KYBERNETIKA — VOLUME 8 (1972), NUMBER 6

A Note on Generation of Sequences of Pseudorandom Numbers with Prescribed Autocorrelation Coefficients

JAROSLAV KRÁL

In many applications (for example if the effect of an filtering of a random process is tested) a sequence of pseudorandom numbers with a prescribed autocorrelation function must be generated. In the paper a method is discussed allowing to generate sequences of pseudorandom numbers with a autocorrelation function near the autocorrelation function of the white noise after the filtering by an filter with the transfer function $F(p)$. The white noise is approximated on a digital computer by a telegraph signal S. On S some integral transformation is applied. The experimental results show, that the generated autocorrelation coefficients have the values near to the expected ones. The discussed method allows to generate pseudorandom sequences having a great number of nonzero autocorrelation coefficients.

Let $P_\mu = \{X(t) \mid t \geqq 0\}$ be an ergodic (Gaussian) process with the (tridiagonal) correlation function $R_\mu(\tau)$, $R_\mu(\tau) = |1 - |\tau|/\mu|$ for $|\tau| \leqq \mu$, $R_\mu(\tau) = 0$ elsewhere. Let $x(t)$ be a realization of the process P_μ. Let $F(p)$ be the transfer function of a filter F and $\tilde{P}_\mu$ the process P_μ after the filtration by F and $\tilde{x}(t)$ the filtered realization $x(t)$ of P_μ. If we put $x(t) \equiv 0$ for $t < 0$ then

$$(1) \qquad \tilde{x}(t) = \int_0^t x(\tau)\, q(t - \tau)\, \mathrm{d}\tau\,,$$

where

$$q(u) = c \int_{u-\mathrm{i}\infty}^{u+\mathrm{i}\infty} F(z)\, \mathrm{e}^{pz}\, \mathrm{d}z\,,$$

$c = 1/2\pi\mathrm{i}$, $\mathrm{i} = \sqrt{-1}$. Let for $t \geqq 0$ $|q(t)| \leqq \mathrm{e}^{-at}$, $a > 0$, (this assumption is not too limitting) and with the probability one $|x(t)| \leqq M$, M is an appropriate constant. Then to every $\varepsilon > 0$ there is a $t_0 > 0$ such that for $t > t_0$

$$(2) \qquad \left|\tilde{x}(t) - \int_{t-t_0}^{t} x(\tau)\, q(t - \tau)\, \mathrm{d}\tau\right| < \varepsilon\,.$$

It obviously suffices to choose t_0 such that it holds

$$\varepsilon \geqq \left|M \int_{t_0}^{\infty} \mathrm{e}^{-at}\,\mathrm{d}t\right| . \tag{3}$$

For sufficiently small μ P_μ can be assumed to be a good approximation of the white noise. For the autocorrelation function $\tilde{R}_\mu$ of the proces $\tilde{P}_\mu$ then it holds approximately (see [2] or [3])

$$\tilde{R}_\mu(\tau) = \frac{c}{2\pi} \int_{-\infty}^{+\infty} |F(\mathrm{i}\omega)|^2\, \mathrm{e}^{\mathrm{i}\omega\tau}\,\mathrm{d}\omega \tag{4}$$

where as above $\mathrm{i} = \sqrt{-1}$.

We shall use the identity (4) in designing of a pseudorandom generator.

The main problem is how to represent a continuous phenomena on a discrete device.

Let us consider a random process $P_1 = \{Z(t), t \geqq 0\}$ of the following properties. Every realization $z(t)$ of P_1 is a stepwise function with discontinuity points $0, b_0, b_1, b_2, \ldots$. Let for $i = 1,2,3, \ldots$ a_i be the value of $z(t)$ on (b_{i-1}, b_i). Let for $i = 1, 2, \ldots$ $(b_i - b_{i-1})$ be independent random variables uniformly distributed on $(0, \mu)$ and $a_1, a_2, \ldots, a_n, \ldots$ independent random variables with the distribution function $F(x)$,

$$F(x) = 0 \quad \text{for} \quad x < -1\,, \quad F(x) = 1 \quad \text{for} \quad x > 1\,,$$

$$F(x) = G \int_{-1}^{x} \exp\left(-9t^2\right) \mathrm{d}t \quad \text{for} \quad -1 \leqq x \leqq +1\,,$$

$$G = \left(\int_{-1}^{1} \exp\left(-9t^2\right) \mathrm{d}t\right)^{-1} .$$

It is easily seen, that P_1 is an ergodic process with the autocorrelation function R_μ. P_1 is not a Gaussian process because, for example, for $|\Delta t| < \mu$

$$\begin{aligned} &P(Z(t) < A, Z(t + \Delta t) < B) = \\ &= P(Z(t) < A) \left[\frac{|\Delta t|}{\mu} P(Z(t) < B) + \left(1 - \frac{|\Delta t|}{\mu}\right) H_A(B)\right] \end{aligned} \tag{5}$$

where $H_A(B) = 1$ for $B > A$ and $H_A(B) = 0$ for $B \leqq A$, The process P_1 can be, however, easily generated on a computer (see bellow). Using (1) we obtained for the process P_1

$$\tilde{z}(t) = \sum_{i=0}^{i(t)-1} \int_{b_i}^{b_{i+1}} a_i q(t - \tau)\,\mathrm{d}\tau + \int_{b_{i(t)}}^{t} a_{i(t)}\, q(t - \tau)\,\mathrm{d}\tau \tag{6}$$

where $i(t)$ is the greatest integer for which $b_{i(t)} \leqq t$ can be expressed in the following form

$$(7)\qquad \tilde{z}(t) = a_{i(t)}[G(0) - G(t - b_{i(t)})] + \sum_{i=0}^{i(t)} a_{i+1}[G(t - b_{i+1}) - G(t - b_i)]$$

where G is a primitive function for q.

The process P_1 can be easily generated (in a pseudorandom manner) on a digital computer. It suffices to produce the sequence $a_1, a_2, a_3, \ldots$ by one pseudorandom number (normal) generator and the sequence $b_1 - 0, b_2 - b_1, b_3 - b_2, \ldots$ by a uniform pseudorandom number generator. Using (7) we can easily generate the sequence $\tilde{z}(t_0), \tilde{z}(t_0 + h), \tilde{z}(t_0 + 2h), \ldots$, where h is a positive number greather than μ.

Numerical experiments show, that the sequences of pseudorandom numbers produced in such a way have autocorrelation coefficients near the expected values (see the figures 1–6).

Numerical results

Example 1.

$$F(p) = \frac{k}{p - \beta_1}\,, \quad R_\mu(\tau) = e^{\beta_1|\tau|}\,, \quad \beta_1 = -0{\cdot}2$$

(Fig. 1, Fig. 2).

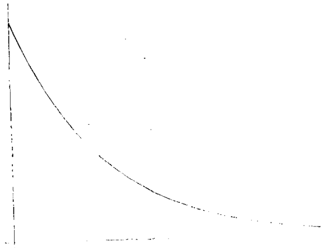

Fig. 1. Graph of $R_\mu(\tau)$.

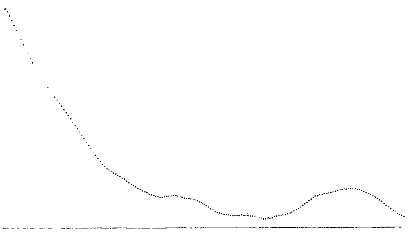

Fig. 2. Autocorrelation coefficients ($n = 2000$).

Example 2.

$$F(p) = \frac{k}{(p_1 - \beta_1)(p - \beta_2)}\,,$$

$$R_\mu(\tau) = \frac{\beta_1}{\beta_2 - \beta_1}\, e^{\beta_1|\tau|} + \frac{\beta_2}{\beta_1 - \beta_2}\, e^{\beta_2|\tau|}\,,$$

$$\beta_1 = -0{\cdot}4\,, \quad \beta_2 = -0{\cdot}44$$

(Fig. 3, Fig. 4).

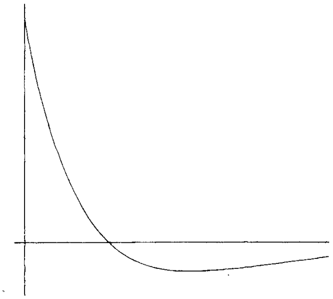

Fig. 3. Graph of $R_\mu(\tau)$.

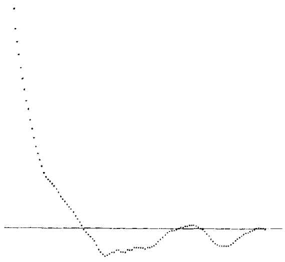

Fig. 4. Autocorrelation coefficients ($n = 2000$).

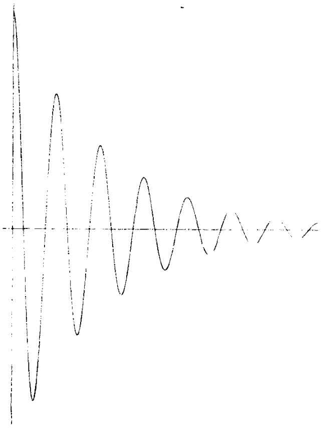

Fig. 5. Graph of R_μ.

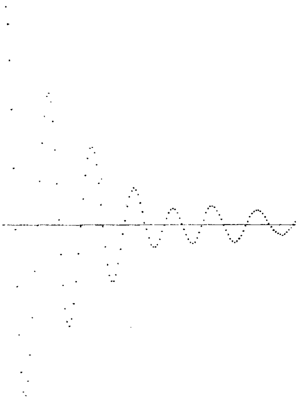

Fig. 6. Autocorrelation coefficients ($n = 2500$).

Example 3.

$$F(p) = \frac{k}{(p - \beta_1)(p - \bar{\beta}_1)}, \quad R_\mu = e^{\alpha t} \cos \beta t ,$$

$$\beta_1 = \alpha + i\beta , \quad \bar{\beta}_1 = \alpha - i\beta , \quad i = \sqrt{-1} ,$$

$$\alpha = -0{\cdot}4 , \quad \beta = 2\pi$$

(Fig. 5, Fig. 6).

(Received June 23, 1970.)

REFERENCES

[1] Feller, W.: An Introduction to Probability Theory and Its Applications, Vol. 1, Second ed. Wiley, New York 1957.

[2] Janáč K., Vojtášek S.: Solution of Nonlinear Systems. Ilife, London 1969.

[3] Parren E.: Modern Probability Theory and its Applications. John Wiley, New York 1960.

VÝTAH

Poznámka o generování posloupností pseudonáhodných čísel s předepsanými autokorelačními koeficienty

JAROSLAV KRÁL

V řadě aplikací (např. pro posouzení účinku filtrace náhodného procesu) je potřebné generovat posloupnosti pseudonáhodných čísel se zadanou autokorelační funkcí. V článku je diskutován jeden způsob, jež umožňuje poměrně efektivní generování pseudonáhodných čísel s autokorelační funkcí blízkou autokorelační funkci bílého šumu po flltraci analogovým filtrem s funkcí přenosu $F(p)$. Bílý šum je aproximován jistou formou telegrafního signálu, na něž je pak uplatněna jistá integrální transformace. Přiložené experimentální výsledky ukazují, že generované autokorelační koeficienty mají hodnoty blízké očekávaným. Výhoda diskutované metody je v tom, že umožňuje generovat pseudonáhodné posloupnosti, pro něž je velký počet autokorelačních koeficientů nenulový.

RNDr. Jaroslav Král, CSc.; Ústav výpočtové techniky ČVUT (Institute of computation technique — Technical University), Horská 3, Praha 2.