BULLETIN DE LA S. M. F.

JEAN BASS

Suites uniformément denses, moyennes trigonométriques, fonctions pseudo-aléatoires

Bulletin de la S. M. F., tome 87 (1959), p. 1-64
<http://www.numdam.org/item?id=BSMF_1959__87__1_0>

BULLETIN

DE LA

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Bull. Soc. math. France,
87, 1959, p. 1 à 64.

SUITES UNIFORMÉMENT DENSES, MOYENNES TRIGONOMÉTRIQUES, FONCTIONS PSEUDO-ALÉATOIRES;

PAR

JEAN BASS.

(Paris).

I. — Résultats généraux.

1. Introduction. — Dans un précédent travail [3], j'ai montré qu'il pouvait être intéressant d'étudier, en vue de leurs applications physiques, certaines classes de fonctions d'un usage courant, et que je nommerai dans ce qui suit des *fonctions pseudo-aléatoires*. Je ne reviendrai pas ici sur leur origine physique, ni sur celles de leurs propriétés formelles qui ont été déjà établies. Je n'essaierai pas non plus de construire une théorie générale des fonctions pseudo-aléatoires. Je me propose seulement de montrer comment, à partir de certains théorèmes qui se trouvent aux limites de l'arithmétique et de l'analyse, il est possible de former diverses classes de fonctions pseudo-aléatoires élémentaires, que les opérations de l'analyse permettent ensuite de généraliser et de régulariser.

Il semble que N. WIENER [11] soit le premier à avoir signalé l'existence mathématique de fonctions pseudo-aléatoires. Il a étudié sommairement celles qui prennent les valeurs 1 et — 1, les points de discontinuité ayant des abscisses entières. Il a donné à leur sujet un théorème d'existence, qui sera discuté à la section III. L'exemple de WIENER a été repris par J. KAMPÉ DE FÉRIET [8], en vue d'une application possible au problème de la turbulence. Mais les travaux de WIENER se sont orientés ensuite vers le calcul des probabilités. Or la théorie des fonctions pseudo-aléatoires est essentiellement *non probabiliste.*

Elle repose sur des bases arithmétiques. Elle prend comme point de départ la notion de *suite uniformément dense* sur un segment. A l'aide de théorèmes fondamentaux d'H. WEYL [10], je montrerai comment, à certaines suites uniformément denses, on peut associer des fonctions pseudo-aléatoires ayant pour ensemble des valeurs un ensemble dense, et aussi des fonctions pseudo-aléatoires ayant un nombre fini de valeurs. Certaines de ces dernières fonctions fournissent des exemples de fonctions du type étudié par WIENER. Toutes ces fonctions sont, comme celles de Wiener, associées à une suite de points en progression arithmétique sur l'axe des abscisses, et il sera intéressant d'examiner en détail l'effet d'un changement de pas de cette progression.

Bien qu'il s'agisse d'une théorie d'analyse pure, elle présente bien des analogies avec les théories probabilistes. Une suite uniformément dense sur le segment (0, 1) peut en effet être considérée comme une suite dénombrable d'épreuves sur une variable aléatoire uniformément distribuée. Le théorème de H. Weyl donne une forme précise à cette remarque, qui conduirait à considérer toute fonction pseudo-aléatoire comme le résultat d'une épreuve sur une fonction aléatoire convenablement choisie, et à traiter le cas général des fonctions pseudo-aléatoires comme WIENER a été conduit à le faire dans un cas particulier. On obtiendrait ainsi des théorèmes d'existence très généraux, mais d'un emploi peu commode. La théorie des fonctions pseudo-aléatoires fournit des théorèmes qui, s'ils sont peut-être moins généraux, ont l'avantage d'être constructifs et de ne pas laisser d'incertitude sur les cas d'exception. L'analogie probabiliste n'en reste pas moins utile. On verra en particulier (section V) comment on peut construire des fonctions pseudo-aléatoires dont les points de discontinuité soient distribués d'une façon largement arbitraire. L'analogie des méthodes « pseudo-aléatoires » et probabilistes se retrouve d'ailleurs dans l'usage qui sera fait du théorème de Bochner sur les fonctions de type positif pour démontrer d'une façon simple un théorème de VAN DER CORPUT [9] dont le rôle sera fondamental.

Dans la section I, on trouvera des théorèmes généraux sur les fonctions pseudo-aléatoires et sur les suites uniformément denses.

La section II est consacrée à l'étude d'une classe de fonctions pseudo-aléatoires à base uniforme ayant un ensemble de valeurs denses, et la section III à celle de fonctions pseudo-aléatoires à base uniforme ayant un ensemble fini de valeurs.

Dans la section IV, j'étudie le produit de fonctions pseudo-aléatoires définies sur deux bases uniformes d'échelles différentes.

Dans la section V, des cas plus généraux sont examinés (fonctions pseudo-aléatoires à base non uniforme).

Enfin les principaux types de fonctions pseudo-aléatoires connus sont rassemblés dans la section VI, qui constitue un résumé et une conclusion.

J'ai recu de diverses personnes des conseils et d'utiles références. Je désire remercier MM. FAVRE et GAVIGLIO, qui m'ont signalé les défauts de la représentation des grandeurs turbulentes par des fonctions presque périodiques, M. RISS, qui a attiré mon attention sur les suites de Weyl, MM. GIRAULT, MARTINOT-LAGARDE, PISOT, TORTRAT, qui m'ont donné d'intéressantes indications. Je dois aussi remercier MM. BELAYCHE, BERTRANDIAS, CHAMBADAL et KRÉE, avec qui j'ai eu des discussions fréquentes et profitables. La collaboration de M. BERTRANDIAS a été particulièrement efficace, et les principales idées de la section V lui sont essentiellement dues. Je suis enfin reconnaissant à M. GUILLOUD de l'aide qu'il m'a apportée en appliquant les méthodes modernes de calcul numérique à la construction d'exemples de fonctions pseudo-aléatoires et à diverses vérifications expérimentales de résultats théoriques.

2. **Définitions.** — Soit $f(t)$ une fonction complexe de la variable réelle t, bornée, nulle pour $t < 0$.

Soit M l'opérateur de valeur moyenne, défini par

$$M(\quad) = \lim_{T \to \infty} \frac{1}{T} \int_0^T (\quad)\, dt.$$

On suppose que les moyennes

$$Mf(t), \qquad \gamma(h) = M\overline{f(t)}f(t+h)$$

existent. La seconde s'appelle *fonction de corrélation* de $f(t)$. On vérifie facilement qu'elle est prolongeable aux valeurs négatives de t, et que

$$\gamma(-h) = \bar{\gamma}(h).$$

Ceci posé, on dit que $f(t)$ est une *fonction pseudo-aléatoire* si les conditions suivantes sont vérifiées :

$$Mf(t) = 0;$$

$\gamma(h)$ est une fonction continue de h;

$$\gamma(0) \neq 0, \qquad \gamma(\infty) = 0.$$

On peut démontrer que, d'après cette définition, $f(t)$ n'est pas la transformée de Fourier-Stieltjes d'une fonction à variation bornée. Si en particulier cette fonction était continue, $\gamma(0)$ serait nul. Si c'était une fonction de sauts, $\gamma(\infty)$ ne serait pas nul, et $f(t)$ serait presque périodique.

Dans ce qui suit, nous étudierons exclusivement des fonctions pseudo-aléatoires en escalier, prenant des valeurs de module 1. Elles appartiendront aux divers types que voici :

a. $f(t) = \exp[2i\pi\,\varphi(n)]$, si $n < t < n+1$, $\varphi(t)$ fonction réelle donnée;

b. $f(t) = \exp\{2i\pi/m\ [\text{partie entière de } \varphi(n)]\}$, si $n < t < n+1$, m donné entier;

c. $f(t) = \exp[2i\pi\,\varphi(n)]$, si $t_n < t < t_{n+1}$, la suite t_n étant convenablement choisie.

Nous examinerons aussi les propriétés du produit $f(t)g(\alpha t + \beta)$, où f et g sont des fonctions du type a, et où α et β sont deux nombres réels donnés.

Pour simplifier les notations, nous désignerons par :

$\hat{t}$ la partie entière de t;

$\underset{\vee}{t} = t - \hat{t}$ la partie décimale de t (1).

Avec ces notations, les fonctions a ont pour expression

$$f(t) = \exp[2i\pi\,\varphi(\hat{t})]$$

et les fonctions b

$$f(t) = \exp\left[(2i\pi/m)\,\widehat{\varphi(\hat{t})}\right].$$

Les transformées par convolution de ces fonctions discontinues ont été étudiées en [3] et il n'y sera pas fait allusion, sauf dans la conclusion. Rappelons seulement qu'elles fournissent des fonctions pseudo-aléatoires continues, et éventuellement dérivables ou analytiques.

3. Fonction admettant un carré moyen. — Considérons l'ensemble E des fonctions complexes $f(t)$, bornées, nulles, pour $t < 0$, et telles que

$$\lim_{T\to\infty} \frac{1}{T}\int_0^T |f(t)|^2\,dt$$

existe. Nous allons montrer que ces *fonctions ne constituent pas un espace vectoriel.*

Il y a donc des différences essentielles entre les fonctions de carré sommable, et les fonctions de carré *moyen* sommable.

Pour le voir, montrons que, si $f(t) \in E$, $g(t) \in E$, $f(t) + g(t)$ peut ne pas appartenir à E. Il revient au même de montrer que

$$\frac{1}{T}\int_0^T \bar{f}(t)\,g(t)\,dt$$

peut ne pas avoir de limite lorsque $T \to \infty$.

La fonction $g(t) = 1$ appartient à E. Il suffit donc de trouver une fonction

(1) Les signes $\widehat{\quad}$ et $\widecheck{\quad}$ seront dans certains cas, pour des raisons typographiques, remplacés par $\_\wedge\_$ et $\overline{\ }\vee\overline{\ }$.

$f(t) \in E$ dont la moyenne

$$\lim_{T \to \infty} \frac{1}{T} \int_0^T f(t)\, dt$$

n'existe pas. Choisissons

$$f(t) = (-1)^{n+1} \qquad \text{si} \quad 2^n < t < 2^{n+1}.$$

Comme $|f(t)| = 1$, $f(t)$ appartient à E. Calculons

$$\frac{1}{T} \int_0^T f(t)\, dt$$

en prenant pour T un entier de la forme 2^N. On cherche la limite, pour $N \to \infty$, de

$$\frac{1}{2^N}[-1 + 2 - 2^2 + \ldots + (-1)^N 2^{N-1}] = \frac{1}{3}\left(-\frac{1}{2^N} + (-1)^N\right).$$

On voit que cette quantité oscille indéfiniment sans avoir de limite.

Les fonctions $f(t)$ et $g(t) = 1$ appartiennent donc à E, et leur somme $f(t) + 1$ n'admet pas de carré moyen.

Prenons, en particulier, pour $g(t)$ la fonction $f(t+h)$, qui a même carré moyen que $f(t)$. Nous allons vérifier que si $f(t) \in E$, c'est-à-dire si $\gamma(0)$ existe, il n'en résulte pas forcément que $\gamma(h) = M\overline{f(t)}f(t+h)$ existe.

Examinons pour cela un exemple. Supposons que $f(t)$ soit une fonction en escalier, prenant la valeur constante $c_n = \pm 1$ dans l'intervalle $n < t < n + 1$.

Soit γ_n la valeur, dans le même intervalle, de la fonction qui a été étudiée au début de ce paragraphe et qui est égale à $(-1)^{k+1}$ dans l'intervalle $2^k < t < 2^{k+1}$. Essayons de calculer les c_n de telle façon que

$$c_n c_{n+1} = \gamma_n.$$

Prenons, par exemple, $c_0 = 1$, d'où

$$c_1 = \gamma_0, \qquad c_2 = \frac{\gamma_1}{\gamma_0}, \qquad c_3 = \frac{\gamma_0\gamma_2}{\gamma_1}, \qquad c_4 = \frac{\gamma_1\gamma_3}{\gamma_0\gamma_2}, \qquad \ldots.$$

Les γ_n étant égaux à ± 1, les c_n sont aussi égaux à ± 1 et définissent une fonction $f(t)$; $f(t+1)$ prend, dans l'intervalle $n < t < n + 1$, la valeur c_{n+1} ; $\gamma(1)$ est donc égal à la moyenne des $c_n c_{n+1}$, c'est-à-dire des γ_n. On a vu que cette moyenne n'existe pas.

L'existence de $\gamma(h)$ ne résulte donc pas de celle de $\gamma(0)$. C'est une hypothèse à faire, qui ne peut pas être beaucoup simplifiée.

4. Théorèmes généraux sur les fonctions pseudo-aléatoires.

Théorème 1. — *Si $\gamma(h)$ existe et est continue, il existe une fonction $\sigma(\omega)$*

non décroissante, à variation totale bornée, telle que

$$\gamma(h) = \int_{-\infty}^{\infty} \exp(i\omega h)\, d\sigma(\omega).$$

D'après le théorème de Bochner, il suffit de montrer que $\gamma(h)$ est du type positif. Soient :

$\xi_1, \ldots, \xi_n$ n nombres complexes arbitraires, non tous nuls;
$h_1, \ldots, h_n$ n nombres réels arbitraires.

On considère la forme hermitique

$$\psi = \sum \xi_k \bar{\xi}_l \gamma(h_k - h_l)$$

et l'on veut vérifier qu'elle est non négative. Or

$$\psi = \lim_{T \to \infty} \frac{1}{T} \int_0^T \sum \xi_k \bar{\xi}_l . \bar{f}(t) f(t + h_k - h_l)\, dt.$$

Dans chaque intégrale, on pose $t - h_l = t'$, d'où

$$\psi = \lim_{T \to \infty} \frac{1}{T} \int_{-h_l}^{T-h_l} \sum \xi_k \bar{\xi}_l . \bar{f}(t' + h_l) f(t' + h_k)\, dt'.$$

On ne modifie pas la limite en remplaçant, dans chaque intégrale, la borne inférieure $-h_l$ par o. On a donc

$$\begin{aligned} \psi &= \sum \lim_{T \to \infty} \frac{T - h_l}{T} \frac{1}{T - h_l} \int_0^{T-h_l} \xi_k f(t' + h_k)\, \overline{\xi_l f(t' + h_l)}\, dt' \\ &= \sum \lim_{T \to \infty} \frac{1}{T} \int_0^T \xi_k f(t' + h_k)\, \overline{\xi_l f(t' + h_l)}\, dt' \\ &= \lim_{T \to \infty} \frac{1}{T} \int_0^T \left| \sum \xi_k f(t' + h_k) \right|^2 dt'. \end{aligned}$$

Cette quantité est visiblement non négative.

Ce théorème montre l'existence d'une *fonction spectrale énergétique* $\sigma(\omega)$ associée à $f(t)$. Il n'entraîne naturellement pas que $f(t)$ puisse être représentée par une intégrale de Fourier-Stieltjes. Il n'existe pas de fonction spectrale locale.

THÉORÈME 2. — *Si $\gamma(h)$ et $Mf(t)$ existent, $\gamma(h)$ a une moyenne par rapport à h, qui est égale à la discontinuité de la fonction spectrale $\sigma(\omega)$ à l'origine.*

Démonstration. — Il s'agit de calculer

$$M\gamma(h) = \lim_{H\to\infty} \frac{1}{H}\int_0^H \gamma(h)\,dh = \lim_{H\to\infty}\frac{1}{H}\int_0^H dh\int_{-\infty}^{\infty}\exp(i\omega h)\,d\sigma(\omega).$$

On peut permuter les intégrations et écrire

$$\begin{aligned} M\gamma(h) &= \lim_{H\to\infty}\frac{1}{H}\int_{-\infty}^{\infty} d\sigma(\omega)\int_0^H \exp(i\omega h)\,dh \\ &= \lim_{H\to\infty}\int_{-\infty}^{\infty}\exp(i\omega H/2)\frac{\sin(\omega H/2)}{\omega H/2}\,d\sigma(\omega). \end{aligned}$$

Supposons d'abord que $\sigma(\omega)$ soit continue à l'origine. ε étant donné, on peut trouver δ, indépendant de H, tel que

$$\int_{-\delta}^{\delta} d\sigma(\omega) < \varepsilon.$$

Par suite,

$$\left|\int_{-\delta}^{\delta}\exp(i\omega H/2)\frac{\sin(\omega H/2)}{\omega H/2}\,d\sigma(\omega)\right| < \int_{-\delta}^{\delta} d\sigma(\omega) < \varepsilon.$$

Or

$$\int_{-\infty}^{\infty} = \int_{-\delta}^{\delta} + \int_{|\omega|>\delta}.$$

La seconde intégrale est inférieure en module à

$$\frac{2}{H\delta}\int_{|\omega|>\delta} d\sigma(\omega) < \frac{2V}{H\delta},$$

où V est la variation totale de $\sigma(\omega)$. On peut choisir H assez grand pour que

$$\frac{2V}{H\delta} < \varepsilon.$$

Finalement, étant donné ε, on peut trouver H assez grand pour que

$$|M\gamma(h)| < \varepsilon.$$

Donc

$$M\gamma(h) = 0.$$

Si maintenant $\sigma(\omega)$ admet une discontinuité σ_0 à l'origine, on pose

$$\sigma(\omega) = \sigma_1(\omega) + \sigma_2(\omega),$$

$\sigma_1(\omega)$ étant continue à l'origine, et $\sigma_2(\omega)$ étant nulle pour $\omega < 0$, et égale à σ_0 pour $\omega > 0$. L'intégrale relative à $\sigma_1(\omega)$ est nulle. On a finalement

$$M\gamma(h) = \lim_{H\to\infty} \frac{1}{H} \int_0^H dh \int_{-\infty}^{\infty} \exp(i\omega h)\, d\sigma_2(\omega) = \sigma_0,$$

ce qui démontre le théorème.

Théorème 3. — *Si $\gamma(h)$ et $Mf(t)$ existent, $M\gamma(h)$ est un nombre réel non négatif qui satisfait à l'inégalité*

$$M\gamma(h) \geqq |Mf(t)|^2 \quad (^1).$$

En effet, d'après le théorème 2, $M\gamma(h)$ existe et a pour valeur le nombre non négatif σ_0. Donc $M\gamma(h)$ est réel et non négatif.

Posons

$$Mf(t) = m, \qquad f(t) = m + f'(t)$$

et désignons par $\gamma'(h)$ la fonction de corrélation de f'. On a

$$f(t)f(t+h) = |m|^2 + m\overline{f'(t)} + \overline{m}f'(t+h) + \overline{f'(t)}f'(t+h).$$

Comme $f'(t)$ et $f'(t+h)$ ont une moyenne nulle,

$$\gamma(h) = |m|^2 + \gamma'(h).$$

D'après le théorème 2, $M\gamma'(h) \geqq 0$. Donc

$$M\gamma(h) \geqq |m|^2.$$

Corollaire 1. — *Si $M\gamma(h) = 0$ et si $Mf(t)$ existe, alors $Mf(t) = 0$.*

Ce corollaire sera constamment utilisé dans la suite, sous la forme suivante :

Corollaire 2. — *Si $\gamma(h)$ s'annule pour tout h supérieur à un nombre $h > 0$ donné, et si $Mf(t)$ existe, alors $Mf(t) = 0$.*

En effet, $M\gamma(h)$ est nul.

On peut d'ailleurs un peu améliorer l'énoncé du corollaire 1, de manière à ne pas faire d'hypothèses inutiles sur l'existence de $Mf(t)$.

Théorème 4. — *Si $\gamma(h)$ existe et tend vers 0 avec $1/h$, alors $M\gamma(h) = 0$, $Mf(t)$ existe et est nul.*

---

(1) On peut démontrer ce théorème (ou du moins uu théorème analogue ayant les mêmes applications) d'une façon élémentaire, sans faire appel au théorème de Bochner. Il suffit d'introduire la fonction

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

et d'en prendre la moyenne dans le carré $0 < h_1 < A$, $0 < h_2 < A$, où A est d'abord fini.

On voit d'abord facilement que si $\gamma(h) \to 0$ avec $1/h$, $M\gamma(h) = 0$.

Si maintenant A est une borne supérieure de f, on a

$$\left| \frac{1}{T} \int_0^T f(t)\, dt \right| < A.$$

L'ensemble $\frac{1}{T} \int_0^T f(t)\, dt$, étant borné, a des points d'accumulation compris entre $-A$ et A. Soit m l'un d'eux. Il existe une suite $T_1, T_2, \ldots, T_n, \ldots$ telle que

$$\lim_{T_n \to \infty} \frac{1}{T_n} \int_0^{T_n} f(t)\, dt = m.$$

D'autre part, puisque $\gamma(h)$ existe, on a en particulier

$$\lim_{T_n \to \infty} \frac{1}{T_n} \int_0^{T_n} \bar{f}(t) f(t+h)\, dt = \gamma(h).$$

On pose

$$f(t) = m + f'(t),$$
$$f(t+h) = m + f'(t+h).$$

On voit que

$$\lim_{T_n \to \infty} \frac{1}{T_n} \int_0^{T_n} f'(t)\, dt = 0.$$

De même,

$$\frac{1}{T_n} \int_0^{T_n} f'(t+h)\, dt = \frac{1}{T_n} \int_h^{T_n+h} f'(t)\, dt = \frac{1}{T_n} \int_h^0 + \frac{1}{T_n} \int_0^{T_n} + \frac{1}{T_n} \int_{T_n}^{T_n+h}.$$

La première intégrale tend vers zéro. La troisième, majorée par

$$\frac{1}{T_n} \int_{T_n}^{T_n+h} A\, dt = \frac{Ah}{T_n},$$

tend aussi vers zéro. La seconde tend vers zéro par définition de f'.

Le premier membre tend vers zéro. On a donc

$$\lim_{T_n \to \infty} \frac{1}{T_n} \int_0^{T_n} \bar{f}(t) f(t+h)\, dt = |m|^2 + \lim_{T_n \to \infty} \frac{1}{T_n} \int_0^{T_n} \overline{f'(t)} f'(t+h)\, dt.$$

La limite du second membre existe et représente la fonction de corrélation $\gamma'(h)$ de $f'(t)$:

$$\gamma(h) = |m|^2 + \gamma'(h).$$

Le raisonnement du théorème 3 montre donc que $m = 0$. Tous les points d'accumulation de la suite $\frac{1}{T}\int_0^T f(t)\,dt$ sont nuls. La limite existe et est nulle.

5. **Propriétés des suites uniformément denses.** — Soit $\varphi(t)$ une fonction réelle. A tout entier n, associons la partie décimale

$$x_n = \underbrace{\varphi(n)}$$

de la suite $\varphi(n)$. Nous obtenons une suite dénombrable de points sur le segment $(0, 1)$.

Supposons que cette suite soit *dense*. Considérons les N premiers points

$$x_1, \quad x_2, \quad \ldots, x_N.$$

Soit L un segment de longueur l intérieur au segment $(0, 1)$. N' des N points $x_1, \ldots, x_N$ appartiennent à L.

Définition. — *On dit que la suite x_n est uniformément dense sur* $(0, 1)$ [*ou équirépartie dans* $(0, 1)$] *si, pour tout segment L, le rapport N'/N tend, lorsque $N \to \infty$, vers une limite égale à la longueur l du segment.*

Pour démontrer qu'une suite x_n est uniformément dense sur $(0, 1)$, on dispose d'un théorème très simple dû à H. Weyl [10]. En voici l'énoncé. On pourra en trouver la démonstration dans le livre de Cassels [7].

Théorème 5 (de H. Weyl). — *Pour que la suite x_n soit uniformément dense sur* $(0, 1)$, *il faut et il suffit que, quelle que soit la fonction $\mu(x)$, intégrable sur* $(0, 1)$, *on ait*

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

Ce théorème exprime que la moyenne arithmétique de la suite dénombrable $\mu(x_n)$ est égale à la moyenne stochastique de la fonction $\mu(x)$, où x est une variable aléatoire uniformément répartie avec une densité de probabilité égale à 1.

Lorsque

$$\mu(x) = \exp(2i\pi lx) \qquad (l \text{ entier} \neq 0),$$

l'intégrale du second membre est nulle, et aussi la moyenne du second membre. Ce résultat admet une réciproque, due à H. Weyl, et qui constitue le :

Théorème 6 (de H. Weyl). — *Pour que la suite x_n soit uniformément dense* *sur le segment* $(0, 1)$, *il faut et il suffit que, quel que soit l'entier* l *non nul*,

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

Ces définitions et ces résultats s'étendent facilement à des suites de points à plusieurs dimensions, par exemple dans le plan.

DÉFINITION. — Soit (x_n, y_n) une suite de points appartenant au carré $C(0 < x < 1, 0 < y < 1)$. Soit D un domaine quarrable arbitraire d'aire S intérieur à C.

Supposons que, parmi les N premiers points de la suite, N' appartiennent à D. La suite est dite uniformément dense dans C si, lorsque $N \to \infty$, N'/N tend vers une limite égale à S.

THÉORÈME 5 *bis*. — *Pour que la suite* (x_n, y_n) *soit uniformément dense dans* C, *il faut et il suffit que, quelle que soit la fonction* $\mu(x, y)$, *intégrable dans* C, *on ait*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N} \mu(x_n, y_n) = \iint_C \mu(x, y)\, dx\, dy.$$

En particulier :

THÉORÈME 6 *bis*. — *Pour que la suite* (x_n, y_n) *soit uniformément dense dans* C, *il faut et il suffit que, quels que soient les entiers* l_1 *et* l_2 *non simultanément nuls*,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N} \exp[2i\pi(l_1 x_n + l_2 y_n)] = 0.$$

En d'autres termes, pour que la suite (x_n, y_n) soit uniformément dense dans C, il faut et il suffit, quels que soient les entiers l_1, l_2 non simultanément nuls, la suite à une dimension $l_1 x_n + l_2 y_n$ soit uniformément dense sur $(0, 1)$.

EXEMPLE. — *Pour que la suite*

$$x_n = An$$

soit uniformément dense sur $(0, 1)$, *il faut et il suffit que* A *soit irrationnel.*

En effet, si A est irrationnel,

$$\frac{1}{N} \sum_{n=0}^{N} \exp(2i\pi l A n) = \frac{\exp[2i\pi l A(2N+1)] - \exp(-i\pi l A)}{2iN \sin \pi l A}.$$

Cette quantité tend bien vers zéro avec $1/N$.

Si A est rationnel, la suite $\underset{\vee}{An}$ n'est pas dense. Elle prend un nombre fini de valeurs. Bien entendu, la moyenne $\frac{1}{N}\sum_{n=0}^{N}\exp(2i\pi lAn)$ n'est alors pas nulle quel que soit l.

Ce résultat peut se généraliser à deux dimensions.

THÉORÈME 7. — *Pour que la suite*

$$x_n = \underset{\vee}{An}, \qquad y_n = \underset{\vee}{Bn}$$

soit uniformément dense dans le carré C, il faut et il suffit qu'entre les nombres A, B, 1, il n'existe aucune relation linéaire à coefficients entiers l_1 non simultanément nuls, de la forme

$$l_1 A + l_2 B + l_3 = 0.$$

En effet,

$$\frac{1}{N}\sum_{n=0}^{N}\exp\left[2i\pi\left(l_1\underset{\vee}{An} + l_2\underset{\vee}{Bn}\right)\right] = \frac{1}{N}\sum_{n=0}^{N}\exp[2i\pi(l_1 A + l_2 B)n].$$

La suite $(l_1 A + l_2 B)n$ est uniformément dense sur $(0, 1)$ si $l_1 A + l_2 B$ n'est pas entier, et dans ce cas seulement.

On peut de ces théorèmes déduire une conséquence simple qui servira plus loin.

THÉORÈME 8. — *Considérons une suite (x_n, y_n) uniformément dense dans le carré C. Quel que soit le nombre λ, la suite*

$$x'_n = x_n, \qquad y'_n = \underset{\vee}{\lambda y_n}$$

est uniformément dense dans C.

Considérons en effet la fonction

$$\mu(x, y) = \exp[2i\pi(l_1 x + l_2 \lambda y)].$$

Puisque la suite (x_n, y_n) est uniformément dense, on a

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N}\exp[2i\pi(l_1 x_n + l_2\lambda y_n)] = \iint_C \exp[2i\pi(l_1 x + l_2\lambda y)]\,dx\,dy$$
$$= \int_0^1 \exp(2i\pi l_1 x)\,dx \int_0^1 \exp(2i\pi l_2\lambda y)\,dy.$$

La seconde intégrale du second membre n'est pas nulle en général, mais la première l'est. Le premier membre est nul. On a donc aussi

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N} \exp\left[2i\pi\left(l_1 x_n + l_2 \underbrace{\lambda y_n}\right)\right] = 0$$

et la suite x_n, $\underbrace{\lambda y_n}$ est uniformément dense dans C.

Par exemple, dans les conditions du théorème 7, la suite

$$An, \quad \underbrace{\lambda Bn} \qquad (\operatorname{mod} 1)$$

est uniformément dense dans C, quel que soit λ.

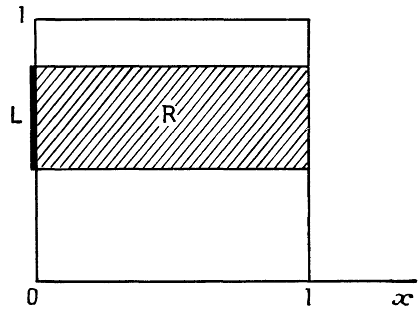


Fig. 1.

Voici enfin un théorème relatif aux suites partielles extraites de suites uniformément denses :

THÉORÈME 9. — *Soit* $x_n = \underbrace{\varphi(n)}$, $y_n = \underbrace{\psi(n)}$ *une suite uniformément dense dans le carré* C $(0 < x < 1,\ 0 < y < 1)$. *Soit* L *un intervalle intérieur à* $(0, 1)$. *Soit* E *l'ensemble des* n *tels que* $\underbrace{\psi(n)} \in L$. *La suite* $x'_n = \underbrace{\varphi(n)}$, *étendue aux valeurs de* $n \in E$, *est uniformément dense sur* $(0, 1)$, *et si* E_N *désigne l'ensemble des* $n \in E$ *pour lesquels* $n \leq N$, *on a*

$$\lim_{n \to \infty} \frac{1}{N} \sum_{n \in E_N} \exp[2i\pi\,\varphi(n)] = 0.$$

Par une transformation linéaire convenable $y' = ay + b$, on applique le segment L sur $(0, 1)$. Soit R le rectangle de base $(0, 1)$, de hauteur L (*fig.* 1).

A deux domaines d'aires égales D_1 et D_2 contenus dans R, la transformation

$$x' = x, \qquad y' = ay + b$$

fait correspondre deux domaines d'aires égales D'_1 et D'_2 contenus dans C.

Or D_1 et D_2 contiennent la même proportion de points de la suite

$$x_n = \underbrace{\varphi(n)}, \qquad y_n = \underbrace{\psi(n)}$$

(il est donc inutile de préciser ici que $n \in E$). Donc D'_1 et D'_2 contiennent la même proportion de points de la suite

$$x'_n = \underbrace{\varphi(n)}, \qquad y'_n = a\underbrace{\psi(n)} + b, \qquad n \in E.$$

Cette suite est uniformément dense dans C. Il en résulte que, quel que soit le couple non nul d'entiers l_1 et l_2,

$$\lim_{N' \to \infty} \frac{1}{N'} \sum_{n \in E_N} \exp[2i\pi(l_1 x'_n + l_2 y'_n)] = 0,$$

N' désignant le nombre de valeurs de n contenues dans E_N. En faisant $l_2 = 0$, on voit que la suite $\underbrace{\varphi(n)}$, $n \in E$, est uniformément dense sur $(0, 1)$.

Or, la suite $\underbrace{\varphi(n)}$ étant uniformément dense dans le segment $(0, 1)$, le rapport N'/N tend, lorsque $N \to \infty$, vers une limite égale à la longueur du segment L. On peut donc remplacer dans la relation ci-dessus N' par N. Pour $l_2 = 0$, on trouve que

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n \in E_N} \exp\left[2i\pi\, l_1 \underbrace{\varphi(n)}\right] = 0,$$

ce qui achève de démontrer le théorème.

II. — Fonctions pseudo-aléatoires de la forme [1]

$$f(t) = \exp[2i\pi\, \varphi(\hat{t})].$$

6. Fonctions pseudo-aléatoires et suites uniformément denses. — Soit $f(t)$ une fonction nulle pour $t < 0$, et prenant, dans chaque intervalle $n < t < n + 1$, une valeur constante de module 1. Cette fonction peut se représenter par

$$f(t) = \exp[2i\pi\, \varphi(\hat{t})].$$

Soit $\gamma(h)$ la fonction de corrélation de $f(t)$. On peut démontrer un théorème remarquable, qui a été utilisé par Wiener [11] dans un cas particulier, et qui précise la structure de $\gamma(h)$:

Théorème 10. — *$f(t)$ ayant la forme qui vient d'être précisée, si $\gamma(h)$*

---

[1] Références : J. Bass [3], J. Bass et J.-P. Bertrandias [4].

existe pour toute valeur de h entière non négative, $\gamma(h)$ *existe pour tout* **h**. *C'est une fonction continue, qui varie linéairement dans chaque intervalle* $n \leqq h \leqq n+1$.

DÉMONSTRATION. — On peut évidemment se limiter à un intervalle T entier. On cherche donc si

$$\frac{1}{N}\int_0^N \exp\left\{2i\pi\left[\varphi\left(\widehat{t+h}\right)-\varphi(\hat{t})\right]\right\}dt$$

a une limite quand $N \to \infty$. On écrit

$$\int_0^N = \sum_{n=0}^{N-1}\int_n^{n+1}.$$

Dans chaque intégrale, on fait le changement de variable

$$t = n+\xi \qquad (0<\xi<1).$$

On remarque que

$$\widehat{n+\xi} = n$$

et que

$$\begin{aligned}\widehat{n+\xi+h} &= \widehat{n+\xi}+\hat{h} = n+\hat{h} && \text{si } \xi < 1-\underset{\vee}{h},\\ &= \widehat{n+\xi}+\hat{h}+1 = n+\hat{h}+1 && \text{si } \xi \geqq 1-\underset{\vee}{h}.\end{aligned}$$

On a donc à étudier

$$\begin{aligned}&\frac{1}{N}\int_0^1 \sum^{N-1} \exp\left\{2i\pi\left[\varphi\left(\widehat{n+\xi+h}\right)-\varphi(n)\right]\right\}d\xi\\
&= \frac{1}{N}\int_0^{1-\underset{\vee}{h}} \sum_{n=0}^{N-1} \exp\{2i\pi[\varphi(n+\hat{h})-\varphi(n)]\}\,d\xi\\
&\quad + \frac{1}{N}\int_{1-\underset{\vee}{h}}^1 \sum_{n=0}^{N-1} \exp\{2i\pi[\varphi(n+\hat{h}+1)-\varphi(n)]\}\,d\xi\\
&= (1-\underset{\vee}{h})\frac{1}{N}\sum_{n=0}^{N-1}\exp\{2i\pi[\varphi(n+\hat{h})-\varphi(n)]\}\\
&\quad + \underset{\vee}{h}\,\frac{1}{N}\sum_{n=0}^{N-1}\exp\{2i\pi[\varphi(n+\hat{h}+1)-\varphi(n)]\}.\end{aligned}$$

Les deux sommes ci-dessus ont, par hypothèse, des limites égale à $\gamma(\hat{h})$

et $\gamma(\hat{h}+1)$. Donc $\gamma(h)$ existe et satisfait à la *formule d'interpolation linéaire*

$$\gamma(h) = (1-\underset{\vee}{h})\gamma(\hat{h}) + \underset{\vee}{h}\,\gamma(\hat{h}+1).$$

Lorsque $\underset{\vee}{h} \to 0$, $\gamma(h)$ tend vers $\gamma(\hat{h})$. Lorsque $\hat{h} \to 1$, $\gamma(h)$ tend vers $\gamma(\hat{h})$. Donc $\gamma(h)$ est bien une fonction continue de h.

La représentation graphique de h est donnée par la figure 2.

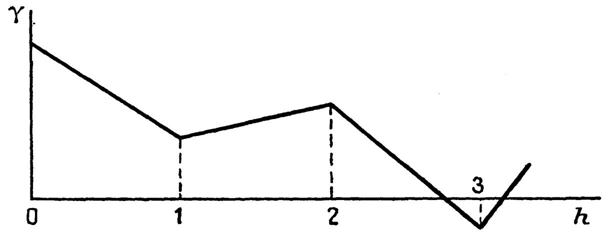


Fig. 2.

Si l'on prend $\varphi(t)$ n'importe comment, $f(t)$ n'est naturellement pas pseudo-aléatoire. Mais nous allons voir que, à l'aide des suites uniformément denses, on peut facilement construire des fonctions pseudo-aléatoires du type considéré. Nous avons besoin pour cela d'un théorème, dû initialement à J. G. Van der Corput [9], et dont la démonstration résulte très simplement des propriétés des fonctions de corrélation.

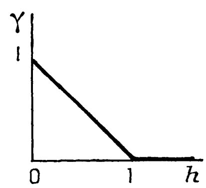


Fig. 3.

Théorème 11. — *Soit* $\gamma(h)$ *la fonction de corrélation de la fonction* $f(t) = \exp[2i\pi\,\varphi(\hat{t})]$. *Si* $\gamma(p) = 0$ *pour tout entier* $p \geq 1$, $f(t)$ *est pseudo-aléatoire.* $\gamma(h)$ *est égale à* $1 - h$ *si* $0 \leq h \leq 1$, *à* 0 *si* $h \geq 1$.

En effet, d'après le théorème 10, $\gamma(h)$ existe et est nulle pour tout $h \geq 1$. D'après le corollaire 2 (§ 4), $Mf(t) = 0$; $f(t)$ est donc pseudo-aléatoire. La forme de $\gamma(h)$ est représentée sur la figure 3.

On peut énoncer le théorème 11 sous une forme qui ne fasse pas intervenir la notion de fonction pseudo-aléatoire, et qui corresponde à l'énoncé original de Van der Corput. C'est une simple question de langage et d'écriture.

THÉORÈME 11 *bis* (VAN DER CORPUT). — *Si, pour tout entier* $p \geqq 1$,

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

alors

$$\lim_{N \to \infty} \sum_{n=0}^{N} \exp[2i\pi\,\varphi(n)] = 0.$$

En remplaçant $\varphi(n)$ par $l\varphi(n)$ où l est un entier arbitraire, et en appliquant le théorème 6, on transforme facilement l'énoncé précédent, et l'on obtient un résultat sur les suites uniformément denses :

COROLLAIRE 3. — *Si, pour tout entier* $p \geqq 1$, *la suite* $\varphi(n+p) - \varphi(n)$ *est uniformément dense sur* $(0, 1)$, *il en est de même de la suite* $\varphi(n)$.

7. Polynomes de H. Weyl et fonctions pseudo-aléatoires associées. — Prenons pour $\varphi(t)$ un polynome de degré $\nu \geqq 2$ et supposons que le coefficient A de t^ν soit irrationnel. Nous allons démontrer que :

THÉORÈME 12. — *Dans les conditions qui viennent d'être indiquées, la fonction*

$$f(t) = \exp[2i\pi\,\varphi(\hat{t})]$$

est pseudo-aléatoire. Sa fonction de corrélation $\gamma(h)$ *est nulle pour* $h \geqq 1$, *égale à* $1 - h$ *pour* $0 \leqq h \leqq 1$.

Il suffit pour cela de démontrer que $\gamma(p) = 0$ pour tout entier $p \geqq 1$, et d'appliquer le théorème 11.

Pour montrer que $\gamma(p) = 0$, on procède par récurrence.

1° *Cas d'un polynome du premier degré* $\varphi(t) = At$.

La moyenne de $f(t)$ est alors égale à

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

Pour p entier, la fonction de corrélation a pour valeur

$$\gamma(p) = \lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N} \exp(2i\pi A p) = \exp(2\pi i A p) \qquad (p \text{ entier}).$$

Lorsque h est compris entre p et $p+1$, elle s'interpole linéairement.

Formons la moyenne de $\gamma(h)$. H étant un entier, on a

$$\frac{1}{H}\int_0^H \gamma(h)\,dh = \frac{1}{H}\sum_{p=0}^{H-1}\int_p^{p+1}\gamma(h)\,dh$$

$$= \frac{1}{2H}\sum_{p=0}^{H-1}[\exp(2i\pi Ap) + \exp(2i\pi A(p+1))]$$

(formules des trapèzes)

$$= \frac{1+\exp(2i\pi AH)}{2H} + \frac{1}{H}\sum_{n=1}^{H-1}\exp(2i\pi nA).$$

Le premier terme tend vers zéro avec $1/H$. Le second est une progression géométrique classique, que nous avons déjà rencontrée. A étant irrationnel, la limite est nulle.

En conclusion, $f(t) = \exp(2i\pi At)$ n'est pas une fonction pseudo-aléatoire, car $\gamma(p)$ ne s'annule pas, si grand que soit l'entier p. Mais $M\gamma(h) = 0$ et, par suite, $Mf(t) = 0$, ce que nous avons d'ailleurs vérifié directement.

2° *Cas d'un polynome du deuxième degré.* — Il faut donc faire partir la récurrence d'un polynome de degré $\nu = 2$, soit

$$\varphi(t) = At^2 + Bt + C.$$

On a alors

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

A un facteur près, la fonction de corrélation $\gamma(p)$ est égale à la moyenne

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N}\exp(4i\pi Apn).$$

Donc $\gamma(p) = 0$, $M\gamma(h) = 0$, $Mf(t) = 0$. La fonction

$$f(t) = \exp[2i\pi(A\hat{t}^2 + B\hat{t} + C)] \qquad (A \text{ irrationnel})$$

est pseudo-aléatoire.

3° *Cas général.* — Supposons que, pour tout polynome de degré $\geqq \nu - 1$ satisfaisant aux hypothèses, la moyenne

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

soit nulle.

Soit maintenant $\varphi(t)$ un polynome de degré ν. La fonction de corrélation de $\exp[2i\pi\varphi(\hat{t})]$ est égale, pour $h=p$ entier $\geqq 1$, à

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

C'est la moyenne attachée à un polynome $\varphi(t+p)-\varphi(t)$ de degré $\nu-1$, et le coefficient de $t^{\nu-1}$ a pour coefficient νpA, nombre irrationnel. Par hypothèse, $\gamma(p)=0$. D'après le théorème **11**, $Mf(t)=0$ et $f(t)$ est pseudo-aléatoire.

On peut énoncer ce théorème avec la terminologie des suites de Weyl.

Appelons polynome W un polynome de degré ν tel que le coefficient A de t^ν soit irrationnel.

Théorème **12** *bis*. — *Si $\varphi(t)$ est un polynome W, la suite $\varphi(n)$ est uniformément dense sur* $(0, 1)$.

On remarquera que $\varphi(t)$ peut être du premier degré, mais que $\exp[2i\pi\varphi(\hat{t})]$ n'est pseudo-aléatoire que si le degré de φ est au moins égal à 2.

Exemple. — Si A est irrationnel, la fonction $\exp[2i\pi A(\hat{t})^2]$ est pseudo-aléatoire. La suite An^2 est uniformément dense sur $(0, 1)$, et l'on a

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

8. Extension des polynomes W. Polynomes W'. — Soit

$$\varphi(t)=A_0+A_1t+\ldots+A_\nu t^\nu$$

un polynome de degré ν.

Si tous les coeficients de ce polynome (sauf peut-être A_0) sont rationnels, la fonction

$$f(t)=\exp[2i\pi\varphi(\hat{t})]$$

n'est pas pseudo-aléatoire, mais *périodique*. Soit, en effet, M le plus petit commun multiple des dénominateurs des fractions $A_1, \ldots, A_\nu$. On peut poser

$$A_k=\frac{A'_k}{M}\qquad (A'_k \text{ entier})$$

et

$$\varphi(n)=A_0+\frac{1}{M}(A'_1n+\ldots+A'_\nu n^\nu).$$

Or

$$(n+M)^k\equiv n^k \pmod{M}\qquad\text{et}\qquad \frac{(n+M)^k}{M}\equiv\frac{n^k}{M}\pmod{1}.$$

On a donc

$$\varphi(n+M) = \varphi(n) + \text{entier}$$

et

$$\exp[2i\pi\,\varphi(n+M)] = \exp[2i\pi\,\varphi(n)]:$$

$f(t)$ est périodique de période M.

Supposons maintenant que l'un des coefficients A_k soit irrationnel.

DÉFINITION. — *Soit* $\varphi(t) = A_0 + A_1 t + \ldots + A_\nu t^\nu$ *un polynome de degré* $\nu \geqq 2$. *Si l'un au moins des coefficients* A_k, $k \geqq 2$, *est irrationnel, nous dirons que* $\varphi(t)$ *est un polynome* W'.

THÉORÈME 13. — *Si* $\varphi(t)$ *est un polynome* W', *la fonction*

$$f(t) = \exp[2i\pi\,\varphi(\hat{t})]$$

est pseudo-aléatoire

Ce théorème est connu pour $k = \nu$. Si $k < \nu$, on peut convenir d'appeler k le plus grand entier tel que A_k soit irrationnel, et que $A_{k+1}, \ldots, A_\nu$ soient rationnels.

Posons

$$\varphi_1(t) = A_0 + \ldots + A_k t^k, \qquad \varphi_2(t) = A_{k+1}\, t^{k+1} + \ldots + A_\nu t^\nu,$$

et désignons par M le plus petit dénominateur commun des nombres rationnels $A_{k+1}, \ldots, A_\nu$.

Si $\gamma(h)$ est la fonction de corrélation de $f(t)$, on a, pour p entier,

$$\gamma(p) = \lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N} \exp\{2i\pi[\varphi_1(n+p) - \varphi_1(n)]\} \times \exp\{2i\pi[\varphi_2(n+p) - \varphi_2(n)]\}.$$

Posons

$$n = Mr + s$$

et faisons prendre à r toutes les valeurs entières à partir de 0, à s toutes les valeurs entières de 0 à $M-1$. Sans restreindre la généralité, nous pouvons poser $N = MR - 1$, et écrire

$$\sum_{n=0}^{N} = \sum_{s=0}^{M-1} \sum_{r=0}^{R-1}.$$

Considérons pour chacune des valeurs de s, les sommes

$$\frac{1}{MR-1} \sum_{r=0}^{R-1} \exp\{2i\pi[\varphi_1(n+p) - \varphi_1(n)] \exp\{2i\pi[\varphi_2(n+p) - \varphi_2(n)]\}$$

$$= \frac{R}{MR-1} \frac{1}{R} \sum_{r=0}^{R-1} \exp\{2i\pi[\varphi_1(Mr+s+p) - \varphi_1(Mr+s)]\} \times \exp\{2i\pi[\varphi_2(Mr+s+p) - \varphi_2(Mr+s)]\}.$$

$\varphi_2(Mr+s+p)-\varphi_2(Mr+s)$ est un polynome en r dont tous les coefficients sont des fractions de dénominateur M. Sauf peut-être le terme constant, tous ses termes sont des entiers, et

$$\exp\{2i\pi[\varphi_2(Mr+s+p)-\varphi_2(Mr+s)]\}$$

est un nombre indépendant de r. A un facteur près, on a donc à étudier

$$\lim_{R\to\infty}\frac{1}{R}\sum_{r=0}^{R-1}\exp\{2i\pi[\varphi_1(Mr+s+p)-\varphi_1(Mr+s)]\}.$$

Si φ_1 est un polynome de degré 2 au moins, l'exposant est un polynome W, et la limite est nulle; $f(t)$ est donc pseudo-aléatoire. Si φ_1 est du premier degré, c'est-à-dire si $A_2, \ldots, A_\nu$ sont tous rationnels, l'exposant ne dépend pas de r, et la limite n'est pas nulle, que A_1 soit ou non irrationnel.

COROLLAIRE 4. — *Soit* $\varphi(t)=A_0+A_1t+\ldots+A_\nu t^\nu$ *un polynome de degré* $\nu\geqq 2$.

Pour que la fonction

$$f(t)=\exp[2i\pi\,\varphi(\hat{t})]$$

soit pseudo-aléatoire, il faut et il suffit que l'un au moins des coefficients $A_2, \ldots, A_\nu$ *soit irrationel.*

9. Fonctions pseudo-aléatoires et fonctions périodiques. — Si tous les coefficients du polynome $\varphi(t)=A_0+A_1t+\ldots+A_\nu t^\nu$ sont rationnels (sauf peut-être A_0), la fonction $f(t)=\exp[2i\pi\,\varphi(\hat{t})]$ est périodique. Elle a pour période le plus petit commun multiple M des dénominateurs des fractions irréductibles $A_1, \ldots, A_\nu$.

La fonction de corrélation de $f(t)$ est égale à 1 pour $h=0, M, 2M, \ldots$. Elle est nulle pour toute autre valeur entière de h, d'où sa forme (*fig.* 4).

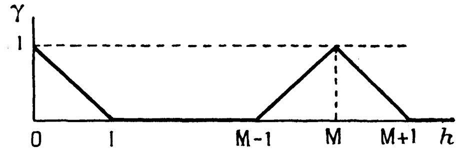


Fig. 4.

Si A_k est irrationnel, $A_{k+1}, \ldots, A_\nu$ étant rationnels, on pose

$$\varphi_1(t)=A_0+\ldots+A_kt^k \qquad (k\geqq 2),$$
$$\varphi_1(t)=A_{k+1}t^{k+1}+\ldots+A_\nu t^\nu,$$
$$f(t)=\exp[2i\pi\,\varphi_1(\hat{t})]\exp[2i\pi\,\varphi_2(\hat{t})];$$

$\varphi_1(t)$ est un polynome W, et $f(t)$ *est le produit d'une fonction pseudo-aléatoire par une fonction périodique.*

Ces fonctions ne sont d'ailleurs pas quelconques. La première est attachée à un polynome W. La seconde est une fonction périodique en escalier, dont la série de Fourier converge lentement.

La fonction de corrélation de $f(t)$ est identique à celle du facteur pseudo-aléatoire. Elle n'est pas influencée par le facteur périodique.

On peut d'ailleurs généraliser ce résultat. Si $\varphi(t)$ est un polynome W', et si $\psi(t)$ est un polynome à coefficients rationnels, la fonction

$$f(t) = \exp[2i\pi\,\varphi(\hat{t})]\exp[2i\pi\,\psi(\hat{t})]$$

produit d'une fonction pseudo-aléatoire par une fonction périodique, est pseudo-aléatoire. Sa fonction de corrélation est la même que celle du facteur pseudo-aléatoire.

Exemple. — A $\exp[2i\pi\,\varphi(\hat{t})]$ associons une fonction $f(t)$ égale à

$$\begin{array}{lll} \exp[2i\pi\,\varphi(\hat{t})] & \text{si} & 2n < t < 2n+1, \\ -\exp[2i\pi\,\varphi(\hat{t})] & \text{si} & 2n+1 < t < 2n+2. \end{array}$$

Cette fonction prend la valeur

$$\exp[2i\pi\,\varphi(n)]\exp[i\pi n]$$

dans l'intervalle

$$n < t < n+1.$$

Elle est égale à

$$\exp[2i\pi\,\varphi(\hat{t})]\exp\left[2i\pi\left(\frac{1}{2}\hat{t}\right)\right].$$

C'est le produit de $\exp[2i\pi\,\varphi(\hat{t})]$ par la fonction périodique de période 2 égale à 1 si $0 < t < 1$, à -1 si $1 < t < 2$. Elle est bien pseudo-aléatoire car, si $\varphi(t)$ est un polynome W', il en est de même de $\varphi(t) + \frac{1}{2}t$.

Il est intéressant d'examiner le comportement du produit d'une fonction pseudo-aléatoire par une fonction périodique, ou presque périodique, *continue*. On peut à ce sujet énoncer le :

Théorème 14. — *Soit $\varphi(t)$ un polynome de degré $\nu \geqq 3$, dont au moins un coefficient A_k est irrationnel ($k \geqq 2$). Soit $g(t)$ une fonction admettant un développement en série trigonométrique absolument convergente*

$$g(t) = \sum_k c_k \exp(2i\pi\omega_k t) \qquad \sum |c_k| < \infty.$$

Si les différences $\omega_l - \omega_k$ ($k \neq l$) ne sont jamais entières, le produit $f(t)$

de la fonction pseudo-aléatoire $\exp[2i\pi\,\varphi(\hat{t})]$ *par la fonction presque périodique ou périodique* $g(t)$ *est pseudo-aléatoire. Sa fonction de corrélation* $\gamma_f(h)$ *est le produit de la fonction de corrélation* $\gamma(h)$ *de* $\exp[2i\pi\,\varphi(\hat{t})]$ *par la fonction de corrélation* $\gamma_g(h)$ *de* $g(t)$.

Pour démontrer ce théorème, on va d'abord former la moyenne de

$$\exp\left[2i\pi\,\varphi\left(\widehat{t+h}\right)\right]\exp[-2i\pi\,\varphi(\hat{t})]\exp(2i\pi\omega t),$$

où ω est un nombre réel quelconque. Il s'agit de la quantité

$$\mu = \lim_{N\to\infty}\frac{1}{N}\int_0^N \exp\left\{2i\pi\left[\varphi\left(\widehat{t+h}\right) - \varphi(\hat{t}) + \omega t\right]\right\} dt.$$

Par un raisonnement déjà utilisé (§ 6) lorsque $\omega = 0$, on voit que

$$\begin{aligned}
\mu &= \lim_{N\to\infty}\frac{1}{N}\int_0^1 \sum_{n=0}^{N} \exp\left\{2i\pi\left[\varphi\left(\widehat{n+\xi+h}\right) - \varphi\left(\widehat{n+\xi}\right) + \omega n\right\}\right. \exp(2i\pi\omega\xi)\,d\xi \\
&= \lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N} \exp\left\{2i\pi[\varphi(n+\hat{h}) - \varphi(n) + \omega n]\right\}\int_0^{1-\check{h}} \exp(2i\pi\omega\xi)\,d\xi \\
&\quad + \lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N} \exp\left\{2i\pi[\varphi(n+\hat{h}+1) - \varphi(n) + \omega n]\right\}\int_{1-\check{h}}^{1} \exp(2i\pi\omega\xi)\,d\xi.
\end{aligned}$$

Si $h \geqq 1$, les deux sommes trigonométriques ci-dessus ont pour exposants des polynomes W'. Elles tendent vers zéro et $\mu = 0$.

Si $0 \leqq h \leqq 1$, la seconde tend vers zéro, et il reste

$$\mu = \lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N}\exp(2i\pi\omega n)\int_0^{1-h}\exp(2i\pi\omega\xi)\,d\xi.$$

Donc :

$\mu = 0$ si ω n'est pas entier;

$\mu = \int_0^{1-h}\exp(2i\pi\omega\xi)\,d\xi$ si ω est un entier non nul, et en particulier :

$\mu = 1 - h$ si $\omega = 0$.

Considérons maintenant le produit

$$f(t) = \exp[2i\pi\,\varphi(\hat{t})]g(t) = \sum_k c_k \exp[2i\pi\,\varphi(\hat{t})]\exp(2i\pi\omega_k t)$$

Sa fonction de corrélation est représentée par la série

$$\gamma_f(h) = \sum_{kl} \bar{c}_k c_l \exp(2i\pi\omega h)$$
$$\times \lim_{T\to\infty} \frac{1}{T}\int_0^T \exp\left\{2i\pi\left[\varphi\left(\widehat{t+h}\right) - \varphi(\hat{t})\right]\right\} \exp[2i\pi(\omega_l - \omega_k)t]\,dt.$$

Elle est nulle si $h \geqq 1$. Si $h \leqq 1$, il subsiste tous les termes pour lesquels $k = l$, qui donnent

$$\gamma(h)\sum_k |c_k|^2 \exp(2i\pi\omega_k h) = \gamma(h)\gamma_g(h).$$

Par hypothèse, $\omega_l - \omega_k$ n'est jamais un entier. Les autres termes sont donc nuls, et l'on obtient bien

$$\begin{aligned}\gamma_f(h) &= \gamma(h)\,\gamma_g(h) = (1-h)\sum_k |c_k|^2 \exp(2i\pi\omega_k h) \qquad &\text{si}\quad 0 \leqq h \leqq 1,\\ &= 0 &\text{si}\quad h \geqq 1.\end{aligned}$$

Le résultat est en particulier valable si $g(t)$ est une *fonction périodique de période non entière.*

Si, pour certaines valeurs de k et l, $\omega_l - \omega_k$ est entier, la formule précédente n'est plus exacte. On doit ajouter au produit $\gamma(h)\,\gamma_g(h)$ les termes

$$\bar{c}_k c_l \exp(2i\pi\omega_l h)\int_0^{1-h} \exp[2i\pi(\omega_l - \omega_k)\xi]\,d\xi \qquad (\omega_l - \omega_k \text{ entier}).$$

C'est ce qui ce passe lorsque $g(t)$ est périodique, la période M étant entière. On a, en particulier, le théorème suivant :

Théorème 15. — *Si $g(t)$ est une fonction périodique de période* 1, *développable en série de Fourier absolument convergente, et si $\varphi(t)$ est un polynome de degré $\nu \geqq 3$ dont au moins un coefficient A_k est irrationnel* ($k \geqq 2$), *le produit*

$$f(t) = \exp[2i\pi\,\varphi(\hat{t})]g(t)$$

est pseudo-aléatoire. Sa fonction de corrélation est nulle pour $h \geqq 1$, égale à

$$\int_0^{1-h} \bar{g}(\xi)\,g(\xi+h)\,d\xi \qquad si \quad 0 \leqq h \leqq 1.$$

On a, en effet,

$$g(t) = \sum_k c_k \exp(2i\pi kt),$$

et, d'après la méthode employée pour démontrer le théorème **14**,

$$\begin{aligned}\gamma_f(h) &= \sum_{kl} \bar{c}_k c_l \exp(2i\pi lh) \\ &\quad \times \lim_{T\to\infty} \frac{1}{T} \int_0^T \exp\left\{2i\pi\left[\varphi\left(\widehat{t+h}\right) - \varphi(\hat{t})\right]\right\} \exp[2i\pi(l-k)t]\, dt \\ &= \sum_{kl} \bar{c}_k c_l \exp(2i\pi lh) \int_0^{1-h} \exp[2i\pi(l-k)\xi]\, d\xi \\ &= \int_0^{1-h} \sum_k \overline{c_k \exp(2i\pi k\xi)} \sum_l c_l \exp[2i\pi l(\xi+h)]\, d\xi \\ &= \int_0^{1-h} \bar{g}(\xi) g(\xi+h)\, d\xi.\end{aligned}$$

Remarque. — Les théorèmes **14** et **15**, établis pour des fonctions $g(t)$ continues, ne sont pas cependant incompatibles avec les considérations du début de ce paragraphe. Reprenons l'exemple de la fonction $g(t)$, périodique de période 2, égale à 1 si $0 < t < 1$, à -1 si $-1 < t < 2$. Cette fonction admet un développement en série de Fourier de la forme

$$g(t) = \sum_k c_k \exp(i\pi kt).$$

Mais la propriété

$$g(t+1) = -g(t)$$

entraîne que les c_k sont nuls pour les valeurs paires de k

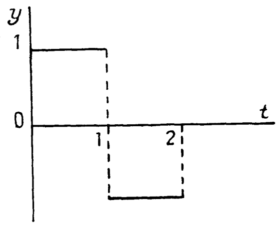


Fig. 5.

On a donc

$$g(t) = \sum_k c_{2k+1} \exp[i\pi(2k+1)t].$$

Appliquons formellement, sans nous préoccuper de vérifier la convergence, la méthode du théorème **14**, avec $\omega_k = (2k+1)/2$. Les différences

$$\omega_l - \omega_k = l - k$$

sont toujours entières.

On a donc

$$\gamma_f(h) = \sum_{kl} \bar{c}_{2k+1} c_{2l+1} \exp[i\pi(2l+1)h] \int_0^{1-h} \exp[2i\pi(l-k)\xi]\, d\xi$$
$$= \int_0^{1-h} \bar{g}(\xi) g(\xi + h)\, d\xi \qquad (0 \leqq h \leqq 1).$$

Comme, dans l'intervalle (0, 1), $g(\xi)$ est égal à 1, il reste bien

$$\gamma_f(h) = \int_0^{1-h} d\xi = 1 - h = \gamma(h).$$

Le facteur $g(t)$ n'a pas dans ce cas d'influence sur la fonction de corrélation du produit ([1]).

III. — Fonctions pseudo-aléatoires de la forme ([2])

$$\exp\left[(2i\pi/m)\,\widehat{\varphi(\hat{t})}\right].$$

10. Propriétés générales. — Dans les paragraphes qui précèdent, on a montré que, sous certaines conditions, la fonction

$$\exp[2i\pi\,\varphi(\hat{t})]$$

est pseudo-aléatoire. Les valeurs prises par cette fonction sont les nombres complexes $\exp[2i\pi\,\varphi(n)]$, qui sont denses sur le cercle unité. Nous allons maintenant étudier une classe de fonctions pseudo-aléatoires dont les valeurs, au lieu d'être denses, sont en nombre fini. Leur existence est cependant toujours liée à celle de suites uniformément denses, d'après le

Théorème 16. — *Si $\varphi(t)$ est un polynome W', la fonction*

$$f(t) = \exp\left[(2i\pi/m)\,\widehat{\varphi(\hat{t})}\right]$$

est pseudo-aléatoire pour tout entier $m \geqq 2$. Elle prend les m valeurs

$$\exp(2i\pi l/m) \qquad (l = 0, 1, \ldots, m-1).$$

Démonstration. — D'après le corollaire 2, il suffit de prouver que la fonction de corrélation $\gamma(h)$ de $f(t)$ est nulle pour tout entier $p \geqq 1$.

([1]) Suivant une remarque de M. Chambadal, le théorème 15 reste valable si l'on suppose seulement que $g(t)$ est de période 1 et appartient à $L^2(0, 1)$. Il suffit de reprendre le début de la démonstration du théorème 14, en y remplaçant $\exp(2i\pi\omega t)$ par $\bar{g}(t) g(t+h)$, sans utiliser la représentation de $g(t)$ par une série de Fourier.

([2]) Références : J. Bass [2].

Montrons d'abord que la suite

$$x_n = \underbrace{\varphi(n)}, \qquad y_n = \underbrace{\varphi(n+p)}$$

est uniformément dense dans le carré $C(0 < x < 1,\ 0 < y < 1)$.

Il suffit de prouver que, quel que soit le couple l_1, l_2 non identiquement nul d'entiers, la suite

$$\psi(n) = l_1 \underbrace{\varphi(n)} + l_2 \underbrace{\varphi(n+p)}$$

est uniformément dense sur $(0, 1)$. Il suffit pour cela que

$$\psi(t) = l_1 \varphi(t) + l_2 \varphi(t+p)$$

soit un polynome W'.

Par hypothèse, le coefficient A_k de t^k dans $\varphi(t)$ est irrationnel $(k \geqq 2)$, et $A_{k+1}, \ldots, A_\nu$ sont rationnels. Cherchons le coefficient de t^k dans $\psi(t)$.

Si $l_1 + l_2 \neq 0$, c'est

$$(l_1 + l_2) A_k + l_2 A_{k+1} C^1_{k+1} p + \ldots + A_\nu C_\nu^{\nu-k} p^{\nu-k}.$$

Le premier terme est irrationnel. Tous les autres sont rationnels. La somme est donc irrationnelle, et $\psi(t)$ est un polynome W'.

Si $l_1 = -l_2$, t^{k-1} a pour coefficient

$$l_2 [A_k C_k^1 p + \ldots + A_\nu C_\nu^{\nu-k+1} p^{\nu-k+1}] \qquad (k - 1 \geqq 1).$$

C'est sûrement un nombre irrationnel. Dans ce cas, $\psi(t)$ a au moins un coefficient irrationnel autre que le coefficient constant, et $\underbrace{\psi(n)}$ est uniformément dense sur $(0, 1)$.

La suite $\left[\underbrace{\varphi(n)}, \underbrace{\varphi(n+p)}\right]$ est donc uniformément dense dans le carré C.

La suite

$$x_n = \underbrace{\frac{1}{m}\varphi(n)}, \qquad y_n = \underbrace{\frac{1}{m}\varphi(n+p)}$$

est aussi uniformément dense dans C, car le polynome $\dfrac{\varphi(t)}{m}$ a les mêmes propriétés que $\varphi(t)$.

La suite

$$x_n = m\underbrace{\frac{1}{m}\varphi(n)}, \qquad y_n = m\underbrace{\frac{1}{m}\varphi(n+p)}$$

est donc uniformément dense dans le carré $0 < x < m$, $0 < y < m$ (*fig.* 6). Tous les carrés

$$\lambda < x < \lambda + 1, \qquad \mu < y < \mu + 1$$

contiennent à la limite la même proportion de points (x_n, y_n). Les parties entières des points contenus dans le carré hachuré sont rassemblées au point (λ, μ).

Les m^2 points (λ, μ), pour $\lambda = 0, \ldots, m-1$, $\mu = 0, \ldots, m-1$, contiennent donc à la limite la même proportion de points

$$x_n = \overparen{m \underparen{\frac{1}{m}\varphi(n)}}, \qquad y_n = \overparen{m \underparen{\frac{1}{m}\varphi(n+p)}}$$

Or

$$\underparen{\overparen{m \frac{1}{m}\varphi(n)}} = \overparen{m \frac{1}{m}\varphi(n)} = \overparen{\varphi(n)} \qquad (\operatorname{mod} m).$$

Les points

$$x_n = \overparen{\varphi(n)}, \qquad y_n = \overparen{\varphi(n+p)}$$

occupent donc mod m les m^2 positions (λ, μ), avec la même fréquence $1/m^2$.

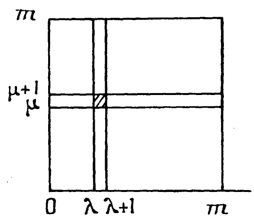


Fig. 6.

Formons maintenant

$$\gamma(p) = \lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N} \exp\left\{ (2i\pi/m) \left[\overparen{\varphi(n+p)} - \overparen{\varphi(n)} \right] \right\}.$$

Le couple $\underparen{\varphi(n)}$, $\underparen{\varphi(n+p)}$ n'intervenant que mod m, on peut écrire

$$\gamma(p) = \frac{1}{m^2} \sum_{\lambda, \mu} \exp[(2i\pi(\lambda - \mu)/m] = \left| \frac{1}{m} \sum_{\lambda=0}^{m-1} \exp(2i\pi\lambda/m) \right|^2 = 0.$$

Pour que le théorème soit démontré, il reste à prouver que, pour $k = 0$ et $k = 1$, $f(t)$ n'est pas pseudo-aléatoire.

Si tous les coefficients de $\varphi(t)$ sont rationnels, on voit d'abord que $f(t)$ est périodique, et non pseudo-aléatoire.

Supposons enfin que

$$\varphi(t) = A_1 t + \varphi_2(t),$$

où $\varphi_2(t) = A_2 t^2 + \ldots + A_\nu t^\nu$ est un polynome à coefficients rationnels et où A_1 est irrationnel. Soit $\gamma(h)$ la fonction de corrélation de $f(t)$. Calculons $\gamma(qmM)$, q entier,

$$\gamma(qmM) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N} \exp(2i\pi/m) \times$$
$$\left[\overbrace{A_1(n+qmM) + \varphi_2(n+qmM)} - \overbrace{A_1 n + \varphi_2(n)}\right].$$

Mais

$$\varphi_2(n+qmM) = \varphi_2(n) + qme \qquad (e \text{ entier}).$$

Il reste donc

$$\gamma(qmM) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N} \exp(2i\pi/m) \left[\overbrace{A_1(n+qmM) + \varphi_2(n)} - \overbrace{A_1 n + \varphi_2(n)}\right].$$

Or la quantité $\overbrace{A_1(n+qmM) + \varphi_2(n)}$ prend la valeur :

$$\overbrace{A_1 n + \varphi_2(n)} + \overbrace{A_1 qmM}$$

si

$$\underbrace{A_1 n + \varphi_2(n)} < 1 - \underbrace{A_1 qmM},$$

et la valeur :

$$\overbrace{A_1 n + \varphi_2(n)} + \overbrace{A_1 qmM} + 1$$

si

$$\underbrace{A_1 n + \varphi_2(n)} \geqq 1 - \underbrace{A_1 qmM}.$$

A_1 étant irrationnel, la suite

$$x_n = \underbrace{A_1 n + \varphi_2(n)}$$

est uniformément dense sur $(0, 1)$. Parmi les N premiers points de cette suite, il y en a N' qui vérifient l'inégalité

$$x_n < 1 - \underbrace{A_1 qmM}$$

et N'/N tend, lorsque $N \to \infty$, vers $1 - \underbrace{A_1 qmM}$.

Or on peut écrire

$$\gamma(qmM) = \lim_{N\to\infty} \frac{1}{N} \left\{ \sum\nolimits_1 \exp\left(\frac{2i\pi}{m} \overbrace{A_1 qmM}\right) + \sum\nolimits_2 \exp\left[\frac{2i\pi}{m}\left(\overbrace{A_1 qmM} + 1\right)\right] \right\},$$

les sommes $\sum_1$ et $\sum_2$ étant étendues respectivement aux valeurs de $n \leqq N$ telles que $x_n < 1 - \underbrace{A_1 qmM}$ et $x_n \geqq 1 - \underbrace{A_1 qmM}$. $\sum_1$ est le produit par $\exp\left(\frac{2i\pi}{m}\underbrace{A_1 qmM}\right)$ de N' termes égaux à 1, N' étant asymptotiquement égal à $N\left(1-\underbrace{A_1 qmM}\right)$. Résultats analogues pour $\sum_2$. Finalement, pour tout entier $q \geqq 1$,

$$\begin{aligned}\gamma(qmM) &= \exp\left(\frac{2i\pi}{m}\widehat{A_1 qmM}\right)\left[1-\underbrace{A_1 qmM}+\exp\left(\frac{2i\pi}{m}\underbrace{A_1 qmM}\right)\right]\\ &= \exp\left(\frac{2i\pi}{m}\widehat{A_1 qmM}\right)\left[1-\left(1-\exp\left(\frac{2i\pi}{m}\right)\right)\underbrace{A_1 qmM}\right].\end{aligned}$$

Il existe des valeurs $h = qmM$ aussi grandes qu'on le désire pour lesquelles $\gamma(h) \neq 0$. $\gamma(h)$ ne tend pas vers 0 avec $1/h$ et $f(t)$ n'est pas pseudo-aléatoire. Ce résultat achève la démonstration.

Exemple. — Supposons pour fixer les idées que $\varphi_2(t) = 0$. Étudions directement la fonction

$$f(t) = \exp\left(\frac{2i\pi}{m}\widehat{A_1 t}\right).$$

On a

$$\gamma(p) = \lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N}\exp\left\{\frac{2i\pi}{m}\left[\widehat{A_1(n+p)}-\widehat{A_1 n}\right]\right\}.$$

Or

$$\begin{aligned}\widehat{A_1(n+p)} &= \widehat{A_1 n}+\widehat{A_1 p} && \text{si } \underbrace{A_1 n} < 1-\underbrace{A_1 p}\\ &= \widehat{A_1 n}+\widehat{A_1 p}+1 && \text{si } \underbrace{A_1 n} \geqq 1-\underbrace{A_1 p}.\end{aligned}$$

On a donc

$$\begin{aligned}\gamma(p) &= \left(1-\underbrace{A_1 p}\right)\exp\left(\frac{2i\pi}{m}\widehat{A_1 p}\right)+\underbrace{A_1 p}\exp\left[\frac{2i\pi}{m}\left(\widehat{A_1 p}+1\right)\right]\\ &= \exp\left(\frac{2i\pi}{m}\widehat{A_1 p}\right)\left[1-\left(1-\exp\left(\frac{2i\pi}{m}\right)\right)\underbrace{A_1 p}\right].\end{aligned}$$

Le résultat auquel on est arrivé ci-dessus correspond à $M = 1$, $p = mq$. Mais ici, on obtient l'expression générale de $\gamma(p)$, qui entraîne celle de $\gamma(h)$ par interpolation linéaire.

11. Relation avec certains résultats de N. Wiener. — N. Wiener [11] semble avoir été le premier à introduire des fonctions appartenant à la classe générale des fonctions pseudo-aléatoires. Celles qu'il a étudiées prennent seulement les deux valeurs 1 et -1. Il est alors possible d'établir une correspondance entre l'ensemble des fonctions de Wiener et l'ensemble des nombres ρ compris entre 0 et 1. Il suffit de représenter ρ par son développement binaire

$$\rho = \frac{\rho_1}{2} + \ldots + \frac{\rho_n}{2^n} + \ldots, \qquad \rho_n = 0 \quad \text{ou} \quad 1,$$

et de poser

$$f(t) = 2\rho_n - 1 \qquad \text{si} \quad n < t < n+1.$$

WIENER a démontré que, *si l'on choisit* ρ *au hasard entre* 0 *et* 1, *il y a une probabilité* 1 *pour que* $f(t)$ *soit pseudo-aléatoire.*

L'ensemble des ρ qui ne conviennent pas est donc de mesure de Lebesgue nulle, mais il n'est pas spécifié par l'énoncé, et l'on n'en connaît pas la structure.

Or, si l'on choisit $m = 2$, les fonctions

$$f(t) = \exp\left[i\pi\, \widehat{\varphi(\hat{t})}\right]$$

prennent bien les valeurs 1 et -1, suivant que $\widehat{\varphi(\hat{t})}$ est pair ou impair. Mais l'énoncé du théorème du paragraphe **10** est très différent de celui de WIENER. Il affirme que, si $\varphi(t)$ est un polynome de la forme

$$A_0 + A_1 t + \ldots + A_\nu t^\nu \qquad (\nu \geqq 2),$$

$f(t)$ n'est pas pseudo-aléatoire si $A_2, \ldots, A_\nu$ sont rationnels, et est pseudo-aléatoire lorsque l'un au moins des coefficients $A_2, \ldots, A_\nu$ est irrationnel. Ce n'est donc pas un théorème d'existence presque sûre. C'est un théorème précis et en même temps constructif. Il présente cependant l'inconvénient de ne pas fournir une représentation de *toutes* les fonctions pseudo-aléatoires prenant les valeurs 1 ou -1.

IV. — Problèmes de changements d'échelle et de translations (3).

12. Position du problème. — Les fonctions pseudo-aléatoires qui ont été étudiées dans les paragraphes précédents sont des fonctions en escalier dont les points de discontinuité ont pour abscisses les entiers successifs. Un changement d'échelle ne modifie pas leurs propriétés. Mais il est intéressant d'examiner l'effet de la superposition de deux divisions différentes de l'axe des t. Donnons-nous deux fonctions pseudo-aléatoires $f(t)$ et $g(t)$, et proposons-nous de chercher sous quelles conditions le produit

$$u(t) = f(t)\, g(\alpha t + \beta)$$

est pseudo-aléatoire, α et β étant deux nombres réels donnés, $\alpha > 0$.

---

(3) Références : J. BASS et P. KRÉE [5].

Nous supposerons que f et g sont de la forme

$$f(t)=\exp[2i\pi\,\varphi(\hat{t})], \qquad g(t)=\exp[2i\pi\,\psi(\hat{t})],$$

φ et ψ étant des fonctions réelles au sujet desquelles nous ne faisons pour le moment aucune hypothèse.

L'étude de $u(t)$ va naturellement résulter de celle de sa fonction de corrélation $\gamma(h)$. On peut écrire

$$\begin{aligned}\gamma(h)=\lim_{N\to\infty}\frac{1}{N}\int_0^N \exp\Big\{2i\pi\Big[\varphi\big(\widehat{t+h}\big)-\varphi(\hat{t})\\ +\psi\big(\widehat{\alpha t+\alpha h+\beta}\big)-\psi\big(\widehat{\alpha t+\beta}\big)\Big]\Big\}\,dt\end{aligned}$$

(N entier).

On transforme $\gamma(h)$ en remplaçant

$$\int_0^N \quad \text{par} \quad \sum_{n=0}^{N-1}\int_n^{n+1}.$$

Dans l'intégrale $\int_n^{n+1}$, on pose $t=n+\xi$. On obtient

$$\begin{aligned}\gamma(h)=\lim_{N\to\infty}\int_0^1\frac{1}{N}\sum_{n=0}^{N-1}\exp\Big\{2i\pi\Big[\varphi\big(\widehat{n+\xi+h}\big)-\varphi(n)\\ +\psi\big(\widehat{\alpha n+\alpha\xi+\alpha h+\beta}\big)\\ -\psi\big(\widehat{\alpha n+\alpha\xi+\beta}\big)\Big]\Big\}\,d\xi.\end{aligned}$$

On remarque ensuite que

$$\begin{aligned}\widehat{n+\xi+h}=\widehat{n+\xi}+\hat{h}&=n+\hat{h} &&\text{si}\quad \xi<1-\underset{\vee}{h}\\ &=n+\hat{h}+1 &&\text{si}\quad \xi\geqq 1-\underset{\vee}{h}.\end{aligned}$$

On peut, par suite, mettre $\gamma(h)$ sous la forme

$$\begin{aligned}\gamma(h)=\ &\lim_{N\to\infty}\int_0^{1-\underset{\vee}{h}}\frac{1}{N}\sum_{n=0}^{N-1}\exp\Big\{2i\pi\Big[\varphi(n+\hat{h})-\varphi(n)\\ &\qquad +\psi\big(\widehat{\alpha n+\alpha\xi+\alpha h+\beta}\big)\\ &\qquad -\psi\big(\widehat{\alpha n+\alpha\xi+\beta}\big)\Big]\Big\}\,d\xi,\\ &+\lim_{N\to\infty}\int_{1-\underset{\vee}{h}}^1\frac{1}{N}\sum_{n=0}^{N-1}\exp\Big\{2i\pi\Big[\varphi(n+\hat{h}+1)-\varphi(n)\\ &\qquad +\psi\big(\widehat{\alpha n+\alpha\xi+\alpha h+\beta}\big)\\ &\qquad -\psi\big(\widehat{\alpha n+\alpha\xi+\beta}\big)\Big]\Big\}\,d\xi.\end{aligned}$$

Cette expression de $\gamma(h)$ permet d'énoncer le lemme suivant :

Lemme 1. — *Si, pour tout entier $l \geqq 1$ et pour tout ξ compris entre* o *et* 1,

$$\lim_{N\to\infty} \frac{1}{N}\sum_{n=0}^{N-1} \exp\left\{2i\pi\left[\varphi(n+h)-\varphi(n)+\psi\left(\widehat{\alpha n+\alpha\xi+\alpha h+\beta}\right)\right.\right.$$
$$\left.\left.-\varphi\left(\widehat{\alpha n+\alpha\xi+\beta}\right)\right]\right\}=0,$$

$u(t)$ est pseudo-aléatoire. Sa fonction de corrélation $\gamma(h)$ est nulle pour $h>1$, égale à

$$\gamma(h)=\lim_{N\to\infty}\frac{1}{N}\int_0^{1-h}\sum_{n=0}^{N-1}\exp\left\{2i\pi\left[\psi\left(\widehat{\alpha n+\alpha\xi+\alpha h+\beta}\right)\right.\right.$$
$$\left.\left.-\psi\left(\widehat{\alpha n+\alpha\xi+\beta}\right)\right]\right\}d\xi$$

si $0<h<1$.

Si en effet $h>1$, on voit que $\gamma(h)$ est la somme de deux intégrales de la forme

$$\lim_{N\to\infty}\int\frac{1}{N}\sum_{n=0}^{N-1}\exp\left\{2i\pi\left[\varphi(n+l)-\varphi(n)+\psi\left(\widehat{\alpha n+\alpha\xi+\beta+\alpha h}\right)\right.\right.$$
$$\left.\left.-\psi\left(\widehat{\alpha n+\alpha\xi+\beta}\right)\right]\right\}d\xi,$$

étendues à un intervalle intérieur à (o, 1), et où l désigne un entier égal à $\hat{h}$ ou à $\hat{h}+1$. La quantité $\frac{1}{N}\sum_{n=0}^{N-1}$ constitue une suite de fonctions inférieures à 1 en module, et intégrables. Si la limite de cette suite est o, l'intégrale a une limite, qui est aussi o. $\gamma(h)$ est alors égal à o.

Il y a exception si $\hat{h}=0$, soit $0\leqq h<1$. La première intégrale subsiste et fournit l'expression indiquée de $\gamma(h)$.

$\gamma(h)$ étant nulle pour $h>1$, on sait (théorème 4) que $u(t)$ est pseudo-aléatoire.

Une nouvelle réduction peut être faite maintenant. On a, en effet,

$$\begin{aligned}\widehat{\alpha n+\alpha\xi+\alpha h+\beta}&=\widehat{\alpha n+\alpha\xi+\beta}+\widehat{\alpha h} &&\text{si}\quad \undergroup{\alpha n+\alpha\xi+\beta}<1-\underset{\vee}{\alpha h}\\ &=\widehat{\alpha n+\alpha\xi+\beta}+\widehat{\alpha h}+1 &&\text{si}\quad \undergroup{\alpha n+\alpha\xi+\beta}\geqq 1-\underset{\vee}{\alpha h}.\end{aligned}$$

On est conduit à introduire l'ensemble S des n tels que

$$\undergroup{\alpha n+\alpha\xi+\beta}<1-\underset{\vee}{\alpha h},$$

et son complément S' sur (o, 1). On désigne par S_N, S'_N les parties de ces ensembles correspondant à $n \leqq N-1$, par S''_N l'ensemble des n tels que

$$\underbrace{\alpha n+\alpha\xi+\beta} \in L, \qquad n \leqq N-1,$$

L étant un intervalle quelconque intérieur à $(0, 1)$. On transforme alors le lemme 1 en :

Lemme 2. — *Si, quel que soit le couple non identiquement nul d'entiers* l_1, l_2, *l'ensemble* S''_N *défini ci-dessus, et le nombre* ξ *compris entre* 0 *et* 1, *la condition*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{S''_N} \exp\left\{2i\pi\left[\varphi(n+l_1)-\varphi(n)+\psi\left(\overbrace{\alpha n+\alpha\xi+\beta}+l_2\right)\right.\right.$$
$$\left.\left.-\psi\left(\overbrace{\alpha n+\alpha\xi+\beta}\right)\right]\right\}=0$$

est vérifiée. alors $u(t)$ *est pseudo-aléatoire. Sa fonction de corrélation est nulle pour* $h > \min\left(1, \frac{1}{\alpha}\right)$; *elle est égale dans le cas contraire à*

$$\gamma(h)=\int_0^{1-h} r(\xi)\, d\xi,$$

$r(\xi)$ *désignant la proportion limite de valeurs de* n *pour lesquelles*

$$\underbrace{\alpha n+\alpha\xi+\beta} < 1-\underset{\vee}{\alpha h}$$

En effet, le lemme 2 entraîne le lemme 1, et par suite $\gamma(h)=0$, dans les deux circonstances suivantes :

$$(a)\quad \underset{\vee}{\alpha h} > 1; \qquad (b)\quad \underset{\vee}{\alpha h} < 1, \quad h > 1.$$

En d'autres termes,

$$\text{si}\quad \alpha > 1, \qquad \gamma(h) \text{ est nul pour } h > \frac{1}{\alpha};$$
$$\text{si}\quad \alpha < 1, \qquad \gamma(h) \text{ est nul pour } h > 1.$$

Dans les deux cas, on peut dire que $\gamma(h)=0$ pour $h > \min\left(1, \frac{1}{\alpha}\right)$.

Si maintenant $h < \min\left(1, \frac{1}{\alpha}\right)$, l'expression donnée pour $\gamma(h)$ dans l'énoncé du lemme 1 se précise. La quantité en exposant est nulle, et la sommation se limite aux valeurs de $n \in S_N$, c'est-à-dire telles que

$$\underbrace{\alpha n+\alpha\xi+\beta} < 1-\underset{\vee}{\alpha h} \qquad (n \leqq N).$$

Si $N'(\xi)$ est le nombre de ces valeurs, on a

$$\gamma(h) = \lim_{N\to\infty} \int_0^{1-h} \frac{N'(\xi)}{N}\,d\xi = \int_0^{1-h} r(\xi)\,d\xi,$$

où $r(\xi) = \lim\limits_{N\to\infty} \dfrac{N'(\xi)}{N}$ est la *proportion* limite de valeurs de $n \in S_N$ lorsque $N \to \infty$.

13. Cas où α est irrationnel. — Pour pouvoir aboutir à un théorème précis, il est maintenant nécessaire de faire sur φ el ψ des hypothèses particulières. Mais la forme des résultats diffère suivant que α est ou non irrationnel. Les deux cas doivent être examinés séparément.

Si α est irrationnel, la suite $\undergroup{\alpha n + \alpha\xi + \beta}$ est uniformément dense sur $(0, 1)$. Le nombre $r(\xi)$ du lemme 2 est donc égal à $1 - \underset{\vee}{\alpha h}$, ou plutôt à $1 - \alpha h$, puisque $\alpha h < 1$. Il ne dépend pas de ξ. Dans la mesure où les hypothèses du lemme 2 sont vérifiées, on a alors

$$\begin{aligned} \gamma(h) &= (1-h)(1-\alpha h) \qquad && \text{si} \quad h < \min\left(1, \frac{1}{\alpha}\right), \\ &= 0 && \text{si} \quad h \geqq \min\left(1, \frac{1}{\alpha}\right). \end{aligned}$$

Ce résultat est valable si, pour tout couple (l_1, l_2) non identiquement nul d'entiers, on a

$$\lim_{N\to\infty} \frac{1}{N} \sum_{S''_N} \exp\Big\{ 2i\pi\Big[\varphi(n+l_1) - \varphi(n) \\ + \psi\big(\overgroup{\alpha n + \alpha\xi + \beta} + l_2\big) - \psi\big(\overgroup{\alpha n + \alpha\xi + \beta}\big)\Big]\Big\} = 0,$$

S''_N étant défini par

$$\undergroup{\alpha n + \alpha\xi + \beta} \in L \in (0, 1) \qquad (n \leqq N - 1).$$

Or il résulte du théorème 9 (fin du § 5) que cette condition est vérifiée si la suite

$$\begin{aligned} x_n &= \varphi(n+l_1) - \varphi(n) + \psi\big(\overgroup{\alpha n + \alpha\xi + \beta} + l_2\big) - \psi\big(\overgroup{\alpha n + \alpha\xi + \beta}\big), \\ y_n &= \alpha n + \alpha\xi + \beta \end{aligned}$$

est uniformément dense (mod 1) dans le carré C $(0 < x < 1,\ 0 < y < 1)$.

Avant d'énoncer le théorème auquel nous voulons aboutir, nous allons établir un dernier lemme.

LEMME 3. — *Si la suite*

$$\begin{aligned} x_n &= \varphi(n+l_1) - \varphi(n) + \psi\big(\overgroup{\alpha n + \alpha\xi + \beta} + l_2\big) - \psi\big(\overgroup{\alpha n + \alpha\xi + \beta}\big), \\ y_n &= \alpha n + \alpha\xi + \beta \end{aligned}$$

est uniformément dense (mod 1) *dans le carré C pour tout couple d'entiers* l_1, l_2 *non simultanément nuls, et pour deux polynomes W arbitraires* φ, ψ *de degré* $\nu - 1$, *elle l'est pour tout couple de polynomes W de degré* ν.

On veut en effet établir que

$$(1)\qquad \lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N}\exp\Big(2i\pi\Big\{m_1\Big[\varphi(n+l_1)-\varphi(n) + \psi\big(\widehat{\overline{\alpha n+\alpha\xi+\beta}}+l_2\big) - \psi\big(\widehat{\overline{\alpha n+\alpha\xi+\beta}}\big)\Big] + m_2(\alpha n+\alpha\xi+\beta)\Big\}\Big)=0.$$

On pose

$$\varphi'(n)=\varphi(n+l_1)-\varphi(n),$$
$$\psi'(\alpha n+\alpha\xi+\beta)=\psi\big(\widehat{\overline{\alpha n+\alpha\xi+\beta}}+l_2\big)-\psi\big(\widehat{\overline{\alpha n+\alpha\xi+\beta}}\big).$$

(1) s'écrit :

$$(2)\qquad \lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N}\exp\Big(2i\pi\Big\{m_1\Big[\varphi'(n)+\psi'\big(\widehat{\overline{\alpha n+\alpha\xi+\beta}}\big)\Big] + m_2(\alpha n+\alpha\xi+\beta)\Big\}\Big)=0.$$

Cette moyenne est nulle si la fonction de corrélation correspondante est nulle, c'est-à-dire si, pour tout entier $p \geqq 1$,

$$(3)\qquad \lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N}\exp\Big\{2i\pi m_1\Big[\varphi'(n+p)-\varphi'(n) + \psi'\big(\widehat{\overline{\alpha n+\alpha\xi+\beta+\alpha p}}\big)-\psi'\big(\widehat{\overline{\alpha n+\alpha\xi+\beta}}\big)\Big]=0$$

(les termes en m_2 sont constants et n'interviennent plus).

Ceci s'écrit

$$(4)\qquad \lim_{N\to\infty}\frac{1}{N}\sum_{S_N}\exp\Big\{2i\pi m_1\Big[\varphi'(n+p)-\varphi'(n) + \psi'\big(\widehat{\overline{\alpha n+\alpha\xi+\beta}}+\widehat{\alpha p}\big)-\psi'\big(\widehat{\overline{\alpha n+\alpha\xi+\beta}}\big)\Big]\Big\}$$
$$+\lim_{N\to\infty}\frac{1}{N}\sum_{S'_N}\exp\Big\{2i\pi m_1\Big[\varphi'(n+p)-\varphi'(n) + \psi'\big(\widehat{\overline{\alpha n+\alpha\xi+\beta}}+\widehat{\alpha p}+1\big)-\psi'\big(\widehat{\overline{\alpha n+\alpha\xi+\beta}}\big)\Big]\Big\}.$$

Si φ et ψ sont des polynomes W (polynomes dont le terme de plus haut degré a un coefficient irrationnel), il en est de même de φ' et ψ'.

Si φ et ψ sont de degré ν, φ' et ψ' sont de degré $\nu - 1$.

Or les deux limites intervenant dans (4) sont nulles, comme conséquence des hypothèses et du théorème 9. L'inégalité (1) en résulte et exprime la validité du théorème pour des polynomes de degré ν.

Nous pouvons maintenant énoncer le théorème définitif que nous avions en vue :

THÉORÈME 17. — *Si $\varphi(t)$ et $\psi(t)$ sont des polynomes de degré $\nu \geqq 2$, si les coefficients A et B de t sont irrationnels, et si, entre A, B et le nombre α, il n'existe pas de relation linéaire à coefficients entiers de la forme*

$$\lambda_1 \alpha + \lambda_2 A + \lambda_3 B\alpha + \lambda_4 = 0,$$

le produit $u(t)$ des fonctions $\exp[2i\pi\,\varphi(\hat{t})]$ *et* $\exp\left[2i\pi\,\psi\left(\widehat{\alpha t+\beta}\right)\right]$ *est pseudo-aléatoire. Sa fonction de corrélation est égale à*

$$\begin{aligned} \gamma(h) &= (1-h)(1-\alpha h) && \text{si } h < \min\left(1, \frac{1}{\alpha}\right), \\ &= 0 && \text{si } h \geqq \min\left(1, \frac{1}{\alpha}\right). \end{aligned}$$

DÉMONSTRATION. — Nous avons déjà vu que, si $u(t)$ est pseudo-aléatoire, $\gamma(h)$ a la forme annoncée. Il reste à prouver que, dans les conditions indiquées, $u(t)$ est bien pseudo-aléatoire.

Or les conditions du lemme 2 seront vérifiées si, conformément au lemme 3, la suite

$$\begin{aligned} x_n &= \varphi(n+l_1) - \varphi(n) + \psi\left(\widehat{\overline{\alpha n + \alpha\xi + \beta}} + l_2\right) - \psi\left(\widehat{\overline{\alpha n + \alpha\xi + \beta}}\right), \\ y_n &= \alpha n + \alpha\xi + \beta \end{aligned}$$

est uniformément dense (mod 1) pour tout couple de polynomes *du second degré.*

Posons donc, sans écrire les termes constants,

$$\varphi(t) = At^2 + A't, \qquad \psi(t) = Bt^2 + B't.$$

Il s'agit de prouver la relation

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N} \exp\left\{2i\pi\left[2m_1 l_1 A n + 2m_1 l_2 B\, \widehat{\overline{\alpha n + \alpha\xi + \beta}} + m_2(\alpha n + \alpha\xi + \beta)\right]\right\} = 0,$$

ou

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N} \exp\left\{2i\pi\left[(2m_1 l_1 A + 2m_1 l_2 \alpha B + m_2\alpha)n \right.\right.$$
$$\left.\left. - 2m_1 l_2 B\, \underbrace{\alpha n + \alpha\xi + \beta}\right]\right\} = 0.$$

Cette relation doit être vérifiée par tous les couples d'entiers (m_1, m_2) et (l_1, l_2) non identiquement nuls.

Si d'abord $m_1 l_2 = 0$, il reste

$$\lim_{N \to \infty} \sum_{n=0}^{N} \exp[2i\pi(2m_1 l_1 A + m_2 \alpha) n] = 0,$$

ceci, pour tout couple d'entiers $2m_1 l_1$ et m_2 non simultanément nuls. Car si $m_1 = 0$, $m_2 \neq 0$, et si $m_1 \neq 0$, l_2 doit être nul, et l_1 ne l'est donc pas.

Cette relation est vérifiée s'il n'existe entre A, α et 1 *aucune* relation linéaire à coefficients entiers. En particulier, A et α sont irrationnels.

Si maintenant $m_1 l_2 \neq 0$, le coefficient $2m_1 l_2 B$ de $\alpha n + \alpha\xi + \beta$ n'est pas nul (à moins que $B = 0$, ce que l'énoncé a exclu).

D'après le théorème 8, la condition cherchée est vérifiee si, quels que soient les deux couples d'entiers (m_1, m_2), (l_1, l_2) satisfaisant à

$$|m_1| + |m_2| \neq 0, \qquad |l_1| + |l_2| \neq 0, \qquad m_1 l_2 \neq 0,$$

la suite

$$x_n = (2m_1 l_1) A + (2m_1 l_2)\alpha B + m_2 \alpha,$$
$$y_n = \alpha n + \alpha\xi + \beta$$

est uniformément dense dans le carré C. Pour que cela ait lieu, il faut et il suffit qu'il n'existe pas d'entiers μ_1, μ_2, μ_3 non tous nuls tels que

$$2\mu_1 m_1 l_1 A + 2\mu_1 m_1 l_2 \alpha B + (\mu_1 m_2 + \mu_2)\alpha + \mu_3 = 0.$$

Si $\mu_1 = 0$, il reste $\mu_2 \alpha + \mu_3 = 0$. Comme α est irrationnel, cette relation ne peut pas être vérifiée par des entiers μ_1, μ_2 non nuls. Supposons enfin que

$$\mu_1 \neq 0.$$

Le coefficient de αB n'est alors pas nul.

La relation qui ne doit pas être vérifiée entre

$$\alpha, \quad A, \quad B\alpha, \quad 1$$

est donc dans ce cas une relation à coefficients entiers non tous nuls.

Finalement, si l'on suppose d'une façon générale qu'une relation de cette sorte ne peut être vérifiée, on satisfait aux diverses conditions rencontrées dans les cas successifs, ce qui démontre le théorème.

Remarque 1. — Le lemme 3 reste encore valable si, au lieu de prendre pour $\varphi(t) = At^\nu + \ldots$, $\psi(t) = Bt^\nu + \ldots$ un couple de polynomes W arbitraires de degré ν, on suppose que $\varphi(t)$ est un polynome W, et que entre A et B

existe une relation linéaire à coefficients entiers non tous nuls de la forme

$$r_1 A + r_2 B + r_3 = 0.$$

A étant irrationnel, r_2 ne peut d'ailleurs être nul. Mais r_1 peut être nul. B est alors rationnel, et au besoin nul.

Or la démonstration du théorème **17** n'est pas modifiée. On arrive ainsi au

COROLLAIRE 5. — *L'énoncé du théorème* 17 *reste valable avec les hypothèses suivantes :*

1° *A est irrationnel;*

2° *Il n'y a pas relation linéaire à coefficients entiers non tous nuls entre A et B;*

3° *A n'est pas une fonction homographique à coefficients entiers de α.*

REMARQUE 2. — Supposons que φ et ψ soient de même degré ν et que A et B soient irrationnels. Partons du produit

$$\exp[2i\pi\,\varphi(\widehat{t})]\exp\left[2i\pi\,\psi\left(\widehat{\alpha t+\beta}\right)\right].$$

Faisons le changement de variable

$$\alpha t + \beta = \alpha',$$

qui ne modifie pas essentiellement la structure des fonctions considérées. Nous sommes ramené à étudier

$$\exp\left\{2i\pi\left[\psi(t)+\varphi\left(\widehat{\frac{t'}{\alpha}-\frac{\beta}{\alpha}}\right)\right]\right\}.$$

Cette fonction est pseudo-aléatoire si, entre les nombres

$$\frac{1}{\alpha},\quad B,\quad \frac{A}{\alpha},\quad 1$$

il n'existe pas de relation linéaire à coefficients entiers.

On vérifie que cette condition est identique à la condition primitive, qui introduisait une relation linéaire entre

$$\alpha,\quad A,\quad B\alpha,\quad 1,$$

ou plutôt

$$1,\quad B\alpha,\quad A,\quad \alpha.$$

Si, plus symétriquement, on considère

$$\exp\left\{2i\pi\left[\varphi\left(\widehat{\alpha t+\beta}\right)+\psi\left(\widehat{\alpha' t+\beta'}\right)\right]\right\},$$

on voit qu'il ne doit pas exister de relation linéaire et homogène de la forme

$$\mu_1\alpha + \mu_2\alpha' + \mu_3 A\alpha + \mu_4 B\alpha' = 0.$$

14. Cas où α est rationnel. — D'après le lemme 1, la fonction

$$u(t) = \left\{\exp 2i\pi\left[\varphi(\hat{t}) + \psi\left(\widehat{\alpha t + \beta}\right)\right]\right\}$$

est pseudo-aléatoire si

$$\begin{aligned}\lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N-1}\exp\Big\{2i\pi\Big[&\varphi(n+l)-\varphi(n)\\ &+\psi\left(\widehat{\alpha n+\alpha\xi+\beta+\alpha h}\right)-\psi\left(\widehat{\alpha n+\alpha\xi+\beta}\right)\Big]\Big\}=0\end{aligned}$$

pour tout entier $l \geqq 1$.

Supposons que α soit de la forme p/q, où p et q sont deux entiers premiers entre eux.

Classons d'autre part les valeurs de n suivant la formule

$$n = rq + s \qquad (s = 0, 1, \ldots, q-1).$$

On a

$$\alpha n = pr + \alpha s,$$

de sorte que qr sort du signe des parties entières.

On peut se limiter à des valeurs de N de la forme $Rq + q - 1$. On doit alors donner à s les valeurs $0, 1, \ldots, q-1$ et à r, indépendamment, les valeurs $0, 1, \ldots, R$. On a donc à considérer l'expression

$$\begin{aligned}\sum_{s=0}^{q-1}\lim_{R\to\infty}\frac{1}{R+q-1}\sum_{r=0}^{R}\exp\Big\{2i\pi\Big[&\varphi(rq+s+l)-\varphi(rq+s)\\ &+\psi\left(pr+\widehat{\alpha s+\alpha\xi+\alpha h+\beta}\right)\\ &-\psi\left(pr+\widehat{\alpha s+\alpha\xi+\beta}\right)\Big]\Big\}.\end{aligned}$$

Si donc on a, pour $h > 1$,

$$\begin{aligned}\lim_{R\to\infty}\frac{1}{R}\sum_{r=0}^{R}\exp\Big\{2i\pi\Big[&\varphi(rq+s+l)-\varphi(rq+s)\\ &+\psi\left(pr+\widehat{\alpha s+\alpha\xi+\alpha h+\beta}\right)\\ &-\psi\left(pr+\widehat{\alpha s+\alpha h+\beta}\right)\Big]\Big\}=0,\end{aligned}$$

la fonction $u(t)$ est pseudo-aléatoire.

Ceci peut s'écrire

$$\lim_{R\to\infty}\frac{1}{R}\sum_{r=0}^{R}\exp\{2i\pi[\varphi(rq+s+l)-\varphi(rq+s)+\psi(pr+l_1)-\psi(pr+l_2)]\},$$

s, l, l_1, l_2 étant des entiers, $s \geqq 0$, $l \geqq 1$.

Supposons que φ et ψ soient des polynomes de degré ν, les termes en t^ν ayant respectivement pour coefficients A et B. L'exposant est un polynome de degré ν en r, dont le terme en r^ν a pour coefficient

$$A\nu lq^{\nu-1}+B\nu(l_1-l_2)p^{\nu-1} \qquad (l \text{ entier non nul}).$$

S'il n'existe entre A et B aucune relation linéaire à coefficients entiers, ce coefficient est irrationnel, et la fonction $u(t)$ est pseudo-aléatoire. Le résultat reste encore valable si A est irrationnel et si B ne l'est pas, et en particulier si $B=0$. Ainsi :

Théorème 18. — *Si α est un nombre rationnel, et si*

$$\varphi(t)=At^\nu+\ldots, \qquad \psi(t)=Bt^\nu+\ldots$$

sont deux polynomes de degré ν, la fonction

$$u(t)=\exp\left\{2i\pi\left[\varphi(\hat{t})+\psi\left(\widehat{\alpha t+\beta}\right)\right]\right\}$$

est pseudo-aléatoire dans les deux cas suivants :

a. A et B sont deux nombres irrationnels entre lesquels il n'existe aucune relation linéaire à coefficients entiers non tous nuls;

b. A est irrationnel, B est rationnel, et en particulier $B=0$.

15. Cas où α est rationnel (*suite*). Calcul de la fonction de corrélation. — D'après le lemme 1, on a

$$\gamma(h)=\lim_{N\to\infty}\frac{1}{N}\int_0^{1-h}\sum_{n=0}^{N}\exp\left\{2i\pi\left[\psi\left(\overline{\alpha n+\widehat{\alpha\xi}+\beta+\alpha h}\right)\right.\right.$$
$$\left.\left.-\psi\left(\overline{\alpha n+\widehat{\alpha\xi}+\beta}\right)\right]\right\}d\xi \qquad (0<h<1).$$

Or

$$\overline{\alpha n+\widehat{\alpha\xi+\alpha h}+\beta}=\overline{\alpha n+\widehat{\alpha\xi}+\beta}+\widehat{\alpha h} \qquad \text{si} \quad \left(\underline{\alpha n+\widecheck{\alpha\xi}+\beta}\right)<1-\check{\alpha h}$$
$$=\overline{\alpha n+\widehat{\alpha\xi}+\beta}+\widehat{\alpha h}+1 \ \text{si} \quad \left(\underline{\alpha n+\widecheck{\alpha\xi}+\beta}\right)\geqq 1-\check{\alpha h}.$$

$\gamma(h)$ est donc somme de deux intégrales où figurent des limites de la forme

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N}\exp\left\{2i\pi\left[\psi\left(\overbrace{\alpha n+\alpha\xi+\beta}+l\right)-\psi\left(\overbrace{\alpha n+\alpha\xi+\beta}\right)\right]\right\}$$

$$(l \text{ entier} \geqq 0).$$

Si le polynome ψ est un polynome W de degré $\geqq 2$, et si l est $\geqq 1$, ces limites sont nulles. En effet, en posant $n=rq+s$. on a comme exposant

$$\psi\left(pr+\overbrace{\alpha s+\alpha\xi+\beta}+l\right)-\psi\left(pr+\overbrace{\alpha s+\alpha\xi+\beta}\right)$$

et le théorème de Weyl s'applique. $\gamma(h)$ est donc nul si $\overbrace{\alpha h}\geqq 1$. Si $0<\alpha h<1$, on a

$$\gamma(h)=\int_0^{1-h} r(\xi)\,d\xi,$$

où $r(\xi)$ représente la proportion limite de valeurs de n telles que

$$\underbrace{\alpha n+\alpha\xi+\beta}<1-\underbrace{\alpha h},$$

c'est-à-dire la limite, lorsque $N\to\infty$, du quotient par N du nombre de ces valeurs $\leqq N$. Cette formule est valable si $0<h<\min\left(1,\frac{1}{\alpha}\right)$.

ξ étant un nombre donné compris entre 0 et 1, on cherche donc le nombre de valeurs de n telles que

$$\underbrace{\alpha n+\alpha\xi+\beta}<1-\alpha h.$$

Posons

$$\alpha\xi+\beta=\lambda,\qquad 1-\alpha h=\mu\qquad(0<\mu<1)$$

et étudions l'inégalité

$$\underbrace{\frac{p}{q}n+\lambda}<\mu.$$

Les valeurs de n sont évidemment définies mod q. Or, p et q étant premiers entre eux, les points des suites n et pn sont les mêmes mod q. On ne modifie donc pas le résultat en remplaçant pn par n et en prenant pour n un ensemble de q valeurs consécutives, telles que

$$\underbrace{\frac{n}{q}+\lambda}=\frac{n}{q}+\lambda.$$

On est ramené à l'inégalité

$$0<\frac{n}{q}+\lambda<\mu.$$

Elle s'écrit

$$0 < n + \lambda q < \mu q$$

ou

$$-\underbrace{\lambda q} < n + \widehat{\lambda q} < \widehat{\mu q} + \left(\underbrace{\mu q} - \underbrace{\lambda q}\right).$$

Les valeurs extrêmes possibles de l'entier n sont donc

$$\begin{array}{llll} -\widehat{\lambda q} & \text{et} \quad \widehat{\mu q} - \widehat{\lambda q} & \text{si} & \underbrace{\mu q} - \underbrace{\lambda q} > 0, \\ -\widehat{\lambda q} & \text{et} \quad \widehat{\mu q} - \widehat{\lambda q} - 1 & \text{si} & \underbrace{\mu q} - \underbrace{\lambda q} < 0. \end{array}$$

Le nombre cherché est finalement égal à

$$\begin{array}{lll} \widehat{\mu q} + 1 & \text{si} & \underbrace{\mu q} - \underbrace{\lambda q} > 0, \\ \widehat{\mu q} & \text{si} & \underbrace{\mu q} - \underbrace{\lambda q} < 0. \end{array}$$

On en conclut que

$$\begin{aligned} r(\xi) &= \frac{1}{q}\left(\widehat{q - ph}\right) & &\text{si} \quad \underbrace{p\xi + q\beta} > \underbrace{q - ph} \\ &= \frac{1}{q}\left(\widehat{\overline{q - ph + 1}}\right) & &\text{si} \quad \underbrace{p\xi + q\beta} < \underbrace{q - ph}. \end{aligned}$$

Il ne reste plus qu'à calculer

$$\gamma(h) = \int_0^{1-h} r(\xi)\, d\xi.$$

On peut écrire

$$r(\xi) = \frac{1}{q}\left(\widehat{q - ph}\right) + \frac{1}{q}\, r'(\xi),$$

avec

$$\begin{aligned} r'(\xi) &= 1 & &\text{si} \quad \underbrace{p\xi + q\beta} < \underbrace{q - ph} \\ &= 0 & &\text{si} \quad \underbrace{p\xi + q\beta} > \underbrace{q - ph}. \end{aligned}$$

On a donc

$$\gamma(h) = \frac{1 - h}{q}\left(\widehat{q - ph}\right) + \frac{1}{q}\gamma',$$

où γ' est la mesure de l'ensemble des ξ tels que

$$\underbrace{p\xi + q\beta} < \underbrace{q - ph} \qquad (0 < \xi < 1 - h).$$

Posons

$$\begin{aligned} &p\xi + q\beta = x, & &q\beta = \lambda, \\ &\underbrace{q - ph} = c \quad (0 < c < 1), & &q\beta + p - ph = \mu. \end{aligned}$$

γ' est le quotient par p de la mesure γ'' de l'ensemble des x tels que

$$\underset{\vee}{x} < c, \qquad \lambda < x < \mu.$$

x est compris entre k et $k + c$, où k est un entier non encore précisé. Si l'on pose

$$k_0 = \widehat{\lambda + 1}, \qquad k_1 = \widehat{\mu - c},$$

les segments $(k_0,\ k_0 + c)$, $(k_0 + 1,\ k_0 + c + 1)$, $\ldots$, $(k_1,\ k_1 + c)$ sont intérieurs à (λ, μ) et fournissent à γ'' une contribution

$$c(k_1 - k_0 + 1).$$

Les extrémités du segment (λ, μ) fournissent d'autre part des contributions

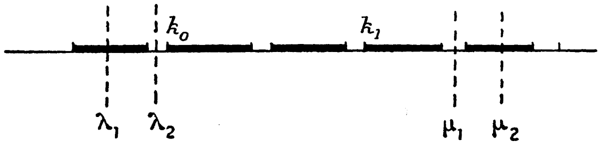


Fig. 7.

qui dépendent des valeurs relatives de λ, μ et c. Elles ont pour valeurs

$$\begin{array}{lll} c - \underbrace{\lambda + 1} & \text{si} & \underbrace{\lambda + 1} < c, \\ 0 & \text{si} & \underbrace{\lambda + 1} > c, \end{array}$$

et

$$\begin{array}{lll} \underbrace{\mu - c} - (1 - c) & \text{si} & \underbrace{\mu - c} > 1 - c, \\ 0 & \text{si} & \underbrace{\mu - c} < 1 - c. \end{array}$$

On remarque enfin que

$$c - \underbrace{\lambda + 1} = c - \underset{\vee}{\lambda} = c - \underset{\vee}{q\beta},$$

$$\underbrace{\mu - c} - (1 - c) = \underbrace{q\beta + p - ph - \underbrace{q - ph}} - (1 - c) = \underset{\vee}{q\beta} - (1 - c),$$

$$k_1 - k_0 + 1 = \widehat{\mu - c} - \widehat{\lambda + 1} + 1 = \widehat{p - ph}.$$

On a donc

$$\gamma'' = c\left(\widehat{p - ph}\right) + \left\{ \begin{array}{ll} c - \underset{\vee}{q\beta} \text{ ou } 0 & \text{suivant que } c - \underset{\vee}{q\beta} \text{ est positif ou négatif;} \\ \underset{\vee}{q\beta} - (1 - c) \text{ ou } 0 & \text{suivant que } \underset{\vee}{q\beta} - (1 - c) \text{ est positif ou négatif;} \end{array} \right.$$

$$= c\left(1 + \widehat{p - ph}\right) - \left\{ \begin{array}{c} c \\ \underset{\vee}{q\beta} \\ 1 - \underset{\vee}{q\beta} \\ 1 - c \end{array} \right\} \quad \text{suivant les positions relatives de } c,\ 1 - c,\ \underset{\vee}{q\beta},\ 1 - \underset{\vee}{q\beta}.$$

On voit facilement que le résultat peut s'écrire

$$\gamma'' = c\left(1 + \overparen{p - ph}\right) - \min\left(c,\ 1 - c,\ \underparen{q\beta},\ 1 - \underparen{q\beta}\right).$$

Il faut diviser maintenant γ'' par pq, et ajouter

$$\frac{1-h}{q}\overparen{q - ph} = \frac{1-h}{q}(q - ph - c) = (1-h)(1-\alpha h) - \frac{c(p - ph)}{pq}.$$

On trouve finalement

$$\begin{aligned}\gamma(h) = (1-h)(1-\alpha h) &+ \frac{1}{pq}\underparen{p - ph}\left(1 - \underparen{p - ph}\right)\\ &- \frac{1}{pq}\min\left(\underparen{p - ph},\ 1 - \underparen{p - ph},\ \underparen{q\beta},\ 1 - \underparen{q\beta}\right).\end{aligned}$$

THÉORÈME 19. — *Soit α un nombre rationnel, égal à une fraction irréductible p/q. Soient $\varphi(t)$ et $\psi(t)$ deux polynomes de degré $\nu \geqq 2$ tels que les coefficients A et B de t^ν ne soient liés par aucune relation linéaire à coefficients entiers non tous nuls. La fonction*

$$u(t) = \exp\left\{2i\pi\left[\varphi(\hat{t}) + \psi\left(\overparen{\alpha t + \beta}\right)\right]\right\}$$

est pseudo-aléatoire. Sa fonction de corrélation est nulle si $h > \min\left(1, \frac{1}{\alpha}\right)$, égale à

$$\begin{aligned}\gamma(h) = (1-h)(1-\alpha h) &+ \frac{1}{pq}\underparen{p - ph}\left(1 - \underparen{p - ph}\right)\\ &- \frac{1}{pq}\min\left(\underparen{p - ph},\ 1 - \underparen{p - ph},\ \underparen{q\beta},\ 1 - \underparen{q\beta}\right)\end{aligned}$$

dans le cas contraire.

16. Discussion et exemple. — Lorsque $\beta = 0$, le troisième terme de $\gamma(h)$ est nul, et il reste

$$\gamma(h) = (1-h)(1-\alpha h) + \frac{1}{pq}\underparen{p - ph}\left(1 - \underparen{p - ph}\right)$$
$$\left[0 < h < \min\left(1, \frac{1}{\alpha}\right)\right].$$

Lorsque le dénominateur q de la fraction α augmente indéfiniment, les deux derniers termes de $\gamma(h)$ tendent vers zéro. Si p augmente en même temps, de telle sorte que p/q tende vers une limite irrationnelle, on trouve à la limite

$$\gamma(h) = (1-h)(1-\alpha h).$$

C'est la formule qui a été établie directement au paragraphe 13.

Si p reste borné, α tend vers zéro, et il reste

$$\gamma(h) = 1 - h \qquad (0 < h < 1).$$

On a, dans ce cas,

$$u(t) = \exp\{2 i\pi[\varphi(\hat{t}) + \psi(\hat{\beta})]\} = \exp[2 i\pi\, \varphi(\hat{t})] \times \text{constante}.$$

On retrouve à la limite les résultats élémentaires du paragraphe 7.

Si $p = q = 1$, $\alpha = 1$, on trouve

$$\begin{aligned}\gamma(h) &= (1-h)^2 + h(1-h) - \min(1-h,\ h,\ \underset{\vee}{\beta},\ 1-\underset{\vee}{\beta}) \qquad (0<h<1)\\ &= 1 - h - \min(1-h,\ h,\ \underset{\vee}{\beta},\ 1-\underset{\vee}{\beta}).\end{aligned}$$

En particulier, pour $\beta = 0$, on retrouve

$$\gamma(h) = 1 - h.$$

Mais ce passage à la limite, effectué sur des fonctions de corrélation, ne prouve pas que, pour $\alpha = 1$, la fonction étudiée soit pseudo-aléatoire. Le cas $\alpha = 1$ a, en effet, été écarté de la discussion, car on a supposé d'abord que α était irrationnel, puis que $\alpha = p/q \neq 1$. Ce cas sera examiné au paragraphe 17.

On remarque que, lorsque $\beta = 0$, $\gamma(h)$ est représentée par une ligne brisée inscrite dans la parabole $(1-h)(1-\alpha h)$. En effet, le terme

$$\frac{1}{pq}\underbrace{p-ph}\left(1-\underbrace{p-ph}\right)$$

est de la forme

$$\begin{aligned}&\frac{1}{pq}(A-ph)(1-A+ph) \qquad (A \text{ entier})\\ &\qquad = -\alpha h^2 + \text{termes du } 1^{\text{er}} \text{ degré}.\end{aligned}$$

$\gamma(h)$ varie donc linéairement par sections. Les points anguleux sont ceux où $\underbrace{p-ph}$ prend l'une des valeurs 0 ou 1. Ils sont bien sur le parabole.

Exemple. — Choisissons $\alpha = \frac{2}{3}$, $\beta = 0{,}6$ et construisons $\gamma(h)$ pour $0 < h < 1 < \frac{3}{2}$.

On a ici

$$p = 2, \qquad q = 3, \qquad \underset{\vee}{q\beta} = \underset{\vee}{1{,}8} = 0{,}8, \qquad 1 - \underset{\vee}{q\beta} = 0{,}2,$$

$$\underbrace{p-ph} = \underbrace{2-2h} = \begin{cases} 1 - 2h & \text{si } 0 < h < \frac{1}{2},\\[1ex] 2 - 2h & \text{si } \frac{1}{2} < h < 1.\end{cases}$$

La somme des deux premiers termes de $\gamma(h)$ vaut donc

$$1-\frac{4}{3}h \qquad \text{si} \quad 0<h<\frac{1}{2},$$

$$\frac{2}{3}-\frac{2}{3}h \qquad \text{si} \quad \frac{1}{2}<h<1.$$

Le terme complémentaire à retrancher vaut

$$\frac{1}{6}\min\left(\underbrace{2-2h}, 1-\underbrace{2-2h}, 0, 2\right),$$

soit

$$\frac{1}{6}\min(1-2h, 0, 2h, 0, 2) \qquad \text{si} \quad 0<h<\frac{1}{2},$$

$$\frac{1}{6}\min(2-2h, 2h-1, 0, 2) \qquad \text{si} \quad \frac{1}{2}<h<1.$$

Le tableau suivant donne ses valeurs, puis celles de $\gamma(h)$, en fonction des valeurs de h :

h.............	0.		0,1.		0,4.		0,5.		0,6.		0,9.		1.
Terme complémentaire....	0	$\frac{h}{3}$	$\frac{1}{30}$	$\frac{1}{30}$	$\frac{1}{30}$	$\frac{1-2h}{6}$	0	$\frac{2h-1}{6}$	$\frac{1}{30}$	$\frac{1}{30}$	$\frac{1}{30}$	$\frac{1-h}{3}$	0
$\gamma(h)$.......		$1-\frac{5}{3}h$		$\frac{29}{30}-\frac{4}{3}h$		$\frac{5}{6}-h$		$\frac{5}{6}-h$		$\frac{19}{30}-\frac{2}{3}h$		$\frac{1}{3}-\frac{1}{3}h$	

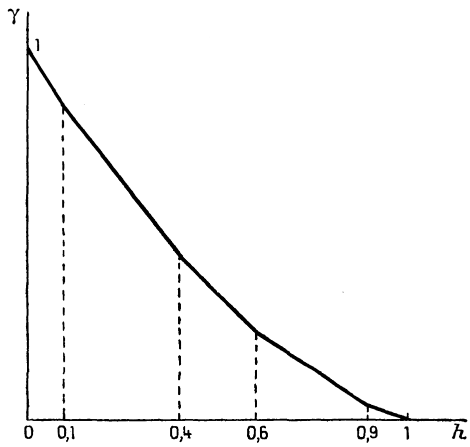


Fig. 8.

On notera que la parabole $(1-h)\left(1-\frac{2}{3}h\right)$ est tangente aux points $h=0$ et $h=1$ à la ligne brisée représentative de $\gamma(h)$ (*fig*. 8).

17. Étude particulière des translations sans changement d'échelle. — Considérons un polynome $\varphi(t)$ de degré $\nu \geqq 3$, dont le coefficient A de t^ν soit irrationnel. Proposons-nous d'examiner la nature de la fonction

$$u = \exp\left\{2i\pi\left[\varphi\left(\widehat{t+\beta}\right) - \varphi(\hat{t})\right]\right\}$$

produit de la fonction pseudo-aléatoire $\exp\overline{\left[2i\pi\varphi(\hat{t})\right]}$ par la translatée de $\exp\left[2i\pi\varphi(\hat{t})\right]$ d'une quantité $\beta > 0$.

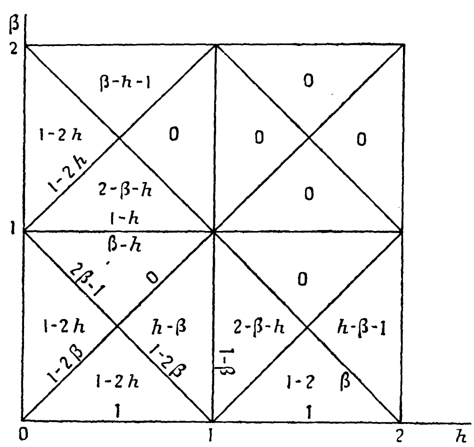
Cette fonction n'est pas pseudo-aléatoire si $0 < \beta < 1$, car sa moyenne n'est pas nulle.

Le calcul de sa fonction de corrélation $\gamma(h)$ est un peu long, mais ne présente pas de difficultés. Voici seulement les résultats :

Si $0 < \beta < 1$, $\gamma(h)$ prend les mêmes valeurs aux points

$$h = \underset{\vee}{h} + k \qquad (k \text{ entier arbitraire} \geqq 1).$$

Enfin les diverses valeurs de $\gamma(h)$ sont rassemblées dans le tableau ci-dessous.



La figure 9 indique la forme de $\gamma(h)$ pour quatre valeurs de β, comprises respectivement dans les intervalles

$$0 < \beta < \frac{1}{2}, \qquad \frac{1}{2} < \beta < 1, \qquad 1 < \beta < \frac{3}{2}, \qquad \frac{3}{2} < \beta < 2.$$

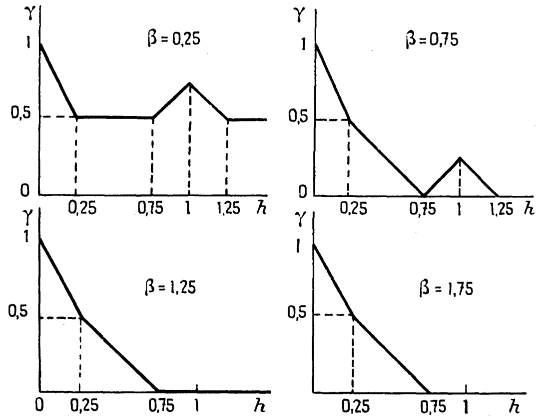


Fig. 9.

De ces résultats on déduit le

Théorème 20. — *Si $\varphi(t)$ est un polynome W de degré $\nu \geqq 3$, et si β est un nombre au moins égal à* 1, *la fonction*

$$u(t) = \exp\left\{2i\pi\left[\varphi(\widehat{t+\beta}) - \varphi(\hat{t})\right]\right\}$$

est pseudo-aléatoire. Sa fonction de corrélation est nulle pour $h > 1$, et égale pour $0 < h < 1$ à

$$\gamma(h) = 1 - h - \min(h,\ 1 - h,\ \check{\beta},\ 1 - \check{\beta}).$$

V. — Fonctions pseudo-aléatoires définies sur une base non uniforme (4).

18. Introduction. — Les fonctions pseudo-aléatoires qui ont été étudiées jusqu'ici étaient des fonctions en escalier dont les points de discontinuité constituaient des progressions arithmétiques. Nous dirons qu'elles étaient définies sur une base uniforme. A la section IV, nous avons construit des fonctions pseudo-aléatoires définies sur une base qui est la réunion de deux bases uniformes d'échelles différentes. Nous nous proposons maintenant de

(4) Références : J.-P. Bertrandias [6].

traiter un problème plus général, et de construire des fonctions pseudo-aléatoires sur des bases largement arbitraires.

Soit $t_1, t_2, \ldots, t_n, \ldots$ une suite infinie croissante de nombres positifs. Désignons par $f(t)$ la fonction qui est égale à

$$\exp[2i\pi\varphi(n)] \qquad \text{si} \quad t_n < t < t_{n+1}.$$

Comment faut-il choisir la suite t_n pour que $f(t)$ soit pseudo-aléatoire ?

Soit $r(x)$ une fonction bornée, intégrable au sens de Riemann, non négative, définie sur l'intervalle $(0, 1)$. Soit x_n une suite uniformément dense sur $(0, 1)$.

Posons

$$\delta_n = t_{n+1} - t_n = r(x_n).$$

La suite δ_n est bornée. D'autre part, d'après le théorème de H. Weyl,

$$\lim_{N \to \infty} \frac{1}{N}[r(x_1) + \ldots + r(x_N)] = \int_0^1 r(x)\,dx = R.$$

Comme $t_N = \delta_1 + \ldots + \delta_{N-1}$, on voit que t_N/N tend vers une limite R lorsque $N \to \infty$. La suite t_N est donc indéfiniment croissante avec N.

La fonction de corrélation de $f(t)$ a pour expression

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

Comme les δ_n sont bornés, on peut remplacer T par un nombre t_N et écrire

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

$$= \frac{1}{R}\lim_{N \to \infty} \frac{1}{N}\int_0^{t_N} \bar{f}(t)f(t+h)\,dt.$$

Désignons par E_p l'ensemble des $t < t_N$ tels que les intervalles de la suite δ_n contenant respectivement t et $t+h$ soient séparés par *au moins* p intervalles. Nous allons montrer d'abord que, ε étant donné, on peut trouver un nombre p_0 indépendant de N tel que, si $p > p_0$,

$$\left|\frac{1}{N}\int_{E_p} \bar{f}(t)f(t+h)\,dt\right| < \varepsilon.$$

h ayant une valeur fixée, ce résultat est évident lorsque $r(x)$ admet une borne inférieure b positive.

Dans le cas contraire, le module de l'intégrale ci-dessus est inférieur à

$$\frac{1}{N}\int_{E_p} dt,$$

où l'intégrale représente la mesure de l'ensemble des $t \in E_p$.

Soit t'_1 la plus petite valeur de t telle que $t'_1 \in E_p$. Soit t'_2 la plus petite valeur de t, à droite de $t'_1 + h$, telle que $t'_2 \in E_p$. On construit, par itération de ce procédé, une suite de k intervalles

$$(t'_1, t'_1 + h), \quad (t'_2, t'_2 + h), \quad \ldots, \quad (t'_k, t'_k + h), \quad t'_k + h \geqq t_N,$$

qui recouvrent E_p (*fig.* 10).

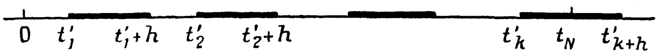


Fig. 10.

Chacun de ces intervalles contient au moins p intervalles de la suite δ_n. Il y a donc au moins $(k-1)p$ de ces intervalles entre o et t_N, de sorte que

$$(k-1)p < N, \qquad k < \frac{N}{p} + 1.$$

La longueur totale de ces intervalles est $< h\left(\frac{N}{p} + 1\right)$, et

$$\frac{1}{N}\int_{E_p} dt < \frac{h}{p} + \frac{h}{N}.$$

Choisissons *a priori* des valeurs de N telles que

$$\frac{h}{N} < \frac{\varepsilon}{2};$$

choisissons ensuite p tel que

$$\frac{h}{p} < \frac{\varepsilon}{2}, \qquad p > \frac{2h}{\varepsilon}.$$

Alors

$$\frac{1}{N}\int_{E_p} dt < \varepsilon.$$

L'étude de la fonction de corrélation $\gamma(h)$ est donc ramenée à celle de

$$\lim_{N \to \infty} \frac{1}{N}\int \bar{f}(t) f(t+h)\, dt,$$

l'intégrale étant étendue aux valeurs de $t < t_N$ telles que t et $t+h$ soient séparées par moins de p_0 intervalles, où p_0 est un nombre *fini* et fixé, dépendant seulement de ε (et de h).

19. Le théorème fondamental. — On peut écrire sans aucune restriction

$$R\gamma(h) = \lim_{N\to\infty} \frac{1}{N}\int_0^{t_N} \bar{f}(t) f(t+h)\, dt = \lim_{N\to\infty} \sum_{n=0}^{N-1} \frac{1}{N}\int_{t_n}^{t_{n+1}} \bar{f}(t) f(t+h)\, dt.$$

Soit μ_{np} la mesure de l'ensemble des $t \in \delta_n$ tels que $t+h \in \delta_{n+p}$. L'intégrale ci-dessus devient

$$R\gamma(h) = \lim_{N\to\infty} \sum_{p=0}^{\infty} \sum_{n=0}^{N-1} \frac{1}{N} \exp\{2i\pi[\varphi(n+p) - \varphi(n)]\}\, \mu_{np}.$$

Mais, d'après le résultat qui a été démontré à la fin du paragraphe précédent, on fait une erreur arbitrairement petite sur $\gamma(h)$ en ne prenant qu'un nombre fini de valeurs de p. On peut alors permuter les limites et écrire

$$R\gamma(h) = \sum_{p=0}^{p_0} \lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} \exp\{2i\pi[\varphi(n+p) - \varphi(n)]\}\, \mu_{np}.$$

Nous allons montrer que, pour tout $p \geqq 1$, et dans des conditions qui seront précisées,

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

et que, par suite,

$$R\gamma(h) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} \mu_{n0}.$$

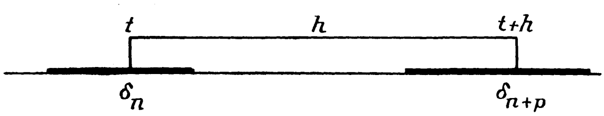


Fig. 11.

On voit d'abord facilement que

$$\mu_{np} = 0 \quad \text{si} \quad h < \delta_{n+1} + \ldots + \delta_{n+p-1} \qquad (p \geqq 2),$$
$$\text{ou} \quad h > \delta_n + \ldots + \delta_{n+p}$$
$$\mu_{np} = \min(\delta_n, \delta_{n+p}, \delta_n + \ldots + \delta_{n+p} - h, h - \delta_{n+1} - \ldots - \delta_{n+p+1})$$

dans le cas contraire.

Or on a posé $\delta_n = r(x_n)$.

μ_{np} est donc une fonction de $x_n, x_{n+1}, \ldots, x_{n+p}$ et, si l'on considère $x_n, \ldots, x_{n+p}$ comme des variables indépendantes, c'est une fonction intégrable de ces variables.

Supposons que $x_n = \psi(n)$ soit un *polynome* en n de degré $\nu \geqq 1$. Les polynomes

$$\psi(t), \quad \psi(t+1), \quad \ldots, \quad \psi(t+\nu-1)$$

sont linéairement indépendants. D'autre part, la théorie des différences montre que

$$\psi(t+\nu) = C_\nu^1\, \psi(t+\nu-1) - C_\nu^2\, \psi(t+\nu-2) + \ldots + (-1)^{\nu-1}\psi(t) + C,$$

où C est indépendant de t. Par suite, si $p \geqq \nu$, $\psi(n+p)$ est une combinaison linéaire à *coefficients entiers* de $\psi(n), \psi(n+1), \ldots, \psi(n+\nu-1)$, à une constante additive près C.

Établissons d'abord le

Lemme 4. — *Si $\varphi(n)$, $\psi(n)$ sont deux polynomes W, $\varphi(n)$ étant de degré $\geqq 2$ et $\psi(n)$ de degré $\geqq 1$, et si la suite de points $\varphi(n)$, $\psi(n)$ est uniformément dense* mod 1 *dans le carré C, la suite*

$$\varphi(n+p) - \varphi(n), \quad \underbrace{\psi(n)}, \quad \underbrace{\psi(n+1)}, \quad \ldots, \quad \underbrace{\psi(n+p)}$$

est, pour $p \leqq \nu - 1$, uniformément dense dans l'hypercube fondamental C_{p+2} de l'espace à $p+2$ dimensions.

Il suffit de vérifier que, quels que soient les entiers $l_1, \ldots, l_{p+2}$ non tous nuls,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N} \exp[2i\pi\{l_1[\varphi(n+p) - \varphi(n)] + l_2\psi(n) + \ldots + l_{p+2}\psi(n+p)\}] = 0.$$

Si $\varphi(t)$ est de degré $\geqq \nu + 2$, le résultat est évident. Dans le cas contraire, le degré de $\varphi(n+p) - \varphi(n)$ est au plus égal au degré ν de $\psi(n)$. Le terme de plus haut degré de l'exposant a pour coefficient

$$(l_2 + \ldots + l_{p+2})B + l_1 A\, p(\nu+1) \qquad \text{si degré } \varphi = \nu + 1,$$
$$(l_2 + \ldots + l_{p+2})B \qquad \text{si degré } \varphi < \nu + 1.$$

Il est irrationnel si $l_2 + \ldots + l_{p+2} \neq 0$. Dans le cas contraire, on voit facilement que l'exposant de l'exponentielle reste un polynome W, de degré inférieur à ν.

Il en résulte que, si $p \leqq \nu - 1$,

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

En effet, la somme trigonométrique du premier membre est égale, d'après le théorème de Weyl, à une intégrale multiple étendue à l'hypercube C_{p+2} d'un espace à $p+2$ dimensions, de la forme

$$\int_{C_{p+2}} \exp(2i\pi x_0)\,\mu_{np}(x_1, \ldots, x_{p+1})\,dx_0\,dx_1 \ldots dx_{p+1}.$$

Elle se décompose en un produit de deux intégrales dont la première

$$\int_0^1 \exp(2i\pi x_0)\,dx_0$$

est nulle. Le produit est donc nul, d'où le résultat.

Si maintenant $p \geqq \nu$, μ_{np} est une fonction de $\underbrace{\psi(n)}$, $\underbrace{\psi(n+1)}$, $\ldots$, $\underbrace{\psi(n+\nu-1)}$, $\underbrace{\psi(n+\nu)}$, $\ldots$, $\underbrace{\psi(n+p)}$. Mais la théorie des différences montre que $\psi(n+\nu)$, $\ldots$, $\psi(n+p)$ sont des combinaisons linéaires à *coefficients entiers* a_{jk} de $\psi(n)$, $\ldots$, $\psi(n+\nu-1)$, soit

$$\psi(n+k) = \sum_{j=0}^{\nu-1} a_{jk}\psi(n+j) + b_k \qquad (k \geqq \nu).$$

On a donc

$$\underbrace{\psi(n+k)} = \underbrace{\sum_{j=0}^{\nu-1} a_{jk}\psi(n+j) + b_k} = \underbrace{\sum_{j=0}^{\nu-1} a_{jk}\underbrace{\psi(n+j)} + b_k}.$$

La fonction

$$x_{n+k} = \underbrace{\sum_{j=0}^{\nu-1} a_{jk}x_{n+j} + b_k}$$

est une fonction intégrable de x_n, x_{n+1}, $\ldots$, $x_{n+\nu-1}$. Donc

$$\mu_{np}\left(x_n, x_{n+1}, \ldots, x_{n+\nu-1}, \underbrace{\sum_{j=0}^{\nu-1} a_{j\nu}x_{n+j} + b_\nu}, \underbrace{\sum_{j=0}^{\nu-1} a_{jp}x_{n+j} + b_p} \right).$$

est une fonction intégrable

$$\mu(x_n, \ldots, x_{n+\nu-1}).$$

On est finalement ramené à des conditions tout à fait analogues à celles qu'on a rencontrées pour $p \leqq \nu - 1$; par suite, quel que soit $p \geqq 1$,

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

Il reste à calculer la valeur exacte de $\gamma(h)$, qui résulte du seul terme relatif à $p = 0$:

$$R\gamma(h) = \lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N-1} \mu_{n0} \,;$$

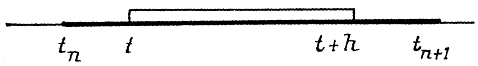


Fig. 12.

μ_{n0} est la mesure de l'ensemble des t tels que t et $t+h$ appartiennent au même intervalle δ_n, $n \leqq N$,

$$\begin{aligned} \mu_{n0} &= 0 & &\text{si } \delta_n - h < 0, \\ &= \delta_n - h & &\text{si } \delta_n - h > 0. \end{aligned}$$

Si donc on introduit la fonction intégrable $\mu(x)$ telle que

$$\begin{aligned} \mu(x) &= 0 & &\text{si } r(x) - h < 0, \\ &= r(x) - h & &\text{si } r(x) - h > 0, \end{aligned}$$

on a

$$R\gamma(h) = \lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N-1} \mu[r(x_n)] = \int_0^1 \mu[r(x)]\,dx = \int_{r(x)-h>0} [r(x) - h]\,dx.$$

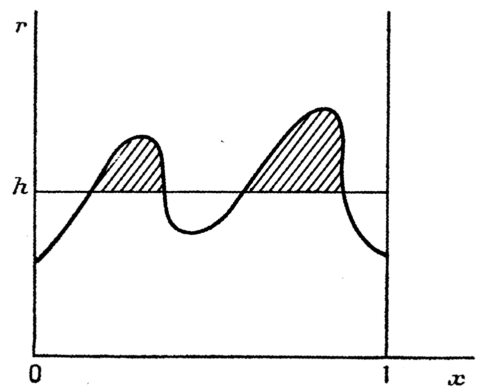


Fig. 13.

On arrive au théorème fondamental :

THÉORÈME 21. — *Soient* $\varphi(t)$, $\psi(t)$ *deux polynomes W de degrés respectivement supérieurs à* 2 *et à* 1. *On suppose que la suite de points* $\varphi(n)$, $\psi(n)$ *est uniformément dense* (mod 1) *dans le carré* $C(0<x<1,\ 0<y<1)$. *On se donne d'autre part une fonction* $r(x)$ *bornée, intégrable et non négative sur* $(0, 1)$ *et une suite* $t_1, t_2, \ldots, t_n, \ldots$, *telle que* $t_{n+1}-t_n=r\left[\underbrace{\psi(n)}\right]$. *Alors la fonction égale à* $f(t)=\exp[2i\pi\,\varphi(n)]$ *lorsque* $t_n<t<t_{n+1}$ *est pseudo-aléatoire. Sa fonction de corrélation est égale à*

$$\begin{aligned}\gamma(h)&=\frac{1}{R}\int_{r(x)-h>0}[r(x)-h]\,dx &&\text{si}\quad h<\sup r(x),\\ &=0 &&\text{si}\quad h>\sup r(x),\end{aligned}$$

avec

$$R=\int_0^1 r(x)\,dx.$$

REMARQUE 1. — L'expression obtenue pour $\gamma(h)$ est en réalité une intégrale de Lebesgue. Si l'on désigne par $m(y)$ la mesure de l'ensemble des valeurs de y telles que $r(x)>y$, on a

$$\gamma(h)=\frac{1}{R}\int_{y>h}m(y)\,dy=\frac{1}{R}\int_h^\infty m(y)\,dy.$$

On voit que la forme de $\gamma(h)$ est directement liée à celle de $m(y)$, fonction non négative et non croissante. Si l'on se donne convenablement $\gamma(h)$, on en déduit $m(y)$, et il existe une infinité de fonctions $r(x)$ correspondant à une fonction $m(y)$ donnée. On a donc un moyen de construire de très nombreuses fonctions pseudo-aléatoires ayant une fonction de corrélation $\gamma(h)$ donnée. Voici un exemple.

Donnons-nous une fonction continue $r_1(x)$, croissante, variant de 0 à 1 lorsque x varie de 0 à $a<1$. Cherchons une fonction continue $r_2(x)$, croissante, variant de 0 à 1 lorsque x varie de a à 1, telle que la fonction $r(x)$ égale à $r_1(x)$ si $0<x<a$, à $r_2(x)$ si $a<x<1$, corresponde à une fonction $m(y)$ donnée (*fig.* 14).

Désignons par $\rho_1(y)$, $\rho_2(y)$ les fonctions inverses de r_1 et r_2. Ce sont des fonctions monotones définies pour $0<y<1$. On doit avoir

$$a-\rho_1(y)+1-\rho_2(y)=m(y),$$

d'où

$$\rho_2(y)=a+1-\rho_1(y)-m(y).$$

Si l'on se donne $\rho_1(y)$, $\rho_2(y)$ se trouve déterminée. Si l'on se donne pour $\gamma(h)$ une fonction pourvue d'une dérivée continue, on a alors

$$m(h)=-R\gamma'(h),$$

d'où

$$\rho_2(h) = a + 1 - \rho_1(h) + R\gamma'(h).$$

Si donc on se donne *arbitrairement* $r_1(x)$, on peut construire par ce procédé (qui n'est qu'un cas particulier) une fonction pseudo-aléatoire ayant $\gamma(h)$ comme fonction de corrélation.

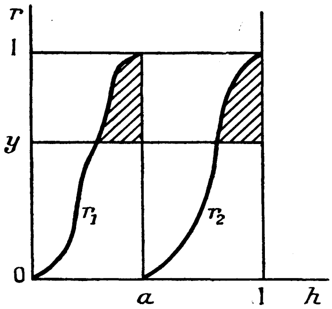


Fig. 14.

Remarque 2. — Pour une valeur fixée de x, la fonction égale à

$$r(x) - h \qquad \text{si} \quad h < r(x)$$

et à

$$0 \qquad \text{si} \quad h > r(x)$$

est une fonction de corrélation [nous l'avons rencontrée souvent lorsque $r(x) = 1$. Elle correspond à une fonction pseudo-aléatoire à base uniforme].

La fonction $\gamma(h)$ qui vient d'être construite est une somme de fonctions de ce type élémentaire. On vérifie ainsi qu'elle a bien la structure d'une fonction de corrélation.

20. Exemples

1° $r(x) = 1$. — On a alors $t_{n+1} - t_n = 1$. On retrouve le cas particulier déjà étudié à la section II (*fig.* 15).

On a bien

$$\gamma(h) = 1 - h \qquad \text{si} \quad h < 1,$$
$$= 0 \qquad \text{si} \quad h > 1.$$

2° $r(x) = x$ (*fig.* 16) :

$$\gamma(h) = (1 - h)^2 \qquad \text{si} \quad h < 1,$$
$$= 0 \qquad \text{si} \quad h > 1.$$

Les t_n se succèdent sur l'axe des t de telle sorte que $t_{n+1} - t_n = x_n$. Leur répartition est « pseudo-aléatoire pure ».

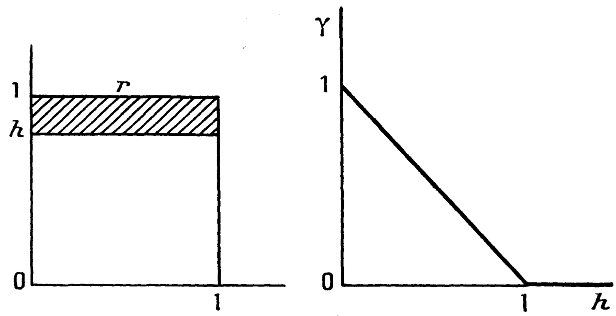


Fig. 15.

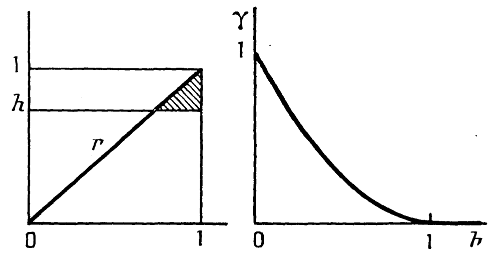


Fig. 16.

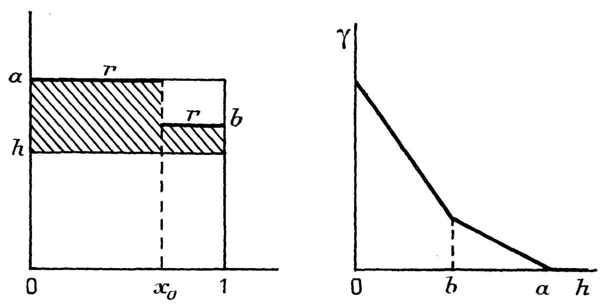


Fig. 17.

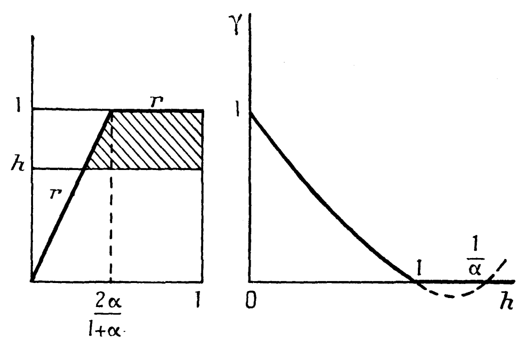


Fig. 18.

3°
$$r(x) = a \quad \text{si } 0 < x < x_0,$$
$$ = b \quad \text{si } x_0 < x < 1.$$

Suivant une loi pseudo-aléatoire, les intervalles successifs valent a ou b. La fonction de corrélation est représentée par une ligne brisée (*fig.* 17).

4°
$$r(x) = \frac{1+\alpha}{2\alpha}x \quad \text{si } x < \frac{2\alpha}{1+\alpha} \quad (0 < \alpha < 1),$$
$$= 1 \qquad \text{si } x > \frac{2\alpha}{1+\alpha},$$
$$\gamma(h) = 0 \qquad \text{si } h > 1,$$
$$= (1-h)(1-\alpha h) \qquad \text{si } h < 1.$$

On retrouve la fonction de corrélation de la fonction pseudo-aléatoire étudiée dans la section IV. Il ne s'agit d'ailleurs pas de la même fonction pseudo-aléatoire. L'ensemble des valeurs de t_n n'est pas ici la réunion de deux bases uniformes d'échelles différentes. Suivant une loi pseudo-aléatoire, les t_n se succèdent à intervalles constants ou à intervalles égaux à x_n, d'une façon très irrégulière (*fig.* 18).

21. Fonctions pseudo-aléatoires réelles. — Dans les conditions du théorème 21, les deux fonctions $f(t)$ et $\bar{f}(t)$ égales respectivement à $\exp[2i\pi\,\varphi(n)]$ et à $\exp[-2i\pi\,\varphi(n)]$ dans l'intervalle $t_n < t < t_{n+1}$ sont pseudo-aléatoires. Leur demi-somme est une fonction *réelle* $g(t)$ prenant la valeur
$$\cos 2\pi\,\varphi(n)$$
dans le même intervalle. Montrons que cette fonction est pseudo-aléatoire. [Un raisonnement analogue est valable pour $\sin 2\pi\,\varphi(n)$.] $g(t)$ a pour covariance la limite, pour $T \to \infty$, de

$$\frac{1}{4}\left[\frac{1}{T}\int_0^T \bar{f}(t)f(t+h)\,dt + \frac{1}{T}\int_0^T f(t)\bar{f}(t+h)\,dt\right]$$
$$+\frac{1}{4}\left[\frac{1}{T}\int_0^T f(t)f(t+h)\,dt + \frac{1}{T}\int_0^T \bar{f}(t)\bar{f}(t+h)\,dt\right].$$

Les termes de la première ligne donnent comme limite $\frac{1}{2}\gamma(h)$, où $\gamma(h)$ est la fonction de corrélation de $f(t)$. Montrons que

$$\lim_{T\to\infty}\frac{1}{T}\int_0^T f(t)f(t+h)\,dt = 0.$$

Il suffit de reprendre la démonstration du théorème 21, en écrivant partout f à la place de $\bar{f}$, et $+\varphi(n)$ à la place de $-\varphi(n)$. Le polynome $\varphi(n+p)+\varphi(n)$ a les mêmes propriétés que le polynome $\varphi(n+p)-\varphi(n)$, à cela près que, pour $p=0$, il ne disparaît pas, mais conserve la structure d'un polynome W. Donc les expressions qui interviennent à la fin de la démonstration du théorème 21 sont toutes nulles, même pour $p=0$, et la limite est nulle. Par suite :

Corollaire 6. — *Avec les hypothèses et les notations du théorème* 21, *les fonctions égales à* $\cos 2\pi\varphi(n)$ *et à* $\sin 2\pi\varphi(n)$ *lorsque* $t_n < t < t_{n+1}$ *sont pseudo-aléatoires et ont pour covariance* $\frac{1}{2}\gamma(h)$. *Ce sont des fonctions pseudo-aléatoires réelles.*

VI. — Résumé et conclusions.

Nous allons rassembler ici les principaux résultats obtenus. Nous avons défini diverses classes de fonctions pseudo-aléatoires, et nous avons calculé leurs fonctions de corrélation. Il s'agit dans tous les cas de fonctions pseudo-aléatoires discontinues, restant constantes dans des intervalles successifs $\delta_1, \delta_2, \ldots, \delta_n, \ldots$, et changeant brusquement de valeurs aux extrémités $t_1, t_2, \ldots, t_n, \ldots$ de ces intervalles. Leurs fonctions de corrélation $\gamma(h)$ s'annulent à partir d'une valeur finie de h. A cela près, leur structure est largement arbitraire, bien qu'elle résulte par des opérations simples de la fonction de corrélation élémentaire attachée à une base t_n uniforme.

Nous rappellerons, en outre, pour finir quelques résultats qui ont été démontrés dans une publication antérieure [3] et qui sont relatifs à des fonctions pseudo-aléatoires continues obtenues par régularisation (convolution) de fonctions pseudo-aléatoires à base uniforme.

Toutes ces fonctions pseudo-aléatoires sont construites à l'aide de suites uniformément denses, définies elles-mêmes par les parties décimales de polynômes. Ce sont ces suites qui introduisent l'irrégularité apparente et l'aspect aléatoire de la succession des valeurs. L'ensemble des résultats est donc assez cohérent. Mais il ne constitue pas une véritable théorie des fonctions pseudo-aléatoires. Il n'est d'ailleurs pas sûr que la définition des fonctions pseudo-aléatoires, qui ne fait en somme intervenir que leur structure au voisinage de l'infini, soit suffisamment complète pour permettre l'édification d'une telle théorie. La classe des fonctions pseudo-aléatoires semble plus étendue et plus difficile à qualifier que celle des fonctions presque périodiques, dont elle est en un certain sens la contrepartie.

Dans tout ce qui suit, nous utiliserons le polynôme

$$\varphi(t) = A_0 + A_1 t + \ldots + A_\nu t^\nu \qquad (\nu \geqq 2),$$

et nous supposerons que l'un au moins des coefficients $A_2, \ldots, A_\nu$ est irrationnel.

1° La fonction $f(t) = \exp[2i\pi\,\varphi(\hat{t})]$ est pseudo-aléatoire; elle a pour fonction de corrélation (*fig.* 19).

$$\begin{aligned} \gamma(h) &= 1 - h \qquad \text{si} \quad 0 \leqq h \leqq 1, \\ &= 0 \qquad\qquad \text{si} \quad h \geqq 1. \end{aligned}$$

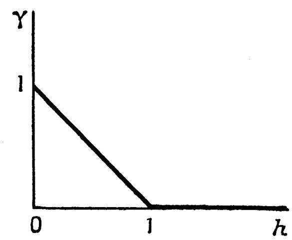


Fig. 19.

2° La fonction $f(t) = \exp\left[\dfrac{2i\pi}{m}\widehat{\varphi(\hat{t})}\right]$ (m entier $\geqq 2$) est pseudo-aléatoire; elle a pour fonction de corrélation

$$\begin{aligned} \gamma(h) &= 1 - h \qquad \text{si} \quad 0 \leqq h \leqq 1, \\ &= 0 \qquad\qquad \text{si} \quad h \geqq 1. \end{aligned}$$

3° Soit $g(t)$ une fonction presque périodique ou périodique de la forme

$$g(t) = \sum c_k \exp(2i\pi\omega_k t), \qquad \text{avec} \quad \sum |c_k| < \infty.$$

Si les différences $\omega_l - \omega_k$ ne sont jamais entières et si $\nu \geqq 3$, la fonction

$$\exp[2i\pi\,\varphi(\hat{t})]\,g(t)$$

est pseudo-aléatoire; elle a pour fonction de corrélation

$$\begin{aligned} \gamma(h) &= (1-h)\sum |c_k|^2 \exp(2i\pi\omega_k h) \qquad \text{si} \quad 0 \leqq h \leqq 1, \\ &= 0 \qquad\qquad\qquad\qquad\qquad\qquad\quad \text{si} \quad h \geqq 1. \end{aligned}$$

4° Soit $g(t)$ une fonction périodique de période 1, appartenant à $L^2(0, 1)$. Si $\nu \geqq 2$, la fonction

$$g(t)\exp[2i\pi\,\varphi(\hat{t})]$$

est pseudo-aléatoire; elle a pour fonction de corrélation

$$\gamma(h) = \int_0^{1-h} \bar{g}(\xi)\, g(\xi+h)\, d\xi \qquad \text{si} \quad 0 \leqq h \leqq 1,$$
$$= 0 \qquad \text{si} \quad h \geqq 1.$$

5° Soient

$$\varphi(t) = A_0 + \ldots + A_\nu t^\nu, \qquad \psi(t) = B_0 + \ldots + B_\nu t^\nu$$

deux polynomes de degré $\nu \geqq 2$. Soit α un nombre irrationnel. Si A et B sont irrationnels et si les nombres α, A, $B\alpha$, 1 ne sont pas liés par une

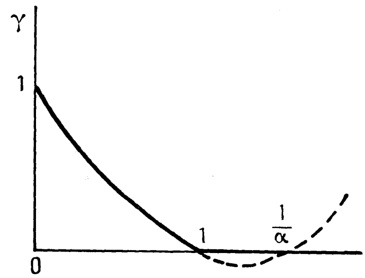


Fig. 20.

relation linéaire à coefficients entiers, la fonction

$$\exp\left\{ 2i\pi\left[\varphi(\hat{t}) + \psi\left(\widehat{\alpha t + \beta}\right)\right]\right\}$$

est pseudo-aléatoire. Elle a pour fonction de corrélation (*fig.* 20)

$$\gamma(h) = (1-h)(1-\alpha h) \qquad \text{si} \quad h \leqq \min\left(1, \frac{1}{\alpha}\right),$$
$$= 0 \qquad \text{si} \quad h \geqq \min\left(1, \frac{1}{\alpha}\right).$$

6° Si $\alpha = p/q$ est une fraction irréductible, et si A et B sont deux nombres irrationnels entre lesquels n'existe aucune relation linéaire à coefficients entiers, la fonction

$$\exp\left\{ 2i\pi\left[\varphi(\hat{t}) + \psi\left(\widehat{\alpha t + \beta}\right)\right]\right\}$$

est pseudo-aléatoire; elle a pour fonction de corrélation

$$\gamma(h) = (1-h)(1-\alpha h) + \frac{1}{pq}\underbrace{p - ph}\left(1 - \underbrace{p - ph}\right)$$
$$- \frac{1}{pq}\min\left(\underbrace{p-ph},\ 1 - \underbrace{p-ph},\ \underbrace{q\beta},\ 1 - \underbrace{q\beta}\right) \qquad \text{si} \quad h \leqq \min\left(1, \frac{1}{\alpha}\right),$$
$$= 0 \qquad \text{si} \quad h \geqq \min\left(1, \frac{1}{\alpha}\right).$$

$\gamma(h)$ est représentée par une ligne polygonale.

7° Si $\varphi(t)$ est un polynome de degré $\nu \geqq 3$, si A_ν est irrationnel, et si $\beta \geqq 1$, la fonction

$$\exp\left\{2i\pi\left[\varphi\left(\widehat{t+\beta}\right) - \varphi(\hat{t})\right]\right\}$$

est pseudo-aléatoire; elle a pour fonction de corrélation

$$\begin{aligned}\gamma(h) &= 1 - h - \min(h, 1-h, \check{\beta}, 1-\check{\beta}) &\quad \text{si} \quad 0 \leqq h \leqq 1,\\ &= 0 &\quad \text{si} \quad h \geqq 1,\end{aligned}$$

$\gamma(h)$ est représentée par une ligne polygonale.

8° Soit $\varphi(t)$ un polynome de degré $\geqq 2$. Soit $\psi(t)$ un polynome de degré $\geqq 1$. On suppose que la suite $\varphi(n)$, $\psi(n)$ est uniformément dense mod 1

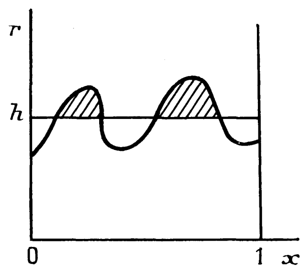


Fig. 21.

dans le carré fondamental. Soit $r(x)$ une fonction bornée, non négative, intégrable sur $(0, 1)$. La fonction $f(t)$ égale à

$$\exp[2i\pi\,\varphi(n)] \quad \text{si} \quad t_n < t < t_{n+1}, \qquad \text{avec} \quad t_{n+1} - t_n = r\left[\widecheck{\psi(n)}\right]$$

est pseudo-aléatoire; elle a pour fonction de corrélation (*fig.* 21)

$$\begin{aligned}\gamma(h) &= \frac{1}{R}\int_{r(x)-h>0} [r(x) - h]\,dx &\quad \text{si} \quad h < \sup r(x),\\ &= 0 &\quad \text{si} \quad h > \sup r(x),\end{aligned}$$

avec

$$R = \int_0^1 r(x)\,dx.$$

9° Soit $f(t)$ une fonction pseudo-aléatoire quelconque. Soit $s(\lambda)$ une fonction complexe de la variable réelle λ, telle que

$$\int_{-\infty}^{\infty} |s(\lambda)|\,d\lambda < \infty.$$

Désignons par $\gamma_f(h)$ la fonction de corrélation de $f(t)$. A $f(t)$ faisons correspondre la fonction

$$g(t) = \int_{-\infty}^{\infty} f(\lambda)\, s(t-\lambda)\, d\lambda = f(t) * s(t),$$

où $*$ est le symbole de la convolution.

$g(t)$ est pseudo-aléatoire; elle a pour fonction de corrélation

$$\gamma_g(h) = \gamma_f(h) * \Gamma(h),$$

avec

$$\Gamma(h) = \bar{s}(-h) * s(h).$$

BIBLIOGRAPHIE.

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

[2] Bass (Jean). — *Fonctions pseudo-aléatoires et fonctions de Wiener* (*C. R. Acad. Sc.*, 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.*, t. 37, 1958, p. 173-205).

[4] Bass (J.) et Bertrandias (J.-P.). — *Moyennes de sommes trigonométriques et fonctions d'autocorrélation* (*C. R. Acad. Sc.*, t. 245, 1957, p. 2457-2459).

[5] Bass (J.) et Kree (P.). — *Sur les fonctions pseudo-aléatoires* (*C. R. Acad. Sc.*, t. 247, 1958, p. 1083-1085).

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

[7] Cassels (J. W. S.). — *An introduction to diophantine approximation*, Cambridge, University Press, 1957 (*Cambridge Tracts in Mathematics and mathematical Physics*, 45).

[8] Kampé de Fériet (Joseph). — *Les fonctions aléatoires stationnaires et la théorie statistique de la turbulence homogène* (*Ann. Soc. scient. Bruxelles*, série 1, t. 59, 1939, p. 145-210).

[9] Van der Corput (J. G.). — *Diophantische Ungleichungen;* I. *Zur Gleichverteilung modulo Eins* (*Acta Math.*, t. 56, 1931, p. 373-456).

[10] Weyl (Hermann). — *Ueber die Gleichverteilung von Zahlen modulo Eins* (*Math. Annalen*, t. 77, 1916, p. 313-352).

[11] Wiener (Norbert). — *Generalized harmonic anolysis* (*Acta Math.*, t. 55, 1930, p. 117-258).

(Manuscrit reçu le 19 janvier 1959.)

Jean Bass,
24, rue Ferdinand-Jamin
Bourg-la-Reine (Seine).