УДК 621.37/.39:51-7; 621.37/.39.001.57

Билык Н.М., *к.т.н.;* **Казакова Н.Ф.,** *к.т.н.*

АНАЛИЗ АЛГОРИТМОВ ФОРМИРОВАНИЯ ДАТЧИКОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ С РАВНОМЕРНЫМ РАСПРЕДЕЛЕНИЕМ

Білик Н.М., Казакова Н.Ф. Аналіз алгоритмів формування датчиків псевдовипадкових чисел з рівномірним розподілом. Наводяться результати аналізу алгоритмів формування датчиків псевдовипадкових чисел з рівномірним розподілом. На основі отриманих даних пропонується процедура поліпшення алгоритму, який реалізує мультиплікативний конгруентний метод.

Билык Н.М., Казакова Н.Ф. Анализ алгоритмов формирования датчиков псевдослучайных чисел с равномерным распределением. Приводятся результаты анализа алгоритмов формирования датчиков псевдослучайных чисел с равномерным распределением. На основе полученных данных предлагается процедура улучшения алгоритма, который реализует мультипликативный конгруэнтный метод.

Bilyk N.M., Kazakova N.F. Analysis of uniformly distributed pseudo-random number transducers generating algorithm. Analysis results of uniformly distributed pseudo-random number transducers generating algorithm are given. On the basis of data obtained the procedure for the improvement of multiplicative congruent algorithm is proposed.

Ключевые слова: ДАТЧИК ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ, ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ, ЗАКОН РАСПРЕДЕЛЕНИЯ, КОДОВОЕ РАЗДЕЛЕНИЕ КАНАЛОВ

В настоящее время, принимая во внимание интенсивное развитие систем связи с кодовым разделением каналов, все актуальней становится задача создания новых алгоритмов и технических устройств для формирования псевдослучайних чисел и их последовательностей (ПСП), а также имитационное моделирование, как одно из наиболее эффективных средств исследования сложных систем и процессов [1…3]. Одной из основных процедур при формировании ПСП является выработка последовательности чисел, подчиняющихся заданному закону распределения. Генерирование ПСП (выборка) осуществляется датчиками псевдослучайных чисел. Датчики должны образовывать числовые выборки, достаточно хорошо имитирующие псевдослучайные процессы с заданными законами распределения. Количество псевдослучайных чисел при этом колеблется в достаточно широких пределах: от десятков тысяч для простых задач, до сотен тысяч и более для сложных систем. Поэтому важной задачей является обеспечение быстродействия.

Датчики с заданным законом распределения (например, нормальным, экспоненциальным и т.д.) реализуются обычно программно, и работа их основана на преобразовании последовательности псевдослучайных чисел с равномерным распределением в интервале [0, 1] в ПСП с заданным законом распределения. Поэтому качество и эффективность процедур формирования в значительной мере зависят от свойств используемого датчика равномерно распределенных псевдослучайных чисел [2].

Известны три способа получения псевдослучайных чисел с равномерным распределением в интервале [0; 1]: *табличный, физический, программный.*

Использование при формировании ПСП таблиц псевдослучайных чисел широкого применения не нашло, поскольку, для хранения информации о таблице требуются значительные объемы памяти ЭВМ (или микропроцессора).

Работа физических датчиков, которые выполнены в виде специальной приставки к ЭВМ (отдельного устройства в связном терминале), основана на преобразовании некоторого случайного физического процесса по определенному правилу в псевдослучайные числа с равномерным распределением на интервале [0, 1]. Основным недостатком этого способа является нестабильность вероятностных характеристик случайной величины используемого процесса и невозможность повторного получения одной и той же реализации.

Наиболее предпочтительным, в настоящее время, для задач формирования ПСП

является программный способ. Достоинства этого способа заключаются в следующем:

– использование проверенной выборки псевдослучайных чисел, т.е. выборка с предварительно проверенными статистическими свойствами обладает требуемой стабильностью и не нуждается в периодическом тестировании;

– возможность многократного воспроизведения чисел. Программное генерирование случайных чисел в интервале [0, 1] осуществляется по специальным алгоритмам, когда каждое последующее случайное число получается из предыдущего;

– генерируемая выборка имеет структуру в достаточной степени близкую к структуре равномерной (или квазиравномерной) выборки;

– количество операций, необходимое для выработки каждого числа последовательности, в основном, минимально;

– вычислительный процесс датчика не требует больших объемов памяти;

– запас чисел датчика, в основном, достаточен для реализации моделируемого процесса (т.е. период генерируемой последовательности датчика всегда не меньше моделируемого процесса).

Относительно второго пункта перечисленных достоинств отметим, что поскольку последовательность чисел вычисляется в уравнении детерминированно, числа, естественно, не являются случайными, но по своим статистическим свойствам близки к истинно случайным числам, поэтому такие случайные числа называются *псевдослучайными*.

Цель статьи. Разработанные алгоритмы получения псевдослучайных чисел с равномерным распределением в интервале [0, 1] достаточно просто реализуются программно, однако не все известные датчики подходят к задачам формирования ПСП. Поэтому к датчикам с равномерным распределением (первичные датчики), предназначенных для реализации процессов формирования ПСП, можно предъявить следующие требования:

– генерируемая выборка должна иметь структуру в достаточной степени близкой к структуре равномерной (или квазиравномерной) выборки;

– количество операций, необходимое для выработки каждого числа последовательности, должно быть по возможности минимально;

– вычислительный процесс не должен занимать больших объемов памяти;

– запас чисел датчика должен быть достаточным для реализации формируемого процесса (т.е. период генерируемой последовательности должен быть не меньше этого процесса).

В связи с увеличением масштабов формируемых процессов, который связан с постоянным ростом сложности решаемых задач, соответственно возрастают и требования, предъявляемые к выбору первичных датчиков [2, 5].

Исследование датчиков с равномерным распределением показывает, что подбор генерируемых выборок с требуемыми качественными показателями является непростой задачей и требует довольно больших трудоемких вычислений. С этой точки зрения для пользователей датчиков важны рекомендации по выбору соответствующего алгоритма, учитывающего необходимые параметры. Т.о., ***целью статьи*** является сравнительный анализ наиболее известных алгоритмов датчиков псевдослучайных чисел.

Изложение основного материала

Простейшими алгоритмами получения псевдослучайных чисел (и на их основе – ПСП) являются арифметические процедуры. Примером может служить последовательность цифр разложения в десятичную дробь иррациональных чисел, в частности известных чисел: π=3,14..., $\sqrt{3}$ =1,73…, e=2,17... [6].

Подобные датчики обычно успешно проходят проверку с помощью различных статистических критериев, однако использование их ограничено, так как при вычислении

очередного числа используются все предшествующие числа последовательности, в связи с чем быстро растет число занятых ячеек памяти и увеличивается машинное время.

Некоторое время успехом пользовался алгоритм для получения псевдослучайных чисел, предложенный Дж. Нейманом [6]. Алгоритм называется *методом середины квадратов*. В этом методе *s*-значное число x_1 возводится в квадрат, из полученного числа выбирается *s* цифр в средней его части, которые образуют псевдослучайное число x_2. Аналогичным образом из числа x_2 получают следующее число последовательности и т.д.

В общем виде этот алгоритм можно записать следующим образом:

Пусть x_{n-1} есть *s*-разрядное двоичное число вида $x_{n-1}=p_1 2^{-1}+p_2 2^{-2}+\ldots+p_m 2^{-s}$, где p=0 или 1. Квадрат этого числа имеет вид $x_n^2 = d_1 2^{-1} + d_2 2^{-2} + \ldots + d_{2m} 2^{-2s}$. Выделяем середину полученного числа, считая *s* четным: $x_n = d_{\frac{s}{2}+1} 2^{-1} + d_{\frac{s}{2}+2} 2^{-2} + \ldots + d_{\frac{3}{2}s} 2^{-s}$.

Недостаточно разработанная методика выбора исходных параметров датчика, построенного по методу середины квадратов, требует достаточно трудоемких вычислений по подбору выборки чисел с удовлетворительным качеством. Связано это с тем, что в процессе генерирования датчиком чисел при определенных их значениях статистические свойства последовательности могут начать ухудшаться, а в некоторых случаях она и вовсе вырождается. Например, если в генерируемой последовательности с 2*s*-значными числами, появляется число, у которого *s* старших разрядов имеют нули, то можно заранее прогнозировать, что последующие вырабатываемые числа начнут уменьшаться и в конечном итоге появятся бесконечно повторяющиеся нули, т.е. выборка вырождается.

Модификацией метода середины квадратов является метод середины произведения, который дает значительно лучшие результаты. Алгоритм этого метода следующий:

Два *s*-значных числа x_1 и x_2 перемножаются и берется *s* средних знаков, которые образуют число x_3. Далее перемножаются числа x_2 и x_3 и аналогично получают число x_4 и т.д. В [4, 7] доказано, что этот рекуррентный процесс дает меньшее отклонение образуемых псевдослучайных чисел от равномерного распределения, нежели метод середины квадратов.

Наибольшее распространение на практике получили линейные конгруэнтные методы [4, 6, 7] генерации псевдослучайных чисел с равномерным распределением и формирование на их основе ПСП заданной длины и обладающих заданными свойствами. В общем виде алгоритм таких датчиков реализуется с помощью рекуррентного соотношения:

$$x_{n+1} = \sum_{i=0}^{j} a_i x_{n-1} + c \left(\mathrm{mod}\, M\right), \qquad (1)$$

где: a_0, a_1, ... , a_j, c>1, M>1, а также получаемые числа x_1, x_2, ... являются целыми числами. Модуль M означает: число $A = \sum_{i=0}^{j} a_i x_{n-1} + c$ делится на M; получаемое целое число q и целочисленный остаток x_{n-1}, представляется в виде: $A = qM + x_{n+1};\ 0 \le x_{n-1} \le M-1$.

Так как x_{n+1} – число между 0 и M, то его еще нужно разделить на M, чтобы получить число между 0 и 1: $$R_{n+1} = \frac{x_{n+1}}{M}. \qquad (2)$$

Последовательности, полученные линейными конгруэнтными методами, периодически повторяются. Это связано с тем, что числа x могут принимать только значения 0, 1, 3, ... , M-1. Максимальная длина периода последовательности не может превышать $M=2^m$, поэтому обычно принимают $m=N$, где N – число значащих разрядов для представления целых чисел используемой для генерации ЭВМ (микропроцессора).

Из соотношения (1) можно получить различные модификации линейных алгоритмов датчиков псевдослучайных чисел.

Смешанный конгруэнтный метод генерирования псевдослучайных чисел, предложенный Лемером, мы получим из (1) при $a_1=a_2=$, ..., $=a_j=0$ и приняв $a_0>0$, $c>0$. Тогда:

$$x_{n+1} = ax_n + c \pmod{M}, \quad (3)$$

Усовершенствуем алгоритм, реализующий мультипликативный конгруэнтный метод. Для этого в (1) подставим $c=a_1=a_2=$, ..., $=a_j=0$ и приняв $a_0>0$. В этом случае:

$$x_{n+1} = ax_n + c\,. \quad (4)$$

Качество чисел, вычисляемых по этому алгоритму, хуже, чем в алгоритме (3), но реализующая его программа проще и позволяет вырабатывать числа с более высокой скоростью. Это имеет значение при проведении экспериментов с имитационными моделями, так как уменьшается время прогона.

В датчиках (3) и (4) при M-1, $0<x_0<1$, $0 \le c \le 1$, a – целое положительное число, получаемые псевдослучайные числа лежат в интервале [0; 1], поэтому формула (2) не требуется.

Если в (1) положить $c=a_2=$, ..., $=a_j=0$ и $a_0=a_1=1$, то получим аддитивный датчик псевдослучайных чисел: $x_{n+1} = x_n + x_{n-1} \pmod{M}$. (5)

Обобщением линейного генератора (1) является квадратичный генератор:

$$x_{n+1} = \left(a_1 x_n^2 + a_2 x_n + a_3\right) \pmod{M}.$$

Этот датчик по своим статистическим качествам не превосходит чем-либо датчики (3...5), однако требует большего количества операций для получения одного псевдослучайного числа. С этой точки зрения для задач имитационного формирования предпочтительно использовать линейные генераторы.

Числа c, M, a_0, a_1, …, a_j, x_0 в литературе называют *параметрами датчика*. x_0 – это начальное значение числа, с которого начинается генерирование выборки. Качество генерирования выборки зависит от параметров датчика, поэтому они не могут быть подобраны случайным образом. Правила выбора параметров линейных датчиков рассмотрены в [6]. Однако датчики, с подобранными по соответствующим правилам параметрами, не могут еще гарантировать генерирование последовательности псевдослучайных чисел с требуемым качеством.

Выводы. Усовершенствование алгоритма, который реализует мультипликативный конгруэнтный метод, позволило установить, что качество чисел, вычисляемых по этому алгоритму, хуже, чем в алгоритме (3), но реализующая его программа проще и позволяет вырабатывать числа с более высокой скоростью. Это имеет значение при проведении экспериментов с имитационными моделями, так как уменьшается время прогона.

Литература

1. Апанасович В.В., Тихоненко О.М. Цифровое формирование стохастических систем. – Минск: Университетское, 1986. – 125 с.

2. Корчинский В.В., Филькин К.М. О выборе первичного датчика для задач имитационного моделирования // Моделювання та інф. технології. Збірн. наук. праць ІПМЕ. – 2007. – Вип. 42. – С. 81-90.

3. Гоинштейн А.М. Численное решение задач радиотехники и техники связи на ЭВМ. – М.: Связь, 1972. – 200 с.

4. Голенко Д.И. Формирование и статический анализ псевдослучайных чисел на ЭВМ. – М.: Наука, 1965. – 227 с.

5. Корчинский В.В., Филькин К.М. Анализ моделей первичных датчиков псевдослучайных чисел / Матер. II наук.-практ. семін. молодих науковців та студентства «Сучасні телекомунікаційні та інформаційні технології», 12-14 грудня 2007 р., Київ: УНДІЗ. – С.20-24.

6. Кнут Д. Искусство программирования для ЭВМ. – М.: Мир, 1977. – Т.2. – 726 с.

7. Соболь И.М. Численные методы Монте-Карло. – М.: Наука, 1973. – 327 с.