Séminaire Delange-Pisot-Poitou. Théorie des nombres

Michel Mendès France

Étude d'une classe de fonctions pseudo-aléatoires

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 4 (1962-1963), exp. n° 10, p. 1-5

<http://www.numdam.org/item?id=SDPP_1962-1963__4__A9_0>

Séminaire DELANGE-PISOT
(Théorie des nombres)
4e année, 1962/63, n° 10

28 janvier 1963

ÉTUDE D'UNE CLASSE DE FONCTIONS PSEUDO-ALÉATOIRES

par Michel MENDÈS FRANCE

I. Définition d'une fonction pseudo-aléatoire.

On appellera fonction pseudo-aléatoire, une fonction complexe de la variable réelle t, localement intégrable, nulle pour $t < 0$ et telle que la fonction de corrélation

$$\gamma(h) = \lim_{T\to\infty} \frac{1}{T} \int_0^T \overline{f}(t)\, f(t+h)\, dt \tag{1}$$

existe, soit continue non nulle à l'origine et tende vers 0 lorsque h augmente indéfiniment [1].

Dans ce qui suit, nous aurons à nous occuper uniquement de fonctions pseudo-aléatoires constantes dans tout intervalle $[k, k+1[$ où $k = 0, 1, 2, \ldots$

Si t est un nombre réel, les symboles $\hat{t}$ et $\check{t}$ désigneront respectivement la partie entière et la partie fractionnaire de t.

LEMME 1. - *Soit $f(t)$ une fonction complexe de la variable réelle t telle que $f(t) \equiv f(\hat{t})$. Si la fonction de corrélation $\gamma(h)$ de f existe pour les valeurs entières de h, elle existe pour tout h, est continue et varie linéairement dans tout intervalle $[k, k+1]$, $k = 0, 1, 2, \ldots$*

La démonstration de ce lemme est élémentaire. On la trouvera par exemple dans BASS ([1], p. 17).

II. Fonctions de Rademacher.

On sait que tout nombre x de l'intervalle $[0, 1)$ admet une représentation de la forme

$$x = \sum_{k=1}^{\infty} \frac{\varepsilon_k(x)}{2^k} \tag{2}$$

où $\varepsilon_k(x)$ est soit 0, soit 1, suivant les valeurs de k. L'égalité $\frac{1}{2^p} = \frac{1}{2^{p+1}} + \frac{1}{2^{p+2}} + \ldots$ montre que pour certains nombres x exceptionnels, il

peut y avoir deux représentations de la forme (2). On conviendra de choisir celle pour laquelle $\varepsilon_k(x)$ est nulle pour k assez grand. Dans ces conditions, l'ensemble des nombres de $[0, 1)$ et l'ensemble des suites $\{\varepsilon_k\}_{k=1}^{\infty}$ sont en bijection.

On appelle fonctions de Rademacher les fonctions $\Gamma_k(x) = 1 - 2\varepsilon_k(x)$. Elles prennent donc les valeurs $+1$ et -1 et vérifient l'identité

$$1 - 2x = \sum_{k=1}^{\infty} \frac{\Gamma_k(x)}{2^k} . \tag{3}$$

Ces fonctions peuvent d'ailleurs être définies par

$$\Gamma_k(x) = (-1)^{\widehat{2^k x}} . \tag{4}$$

Un des buts de cet exposé est de démontrer le théorème suivant, dû à WIENER [6]:

La fonction $f(t) = \Gamma_{\hat{t}}(x)$ de la variable réelle $t \geq 1$ est pseudo-aléatoire pour presque tous les nombres x de l'intervalle $[0, 1)$.

Nous construirons ensuite un ensemble E de nombres x pour lesquels on soit sûr que la fonction $f(t)$ soit pseudo-aléatoire.

L'obtention de ces résultats découlera du lemme suivant et du théorème ergodique de Birkhoff.

LEMME 2. - Soit $k_1, k_2, \ldots, k_s$ une suite d'entiers strictement croissants. Alors l'égalité

$$\int_0^1 \Gamma_{k_1}(x)\, \Gamma_{k_2}(x) \cdots \Gamma_{k_s}(x)\, dx = 0 \tag{5}$$

a lieu.

En effet

$$I = \int_0^1 \Gamma_{k_1}(x) \cdots \Gamma_{k_s}(x)\, dx = \int_0^1 (-1)^{\widehat{2^{k_1}x + \cdots + 2^{k_s}x}}\, dx$$

$$= \sum_{j=0}^{2^{k_1}-1} \int_{j/2^{k_1}}^{(j+1)/2^{k_1}} (-1)^{\widehat{j + 2^{k_2}x + \cdots + 2^{k_s}x}}\, dx .$$

Dans l'intégrale on effectue le changement de variable $x = \dfrac{y + j}{2^{k_1}}$, d'où

$$I = \sum_{j=0}^{2^{k_1}-1} \frac{(-1)^j}{2^{k_1}} \int_0^1 (-1)^{\widehat{2^{k_2-k_1}y + \cdots + 2^{k_s-k_1}y}}\, dy$$

$$= \left[\sum_{j=0}^{2^{k_1}-1} (-1)^j\right] \frac{1}{2^{k_1}} \int_0^1 (-1)^{\widehat{2^{k_2-k_1}y + \cdots}}\, dy = 0 .$$

III. Théorème ergodique individuel de Birkhoff.

Avant d'énoncer le théorème de Birkhoff donnons quelques définitions :

Soit X un ensemble. $\mathcal{B}$ désigne une famille de parties de X stable par réunions et intersections dénombrables et par passage au complémentaire ($\mathcal{B}$ est une tribu). μ représente une mesure positive sur X, de masse totale finie.

Soit T une application $X \to X$. On dit que T est mesurable si $T^{-1}\,\mathcal{B} \subseteq \mathcal{B}$. On dit que T conserve la mesure si quel que soit E dans $\mathcal{B}$, on a

$$\mu(T^{-1}\,E) = \mu(E) \quad .$$

Enfin, une transformation T mesurable conservant la mesure est ergodique (ou indécomposable) si tout ensemble mesurable invariant par T a une mesure nulle ou si son complémentaire a une mesure nulle.

THÉORÈME 1 (BIRKHOFF). - Sur $(X, \mathcal{B}, \mu)$ soit T une application $X \to X$, mesurable, conservant la mesure et ergodique.

On suppose que la mesure de X est finie. Si g désigne une fonction sommable $X \to R$, alors

$$\lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} g(T^k x) = \int_X g \, d\mu$$

pour presque tout x de X.

IV. THÉORÈME 2. - Soit $p_1\ p_2 \cdots p_s$ une suite strictement croissante d'entiers. Pour presque tous les nombres x de l'intervalle $(0, 1)$, on a l'égalité

$$\lim_{N\to\infty} \frac{1}{N} \sum_{k=1}^{N} \Gamma_k(x)\, \Gamma_{k+p_1}(x) \cdots \Gamma_{k+p_s}(x) = 0 \quad . \tag{6}$$

En effet soit X l'ensemble des nombres irrationnels dans $(0, 1)$. On définit sur X la tribu $\mathcal{B}$ engendrée par la famille des intervalles de $(0, 1)$. μ sera la mesure de Lebesgue.

Considérons l'application $T : X \to X$ définie par

$$Tx = \underbrace{2x} \quad . \tag{7}$$

On vérifie aisément que si (α, β) appartient à $\mathcal{B}$, alors

$$T^{-1}(\alpha, \beta) = \left(\frac{\alpha}{2}, \frac{\beta}{2}\right) \cup \left(\frac{\alpha + 1}{2}, \frac{\beta + 1}{2}\right)$$

où les deux intervalles $\left(\frac{\alpha}{2}, \frac{\beta}{2}\right)$ et $\left(\frac{\alpha + 1}{2}, \frac{\beta + 1}{2}\right)$ sont disjoints. Il vient alors

$$\mu[T^{-1}(\alpha, \beta)] = \frac{\beta - \alpha}{2} + \frac{(\beta + 1) - (\alpha + 1)}{2} = \beta - \alpha = \mu[\alpha, \beta] \quad .$$

Ainsi T conserve la mesure. Nous admettrons que la transformation T est ergodique. On pourra trouver une démonstration de ce fait dans [4].

Choisissons alors pour fonction g la fonction définie par

$$g(x) = \Gamma_1(x)\ \Gamma_{1+p_1}(x) \cdots \Gamma_{1+p_s}(x) \ . \tag{8}$$

On voit aisément que $\Gamma_1(Tx) = \Gamma_2(x)$ et plus généralement

$$\Gamma_k(T^\ell\ x) = \Gamma_{k+\ell}(x) \quad \text{où} \quad k\ ,\ \ell \in \underset{\sim}{N} \ .$$

Par suite

$$g(T^k\ x) = \Gamma_{1+k}(x)\ \Gamma_{1+p_1+k}(x) \cdots \Gamma_{1+p_s+k}(x) \ .$$

Le théorème de Birkhoff montre alors que

$$\lim_{N\to\infty} \frac{1}{N} \sum_{k=1}^{N} \Gamma_k(x)\ \Gamma_{k+p_1}(x) \cdots \Gamma_{k+p_s}(x) = \int_0^1 \Gamma_1(x)\ \Gamma_{1+p_1}(x) \cdots \Gamma_{1+p_s}(x)\ dx \quad \text{p. p.}$$

$$= 0 \quad \text{p. p.}$$

d'après le lemme 2. Ceci démontre le théorème.

COROLLAIRE 1 (BOREL). - Presque tous les nombres sont simplement normaux.

En effet il suffit de choisir $s = 0$ dans le théorème précédent $(p_0 = 0)$ c'est-à-dire $g(x) = \Gamma_1(x)$.

COROLLAIRE 2 (WIENER) [6]. - Pour presque tous les nombres x de $(0\ ,\ 1)$, la fonction $f(t) = \Gamma_{\hat{t}}(x)$ est pseudo-aléatoire.

En effet dans le théorème précédent on choisit $s = 1$. Si γ désigne la fonction de corrélation, on voit alors que $\gamma(p_1) = 0\ ,\ p_1 = 1\ ,\ 2\ ,\ 3\ ,\ \ldots$

Par ailleurs, il est évident que $\gamma(0) = 1$. Le lemme 1 montre que $\gamma(h)$ est définie par

$$\gamma(h) = \max(0\ ,\ 1 - |h|) \ .$$

C'est bien une fonction non nulle à l'origine, continue et nulle à l'infini. Ceci achève de démontrer le corollaire 2.

Ce corollaire ne nous permet pas de construire un nombre x tel que $\Gamma_{\hat{t}}(x)$ soit pseudo-aléatoire. Cependant dans [2], J. BASS a démontré que si $\varphi(t)$ désigne un polynôme réel

$$\varphi(t) = A_0 + A_1\ t + A_2\ t^2 + \cdots + A_\nu\ t^\nu$$

de degré $\nu \geqslant 2$ et tel que le coefficient A_ν soit irrationnel, alors le nombre x défini par $\Gamma_{\hat{t}}(x) = (-1)^{\widehat{\varphi(t)}}$ donne lieu à une fonction $\Gamma_{\hat{t}}(x)$ pseudo-aléatoire.

Nous dirons que φ est un polynôme W . Démontrons pour conclure le théorème suivant.

THÉORÈME 3. - L'ensemble des nombres x définis par $\Gamma_k(x) = (-1)^{\widehat{\varphi(k)}}$, où φ est un polynôme W , est de mesure nulle.

La démonstration se fait en remarquant que si φ' est un polynôme à coefficients non tous rationnels, alos la suite $u_n = \widehat{\varphi(n)}$ est non seulement équirépartie, mais aussi uniformément équirépartie. On en déduit l'existence d'une suite finie de 0 et de 1 qui n'apparaît pas dans le développement binaire du nombre x défini par $\Gamma_k(x) = (-1)^{\widehat{\varphi(k)}}$. Le nombre x n'est donc pas normal : le théorème 3 en découle.

BIBLIOGRAPHIE

[1] BASS (Jean). - Les fonctions pseudo-aléatoires. - Paris, Gauthier-Villars, 1962 (Mémorial des Sciences mathématiques, 153).

[2] BASS (Jean). - Fonctions pseudo-aléatoires et fonctions de Wiener, C. R. Acad. Sc. Paris, t. 247, 1958, p. 1163-1165.

[3] KAC (Marc). - Statistical independence in probability, analysis and number theory. - Buffalo, Mathematical Association of America, 1959 (The Carus mathematical Monographs, 12).

[4] POSTNIKOV (A. G.). - Arifmetičeskoe modelirovanie slučajnykh processov, Trudy mat. Inst. Stekl., t. 57, 1960, 84 p. ; Modèle arithmétique de processus stochastiques. - Paris, Service de Documentation et d'Information de l'Aéronautique, 1961.

[5] WIENER (Norbert). - Generalized harmonic analysis, Acta Math., t. 55, 1930, p. 117-258.

[6] WIENER (Norbert). - The spectrum of an array and its application to the study of the translation properties of a simple class of arithmetical functions, J. of Math. and Phys., Mass. Inst. Techn., t. 6, 1927, p. 145-157.