УДК 518.5:519.2

О КОРРЕЛЯЦИОННОМ КОЭФФИЦИЕНТЕ ПОЛНОГО ПЕРИОДА ПСЕВДОПОСЛЕДОВАТЕЛЬНОСТИ

М.В. Антинов

В 1951 г. Лемером [1] был предложен метод вычетов (мультипликативный метод сравнения) для получения последовательности псевдослучайных чисел на ЭВМ.

В практических вычислениях используется генератор (датчик) псевдослучайных чисел вида:

$$x_{n+1} \equiv \lambda x_n \pmod{M} \tag{1}$$

или

$$x_{n+1} \equiv \lambda x_n + c \pmod{M}, \tag{2}$$

называемый мультипликативным датчиком смешанного типа.

Пусть даны две конечные числовые последовательности: $X = \{x_i\}$ и $Y = \{y_i\}$, где $i = 1,2,\ldots,n$. Вычислены их средние значения

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i \quad \text{и} \quad \bar{y} = \frac{1}{n}\sum_{i=1}^{n} y_i$$

Одним из способов определения независимости между X и Y является вычисление коэффициента корреляции [12]:

$$\rho(X,Y) = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\left(\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2\right)^{1/2}} \tag{3}$$

причем ρ может изменяться в интервале $[-1,1]$. Мерой независимости последовательностей служит близость $|\rho|$ к нулю.

Покажем, что этот критерий не является достаточно эффективным. Например, пусть X и Y - последовательности с периодом n, причем

а) соответствующие члены последовательностей связаны соотношением

$$y_i \equiv x_i + c \pmod M,$$

где M - целое, $M \geqslant n$, $0 \leqslant x_i, y_i \leqslant M-1$;

б) после нормирования последовательности, т.е. деления членов последовательности на M, имеем $0 \leqslant \frac{x_i}{M}, \frac{y_i}{M} < 1$;

в) пусть S - множество тех i, для которых $x_i + c \geqslant M$, а c таково, что для каждого $x_i \in X$ найдется такое $y_j \in Y$, что $x_i = y_j$ (последнее предложение дается для упрощения выкладок). Тогда из формулы (3) следует:

$$\rho(X,Y) \sim 1 - \frac{12}{n} \sum_{i \in S} \left(\frac{x_i}{M} - \frac{\bar{x}}{M} \right),$$

то есть при различных c величина $\rho(X,Y)$ может изменяться от $-\frac{1}{2}$ (при $c \sim \frac{M}{2}$) до 1 (при c, близких к M или нулю). Можно, в частности, найти такое $c = c_0$, что $\rho(X,Y)$ будет близок к нулю. Большие колебания $\rho(X,Y)$ в зависимости от c дают основания предположить, что вычисления одного корреляционного коэффициента недостаточно для оценки зависимости последовательностей.

Рассмотрим датчики $x_{n+1} \equiv \lambda x_n \pmod M$ и $x_{n+1} \equiv \lambda x_n + c \pmod M$. Если λ и M взаимно просты (а это всегда будет предполагаться), то введем и понятие обратного датчика.

ОПРЕДЕЛЕНИЕ 1. Датчик $f(\lambda_1, c_1)$ будет **обратным** для датчика $f(\lambda_2, c_2)$, если последовательности, полученные датчиками, связаны соотношением: $x_i^1 = x_{n-i}^2$ для $i = 0,1,\ldots, n-1$, где n - период последовательностей.

Для датчика $x_{i+1} \equiv \lambda x_i \pmod M$ это означает, что найдется такое $\lambda^{-1} (\lambda\lambda^{-1} \equiv 1 \pmod M)$, что $x_{i+1}\lambda^{-1} \equiv x_i \pmod M$. Аналогично для датчика $x_{i+1} \equiv \lambda x_i + c \pmod M$ найдется λ^{-1}, а $c^{-1} \equiv \lambda^{-1}(M-c) \pmod M$.

Датчик, обратный для f, обозначим f^{-1}. Заметим, что

$(f^{-1})^{-1} = f$, так как $(\lambda^{-1})^{-1} \equiv \lambda \pmod M$, а $c \equiv \lambda(M - \lambda^{-1}(M - c)) \pmod M$.

ОПРЕДЕЛЕНИЕ 2. Датчики f и g назовем **эквивалентными** $(f \sim g)$, если для каждой последовательности $X = \{x_i\}$ произведение корреляционных коэффициентов

$$\rho\{X, f(X) - g(X)\} \cdot \rho\{X, f^{-1}(X) - g(X)\} = 0.$$

Здесь знак минус означает, что для каждого i находится разность $\{f(x_i) - g(x_i)\} \pmod M$.

Из этих определений вытекают следующие 6 предложений:

1. $f \sim f$.
2. $f + c_1 \sim f + c_2$.
3. Если $f \sim g$, то $f^{-1} \sim g$, $f \sim g^{-1}$, $f^{-1} \sim g^{-1}$.
4. Если $f \sim g$, то $cf \sim cg$.
5. Если $f \sim g$ и $g \sim h$, то $f \sim h$.
6. Если $f_1 \sim g_1$ и $f_2 \sim g_2$, то либо $f_1 + f_2 \sim g_1 + g_2$, либо $f_1^{-1} + f_2 \sim g_1 + g_2$.

Наиболее важным представляется

СЛЕДСТВИЕ 1. **Датчик** $x_{i+1} \equiv \lambda x_i \pmod M$ **эквивалентен датчикам** $x_{i+1} \equiv \lambda x_i + c \pmod M$ **и** $x_{i+1} \equiv \lambda^{-1} x_i + c \pmod M$.

Заметим, что представление датчиков в более общем виде [9]:

$$x_{i+\kappa} \equiv \lambda^\kappa x_i \pmod M \quad \text{и} \quad x_{i+\kappa} \equiv \lambda^\kappa x_i + \frac{c(\lambda^\kappa - 1)}{\lambda - 1} \pmod M$$

$(\kappa \geqslant 1)$ не повлияет на справедливость следствия, ибо для каждого фиксированного κ величина

$$\frac{c(\lambda^\kappa - 1)}{\lambda - 1} = c_\kappa$$

будет константой.

Статистические проверки [2-11], а также теоретическая оценка мультипликативного датчика [9] позволяют утверждать, что датчик смешанного типа несколько предпочтительнее датчика несмешанного типа для одного и того же λ. Это можно объяснить тем, что период последовательности, получаемой первым датчиком, в четыре раза больше. Для больших периодов (порядка $2^{30} - 2^{40}$) можно считать, что статистические характеристики этих двух датчиков совпадают.

В дальнейшем будем рассматривать только датчики (I) с основанием 2^ρ.

Пусть в формуле (3) $X=\{x_i\}=\{\lambda^i x_0\}$, а $Y=\{x_{i+\kappa}\}=\{\lambda^{i+\kappa}x_0\}$, то есть последовательность Y начинается с κ-го члена последовательности X.

Обозначим период последовательности X через n, тогда имеем:

$$\frac{\sum_{i=1}^{n}(x_i-\bar{x})(x_{i+\kappa}-\bar{x})}{\sum_{i=1}^{n}(x_i-\bar{x})^2} \qquad (4)$$

В работе [2] показано, что максимальный период для $M=2^\rho$ достигается при $\lambda\equiv 3(mod8)$, $\lambda\equiv 5(mod8)$, $x_0=2s+1$ и равен $2^{\rho-2}$. Тогда $\bar{x}=2^{\rho-1}+\bar{\varepsilon}$, где $|\bar{\varepsilon}|\le 2$ [II]. Члены последовательности X расположим в порядке возрастания. Вновь полученную последовательность обозначим X^*. Тогда для каждого $i\,(0\le i\le 2^{\rho-2}-1)$ возможно такое представление: $x_i^*=4i+\varepsilon_i$, где $-1\le\varepsilon_i\le 5$. Например, для $\lambda\equiv 5(mod8)$ величина ε_i – константа и равна либо I, если $x_0=1$, либо 3, если $x_0=7$ [II].

Обозначим $\lambda^\kappa(mod2^\rho)=\lambda_\kappa$. Тогда из формулы (4) следует:

$$\rho(X,Y)=\frac{\sum_{i=0}^{2^{\rho-2}-1}(4i+\varepsilon_i-2^{\rho-1}-\bar{\varepsilon})(\lambda_\kappa(4i+\varepsilon_i)(mod2^\rho)-2^{\rho-1}-\bar{\varepsilon})}{\sum_{i=0}^{2^{\rho-2}-1}(4i+\varepsilon_i-2^{\rho-1}-\bar{\varepsilon})^2}.$$

Рассмотрим случай $\lambda\equiv 5(mod8)$, тогда $\varepsilon_i=\bar{\varepsilon}$ и

$$\rho(X,Y)=\frac{\sum_{i=0}^{2^{\rho-2}-1}(i-2^{\rho-3})(\lambda_\kappa(4i+\bar{\varepsilon})(mod2^\rho)-2^{\rho-1})}{4\sum_{i=0}^{2^{\rho-2}-1}(i-2^{\rho-3})^2}=$$

$$=\frac{12}{(2^{\rho-2})^3+2^{\rho-1}}\sum_{i=0}^{2^{\rho-2}-1}(i-2^{\rho-3})((\lambda_\kappa i+\frac{\lambda_\kappa\bar{\varepsilon}}{4})(mod2^{\rho-2})-2^{\rho-3}).$$

Согласно предложению 2 об эквивалентности, датчик

$$x_{i+1}\equiv(\lambda_\kappa x_i+\frac{\lambda_\kappa\bar{\varepsilon}}{4})(mod2^{\rho-2})$$

эквивалентен датчику

$$x_{i+1}\equiv\lambda_\kappa x_i\,(mod2^{\rho-2})$$

Тогда после замены датчиков и некоторых преобразований получаем:

$$\rho^*(X,Y)=(\frac{12}{(2^{\rho-2})^3}-\frac{24}{(2^{\rho-2})^5})\sum_{i=0}^{2^{\rho-2}-1}(i-2^{\rho-3})(\lambda_\kappa i(mod2^{\rho-2})-2^{\rho-3})=$$

$$=(\frac{12}{2^{\rho-2}}-\frac{24}{(2^{\rho-2})^3})\sum_{i=0}^{2^{\rho-2}-1}(\frac{i}{2^{\rho-2}}-\frac{1}{2})(\frac{\lambda_\kappa i(mod2^{\rho-2}}{2^{\rho-2}}-\frac{1}{2}).$$

$$\left|\sum_{i=0}^{2^{\rho-2}-1}(\frac{i}{2^{\rho-2}}-\frac{1}{2})(\frac{\lambda_\kappa i(mod2^{\rho-2}}{2^{\rho-2}}-\frac{1}{2})\right|\le$$

$$\le\sum_{i=0}^{2^{\rho-2}}(\frac{i}{2^{\rho-2}}-\frac{1}{2})^2=\frac{2^{\rho-2}}{12}+\frac{1}{6\cdot 2^{\rho-2}},$$

даже при сравнительно небольших ρ величиной порядка $\frac{2}{(2^{\rho-2})^2}$ можно пренебречь, и тогда

$$\rho^*(X,Y)=\frac{12}{2^{\rho-2}}\sum_{i=0}^{2^{\rho-2}-1}(\frac{i}{2^{\rho-2}}-\frac{1}{2})(\frac{\lambda_\kappa i(mod2^{\rho-2})}{2^{\rho-2}}-\frac{1}{2}). \qquad (5)$$

Во втором случае, $\lambda\equiv 3(mod8)$, имеем (см., [II]) $\varepsilon_{2i+1}=\varepsilon_1$, $\varepsilon_{2i}=\varepsilon_2$ $(i=0,1,\dots,\ 2^{\rho-3}-1)$. Последовательность X распадается на две, в каждой из них ε_i – постоянная. Тогда мы возвращаемся к предыдущему случаю $\lambda\equiv 5(mod8)$. После аналогичных преобразований получим формулу (5).

В формуле (5) выражение

$$\frac{\lambda_\kappa i(mod2^{\rho-2})}{2^{\rho-2}}$$

есть дробная часть $\frac{\lambda_\kappa i}{2^{\rho-2}}$, обозначаемая обычно $\{\frac{\lambda_\kappa i}{2^{\rho-2}}\}$. Подставим $\{\frac{\lambda_\kappa i}{2^{\rho-2}}\}$ в (5) и преобразуем:

$$\rho^{*}(X,Y)=\frac{12}{2^{\rho-2}}\sum_{i=0}^{2^{\rho-2}-1}\left(\frac{i}{2^{\rho-2}}-\frac{1}{2}\right)\left(\left\{\frac{\pi_{\kappa} i}{2^{\rho-2}}\right\}-\frac{1}{2}\right)= \tag{6}$$

$$=\frac{12}{(2^{\rho-2})^{2}}\sum_{i=0}^{2^{\rho-2}-1} i\left\{\frac{i\pi_{\kappa}}{2^{\rho-2}}\right\}-3+6/2^{\rho-2}.$$

ЛЕММА I. Если π и n взаимно просты, то

$$\sum_{i=0}^{n-1}\left[\frac{i\pi}{n}\right]=\frac{(n-1)(\pi-1)}{2},$$

где $[x]$ - целая часть числа x.

ЛЕММА 2. Если π и n взаимно просты, то

$$\sum_{i=0}^{n-1}\left\{\frac{i\pi}{n}\right\}^{2}=\frac{(n-1)(2n-1)}{6n}$$

ДОКАЗАТЕЛЬСТВО этих лемм можно найти у Янссона [I4].

ЛЕММА 3. При взаимно простых π и n

$$\sum_{i=0}^{n-1}\frac{i}{n}\left\{\frac{i\pi}{n}\right\}=\frac{\pi(3n+1)}{12n}+\frac{n-3}{4}+\frac{n^{2}+1}{12\pi n}-\sum_{j=0}^{\pi-1}\frac{j}{\pi}\left\{\frac{jn}{\pi}\right\}.$$

ДОКАЗАТЕЛЬСТВО (см. [I5]).

Обозначим $2^{\rho-2}=\lambda_{0}$ и $\pi=\lambda_{1}$; λ_{0} и λ_{1} взаимно просты, поэтому наибольший общий делитель λ_{0} и λ_{1} равен единице. Рассмотрим известный алгоритм Евклида (доказательство взаимной простоты двух чисел):

$$\begin{aligned}
&\lambda_{0}=k_{1}\lambda_{1}+\lambda_{2}, && \lambda_{s-1}=k_{s}\lambda_{s}+1,\\
&\lambda_{1}=k_{2}\lambda_{2}+\lambda_{3}, && \lambda_{s}=k_{s+1}, \qquad (7)\\
&\dots\dots\dots\dots && \lambda_{s+1}=1,
\end{aligned}$$

где все числа целые и положительные, а $k_{1}, k_{2}, \dots, k_{s+1}$, I-коэффициенты разложения.

ТЕОРЕМА I. Значение корреляционного коэффициента определяется по формуле

$$\rho=\frac{1}{2^{\rho-2}}\sum_{i=1}^{s+2}(-1)^{i+1}k_{i}+\varepsilon,$$

где

$$|\varepsilon|<\frac{5}{2^{\rho-2}} \tag{8}$$

ДОКАЗАТЕЛЬСТВО. Преобразуем формулу леммы 3, предварительно домножив ее на число I2:

$$12\sum_{i=0}^{\lambda_{0}-1}\frac{i}{\lambda_{0}}\left\{\frac{i\lambda_{1}}{\lambda_{0}}\right\}=3\lambda_{1}+\frac{\lambda_{1}}{\lambda_{0}}+3\lambda_{0}-9+\frac{\lambda_{0}}{\lambda_{1}}+\frac{1}{\lambda_{0}\lambda_{1}}-\sum_{j=0}^{\lambda_{1}-1}\frac{j}{\lambda_{1}}\left\{\frac{j\lambda_{0}}{\lambda_{1}}\right\}. \tag{9}$$

Так как из (7) следует, что

$$\left\{\frac{j\lambda_{0}}{\lambda_{1}}\right\}=\left\{\frac{j\lambda_{2}}{\lambda_{1}}\right\},$$

то формула (9) становится рекуррентной:

$$12\sum_{i=0}^{\lambda_{0}-1}\frac{i}{\lambda_{0}}\left\{\frac{i\lambda_{1}}{\lambda_{0}}\right\}=\sum_{i=0}^{s}(-1)^{i}\left(3\lambda_{i+1}+\frac{\lambda_{i}}{\lambda_{i+1}}+3\lambda_{i}-9+\frac{\lambda_{i+1}}{\lambda_{i}}+\frac{1}{\lambda_{i}\lambda_{i+1}}\right).$$

Отсюда видно, что сумма первых и третьих членов даст

$$3\lambda_{0}+(-1)^{s}\cdot 3\lambda_{s+1},$$

вторых и пятых —

$$\sum_{i=1}^{s+1}(-1)^{i+1}k_{i}+\frac{\lambda_{1}}{\lambda_{0}},$$

ибо из формул (7):

$$\frac{\lambda_{i-1}}{\lambda_{i}}-\frac{\lambda_{i+1}}{\lambda_{i}}=k_{i}, \quad \text{а} \quad \lambda_{s+1}=1 \quad \text{и} \quad \lambda_{s}=k_{s+1}.$$

Итак,

$$12\sum_{i=0}^{\lambda_{0}-1}\frac{i}{\lambda_{0}}\left\{\frac{i\lambda_{1}}{\lambda_{0}}\right\}=3\lambda_{0}+\sum_{i=1}^{s+1}(-1)^{i+1}k_{i}+\frac{\lambda_{1}}{\lambda_{0}}+(-1)^{s}3+\sum_{i=0}^{s}\frac{(-1)^{i}}{\lambda_{i}\lambda_{i+1}}-9\left(\frac{1}{2}+\frac{(-1)^{s}}{2}\right). \tag{10}$$

Сумма знакопеременного ряда

$$\sum_{i=0}^{s}\frac{(-1)^{i}}{\lambda_{i}\lambda_{i+1}}$$

не превосходит по абсолютной величине $\frac{1}{\lambda_S}$ и имеет тот же знак, что и S - й член суммы. Подставим (I0) в выражение корреляционного коэффициента (6):

$$\rho^*(X,Y)=\rho-\frac{1}{2^{\rho-2}}\sum_{i=1}^{S+2}(-1)^{i+1}\varkappa_i+\varepsilon,$$

где

$$\varepsilon=\frac{1}{2^{\rho-2}}\left\{\frac{\lambda_1}{\lambda_0}+(-1)^S 3+\sum_{i=0}^{S}\frac{(-1)^i}{\lambda_i\lambda_{i+1}}-4{,}5\left(1+(-1)^S\right)+6+(-1)^S\right\}.$$

При S четном:

$$\left(\frac{1}{2^{\rho-2}}<\varepsilon<\frac{2{,}5}{2^{\rho-2}}\right),$$

а при S нечетном:

$$\left(-\frac{3{,}5}{2^{\rho-2}}<\varepsilon<\frac{5}{2^{\rho-2}}\right)$$

Теорема доказана.

Для простоты практического вычисления корреляционного коэффициента введем рекуррентный оператор ν. Пусть дано начальное

$$\nu_0=\frac{\lambda}{2^{\rho-2}},\quad \nu_{i+1}=\frac{1}{\{\nu_i\}}.$$

Тогда формула (8) примет вид:

$$\rho\sim\frac{1}{2^{\rho-2}}\sum_{i=1}^{S+1}(-1)^{i+1}\left[\nu_i\right] \qquad (II)$$

Вычисление суммы заканчивается, как только ν_i станет целым числом. В формуле (II) отброшены ε и последний член суммы корреляционного коэффициента (8), так как при больших ρ величинами порядка $5/2^{\rho-2}$ можно пренебречь.

Возникает вопрос о величине S, имеющей немаловажное значение для практического вычисления. Например, если λ_0 - число Фибоначчи, то алгоритм Евклида (7) будет максимальной длины тогда, когда λ_1 - соседнее меньшее число Фибоначчи. Это видно непосредственно из записи алгоритма Евклида, ибо любое $\varkappa_i\neq 1$ сокращает длину алгоритма, а все $\varkappa_i=1$ ($i=1,2,\ldots,S,\ S+1$) при любом S дают числа Фибоначчи. Если λ_0 таково, что лежит между соседними числами Фибоначчи $F_S<\lambda<F_{S+1}$, то

максимальная длина алгоритма Евклида равна $S+1$, так как для $\lambda_0=F_S$ длина алгоритма S, а для $\lambda_0=F_{S+1}$ равна $S+1$. Итак, если F_S - наибольшее число Фибоначчи, такое что $F_S\leq\lambda_0$, то найдется такое $\lambda_1<\lambda_0$, что доказательство взаимной простоты λ_0 и λ_1 потребует максимального числа разложений S.

Из формулы Бине [I3] для общего члена ряда Фибоначчи вычисляется значение S:

$$F_S=\frac{\left(\frac{1+\sqrt{5}}{2}\right)^S-\left(\frac{1-\sqrt{5}}{2}\right)^S}{\sqrt{5}};\quad S\sim\frac{\log_2(\sqrt{5}\lambda_0)}{\log_2\frac{1+\sqrt{5}}{2}}\sim\frac{3}{2}\log_2\lambda_0+2.$$

Если $\lambda_0=2^{\rho-2}$, то S может достигать величины $1{,}5\rho$.

СЛЕДСТВИЕ 2. Если для некоторого λ_1 все $\varkappa_i=\ell$ ($i=1,\ldots,S+1$), то ρ близок к нулю.

ТЕОРЕМА 2. (Обобщенное тождество Симсона.) Если λ_1 и λ_0 таковы, что S нечетно и все $\varkappa_i=\ell$, то $\lambda_1^2\ (\mathrm{mod}\,\lambda_0)=1$

ДОКАЗАТЕЛЬСТВО. Рассмотрим обобщенный ряд Фибоначчи

$$F_{n+1}=\ell F_n+F_{n-1},\quad F_0=0,F_1=1.$$

Тождество Симсона для ряда Фибоначчи дается формулой

$$f_S^*=f_{S-1}f_{S+1}+(-1)^{S-1}$$

Докажем, что оно верно для обобщенного ряда.

Формула Бине для него дается в виде

$$F_S=\frac{\left(\frac{\ell+\sqrt{\ell^2+4}}{2}\right)^S-\left(\frac{\ell-\sqrt{\ell^2+4}}{2}\right)^S}{\sqrt{\ell^2+4}}$$

Подстановка F_S в тождество Симсона доказывает справедливость тождества для обобщенного ряда, а справедливость теоремы следует из тождества при S нечетном, ибо λ_0 и λ_1 - члены обобщенного ряда Фибоначчи.

СЛЕДСТВИЕ 3. Если λ_0 и λ_1 - соседние члены обобщенного ряда Фибоначчи, то, несмотря на минимальные парные корреляции, датчик с $\lambda=\lambda_1$

следует отвергнуть из-за чрезмерно больших тройных корреляций.

СЛЕДСТВИЕ 4. Датчик со значением $\lambda_1 = \lambda \simeq \sqrt{n_0}$ должен быть также отвергнут, так как приводит к частному случаю обобщенного ряда Фибоначчи с $t = \lambda_1$ и $s = 1$.

СЛЕДСТВИЕ 5. Корреляционный коэффициент находится в пределах:

$$-\frac{1}{3} < \rho < \frac{1}{5} \quad \text{для} \quad \lambda \equiv 5 \pmod 8 \text{ и}$$

$$-\frac{1}{5} < \rho < \frac{1}{3} \quad \text{для} \quad \lambda \equiv 3 \pmod 8 .$$

ДОКАЗАТЕЛЬСТВО следует из теоремы I, если придавать λ значения $5, 2^{\rho-2}-3$ и $3, 2^{\rho-2}-5$, соответственно.

ТЕОРЕМА 3. Если $\lambda \equiv 2^{\rho-2} \pm a \pmod{2^{\rho-2}}$, где $a < \sqrt{2^{\rho-2}}$, то $|\rho| \sim \frac{1}{a}$.

ДОКАЗАТЕЛЬСТВО. $\lambda = 2^{\rho-2} + a \equiv a \pmod{2^{\rho-2}}$ подставим в формулу (8). Так как $a < \sqrt{2^{\rho-2}}$, то $K_1 > \sqrt{2^{\rho-2}}$, а все остальные $K_i \ (i > 1)$ меньше K_1, тогда

$$\rho \sim \frac{K_1}{2^{\rho-2}} \sim \frac{1}{2^{\rho-2}} \left[\frac{2^{\rho-2}}{a}\right] \sim \frac{1}{a}$$

Для $\lambda = 2^{\rho-2} - a$ после подстановки в формулу (8) получим:

$$\rho \sim \left(\left[\frac{2^{\rho-2}}{2^{\rho-2}-a}\right] - \left[\frac{2^{\rho-2}-a}{a}\right] + \dots\right)\frac{1}{2^{\rho-2}} \sim \frac{1}{2^{\rho-2}}\left(1 - \left[\frac{2^{\rho-2}}{a}\right] + \dots\right).$$

Как и в предыдущем случае, все K_i, начиная с третьего, меньше K_2, поэтому $\rho \sim -\frac{1}{a}$, что и доказывает теорему.

ТЕОРЕМА 4. Если $\lambda = \mu \cdot 2^{\rho-2-t} \pm a$, причем μ нечетно, $2^{\frac{3}{2}t} a < \sqrt{2^{\rho-2}}$, тогда $|\rho| \sim \frac{1}{4^t a}$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим алгоритм Евклида для чисел 2^t и μ:

$$\begin{aligned} 2^t &= \mu_0 = k_1\mu_1 + \mu_2, & \mu_{s-1} &= k_s\mu_s + 1, \\ \mu &= \mu_1 = k_2\mu_2 + \mu_3, & \mu_s &= k_{s+1}, \\ \mu_2 &= k_3\mu_3 + \mu_4, & \mu_{s+1} &= 1, \\ & & \mu_{s+2} &= 0. \end{aligned}$$

Тогда, согласно теореме I,

$$\rho = \frac{1}{2^{\rho-2}}\left\{k_1 - k_2 + \dots \pm k_{s+1}\right\} \mp \rho(2^{\rho-2-t} \pm \mu a, 2^t a).$$

Действительно,

$$\rho(2^{\rho-2}, \mu 2^{\rho-2-t} \pm a) = \rho(2^t 2^{\rho-2-t} \pm 0 \cdot a, \mu \cdot 2^{\rho-2-t} \pm a),$$

разложением Евклида будем пользоваться до тех пор, пока коэффициенты при $2^{\rho-2-t}$ в формуле ρ не станут соответственно I и 0, то есть коэффициентами при a до применения алгоритма Евклида. По условию, все $k_i < 2^t$, поэтому:

$$\frac{1}{2^{\rho-2}}\left\{k_1 - k_2 + \dots \pm k_{s+1}\right\} < \frac{1}{2^{\rho-2-t}}.$$

По теореме 3,

$$\rho(2^{\rho-2-t} \pm \mu a, 2^t a) \sim \frac{1}{2^{\rho-2}} \cdot \frac{2^{\rho-2-t}}{2^t a} = \frac{1}{4^t a},$$

если $\sqrt{2^{\rho-2-t}} > 2^t a$, то есть $2^{\frac{3}{2}t} a < \sqrt{2^{\rho-2}}$. Так как k_i не могут существенно повлиять на величину ρ (по условию $2^{\rho-2-t} > 4^t a$), то теорема доказана.

ТЕОРЕМА 5. Если числа a и b взаимно просты, $a < b$ и найдется такое α (необязательно целое), что

$$\lambda = \frac{a}{b} 2^{\rho-2} \pm \alpha,$$

причем $b^3\alpha^2 < 2^{\rho-2}$ и $b^3\alpha < 2^{\rho-2}$, тогда

$$|\rho| \sim \frac{1}{b^2\alpha}.$$

ДОКАЗАТЕЛЬСТВО проводится аналогично приведенному выше, если учесть, что α может быть меньше единицы, и условие $b^3\alpha < 2^{\rho-2}$, опущенное в доказательстве теоремы 4, здесь не является лишним.

СЛЕДСТВИЕ 6. Значение корреляционного коэффициента $\rho(2^{\rho-2}, \lambda^{\mu \cdot 2^s})$ при больших $s \ (s > \frac{\rho}{2} - 3)$, μ нечетном не зависит от λ.

Это справедливо, так как, например, для $\lambda^{2^s} \pmod{2^{s+2}} \equiv 1$ и, по теореме 4, при $s > \frac{\rho}{2} - 3$, $|\rho| \sim \frac{1}{4^{\rho-4-s}}$.

Итак, полученные результаты позволяют легко вычислять корреляционный коэффициент последовательностей вида X и λX; показана эквивалентность датчиков смешанного и несмешанного типов. Показана также целесообразность выбора множителя λ близким к $\sqrt{M}$, и найдены численные выражения корреляционного коэффициента для некоторых множителей λ.

Литература

1. LEHMER D. Mathematical methods in large scale computing units. Ann.Comput.Labor. Harvard Univ., 1951, N 26,p.141-146.

2. BOFINGER B., BOFINGER V.J. On a Periodic Property of Pseudo-Random Sequences. - J.ACM,1958, N 5,p.261-265.

3. GRUENBERGER M. Notes on a New Presudo-Random Number Generators, ibid,1961, N 8, p.163-167.

4. MACLAREN D., MARSAGLIA G. Uniform Random Number Generators, ibid, 1965, vol.12, N 1,p.83-89.

5. BARNETT V.D. The Behaviour of Pseudo-Random Sequences Generated on Computers by the Multiplicative Congruential Method. - Math.Comp., 1962, N 16, p.69-69.

6. DONNELLY T. Some techniques for using pseudo-random numbers in computer simulation.-Comm.ACM,1969,vol.12,N 7,p.392.

7. HEMMERLE W.J. Generating pseudo-random nubers on a two's complement machine such as the IBM 360.-Comm.ACM,1969,vol. 12, N 7,p.382-383.

8. GELDER A.van. Some new results in pseudo-random numbers generation. - J.Ass.Comp.Mach.,1967,vol.14, N 4,p.785-792.

9. COVEYOU R.R., MacPHERSON R.D. Fourier analysis of random number generations.- J.ACM,1967,vol.14, N 1,p.100-119.

10. АНТИПОВ М.В., ИЗРАЙЛЕВ Ф.М., ЧИРИКОВ Б.В. Статистическая проверка датчика псевдослучайных чисел. -"Вычислительные системы", Новосибирск, "Наука" СО, 1968, вып. 30, стр. 77-85.

11. АНТИПОВ М.В. К оценке датчика псевдослучайных чисел. - "Вычислительные системы", Новосибирск, 1970, вып. 42,стр.81-88.

12. ГОЛЕНКО Д.И. Моделирование и статистический анализ псевдослучайных чисел на электронных вычислительных машинах. М., "Наука", 1965.

13. ВОРОБЬЕВ Н.Н. Числа Фибоначчи. М.-Л., 1951.

14. JANSSON B. Random Number Generators. Stocholm,1966.

15. АНТИПОВ М.В. Анализ производящих множителей мультипликативного датчика псевдослучайных чисел. Препринт ИМ СО АН СССР, 1971.

Поступила в ред.-изд.отд.
20. XI. 1971 г.