СИБИРСКОЕ ОТДЕЛЕНИЕ АКАДЕМИИ НАУК СССР

Препринт.

В.Д.Беренов, Б.В.Чириков.

ОБ АРИФМЕТИЧЕСКОМ МОДЕЛИРОВАНИИ СЛУЧАЙНЫХ ВЕЛИЧИН.

Новосибирск
1964 г.

V.D.BERENOV, B.V.CHIRIKOV.

CONCERNING ARITHMETICAL IMITATION OF RANDOM NUMBERS.

Arguments are put forward the algorism written below appears to be universal one for producing pseudorandom numbers by digital computer. The algorism is given by the expression: $x_{n+1} = \{\beta x_n\}$ where curly brackets indicate fractional part of argument. Requirements for β, x_0 are following: a) $1 \ll \beta < \sqrt{m}$ where m is the full quantity of different numbers in computer; b) all digits of β, x_0 are random. The item b) distinguishes the algorism suggested from a common multiplicative congruential one. In the latter case the quantity β is a very round number. The results of five different statistical tests of the algorism agree with the assumption that numbers x_n are random.

В настоящее время наиболее широко распространенным методом получения так называемых псевдослучайных чисел на ЭВМ является арифметический метод, т.е. задание определенного алгоритма. Насколько нам известно, в настоящее время не существует теории построения соответствующих алгоритмов. Действующие алгоритмы основаны на чисто эмпирических и наглядных соображениях о "хорошем перемешивании" цифр.[x] Более того, в некоторых работах (например /3/) стараются построить такой алгоритм, который давал бы так называемый полный период ($= m$, где m - число различных чисел в ЭВМ), что противоречит требованию случайности получаемых чисел. Существует даже мнение, что следует разрабатывать специализированные алгоритмы, моделирующие лишь некоторые черты случайных процессов.

Нам кажется, однако, что имеется один естественный путь построения универсальных алгоритмов псевдослучайных чисел. Он основан на моделировании случайного процесса с помощью динамической системы с перемешиванием /4/. Последний термин означает определенный тип движения, похожий на случайное. Единственное отличие связано с некоторой корреляцией между значениями координат системы в различные моменты времени. Эти корреляции являются принципиальными, поскольку движение динамической системы подчиняется точным уравнениям (алгоритму), не содержащим никакого случайного элемента. Однако для специального случая перемешивания - так называемого движения с конечной энтропией /5/, упомянутые корреляции экспоненциально убывают со временем и потому практически несущественны. Кроме того, если фиксировать лишь округленные значения координат динамической системы, то корреляции могут быть полностью устранены.

Одна из простейших динамических систем с перемешиванием и конечной энтропией задается уравнением:

$$x_{n+1} = \{\beta x_n\} \qquad (1)$$

где фигурная скобка означает дробную часть аргумента. Свойства этой динамической системы подробно исследованы в /6/. Перемешивание имеет место при $\beta > 1$. Энтропия на один шаг равна $\ln \beta$ (для целых β). Это означает, в частности, что парные корреляции убывают по закону

$$\rho(k) = \frac{\langle (x_{n+1} - 1/2)(x_n - 1/2) \rangle}{\langle (x_n - 1/2)^2 \rangle} = \beta^{-k} \qquad (2)$$

---

x) Исключение составляют работы /1,2/. Однако, насколько нам известно, алгоритмы, предложенные в этих работах, не находят пока практического применения ввиду их сложности.

Для устранения этих остаточных корреляций с помощью округления необходимо, чтобы $\Delta x_n > \beta^{-l}$, где Δx_n - погрешность округления, а l - расстояние между используемыми числами в последовательности (I).

Основная трудность, возникающая при попытке применить алгоритм (I) для получения случайных чисел на ЭВМ, связана с конечным числом разрядов в машине. Аналитическое исследование поведения последовательности (I) в этом случае представляет значительные трудности. x) Можно, однако, надеяться, что если выбрать в качестве β и x_0 не слишком "круглые" числа, то в пределах периода ($\sim\sqrt{m}$) отклонения последовательности (I) от случайной будут незначительны.

Нами произведена проверка статистических свойств указанного алгоритма для серии в 10^4 чисел. Никакого специального подбора "счастливых" чисел β, x_0 не требуется, необходимо только чтобы $\beta >> 1$ (для уменьшения корреляций (2)), но не больше $\sim\sqrt{m}$, так как в противном случае корреляции снова возрастают из-за конечного числа разрядов /3/. Кроме того при выборе чисел β, x_0 должны быть использованы все разряды машины; мантиссы β, x_0 лучше всего взять в виде набора случайных цифр. В этом пункте алгоритм (I) существенно отличается от известного мультипликативного алгоритма

$$x_{n+1} = \beta x_n \pmod m \qquad (3)$$

поскольку в последнем случае β всегда целое, т.е. является слишком "круглым" (по крайней мере половина разрядов - нули), что ухудшает статистические свойства алгоритма (3).

Для проверки статистических свойств алгоритма (I) использовались следующие тесты:

I) Проверка частот величины (x_n) /7/, 256 интервалов.

2) Проверка частот двумерной величины (x_n , $x_{n+\kappa}$) /7/, I6xI6 интервалов, для исследования парных корреляций ($\kappa = 5 \div 700$).

3) Проверка частот величины ($\xi_n^{(i)}, \xi_{n+1}^{(i)}, \dots, \xi_{n+l-1}^{(i)}$), где $\xi_n^{(i)}$ значение i-го разряда числа x_n, для оценки l -кратных корреляций Производилась проверка на равномерность нового l -разрядного числа, составленного из величин $\xi_n^{(i)}, \dots, \xi_{n+l-1}^{(i)}$ ($l = 8$; $i = 3; 12$).

4) Проверка частот величины $\{2^K x_n\}$ для K=6; I6.

---

x) В этом смысле работа /I/ находится в исключительном положении, поскольку один из предлагаемых в ней алгоритмов годится для любого числа разрядов.

5) Проверка на случайность методом серий /7/. Все методы проверки дали удовлетворительные результаты, не противоречащие предположению о случайности чисел (x_n). Желательна дальнейшая проверка этого алгоритма.

Пользуемся случаем выразить благодарность А.А.Боровкову, Ю.М.Волошину и А.П.Ермову за полезные обсуждения.

Литература

I. А.Г.Постников. Арифметическое моделирование случайных процессов. Труды мат.ин-та им.Стеклова, LVII, I960.

2. И.Б.Кубилюс, Ю.В.Линник. Изв. вузов, мат., I959, № 6 (I3), 88.

3. T.E. Hull, SIAM Review, 4, n3 (1962).

4. П.Р.Халмош. Лекции по эргодической теории, ИЛ, I959.

5. Я.Г.Синай, ДАН, I25, I200 (I959)

6. В.А.Рохлин. Изв.АН СССР, мат., 25, 499 (I96I).

7. Метод статистических испытаний. Физматгиз, I962.

Ответственный за выпуск Г.Б.Глаголев
Подписано к печати 4.09.64. МН00617
Формат бумаги 270xI90, тираж 250 экз.

Отпечатано на ротопринте в Институте ядерной физики СО АН СССР.