Séminaire Dubreil.
Algèbre et théorie
des nombres

Jean Bass

Fonctions de corrélation et suites équiréparties

Séminaire Dubreil. Algèbre et théorie des nombres, tome 12, n° 2 (1958-1959), exp. n° 27, p. 1-9

<http://www.numdam.org/item?id=SD_1958-1959__12_2_A10_0>

Faculté des Sciences de Paris
-:-:-:-
Séminaire P. DUBREIL
M.-L. DUBREIL-JACOTIN et C. PISOT
(ALGÈBRE et THÉORIE DES NOMBRES)
Année 1958/59
-:-:-:-

11 mai 1959

FONCTIONS DE CORRÉLATION ET SUITES ÉQUIRÉPARTIES

par Jean BASS

Les problèmes dont il va être question peuvent être envisagés du point de vue de l'arithmétique, de l'analyse, et du calcul des probabilités : leur origine est hydrodynamique : la mécanique des fluides turbulente utilise des fonctions dont on ne connaissait pas jusqu'ici de représentations, sauf sous la forme indirecte de fonctions aléatoires. Ces fonctions, que je désignerai sous le nom de fonctions pseudo-aléatoires, peuvent se rattacher à la notion de suite équirépartie, et réciproquement, leur étude simplifie celle des suites équiréparties.

Soit $f(t)$ une fonction complexe bornée, nulle pour $t < 0$, intégrable au sens de Riemann, satisfaisant aux conditions suivantes :

1) $$m = \lim_{T \to \infty} \frac{1}{T} \int_0^T f(t)\, dt \quad \text{existe ;}$$

2) $$\gamma(h) = \lim_{T \to \infty} \frac{1}{T} \int_0^T \overline{f(t)}\, f(t+h)\, dt \quad \text{existe, pour tout } h > 0 ,$$

est une fonction continue de h, et a une valeur positive pour $h = 0$.

DÉFINITION. - Si $m = 0$, et si $\gamma(h)$ tend vers 0 lorsque $h \to \infty$, on dit que $f(t)$ est pseudo-aléatoire. $\gamma(h)$ s'appelle fonction de corrélation de $f(t)$. On vérifie que $\gamma(h)$ est définie pour tout h, et que $\gamma(-h) = \overline{\gamma(h)}$.

Considérons pour commencer une fonction $f(t)$ non nécessairement pseudo-aléatoire et étudions les relations générales qui existent entre m et $\gamma(h)$.

Au lieu de $\gamma(h)$, introduisons plutôt la fonction

$$g(h_1, h_2) = \lim_{T \to \infty} \frac{1}{T} \int_0^T \overline{f}(t + h_1)\, f(t + h_2)\, dt$$

Prenons sa moyenne dans le carré C :

$$0 < h_1 < A \quad , \quad 0 < h_2 < A$$

$$\frac{1}{A^2} \int_0 g(h_1 , h_2)\, dh_1\, dh_2 = \lim_{T \longrightarrow \infty} \frac{1}{T} \int_0^T dt \left| \frac{1}{A} \int_0^A f(t + h)\, dh \right|^2$$

$g(h_1 , h_2)$ est une fonction complexe. Mais <u>sa moyenne</u> est une fonction réelle <u>non négative.</u>

La changement de variable $t + h_1 = t'$ montre d'ailleurs tout de suite que

$$g(h_1 , h_2) = \gamma(h_2 - h_1) .$$

On voit ainsi que

$$\frac{1}{A^2} \int_c \gamma(h_2 - h_1)\, dh_1\, dh_2 = \frac{1}{A} \int_0^A R\gamma(h) \left(1 - \frac{h}{A}\right) dh \geqslant 0 .$$

Le résultat est valable à la limite lorsque $A \longrightarrow \infty$, mais la limite du premier membre n'est pas en général égale à

$$\lim_{T \longrightarrow \infty} \frac{1}{T} \int_0^T dt \left| \lim_{A \longrightarrow \infty} \frac{1}{A} \int_0^A f(t + h)\, dh \right|^2 = |m|^2 ,$$

comme je le montrerai plus loin sur un exemple.

On peut cependant améliorer le résultat précédent en posant

$$f(t) = m + f_1(t) .$$

$f_1(t)$ a une moyenne nulle. On a alors

$$g(h_1 , h_2) = \lim_{T \longrightarrow \infty} \frac{1}{T} \int_0^T [\bar{m} + \bar{f}_1(t + h_1)][m + f_1(t + h_2)]\, dt =$$

$$= \lim_{T \longrightarrow \infty} \frac{1}{T} \int_0^T \bar{f}_1(t + h_1) f_1(t + h_2)\, dt + |m|^2 .$$

Le premier terme a pour moyenne, dans le carré C , une quantité non négative.

Donc

$$\boxed{\frac{1}{A^2}\int_C \gamma(h_2 - h_1)\, dh_1\, dh_2 \geqslant |m|^2}$$

Ce résultat est valable éventuellement à la limite lorsque $A \longrightarrow \infty$. Il n'y a pas en général égalité.

Considérons en particulier une fonction $f(t)$ de la forme

$$f(t) = e^{2i\pi\varphi(n)} \quad \text{si} \quad n < t < n+1 \quad , \quad n \ \text{entier},$$

soit

$$f(t) = e^{2i\pi\varphi[E(t)]} \quad , \qquad t > 0 \, .$$

On démontre facilement le theorème suivant.

THÉORÈME. - Si la fonction de corrélation de $f(t)$ existe pour h entier, elle existe pour tout h , est continue, et varie linéairement lorsque $p < h < p+1$, p entier non négatif.

Ce théorème a pour conséquence le théorème suivant, qui joue un rôle central dans la suite :

THÉORÈME. - Si, pour tout entier $p \geqslant 1$ (ou supérieur à un nombre positif fixé) ,

$$\gamma(p) = 0 \ , \quad \text{alors} \quad m = 0 \ .$$

En effet, $\gamma(h)$ est alors nul pour tout $h \geqslant 1$, donc la moyenne de $\gamma(h_2 - h_1)$ dans le carré C tend vers 0 lorsque $A \longrightarrow \infty$. $|m|$, nombre non négatif arbitrairement petit, est nul.

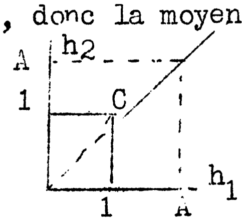

fig 1

REMARQUE 1. - On peut retrouver ce résultat en étudiant directement la moyenne de $\gamma(h)$ par rapport à h . $\gamma(h)$ est une fonction du type positif. On peut donc (théorème de Bochner) le représenter par une intégrale de Fourier-Stieltjes

$$\gamma(h) = \int_{-\infty}^{\infty} e^{ih\omega}\, d\sigma(\omega) \quad ,$$

où $\sigma(\omega)$ est une fonction réelle telle que $\int_{-\infty}^{\infty} |d\sigma(\omega)| < \infty$.

On démontre alors que

$$\lim_{A \to \infty} \frac{1}{A} \int_0^A \gamma(h)\, dh$$

existe et a pour valeur le saut réel non négatif de la fonction spectrale $\sigma(\omega)$ à l'origine. Le résultat précédemment utilisé était légèrement différent. Il avait comme conséquence que, pour tout $A > 0$,

$$\frac{1}{A} \int_0^A R\, \gamma(h)\, dh \geqslant 0 .$$

REMARQUE 2. - L'inégalité fondamentale se généralise facilement. Considérons la fonction

$$g(h_1 , h_2 , \dots , h_{2k}) = \lim_{T \to \infty} \frac{1}{T} \int_0^T \bar{f}(t+h_1) \dots \bar{f}(t+h_k)\, f(t+h_{k+1}) \dots f(t+h_{2n})dt.$$

Si les moyennes utilisées existent, on a, pour tout A fixé,

$$\mathcal{M}_{2k} (g , A) = \frac{1}{A^{2k}} \int_{C_{2k}} g(h_i)\, dh = \lim_{T \to \infty} \frac{1}{T} \int_0^T |F(t)|^{2k}\, dt ,$$

où C_{2k} est l'hypercube $(0 , A)$ à $2k$ dimensions, et où

$$F(t) = \frac{1}{A} \int_0^A f(t + h)\, dh$$

La moyenne $\mathcal{M}_{2k}(g , A)$ de g dans C_{2k} est donc le "moment temporel" d'ordre $2k$ de la fonction positive $|F(t)|$. Les moments $\mathcal{M}_{2k}$ vérifient des <u>inégalités de convexité</u> classiques. On a en effet, d'après l'inégalité de Schwarz,

$$\mathcal{M}_{(k+\ell)} \leq \sqrt{\mathcal{M}_{2k}\, \mathcal{M}_{2\ell}}$$

$\log \mathcal{M}_k$, considéré comme une fonction de k , est convexe.

Lorsque $f(t) = e^{2i\pi \varphi[E(t)]}$, on a $\mathcal{M}_0 = 1$, $0 \leq \mathcal{M}_k \leq 1$.

En fonction de k , $\log \mathcal{M}_k$ est représenté par la courbe de la figure 2.

Si en particulier $\mathcal{M}_2 = 0$, on a $\log \mathcal{M}_2 = -\infty$. La convexité entraîne que

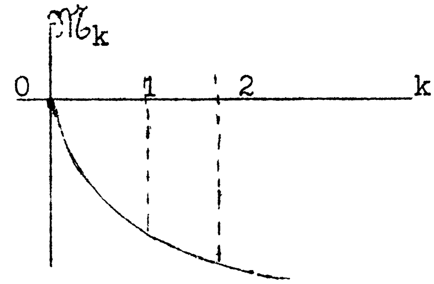

fig. 2

tous les moments sont nuls, et en particulier $\mathcal{M}_1$, d'où il résulte que $m = 0$.

Revenons maintenant à la fonction

$$f(t) = e^{2i\pi \varphi[E(t)]}$$

et exprimons sa moyenne et sa fonction de corrélation.

On a d'abord

$$m = \lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N} e^{2i\pi \varphi(n)}$$

D'autre part les valeurs de $\gamma(h)$ se déduisent de celles de $\gamma(p)$, p entier. Or

$$\gamma(p) = \lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N} e^{2i\pi [\varphi(n+p) - \varphi(n)]}$$

On en déduit que :

THÉORÈME. - <u>Si</u>

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N} e^{2i\pi [\varphi(n+p) - \varphi(n)]} = 0$$

<u>pour tout entier</u> $p \geqslant 1$ (<u>ou</u> $\geqslant p_0$, $p_0 > 0$ <u>arbitraire</u>), <u>alors</u>

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N} e^{2i\pi \varphi(n)} = 0 .$$

Ce résultat, utilisé par H. WEYL, puis généralisé par VAN DER CORPUT, est en relation intime avec la théorie des suites équiréparties. On sait en effet que la condition nécessaire et suffisante pour qu'une suite réelle $\varphi(n)$ soit équirépartie mod 1 est que, quel que soit l'entier ℓ non nul,

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N} e^{2i\pi \ell \varphi(n)} = 0 ,$$

c'est-à-dire que la suite ordonnée $e^{2i\pi \ell \varphi(n)}$ converge vers 0 au sens de CESARO. Ce théorème est d'ailleurs une conséquence du théorème plus général suivant lequel, pour que la suite $\varphi(n)$ soit équirépartie mod 1, il faut et il suffit que, quelle que soit la fonction $\mu(x)$ bornée et intégrable au sens de Riemann, périodique de période 1,

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N} \mu[\varphi(n)] = \int_0^1 \mu(x)\, dx$$

En remplaçant $\varphi(n)$ par $\ell\varphi(n)$, on voit que, <u>pour que</u> $\varphi(n)$ <u>soit équirépartie mod. 1, il faut et il suffit que</u> $\varphi(n+p) - \varphi(n)$ <u>le soit pour tout entier</u> $p \geqslant 1$. C'est le théorème de Van Der Corput.

Ce théorème permet effectivement de construire des suites équiréparties, et en même temps des fonctions pseudo-aléatoires.

On connaît en effet des cas particuliers très simples de suites équiréparties.

<u>Si</u> A <u>est irrationnel, la suite</u> An <u>est équirépartie mod. 1.</u> Car

$$\frac{1}{N} \sum_{n=0}^{N} e^{2i\pi\ell An} = \frac{e^{i\pi\ell A(2N+1)} - e^{-i\pi\ell A}}{2iN \sin \pi\ell A}$$

et cette quantité tend vers 0 avec $\frac{1}{N}$.

Si A est rationnel, il existe des entiers ℓ tels que $e^{2i\pi\ell An} = 1$ pour tout n, et le théorème de Weyl ne s'applique pas.

Si maintenant $\varphi(t)$ est un polynôme du second degré $At^2 + Bt + C$,

on a

$$\varphi(n+p) - \varphi(n) = 2Anp + Ap^2 + Bp \quad .$$

Pour chaque $p \geqslant 1$, la fonction de corrélation de $e^{2i\pi\varphi[E(t)]}$ s'annule.

Donc la fonction $e^{2i\pi\varphi[E(t)]}$ est pseudo-aléatoire, et $\varphi(n)$ est équirépartie mod 1.

La méthode se généralise aisément et permet de démontrer que, <u>si</u> $\varphi(t)$ <u>est un polynôme dont le terme de plus haut degré a un coefficient irrationnel, la suite</u> $\varphi(n)$ <u>est équirépartie mod 1</u>. C'est le théorème de Weyl.

Ce théorème peut être légèrement généralisé. <u>Pour que le polynôme</u> $\varphi(n)$ <u>soit équiréparti mod 1, il faut et il suffit que l'un de ses coefficients, autre que le terme constant, soit irrationnel</u>. Corrélativement, pour que la fonction $e^{2i\pi\varphi[E(t)]}$ soit pseudo-aléatoire, il faut et il suffit que l'un des coefficients du polynôme $\varphi(t)$, autre que celui du terme en t et le terme constant, soit irrationnel.

Si en effet tous les coefficients sont rationnels, $e^{2i\pi\varphi[E(t)]}$ est une fonction périodique, donc non pseudo-aléatoire. Dans le cas contraire, on décompose $e^{2i\pi\varphi[E(t)]}$ en produit d'une fonction pseudo-aléatoire et d'une fonction périodique, qui n'a pas d'influence sur la fonction de corrélation.

Pour toutes ces fonctions, la fonction de corrélation est égale à $1 - |h|$ pour $|h| \leq 1$, à 0 pour $|h| \geq 1$.

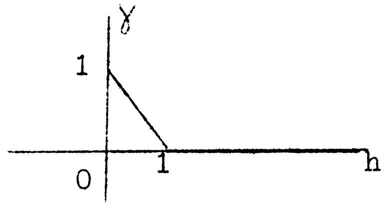

fig. 3

Si l'on considère la suite An^{α}, $0 < \alpha < 1$, on peut démontrer qu'elle est équirépartie mod 1, mais la méthode des fonctions de corrélation ne s'applique pas. Car, pour la fonction

$$f(t) = e^{2i\pi An^{\alpha}}, \quad n < t < n+1$$

On a

$$\gamma(p) = \lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N} e^{2i\pi A[(n+p)^{\alpha} - n^{\alpha}]} = \lim_{N \to \infty} \sum_{n=0}^{N} e^{2i\pi A[\alpha pn^{\alpha-1} + \ldots]}$$

Le crochet tend vers 0 avec $\frac{1}{N}$, donc $\gamma(p) = 1$ et $\gamma(h) = 1$. $\gamma(h)$ a pour moyenne 1, alors que $m = 0$. On a là un exemple de fonction $f(t)$ pour laquelle la moyenne de $\gamma(h)$ est strictement supérieure à $|m|^2$.

VAN DER CORPUT a démontré que la suite An^{α} est équirépartie en utilisant l'inégalité.

$$\left| \frac{e^{iu} - e^{iv}}{u - v} - ie^{iv} \right| < \frac{1}{2} |u - v|, \quad \text{avec} \quad u = (n+1)^{\alpha}; \quad v = n^{\alpha}.$$

Le théorème fondamental permet ensuite d'étendre le résultat à n^{α}, $\alpha > 1$.

La méthode des fonctions de corrélation peut-elle servir à démontrer des résultats nouveaux ? Son but était de construire des fonctions pseudo-aléatoires, et les fonctions obtenues à partir de polynômes $\varphi(t)$ semblent constituer une classe intéressante. On peut d'ailleurs largement la généraliser sans cesser de faire appel à des polynômes. Examinons maintenant comment se présente le problème lorsque $\varphi(t)$ est une fonction à croissance plus rapide, par exemple $\varphi(t) = \lambda\theta^t$, $\theta > 1$.

Formons un moment quelconque de la fonction égale à

$$f(t, \lambda) = e^{2i\pi\lambda\theta^n} \quad \text{si} \quad n < t < n+1 .$$

Il s'agit de la moyenne du produit

$$f^{m_1}(t + h_1) \dots f^{m_k}(t + h_k) ,$$

Si $h_1, h_2, \dots, h_k$ sont des entiers $p_1, p_2, \dots, p_k$, on obtient

$$\lim_{N \to \infty} \frac{1}{N} \sum e^{2i\pi\lambda[m_1\theta^{n+p_1} + \dots + m_k\theta^{n+p_k}]} = \lim_{N \to \infty} \frac{1}{N} \sum e^{2i\pi\lambda\psi(\theta)\theta^n}$$

où

$$\psi(\theta) = m_1\theta^{p_1} + \dots + m_k\theta^{p_k} .$$

Tout moment de $f(t, \lambda)$ est donc moyenne ordinaire d'une fonction $f[t, \lambda\psi(\theta)]$ de forme analogue, où λ est remplacé par $\lambda\psi(\theta)$.

Si en particulier on prend tous les m égaux à ± 1, les coefficients du polynôme $\psi(\theta)$ sont tous égaux à 1, -1 ou 0.

La fonction

$$g(h_1, \dots, h_k) = \lim_{T \to \infty} \frac{1}{T}\int_0^T f(t + h_1) \dots f(t + h_k)\, dt$$

(dans laquelle certains des f peuvent être remplacés par leurs conjugués) est le "<u>moment multi-linéaire</u>" temporel de la fonction $f(t, \lambda)$.

Si les h_i sont des nombres entiers p_i, on voit que $g(p_1, \dots, p_k)$ s'identifie à la moyenne ordinaire, ou moment d'ordre 1, de la fonction

$$f[t, \lambda\psi(\theta)] .$$

Comme la fonction $g(h_1, \dots, h_k)$ vérifie des propriétés d'interpolation linéaire à partir de ses valeurs pour h_i entiers, son étude résulte de celle de $g(p_1, \dots, p_k)$. On peut alors énoncer des théorèmes analogues à celui de Van Der Corput. Mais comme on ne connaît pas d'exemple de suite $\lambda\theta^n$ équirépartie mod 1 , ces théorèmes n'ont que la valeur d'hypothèses et ne fournissent pas jusqu'à nouvel ordre d'information intéressante.

BIBLIOGRAPHIE

[1] BASS (Jean). - Sur certaines classes de fonctions admettant une fonction d'autocorrélation continue, C. R. Acad. Sc. Paris, t. 245, 1957, p. 1217-1219.

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

[3] BASS (Jean). - Contribution à l'étude de certaines fonctions susceptibles de représenter la vitesse d'un fluide turbulent, J. Math. pures et appl., Série 9, t. 37, p. 173-205.

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

[5] BASS (J.) et BERTRANDIAS (J.-P.). - Moyennes de sommes trigonometriques et fonctions d'autocorrélation, C. R. Acad. Sc. Paris, t. 245, 1957, p. 2457-2459.

[6] BASS (J.) et KRÉE (P.). - Sur les fonctions pseudo-aleatoires, C. R. Acad. Sc. Paris, t. 247, 1958, p. 1083-1085.

[7] BERTRANDIAS (Jean-Paul). - Formation d'une classe de fonctions pseudo-aléatoires, C. R. Acad. Sc. Paris, t. 248, 1959, p. 513-515.