ИНСТИТУТ ЯДЕРНОЙ ФИЗИКИ СО АН СССР

А.Д. Букин

О МУЛЬТИПЛИКАТИВНЫХ ГЕНЕРАТОРАХ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

ПРЕПРИНТ 86-37

НОВОСИБИРСК
1986

ON MULTIPLICATIVE GENERATORS OF PSEUDO-RANDOM NUMBERS

A.D. Bukin

ABSTRACT

In the paper the recurrent formula for pair correlation coefficient in the multiplicative sequence of pseudo-random numbers is derived. The variant of multiplicative generator for the ES-type computer is suggested.

АННОТАЦИЯ

В работе получена рекуррентная формула для парных корреляций в мультипликативной последовательности псевдослучайных чисел. Предложен вариант мультипликативного генератора для ЭВМ серии ЕС.

Моделирование случайных процессов на ЭВМ принципиально нельзя сделать без каких-либо генераторов случайных чисел. В настоящее время наибольшее распространение получили генераторы псевдослучайных чисел по методу вычетов. Впервые этот метод был предложен в [1], 1951 г. Простейшая реализация этого метода—умножение последнего случайного числа на константу k и образование из младших двоичных разрядов произведения нового случайного числа—используется в так называемых мультипликативных генераторах случайных чисел. Такую рекуррентную связь между новым z_{i+1} и старым z_i случайными числами можно записать следующим образом:

$$z_{i+1} = kz_i \pmod{2^n}, \qquad (1)$$

где целые числа z_i, z_{i+1}, k больше нуля и меньше 2^n. Здесь и далее будут обсуждаться целые псевдослучайные числа, числа с плавающей точкой получаются обычно делением получающихся целых чисел на 2^n, где n—количество двоичных разрядов в представлении целых чисел на ЭВМ. Для записи чисел, кроме десятичной системы, далее иногда будет применяться шестнадцатиричная система со стандартными обозначениями дополнительных цифр: A—10, B—11, C—12, D—13, E—14, F—15, например: $k_1 = 1\text{AFD498D}_{16}$, $k_2 = 10\text{DCD}_{16}$. Кстати, k_1 используется в качестве константы k ряда псевдослучайных чисел в генераторе RANDM в нашем Институте, а константа k_2—в генераторе RNDM в ЦЕРНе и в ряде других лабораторий, пользующихся математическим обеспечением ЦЕРНа. В литературе по методам Монте-Карло рекомендуются

константы вида $5^{(2i+1)}$, впрочем без достаточного обоснования их выделенности, а больше потому, что свойства рядов, генерируемых этими константами, лучше исследованы.

Основные свойства последовательностей псевдослучайных чисел описаны во многих учебниках по методам Монте-Карло [2, 3, 4]. Перечислим здесь результаты, касающиеся мультипликативных последовательностей.

Существование периода для последовательности z_i очевидно. Всего по модулю $N=2^n$ имеется N целых чисел, процедура получения из текущего случайного числа нового числа однозначна, поэтому не позже, чем через N чисел, снова встретится исходное случайное число и ряд чисел начнет в точности повторяться.

Очевидно, что константа ряда и все числа z_i должны быть нечетные, иначе просто младшие двоичные разряды не будут использоваться, что приведет к ухудшению статистических свойств ряда.

Теоретические результаты по периоду мультипликативной последовательности получены в 1958 году [5]. Максимальный период для мультипликативной последовательности равен $M=2^m$, где $m=n-2$, и достигается в тех последовательностях, где константа ряда принимает значение 3 или 5 по модулю 8. Примеры таких констант: 3, 5, 13, $3^{(2i+1)}$, $5^{(2i+1)}$. Всего разных констант, обеспечивающих максимальный период ряда, получается 2^m, т.е. достаточно много.

Далее везде будут приводиться результаты только для констант $k=5 \pmod 8$ по той причине, что некоторые свойства последовательностей, генерируемых такими константами, проще формулируются, чем для констант $k=3 \pmod 8$.

В зависимости от начального случайного числа любая константа $k=5 \pmod 8$ может генерировать два непересекающихся псевдослучайных ряда одинакового периода M. К одному ряду принадлежат целые числа, два младших двоичных разряда которых равны 01, к другому ряду принадлежат все целые числа с младшими двоичными разрядами 11. Объединение этих двух последовательностей дает множество всех нечетных чисел.

Если упорядочить мультипликативный ряд чисел с константой $k=5 \pmod 8$, то получится арифметическая прогрессия с разностью 4, причем в одном из двух возможных рядов минимальным числом будет 1, а в другом 3. Это означает, что в одномерном пространстве мультипликативные генераторы обеспечивают идеальную равномерность распределения случайных чисел.

Случайные числа могут использоваться для образования случайных векторов в r-мерном пространстве во многих задачах. В 1968 году в [6] было показано, что если каждые r последовательных чисел мультипликативной последовательности рассматривать как координаты точки в r-мерном пространстве, то все эти точки укладываются на довольно ограниченное количество гиперплоскостей, а именно: не более чем на $(r!2^n)^{1/r}$ гиперплоскостей. В таблице 1 выписаны результаты работы [6] для $n=32$, $n=63$ и $n=64$ и различных r. Для конкретной константы ряда число плоскостей может оказаться значительно меньше, чем указано в таблице, так как в таблице приводится верхний предел для количества гиперплоскостей, на которые укладываются все точки.

Таблица 1

r	3	4	5	6	7	8	9	10
$n=32$	2953	566	220	120	80	60	48	41
$n=63$	3811000	122000	16170	4335	1731	884	531	357
$n=64$	4801000	145000	18580	4866	1911	964	573	382

Идеальный генератор случайных чисел должен иметь нулевой коэффициент корреляции между величинами z_i и z_{i+l}. Коэффициент корреляции можно записать так:

$$Q=\frac{\langle (z_i-\langle z_i\rangle)(z_{i+l}-\langle z_{i+l}\rangle)\rangle}{\langle z_i^2-\langle z_i\rangle^2\rangle}, \qquad (2)$$

где скобками $\langle\rangle$ обозначено усреднение по периоду ряда. Так как z_i и z_{i+l} одна и та же последовательность, только сдвинутая на l позиций, $\langle z_i\rangle=\langle z_{i+l}\rangle$. Естественно, отсутствие корреляций между случайными числами является необходимым требованием, но не достаточным.

Вопросу вычисления по всему периоду ряда коэффициента корреляции Q между величинами z_i и z_{i+l} было посвящено много работ, результатом которых, в основном, были некоторые ограничения сверху на величину коэффициента корреляции. Формулу для приближенного вычисления коэффициента корреляции удалось получить в 1972 г. [7]:

$$Q^*=\frac{1}{M}\sum_{i=1}^{g-1}(-1)^{i-1}y_i+\varepsilon, \qquad (3)$$

где $|\varepsilon|<4/M$, y_i—коэффициенты разложения Евклида взаимно простых чисел M и $k_l=k^l(\mathrm{mod}\ M)$. Если обозначить $A_1=M$, $A_2=k_l$, то

$$\begin{aligned} A_1&=A_2y_1+A_3 & A_{g-2}&=A_{g-1}y_{g-2}+1\\ A_2&=A_3y_2+A_4 & A_{g-1}&=A_gy_{g-1} \qquad (4)\\ &\ldots & A_g&=1 \end{aligned}$$

Подробная информация об этой формуле, в том числе о следствиях, которые можно получить с ее помощью, содержится в [8].

В настоящей работе получена рекуррентная формула для точного вычисления коэффициента корреляции. Сама формула и ее вывод приведены в приложении 1. Естественно, при точном вычислении коэффициента корреляции появляется, вообще говоря, зависимость от того, по какому из двух возможных для данного k рядов ведется усреднение. Обозначим далее через $Q^{(1)}$ коэффициент корреляции для ряда, к которому принадлежит 1, а через $Q^{(2)}$—для ряда, содержащего 3. При численных расчетах оказалось, что $Q^{(1)}$ и $Q^{(2)}$ довольно хорошо совпадают, в редких случаях разница между ними достигает 10—20%.

Таблица 2

l	k_1		k_2		
	Q^*	$Q^{(1)}$ и $Q^{(2)}$	Q^*	$Q^{(1)}$	$Q^{(2)}$
1	$1.0\cdot10^{-8}$	$2.5\cdot10^{-9}$	$1.4\cdot10^{-5}$	$1.4\cdot10^{-5}$	$1.4\cdot10^{-5}$
2	$7.5\cdot10^{-9}$	$1.8\cdot10^{-9}$	$1.0\cdot10^{-8}$	$2.3\cdot10^{-8}$	$2.3\cdot10^{-8}$
3	$4.9\cdot10^{-8}$	$-4.8\cdot10^{-9}$	$9.3\cdot10^{-9}$	$1.2\cdot10^{-10}$	$1.2\cdot10^{-10}$
4	$-1.9\cdot10^{-8}$	$2.0\cdot10^{-8}$	$1.3\cdot10^{-7}$	$-1.6\cdot10^{-8}$	$-1.6\cdot10^{-8}$
5	$9.9\cdot10^{-8}$	$1.1\cdot10^{-7}$	$-3.3\cdot10^{-8}$	$1.4\cdot10^{-8}$	$1.6\cdot10^{-8}$
6	$-3.5\cdot10^{-8}$	$-1.3\cdot10^{-8}$	$-4.6\cdot10^{-8}$	$-1.1\cdot10^{-8}$	$-1.1\cdot10^{-8}$
7	$1.7\cdot10^{-7}$	$-1.8\cdot10^{-8}$	$2.4\cdot10^{-8}$	$2.6\cdot10^{-8}$	$2.6\cdot10^{-8}$
8	$-6.9\cdot10^{-8}$	$2.6\cdot10^{-9}$	$-6.5\cdot10^{-9}$	$6.0\cdot10^{-9}$	$6.0\cdot10^{-9}$
9	$-6.7\cdot10^{-8}$	$-1.0\cdot10^{-7}$	$1.1\cdot10^{-5}$	$-1.4\cdot10^{-6}$	$-1.4\cdot10^{-6}$
10	$-1.3\cdot10^{-8}$	$4.3\cdot10^{-9}$	$4.9\cdot10^{-8}$	$-2.0\cdot10^{-8}$	$-2.0\cdot10^{-8}$

В таблице 2 приведены результаты расчетов коэффициента корреляции для констант ряда k_1 и k_2. В коэффициенте корреляции Q^* по формуле Антипова величина ε отброшена. Для $n=32$ $\varepsilon\leqslant4/M\approx3.7\cdot10^{-9}$. Коэффициенты корреляции расчитаны для нескольких значений смещения l, т.е. при $l=3$ исследуются корреляции случайного числа z_i и следующего за ним через два числа z_{i+3}. Оказалось, что для константы k_1 коэффициенты корреляции $Q^{(1)}$ и $Q^{(2)}$ совпадают с точностью до приведенного количества значащих цифр, поэтому в таблицах колонки для этих величин совмещены.

Из таблицы 2 видно, что формула Антипова (3) дает хорошее приближение для коэффициента корреляции, хотя в некоторых случаях отклонение больше, чем $4/M$.

Зависимость коэффициента корреляции от l носит немонотонный характер, однако, чем больший интервал значений l просматривать, тем вероятнее получить значение коэффициента корреляции, больше заданного. Максимальное значение Q, равное 1, будет достигнуто, по крайней мере, при $l=M$. Таблица 3 дает представление о «глубине некоррелированности». В некотором смысле она является продолжением таблицы 2. В каждой клетке таблицы приведено два числа: значение коэффициента корреляции Q и l, при котором это значение достигнуто, причем это значение по абсолютной величине больше коэффициентов корреляции при меньших l Вычисления проводились до $l=5500$ и, естественно, независимо для двух констант k_1, k_2 и для Q^*, $Q^{(1)}$, $Q^{(2)}$. В таблице 3 оказалось возможным объединить колонки с $Q^{(1)}$ и $Q^{(2)}$ для обеих констант.

Погрешность в расчетах по методу Монте-Карло, которую вносит коррелированность чисел в генераторе случайных чисел, совсем не просто оценить. Более того, величина погрешности зависит от характера решаемой задачи. Поэтому очевидно, что при прочих равных условиях желательно иметь пренебрежимо малый коэффициент корреляции.

Для машин серии ЕС легко сделать генератор псевдослучайных чисел с $n=32$, так как в наборе команд имеется команда умножения целых 32-разрядных чисел. Однако, с учетом быстродействия современных ЭВМ мультипликативный генератор с $n=32$ производит впечатление недостаточно хорошего для многих задач. В частности, вполне реально по времени достижение периода ряда ($M\approx10^9$ для $n=32$). При интегрировании функций, скажем, в 5-мерном пространстве тот факт, что все точки в гиперкубе ложат-

ся не более, чем на 220 гиперплоскостей, будет вызывать беспокойство и вынуждать проводить довольно тяжелые исследования систематической ошибки, порождаемой этим свойством случайных чисел.

Таблица 3

k_1		k_2	
Q^*	$Q^{(1)}$ и $Q^{(2)}$	Q^*	$Q^{(1)}$ и $Q^{(2)}$
$2.6\cdot10^{-7}$ 33	$-1.3\cdot10^{-7}$ 33	$-1.9\cdot10^{-5}$ 99	$-1.5\cdot10^{-5}$ 466
$1.8\cdot10^{-6}$ 35	$1.9\cdot10^{-6}$ 35	$1.2\cdot10^{-4}$ 466	$5.9\cdot10^{-5}$ 565
$2.1\cdot10^{-5}$ 241	$-2.5\cdot10^{-6}$ 241	$-4.7\cdot10^{-4}$ 565	$6.3\cdot10^{-5}$ 2749
$1.8\cdot10^{-4}$ 2648	$-3.1\cdot10^{-6}$ 466	$-5.0\cdot10^{-4}$ 2749	
$-7.1\cdot10^{-4}$ 5125	$6.3\cdot10^{-6}$ 924		
	$1.8\cdot10^{-4}$ 2648		

Представляется очень привлекательным существенно улучшить статистические свойства генератора случайных чисел на ЭВМ серии ЕС за счет программной реализации команды умножения целых чисел с $n>32$. Естественно, генератор случайных чисел с двойной точностью недопустимо делать, объединяя по два числа из одного ряда 32-разрядных чисел в одно число с двойной точностью. Период ряда при этом, например, уменьшится в два раза.

Вариант возможного генератора (программа названа DRANDM) с «почти двойной» точностью ($n=63$) на языке Ассемблер приведен в приложении 2. Константа ряда выбрана равной $k_3=40010115_{16}$. Коэффициент корреляции для нескольких первых значений l приведен в таблице 4.

Из-за малой величины k, по сравнению с M, для $l=1$ получается относительно большая величина Q, а затем она сильно уменьшается. В интервале $l=2, 3, \ldots, 6000$ любой из трех коэффициентов корреляции (Q^*, $Q^{(1)}$, $Q^{(2)}$) не превышает по абсолютной величине $2\cdot10^{-13}$.

Таблица 4

l	1	2	3	4	5
Q^*	$9.3\cdot10^{-10}$	$1.8\cdot10^{-15}$	$-3.6\cdot10^{-17}$	$-4.1\cdot10^{-17}$	$-1.6\cdot10^{-17}$
$Q^{(1)}$	$9.3\cdot10^{-10}$	$-2.3\cdot10^{-16}$	$9.6\cdot10^{-18}$	$-4.1\cdot10^{-17}$	$5.9\cdot10^{-18}$
$Q^{(2)}$	$9.3\cdot10^{-10}$	$-2.3\cdot10^{-16}$	$1.2\cdot10^{-17}$	$-4.2\cdot10^{-17}$	$-1.0\cdot10^{-17}$

Проверка статистических свойств генератора должна включать проверку на равномерность распределения случайных векторов, образованных r последовательными случайными числами, в единичном гиперкубе. В таблице 5 приведена степень согласия распределения случайных векторов с равномерным распределением по критерию χ^2: p—количество одинаковых отрезков, на которые разбивается каждое ребро единичного гиперкуба, N—количество случайных векторов, вошедших в данную выборку.

Таблица 5

r	1	2	3	4	5
p	100	20	20	10	6
N, тыс.	490	1380	920	706	543
$P(\chi^2)$	0.415	0.280	0.287	0.604	0.524

Период последовательности с $n=63$ и $k=k_3$ равен $M=2^{61}\approx2.3\cdot10^{18}$. Такой генератор обладает гораздо лучшими статистическими свойствами, чем генератор с $n=32$. Единственным возражением может быть только то, что на генерацию одного числа требуется больше времени при программной реализации команды умножения. Непосредственное измерение времени на одно обращение дало для RANDM 18.5, для RNDM—12.9, для DRANDM—23.0 микросекунд. Различие в два раза, по-видимому, является пренебрежимо малым, так как, кроме генерации случайных чисел, как правило, необходимо производить достаточно много арифметических и логических операций. Таким образом, в большинстве случаев увеличение общего времени счета при использовании генератора с двойной точностью будет не больше 10%. В тех же случаях, когда счет в основном состоит из вызовов генератора случайных чисел, этих случайных чисел будет использоваться

много, и их статистические свойства более существенны.

В заключение автор выражает благодарность М.В. Антипову за полезные обсуждения.

Приложение 1.

ВЫЧИСЛЕНИЕ КОЭФФИЦИЕНТА КОРРЕЛЯЦИИ

Коэффициент корреляции между случайными числами одного и того же ряда z_i можно записать так:

$$Q=\frac{\langle (z_i-\langle z_i\rangle)(z_{i+l}-\langle z_{i+l}\rangle)\rangle}{\langle z_i^2-\langle z_i\rangle^2\rangle}, \qquad (\text{П1.1})$$

где усреднение в виде суммы записывается, как

$$\langle z_i\rangle=\frac{1}{M}\sum_{i=0}^{M-1} z_i,$$

M—период ряда.

Так как z_i и z_{i+l} одна и та же последовательность, только циклически смещенная на l членов, то $\langle z_i\rangle=\langle z_{i+l}\rangle$. Здесь мы будем рассматривать только константы ряда $k=5 \pmod 8$. Как уже указывалось в основном тексте, период такого ряда $M=2^{n-2}$. Пользуясь тем, что мы знаем состав мультипликативной последовательности, можно поменять порядок суммирования в (П1.1) так, чтобы все z_i были упорядочены по величине. Тогда z_i можно записать в виде

$$z=z_0+4q, \quad q=0, 1, 2, \ldots, M-1, \qquad (\text{П1.2})$$

$M=2^{n-2}=2^m$—период ряда, z_0 может иметь значение 1 или 3.

Легко вычислить $\langle z\rangle$ и дисперсию z:

$$\langle z_i\rangle=\langle z_{i+l}\rangle=z_0+\frac{4}{M}\sum_{q=0}^{M-1} q=z_0+2\cdot(M-1), \qquad (\text{П1.3})$$

$$\langle z_i^2-\langle z_i\rangle^2\rangle=\frac{4}{3}(M^2-1). \qquad (\text{П1.4})$$

Очевидно, что величина $z_{i+l}=z_i k^l \pmod N$. Вместо k^l можно ввести константу $k_l=k^l \pmod N$. Теперь $u=k_l z$ можно записать в виде

$$u=k_l z_0+4k_l q \pmod N, \quad q=0, 1, 2, \ldots, M-1, \qquad (\text{П1.5})$$

$$k_l z_0 \pmod N=z_0+4d, \qquad (\text{П1.6})$$

где

$$d=(k_l-1)\ z_0/4 \pmod M . \qquad (\text{П1.7})$$

Из последнего равенства следует, что $0\leqslant d<M$. Теперь можно переписать (П1.5) в другом виде

$$u=z_0+4(d+k_l q-sM) . \qquad (\text{П1.8})$$

Здесь вместо обозначения mod M введена целочисленная функция $s(q)$ такая, что $0\leqslant d+kq-sM<M$. Учитывая, что $\langle z-\langle z\rangle\rangle=0$, можно выражение для Q записать следующим образом:

$$Q=\frac{6}{M(M^2-1)}\sum_{q=0}^{M-1}(2q+1-M)(k_l q-sM) , \qquad (\text{П1.9})$$

где функция $s(q)$ такая, что

$$0\leqslant d+k_l q-s(q)\ M<M . \qquad (\text{П1.10})$$

В такой записи становится очевидным, что если $k_l>M$, то вместо k_l можно использовать его значение по модулю M, что просто сведется к переопределению функции $s(q)$, а Q останется неизменным. Обозначим теперь $A_1=M$, $A_2=k_l \pmod M$, $B_1=z_0(k_l-1)/4 \pmod M$ и проведем разложение Евклида:

$$\begin{aligned} &A_1=A_2y_1+A_3, && A_{g-2}=A_{g-1}y_{g-2}+1,\\ &A_2=A_3y_2+A_4, && A_{g-1}=A_g y_{g-1}, \\ &\ldots && A_g=1, \end{aligned} \qquad (\text{П1.11})$$

$$B_i=A_{i+1}x_i+B_{i+1}, \qquad (\text{П1.12})$$

где $A_i>A_{i+1}>0$, $A_i>B_i\geqslant 0$.

Длина ряда A_i существенно меньше M при больших M. Введем систему целочисленных функций $q_{i+1}(q_i)$ таких, что

$$0\leqslant B_i+(-1)^{i-1}\ (q_i A_{i+1}-q_{i+1}A_i)<A_i . \qquad (\text{П1.13})$$

Если обозначить через D_i вспомогательные суммы вида

$$D_i=\frac{2}{A_i}\sum_{q_i=0}^{A_i-1}(2q_i+1-A_i)\ (q_iA_{i+1}-q_{i+1}A_i)\ , \qquad (\text{П1.14})$$

то коэффициент корреляции Q запишется так:

$$Q=\frac{3}{A_1^2-1}D_1\ . \qquad (\text{П1.15})$$

Для того, чтобы сводить суммы по q_i к другим суммам по q_{i+1}, необходимо ввести целочисленные функции $b_i(q_{i+1})$, которые принимают наименьшее возможное значение q_i при заданном q_{i+1}. Тогда любую сумму по q_i от произвольной функции $f(q_i, q_{i+1})$ можно записать в виде

$$\sum_{q_i=0}^{A_i-1} f(q_i, q_{i+1})=\sum_{q_{i+1}=0}^{A_{i+1}}\ \sum_{q_i=b_i(q_{i+1})}^{b_i(q_{i+1}+1)-1} f(q_i, q_{i+1})\ . \qquad (\text{П1.16})$$

Однако, чтобы преобразование сумм было правильным, необходимо данное выше определение функций b_i дополнить двумя выделенными значениями:

$$b_i(0)=0, \qquad b_i(A_{i+1}+1)=A_i\ . \qquad (\text{П1.17})$$

Легко убедиться, анализируя неравенства (П1.13), что при нечетном i функция $b_i(q_{i+1})$ принимает значения:

$$b_i\ (q_{i+1})=y_i\ q_{i+1}-x_i+q_{i+2}\ (q_{i+1})\ , \qquad (\text{П1.18})$$

а при четном i

$$b_i\ (q_{i+1})=y_i\ q_{i+1}+x_i-y_i+1+q_{i+2}\ (q_{i+1}-1)\ . \qquad (\text{П1.19})$$

Введем функции c_i^+ и c_i^-, которые позволят объединить формулы (П1.18) и (П1.19):

$$c_i^+=\frac{1}{2}[1+(-1)^i], \quad c_i^-=\frac{1}{2}[1-(-1)^i]\ . \qquad (\text{П1.20})$$

$$b_i\ (q_{i+1})=y_i\ q_{i+1}+q_{i+2}\ (q_{i+1}-c_i^+)+(c_i^+-c_i^-)x_i-c_i^+(y_i-1)\ . \qquad (\text{П1.21})$$

Введем также вспомогательные суммы:

$$P_i=\sum_{q_i=0}^{A_i-1} q_{i+1}\ , \qquad (\text{П1.22})$$

$$R_i=\sum_{q_i=0}^{A_i-1} q_i\,q_{i+1}\ , \qquad (\text{П1.23})$$

$$L_i=\sum_{q_i=0}^{A_i-1} q_{i+1}^2\ , \qquad (\text{П1.24})$$

$$H_{i+1}=\sum_{q_{i+1}=0}^{A_{i+1}} b_i\ (q_{i+1})\ , \qquad (\text{П1.25})$$

$$G_{i+1}=\sum_{q_{i+1}=0}^{A_{i+1}} b_i^2\ (q_{i+1})\ . \qquad (\text{П1.26})$$

Последовательно применяя замену суммирования, можно получить следующие соотношения между введенными суммами:

$$D_i=\frac{A_{i+1}\ (A_i^2-1)}{3}+2\ (A_i-1)\ P_i-4R_i\ , \qquad (\text{П1.27})$$

$$P_i=A_i\ A_{i+1}-H_{i+1}\ , \qquad (\text{П1.28})$$

$$R_i=0.5\ (A_i\ (A_i-1)\ A_{i+1}-G_{i+1}+H_{i+1})\ , \qquad (\text{П1.29})$$

$$H_{i+1}=c_i^-\ A_i+(c_i^++x_i(c_i^+-c_i^-))\,A_{i+1}+P_{i+1}+y_i\frac{(A_{i+1}-1)\,A_{i+1}}{2}\ , \qquad (\text{П1.30})$$

$$G_{i+1}=c_i^-\ (A_i-2x_i)\ A_i+y_i^-\frac{A_{i+1}\ (A_{i+1}-1)\ (2A_{i+1}-1)}{6}+2y_i\ R_{i+1}+$$

$$+[c_i^+\ +(c_i^+-c_i^-)\,x_i]^2\,A_{i+1}+L_{i+1}+ \qquad (\text{П1.31})$$

$$+2[c_i^+\ +(c_i^+-c_i^-)\,x_i]\left[\frac{y_i\,A_{i+1}\ (A_{i+1}-1)}{2}+P_{i+1}\right],$$

$$L_{i+1}=(A_{i+2}-2c_i^+)\ P_{i+1}+c_i^+[A_{i+1}\ (A_{i+2}-1)+2x_{i+1}\,A_{i+2}]+ \qquad (\text{П1.32})$$

$$+\frac{D_{i+2}}{2}-\sum_{q_{i+2}=0}^{A_{i+2}-1}(2q_{i+2}+1-A_{i+2})\left[\frac{A_{i+1}}{A_{i+2}}q_{i+2}-(c_i^+-c_i^-)\ x_{i+1}+c_i^-\right],$$

$$R_{i+1}=\frac{A_{i+2}\ (A_{i+1}^2-1)}{12}+\frac{A_{i+1}-1}{2}P_{i+1}-\frac{D_{i+1}}{4}\ . \qquad (\text{П1.33})$$

Если ввести еще одну вспомогательную сумму

$$W_i=P_i-\frac{(A_i-1)\ (A_{i+1}+c_i^+-c_i^-)}{2}+(c_i^+-c_i^-)\,B_i\ , \qquad (\text{П1.34})$$

то нетрудно убедиться, что для нее рекуррентное соотношение

получается совсем простым:

$$W_i = -W_{i+1} \qquad (П1.35)$$

При $i=g$, т.е. в конце ряда A_i, многие суммы принимают нулевое значение:

$$P_g = R_g = L_g = D_g = W_g = 0\ . \qquad (П1.36)$$

Для суммы W_i это приводит к тому, что $W_i=0$ при любом i. Учитывая это, для P_i можно написать явное выражение:

$$P_i = \frac{(A_i-1)\ (A_{i+1}+c_i^+-c_i^-)}{2} - (c_i^+ - c_i^-)\ B_i\ . \qquad (П1.37)$$

Подставляя полученные соотношения в выражение (П1.27) для D_i, получаем рекуррентную формулу:

$$D_i = -D_{i+1}\ y_i + D_{i+2} + \frac{1}{3} Z_i\ , \qquad (П1.38)$$

где

$$Z_i = \frac{1}{A_{i+1}}[6\ (A_i B_{i+1} - 2c_i^+\ A_{i+1}\ B_{i+2} -$$

$$-(c_i^+ - c_i^-)\ (A_i B_{i+1} - A_{i+1}\ B_i - A_{i+2}\ B_{i+1}) + \qquad (П1.39)$$

$$+B_i\ (B_i - A_i + 1) - B_{i+1}\ (B_{i+1} - A_{i+1} + 1)) +$$

$$+(A_i - A_{i+2})\ (A_i + A_{i+2} - 3\ (A_{i+1} + c_i^+ - c_i^-))]\ .$$

Для промежуточных преобразований выражений была использована программа REDUCE [7].

Если ввести такие величины Q_i, что $Q = Q_1$:

$$Q_i = \frac{3}{A_i^2 - 1} D_i\ , \qquad (П1.40)$$

то можно переписать рекуррентное соотношение (П1.38) для них:

$$Q_i = a_1\ Q_{i+1} + a_2\ Q_{i+2} + a_3\ , \qquad (П1.41)$$

где

$$a_1 = -\frac{(A_i - A_{i+2})\ (A_{i+1}^2 - 1)}{A_{i+1}\ (A_i^2 - 1)}\ ,$$

$$a_2 = \frac{A_{i+2}^2 - 1}{A_i^2 - 1}\ ,$$

$$a_3 = \frac{Z_i}{A_i^2 - 1}\ .$$

Приложение 2.

ВАРИАНТ ГЕНЕРАТОРА С $n=63$

Программная реализация умножения целых чисел с $n=63$ двоичных разрядов на языке Ассемблер для ЭВМ серии ЕС может выглядеть следующим образом:

```
DRANDM  START
        STM     14,12,12(13)
        USING   DRANDM,15       Y=DRANDM(X)
        USING   DRAND,12        или
        L       12,=A(DRAND)    QY=DRANDM(X) DOUBLE PREC.QY
        LM      6,7,K1
        SLDL    6,1             генератор с 63 двоич.разрядами
        LR      9,6
        SRL     7,1             23.0 мкс/DRANDM на EC-1061
        M       6,KK
        M       8,KK
        SLDL    6,1
        ALR     6,9
        SRDL    6,1
        STM     6,7,K1
        SRDL    6,7
        STM     6,7,F
        MVI     F,X'40'
        SDR     0,0
        AD      0,F
        LM      14,12,12(13)
        BR      14
F       DS      D
KK      DC      XL4'40010115'
        LTORG
DRAND   CSECT
K1      DC      F'0'
```

```
K2      DC      F'1'
        END
```

На языке Фортран к этой программе надо обращаться, как к программе-функции, например, Q= DRANDM(*X*), где *X*—фиктивный аргумент (никак не используется). Если тип DRANDM никак не описан в вызывающей программе, то от сформированного случайного числа двойной точности будет взята только старшая часть мантиссы, если же в вызывающей программе описать

```
DOUBLE PRECISION DRANDM
```

то будут использоваться случайные числа двойной точности.

Исходное случайное число задается в общем блоке /DRAND/ в виде двойного слова, причем самый старший из 64 двоичных разрядов игнорируется.

ЛИТЕРАТУРА

1. *D.H Lehmer.* Ann. Comp. Lab. Harvard Univ. 26 (1951) 141.
2. *С.М. Ермаков, Г.А. Михайлов.* Статистическое моделирование. М.: Наука, 1982.
3. *С.М. Ермаков.* Метод Монте-Карло и смежные вопросы. М.: Наука, 1975.
4. *И.М. Соболь.* Численные методы Монте-Карло. М.: Наука, 1973.
5. *Eve Bofinger and V.J. Bofinger.* On a Periodic Property of Pseudo-Random Sequences.—J. of the Association for Computing Machinery, 5 (1958) 261—265.
6. *G. Marsaglia.* Proc. Nat. Acad. Sci, 61 (1968) 25.
7. *М.В. Антипов.* О корреляционном коэффициенте полного периода псевдопоследовательности.—Вычислительные системы, ИМ СО АН СССР, 50 (1972), с.143—154. Новосибирск.
8. *М.В. Антипов.* Исследование псевдослучайных чисел в связи с решением задач математической физики. Кандидатская диссертация, ВЦ СО АН СССР. Новосибирск, 1983.
9. *A.C. Hearn.* RAND publ. CP-78 (4/83).

А.Д. Букин

О мультипликативных генераторах псевдослучайных чисел

Ответственный за выпуск С.Г.Попов

Работа поступила 4 февраля 1986 г.
Подписано в печать 17.02.1986 г. МН 11663
Формат бумаги 60×90 1/16 Объем 1,7 печ.л., 1,4 уч.-изд.л.
Тираж 290 экз. Бесплатно. Заказ № 37

Набрано в автоматизированной системе на базе фотонаборного автомата ФА1000 и ЭВМ «Электроника» и отпечатано на ротапринте Института ядерной физики СО АН СССР,
Новосибирск, 630090, пр. академика Лаврентьева, 11.