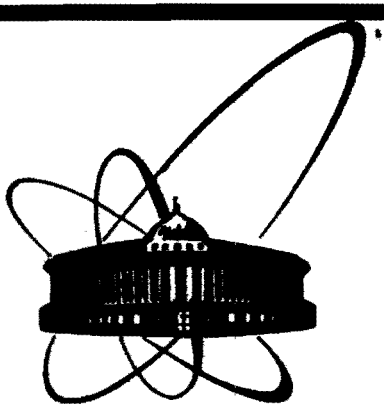


сообщения
объединенного
института
ядерных
исследований
дубна

Q-756

P11-87-816

Г.А.Ососков, Е.С.Пшенин*, Е.Шандрикова

ОБ ОДНОМ МНОГОМЕРНОМ ТЕСТЕ ПРОВЕРКИ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ

*Институт физики высоких энергий АН КазССР, Алма-Ата

1987

При решении многих задач фундаментального и прикладного характера большую роль играет статистическое моделирование исследуемых процессов на ЭВМ. Монте-карловская модель процесса позволяет решать конкретную задачу и допускает обобщения на другие случаи.

Для имитационного моделирования необходимо уметь получать на ЭВМ выборки из вероятностных моделей - последовательности случайных величин с заданным законом распределения. Для этого необходимо иметь:

1/ генератор случайных чисел /ГСЧ/, равномерно распределенных на интервале $[0,1]$, удовлетворяющих необходимым критериям случайности генерируемой последовательности $\{\xi_i\}$;

2/ набор алгоритмов для преобразования равномерно распределенных чисел $\{\xi_i\}$ в последовательность случайных величин с заданными характеристиками;

3/ компактную систему достаточно мощных критериев для верификации соответствия полученной случайной последовательности и моделируемого стохастического процесса.

Многолетный опыт расчетов по методу Монте-Карло показал преимущества программной генерации случайных чисел по сравнению с источником в виде таблиц или датчиков случайных чисел. Используя равномерный на $[0,1]$ генератор, можно построить процедуру получения псевдослучайных чисел с практически любым законом распределения[1]:

$$\xi_i = \frac{\int_{-\infty}^{x_i} f(X)dX}{\int_{-\infty}^{+\infty} f(X)dX}, \qquad /1/$$

где x_i - псевдослучайная величина с законом распределения $f(X)$.

Математическое обоснование алгоритма преобразования равномерно распределенных случайных чисел $\{\xi_i\}$ /1/ в случайную последовательность с требуемыми характеристиками освобождает от необходимости проверки качества этой последовательности, если случайность и равномерность исходной последовательности $\{\xi_i\}$ гарантированы.

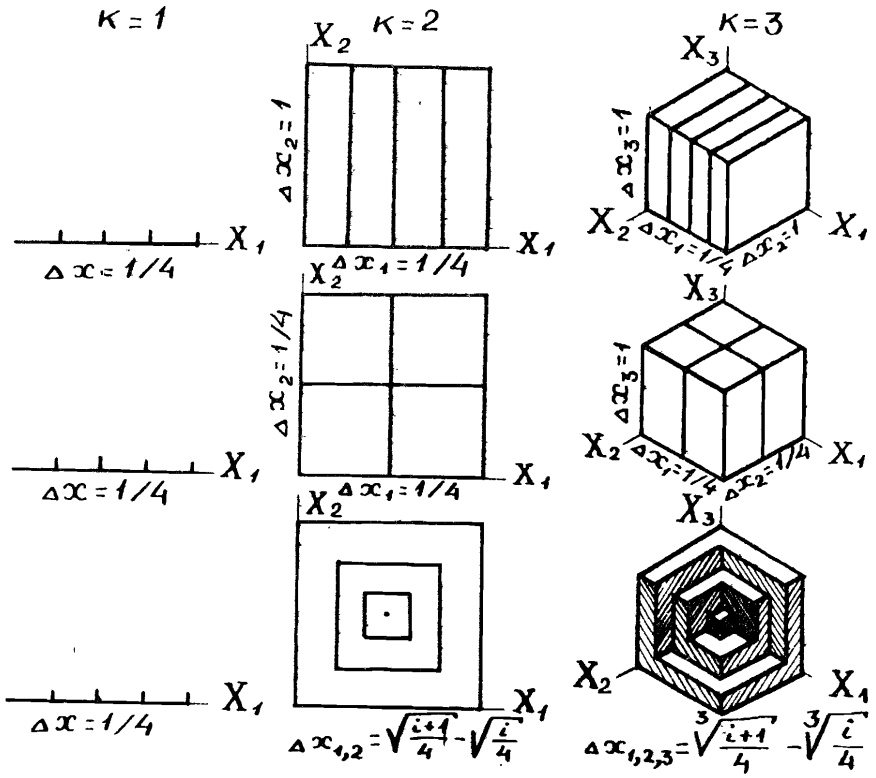
Высокие требования, предъявляемые к ГСЧ в многолетней практике расчетов по методу Монте-Карло, привели к необходимости де-

Вычислительный институт
сибирского отделения

тальной проверки качества получаемых псевдослучайных последовательностей на различных ЭВМ.

Широкое применение линейно-конгруэнтного метода[2] получения ГСЧ на ЭВМ с малой разрядностью слова может привести к нежелательным эффектам типа петель с малым периодом, из-за общности области определения и области значений функции ГСЧ и неправильного подбора ее параметров, или попарной корреляции, из-за решетчатой структуры области значений таких генераторов. Последний дефект ГСЧ практически не диагностируется стандартными методами проверки на равномерность.

Разрабатываемые в последнее время генераторы случайных чисел для персональных ЭВМ, не основанные на теоретико-числовых законах[3], а также многомерные ГСЧ, использующие физические модели[4], не допускают проверки по теоретическим тестам/то есть тестам, основанным на исследовании теоретико-числовых свойств исходного рекуррентного соотношения, см., например,[2,5,6]/, необходима тщательная проверка ГСЧ по какой-либо системе статистических тестов, которую мы, следуя Д.Кнуту[2], будем называть эмпирической. Приведенный, например, в[2] достаточно полный набор таких тестов довольно громоздок и требует значительных затрат машинного времени.



Виды разбиения единичного куба в R^1, R^2 и R^3.

Все это привело авторов к идее конструирования такого теста, который при достаточной мощности был бы по возможности прост в вычислениях /что особенно важно при работе на мини-, микро- и персональных ЭВМ/.

Предложение одного из авторов[7] использовать в качестве критерия, учитывающего сразу все виды зависимостей между членами последовательности $\{\xi_i\}$, информационную систему С.Кульбака[8] также привело к громоздким вычислениям, объем которых быстро увеличивается с ростом размерности единичного гиперкуба из-за степенного роста числа ячеек гистограммы.

В этой связи предлагается такое специальное разбиение единичного гиперкуба, которое сохраняет при любой размерности число и равенство объемов ячеек многомерной гистограммы /рис.1/.

Теоретическое представление. Имеется выборка из n чисел $\{a_1, a_2, \ldots, a_n\}$, каждое из которых может принимать значения 0, 1,..., к-1 /к - основание принятой системы счисления/.

Определим вероятность появления комбинации с максимальным значением a_i.

Рассмотрим следующие выборки:

I. $n = 2$; $k = 2$; $a_i = 0,1$; $i = 1,2$. Возможные комбинации: {0, 0}, {0,1}, {1,0}, {1,1}.

В соответствии с условием разобъем все возможные комбинации на две группы:

а/ {0,0}, $p_1 = 1/4$;

б/ {0,1}, {1,0}, {1,1}; $p_2 = 3/4$.

II. $n = 3$; $k = 2$; $a_i = 0,1$; $i = 1,2,3$. Возможные комбинации: {0,0,0}, {0,0,1}, {0,1,0}, {0,1,1}, {1,0,0}, {1,0,1}, {1,1,0}, {1,1,1};

а/ {0,0,0}; $p_1 = 1/8$;

б/ {0,0,1}, {0,1,0}, {0,1,1}, {1,0,0}, {1,0,1}, {1,1,0}, {1,1,1}; $p_2 = 7/8$.

III. $n = 4$; $k = 2$; $a_i = 0,1$; $i = 1,2,3,4$; $p_1 = 1/16$; $p_2 = 15/16$.

IV. $n = 2$; $k = 3$; $a_i = 0,1,2$; $i = 1,2$. Возможные комбинации: {0,0}, {0,1}, {0,2}, {1,0}, {1,1}, {1,2}, {2,0}, {2,1}, {2,2}.

В соответствии с условием разобъем все возможные комбинации на три группы:

а/ {0,0}; $p_1 = 1/9$;

б/ {0,1}; {1,0}; {1,1}; $p_2 = 3/9$;

в/ {0,2}, {1,2}, {2,0}, {2,1}, {2,2}; $p_3 = 5/9$.

V. $n = 2$; $k = 4$; $a_i = 0,1,2,3$; $i = 1,2$.

а/ {0,0}; $p_1 = 1/16$;

б/ {0,1}, {1,0}, {1,1}; $p_2 = 3/16$;
в/ {0,2}, {1,2}, {2,0}, {2,1}, {2,2}; $p_3 = 5/16$;
г/ {0,3}, {1,3}, {2,3}, {3,0}, {3,1}, {3,2}, {3,3}; $p_4 = 7/16$.

VI. $n = 3$; $k = 3$; $a_i = 0,1,2$; $i = 1,2,3$; $p_1 = 1/27$; $p_2 = 7/27$; $p_3 = 19/27$.

VII. $n = 4$; $k = 3$; $a_i = 0,1,2$; $i = 1,2,3,4$; $p_1 = 1/81$; $p_2 = 15/81$; $p_3 = 65/81$.

VIII. $n = 4$; $k = 4$; $a_i = 0,1,2,3$; $i = 1,2,3,4$; $p_1 = 1/256$; $p_2 = 15/256$; $p_3 = 65/256$; $p_4 = 175/256$.

Очевидно, что в общем случае число комбинаций равно k^n и вероятность появления i-той комбинации в соответствии с условием будет равна

$$p_i = \frac{i^n - (i-1)^n}{k^n}, \quad i = 1,2,\ldots,k. \qquad /2/$$

Выражение /2/ представляет собой вероятность, так как

$$\sum_{i=1}^{k} p_i = \sum_{i=1}^{k} \frac{i^n - (i-1)^n}{k^n} = 1$$

или

$$\sum_{i=1}^{k} [i^n - (i-1)^n] = \sum_{i=1}^{k} i^n - \sum_{i=1}^{k} (i-1)^n = k^n. \qquad /3/$$

Развернув левую часть выражения /3/, получим

$$1^n + 2^n + \ldots + (k-1)^n + k^n - 0^n - 1^n - \ldots - (k-1)^n = k^n. \qquad /4/$$

Сокращая общие члены в левой части /4/, получим равенство правой и левой частей. Это позволяет заключить, что выражение /2/ представляет собой вероятность появления выборки из n элементов с максимальным значением в k-ричной системе счисления.

Следствие. При равномерном распределении значений a_i в выборке из n чисел вероятность появления выборки с максимальным значением зависит от диапазона чисел k, номера числа в выборке i, количества чисел в выборке n и определяется выражением /2/.

Представление выборки. Рассмотрим массив случайных чисел в единичном гиперкубе в R^n.

Разделим гиперкуб на k вложенных гиперколец объемом V /см. рис.1/ и определим координаты точек, ограничивающих гиперкольца на n осях $0X_1, 0X_2, \ldots, 0X_n$.

Первое кольцо ограничивается отрезками $\{(0, x_{11}), (0, x_{21}), \ldots, (0, x_{n1})\}$, и объем его равен

$$V_1 = x_{11}x_{21}\ldots x_{n1} = V.$$

Принимая $x_{11} = x_{21} = \ldots = x_1$, получим

$$V_1 = V = x_1^n. \qquad /5/$$

Второе гиперкольцо ограничивают $\{(x_{11}, x_{12}), (x_{21}, x_{22}), \ldots, (x_{n1}, x_{n2})\}$. Принимая расстояние от начала координат до x_{i2} равным x_2, получим

$$V_2 = x_2^n - V_1 = V. \qquad /6/$$

Из /5/ и /6/ получим

$$x_2^n = 2V. \qquad /7/$$

По аналогии с /5/-/7/ выведем

$$x_i^n = iV. \qquad /8/$$

При $i = k$ и $x_k = 1$ $kV = 1$, а объем элементарного гиперкольца равен

$$V = \frac{1}{k}. \qquad /9/$$

Из /8/ и /9/ получим выражение для вычисления координат точек, ограничивающих произвольное гиперкольцо:

$$x_i = (iV)^{1/n} = (i/k)^{1/n}. \qquad /10/$$

Легко показать, что данная точка гиперкуба будет принадлежать тому гиперкольцу, в пределах координат ограничивающих точек которого будет находиться максимальное из значений координат этой точки.

Вероятность принадлежности данной точки данному гиперкольцу определяется выражением /2/.

Если в /2/ подставить /10/, получим

$$p_i = \frac{1}{k^{n+1}}. \qquad /11/$$

Выражение /11/ определяет вероятность попадания выборки в интервал (x_{i-1}, x_i) равномерно распределенных гиперколец.

Алгоритм программы теста. Примем величину выборки равной n /метрика гиперкуба/. Делим интервал [0,1] на k частей с граничными точками, вычисленными по /10/:

а/ разыгрываем с помощью исследуемого ГСЧ N случайных чисел и выбираем большее из них;

б/ в часть, соответствующую этому значению, добавляем единицу;

в/ повторяем процесс с пункта "а" до набора заданного числа выборок;

г/ приняв за теоретическое значение выражение /9/, вычисляем среднеквадратичное отклонение;

д/ для полученного значения определим уровень значимости χ^2 с (k-1) степенями свободы /9/.

Программа печатает значения χ^2 для исследуемого теста, значения χ^2 для 0,05- и 0,95-уровней значимости с (k-1) степенями свободы, а также уровень значимости исследуемого ГСЧ.

Результаты расчетов и выводы. Для проверки работоспособности теста была проведена работа по анализу ГСЧ, основанного на получении чисел Фибоначчи, который является заведомо неудовлетворительным по критериям теста на монотонность серий из /2/.

Проверка показала, что полученный тест отвергает последовательность Фибоначчи уже после 1000 испытаний.

Дальнейшая проверка ГСЧ для персональных ЭВМ, приводимого в /3/, по предлагаемому равномерному тесту /М-тесту/ и по наиболее мощному из тестов Д.Кнута на монотонность серий /см. /2/, раздел 3.3.2/ показала, что наш тест не уступает по мощности критерию монотонности. Как видно из табл.1, ГСЧ из /3/, имеющий период около 500 тысяч чисел, был забракован М-тестом после выхода за 80 тысяч псевдослучайных чисел, что быстрее, чем с использованием теста Д.Кнута.

Таблица 1. Значения тестов для генератора случайных чисел /3/

1. Для М-теста при k = 32 размерность N = 10, 0,05 - критический уровень Q_{32} = 46,19

Число испытаний /тыс.чисел/	20	40	60	80	100
χ^2_{32}	35,8	21,2	20,5	29,7	111,5

2. Для теста на монотонность серий из /2/ при k=6, размерности N=10 0,05 - критический уровень Q_6=12,6

Число испытаний /тыс.чисел/	20	40	60	80	100
χ^2_6	3,08	5,61	8,31	11,46	13,29

Качество ГСЧ было улучшено методом "возмущения" с помощью засылки в него дробных долей {klg2} через каждые 32767 чисел /максимальная длина слова для мини-ЭВМ/, что также было установлено применением М-теста /см. табл.2/.

Таблица 2. Значения тестов для ГСЧ с использованием метода "возмущения"

1. Для М-теста при k = 32 размерность N = 10, 0,05 - критический уровень Q_{32} = 46,19

Число испытаний /тыс.чисел/	20	40	60	80	100
χ^2_{32}	25,2	32,9	31,7	29,2	32,7

2. Для теста на монотонность серий из /2/ при k = 6, размерности N = 10 0,05 - критический уровень Q_6 = 12,6

Число испытаний /тыс.чисел/	20	40	60	80	100
χ^2_6	2,78	2,07	6,84	5,86	7,19

Кроме того, на ЭВМ БЭСМ-6 был проверен генератор RNDM из стандартной библиотеки мониторной системы "Дубна" /10/. В проводившихся испытаниях N = 100, K = 1000, количество анализируемых выборок - 1000 /общее число анализируемых чисел - 10^6/, $\chi^2_{0,05}$ = 124,34; $\chi^2_{0,95}$ = 77,93; χ^2_{RNDM} = 104,14; уровень значимости Q_{RNDM} = 0,305.

ЛИТЕРАТУРА

1. Ермаков С.М. Метод Монте-Карло и смежные вопросы. М.: Наука, 1975.
2. Кнут Д. Искусство программирования для ЭВМ. М.: Мир, 1977, т.2.
3. Ososkov G.A. Pseudo-random number generators for microcomputers and their applications, Budapest, 1980, p.345-349.
4. Акопов Н.З., Саввиди Г.К., Тер-Арутюнян-Саввиди Н.К. Препринт ЕФИ-867/18/-86, ЦНИИатоминформ, Ереван, 1986.

5. Акишкин П.Г., Ососков Г.А. Препринт ОИЯИ, Р5-8411, Дубна, 1974.
6. Marsaglia G. The structure of linear congruentiel sequences. App. of Number theory to numerical Analysis, Ed.S.K. Zaremba, N.-Y., Acad.Press, 1972.
7. Ososcov G.A. - In: Proc. in Computasional Statistics 6th Symp., Vienna for IASC, Phys.-Verlag, 1982, p.207-208.
8. Кульбак С. Теория информации и статистика. М.: Наука, 1987.
9. Большев Л.Н., Смирнов Н.В. Таблицы математической статистики. М.: Наука, 1965.
10. Мазный Г.Л. Программирование на БЭСМ-6 в системе "Дубна". М.: Наука, 1978.

Рукопись поступила в издательский отдел
16 ноября 1987 года.

Ососков Г.А., Пшенин Е.С., Шандрикова Е. Р11-87-816

Об одном многомерном тесте проверки генераторов случайных чисел

Описана многомерная процедура тестирования равномерного генератора случайных чисел на интервале /0,1/ с экономным использованием вычислительных ресурсов. Тестирование основано на специальном разбиении многомерного единичного куба, сохраняющем постоянным число ячеек разбиения и их объемы. С помощью процедуры выполняется быстрое вычисление адресов ячеек многомерной гистограммы при ее заполнении псевдослучайными числами, а также вычисляет статистические критерии равномерности заполнения. Приведены результаты проверки различных генераторов случайных чисел, в том числе и для микроЭВМ.

Работа выполнена в Лаборатории вычислительной техники и автоматизации ОИЯИ.

Сообщение Объединенного института ядерных исследований. Дубна 1987

Перевод О.С.Виноградовой

Ososkov G.A., Pshenin E.S., Šandrikova E. P11-87-816

On One Multidimensional Test of Random Number Generators

A multidimentional test of the uniformity on (0,1) of a random number generator with the economical utilizing of computing resources is described. The test is based on a special partition of the multidimentional cube which preserves the number of partitioning cells and their volumes to be constant. The procedure realizes a fast computing of adresses of a multidimentional histogram while filling it by random numbers and computes the statistical criteria of the uniformity of this filling. Results of testing the uniformity of different random number generators including those for microcomputers are given.

The investigation has been performed at the Laboratory of Computing Techniques and Automation, JINR.

Communication of the Joint Institute for Nuclear Research. Dubna 1987