutes les autres lois aussi

Soit q une probabilité sur $\mathbb{R}$ et F sa fonction de répartition : $F(t)=p\left(]-\infty,t]\right)$.

Si F est strictement croissante, F est une bijection de $\mathbb{R}$ sur $]0,1[$, $X=F^{-1}\circ U$ est une variable aléatoire sur $(\Omega,\mathcal{T},p)$, de loi q puisque $p(X\le t)=p(F^{-1}\circ U\le t)=p(U\le F(t))=F(t)$.

Quand F n'est pas bijective, nous allons prouver qu'il existe néanmoins une fonction G de $]0,1[$ dans $\mathbb{R}$ telle que la variable aléatoire $X=G\circ U$ soit de loi q : G s'appelle la pseudo-inverse de F, ou l'inverse de F au sens de Paul Lévy. Rappelons que pour établir que q est la loi de probabilité de X, il suffit de vérifier que $p(X\le t)=F(t)$ pour tout réel t car deux variables aléatoires réelles ayant même fonction de répartition ont la même loi de probabilité.

1) Définition de G

Montrons d'abord que pour t dans $]0,1[$, $\{s:F(s)\ge t\}$ est une partie minorée de $\mathbb{R}$. Si c'était faux, il existerait une suite (s_n) vérifiant à la fois $s_n<-n$ et $F(s_n)\ge t$ et on en déduirait $\lim\limits_n F(s_n)=\lim\limits_{-\infty}F(x)=0\ge t$, or t est >0.

On est donc en droit de poser $G(t)=\inf\{s:F(s)\ge t\}$ quand $t\in]0,1[$; G coïncide avec F^{-1} quand F est bijective (ou strictement croissante).

2) Propriétés de G

Le lecteur vérifiera sans peine que :

a) G croissante et continue à gauche,

b) $G\circ F\le id$ et $F\circ G\ge id$,

c) $F(s)\ge t$ équivaut à $G(t)\le s$.

3) $G\circ U$ a pour loi q

En effet, $p(G\circ U\le t)=p(F(t)\ge U)=F(t)$.

On a donc montré que si p est sans atome sur $(\Omega,\mathcal{T})$, il existe pour toute variable aléatoire X sur $(\Omega,\mathcal{T},p)$ une fonction numérique croissante F sur $]0,1[$ telle $F\circ U$ ait même loi de probabilité que X, U étant uniforme sur $]0,1[$. Attention, il ne s'ensuit pas que X puisse coïncider avec une $F\circ U$, ni même avec un composé $\varphi\circ U$, où φ est une fonction borélienne (ou mesurable) : en effet, l'égalité $X=\varphi\circ U$ est impossible si X et U sont indépendantes.

C) L'existence d'une loi uniforme équivaut à l'existence d'une suite de lois de Bernoulli indépendantes $B(1/2)$

Supposons l'existence sur $(\Omega,\mathcal{T},p)$ d'une variable aléatoire U à valeurs dans $[0,1[$.

On sait que le réel $x = U(\omega)$ s'écrit d'une seule façon $\sum_1^\infty x_n / 2^n$, avec $x_n \in \{0,1\}$ pour tout n et $x_n = 0$ pour une infinité de n : x_n est le nième chiffre de x en base deux dans le *développement dyadique propre* de x. Par exemple, $x = 1/2$ se décompose en $0,1000...$, mais aussi en $0,0111....$ (développement *impropre*).

Pour $n \geq 1$, soit $B_n : \Omega \to \mathbb{R}$ définie par $B_n(\omega) = U(\omega)_n$.

Chaque B_n est une variable aléatoire de Bernoulli $B(1/2)$ de paramètre $1/2$.

Explicitons d'abord x_n en fonction de x. On a $2^{n-1}.x = k + \frac{x_n}{2} + 2^{n-1}\sum_{n+1}^\infty \frac{x_i}{2^i}$, avec k entier, mais comme *un au moins des x_i est nul*, $2^{n-1}\sum_{n+1}^\infty \frac{x_i}{2^i} < 2^{n-1}\sum_{n+1}^\infty \frac{1}{2^i} = \frac{1}{2}$ et donc $2^{n-1}.x = k + \frac{x_n}{2} + r$ avec $0 \leq r < \frac{1}{2}$. On en déduit $2^n.x = 2k + x_n + 2r$, puis $k = \text{int}(2^{n-1}x)$, $\text{int}(2^n.x) = 2k + x_n$, d'où $x_n = \text{int}(2^n x) - 2\,\text{int}(2^{n-1}x)$. Autrement dit,

$$x_n = 0 \Leftrightarrow 0 \leq 2^{n-1}x - \text{int}(2^{n-1}x) < 1/2\,,\quad x_n = 1 \Leftrightarrow 1/2 \leq 2^{n-1}x - \text{int}(2^{n-1}x) < 1\,.$$

Il en résulte que $B_n = 0$ si et seulement si il existe un entier $k \in \{0,1,...,2^{n-1}-1\}$, k étant la partie entière de $2^{n-1}U(\omega)$, tel que $\frac{k}{2^{n-1}} \leq U(\omega) < \frac{k}{2^{n-1}} + \frac{1}{2^n}$, ce qui montre le caractère mesurable de B_n et donne enfin

$$p(B_n = 0) = 2^{n-1} \times \frac{1}{2^n} = \frac{1}{2}.$$

Les variables aléatoires $(B_n)_{n\geq 1}$ sont indépendantes.

Il s'agit de prouver que, pour $n \geq 1$ et $\varepsilon_i = 0$ ou 1, $p\left(\bigcap_1^n (B_i = \varepsilon_i)\right) = \prod_1^n p(B_i = \varepsilon_i)$.

L'ensemble des réels x pour lesquels $x_i = \varepsilon_i$ pour i allant de 1 à n est l'intervalle $\left[\frac{\varepsilon_1}{2} + ... + \frac{\varepsilon_n}{2^n}, \frac{\varepsilon_1}{2} + ... + \frac{\varepsilon_n}{2^n} + \frac{1}{2^n}\right[$.

Donc $\bigcap_1^n (B_i = \varepsilon_i) = \left\{\omega \in \Omega : \frac{\varepsilon_1}{2} + ... + \frac{\varepsilon_n}{2^n} \leq U_n(\omega) < \frac{\varepsilon_1}{2} + ... + \frac{\varepsilon_n}{2^n} + \frac{1}{2^n}\right\}$ et $p\left(\bigcap_1^n (B_i = \varepsilon_i)\right) = (1/2)^n$.

Réciproquement, s'il existe sur $(\Omega, \mathcal{T}, p)$ une suite $(B_n)_{n\geq 1}$ de $B(1/2)$ indépendantes, alors il existe une variable U uniforme, à savoir $U = \sum_1^\infty B_n / 2^n$. D'abord, $\sum_1^N B_n / 2^n$ est une loi discrète uniforme sur les $\frac{k}{2^{N+1}}$, k variant de 0 à $2^{N+1} - 1$ (vérification laissée au lecteur) ; ensuite $\sum_1^N B_n / 2^n$ a une limite en loi uniforme sur $[0,1]$ car si t est dans $[0,1]$ et si on pose $k_n = \text{int}(2^{n+1}.t)$, alors $\frac{k_n}{2^{n+1}} \leq t \leq 1 + \frac{k_n}{2^{n+1}}$ et $\lim_n \frac{k_n}{2^{n+1}} = t$, et donc

$$p\left(\sum_1^N B_n / 2^n \leq t\right) = k_n / 2^{n+1} \to t\,.$$

Enfin, comme $\sum_1^N B_n / 2^n$ converge aussi en loi vers U (la convergence simple implique la convergence en loi), U est uniforme.

On aurait pu aussi utiliser un théorème de Paul Lévy : pour qu'une suite de variables aléatoires réelles (X_n) converge en loi vers X, il faut et il suffit que pour tout réel t la suite des espérances $E(e^{itX_n})$ ait pour limite $E(e^{itX})$.

Ici, $E(e^{itB_n/2^n}) = \dfrac{1+e^{it/2^n}}{2}$ et donc $E(e^{it\sum_1^N B_n/2^n}) = \prod_1^N \dfrac{1+e^{it/2^n}}{2}$: quand N tend vers l'infini, y a-t-il convergence de $\prod_1^N \dfrac{1+e^{it/2^n}}{2}$ vers $E(e^{itU}) = \int_0^1 e^{itu}du = \dfrac{e^{it}-1}{it}$? On supposera bien sûr $t \neq 0$.

Comme $\dfrac{1+e^{it/2^n}}{2} = \cos(t/2^{n+1})e^{it/2^{n+1}}$, on a $\prod_1^N \dfrac{1+e^{it/2^n}}{2} = \prod_1^N e^{it/2^{n+1}} \prod_1^N \cos(t/2^{n+1})$.

D'une part, $\prod_1^N e^{it/2^{n+1}} = e^{i\sum_2^{N+1} t/2^n} \to e^{it/2}$ quand $N \to +\infty$; d'autre part, avec $\cos a = \sin 2a / 2\sin a$,

$\prod_1^N \cos(t/2^{n+1}) = \dfrac{\sin(t/2)}{2^N.\sin(t/2^{N+1})} \to \dfrac{\sin(t/2)}{t/2}$. Donc, $\prod_1^N \dfrac{1+e^{it/2^n}}{2}$ a pour limite $e^{it/2}\dfrac{\sin(t/2)}{t/2} = \dfrac{e^{it}-1}{it}$.

Enfin, soit $(k,l) \to n(k,l)$ la bijection de $\mathbb{N}^2$ sur $\mathbb{N}^*$ définie par $n(k,l) = 2^k(2l+1)$ (je ne connaissais pas le site http://jeux-et-mathematiques.davalan.org/divers/bij/).

Pour chaque $k \in \mathbb{N}$, $U_k = \sum_{l=1}^{\infty} B_{n(k,l)}/2^l$ suit une loi uniforme sur $[0,1]$; $(U_k)_{k\in\mathbb{N}}$ est une suite de variables aléatoires *indépendantes* car, pour $k \neq k'$, aucun indice $n(k,l)$ ne coïncide avec un $n(k',l')$:

$$\{n(k,l) : l \in \mathbb{N}\} \cap \{n(k',l) : l \in \mathbb{N}\} = \varnothing .$$

EN CONCLUSION, POUR QU'IL EXISTE SUR $(\Omega, \mathcal{T}, p)$ UNE SUITE U_n DE VARIABLES UNIFORMES ET INDÉPENDANTES IL FAUT ET IL SUFFIT QUE p SOIT SANS ATOME SUR $(\Omega, \mathcal{T})$; IL EXISTERA AUSSI UNE SUITE DE VARIABLES INDÉPENDANTES DE LOI DONNÉE EN COMPOSANT U_n PAR G COMME VU EN **B)**.

Nous finissons en donnant des exemples de variables uniformes sur l'univers $\Omega = [0,1]$ muni de sa tribu borélienne et de la mesure m de Borel-Lebesgue qui est une probabilité sans atome sur Ω. Nous nous limiterons aux applications f de Ω dans $[0,1]$, lesquelles doivent vérifier : $m\{t \in [0,1] : f(t) \leq a\} = a$ pour tout a de $[0,1]$.

Exemple 1. Les fonctions $f(x) = x$ et $f(x) = 1-x$, les seules qui soient monotones, ou dérivables, sur $]0,1[$.

Exemple 2. La fonction (dite chaotique) $f(x) = 2x$ sur $[0,1/2]$ et $f(x) = 2-2x$ sur $[1/2,1]$.

Exemple 3. Les fonctions $f(x) = x+a$ pour x dans $[0,1-a]$ et $f(x) = x+a-1$ ailleurs (qui sont des rotations déguisées sur le demi-cercle unité supérieur).

Exemple 4. Les fonctions $f(x) = nx - \text{int}(nx)$, où n est un entier ≥ 2.

- *$f(x) = x$ et $f(x) = 1-x$ sont les seules variables uniformes qui soient monotones*. Supposons f croissante et soit a dans l'intérieur de $[0,1]$: $l^- = \lim_{a^-} f$ et $l^+ = \lim_{a^+} f$ existent et $l^- \leq f(a) \leq l^+$. Comme $x < a$ implique $f(x) \leq l^-$, $m([0,a[) \leq m(f \leq l^-)$ et donc $a \leq l^-$. De même, $x > a$ impliquant $f(x) \geq l^+$, on a $1-a \leq 1-l^+$. D'où $l^+ \leq a \leq l^-$ puis $l^+ = a = l^-$ et enfin $a = f(a)$, ce qui prouve $f = id$. Avec f décroissante, on aurait abouti à $f = 1-id$.

- *$f(x)=x$ et $f(x)=1-x$ sont les seules variables uniformes qui soient dérivables sur* $]0,1[$. Commençons par montrer que pour tout a de $]0,1[$, $|f'(a)|\geq 1$. On traduit que $\left|\frac{f(x)-f(a)}{x-a}\right|$ a pour limite $|f'(a)|$ quand x tend vers a : $\varepsilon>0$ étant fixé, il existe $h>0$ tel que $\left|\frac{f(x)-f(a)}{x-a}\right|\leq \varepsilon+|f'(a)|$ sur $[a-h,a+h]$. On en déduit

$$|f(x)-f(a)|\leq(\varepsilon+|f'(a)|)h \text{ , puis } -(\varepsilon+|f'(a)|)h\leq f(x)-f(a)\leq(\varepsilon+|f'(a)|)h .$$

La mesure de $[a-h,a+h]$ est $2h$ et $m\{t:u\leq f(t)\leq v\}=v-u$, d'où $2h\leq 2(\varepsilon+|f'(a)|)h$, $\varepsilon+|f'(a)|\geq 1$ pour tout $\varepsilon>0$ et donc $|f'(a)|\geq 1$. Une fonction dérivée vérifiant le Théorème des valeurs intermédiaires, il vient $f'\geq 1$ ou $f'\leq -1$: f est donc monotone et on sait alors que $f=id$ ou $1-id$.

D) Complément

Quand il n'existe pas sur $(\Omega,\mathcal{T},p)$ de variable aléatoire réelle de loi q , il est néanmoins possible de trouver un espace probabilisé $(\Omega',\mathcal{T}',p')$ fortement lié à $(\Omega,\mathcal{T},p)$ sur lequel existe une variable aléatoire de loi q .
En effet, posons $\Omega'=\Omega\times R$, munissons Ω' de la tribut produit $\mathcal{T}'=\mathcal{T}\otimes\mathcal{B}(R)$ et de la probabilité $p'=p\otimes q$:

X définie par $X(\omega,r)=r$ est une variable aléatoire sur $(\Omega',\mathcal{T}')$ car $X^{-1}(B)=\Omega\times B$,

et $p'\left(X^{-1}(B)\right)=p'(\Omega\times B)=q(B)$.

Source : Terence Tao,
http://terrytao.wordpress.com/2010/01/01/254a-notes-0-a-review-of-probability-theory/#comment-182404

mon ouvrage : http://books.google.fr/books?id=kq69nXaoV-AC&printsec=frontcover#v=onepage&q&f=false