数理解析研究所講究録 1240 巻 2001 年 152-160



# On pseudorandom functions

神戸大理 福山 克司

(Katusi Fukuyama, Kobe University)

## 0. 擬似乱函数の概念

$\mathbf{R}$ 上の函数 $f$ が擬似乱函数 (pseudorandom function) であるとは極限

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

が全ての $s$ に対して存在し、なおかつこの $\gamma$ が

$$\gamma(0)\neq 0,\qquad \lim_{s\to\infty}\gamma(s)$$

をみたすものとして定義される。この概念は R. Bass [1] により、"non-probabilistic theory of turbulence" の理論を展開するために導入された。

もし半直線 $[0,\infty)$ をその上の (実際には存在しない架空の) 平坦な測度のもとで確率空間とみなしたとすると、この擬似乱函数という概念は、$s$ が大きくなる時の確率変数 $f$ とそのずらし $f(\cdot+s)$ の の漸近独立性と思える。

この架空の確率空間の上の確率変数の分布函数にあたる概念が漸近分布函数 (asymptotic distribution function) である。擬似乱函数 $f$ の 漸近分布函数 $F$ は

$$F(a)=\lim_{T\to\infty}\frac{1}{T}|\{s\in[0,T]:f(t)\leq a\}|$$

と極限が存在する時にのみ定義される。ここで $|\cdot|$ は Lebesgue 測度である。

擬似乱函数という概念は数値解析のために導入されたのものである以上それを効率よく生成する具体的な方法を与えることは重要である。しかも、確率数値解析の立場からは漸近分布函数が Gauss 分布の分布函数であるよう

なものが望ましい。そのような観点から P. P. Hien [4] と小川重義 [5] は以下のような生成法を与えた。

まず数列 $\mathbf{z}=\{z_n\}\in[0,1]^{\mathbf{N}}$ と、$\mathbf{R}$ 上の $L^2$ 函数 $K$, そして以下の条件をみたす $[0,1]$ 上の函数 $h$ を用意する。

$$\text{(1)}\qquad \int_0^1 h(t)\,dt=0,\qquad \int_0^1 h^2(t)\,dt<\infty$$

$\mathbf{R}$ 上の函数 $q(\cdot\,,\mathbf{z})$ を

$$q(t,\mathbf{z})=\mathbf{1}_{[0,\infty)}(t)h(z_{[t]})$$

と定め、パラメーター $\lambda>0$ を用いてその変形 $q_\lambda(t,\mathbf{z})=\sqrt{\lambda}\,q(\lambda t,\mathbf{z})$ を作り、これと $K$ との convolution

$$Q_\lambda^K(t,\mathbf{z})=\int_{-\infty}^{\infty}K(s)q_\lambda(t-s,\mathbf{z})\,ds$$

を作る。

Hien [4] の結果は $\mathbf{z}$ が完全一様分布数列 (completely uniformly distributed) であるならば $Q_\lambda^K(\cdot\,,\mathbf{z})$ は擬似乱函数であり、その漸近分布函数は $\lambda\to\infty$ とした時に Gauss 分布の分布函数に近付くというものである。

この結果は非常に簡単なフレームワークで漸近分布函数が Gauss 分布函数に近い擬似乱函数を生成するという利点はあるが、完全一様分布数列を用意するという難題が課せられている。この点を改善したのが小川 [5] の結果である。これは $\mathbf{z}$ が ergodic な変換で生成された一様分布数列であることの他は $\mathbf{z}$ に何らの仮定をおかない。$h$, $K$ や $\mathbf{z}$ を生成する変換にはある種の仮定をおくがそれもほぼ通常の仮定であって、実用上は全く問題にならないものである。

## 1. 小川による擬似乱函数の構成

以下小川の結果を変形した形で紹介する。そのためには漸近分布函数の背後にある漸近分布の概念を導入すると都合がよいので、まずそれから取り掛かろう。

$\mathbf{R}^n$-値函数 $(f_1, \ldots, f_n)$ を確率空間 $([0,T], dt/T)$ 上の確率変数と思った時の分布が $T \to \infty$ とした時に $\mathbf{R}^n$ 上の確率測度 $\mu$ に弱収束する時に $\mu$ は $(f_1, \ldots, f_n)$ の漸近分布であるという。即ち

$$\lim_{T\to\infty} \frac{1}{T} \int_0^T g(f_1(t), \ldots, f_n(t))\, dt = \int_{\mathbf{R}^n} g(x)\, \mu(dx), \quad (g \in \mathrm{C_b}(\mathbf{R}^n)),$$

が成立することとするわけである。ここで $\mathrm{C_b}(\mathbf{R}^n)$ は $\mathbf{R}^n$ 上の有界連続函数全体を表すこととする。

そして函数の族 $\{f_\pi\}_{\pi\in\Pi}$ の任意の有限系の漸近分布が $\mathbf{R}^\Pi$ 上の確率測度 $\mu$ の対応する marginal distribution である時、$\mu$ を $\{f_\pi\}_{\pi\in\Pi}$ の漸近分布と呼ぶ。

さて小川の定理を変形した形で述べる。$G$ は $([0,1], \mathcal{B}, d\omega)$ 上のエルゴード的な変換で $[0,1]$ 上の函数と見てほとんど至るところ連続なものとする。$h$ は $[0,1]$ 上ほとんど至るところ連続な函数で (1) をみたすものとする。そして和 $\sum h(G^k\omega)$ が函数型中心極限定理をみたすことを仮定する。即ち $D$-値確率変数

$$X_n(t,\omega) = \frac{1}{\sqrt{n}} \sum_{k=1}^{[nt]} h(G^k\omega)$$

が $\sigma B(t)$ に法則収束するとする。ここで $\sigma > 0$ であり、$B(t)$ は標準ブラウン運動を表すとする。$K$ は台がコンパクトで $[0,\infty)$ に含まれる有界変動函数であるとする。即ち $K \in \mathrm{BV_c}[0,\infty)$. そして $x \in [0,1]$ に対して $\mathbf{z}_x = \{G^j x\}$ とおく。エルゴード定理によれば

$$\Omega_0 = \{\, x \in [0,1] \mid \mathbf{z}_x \text{ は単位区間上の一様分布数列 } \}$$

は測度 1 の集合になる。

**定理 1.** 任意の $x_0 \in \Omega_0$ に対して函数系 $\{ Q_\lambda^K(t, \mathbf{z}_{x_0}) : K \in \mathrm{BV_c}[0,\infty) \}$ の漸近分布は、確率空間 $([0,1]\times[0,1], dt\,dx)$ 上での

$$\{ Q_\lambda^K(t, \mathbf{z}_x) : K \in \mathrm{BV_c}[0,\infty) \}$$

の分布に等しい。さらに $\lambda \to \infty$ とすると確率積分で与えられる Gauss 系

$$\left\{ \sigma \int_0^\infty K(s)\, dB(s) \;\middle|\; K \in \mathrm{BV_c}[0,\infty) \right\}$$

の分布に収束する。

$G_K = \sigma \int_0^\infty K(s)\, dB(s)$ と記すことにすればこの Gauss 系は $EG_K = 0$, $EG_{K_1} G_{K_2} = \sigma^2 \int K_1 K_2$ で特徴づけられるものである。特に $K_1$, $K_2$, ... が直交列であれば $G_{K_1}$, $G_{K_2}$, ... は独立列となり、$Q_\lambda^{K_1}(t, \mathbf{z}_{x_0})$, $Q_\lambda^{K_2}(t, \mathbf{z}_{x_0})$, ... は漸近的に独立ということになる。すなわち、仮定をみたす $\mathbf{z}_{x_0}$ をひとつ用意するだけで、独立に近い擬似乱函数の列を生成できることになる。

この定理の小川による証明はかなりの計算を要する複雑なものであったが、この小論では [3] にある部分積分を用いた簡単な証明を紹介する。

ところで、$G$ が二進変換の時には $K$ の属する範囲をさらに広げ上記定理中の $\mathrm{BV_c}[0,\infty)$ を全て $L_c^2[0,\infty)$ と書き換えても定理は成立することを注意しておこう。このことの証明は間隙函数の極限定理の研究手法によって示され、後で紹介する定理 1 の証明とは大きく異なる。

**2.** 安定分布と擬似乱函数

前節までの結果は Gauss 分布を漸近分布に持つ擬似乱函数の構成であったが、安定分布を漸近分布に持つものも重要であると思われる。Hien による Gauss 場合の構成のアイディアを用いると安定分布を漸近分布に持つものを構成することができることがわかる。以下これについて述べよう。

まず $X(t)$ は対称安定加法過程とする。我々は $h$ は $[0,1]$ 上でほとんど至る所連続であるとし、$h$ の確率空間 $([0,1], dt)$ 上での分布が $X(1)$ の分布の牽引域 (domain of attraction) に入っているとする。即ち、$h$ と同分布になる独立確率変数列 $Y_1, Y_2, \ldots$ に対して $(Y_1 + \cdots + Y_n)/A_n$ が $X(1)$ に法則収束するような正数列 $A_n$ が存在することを仮定するわけである。以下この $A_n$ を用いて $q_\lambda(t, \mathbf{z}) = \lambda q(\lambda t, \mathbf{z})/A_{[\lambda]}$ とおき、$Q_\lambda^K$ を前と同様に定める。

**定理 2.** 数列 $\mathbf{z}_0$ は $[0,1]$ 上で完全一様分布するとする。そのとき函数系 $\{ Q_\lambda^K(t, \mathbf{z}_0) : K \in BV_c[0,\infty) \}$ の漸近分布は $\{ Q_\lambda^K(t, \mathbf{z}) : K \in BV_c[0,\infty) \}$ の確率空間 $([0,1] \times [0,1]^{\mathbf{N}}, dt\, d\mathbf{z})$ 上での分布に等しく $\lambda \to \infty$ とすると安定確率積分で与えられる系

$$\left\{ \int_0^\infty K(t)\, dX(t) : K \in \mathrm{BV_c}[0,\infty) \right\}$$

の分布に収束する。

もし $K_1, \ldots, K_n$ の台が互いに素なら漸近分布の極限分布は独立になっている。よってこのようにして得られる擬似乱函数は十分大きく shift してやるともとの函数と漸近的に独立になるというわけである。じつは $h$ には最早可積分性を望むことはできないので、Bass の意味での擬似乱函数にはなっていないわけだが、上に述べた「shift が独立にする」という原初のイメージは保たれているので、これを持って擬似乱函数と呼び慣わしても言葉の乱用というにはあたらないであろう。

**3.** 証明のあらすじ

定理1を示す。まず一次元分布の収束を示す。$K$ の台は $(0, L_0)$ に含まれているとし、$f \in C_b(\mathbf{R})$ は任意とする。$a_t = L_0 + t/\lambda$ とおく。$t \geq L_0$ の時には

$$Q_\lambda^K(t, \mathbf{z}) = \sqrt{\lambda} \int_0^{L_0} K(s) h(z_{[\lambda(t-s)]})\, ds$$

と書き表すことができるので、$\theta$ で $\mathbf{N}$ 上での shift 作用素 $\theta\{z_k\} = \{z_{k+1}\}$ を表すとすると、

$$Q_\lambda^K(t + 1/\lambda, \mathbf{z}) = Q_\lambda^K(t, \theta\mathbf{z}),$$

という基本的な関係が得られる。ここで区間 $[0, a_n]$ を $[0, a_1], [a_1, a_2], \ldots$ に分解し、各々の上で変数変換を行えば結局

$$\frac{1}{a_n} \int_0^{a_n} f(Q_\lambda^K(t, \mathbf{z}))\, dt = \frac{1}{a_n} \sum_{k=0}^{n-1} \int_{a_0}^{a_1} f(Q_\lambda^K(t, \theta^k \mathbf{z}))\, dt + o(1)$$

が得られる。ここで

$$R_\lambda(\mathbf{z}) = \int_{a_0}^{a_1} f(Q_\lambda^K(t, \mathbf{z}))\, dt = \frac{1}{\lambda} \int_0^1 f(Q_\lambda^K(a_t, \mathbf{z}))\, dt, \quad R_{\lambda,G}(x) = R_\lambda(\mathbf{z}_x)$$

とかくことにしよう。$h$, $G$ はほとんど至る所連続なので、$R_{\lambda,G}$ は $x$ に関してほとんど至る所連続で有界であり、したがって Riemann 可積分である。ゆえに $\mathbf{z}_{x_0}$ の一様分布性より、

$$\frac{1}{a_n} \int_0^{a_n} f(Q_\lambda^K(t, \mathbf{z}_{x_0}))\, dt = \frac{1}{a_n} \sum_{k=0}^{n-1} R_{\lambda,G}(G^k x_0) + o(1) \to \lambda \int_0^1 R_{\lambda,G}(x)\, dx$$

が導かれる。それゆえ結局

$$\lim_{L \to \infty} \frac{1}{L} \int_0^L f(Q_\lambda^K(t, \mathbf{z}_{x_0}))\, dt = \int_0^1 dx \int_0^1 f(Q_\lambda^K(a_t, \mathbf{z}_x))\, dt$$

が示されたことになる。$K$ は有界変動であるから、右連続で、左極限が各点で存在する version を取って以下議論する。$K(s)=\nu((-\infty,s])$ となるような符合つき測度 $\nu$ が存在する。部分積分を行えば

$$Q_\lambda^K(a_t,\mathbf{z})=-\int_0^{L_0}\left(\int_0^s q_\lambda^K(a_t-u,\mathbf{z})\,du\right)d\nu(s)$$

が得られる。ここで $s\in[0,L_0]$、$t\in[0,1]$ に対しては

$$\int_0^s q_\lambda(a_t-u,\mathbf{z}_x)\,du=\frac{1}{\sqrt{\lambda}}\sum_{k=[(L_0-s)\lambda+1]}^{[L_0\lambda]}h(G^kx)+o(1)\quad\text{as}\quad\lambda\to 0$$

が $s,t$ について一様な $o(1)$ に対して成り立つので、函数型中心極限定理によれば、$D$ での法則収束

$$\int_0^s q_\lambda(a_t-u,\mathbf{z}_x)\,du\xrightarrow{\mathcal{D}}\sigma\{B(L_0)-B(L_0-s)\}$$

を得る。汎函数 $f\mapsto\int_0^{L_0}f(u)\,d\nu(u)$ の $D$ での不連続点集合は $\sigma\{B(L_0)-B(L_0-s)\}$ の法則に関して零集合であるので、[2] の定理 5.1 を適用すれば

$$\begin{aligned}Q_\lambda^K(a_t,\mathbf{z}_x)&\xrightarrow{\mathcal{D}}-\int_0^{L_0}\sigma\{B(L_0)-B(L_0-s)\}\,d\nu(s)\\&=\sigma\int_0^{L_0}K(s)\,dB(s).\end{aligned}$$

が得られる。これで一次元分布の収束は示された。

最後に有限次元分布の収束を示そう。任意の $K_1,\ldots,K_n\in\mathrm{BV_c}$ と $\beta_1,\ldots,\beta_n\in\mathbf{R}$ に対して $K=\beta_1K_1+\cdots+\beta_nK_n$ とおけば $\beta_1Q_\lambda^{K_1}(t,\mathbf{z}_x)+\cdots+Q_\lambda^{K_n}(t,\mathbf{z}_x)=Q_\lambda^K(t,\mathbf{z}_x)$ が成り立っているので、今示したことより、$Q_\lambda^{K_1}(a_t,\mathbf{z}_{x_0}),\ldots,Q_\lambda^{K_n}(a_t,\mathbf{z}_{x_0})$ の線形結合の $([0,T],dt/T)$ 上での分布は $([0,1]^2,dt\,dx)$ 上での $Q_\lambda^{K_1}(t,\mathbf{z}_x),\ldots,Q_\lambda^{K_n}(t,\mathbf{z}_x)$ の線形結合の分布に収束

している。しかも、後者は $\sigma\int_0^{L_0} K_1(s)\,dB(s), \ldots, \sigma\int_0^{L_0} K_n(s)\,dB(s)$ の線形結合の分布に収束している。Cramér-Wold ([2] Theorem 7.7) の定理を用いればこれで有限次元分布の収束が示されたことがわかる。■

定理2の証明の概略を紹介する。$t$ が与えられると $q_\lambda(t,\mathbf{z})$ は $z_{[\lambda t]}$, にのみ依存する函数になり、よって $Q_\lambda^K(t,\mathbf{z})$ は $z_0, \ldots, z_{[\lambda(t)]}$ にのみ依存する函数である。故に $b_\lambda = [L_0\lambda + 1]$ とおくと $R_\lambda(\mathbf{z})$ は $z_0, \ldots, z_{[\lambda(a_1)]} = z_{b_\lambda}$ の函数とみなせる。この函数は $I_\lambda = [0,1]^{b_\lambda+1}$ 上で有界でほとんど至る所連続なので、Riemann 可積分となる。故に $\mathbf{z}_0$ が完全一様分布列であることを用いれば

$$\frac{1}{n}\sum_{k=0}^{n-1} R_\lambda(\theta^k\mathbf{z}_0) \to \int_{I_\lambda} R_\lambda(z_0,\ldots,z_{b_\lambda})\,dz_0\ldots dz_{b_\lambda} = \int_{I_\infty} R_\lambda(\mathbf{x})\,d\mathbf{x}$$

が得られる。ここで、最後の積分は $I_\infty = [0,1]^{\mathbf{N}}$ 上での Lebesgue 測度の可算直積 $d\mathbf{x} = dx_1\,dx_2\ldots$ についての積分である。ここで

$$\int_0^s q_\lambda(a_t - u, \mathbf{x})\,du = \frac{1}{A_{[\lambda]}} \sum_{k=[(L_0-s)\lambda+1]}^{[L_0\lambda]} h(x_i) + o(1) \quad \text{as} \quad \lambda \to 0,$$

であり、しかも $\{h(x_i)\}$ は $(I_\infty, d\mathbf{x})$ 上で同分布独立確率変数列となり、その法則は $X(1)$ の法則の牽引域にあるので、函数型極限定理より、$D$ 空間での法則収束

$$\int_0^s q_\lambda(a_t - u, \mathbf{x})\,du \xrightarrow{\mathcal{D}} X(L_0) - X(L_0 - s)$$

が得られる。$X$ は確率連続なので、残りの証明は定理1の場合と全く同様に進めることができる。

参考文献

[1] J. Bass, Stationary Functions and Their Applications t
Turbulence, 1. Stationary Functions, *J. Math. Anal.*
354–399.

[2] P. Billingsley, Convergence of Probability Measures, J
York, 1968.

[3] K. Fukuyama and T. Tomokuni, On the asymptotic dist
dorandom functions, Monte Carlo Methods and Applicat
2000.

[4] P. P. Hien, Fonction admettantt une répartition asymptot
*C. R. Acad. Sci. Paris. Ser. A*, **267** (1968) 803–806.

[5] S. Ogawa, Pseudorandom functions whose asymptotic c
asymptotically gaussian, *J. Math. Anal. Appl.*, **158** (199