On pseudorandom functions

Katusi FUKUYAMA
Department of Mathematics, Kobe University
Rokko, Kobe, 657-8501 Japan
fukuyama@math.kobe-u.ac.jp

1 Introduction

In the non-probabilistic theory of turbulence, J. Bass [1] introduced the notion of ‘pseudorandom functions’. A function on \( \mathbb{R} \) is said to be pseudorandom if

\[
\gamma_f(s) = \lim_{T \to \infty} \frac{1}{T} \int_0^T f(t)f(t + s) \, dt \quad \text{exists for all} \quad s,
\]

\[
\gamma_f(0) \neq 0, \quad \text{and} \quad \lim_{s \to \infty} \gamma_f(s) = 0.
\]

If we consider \( \mathbb{R} \) as a probability space with a flat probability measure on \([0, \infty)\), which does not actually exist, and if we regard functions on \( R \) as random variables on this probability space, the notion of pseudorandomness can be interpreted as asymptotic independence among \( f \) and its shift \( f(\cdot + a) \).

Let us consider the joint distribution of functions \( f_1, \ldots, f_n \) on this probability space in the following way: We say that a probability measure \( \mu \) on \( \mathbb{R}^n \) is the asymptotic distribution of \( \mathbb{R}^n \)-valued function \( (f_1, \ldots, f_n) \) on \( \mathbb{R} \) if the distribution of \( (f_1, \ldots, f_n) \) on the probability space \( ([0,T], dt/T) \) converges to \( \mu \) as \( T \to \infty \), i.e.,

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

(1)

where \( C_b(\mathbb{R}^n) \) denotes the set of bounded continuous functions on \( \mathbb{R}^n \). We say that a probability measure \( \mu \) on \( \mathbb{R}^n \) is the asymptotic distribution of the system \( \{ f_\pi \}_{\pi \in \Pi} \) of functions on \( \mathbb{R} \), if the asymptotic distribution of any finite subset of the system equals to the marginal distribution of \( \mu \).

Since it is introduced for the numerical analysis, it is important to give a concrete and efficient way to generate pseudorandom functions with

For a sequence \( z_\lambda = \{z_n\} \in [0,1]^N \) and a function \( h \) on \([0,1]\) with

\[
\int_0^1 h(t) \, dt = 0 \quad \text{and} \quad \int_0^1 h^2(t) \, dt < \infty,
\]

(2)

put

\[
q(t,z) = 1_{[0,\infty)}(t)h(z(t)), \quad q_\lambda(t,z) = \sqrt{\lambda} q(\lambda t, z), \quad \text{and}
\]

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

by using suitable function \( K \). Then \( Q_\lambda^K(t,z) \) is a pseudorandom function with Gaussian asymptotic distribution function, if \( z \) is completely uniformly distributed (Hien [4]), or if \( z \) is a uniformly distributed sequence generated by an ergodic transform on \([0,1]\) (Ogawa [5]).

Let us now state a version of Ogawa’s theorem. Suppose that \( G \) is an ergodic transform on Lebesgue probability space \(([0,1], \mathcal{B}, d\omega)\), which is continuous a.e., and \( h \) is an a.e. continuous function on \([0,1]\) with (2) such that the functional central limit theorem holds for sum \( \sum h(G^k\omega) \), i.e., \( D \)-valued random variables \( X_n(t,\omega) = \sum_{k=1}^{[nt]} h(G^k\omega)/\sqrt{n} \) converges in law to \( \sigma B(t) \), where \( B(t) \) denotes the standard Brownian motion. Let \( K \in \mathcal{B}_c \), where \( \mathcal{B}_c \) denotes the class of functions of bounded variation with compact support. Let us put \( z_x = \{G^jx\} \) for \( x \in [0,1] \). Thanks to ergodic theorem, the set \( \Omega_0 = \{ x \in [0,1] \mid z_x \text{ is uniformly distributed over } [0,1] \} \) has full measure.

**Theorem 1.1** For arbitrary \( x_0 \in \Omega_0 \), the asymptotic distribution of the system \( \{ Q_\lambda^K(t,z_{x_0}) : K \in \mathcal{B}_c \} \) equals to the distribution of \( \{ Q_\lambda^K(t,z_x) : K \in \mathcal{B}_c \} \) on the probability space \(([0,1] \times [0,1], dt \, dx)\). As \( \lambda \to \infty \), it converges to the law of the Gaussian system \( \{ G^K : K \in B \} \) with \( EG^K = 0 \) and \( EG^KG^L = \sigma^2 \int KL \).

If \( K_1, K_2, \ldots \) are orthogonal, then \( G_{K_1}, G_{K_2}, \ldots \) are independent, and hence \( Q_\lambda^{K_1}(t,z_{x_0}), Q_\lambda^{K_2}(t,z_{x_0}), \ldots \) are asymptotically nearly independent. Thus we can generate nearly independent sequence of pseudorandom function from one source \( z_{x_0} \).
When $G$ is a binary transform $x \to 2x - \lfloor x \rfloor$, we can drastically relax the condition on $K$ and $h$ as below. Let $L^2_c$ denote the class of square integrable functions with compact support.

**Theorem 1.2** Let $G$ be the binary transform. Assume that $h$ is a.e. continuous function on $[0,1]$ with (2) and the $L^2$-Dini continuity below:

$$\int_0^1 \frac{\|h(\cdot + \delta) - h(\cdot)\|_2}{\delta} d\delta < \infty.$$  

Then, for arbitrary $x_0 \in \Omega_0$, the asymptotic distribution of the system $\{Q^K(t, z_{x_0}) : K \in L^2_c\}$ equals to the distribution of $\{Q^K(t, z) : K \in L^2_c\}$ on the probability space $([0,1] \times [0,1], dt \, dx)$. As $\lambda \to \infty$, it converges to the law of the Gaussian system $\{G^K : K \in L^2_c\}$ with $EG^K = 0$ and $EG^K G^L = \sigma^2 \int KL$.

Now let us state the third theorem which extends the result by Hien. Let $X(t)$ be a symmetric stable Lévy process. Let us assume that the function $h$ is a.e. continuous and the law of $h$ on $([0,1], dt)$ belongs to the domain of attraction of $X(1)$, i.e., for i.i.d. $Y_1, Y_2, \ldots$, with $Y_1 \sim h$, there exists $A_n$ such that $(Y_1 + \cdots + Y_n)/A_n$ converges in law to $U$. From now on we put $q_\lambda(t, z) = \lambda q(\lambda t, z)/A_\lambda$ and define $Q^K$ as before. Denote by $BV_c[0, \infty)$ the collection of function of bounded variation with compact support included by $[0, \infty)$.

**Theorem 1.3** If $z$ is completely uniformly distributed over $[0,1]$, then the asymptotic distribution of the system $\{Q^K(t, z) : K \in BV_c[0, \infty)\}$ equals the distribution of the system $\{Q^K(t, z) : K \in BV_c[0, \infty)\}$ on the probability space $([0,1] \times [0,1], dt \, dx)$. As $\lambda \to \infty$, it converges to the law of $\{\int_0^\infty K(t) \, dX(t) : K \in BV_c[0, \infty)\}$, which is a system of symmetric stable random variables.

Thus, disjointness of supports of $K$’s implies independence of the limit distribution, and hence the sequence of functions are asymptotically nearly independent. In this case, since $h$ is not square integrable, and thereby the functions are not pseudorandom, but in the above sense, it is nearly independent of the shifted function, and hence roughly considered to be ‘pseudorandom’.
References


**RESUME**

On considère des fonctions réelles $f$ telles que

$$
\lim_{T \to \infty} \frac{1}{T} \int_0^T g(f(t)) \, dt = \int_{\mathbb{R}} g(x) \mu(dx)
$$

existe, pour toute $g$ continue et bornée. On construit des systèmes des fonctions telles que des systèmes des mesures $\mu$ sont asymptotiquement gaussien ou stable.