Séminaire Delange-Pisot-Poitou. Théorie des nombres

Michel Mendès France

Fonctions de Walsh et fonctions pseudo-aléatoires

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 7, n° 1 (1965-1966), exp. n° 4, p. 1-9

<http://www.numdam.org/item?id=SDPP_1965-1966__7_1_A3_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
7e année, 1965/66, n° 4

13 décembre 1965

FONCTIONS DE WALSH ET FONCTIONS PSEUDO-ALÉATOIRES

par Michel MENDÈS FRANCE

1. Fonctions pseudo-aléatoires.

Nous dirons, avec J. BASS [1], qu'une fonction f à valeurs complexes, définie sur les entiers $\underset{\sim}{Z}$, est pseudo-aléatoire si la fonction de corrélation

$$\gamma(p) = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \bar{f}(k)\, f(k+p)$$

(a) est définie pour tout entier p,

(b) $\gamma(0) > 0$,

(c) $\lim_{p\to\infty} \gamma(p) = 0$.

Il est facile de construire des fonctions pseudo-aléatoires au sens de BASS. Des exemples en sont donnés dans [1] et [5]. Par ailleurs, on peut montrer que presque toutes les applications de l'ensemble des entiers $\underset{\sim}{Z}$ sur la circonférence $|z| = 1$ du plan complexe sont pseudo-aléatoires.

Dans [2], J.-P. BERTRANDIAS a élargi la classe des fonctions pseudo-aléatoires en remplaçant la condition (c) par la condition plus faible :

$$(c') \qquad \lim_{p\to+\infty} \frac{1}{p} \sum_{q=1}^{p} |\gamma(q)|^2 = 0 \quad .$$

Dans tout ce qui suit, on entendra par "fonction pseudo-aléatoire", une fonction qui satisfait aux trois conditions (a), (b), et (c').

Notre but est de montrer comment, grâce à l'ensemble de Walsh, on peut construire une fonction pseudo-aléatoire qui ne vérifie pas la condition (c). Au paragraphe 8, on applique certains des résultats obtenus à l'équirépartition modulo 1.

Remarque. - On sait qu'une fonction de corrélation admet la représentation :

$$\gamma(p) = \int_0^1 \exp(2i\pi px)\, d\alpha(x) \quad , \qquad p \in \underset{\sim}{Z} \quad ,$$

où $d\alpha$ désigne une mesure positive bornée. La condition (c') implique que la mesure soit continue. Si, de plus, la condition (c) n'a pas lieu, on sait qu'alors la mesure $d\alpha$ est non absolument continue.

2. L'ensemble de Walsh et la fonction de Walsh.

Dans tout l'exposé, g désigne un nombre entier supérieur ou égal à 2. Soit $G = (\underset{\sim}{Z}/g\underset{\sim}{Z})^{\underset{\sim}{N}}$ le groupe abélien des suites d'entiers modulo g, muni de la topologie discrète. Soit $\varepsilon = (\varepsilon_1 , \varepsilon_2 , \ldots)$ un élément du groupe G. Il est clair que l'application

$$\varepsilon \longrightarrow c_n(\varepsilon) = \exp \frac{2i\pi}{g} \varepsilon_n$$

est un caractère du groupe. Il s'ensuit que si $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_s$ est une suite finie d'entiers positifs, l'application $c_{p_1,p_2,\ldots,p_s} = c_{p_1} c_{p_2} \ldots c_{p_s}$ est un caractère. On montre que réciproquement, tous les caractères c de $(\underset{\sim}{Z}/g\underset{\sim}{Z})^{\underset{\sim}{N}}$ sont de cette forme (produit fini de c_p) [3].

Désignons par $\tilde{\alpha}$ le résidu modulo g du nombre réel α. A chaque élément $\varepsilon = (\varepsilon_1 , \varepsilon_2 , \ldots)$ de $(\underset{\sim}{Z}/g\underset{\sim}{Z})^{\underset{\sim}{N}}$, on peut faire correspondre un nombre x de l'intervalle $[0 , 1)$ par l'application

$$\varepsilon \longrightarrow x = A\varepsilon = \sum_{n=1}^{\infty} \frac{\tilde{\varepsilon}_n}{g^n} .$$

En dehors d'un ensemble dénombrable de points $\frac{a}{g^p}$ (a , p entiers) de l'intervalle unité, l'application A est inversible. Si x est de la forme $\frac{a}{g^p}$, c'est-à-dire si x admet deux représentations g-adiques, on conviendra de ne conserver que celle qui contient un nombre infini de décimales g-adiques non nulles. Dans ces conditions, l'application A est une bijection de $(\underset{\sim}{Z}/g\underset{\sim}{Z})^{\underset{\sim}{N}}$ sur $]0 , 1]$.

On appelle suite de Rademacher (dans la base g) associée au nombre $x \in]0 , 1]$, la suite infinie

$$c_1(A^{-1} x) , c_2(A^{-1} x) , \ldots , c_n(A^{-1} x) , \ldots .$$

On appelle ensemble de Walsh (dans la base g), l'ensemble des applications

$$x \longrightarrow c(A^{-1} x) ,$$

où c est un caractère du groupe $(\underset{\sim}{Z}/g\underset{\sim}{Z})^{\underset{\sim}{N}}$.

Pour simplifier l'écriture, on pose $r_n(x) = c_n(A^{-1} x)$ et $\omega(x) = c(A^{-1} x)$. On prolonge les fonctions ω par périodicité de sorte que $\omega(x + 1) = \omega(x)$.

On peut munir l'ensemble de Walsh d'un ordre de la façon suivante : on pose $\omega_0 = 1$, et si n est un entier positif, $\omega_n = r_{p_1} r_{p_2} \ldots r_{p_s}$ où

$$gn = g^{p_1} + g^{p_2} + \dots + g^{p_s} \qquad (p_j \in \underset{\sim}{N},\ 1 \leqslant p_1 \leqslant p_2 \leqslant \dots \leqslant p_s,\ p_j < p_{j+g-1}) .$$

Par définition, la fonction de Walsh associée au point x est la valeur, au point x, de l'ensemble ordonné de Walsh, l'ordre étant celui précédemment défini. En d'autres termes, la fonction de Walsh associée au point x est l'application

$$n \longrightarrow \omega_n(x) .$$

On prolonge la fonction aux entiers négatifs en posant $\omega_n = \omega_{|n|}$.

THÉORÈME. - Soit x un nombre réel arbitraire (d'après les conventions faites, x admet toujours un développement g-adique infini). La fonction de Walsh associée à x est une fonction pseudo-aléatoire qui ne vérifie pas la condition (c).

COROLLAIRE. - Soit $q(n)$ la somme des chiffres de l'entier n écrit dans le système à base g . La fonction

$$n \longrightarrow \exp\{\frac{2i\pi}{g}\, q(|n|)\}$$

est pseudo-aléatoire, et elle ne vérifie pas la condition (c).

Le corollaire est dû à MAHLER [4]. La démonstration du théorème généralise sa méthode.

3. Démonstration du théorème.

Dans le système à base g , tout nombre entier non négatif n s'écrit sous la forme suivante :

$$n = \sum_{p=0}^{\infty} e_p(n)\, g^p ,$$

où $e_p(n)$ prend ses valeurs parmi les nombres 0 , 1 , ... , $g-1$. (La série précédente ne contient qu'un nombre fini de termes non nuls.) Soit $s = (s_n)_{n \geqslant 0}$ une suite infinie d'entiers rationnels. On pose

$$q_s(n) = \sum_{p=0}^{\infty} e_p(n)\, s_p$$

et

$$f_s(n) = \exp(\frac{2i\pi}{g}\, q_s(|n|)) , \qquad n \in \underset{\sim}{Z} .$$

LEMME 1. - Soit $s = (s_n)_{n \geqslant 0}$ une suite infinie d'entiers non tous nuls modulo g à partir d'un certain rang. On définit le nombre réel :

$$x = \sum_{n=0}^{\infty} \frac{\tilde{s}_n}{g^{n+1}} \quad .$$

L'identité suivante

$$f_s(n) = \omega_n(x) \qquad n = 0 \ , \ 1 \ , \ 2 \ , \ \ldots$$

a alors lieu.

La démonstration est évidente ([6], p. 249).

Le théorème peut alors s'énoncer sous la forme suivante :

Si la suite $s = (s_n)_{n\geqslant 0}$ contient une infinité de nombres entiers non divisibles par g, alors la fonction f_s est pseudo-aléatoire, et elle ne satisfait pas à la condition (c).

4. Existence de la corrélation.

On définit l'opérateur T de translation

$$T\{(s_n)_{n\geqslant 0}\} = \{s_{n+1}\}_{n\geqslant 0} \ ,$$

et ses puissances successives T^2 , T^3 , ...

LEMME 2. - Quelle que soit la suite d'entiers $s = (s_n)_{n\geqslant 0}$, la corrélation

$$\gamma_s(k) = \lim_{n\to\infty} \frac{1}{n} \sum_{\ell=0}^{n-1} \bar{f}_s(\ell)\, f_s(\ell + k) \ , \qquad k \in \mathbb{Z}$$

existe. De plus, si a désigne un des g entiers 0 , 1 , ... , $g-1$, la corrélation vérifie la formule de récurrence

$$\begin{cases} \gamma_s(1) = (1 - \frac{1}{g}) \sum_{k=0}^{\infty} \frac{1}{g^k} \exp\{\frac{2i\pi}{g}(s_k - s_{k-1} - \ldots - s_0)\} \\ \gamma_s(gk + a) = [\frac{g-a}{g} \gamma_{Ts}(k) + \frac{a}{g} \gamma_{Ts}(k+1)] \exp(\frac{2i\pi}{g} a s_0) \quad . \end{cases}$$

La méthode employée pour démontrer ce lemme est calquée sur celle qu'emploie MAHLER dans [4]. On se sert essentiellement de la relation de récurrence

$$f_s(gn + a) = f_{Ts}(n) \exp \frac{2i\pi}{g} a s_0 \ , \qquad a = 0 \ , \ 1 \ , \ \ldots \ , \ g-1 \quad .$$

5. La condition (c) n'est pas satisfaite.

Etablissons le lemme suivant :

LEMME 3. - Si la suite s contient une infinité de termes non divisibles par g, alors $\gamma_s(\ell)$ ne peut pas tendre vers 0 lorsque ℓ croît indéfiniment.

Cela se démontre facilement grâce au lemme 2. En effet :

$$\gamma_s(g^\nu) = \gamma_{T^\nu s}(1) \tag{1}$$
$$= (1 - \frac{1}{g}) \sum_{k=0}^{\infty} \frac{1}{g^k} \exp\{\frac{2i\pi}{g}(s_{k+\nu} - s_{k+\nu-1} - \dots - s_\nu)\} \quad .$$

Si g est un entier supérieur ou égal à 3, les inégalités suivantes ont lieu :

$$|\gamma_s(g^\nu)| \geqslant (1 - \frac{1}{g})(1 - \sum_{k=1}^{\infty} \frac{1}{g^k}) = \frac{g-2}{g} > 0 \quad .$$

Cela démontre le lemme.

Si au contraire g est égal à 2, on emploie l'argument suivant :
Supposons que l'on ait :

$$\lim_{\nu\to\infty} \gamma_s(2^\nu) = 0 \quad .$$

Cela implique que, dans la formule (1), le deuxième et le troisième terme de la somme du second membre aient un même signe pour tout entier ν suffisamment grand. Il existe donc un nombre ν_0 tel que

$$\exp i\pi(s_{\nu+1} - s_\nu) = \exp i\pi(s_{\nu+2} - s_{\nu+1} - s_\nu) , \qquad \nu = \nu_0 + 1 , \nu_0 + 2 , \dots \quad .$$

Donc $s_{\nu+2}$ doit être entier pair pour tout $\nu > \nu_0$. Cela contredit l'hypothèse du lemme 3. Il est donc impossible que $\gamma_s(2^\nu)$ tende vers 0.

6. La condition (c') est satisfaite.

Par une technique très voisine de celle employée pour établir le lemme 2, on démontre le lemme suivant :

LEMME 4. - Quelle que soit la suite s d'entiers, la corrélation

$$\Gamma_s(k) = \lim_{n\to\infty} \frac{1}{n} \sum_{\ell=0}^{n-1} \overline{\gamma_s(\ell)}\, \gamma_s(\ell + k) , \qquad k \in \mathbb{Z}$$

existe. De plus, les deux égalités suivantes :

$$\begin{cases} \Gamma_s(gk) = \dfrac{2g^2+1}{3g^2}\Gamma_{Ts}(k) + \dfrac{g^2-1}{6g^2}[\Gamma_{Ts}(k-1) + \Gamma_{Ts}(k+1)] \\ \Gamma_s(gk+1) = [\dfrac{2(g^2-1)}{3g^2}\Gamma_{Ts}(k) + \dfrac{(g-1)(g-2)}{6g^2}\Gamma_{Ts}(k-1) + \dfrac{(g+1)(g+2)}{6g^2}\Gamma_{Ts}(k+1)]\exp\dfrac{2i\pi}{g}s_0 \end{cases}$$

ont lieu.

En prenant $k = 0$ dans le lemme précédent, et en désignant par $M(s)$ la matrice

$$\frac{1}{6g^2}\begin{pmatrix} 4g^2+2 & g^2-1 & g^2-1 \\ 4(g^2-1)\exp\dfrac{2i\pi}{g}s_0 & (g+1)(g+2)\exp\dfrac{2i\pi}{g}s_0 & (g-1)(g-2)\exp\dfrac{2i\pi}{g}s_0 \\ 4(g^2-1)\exp\dfrac{-2i\pi}{g}s_0 & (g-1)(g-2)\exp\dfrac{-2i\pi}{g}s_0 & (g+1)(g+2)\exp\dfrac{-2i\pi}{g}s_0 \end{pmatrix}$$

on obtient le résultat suivant :

COROLLAIRE. - La corrélation Γ_s vérifie l'égalité suivante :

$$\begin{pmatrix} \Gamma_s(0) \\ \Gamma_s(1) \\ \Gamma_s(-1) \end{pmatrix} = M(s)\begin{pmatrix} \Gamma_{Ts}(0) \\ \Gamma_{Ts}(1) \\ \Gamma_{Ts}(-1) \end{pmatrix} .$$

Grâce à ce résultat, nous allons montrer que $\Gamma_s(0) = 0$, et cela établira complètement le théorème.

Désignons par $\|\ldots\|$ la norme définie sur l'espace vectoriel des matrices d'ordre 3 par

$$\|(a_{ij})\| = \sup_i \sum_j |a_{ij}| .$$

Si A et B sont deux matrices, on vérifie alors sans peine que l'on a : $\|AB\| \leq \|A\|\cdot\|B\|$.

Par ailleurs, l'égalité

$$\begin{pmatrix} \Gamma_s(0) \\ \Gamma_s(1) \\ \Gamma_s(-1) \end{pmatrix} = M(s)\,M(Ts)\,\ldots\,M(T^{\nu-1}s)\begin{pmatrix} \Gamma_{T^\nu s}(0) \\ \Gamma_{T^\nu s}(1) \\ \Gamma_{T^\nu s}(-1) \end{pmatrix} ,$$

(conséquence immédiate du corollaire), et l'inégalité

$$0 \leqslant |\Gamma_{T^\nu s}(1)| \leqslant \Gamma_{T^\nu s}(0) \leqslant 1$$

(conséquence de l'inégalité de Schwarz), montrent que les deux inégalités suivantes

$$(2) \qquad \begin{cases} 0 \leqslant \Gamma_s(0) \leqslant \prod_{m=0}^{\infty} \|M(T^{2m}\, s)\; M(T^{2m+1}\, s)\| \\ 0 \leqslant \Gamma_s(0) \leqslant \prod_{m=0}^{\infty} \|M(T^{2m+1}\, s)\; M(T^{2m+2}\, s)\| \end{cases}$$

sont vraies.

Montrons que, si s contient une infinité de termes non nuls modulo g, l'un au moins des produits infinis précédents est nul.

LEMME 5. - Soient $A = (\alpha_{ij}\ \varepsilon_i)$ et $B = (\beta_{ij}\ \varepsilon'_i)$ $(i, j = 1, 2, 3)$ deux matrices telles que

(i) $$\alpha_{ij} \geqslant 0\ ,\quad \beta_{ij} \geqslant 0\ ,\quad \sum_j \alpha_{ij} = \sum_j \beta_{ij} = 1$$

(ii) $$|\varepsilon_i| = 1\ ,\quad |\varepsilon'_i| = 1\ ,\ \text{et}\ \ \varepsilon'_i \neq \varepsilon'_j\ \ \text{pour}\ \ i \neq j\ .$$

Alors, $\|AB\| < 1$.

La démonstration est évidente.

Dans le lemme 5, on pose $A = M(T^\nu\, s)$ et $B = M(T^{\nu+1}\, s)$. Les conditions (i) et (ii) sont satisfaites pourvu que $s_{\nu+1}$ ne soit pas divisible par g. Ainsi, chaque fois que ν est telle que $s_{\nu+1} \not\equiv 0 \pmod g$, l'inégalité

$$R_\nu = \|M(T^\nu\, s)\; M(T^{\nu+1}\, s)\| < 1$$

a lieu. Le nombre R_ν ne dépend que de s_ν et $s_{\nu+1}$ modulo g. Ainsi lorsque ν parcourt les entiers positifs, R_ν prend au plus g^2 valeurs. Il existe donc un nombre $\delta < 1$ tel que

$$s_{\nu+1} \not\equiv 0 \pmod g \implies R_\nu \leqslant \delta\ .$$

Si alors, par hypothèse, on admet qu'il existe une infinité de $s_{\nu+1} \not\equiv 0 \pmod g$, on voit que l'un des deux produits infinis des formules (2) est nul. Ainsi se trouve démontré le théorème.

7. Démonstration du corollaire du théorème.

Dans le théorème, on choisit $x = 1/g - 1$.

8. Application à l'équirépartition modulo 1 .

Au paragraphe 3, on a supposé que s était une suite infinie d'entiers rationnels. On peut généraliser les résultats en remplaçant la suite s par une suite infinie σ de nombres réels. On pose comme précédemment

$$q_\sigma(n) = \sum_{p=0}^{\infty} e_p(n)\, \sigma_p$$

et $\varphi_\sigma = \exp 2i\pi q_\sigma$. On montre alors que, si $\sigma = \alpha s$ (α irrationnel, $s \in \{(0) , (1)\}^{\underset{\sim}{N}}$), φ_σ est pseudo-aléatoire si, et seulement si, s contient une infinité de termes non nuls. Sachant qu'une fonction pseudo-aléatoire a une moyenne nulle ([1], [2]), on en déduit que, pour α irrationnel, on a

$$\lim_{n\to\infty} \frac{1}{n} \sum_{\ell=0}^{n-1} \exp 2i\pi k\alpha q_s(\ell) = 0 \qquad k = 1 , 2 , \ldots .$$

Le critère de Weyl montre ainsi que la suite $u_n = \alpha q_s(n)$ est équirépartie modulo 1 . En particulier, on obtient le résultat suivant :

COROLLAIRE. - Soit q(n) la somme des chiffres de l'entier n écrit dans le système à base g . La suite $u_n = \alpha q(n)$ est équirépartie modulo 1 si, et seulement si, α est irrationnel.

Cela fournit un exemple de plus de suites $(u_n) = (\alpha\lambda(n))$ ($\lambda(n) \in \underset{\sim}{Z}$) qui sont équiréparties modulo 1 si, et seulement si, α est irrationnel. (On sait que cette propriété a lieu par exemple si $\lambda(n) = h(n)$ ou bien $\lambda(n) = h(p_n)$, h étant un polynôme réel non constant à coefficients entiers et p_n désignant le n-ième nombre premier.)

BIBLIOGRAPHIE

[1] BASS (Jean). - Suites uniformément denses, moyennes trigonométriques, fonctions pseudo-aléatoires, Bull. Soc. math. France, t. 87, 1959, p. 1-64.

[2] BERTRANDIAS (Jean-Paul). - Suites pseudo-aléatoires et critère d'équirépartition modulo 1 , Comp. Math., t. 16, 1964, p. 23-28.

[3] FINE (N. J.). - On the Walsh functions, Trans. Amer. math. Soc., t. 65, 1949, p. 372-414.

[4] MAHLER (Kurt). - The spectrum of an array and its applications of the study of the translation properties of a simple class of mathematical functions, II : On the translation properties of a simple class of mathematical functions, J. of Math. and Phys., t. 6, 1927, p. 158-163.

[5] MENDES FRANCE (Michel). - Nombres normaux et fonctions pseudo-aléatoires, Ann. Inst. Fourier, Grenoble, t. 13, 1963, n° 2, p. 91-104.

[6] VILENKIN (N. Ja.). - Supplement to "Theory of orthogonal series", Amer. math. Soc. Transl., t. 17, 1961, p. 219-250.

[7] WIENER (Norbert). - The spectrum of an array and its applications of the study of the translation properties of a simple class of mathematical functions, I : The spectrum of an array, J. of Math. and Phys., t. 6, 1927, p. 145-157.