

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 псевдослучайных 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 связанном 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: $\pi=3,14\dots$, $\sqrt{3}=1,73\dots$, $e=2,71\dots$ [6].

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

очередного числа використовуються всі предшествуючі числа послідовності, в зв'язі з чим швидко росте число зайнятих ячеек пам'яті і збільшується машинне время.

Некотре время успіхом користувався алгоритм для отримання псевдослучайних чисел, запропонований Дж. Найманом [6]. Алгоритм називається *методом середини квадратів*. В цьому методі s -значне число x_1 возводиться в квадрат, з отриманого числа вибирається s цифр в середній його частині, які утворюють псевдослучайне число x_2 . Аналогічним образом з числа x_2 отримують наступне число послідовності і т.д.

В загальному вигляді цей алгоритм можна записати наступним образом:

Пусть x_{n-1} є s -розрядне двоичне число виду $x_{n-1} = p_1 2^{-1} + p_2 2^{-2} + \dots + p_m 2^{-s}$, де $p=0$ або 1 . Квадрат цього числа має вигляд $x_n^2 = d_1 2^{-1} + d_2 2^{-2} + \dots + d_{2m} 2^{-2s}$. Виділяємо середину отриманого числа, вважаючи s парним: $x_n = d_{\frac{s}{2}+1} 2^{-1} + d_{\frac{s}{2}+2} 2^{-2} + \dots + d_{\frac{3s}{2}} 2^{-s}$.

Недостатньо розроблена методика вибору вихідних параметрів датчика, побудованого за методом середини квадратів, вимагає достатньо трудомістких обчислень по підбору вибірки чисел з задовільним якістю. Зв'язано це з тим, що в процесі генерування датчиком чисел при певних їх значеннях статистичні властивості послідовності можуть почати погіршуватися, а в деяких випадках вона і взагалі вироджується. Наприклад, якщо в генеруваній послідовності з $2s$ -значними числами, з'являється число, у якого s старших розрядів мають нулі, то можна заздалегідь прогнозувати, що наступні вироблювані числа почнуть зменшуватися і в кінцевому підсумку з'являться нескінченно повторювані нулі, т.е. вибірка вироджується.

Модифікацією методу середини квадратів є метод середини добутку, який дає значно кращі результати. Алгоритм цього методу наступний:

Два s -значних числа x_1 і x_2 перемножуються і береться s середніх знаків, які утворюють число x_3 . Далі перемножуються числа x_2 і x_3 і аналогічно отримують число x_4 і т.д. В [4, 7] доведено, що цей рекуррентний процес дає менше відхилення отримуваних псевдослучайних чисел від рівномірного розподілу, ніж метод середини квадратів.

Найбільше поширення на практиці отримали лінійні конгруентні методи [4, 6, 7] генерації псевдослучайних чисел з рівномірним розподілом і формування на їх основі ПСП заданої довжини і володіють заданими властивостями. В загальному вигляді алгоритм таких датчиків реалізується з допомогою рекуррентного співвідношення:

$$x_{n+1} = \sum_{i=0}^j a_i x_{n-i} + c \pmod{M}, \quad (1)$$

де: $a_0, a_1, \dots, a_j, c > 1, M > 1$, а також отримувані числа x_1, x_2, \dots є цілими числами.

Модуль M означає: число $A = \sum_{i=0}^j a_i x_{n-i} + c$ ділиться на M ; отримане ціле число q і

цілочисленний залишок x_{n+1} , представляється в вигляді: $A = qM + x_{n+1}; 0 \leq x_{n+1} \leq M - 1$.

Так як x_{n+1} – число між 0 і M , то його ще потрібно розділити на M , щоб отримати число між 0 і 1 :

$$R_{n+1} = \frac{x_{n+1}}{M}. \quad (2)$$

Послідовності, отримані лінійними конгруентними методами, періодично повторюються. Це пов'язано з тим, що числа x можуть приймати тільки значення $0, 1, 2, \dots, M-1$. Максимальна довжина періоду послідовності не може перевищувати $M=2^m$, звичайно приймають $m=N$, де N – число значущих розрядів для представлення цілих чисел, використовуваних для генерації ЕВМ (мікропроцесора).

З співвідношення (1) можна отримати різні модифікації лінійних алгоритмів датчиків псевдослучайних чисел.

Смешанный конгруэнтный метод генерирования псевдослучайных чисел, предложенный Лемером, мы получим из (1) при $a_1=a_2=, \dots, =a_j=0$ 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 $c=a_1=a_2=, \dots, =a_j=0$ 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 $M-1, 0<x_0<1, 0\leq c\leq 1, a$ – целое положительное число, получаемые псевдослучайные числа лежат в интервале $[0; 1]$, поэтому формула (2) не требуется.

Если в (1) положить $c=a_2=, \dots, =a_j=0$ и $a_0=a_1=1$, то получим аддитивный датчик псевдослучайных чисел:

$$x_{n+1} = x_n + x_{n-1} \pmod{M}. \quad (5)$$

Обобщением линейного генератора (1) является квадратичный генератор:

$$x_{n+1} = (a_1x_n^2 + a_2x_n + a_3) \pmod{M}.$$

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 $c, M, a_0, a_1, \dots, a_j, x_0$ 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. Горинштейн 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. Соболев И.М. Численные методы Монте-Карло. – М.: Наука, 1973. – 327 с.