СООБЩЕНИЯ
ОБЪЕДИНЕННОГО
ИНСТИТУТА
ЯДЕРНЫХ
ИССЛЕДОВАНИЙ
ДУБНА



Р5-8411

П.Г.Акишин, Г.А.Ососков

# НЕКОТОРЫЕ АНАЛИТИЧЕСКИЕ ОЦЕНКИ СТАТИСТИЧЕСКИХ КРИТЕРИЕВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

1974

ЛАБОРАТОРИЯ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И АВТОМАТИЗАЦИИ

Р5-8411

П.Г.Акишин, Г.А.Ососков

# НЕКОТОРЫЕ АНАЛИТИЧЕСКИЕ ОЦЕНКИ СТАТИСТИЧЕСКИХ КРИТЕРИЕВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Акишин П.Г., Ососков Г.А.

P5-8411

Некоторые аналитические оценки статистических критериев псевдослучайных последовательностей

В работе дан аналитический вывод оценок основных статистических критериев , обычно употребляемых при оценке качества псевдослучайных последовательностей: периода, числа серий, коэффициента корреляций.

Предложен новый алгоритм генерации.

Сообщение Объединенного института ядерных исследований
Дубна, 1974

Akishin P.G., Ososkov G.A.

P5-8411

Some Analytical Estimates of Statistical Criteria for Pseudorandom Sequences

The estimates of the main statistical criteria, usually used when estimating the quality of the pseudorandom sequences such as: period, series number and correlation coefficient, are analytically obtained.

New algorithm is suggested for random number generation.

Communications of the Joint Institute for Nuclear Research.
Dubna, 1974

Преимущество программных генераторов случайных чисел (ГСЧ) для использования их в методе Монте-Карло подчеркивается во всех руководствах по статистическому моделированию. Наиболее употребительными являются ГСЧ, появившиеся на основании известного метода вычетов П. Лемера /I/. Последовательность целых чисел, образуемых рекуррентно с помощью сравнения по модулю $2^p$,

$$\gamma_{i+1} \equiv \gamma_i A + C \pmod{2^p} \quad (i = 1,2,\ldots), \qquad \text{(I)}$$

порождает последовательность чисел $\{x_i\}$ ; $x_i = \gamma_i 2^{-p}$ $(i = 1,2\ldots)$, которая при правильном подборе параметров A, C и $\gamma_0$ может оказаться равномерно распределенной в интервале (0,I). Конечно, в силу самой рекуррентной природы последовательности числа $\gamma_i$ зависимы, но, как это будет показано ниже, при статическом подходе, когда эта зависимость определяется путем проверки по какой-либо системе тестов на случайность, удачным выбором A и C можно добиться, чтобы последовательность (I) удовлетворяла этим критериям. Такие последовательности называются "псевдослучайными".

Не менее важным является вопрос о диапазоне изменения чисел $\gamma_i$. Априори можно предположить, что не при всех значениях параметров A,C и $\gamma_0$ в нашей последовательности $x_i$ встретятся все $2^p$ возможных чисел от 0 до $1-2^{-p}$.

Может оказаться, что после некоторой неповторяющейся группы чисел $x_0, x_1, \ldots x_L$ мы получим, что $x_{L+1}$ повторяет какое-то

число $x_H$ ( $H \le L$ ) и в силу (I) эта группа из $T = L - H$ чисел начнет потом повторяться. В этом случае начальный отрезок числовой последовательности называется отрезком апериодичности, а T – периодом последовательности. Так будет, например, в случае четного A. Действительно, в этом случае мы получим, что

$$A^H \equiv 0 \pmod{2^p} \quad (H \ge P). \tag{2}$$

Из (I) мы можем выразить $y_{i+H}$ через $y_i$ :

$$y_{i+H} \equiv A^H y_i + C\left(\frac{A^H - 1}{A - 1}\right) \pmod{2^p}. \tag{3}$$

Если начать с $i = 0$, то в силу (2) после номера $H \ge P$ первое слагаемое в правой части (3) исчезает и $y_{P+1} \equiv y_{P+2} \equiv \equiv C\frac{A^P - 1}{A - 1} \pmod{2^p}$, т.е. при четном A последовательность (I) независимо от выбора $C$ и $y_0$ будет иметь отрезок апериодичности, не превосходящий $P$, и период T = I.

Естественно также при $C \neq 0$ принять C нечетным. В противном случае мы фактически сократим нашу последовательность вдвое, т.к. в зависимости от четности $y_0$ из (I) будем получать либо только четные, либо только нечетные числа.

Итак, мы получим естественные ограничения на A и C :

$$(A,2) = (C,2) = I \ . \tag{4}$$

(Здесь и далее $d = (A,B)$ обозначает наибольший общий делитель чисел A,B.)

В последующих разделах настоящей работы в этих ограничениях будут определены основные статистические критерии, обычно употребляемые при оценке качества случайных последовательностей.

После точного вычисления периода для псевдослучайных последовательностей (I) ( также и при C=0) во втором и третьем разделах работы даются оценки как числа серий подряд идущих нулей и единиц в



произвольном разряде двоичной записи псевдослучайного числа, так и коэффициента корреляции $i$ -го и ( $i+H$ )-го членов псевдослучайной последовательности.

## § I. Определение периода псевдослучайной последовательности

Период T последовательности $x_i$ , т.е. такое минимальное положительное K, что для любого $i$ $x_{i+K} = x_i$ или $y_{i+K} \equiv y_i$ ( $\bmod 2^p$ ), может быть найден на основании следующей теоремы.

Теорема I

Период T последовательности $x_i$ при условиях (4) определяется следующими соотношениями в зависимости от вида параметра A:

$$T = \begin{cases} 2^p, & A = 2^n a + 1, \ (a,2) = 1, \ n \ge 2; \\ 2^{p-n+1}, & A = 2^n a - 1, \ (a,2) = 1, \ n \ge 2. \end{cases}$$

При C=0 (A,2) = I (случай мультипликативного ГСЧ) и $y_0 = 2^l \cdot \beta$ ($\beta$-нечетн.)

$$T = 2^{p-n-e} \qquad (p > n + l).$$

Доказательство:

нечетность A естественным образом определяет оба представления A, содержащихся в условии теоремы. Пусть $C \neq 0$.

Из (3) и (5) имеем

$$\frac{A^K - 1}{A - 1}\left((A-1)y_i + C\right) \equiv 0 \pmod{2^p},$$

что согласно (4) эквивалентно

$$\frac{A^K - 1}{A - 1} \equiv 0 \pmod{2^p}. \tag{6}$$

Пусть $A = 2^n a + 1$.

Тогда из (6)

$$(2^n a+1)^K \equiv 1 \pmod{2^{p+n}}. \qquad (7)$$

Используя разложения по биному Ньютона с учетом условия $n \geq 2$, можно получить для произвольного $n_0$

$$(2^n a+1)^{2^{n_0}} \equiv 2^{n+n_0}+1 \pmod{2^{n+n_0+1}}.$$

Далее, пусть $K=2^{n_0}\ell$, $(\ell,2)=1$. Находим

$$(2^n a+1)^K \equiv \left((2^n a+1)^{2^{n_0}}\right)^\ell \equiv (2^{n+n_0}+1)^\ell \equiv 2^{n+n_0}+1 \pmod{2^{n+n_0+1}}.$$

Отсюда и из (7) следует, что $2^{n+n_0}$ делится на $2^{p+n}$, или $n_0 \geq p$, т.е. период должен быть не меньше чем $2^p$. Простой проверкой убеждаемся, что $T = 2^p$ является периодом.

Если $A = 2^n a - 1$, то (7) заменяется на $(2^n a-1)^K \equiv 1 \pmod{2^{p+1}}$. В результате рассуждений, аналогичных вышеприведенным, получаем, что $T = 2^{p+1-n}$.

Для $C=0$ (7) заменяется на $(2^n a \pm 1)^K \equiv 1 \pmod{2^{p-\ell}}$, откуда период $T = 2^{p-n-\ell}$.

Теорема I доказана.

## § 2. Оценка числа серий

Рассмотрим двоичное представление числа

$$y = \sum_{i=0}^{p-1} a_i 2^i, \quad a_i = 0,1.$$

Коэффициент $a_i$ представляет собой содержимое $i$-го разряда в машинном представлении числа $y$ для ЭВМ с разрядной сеткой длины p. Одним из наиболее чувствительных критериев случайности является тест серий. При его применении к последовательности $x_j$ прослеживается, как меняется содержимое $i$-го разряда числа $x_j$ при $j$, возрастающем от $N$ до $N+L$. Если рассматривать серии подряд идущих нулей и единиц, то числом серий $R_i$ будем называть общее число переходов от 0 к I и от I к 0. Из теории /2/ известно, что, если содержимое $i$-го разряда $a_i$ принимает свои значения 0 и I случайно, с равными вероятностями, то асимптотически

$$R_i \cong \frac{L}{2} + O(\sqrt{L}).$$

Ниже доказывается

Теорема 2

Для $i$-го разряда псевдослучайной последовательности (I) при $A = 2^{n_0}+1$ и $L = 2^l$ справедлива следующая оценка для числа серий $i$-го разряда: $R_i = \frac{L}{2} + O(L)$, где $|O(L)| \leq 2^{i-(n_0-1)} + 2^{n_0-1}$.

Доказательство.

Воспользуемся двоичным представлением числа $x_j$:

$$x_j = 2^{-p} \sum_{i=0}^{p-1} a_{ij} 2^i, \quad a_{ij} = 0 \text{ или } 1,$$

или

$$x_j = 2^{-p}\left(\sum_{i=n+1}^{p-1} a_{ij}2^i + a_{nj}2^n + \sum_{i=0}^{n-1} a_{ij}2^i\right).$$

Учитывая (I), имеем,

$$x_{j+1} = \left\{\frac{A\sum_{i=n+1}^{p-1} a_{ij}2^i + A2^n a_{nj} + A\sum_{i=0}^{n-1} a_{ij}2^i + C}{2^p}\right\} =$$

$$= \left\{\frac{B_j 2^{n+1} + a_{nj}2^n + \left(\sum_{i=0}^{n-1} a_{ij}2^i\right)A + C}{2^p}\right\}; \quad \left(B_j = A\sum_{i=n+1}^{p-1} a_{ij}2^{(i-n-1)}\right).$$

Пусть $\left(\sum_{i=0}^{n-1} a_{ij}2^i\right)A + C \equiv \sum_{\ell=0}^{p-1} \beta_\ell 2^\ell \pmod{2^p}$,

где $\beta_\ell = 0,1$, тогда

$$x_{j+1} = \left\{\frac{B_j 2^{n+1} + (a_{nj}+\beta_n)2^n + \sum_{\ell=0}^{n-1}\beta_\ell 2^\ell}{2^p}\right\}, \text{ где } B_{1j} = B_j + \sum_{\ell=n+1}^{p-1}\beta_\ell 2^{\ell-n-1}.$$

Допустим, что у нас в $j$-м разряде был 0, т.е. $a_{nj} = 0$. Если $\beta_n = 0$, то в нашем разряде числа $x_{j+1}$ так и останется 0; но если $\beta_n = 1$, то $a_{nj+1} = 1$. Аналогичное рассуждение может быть проведено для $a_{nj} = 1$. Таким образом, чтобы подсчитать число серий для нашего разряда, достаточно найти сумму $\beta_n$. Воспользуемся следующим представлением:

$$\beta_{kn} = \left\{ \frac{[(x_k 2^{p-n})A + \frac{C}{2^n}]}{2} \right\} 2 ,$$

$$\sum_{k=0}^{N-1} \beta_{kn} = \sum_{k=0}^{N-1} \left\{ \frac{[(x_k 2^{p-n})A + \frac{C}{2^n}]}{2} \right\} 2 =$$

$$= \sum_{k=0}^{N-1} \left\{ \frac{[(\frac{\gamma_k}{2^n})A + \frac{C}{2^n}]}{2} \right\} .$$

Пусть $N = 2^n$ (C,2) = I.

Тогда $\gamma_k$ пробегает всю систему вычетов по модулю $2^n$.

Поэтому $\sum_{k=0}^{2^n-1} \beta_{kn} = \sum_{k=0}^{2^n-1} \left\{ \frac{[kA+C]}{2^n} \right\} 2 .$ (8)

Воспользуемся следующими очевидными соотношениями :

1) $\{x\} = x - [x],$ (9)

2) при $n$ -целом $\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right],$ (10)

3) $\sum_{k=0}^{2^n-1} \left\{ \frac{A_k + C}{2^n} \right\} = \frac{2^n - 1}{2}$ при (A,2) = I . (11)

Из (8), (9), (10), (11) имеем

$$\sum_{k=0}^{2^n-1} \beta_{kn} = 2 \sum_{k=0}^{2^n-1} \left\{ \frac{A_k + C}{2^{n+1}} \right\} - \frac{2^n - 1}{2} . \quad (12)$$

Для оценки $\sum_{k=0}^{2^n-1} \left\{ \frac{A_k + C}{2^{n+1}} \right\}$ при $A = 2^{n_0} + 1$ нам потребуется лемма I /3/.

Лемма I

Пусть $m > 0$, $(a, m) = 1$, $h \geq 0$, c-вещественное. Для суммы $S = \sum_{x=0}^{m-1} \left\{ \frac{ax + \psi(x)}{m} \right\}$ ,

где $\psi(x)$ для рассматриваемых $x$ ограничена, т.е.

$c \leq \psi(x) \leq c + h$, справедлива оценка, не зависящая от $c$ :

$$\left| S - \frac{1}{2} m \right| \leq h + \frac{1}{2} . \quad (13)$$

Представляя K в виде $K = 2^{n+1-n_0} y + z$ ( $0 \leq y \leq 2^{n_0 - 1}$ , $0 \leq z < 2^{n+1-n_0}$ ) и используя лемму I, оценим (I2) и получим искомое доказательство теоремы 2. Доказательство теоремы 2 было проведено для A вида $2^{n_0} + 1$ . Однако результат теоремы может быть расширен и на случай A произвольного вида. Для этого потребуется более сложная оценка суммы $\sum_{k=0}^{2^n-1} \left\{ \frac{A_k + C}{2^{n+1}} \right\}$ .



## § 3. Аналитическая оценка корреляционной зависимости

Займемся оценкой коэффициента корреляции между $i$ -м и $(i+k)$-м членами псевдослучайной последовательности $\{x_i\}$ :

$$\rho_k = \frac{\frac{1}{2^p} \sum_{i=0}^{2^p-1} x_i x_{i+k} - \left(\frac{1}{2^p} \sum_{i=0}^{2^p-1} x_i\right)^2}{\frac{1}{2^p} \left(\sum_{i=0}^{2^p-1} x_i^2\right) - \left(\frac{1}{2^p} \sum x_i\right)^2} . \quad (14)$$

Выбирая (C,2) =I и A = $2^n + 1$, получаем в соответствии с теоремой I, что последовательность $\{x_i\}$ будет иметь полный период.

Следовательно, $\sum_{i=0}^{2^p-1} x_i = \frac{2^p - 1}{2}$ , (15)

$$\sum_{i=0}^{2^p-1} x_i^2 = \frac{(2^p - 1)(2^{p+1} - 1)}{6 \cdot 2^p} . \quad (16)$$

Таким образом, для оценки (I4) остается вычислить сумму $S = \sum_{i=0}^{2^p-1} x_i x_{i+k}$ . Из (3) получаем

$x_{i+k} = \left\{ A^k x_i + \frac{C(A^k - 1)}{2^p (A-1)} \right\}$ . Меняем порядок суммирования, $S = \sum_{i=0}^{2^p-1} \frac{i}{2^p} \left\{ \frac{A^k i + C \frac{A^k - 1}{A-1}}{2^p} \right\} .$

Пусть $A = 2^n + 1$ . Обозначим $C \frac{A^k - 1}{A - 1} = a .$

Получаем

$$S = \frac{1}{2^p} \sum_{i=0}^{2^p-1} i \left\{ \frac{(2^n+1)^k i + a}{2^p} \right\} .$$

Предствим индекс суммирования в виде

$$x = 2^{p-n}y + z\,, \qquad \begin{matrix} y=0,\dots\dots 2^n-1\,, \\ z=0,\dots\dots 2^{p-n}-1\,. \end{matrix}$$

Получаем

$$S=\frac{1}{2^p}\sum_{y=0}^{2^n-1}\sum_{z=0}^{2^{p-n}-1}(2^{p-n}y+z)\left\{\frac{(2^n+1)^k(2^{p-n}y+z)+a}{2^p}\right\}.$$

Отсюда с учетом

$$(2^n+1)^k 2^{p-n}y \equiv 2^{p-n}y \,(\mathrm{mod}\, 2^p)$$

имеем

$$S=\frac{1}{2^p}\sum_{y=0}^{2^n-1}\sum_{z=0}^{2^{p-n}-1}2^{p-n}y\left\{\frac{2^{p-n}y+(2^n+1)^k z+a}{2^p}\right\}+$$

$$+\frac{1}{2^p}\sum_{y=0}^{2^n-1}\sum_{z=0}^{2^{p-n}-1}z\left\{\frac{2^{p-n}y+(2^n+1)^k z+a}{2^p}\right\}. \qquad (I7)$$

Далее нам понадобится лемма 2.

Лемма 2

$$\sum_{i=0}^{A-1}\left\{x+\frac{i}{A}\right\}=\frac{A-1}{2}+\{Ax\}\,.$$

Доказательство леммы можно найти в /3/. Применим эту лемму ко 2-му слагаемому в (I7):

$$S_2=\frac{1}{2^p}\sum_{y=0}^{2^n-1}\sum_{z=0}^{2^{p-n}-1}z\left\{\frac{2^{p-n}y+(2^n+1)^k z+a}{2^p}\right\}=$$

$$=\frac{1}{2^p}\sum_{z=0}^{2^{p-n}-1}z\left\{\frac{(2^n+1)^k z+a}{2^{p-n}}\right\}+\frac{2^n-1}{2}\cdot\frac{2^{p-n}-1}{2^{n+1}}\,. \qquad (I8)$$

Оценим первое слагаемое в (I7):

$$S_1=\frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{z=0}^{2^{p-n}-1}y\left\{\frac{y}{2^n}+\frac{(2^n+1)^k z+a}{2^p}\right\}=$$

$$=\frac{1}{2^n}\sum_{y=0}^{2^n-1}y\sum_{z=0}^{2^{p-n}-1}\left\{\frac{y}{2^n}+\frac{(2^n+1)^k+a}{2^p}\right\}=$$



$$=\frac{1}{2^n}\sum_{y=0}^{2^n-1}y\sum_{z=0}^{2^{p-n}-1}\left\{\frac{y}{2^n}+\frac{((2^n+1)^k-1)z}{2^p}+\frac{a+z}{2^p}\right\}.$$

Всегда можно найти такие $d$ и нечетное $n_0$, что

$$(2^n+1)^k-1=2^{n+d}n_0\,, \qquad \text{т.е.} \qquad 2^d=(k,2^n).$$

Отсюда

$$S_1=\frac{1}{2^n}\sum_{y=0}^{2^n-1}y\sum_{z=0}^{2^{p-n}-1}\left\{\frac{y}{2^n}+\frac{z}{2^{p-n-d}}+\frac{a+z}{2^p}\right\}.$$

Представим $z$ в виде

$$z=2^{p-n-d}u+v\,, \qquad \begin{matrix} u=0,\dots\dots 2^d-1\,, \\ v=0,\dots\dots 2^{p-n-d}-1\,, \end{matrix}$$

$$S_1=\frac{1}{2^n}\sum_{y=0}^{2^n-1}y\sum_{u=0}^{2^d-1}\sum_{v=0}^{2^{p-n-d}-1}\left\{\frac{y}{2^n}+\frac{n_0 v}{2^{p-n-d}}+\frac{a+2^{p-n-d}u+v}{2^p}\right\}.$$

Применяя лемму I к $S_1$, получаем

$$S_1=\frac{2^{p-n}(2^n-1)}{4}+\theta\left(\frac{2^{p+n-2d}2^d(2^n-1)}{2}+\frac{2^d(2^n-1)}{4}\right);\ |\theta|\le 1.$$

Комбинируя (I7), (I8), (I9) и используя неравенство

$$\frac{1}{2^p}\sum_{z=0}^{2^{p-n}-1}z\left\{\frac{(2^n+1)^k z+a}{2^{p-n}}\right\}\le\frac{2^{p-n}-1}{2^{n+1}}\,,$$

получаем окончательную оценку для $S$:

$$S=\frac{(2^p-1)^2}{4\cdot 2^p}+\theta_0\left(\frac{3}{2}2^{p-2n}+\frac{2^d}{2^n}+\frac{2^{p-n-d}}{2}\right);\ |\theta_0|\le 1.$$

Отсюда с учетом (I4), (I5), (I6) получаем окончательную оценку для $\rho_k$:

$$|\rho_k|\le\frac{18}{2^{2n}}+\frac{24}{2^{p-n-d}}+\frac{24}{2^{n+d}}\,.$$

Таким образом, нами доказана

Теорема 3

Из $(c,2)=1$, $A=2^n+1$, $n\ge 2$

и $2^d = \left(\frac{(2^n+1)^k-1}{2^n}, 2^p\right) = (k, 2^p)$

следует

$$|\rho_k| \leq \frac{18}{2^{2n}} + \frac{24}{2^{p-n-d}} + \frac{24}{2^{n+d}} .$$

## § 4. Выводы и рекомендации

Доказанные теоремы дают возможность простой и быстрой оценки качества генераторов случайных чисел, основанных на методе вычетов. Причем в отличие от чисто статистических тестов, точность которых ограничена допустимыми размерами выборки, т.е. затратами машинного времени, оценки теорем I-3 делаются по всей возможной совокупности получающихся чисел (заметим, что период таких ГСЧ, достигающий при правильном подборе параметров значений порядка $10^{12}$, вообще бессмысленно подсчитывать на ЭВМ непосредственно). Однако в этом же заключается и определенная слабость оценок по всему периоду, т.к. они могут не совпадать с эмпирическими оценками, усредняемыми по значительно меньшей выборке. Не следует также забывать, что комбинации параметров, получаемых в теоремах 2 и 3, являются оценками $R_i$ и $\rho_k$ сверху, т.е. их противоречие с соответствующими статистическими границами еще не дает повода для браковки ГСЧ. В качестве примера можно указать хорошо известный ГСЧ с $A = 2^7 + 1$ и $C=1$.

Теорема 2 для отклонений от среднего числа серий в старших разрядах такого ГСЧ дает величину порядка $2^{p-6}$, намного превышающую среднеквадратичное значение $R_p$, имеющее порядок $2^{p/2}$.



Однако этот генератор часто используется в приложениях, т.к. показал в точных расчетах хорошие корреляционные свойства. /4/

В то же самое время, если параметры какого-либо ГСЧ удовлетворяют всем требованиям теорем I-3, то это дает нам определенную гарантию его качества. В этой связи более перспективным является применение полученных результатов для рекомендации по оптимальному выбору параметров ГСЧ с учетом конкретных особенностей ЭВМ.

Статистические оценки среднеквадратичных отклонений $R_p$ и $\rho_k$ по выборке объема $2^p$, приведенные в /2,4/, дают для них величины порядка $2^{p/2}$ и $2^{-p/2}$ соответственно. Внимательное рассмотрение оценок теорем 2 и 3 показывает, что для смешанного конгруентного генератора с А вида $2^n + 1$ оптимальное значение $n$, обеспечивающее близость этих оценок к тому, что требует статистика, достигается при $n = p/2$ .

При такой рекомендации замена умножения на А комбинацией сложения и сдвига влево на $n$ разрядов, и приведшая, собственно, к появлению смешанных конгруентных ГСЧ, оказывается слишком медленной из-за большой константы сдвига. Однако если увеличить вдвое разрядность случайных чисел, то можно заменить сдвиг на $p$ разрядов на пересылку числа из одной ячейки, изображающей правую половину случайного числа, в другую ячейку, изображающую старшие разряды.

Новый алгоритм генерации псевдослучайных чисел описывается той же формулой (I), в которой $p$ должно быть заменено на 2p, а $A = 2^p+1$. Для реализации этого алгоритма необходимы две рабочие ячейки, $\alpha$ и $\beta$, куда до начала счета должны быть засланы соответственно правая и левая половины 2p -разрядного начального числа $\gamma_0$. Должна быть также записана нечетная p-разрядная константа С. Если обозначить через $\langle x \rangle$ содержимое ячейки с адресом $x$, а зна-

ком $\Rightarrow$ засылку, то генерация очередного случайного числа может быть выполнена с помощью следующих операций:

1. $\langle\alpha\rangle + \langle\beta\rangle \Rightarrow \alpha$ .
2. $\langle\beta\rangle + C \Rightarrow \beta$ .
3. При переполнении в п.2
   $\langle\alpha\rangle + 1 \Rightarrow \alpha$ .
4. $\langle\alpha\rangle$ выдается как текущее случайное число (при необходимости может быть переведено в форму с плавающей запятой).

Сложение в п.п. I и 3 выполняется без учета переполнения, т.е. по $mod 2^P$ .

Такой генератор особенно удобен для малоразрядных ЭВМ,таких, например, как М-6000 (P=I6) или "Электроника-I00" (P=I2), требующих для реализации конгруэнтных ГСЧ обычными путями медленной арифметики с удвоенной длиной слов. Машинам же этим, применяемым обычно в качестве терминальных устройств, управляющих ЭВМ,или как часть аппаратуры на линии с экспериментом, часто требуются последовательности случайных чисел как тестовый набор для проверки каналов данных, аппаратуры и т.д.

В заключение авторы выражают благодарность А.Салтыкову за полезные обсуждения и А.Сапожникову за проведение тестовых расчетов на ЭВМ.

ЛИТЕРАТУРА

I. P.H.Lehmer. Mathematical methods in large-scale Computing units, Ann.Comp.Leb.Harvard University (1951),26, 141-146.

2. Н.В.Дунин-Барковский, Н.В.Смирнов. Теория вероятностей и математическая статистика в технике (общая часть). "Наука", Москва,I955.

3. И.М.Виноградов. Основы теории чисел. "Наука", Москва, I965.

4. Ю.Г.Полляк. Вероятностное моделирование на электронных вычислительных машинах."Сов.Радио", Москва, I97I.

Рукопись поступила в издательский отдел
29 ноября 1974 г.